



This is the accepted manuscript made available via CHORUS. The article has been published as:

Quantum repeaters: From quantum networks to the quantum internet

Koji Azuma, Sophia E. Economou, David Elkouss, Paul Hilaire, Liang Jiang, Hoi-Kwong Lo, and Ilan Tzitrin

Rev. Mod. Phys. **95**, 045006 — Published 20 December 2023

DOI: [10.1103/RevModPhys.95.045006](https://doi.org/10.1103/RevModPhys.95.045006)

Quantum repeaters: From quantum networks to the quantum internet

Koji Azuma,^{1,2,*} Sophia E. Economou,^{3,†} David Elkouss,^{4,5,‡} Paul Hilaire,^{3,6,§} Liang Jiang,^{7,¶} Hoi-Kwong Lo,^{8,9,10,**} and Ilan Tzitrin^{11,††}

¹*NTT Basic Research Laboratories,
NTT Corporation,
3-1 Morinosato Wakamiya,
Atsugi, Kanagawa 243-0198,
Japan*

²*NTT Research Center for Theoretical Quantum Physics,
NTT Corporation,
3-1 Morinosato-Wakamiya,
Atsugi, Kanagawa 243-0198,
Japan*

³*Department of Physics, Virginia Tech,
Blacksburg, Virginia 24061,
USA*

⁴*QuTech, Delft University of Technology,
Lorentzweg 1, 2628 CJ Delft,
The Netherlands*

⁵*Networked Quantum Devices Unit,
Okinawa Institute of Science and Technology Graduate University, Okinawa,
Japan*

⁶*Quandela SAS, 10 Boulevard Thomas Gobert,
91120, Palaiseau,
France*

⁷*Pritzker School of Molecular Engineering,
The University of Chicago,
Chicago, Illinois 60637,
USA*

⁸*Quantum Bridge Technologies, Inc.,
100 College Street,
Toronto, ON M5G 1L5,
Canada*

⁹*Department of Physics,
University of Hong Kong, Pokfulam,
Hong Kong*

¹⁰*Center for Quantum Information and Quantum Control,
Department of Physics and Department of Electrical & Computer Engineering,
University of Toronto,
M5S 3G4 Toronto Canada*

¹¹*Department of Physics,
University of Toronto, Toronto,
Canada*

(Dated: July 20, 2023)

A quantum internet is the holy grail of quantum information processing, enabling the deployment of a broad range of quantum technologies and protocols on a global scale. However, numerous challenges exist before the quantum internet can become a reality. Perhaps the most crucial of these is the realization of a quantum repeater, an essential component in the long-distance transmission of quantum information. As the analog of a classical repeater, extender, or booster, the quantum repeater works to overcome loss and noise in the quantum channels comprising a quantum network. Here, we review the conceptual frameworks and architectures for quantum repeaters, as well as the experimental progress towards their realization. We also discuss the various near-term proposals to overcome the limits to the communication rates set by point-to-point quantum communication. Finally, we overview how quantum repeaters fit within the broader challenge of designing and implementing a quantum internet.

* koji.azuma@ntt.com

† economou@vt.edu

CONTENTS

I. Introduction	2	B. Quantum networks	50
II. Preliminaries	6	1. Elements of a quantum network	50
A. Qubits	6	2. Network architecture	50
B. Quantum no-cloning theorem	8	C. The fundamental limits of communications over network	50
C. Entanglement	8	1. An abstract depiction of networks	51
1. Definition and properties	8	2. Quantum network capacities	52
2. Entanglement in bipartite states	8	3. Entanglement based upper bounds	53
D. Entanglement in multipartite states	9	4. Application of the upper bounds to linear networks	54
1. Graph states	9	5. Capacity lower bounds via the aggregated repeater protocol	55
E. Photonic encodings	10	6. Computability of the network capacities	56
III. Quantum repeaters	12	VII. Concluding remarks	56
A. Repeater primitives	12	Acknowledgments	58
1. Quantum teleportation	13	References	58
2. Entanglement swapping	13		
3. Idealized quantum repeaters	13		
4. Tools for error suppression	15		
B. Generations of quantum repeaters	17		
1. First-generation repeaters	18		
2. Second-generation repeaters	21		
3. Third-generation repeaters	22		
4. Comparison of three generation of QRs	23		
C. All-optical repeaters	24		
1. Original all-photonic repeaters	24		
2. Other optical repeaters	26		
3. Repeater graph state generation	27		
IV. Milestones: Outperforming point-to-point optical communication	31		
A. Adaptive measurement-device-independent QKD	31		
1. Memory-assisted implementation	32		
2. All-optical implementation	33		
3. Challenges	34		
B. Twin-field QKD	34		
C. The single sequential quantum repeater	37		
D. Post-pairing measurement-device-independent QKD	37		
V. Experimental progress towards repeaters	38		
A. Long-lived quantum memories	38		
B. Emission of photons entangled with the quantum memory	40		
C. Distant entanglement generation	41		
D. Entanglement distillation	42		
E. Multi-qubit quantum registers and error correction	42		
F. Loss mitigation, quantum frequency conversion, and photonic source efficiency	43		
G. Progress towards memoryless quantum repeaters	44		
H. Experimental realization of quantum networks	45		
1. Trusted large-scale repeater networks	45		
2. Proof-of-concept of a quantum repeater	46		
3. Untrusted quantum networks	47		
VI. Quantum internet	48		
A. Applications of the quantum internet	48		
1. A set of representative communication tasks	48		
2. Stages of the quantum internet	49		

I. INTRODUCTION

Following its rapid growth this century, the Internet has become an invaluable socioeconomic fixture, inextricable from almost all facets of day-to-day life. Access to a high-speed internet—the ability to send and receive digital information across the globe at almost the speed of light—has transformed from a luxury to a utility. However, the current Internet is not sustainable and scalable without future innovation (Leon-Garcia and Steenstrup, 2021). It has been estimated in 2022 there are currently 7 billion connected IoT (Internet of Things) devices online. This number is projected to increase to 25.4 billion by 2030 (Howarth, 2021). As the number of devices increases exponentially over time, the energy consumption in optical communication also grows exponentially, thereby contributing to climate change. The amount of local computing power needed to monitor and control network traffic also grows exponentially. The task of service and network management is thus becoming more and more complex. To move things forward, new concepts such as distributed intelligence and distributed trust (e.g. blockchain) are probably needed. On the other hand, on the longer term, it is widely recognized that a quantum internet and distributed quantum computing will complement the classical internet. The quantum internet will be provably secure and could provide exponentially more computational power and sensing capability to specific tasks.

Indeed, analogously to this Internet, a new system is steadily emerging in theoretical literature and early experiment: the quantum internet (Kimble, 2008), a means of transmitting quantum information globally. While serving a different purpose from the classical Internet, this new paradigm may prove disruptive in its own way. We dedicate this review to the progress that has been made in designing and building the quantum internet, focusing largely on its main building block, quantum repeaters. In addition to the basic theoretical concepts

[‡] d.elkousscoronas@tudelft.nl

[§] paul.hilaire@quandela.com

[¶] liang.jiang@uchicago.edu

^{**} hklo@ece.utoronto.ca

^{††} itzitrin@physics.utoronto.ca

required to understand the components of the quantum internet, we survey its more technical architectural requirements as well as the experimental advances towards its implementation.

While classical information is often encoded digitally—as sequences of 0s and 1s, usually represented in electronic signals—it can also be housed in quantum mechanical states, which abide by different rules. The quantum states encoding the bits 0 and 1, mathematically represented by vectors and denoted by $|0\rangle$ and $|1\rangle$ (the *computational-basis* states), can correspond to a variety of physical systems. Among the most popular and useful quantum information carriers is light—the state of the electromagnetic field associated with one or multiple photons.

Unlike the analogous classical states, quantum states can be superposed like waves. For instance, equal combinations of $|0\rangle$ and $|1\rangle$ include $|+\rangle \equiv \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|-\rangle \equiv \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$, the *conjugate-basis* states. Measuring a conjugate-basis state in the computational basis collapses the superposition, resulting in $|0\rangle$ or $|1\rangle$ at random with equal probability, a manifestation of a more general postulate of quantum mechanics known as Born’s rule. The fact that the outcome of this measurement is probabilistic rather than deterministic is predicted by Heisenberg’s uncertainty principle.

In addition to quantum superposition, Born’s rule, and Heisenberg’s uncertainty principle, the formalism of quantum mechanics allows for subtle quantum correlations—dubbed *entanglement*—to exist between remote physical systems. For instance, two distant photons that are entangled may be in a so-called singlet state $\frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$, which can exhibit stronger-than-classical correlations upon measurement. Not only is it impossible to describe independently the state of each photon in the singlet, but when measured along any common axis, the two photons always show opposite results. According to Schrödinger, entanglement is the essence of quantum theory, but it is far from a theoretical curiosity. The existence of non-classical correlations associated with entangled states has been proven in several experiments via Bell tests (Brunner *et al.*, 2014; Miller, 2016), which has led three experimental physicists—Alain Aspect, John Clauser, and Anton Zeilinger—to be awarded the Nobel Prize in Physics in 2022. Furthermore, in the last few decades, researchers have shown that entanglement is a powerful resource in quantum information processing, enabling many unusual applications that are impossible or impractical with only classical resources.

The quantum technologies enabled by our continuously evolving ability to understand, generate, manipulate, and entangle delicate quantum systems are the premise behind what is commonly referred to the Second Quantum Revolution (Berry, 1998; Dowling and Milburn, 2003). In the First Quantum Revolution, which occurred in the

last century, lasers and transistors—devices built upon the underlying principles of quantum mechanics—played a crucial part in global economic growth. Now, we are already able to demonstrate primitives or complete protocols for the quintessential applications of quantum information: *quantum cryptography*—unconditionally secure communication between parties—and *quantum computation*—a method for exceeding the best-known scaling of certain classes of classical algorithms.

These and other quantum information tasks can be accessed remotely if embedded within a quantum internet—a global network of quantum information processors, namely sources of quantum states, executors of quantum gates, and devices for quantum measurements (van Dam, 2020; Wehner *et al.*, 2018). Such a network can also provide secure access and enhance the performance of these applications of quantum information.

The security underlying the classical Internet is based on computational conjectures, which makes it vulnerable to hacking and eavesdropping. A quantum computer poses a threat to the contemporary cryptosystem because Shor’s factoring algorithm (Shor, 1997) offers a way to break standard public-key encryption schemes, including RSA, Diffie-Hellman, and elliptic curve cryptosystems within short timescales. Owing to the extensive experimental progress in quantum computing in the last few decades, its threat is now widely acknowledged by many governments and organizations (NIST, 2021). While certain classical solutions have been proposed to counter the threat, such as post-quantum cryptographic systems, these are still only conjectured to be secure against quantum attacks. Indeed, three candidate post-quantum crypto-systems in the NIST competition have already been cracked easily by a PC (Townsend, 2022). In reality, quantum key distribution (QKD) is the only known way to allow the unconditionally secure transmission of information—that is, a security founded in tested laws of physics and mathematical proofs (Bennett and Brassard, 2014; Curty *et al.*, 2021; Ekert, 1991; Xu *et al.*, 2020). However, commercialized fiber-based point-to-point QKD is limited to a distance of less than 400 km, whereas satellite-to-ground QKD, intended to extend the communication distances, requires expensive components such as satellites and large telescopes. The quantum internet promises to significantly extend the range of QKD and other cryptographic protocols, thereby securing global communication and transactions.

In particular, a quantum internet will permit secure access to cloud-based quantum computing. Major IT firms such as Google, IBM, Intel, Microsoft, Amazon, and Alibaba are actively constructing their own quantum processors on the way to universal, scalable, and fault-tolerant quantum computers. These companies are working towards this goal alongside dedicated quantum-computing startup companies, which belong to a newly-forming ecosystem of quantum startups. Companies such

as IBM¹ have already put small-scale quantum processors online for external access (Castelvecchi, 2017). The history of conventional computers suggests that the first few years in quantum computing epoch will see only a few large-scale quantum computers in the world. This means that users will have to engage with the devices through classical or quantum networks. With the help of innovative protocols for blind quantum computing (Broadbent *et al.*, 2009), a future quantum internet will allow users to submit their jobs anywhere in the world privately and securely.

Quantum networking is also a crucial ingredient in distributed quantum computing, which allows separate quantum computers to cooperate on an algorithm. At their early stages, quantum processors will be limited in size and complexity; to achieve greater computing power, they will likely need to be networked through quantum channels, with quantum information flowing between them. In this way, quantum networking is important even for short-distance communication between quantum computers. Other protocols enabled or improved by the quantum internet include quantum teleportation (Bennett *et al.*, 1993), quantum fingerprinting (Buhrman *et al.*, 2001), quantum sensing, clock synchronization (Jozsa *et al.*, 2000; Komar *et al.*, 2014), and the linking of distant optical telescopes for sharper images (Gottesman *et al.*, 2012).

Conceptually, it is known that sending quantum information (i.e., qubits) can lower the amount of required communication in distributed information processing tasks, in comparison to sending classical information (bits). The study of the amount of required quantum communication is called quantum communication complexity (Brassard, 2003). Incidentally, the classical communication cost required in quantum information processing is also an important subject (Lo, 2000).

Building a quantum internet requires harnessing quantum states of light. Even in the far future, the photon—or a state of multiple photons—will likely be the information carrier of choice in quantum communication, as it can function as a “flying” qubit (as opposed to matter-based qubits, which are fixed in space) while minimally interacting with its environment. By encoding information in photonic degrees of freedom, quantum information can be transmitted through optical fibers or in free space over long distances with little decoherence.

Despite the advantages of light, there is enough absorption and scattering of photons in the media where they propagate—processes that lead to optical attenuation—that make loss the key physical hurdle in the construction

of a quantum internet. In a standard single-mode optical fiber, close to the standard telecommunication wavelength of 1550 nm, the attenuation is 0.2 dB/km (The Fibre Optic Association, 2019). This means 1 of every 100 photons survives a journey of 100 km on average. Recently, ultra-low-loss (ULL) optical fibers have been commercialized with a loss as low as 0.15 dB/km (Corning[®], 2021). These sorts of losses in optical channels yield fundamental limits to the rate at which two parties can establish a secret key with a point-to-point QKD protocol, given by TGW bound (Takeoka *et al.*, 2014a) and PLOB bound (Pirandola *et al.*, 2017), and discussed in more detail in Secs. IV and VI.

Nevertheless, quantum networks based on such point-to-point QKD links have already been built all over the world. Examples of ground-based fiber networks include the Tokyo QKD network in Japan (Sasaki *et al.*, 2011), the SECOQC network in Europe (Peev *et al.*, 2009), the 2000 km Shanghai-Beijing network in China (Chen *et al.*, 2021b), and the Euro QCI network by the 27 EU member states (Eur, 2022). Additionally, ground-to-satellite quantum transmission has been performed over thousands of kilometers of free space. This line of research has demonstrated that long-distance quantum communication in a global length scale is feasible with current satellite technology (see (Chen *et al.*, 2021b)). Several theoretical papers envisioned a satellite-based quantum repeater network (Boone *et al.*, 2015; Gündoğan *et al.*, 2021; Khatri *et al.*, 2021). However, because their foundation is point-to-point QKD, existing quantum networks rely on trusted relay nodes to achieve information-theoretically secure communication. In these nodes, optical signals are measured to yield a classical output, and then new optical signals are generated and sent out. This classical output is vulnerable to hacking and eavesdropping, meaning security is only achieved if the nodes can be trusted.

The architectural challenge of a long-distance quantum network is therefore to overcome the fundamental limit of point-to-point quantum communication, achieving high-rate secure communication without using trusted relay nodes. Unfortunately, conventional signal boosters, repeaters, extenders or amplifiers do not work for quantum signals because of the famous quantum no-cloning theorem (Dieks, 1982; Wootters and Zurek, 1982), which states that an unknown quantum state cannot be copied reliably. However, it is still possible to combat loss and noise without cloning quantum states; this is achieved with the help of quantum repeaters.

In quantum repeater protocols, instead of sending quantum signals (photons) directly from one user to another, a sequence of intermediate nodes are set up. There, certain strategies can be used to combat errors induced by losses and other forms of noise, including entanglement distillation and purification, and quantum error detection and correction. While practical quan-

¹ This was followed by other companies—including ionQ, Quantinuum, Quandela, and Xanadu—proposing cloud accessible platforms based on either ion traps or photonics, potentially more promising platforms for remote access using quantum channels.

Reference	Topic
(Sangouard <i>et al.</i> , 2011)	Quantum repeaters based on atomic ensembles and linear optics
(Reiserer and Rempe, 2015)	Cavity-based quantum networks with single atoms and optical photons
(Heshami <i>et al.</i> , 2016)	Quantum memories and applications
(Atatüre <i>et al.</i> , 2018)	Material platforms for spin-based photonic quantum technologies
(Awschalom <i>et al.</i> , 2018)	Quantum technologies with optically interfaced solid-state spins
(Ruf <i>et al.</i> , 2021)	Quantum networks based on color centers in diamond
(Munro <i>et al.</i> , 2015)	Primitives of quantum repeaters
(Muralidharan <i>et al.</i> , 2016)	Generations of quantum repeaters
(Kimble, 2008)	Introductory work to the quantum internet
(Wehner <i>et al.</i> , 2018)	Developmental stages of the quantum internet
(Xu <i>et al.</i> , 2015)	Measurement-device-independent quantum cryptography
(Xu <i>et al.</i> , 2020)	Realistic QKD
(Broadbent and Schaffner, 2016)	Quantum cryptography beyond QKD
(Fitzsimons, 2017)	Blind quantum computing
(Pirandola <i>et al.</i> , 2020)	Advances in quantum cryptography
(Azuma <i>et al.</i> , 2021)	Tools for quantum network design

TABLE I Related review articles.

tum repeaters are not possible with existing technology, research towards this goal is active and involves many different fields of inquiry. Several matter-based systems exist to facilitate their implementation, including atomic ensembles, which can function as quantum memories; quantum dots, which can be used as on-demand sources of a host of photonic states; and cavity QED, which can be used to enhance light-matter interactions. Since photons are often used as flying qubits and quantum memories often involve matter, the quantum interface between light and matter is regarded as a key ingredient in quantum repeaters.

In addition to the many subfields of physics involved in the effort to build quantum repeaters, the pursuit of a quantum internet more generally is an interdisciplinary theoretical and experimental endeavor involving mathematicians, computer scientists, and engineers. Classical tools from network topology, protocol design, information theory, and error correction, in addition to topics within quantum information, e.g., state preparation, quantum channels and measurements, and quantum error correction, are all needed for investigations into the quantum internet.

Several of the topics discussed in this work have been the focus of—or at least have gotten a mention in—previous reviews. We build on this body of work while discussing newer theoretical and experimental developments to keep pace with the dynamic field of quantum communication. For instance, the review (Sangouard *et al.*, 2011) chiefly covers quantum repeaters whose memories are implemented with atomic ensembles, while Ref. (Munro *et al.*, 2015) focuses on the primitives

used in quantum repeaters. Reference (Muralidharan *et al.*, 2016) (and Ref. (Munro *et al.*, 2015) also) categorizes quantum repeater protocols into relevant generations which differ in performance and technological requirements. In our review, we revisit this categorization, sorting repeaters based on the associated mechanisms for suppressing losses and errors. This gives us a more natural structure to understand newly emerging classes of repeaters, notably memoryless, error-corrected, and all-photonic repeaters, which have not been extensively featured in reviews. In addition to our discussion of full-fledged repeaters, we dedicate a portion of our review to simpler protocols believed to be sufficient to beat repeaterless bounds, an important milestone for long-distance quantum communication. Reference (Xu *et al.*, 2020) already tackles some of these ideas with an approach centered around their security in realistic implementations; in our work, we focus on performance, chiefly in terms of key distribution metrics. References (Kimble, 2008; Wehner *et al.*, 2018) review the progress towards the realization of the quantum internet. Notably, Reference (Wehner *et al.*, 2018) introduces stages of development for the quantum internet, aligning with applications that grow in technological complexity. Here, we continue this discussion but additionally introduce an information-theoretic framework to derive fundamental limits of quantum communication over a quantum network, with views different from Refs. (Pirandola *et al.*, 2020) and (Azuma *et al.*, 2021). In Table I, we provide a list of the reviews just mentioned together with other works on applications of quantum communication that are not covered here.

The rest of this review is organized as follows. In Secs. II and III.A, we present the preliminaries required to understand quantum repeaters and the physics behind the quantum internet. In Sec. III.B, we overview the conceptual frameworks of quantum repeaters and use them to organize the existing proposals. In Sec. III.C we discuss an important class of memoryless repeaters that intersect with the latest generations of theoretical proposals. In Sec. IV, we review various near-term protocols, such as an adaptive version of measurement-device-independent QKD (Lo *et al.*, 2012) and twin-field QKD (Lucamarini *et al.*, 2018), which are regarded as milestones in the path to outperforming the PLOB bound en route to quantum repeaters. In Sec. V, we describe experimental advances towards optical-fiber-based quantum communication schemes featuring quantum repeaters. Section VI is dedicated to a discussion on the quantum internet, including the quantum/private capacities of quantum internet protocols and upper bounds on the capacities. Some concluding remarks are provided in Sec. VII.

For clarity, we present the list (Table II) of abbreviations that are used throughout the review.

II. PRELIMINARIES

In this section, we summarize relevant background concepts, including qubits, entanglement, and possible photonic encodings. Repeater primitives—including teleportation and entanglement swapping—are left to Sec. III.A. Standard references, including (Nielsen and Chuang, 2010), can be used to supplement this part of the review.

A. Qubits

A *qubit*—the quantum mechanical analog of the classical bit and the fundamental unit of quantum information—is another name for a two-dimensional complex Hilbert space. A pure state $|\psi\rangle$ of any qubit can be written in the computational basis through

$$|\psi\rangle = a|0\rangle + b|1\rangle, \quad (1)$$

where $a, b \in \mathbb{C}$ and $|a|^2 + |b|^2 = 1$. Setting $a = \frac{1}{\sqrt{2}}$ and $b = \pm \frac{1}{\sqrt{2}}$ gives states in the conjugate basis:

$$|\pm\rangle \equiv \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle). \quad (2)$$

In quantum mechanics, the global phase of a state is irrelevant; thus, one can parametrize any pure qubit through two parameters, $a = \cos \frac{\theta}{2}$ and $b = e^{i\phi} \sin \frac{\theta}{2}$, revealing its Bloch sphere representation, illustrated in Fig. 1, where θ and ϕ are the polar and azimuthal angles, respectively. A qubit is realized experimentally by associating it with a

Abbreviation	Meaning
BBSM	Boosted Bell State Measurement
BDCZ	Briegel-Dür-Cirac-Zoller
BM/BSM	Bell (State) Measurement
CPTP	Completely Positive and Trace-Preserving
CSS	Calderbank-Shor-Steane
CTSL	Childress-Taylor-Sørensen-Lukin
CV	Continuous Variable
DLCZ	Duan-Lukin-Cirac-Zoller
DV	Discrete Variable
EG	Entanglement Generation
ES	Entanglement Swapping
GBS	Gaussian Boson Sampling
GHZ	Greenberger-Horne-Zeilinger
GKP	Gottesman-Kitaev-Preskill
HEGP	Heralded Entanglement Generation Protocol
LHC	Large Hadron Collider
LIGO	Laser Interferometer Gravitational-Wave Observatory
LOCC	Local Operations and Classical Communication
MBQC	Measurement-Based Quantum Computing
MDI	Measurement Device Independent
MIT	Massachusetts Institute of Technology
NISQ	Noisy Intermediate Scale Quantum
NIST	National Institute for Standards in Technology
NV	Nitrogen Vacancy
PBS	Polarizing Beamsplitter
PLOB	Pirandola-Laurenza-Ottaviani-Banchi
PNR	Photon-Number-Resolving Detector
PRCS	Phase-Randomized Coherent State
EuroQCI	European Quantum Communication Infrastructure
QD	Quantum Dot
QED	Quantum Electrodynamics
QKD	Quantum Key Distribution
QM	Quantum Memory
QND	Quantum Non-Demolition
QR	Quantum Repeater
RGS	Repeater Graph State
RSA	Rivest-Shamir-Adleman
SECOQC	Secure Communication based on Quantum Cryptography
SNSPD	Superconducting Nanowire Single Photon Detector
SPD	Single Photon Detector
SPDC	Spontaneous Parametric Downconversion
SW	(Optical) Switches
TF-QKD	Twin-Field Quantum Key Distribution
TGW	Takeoka-Guha-Wilde
ULL	Ultra Low Loss

TABLE II Abbreviations used in this review.

two-dimensional space or subspace of a physical system. Although we will encounter matter (chiefly spin) qubits in this review, we are particularly interested in encodings into photonic systems, which we survey in Sec. II.E.

Interactions with the environment or preparation errors can diminish the purity of a qubit—that is, introduce

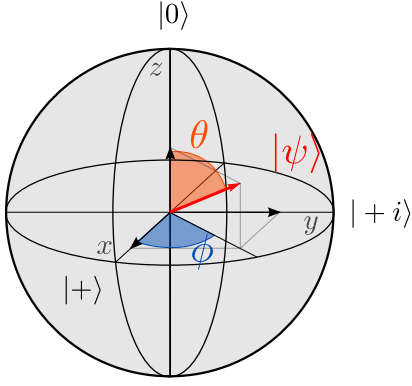


FIG. 1 The Bloch sphere representation of a qubit. The (x, y, z) -components of a Bloch vector (displayed as an arrow) give the expectation values of the Pauli observable X , Y , and Z . For instance, points $(0, 0, 1)$, $(1, 0, 0)$, and $(0, 1, 0)$ correspond to eigenstates $|0\rangle$, $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$, and $|+i\rangle = (|0\rangle + i|1\rangle)/\sqrt{2}$ of Pauli operators Z , X , and Y with the eigenvalue of $+1$, respectively.

classical uncertainty. In this case, we must turn to a representation of the qubit as a statistical mixture of pure quantum states. The general description of a state, which include *mixed states*, is as a positive operator ρ with unit trace, called a *density operator*. The density operator of a pure state $|\psi\rangle$ is $\rho = |\psi\rangle\langle\psi|$ with $\text{Tr}[\rho^2] = 1$, while a density operator ρ with $\text{Tr}[\rho^2] < 1$ describes a mixed state. In the case of a qubit, it can be written as

$$\rho = \rho_{00} |0\rangle\langle 0| + \rho_{01} |0\rangle\langle 1| + \rho_{10} |1\rangle\langle 0| + \rho_{11} |1\rangle\langle 1|, \quad (3)$$

where the *populations*, ρ_{00} and ρ_{11} , are real and add to unity ($\rho_{00} + \rho_{11} = 1$), the *coherences*, ρ_{01} , and ρ_{10} , are complex conjugates ($\rho_{01} = \rho_{10}^*$), and $\det[\rho] = \rho_{00}\rho_{11} - \rho_{01}\rho_{10} \geq 0$.

Unitary transformations—operators U with $U^\dagger U = U U^\dagger = \mathbb{1}$ —describe reversible, probability-preserving operations on qubits, i.e., *quantum gates*. The *Pauli gates* are defined through

$$X = |0\rangle\langle 1| + |1\rangle\langle 0|, \quad (4)$$

$$Y = -i|0\rangle\langle 1| + i|1\rangle\langle 0|, \quad (5)$$

$$Z = |0\rangle\langle 0| - |1\rangle\langle 1|. \quad (6)$$

X , Z , and Y effect a phase flip, a bit flip, and a combination of the two on the qubit, respectively. A unitary U is *Clifford* if it maps any Pauli gate P to a Pauli gate under conjugation, that is, $U P U^\dagger$ is also a Pauli gate. An example of a non-Pauli Clifford gate is the *Hadamard gate*, defined by

$$H = \frac{1}{\sqrt{2}}(|0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| - |1\rangle\langle 1|). \quad (7)$$

An example of a non-Clifford gate is the $\frac{\pi}{8}$ or T gate, given through

$$T = |0\rangle\langle 0| + e^{i\pi/4} |1\rangle\langle 1|. \quad (8)$$

The above discussion is generalizable to systems of multiple qubits by taking tensor products; see Sec. II.C.

A *measurement* process on a quantum system in a state ρ is, in general, described by a set of Kraus (linear) operators $\{M_i\}_i$ satisfying $M_i^\dagger M_i = \mathbb{1}$. Performing the associated measurement results in an outcome i with probability $p_i = \text{Tr}[M_i^\dagger M_i \rho]$ and leaves the state in $M_i \rho M_i^\dagger / p_i$. This is a formalization and generalization of Born's rule. For the particular case of a (destructive) Pauli measurement on a qubit, we may associate $M_0 = \langle v_0|$ and $M_1 = \langle v_1|$ with the eigenstates $|v_0\rangle$ and $|v_1\rangle$ of the corresponding operator; *Z-basis measurements* (corresponding to the Pauli Z) are specified by the Kraus operators $\{|0\rangle, |1\rangle\}$, while *X-basis measurements* (corresponding to the Pauli X) are specified by the Kraus operators $\{|+\rangle, |-\rangle\}$.

We also consider a *quantum channel*, \mathcal{N} , which deterministically converts a given state ρ into a state σ . This kind of transformation is useful to describe the actions of noise and transmission channels on quantum systems. Any quantum channel has an operator-sum representation, $\sigma = \mathcal{N}(\rho) = \sum_i M_i \rho M_i^\dagger$, specified by a set of Kraus operators $\{M_i\}_i$. Another representation is

$$\sigma_{A'} = \mathcal{N}_{A \rightarrow A'}(\rho_A) = \text{Tr}_{E'}[U_{AE}(\rho_A \otimes |0\rangle\langle 0|_{E'})U_{AE}^\dagger], \quad (9)$$

where U_{AE} is a unitary operator acting on system $\mathcal{H}_A \otimes \mathcal{H}_E$ and $|0\rangle_{E'}$ is a state of an auxiliary system (environment) E . The map \mathcal{N} must be completely positive and trace-preserving (CPTP).

Three examples of common qubit errors described by channels are *phase-flip*, *bit-flip*, and *depolarizing* noise, respectively written as

$$\mathcal{N}(\rho) = (1-p)\rho + pZ\rho Z, \quad (10)$$

$$\mathcal{N}(\rho) = (1-p)\rho + pX\rho X, \quad (11)$$

$$\mathcal{N}(\rho) = (1-p)\rho + \frac{p}{3}(X\rho X + Y\rho Y + Z\rho Z), \quad (12)$$

where $0 \leq p \leq 1$ corresponds to an error probability or channel strength. A *pure-loss bosonic channel* is written by defining the action of U_{AE} in Eq. (9) as

$$U_{AE} a_A U_{AE}^\dagger = \sqrt{\eta} a_{A'} + \sqrt{1-\eta} a_{E'} \quad (13)$$

in the Heisenberg representation. Here a_X is the annihilation operator on bosonic system X , $0 \leq \eta \leq 1$ is the transmittance of the channel, and $|0\rangle_{E'}$ of Eq. (9) is the vacuum state of the bosonic system E . The pure-loss bosonic channel is used as a model for an optical fiber: in this case, the transmittance η is related to the length L of the fiber through $\eta = e^{-L/L_{\text{att}}}$, with a constant L_{att} denoting the attenuation distance.

B. Quantum no-cloning theorem

The quantum *no-cloning theorem* (Dieks, 1982; Wootters and Zurek, 1982) entails that it is impossible to create a copy of unknown quantum states. More precisely, given an unknown state $|\psi\rangle_A$, the theorem states that there exists no deterministic quantum operation that can copy $|\psi\rangle_A$ onto system B to obtain $|\psi\rangle_A \otimes |\psi\rangle_B$. Originally demonstrated for pure states, the no-cloning theorem has later been extended to mixed states through the *no-broadcasting theorem* (Barnum *et al.*, 1996). This no-go theorem has profound implications—helpful and unhelpful—for quantum information technologies. While it is at the core of the security of quantum key distribution (Bennett *et al.*, 1992; Koashi and Imoto, 1998, 2002), it also precludes building quantum repeaters analogously to classical signal extenders and furthermore creates challenges in the design and performance of quantum error-correcting codes. For example, the no-cloning theorem makes it impossible to use a classical-like repetition code to correct for errors acting on quantum states, and implies an upper bound of 50% on the loss that any quantum error-correcting code can tolerate. This directly impacts the performance of quantum repeater protocols based on quantum error correction, as addressed in Sec. III.A.4.

C. Entanglement

Here we present the formal definition of entanglement and introduce several important classes of entangled states.

1. Definition and properties

Entanglement—per Schrödinger, a defining feature of quantum theory (Schrödinger, 1935)—refers to the impossibility of describing certain composite quantum states through independent specifications of their constituents. The existence of entanglement, as guaranteed by the formalism and postulates of quantum theory and confirmed by many experiments, has profound physical and metaphysical repercussions, as exemplified famously by Einstein, Podolsky and Rosen (EPR) (Einstein *et al.*, 1935) and by Bell (Bell, 1964), and since then by numerous physicists investigating its repercussions on increasingly rigorous footing. There are several equivalent formulations of entanglement—see, e.g., (Horodecki *et al.*, 2009). A useful one for our purpose is the view of entanglement as a resource for quantum information tasks. Entanglement plays a central role in virtually every primitive and application of quantum information; for us, its most relevant uses are for the protocols we describe in Sec. III.A: quantum teleportation and en-

tanglement swapping, entanglement purification and distillation, and quantum error correction, all of which underlie quantum repeaters. As a non-trivial resource with respect to local operations and classical communication (LOCC), entanglement cannot be increased by performing local operations (including local quantum gates and measurements), classical communication (including adaptive schemes based on classical outputs from other parties), or the combination of both. One may establish quantum entanglement by interacting systems via coupling Hamiltonians, physically distributing entangled states between parties (such as by sending photons over fiber channels), or performing collective measurements of observables from different parties. The entanglement generation process depends on the details of the physical system, as discussed in Sec. V.

2. Entanglement in bipartite states

The Hilbert space \mathcal{H} of a bipartite system is the tensor product of the subsystem spaces $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$. A *separable* bipartite pure state is a tensor product of pure states in \mathcal{H}_A and \mathcal{H}_B ,

$$\begin{aligned} |\Psi\rangle_{AB} &= |\varphi\rangle_A \otimes |\phi\rangle_B \\ &=: |\varphi\rangle_A |\phi\rangle_B =: |\varphi, \phi\rangle_{AB} =: |\varphi\phi\rangle_{AB} \end{aligned} \quad (14)$$

with reduced density operators $\Psi_A := \text{Tr}_B[|\Psi\rangle\langle\Psi|_{AB}] = |\varphi\rangle\langle\varphi|_A$ on subsystem A and $\Psi_B := \text{Tr}_A[|\Psi\rangle\langle\Psi|_{AB}] = |\phi\rangle\langle\phi|_B$ on subsystem B , obtained by tracing out the non-subscripted system. By contrast, an entangled bipartite pure state cannot be described as a product of states from the individual subsystems; that is, it cannot be written in the form (14).

Generally, we may write any bipartite pure state as

$$|\Psi\rangle_{AB} = \sum_{i,j} c_{ij} |i\rangle_A \otimes |j\rangle_B, \quad (15)$$

where c_{ij} are complex numbers with $\sum_{i,j} |c_{ij}|^2 = 1$, $\{|i\rangle_A\}$ and $\{|j\rangle_B\}$ are orthonormal bases of the two subsystems. With the *Schmidt decomposition*, we may find convenient orthogonal bases $\{|v_i\rangle_A\}$ and $\{|w_j\rangle_B\}$ for the two subsystems, such that the bipartite pure state can be expressed in a standard form with a single index:

$$|\Psi\rangle_{AB} = \sum_{j=1}^r \sqrt{p_j} |v_j\rangle_A \otimes |w_j\rangle_B, \quad (16)$$

where $p_j > 0$ for $j = 1, \dots, r$ and $\sum_{j=1}^r p_j = 1$. The integer r is called the *Schmidt rank*. The reduced density operators for the two subsystems are $\Psi_A = \text{Tr}_B[|\Psi\rangle\langle\Psi|_{AB}] = \sum_{j=1}^r p_j |v_j\rangle\langle v_j|_A$ and $\Psi_B = \text{Tr}_A[|\Psi\rangle\langle\Psi|_{AB}] = \sum_{j=1}^r p_j |w_j\rangle\langle w_j|_B$. For $r = 1$, the expression reduces to a separable bipartite pure state. For $r \geq 2$, the state $|\Psi\rangle_{AB}$ is entangled.

In the setting of mixed states, the definition of separability must be changed to include classical mixtures of tensor product states:

$$\rho_{AB} = \sum_j p_j \sigma_A^{(j)} \otimes \tau_B^{(j)}, \quad (17)$$

where $\{p_j\}$ is a probability distribution and $\sigma_A^{(j)}$ and $\tau_B^{(j)}$ are density operators. Since ρ_{AB} can freely be generated by Alice and Bob with LOCC, the state must only include classical correlations and no entanglement. This definition includes pure-state separability as a special case; therefore one can say that any state which cannot be written in the form (17) (that is, as a convex combination of product states) is entangled.

Quantifying the degree of entanglement in a mixed quantum state—finding an entanglement *measure* or *monotone* that does not confuse entanglement for classical correlations and does not increase over arbitrary LOCC operations—is a difficult problem. For this purpose one has at one's disposal the Schmidt rank, concurrence, negativity, or various entropic functions of the reduced density operators, such as the von Neumann entropy (Bennett *et al.*, 1996b). For mixed states of two qubits, one can unambiguously compute the entanglement using one of the above tools, the concurrence (Wootters, 1998). However, characterizing entanglement for general mixed states of higher dimensions is still an important and active area of research; see Ref. (Horodecki *et al.*, 2009; Plenio and Virmani, 2005) for detailed discussions of the difficulties of quantifying entanglement and of existing entanglement measures.

The simplest example of useful entanglement for quantum networks is that between two qubits associated with two parties, with $\mathcal{H}_A = \text{span}\{|0\rangle_A, |1\rangle_A\}$ and $\mathcal{H}_B = \text{span}\{|0\rangle_B, |1\rangle_B\}$. Then, the space \mathcal{H} is spanned by the four orthogonal *Bell states* or *EPR pairs*:

$$\begin{aligned} |\Phi^\pm\rangle_{AB} &= \frac{1}{\sqrt{2}}(|0\rangle_A |0\rangle_B \pm |1\rangle_A |1\rangle_B), \\ |\Psi^\pm\rangle_{AB} &= \frac{1}{\sqrt{2}}(|0\rangle_A |1\rangle_B \pm |1\rangle_A |0\rangle_B). \end{aligned} \quad (18)$$

These four Bell states are equivalent up to Pauli gates: $|\Phi^+\rangle_{AB} = Z_B |\Phi^-\rangle_{AB} = iY_B |\Psi^-\rangle_{AB} = X_B |\Psi^+\rangle_{AB}$. Tracing out one of the qubits from any Bell state leaves the remaining qubit in a maximally mixed state, which implies that the Bell states are maximally entangled. We often use the Bell state to calibrate the amount of entanglement shared between two parties; each Bell state counts as one entangled bit or *ebit* of entanglement, which can be used to teleport one qubit of quantum information (Bennett *et al.*, 1993) (see Sec. III.A for a description of quantum teleportation).

D. Entanglement in multipartite states

We can generalize the definitions of entanglement in the previous subsection to systems with more than two parties. In this setting, there are several notions of separability. For example, a *fully* separable state defined over multiple subsystems (A, B, C, \dots) can be written as a convex combination of product states

$$\rho_{ABC\dots} = \sum_j p_j \sigma_A^{(j)} \otimes \tau_B^{(j)} \otimes \gamma_C^{(j)} \otimes \dots \quad (19)$$

Similarly to the bipartite case, a multipartite state is entangled when the state cannot be written in the form (19).

Two well-known families of entangled states of $M > 2$ parties are the *Greenberger–Horne–Zeilinger (GHZ) state*

$$\begin{aligned} |\text{GHZ}_M\rangle &= \frac{1}{\sqrt{2}}(|\overbrace{00\dots 0}^M\rangle + |\overbrace{11\dots 1}^M\rangle) \\ &= \frac{1}{\sqrt{2}}(|0\rangle^{\otimes M} + |1\rangle^{\otimes M}), \end{aligned} \quad (20)$$

and the *W state*

$$|W_M\rangle = \frac{1}{\sqrt{M}}(|100\dots 0\rangle + |010\dots 0\rangle + \dots + |000\dots 1\rangle). \quad (21)$$

The GHZ and W states cannot be transformed into each other through LOCC, thereby representing two different kinds of entanglement for three or more parties (Dür *et al.*, 2000) (see, e.g., Ref. (Horodecki *et al.*, 2009)).

A broad and useful class of multipartite entangled states are the *cluster states* or, more generally, the graph states, which we now describe.

1. Graph states

A *graph state* $|G\rangle$ is a multipartite entangled state associated with an undirected graph $G = (V, E)$, with V a set of vertices and E collection of undirected edges $\{ij\} = \{ji\}$, for $i, j \in V$. $|G\rangle$ is then defined through

$$|G\rangle \equiv \prod_{e \in E} C_e^Z \left(\bigotimes_{v \in V} |+\rangle_v \right), \quad (22)$$

where the controlled- Z (CZ or controlled-phase) gate is a Clifford gate defined on qubits i and j through

$$C_{ij}^Z = |0\rangle\langle 0|_i \otimes \mathbb{1}_j + |1\rangle\langle 1|_i \otimes Z_j. \quad (23)$$

C_{ij}^Z is symmetric over $i \leftrightarrow j$, i.e., $C_{ij}^Z = C_{ji}^Z = C_{\{ij\}}^Z$, and C_{ij}^Z and $C_{i'j'}$ commute for any i, j, i' and j' .

A cluster state is a special kind of graph state whose underlying graph G forms a lattice. Performing single-qubit adaptive measurements on a cluster state allow for the execution of a measurement-based quantum

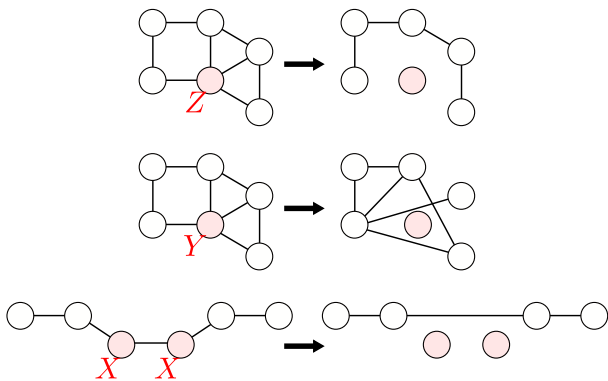


FIG. 2 Graphical rules for operations on graph states. The effects of Pauli operations on the connections in the graph states are shown.

computation (MBQC) (Raussendorf and Briegel, 2001). Whereas one-dimensional (linear) cluster states allow for universal operations on a single qubit, a cluster state of a minimum of two dimensions is necessary to implement a universal set of multi-qubit gates, and additional dimensions are normally needed for error correction and fault tolerance (Raussendorf *et al.*, 2006, 2007; Raussendorf and Harrington, 2007) (see, e.g., Ref. (Terhal, 2015)).

An alternative specification of the graph state is given by the *stabilizer formalism*: $|G\rangle$ is the unique simultaneous eigenstate of all the (stabilizer generator) operators in $\mathcal{S} = \{X_a \otimes Z_{N_a} | a \in V\}$ of commuting operators, where $Z_{N_a} := \bigotimes_{v \in N_a} Z_v$ and N_a is the set of all the vertices adjacent to vertex $a \in V$ in the graph G . We say $|G\rangle$ is *stabilized* by \mathcal{S} , making it a stabilizer state analyzable within the stabilizer formalism (Gottesman, 1997).

A thorough and important review of discrete-variable qubit graph states is given in (Hein *et al.*, 2004, 2006). Let us distill their basic properties, illustrated in Fig. 2:

- Application of local Clifford gates to a graph state is equivalent to that of a sequence of local complementations on the underlying graph (where a local complement of a graph G at a node $a \in V$ is obtained by inverting the subgraph of G induced by the neighborhood N_a).
- Pauli Z measurement on a node decouples the node and breaks off its incident edges.
- Pauli Y measurement on a node takes the local complementation at the node and decouples the node.
- Pauli X measurement on two neighboring qubits in a linear cluster state decouples them but connects their other neighbors with an edge.
- The entanglement in a connected graph state is *localizable*, meaning that it is possible to project any

two qubits in the graph into a Bell pair by performing single-qubit (in particular, Pauli Z or X) measurement on the other qubits.

The concept of the graph state can be generalized to continuous-variable (CV) bosonic systems, describable in the phase space formalism of the quantum harmonic oscillator with position operator q and momentum operator p such that $[q, p] = i$ ($\hbar = 1$). In this case, there is a wealth of possible encodings to choose from. For example, for a Gaussian graph state (Menicucci *et al.*, 2006), the plus state becomes the 0-momentum eigenstate of the momentum operator p ,

$$|+\rangle \rightarrow |p = 0\rangle, \quad (24)$$

while for the Gottesman-Kitaev-Preskill (GKP) encoding (Gottesman *et al.*, 2000), discussed in Sec. II.E, the plus state becomes

$$|+\rangle \rightarrow |+\text{GKP}\rangle = \sum_{n=-\infty}^{\infty} |p = 2n\sqrt{\pi}\rangle, \quad (25)$$

where $|p = 2n\sqrt{\pi}\rangle$ is the eigenstate corresponding to the eigenvalue $2n\sqrt{\pi}$ of the momentum operator p . For both of these CV encodings, the CZ gate can be written as

$$C_{ij}^Z \rightarrow e^{i(q_i \otimes q_j)} \quad (26)$$

with the position operator q_i for bosonic system i . Clifford operations on these encodings correspond to certain Gaussian operations in phase space, which are composed of squeezing, displacements, and rotations. In either case, one uses finitely-squeezed approximations to these states in practice. We give more details on these states in our discussion of photonic encodings in Sec. II.E and as well as in Sec. III.C.2.c on bosonic repeaters.

E. Photonic encodings

There are several degrees of freedom that one can exploit when encoding quantum information into light. Each one has own advantages and challenges. In this section we review some well-known photonic encodings, summarizing some of this information in Table III.

A few ways exist for categorizing photonic encodings. One is through the cardinality of the Hilbert space. The state space of discrete-variable (DV) encodings is spanned by a finite number of orthogonal (more generally, linearly independent) states, whereas continuous-variable (CV) or bosonic encodings are spanned by infinitely (possibly countably) orthogonal (more generally, linearly independent) states. However, the line between the two kinds of encodings may not always be clear: DV systems can be viewed as finite subspaces of CV spaces, and our interest in CV systems may chiefly be to identify two-dimensional (qubit) subspaces. Furthermore, in

	<i>Single-rail encodings</i>			<i>Dual-rail encodings</i>		
	Fock state	Coherent / cat	GKP	Time-bin	Path	Polarization
Cardinality	DV	CV	CV	DV	DV	DV
Physical basis	Vacuum, single photon	Coherent states: $ \pm\alpha\rangle$	GKP-0 and 1: (Eq. (27))	Orthogonal temporal modes	Orthogonal spatial modes	Orthogonal polarizations
Entanglement w/ LO	Deterministic	Deterministic	Deterministic	Probabilistic	Probabilistic	Probabilistic
Single-mode Clifford gates w/ LO	Probabilistic	Probabilistic	Deterministic (w/ squeezing)	Deterministic	Deterministic	Deterministic
Single-mode non-Clifford gates w/ LO	Probabilistic	Probabilistic	Probabilistic	Deterministic	Deterministic	Deterministic

TABLE III Descriptions of selected photonic encodings, including associated gate implementations.

practice, various imperfections and interactions with the environment increase the effective dimensionality of DV systems.

Another characterization of photonic encodings is in the number of “rails.” In the more restrictive definition, a *single-rail* qubit is associated with the presence or absence of a single photon in an optical (spatial or temporal) mode. More broadly, however, one can view single-rail encodings as those where each state—including states of multiple photons—occupies a single optical mode. Conversely, a *dual-rail* qubit is associated with the presence of a single photon in one of two orthogonal modes. For a single-rail encoding, it is possible to generate entanglement deterministically with linear optical resources, while linear-optical entangling operations are necessarily probabilistic in dual-rail encodings. Conversely, single-qubit rotations for certain single-rail encoded qubits may necessitate nonlinearity (because the encoding can be based on a superposition of different photon number states, i.e., energy eigenstates), while there exist dual-rail encodings where arbitrary single-qubit rotations are possible only with linear optical elements. See, e.g., (Kok *et al.*, 2007).

The following photonic encodings have been frequently considered within quantum information protocols:

- *Time-bin*: a photon takes one of two paths of an interferometer of different lengths. Then, $|0\rangle$ is associated with one path, and $|1\rangle$ with the other. This encoding is suited for fiber-based communication as it is unaffected by birefringence in optical fibers; however, it is difficult to interact two time-bin qubits, making the encoding preferred for quantum communication over computation.
- *Polarization*: a kind-of dual rail encoding where a qubit is encoded into the polarization states

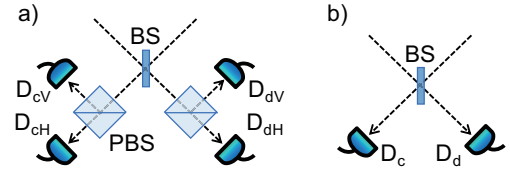


FIG. 3 Examples of implementation of Bell measurement. a) Bell measurement for polarization-encoded qubits, spanned by horizontally and vertically polarized single-photon states $|H\rangle$ and $|V\rangle$. This is implemented by the application of a 50:50 beamsplitter (BS) on optical modes, followed by a polarization beamsplitter (PBS) on each of the two output modes and then by photon counting at all the output modes. Clicks in detectors D_{cH} and D_{cV} , or in D_{dH} and D_{dV} , project the received pair of the qubits into Bell state $|\Psi^+\rangle = (|H\rangle|V\rangle + |V\rangle|H\rangle)/\sqrt{2}$, while clicks in detectors D_{cH} and D_{dV} , or in D_{cV} and D_{dH} , project the received pair of the qubits into Bell state $|\Psi^-\rangle = (|H\rangle|V\rangle - |V\rangle|H\rangle)/\sqrt{2}$. Notice that this Bell measurement can succeed only when the input two optical pulses have 2 (or more) photons in total. b) Bell measurement for Fock-encoded qubits, spanned by the vacuum state $|0\rangle$ and the single-photon state $|1\rangle$. This is implemented by the application of a 50:50 beamsplitter (BS) on optical modes, followed by photon counting at the output modes. A click in the detector D_c (or D_d) at the constructive-interference (destructive-interference) mode projects the received pair of the qubits into Bell state $|\Psi^+\rangle = (|0\rangle|1\rangle + |1\rangle|0\rangle)/\sqrt{2}$ ($|\Psi^-\rangle = (|0\rangle|1\rangle - |1\rangle|0\rangle)/\sqrt{2}$). Both implementations can distinguish $|\Psi^\pm\rangle$ from the other states only, and the success probabilities are thus 1/2 even in the ideal cases.

of a single photon. Conventionally, $|0\rangle$ is associated with a horizontally polarized photon, and $|1\rangle$ with a vertically polarized photon. All single-qubit gates can be performed deterministically with waveplates and phase shifters, while linear-optical entangling gates are probabilistic, requiring beam-

splitters, waveplates, measurements, and postselection. As an example of the two-qubit operations, an implementation of the Bell measurement is given in Fig. 3 (a). This encoding prefers free-space over fiber-based communication, as it is vulnerable to birefringence within optical fibers.

- *Path*: computational basis states are associated with orthogonal spatial modes. All single-qubit gates can be performed deterministically with beamsplitters and phase shifters; as with the polarization encoding, entangling gates with linear optical resources are probabilistic, requiring beamsplitters, phase shifters, measurements and postselection. As with the time-bin encoding, path-encoded photons prefer fiber-based over free-space communication.
- *Fock*: a qubit is encoded into the Hilbert subspace of a single mode spanned by the vacuum state $|0\rangle$ and the single-photon state $|1\rangle$, corresponding to a single-rail qubit. With a phase shifter, we can rotate its Bloch vector along the Z -axis freely, but we cannot do so along the X -axis since $|0\rangle$ and $|1\rangle$ have different energy. On the other hand, a Bell state (such as $|\Psi^\pm\rangle = (|01\rangle \pm |10\rangle)/\sqrt{2}$) can deterministically be obtained with single photon incident on a 50:50 beamsplitter. However, we can discriminate only Bell states $|\Psi^\pm\rangle$ from the others, with a 50:50 beamsplitter followed by two photon detectors (see Fig. 3 (b)). This encoding is sensitive to phase drifts in a transmission channel, and thus, it is preferred in free-space over fiber-based communication.
- *Coherent/Cat*: a qubit is encoded into the Hilbert subspace of a single mode spanned by coherent states $|\alpha\rangle$ and $|\alpha\rangle$ with $\alpha > 0$, corresponding to a single-rail qubit. The qubit basis states $|\pm\rangle$ are associated with cat states $(|\alpha\rangle \pm |-\alpha\rangle)/(2\sqrt{p_\pm})$ with $p_\pm := (1 \pm \langle -\alpha|\alpha\rangle)/2$. The states $|\pm\rangle$ are flipped by a π -phase shifter, and they are distinguished by a photon-number-resolving detector. This encoding is also sensitive to phase drifts in a transmission channel, and thus, it prefers free-space over fiber-based communication.
- *GKP*: the computational basis states are coherent superpositions of infinitely many regularly-spaced position eigenfunctions (i.e., infinitely squeezed states):

$$|0_{\text{GKP}}\rangle = \sum_{n=-\infty}^{\infty} |q = 2n\sqrt{\pi}\rangle, \quad (27)$$

$$|1_{\text{GKP}}\rangle = \sum_{n=-\infty}^{\infty} |q = (2n+1)\sqrt{\pi}\rangle, \quad (28)$$

where $|q = n\sqrt{\pi}\rangle$ is the eigenstate corresponding to the eigenvalue $n\sqrt{\pi}$ of the position operator q . In realistic implementations, these unphysical infinite-energy states are replaced by their normalizable, finitely-squeezed counterparts. All single-qubit (many-qubit) Clifford gates—including entangling gates—are implementable deterministically through single-mode (multi-mode) Gaussian operations. Non-Clifford gates can be implemented with help of ancillary states and gate teleportation, i.e., they are only deterministic conditioned on the availability of the ancillae.

The above encoding schemes are “digital,” because they encode a discrete-variable (DV) quantum system with a finite dimensional Hilbert subspace of photonic modes. In contrast, we may also use the photonic modes for “analog” encoding, to store a continuous-variable (CV) “analog” quantum system with an infinite dimensional Hilbert space. For example, we can encode continuous-variable quantum information using squeezed states, which can be measured via homodyne and heterodyne detectors with a continuous-variable output. For quantum communication, the continuous-variable output can be used to generate secure secret keys (Grosshans and Cerf, 2004).

One major challenge of using CV encodings for quantum repeaters is the suppression of loss errors. Because of the theorem that Gaussian operations are of no use for protecting Gaussian states against Gaussian errors (including loss errors) (Niset *et al.*, 2009), we have to introduce non-Gaussian operations (e.g., “quantum scissors” to truncate the number-state expansion (Pegg *et al.*, 1998)) or non-Gaussian ancillary resources (e.g., GKP stabilizer codes to encode an oscillator into many oscillators assisted by GKP ancilla (Noh *et al.*, 2020)) to overcome loss errors.

III. QUANTUM REPEATERS

This section begins with a review of primitives for quantum repeaters. This is followed with an explanation of quantum repeater protocols through a conceptual classification based on methods to suppress loss and operation errors. We also review all-optical implementations of quantum repeaters.

A. Repeater primitives

Here we review quantum teleportation and entanglement swapping as primitives for quantum repeaters. We also summarize various tools for error suppression, which are necessary for quantum repeaters.

1. Quantum teleportation

Quantum teleportation is a procedure for transferring quantum information from a sender to a distant receiver without transferring the physical system in which it is encoded (Bennett *et al.*, 1993). To accomplish this, the two parties must have established a classical communication link and pre-shared a maximally entangled state. Then, the teleportation consists of two steps. First, the sender locally performs a joint measurement between the state that she wants to transfer and her portion of the pre-shared entangled state. Then, she communicates the measurement outcome to the receiver via the classical channel, who must apply a local unitary operation to his quantum state to recover the original state. There exist quantum teleportation protocols for qudits² (Werner, 2001) and CV systems (Braunstein and Kimble, 1998); here we focus on qubits to illustrate the concept.

Suppose that Alice has a qubit in an arbitrary state $|\psi\rangle_{A_1}$ that she wants to send to Bob. Suppose also that she has already shared a Bell state with Bob, $|\Phi^+\rangle_{A_2B}$, from Eq. (18). By performing a Bell-state measurement on her two qubits A_1 and A_2 —that is, a projection onto one of Bell states of Eq. (18)—she will project Bob’s qubit onto some state. This state of Bob’s qubit B is equal to the initial state $|\psi\rangle$, up to local rotations that are determined by the (random) outcome of Alice’s measurement:

$$\begin{aligned} |\Phi^+\rangle_{A_1A_2} &\rightarrow |\psi\rangle_B, \\ |\Phi^-\rangle_{A_1A_2} &\rightarrow Z_B |\psi\rangle_B, \\ |\Psi^+\rangle_{A_1A_2} &\rightarrow X_B |\psi\rangle_B, \\ |\Psi^-\rangle_{A_1A_2} &\rightarrow Z_B X_B |\psi\rangle_B. \end{aligned} \quad (29)$$

To conclude the teleportation, Alice must transfer the outcome of her measurement to Bob through a classical channel so that Bob can undo the Pauli byproduct and recover the original state $|\psi\rangle$. Even though Bob has a state locally equivalent to Alice’s immediately after the Bell measurement, his ignorance at that point of the precise Pauli gate he has to apply means that Alice cannot transfer quantum information instantly to Bob. The quantum teleportation protocol therefore crucially needs classical communication, making it limited by the speed of light. This impossibility of faster-than-light communication assisted by quantum entanglement is known as the no-signaling principle (Eberhard and Ross, 1989).

Quantum teleportation allows a sender to send arbitrary quantum information encoded into a qubit by consuming an ebit (pre-shared with the receiver) and by sending two bits of classical information to the receiver.

This implies that distributing ebits efficiently or quickly by using a quantum communication network is a fundamental question.

2. Entanglement swapping

Entanglement swapping (Zukowski *et al.*, 1993) can be thought of as an extension of quantum teleportation where Alice and Bob each share a two-qubit maximally entangled state with Charlie, C : $|\Phi^+\rangle_{AC_1}$ and $|\Phi^+\rangle_{C_2B}$. After Charlie performs a Bell measurement on his systems C_1 and C_2 , Alice’s and Bob’s qubits end up in one of the four Bell states, depending on the measurement outcome:

$$\begin{aligned} |\Phi^+\rangle_{C_1C_2} &\rightarrow |\Phi^+\rangle_{AB}, \\ |\Phi^-\rangle_{C_1C_2} &\rightarrow |\Phi^-\rangle_{AB} = Z_B |\Phi^+\rangle_{AB}, \\ |\Psi^+\rangle_{C_1C_2} &\rightarrow |\Psi^+\rangle_{AB} = X_B |\Phi^+\rangle_{AB}, \\ |\Psi^-\rangle_{C_1C_2} &\rightarrow |\Psi^-\rangle_{AB} = Z_B X_B |\Phi^+\rangle_{AB}. \end{aligned} \quad (30)$$

Although their qubits have not directly interacted, Alice and Bob have established a maximally entangled state. This is particularly useful in the context of quantum communication, as it means that entanglement can be propagated through a quantum network even between stationary nodes. Indeed, entanglement swapping is the crux of quantum repeater schemes based on heralded entanglement generation³; see Sec. III.A.3, Sec. III.B.1, and Sec. III.B.2.

3. Idealized quantum repeaters

As shown in the quantum teleportation protocol of Sec. III.A.1, once Alice and Bob share a Bell pair (an ebit), Alice can send an unknown state of a qubit to Bob by LOCC, i.e., they can achieve quantum communication. Thus, the challenge of quantum communication reduces mainly to how to distribute a Bell pair between Alice and Bob in practice. Flying qubits—photons—appear to be the medium of choice for this. However, the transmittance η of an optical fiber (and hence the ratio of photons sent to photons received) decreases exponentially with its length L , according to $\eta = e^{-L/L_{\text{att}}}$ of Eq. (13). In fact, the transmittance decreases as though it is multiplied by 0.1 every 50 km in the case of typical optical fibers with attenuation length $L_{\text{att}} = 22$ km (and even the quantum and private capacity of the pure-loss bosonic channel (13) is now known to be described by $-\log_2(1 - \eta)$ ($\approx \eta$ for $\eta \ll 1$) (Pirandola *et al.*, 2017)

² Recently, such high-dimensional teleportation is refocused in the context of quantum networks (Bacco *et al.*, 2021) thanks to experimental progress (Hu *et al.*, 2020b; Luo *et al.*, 2019).

³ The entanglement swapping operation can also be achieved using quantum Zeno effect, requiring no controlled gates (Bayrakci and Ozaydin, 2022).

(see Sec. VI). Hence, simply linking Alice and Bob directly with an optical fiber is not enough to achieve efficient quantum communication, especially if they are far apart⁴.

Here we introduce a simple example to show how a quantum repeater protocol overcomes such an exponential increase of photon loss with the length of an optical fiber. The example is based on heralded entanglement generation and entanglement swapping; it is a simplified protocol designed to capture the main concept of the first-generation quantum repeater protocols (Briegel *et al.*, 1998; Duan *et al.*, 2001; Sangouard *et al.*, 2011), which will appear in Sec. III.B.1. The protocol is based on a concatenation allowed by the entanglement swapping of Sec. III.A.2, dubbed a *DLCZ*-like protocol after the authors Duan, Lukin, Cirac and Zoller (Duan *et al.*, 2001). For simplicity, we assume that the fiber attenuation is the only error and all other operations are perfect.

Suppose that we have a quantum memory X which can establish a Bell state $|\Phi^+\rangle_{Xx} := (|0\rangle_X |H\rangle_x + |1\rangle_X |V\rangle_x)/\sqrt{2}$ with an optical pulse x , where $\{|0\rangle_X, |1\rangle_X\}$ is the computational basis of the quantum memory while $|H\rangle_x$ and $|V\rangle_x$ are horizontally polarized and vertically polarized single-photon states of the pulse x , respectively. We also assume that an arbitrary state $a|0\rangle + b|1\rangle$ of the quantum memory can be converted into the state $a|H\rangle + b|V\rangle$ of a polarization qubit, if needed. This kind of memory is an idealized version of a quantum memory, which can be realized by using two atomic ensembles (Sangouard *et al.*, 2011) (for example, we ignore any multi-photon excitations that arise in practice). We also use a linear-optical Bell measurement for polarization-encoded qubits in Fig. 3 (a). This implementation works as a probabilistic Bell measurement.

We can generate a Bell state between stations X and Y , separated by distance l , by combining such a quantum memory, the Bell measurement and optical fibers. To achieve this, the party X (and the party Y) first establishes a Bell state $|\Phi^+\rangle_{Xx}$ ($|\Phi^+\rangle_{Yy}$) between her (his) own quantum memory X (Y) and an optical pulse x (y) locally, and then sends the single photon x (y) to a measuring station in the middle of the parties over an optical fiber (modeled by Eq. (13)) (see a schematic for entanglement generation (EG) in Fig. 4). On receiving the pulses from the separated parties, the measuring station performs the linear-optical Bell measurement of Fig. 3 (a) and

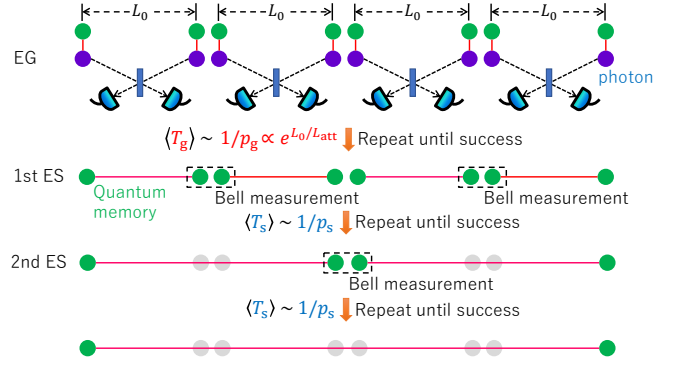


FIG. 4 Idealized quantum repeater protocol. In this figure, three quantum repeater nodes (corresponding to the case of $N_{\text{QR}} = 3$) are located at regular intervals between Alice and Bob, who are separated by distance L , with $L_0 = L/4$. The protocol starts by entanglement generation (EG) between adjacent repeater nodes with success probability $p_g(L_0) = e^{-L_0/L_{\text{att}}}/2$, followed by entanglement swapping (ES) with success probability p_s . The EG protocol establishes a Bell pair between adjacent repeater nodes after the number of trials on the order of $\langle T_g(L_0) \rangle = p_g^{-1}(L_0)$. Given halves of a pair of Bell states, the ES protocol succeeds in swapping the entanglement after the number of trials on the order of $\langle T_s \rangle = p_s^{-1}$. If a trial of ES fails, we need to start again from EG to go back to the trial. Therefore, in the setting of this figure, the average of the total number of trials $T_{\text{tot}}^{(3)}$ needed to establish a Bell pair between Alice and Bob is $\langle T_{\text{tot}}^{(3)} \rangle \sim \langle T_g(L_0) \rangle \langle T_s \rangle^2 = p_s^{-2} p_g^{-1}(L_0) = 2p_s^{-2} e^{L/(4L_{\text{att}})}$. This is of the order of the square root of $\langle T_{\text{tot}}^{(1)} \rangle$, which is further of the order of the square root of $\langle T_{\text{tot}}^{(0)} \rangle$.

those pulses. This Bell measurement succeeds when both single photons x and y from the separated parties arrive at the measuring station without having been lost (during their travel over the lossy optical fiber), and the surviving photons are projected into a Bell state $|\Psi^+\rangle_{xy}$ or $|\Psi^-\rangle_{xy}$, which occurs with probability $p_g(l) = e^{-l/L_{\text{att}}}/2$. This success event entangles the quantum memories XY of the separated parties into $|\Psi^+\rangle_{XY}$ or $|\Psi^-\rangle_{XY}$, according to Eq. (30). This is called an (heralded) entanglement generation protocol.

If Alice and Bob, separated by distance L , run this entanglement generation protocol between them without any quantum repeater, the average of the number $T_{\text{tot}}^{(0)}$ of trials needed to obtain a Bell pair will be

$$\langle T_{\text{tot}}^{(0)} \rangle := \langle T_g(L) \rangle = p_g^{-1}(L) = 2e^{L/L_{\text{att}}}, \quad (31)$$

which grows exponentially with the distance L .

Now, let us introduce an entanglement swapping protocol. Suppose that a single quantum repeater node C is located at the midpoint between Alice and Bob for simplicity, and it runs the above entanglement generation protocols in parallel with Alice and with Bob. Then, each of these entanglement generation protocols gives a Bell pair after trials on the order of $\langle T_g(L/2) \rangle = 2e^{L/(2L_{\text{att}})}$. Once

⁴ Notice that the transmittance η of the typical fiber with the length of 400 km is about 10^{-8} . Therefore, even if the system is designed to achieve the private capacity $-\log_2(1 - \eta)$ with the clock rate of 1 GHz, the possible key rate is on the order of 10 bits per second, which seems to be slow for practical applications. Hence, about 400 km is sometimes said to be a practical distance limit of a fiber-based point-to-point quantum communication.

it succeeds, the obtained Bell pair can be kept in quantum memories until both of the parallel protocols succeed. Thus, they can obtain Bell pairs not only between Alice and the node C , but also between the node C and Bob, after trials on the order of $\langle T_g(L/2) \rangle = 2e^{L/(2L_{\text{att}})}$, thanks to the parallelization. Then, after receiving a classical signal to herald this successful sharing of Bell pairs, the node C converts states of local quantum memories into polarization qubits, and then implements the linear-optical Bell measurement of Fig. 3 (a) (corresponding to a schematic for entanglement swapping (ES) in Fig. 4). This works as entanglement swapping to provide a Bell state between Alice and Bob with success probability $p_s = 1/2$ of the Bell measurement (in the ideal case). Hence, the average of the number T_s of trials needed for the entanglement swapping to succeed (after the success of the entanglement generation protocols) is $\langle T_s \rangle = p_s^{-1}$. On the other hand, if the Bell measurement fails, Alice and Bob start from scratch, i.e., from the parallel entanglement generation protocols. Thus, the average of the total number $T_{\text{tot}}^{(1)}$ of trials needed to establish a Bell pair between Alice and Bob is

$$\langle T_{\text{tot}}^{(1)} \rangle \sim \langle T_g(L/2) \rangle \langle T_s \rangle = p_s^{-1} p_g^{-1} (L/2) = 2p_s^{-1} e^{\frac{L}{2L_{\text{att}}}}, \quad (32)$$

(see, e.g., Refs. (Azuma *et al.*, 2021; Sangouard *et al.*, 2011) about the validity of this approximation). Therefore, by comparing this equation with Eq. (31), we can conclude that, for a large distance L , the existence of a single quantum repeater node C can provide the square-root improvement over the direct entanglement generation between Alice and Bob in the number of trials needed.

The process for achieving this square-root improvement with entanglement swapping can be concatenated. If Alice and Bob use three equally-spaced quantum repeater nodes, they can achieve further square-root improvement (see Fig. 4); if they use seven, they can have further square-root improvement, and so forth. In particular, if Alice and Bob have $N_{\text{QR}} = 2^n - 1$ quantum repeater nodes equally spaced between them, the average of the total number $T_{\text{tot}}^{(N_{\text{QR}})}$ of trials needed to have a Bell pair between Alice and Bob will be

$$\begin{aligned} \langle T_{\text{tot}}^{(N_{\text{QR}})} \rangle &\sim p_s^{-n} p_g^{-1} (L/2^n) = p_s^{-n} e^{\frac{L}{2^n L_{\text{att}}}} \\ &= 2p_s^{-\log_2(N_{\text{QR}}+1)} e^{\frac{L}{(N_{\text{QR}}+1)L_{\text{att}}}}. \end{aligned} \quad (33)$$

(again, see, e.g., Refs. (Azuma *et al.*, 2021; Sangouard *et al.*, 2011) about this approximation). This shows the ultimate advantage of utilizing quantum repeaters: the exponential improvement in the number of trials needed to establish entanglement with the number N_{QR} of quantum repeater nodes. Since p_s is independent of distance L , this exponential improvement enables Alice and Bob to perform quantum communication efficiently over long distances.

This simple model does not include realistic imperfections such as memory errors and imperfect entanglement generation and swapping operations. In practice, these errors will accumulate and become non-negligible over longer distances. However, thanks to the existence of error suppression mechanisms explained in the next Sec. III.A.4, we can devise several kinds of quantum repeaters which work not only in the presence of loss but also other such imperfections.

4. Tools for error suppression

As shown in Sec. III.A.3 above, there exists a quantum repeater protocol which enables Alice and Bob to achieve efficient long-distance quantum communication, even with the use of optical fibers impacted by photon loss. However, this protocol was idealized; we assumed that the optical attenuation in fiber is the only source of error and that all other operations are perfect. In practice, there are many physical imperfections that compromise the quality of the resulting entanglement. Therefore, quantum repeater protocols need to be equipped with error suppression mechanisms, which we discuss in this section.

It is helpful to classify error suppression techniques into two categories: those employing *deterministic* error suppression (including quantum error correction (Lidar and Todd A. Brun, 2013) and one-way entanglement distillation (Bennett *et al.*, 1996c)); and those leveraging *probabilistic* error suppression (including quantum error detection (Lidar and Todd A. Brun, 2013) and two-way entanglement purification (Bennett *et al.*, 1996a; Briegel *et al.*, 1998; Deutsch *et al.*, 1996)). The former class of techniques succeed deterministically, meaning they do not require users to share a heralding signal alerting each other of the success or failure of the error suppression; on the other hand, the probabilistic nature of the latter class necessitates users to alert each other of success or failure via classical communication and discard the failed instances. For networks with large spatial separation between the nodes, the time delay associated with this classical heralding signaling is highly relevant to the performance of the network—for reference, a photon takes roughly 0.5 ms to travel 100 km in an optical fiber. While deterministic error suppression has an advantage in this regard, probabilistic error suppression works even for states which are too noisy to be recovered through deterministic techniques. That is, the probabilistic techniques tend to have higher thresholds on tolerable error or loss probabilities (Bennett *et al.*, 1996c). Let us now briefly summarize both of these types of approaches for suppressing errors.

a. Deterministic error suppression

1. Quantum error correction The essence of *quantum error correction* (QEC) is to use the redundancy in the entanglement of many physical qubits to encode a logical state and correct for errors. In particular, a qubit is encoded into a two-dimensional subspace of a large Hilbert space composed of many physical qubits rather than directly into a single physical system. Quantum error correction is a deterministic process; it is not impacted by the delays associated with classical heralding signals. For large-scale quantum networks, having this determinism favourably affects communication rates; on the other hand, physical implementations of QEC codes are demanding due their complexity, and exhibit lower thresholds (to work) on the errors affecting the physical qubits. These thresholds become more stringent as the variety and magnitude of errors increase.

2. One-way entanglement distillation The purpose of one-way entanglement distillation (1-EDP) is to obtain an almost maximally entangled Bell pair from a set of noisier entangled pairs by applying (direct) one-way LOCC. Here “one-way” means that only one party has to communicate the results during the distillation process via classical communication; there is no backward classical communication. 1-EDP is closely connected to quantum error correction (Horodecki *et al.*, 2009); since there is a direct mapping from a one-way hashing protocol (Bennett *et al.*, 1996c) (or one-way breeding protocol (Bennett *et al.*, 1996a)) to a quantum error-correcting code, we will treat them as equivalent at the protocol level. In practice, there may be subtle differences in the error accumulation and resource counts between one-way hashing protocols and quantum error correction.

b. Probabilistic error suppression

1. Quantum error detection QEC codes can also be used just to detect errors—that is, to herald the presence of error and discard the state without correcting the error. Quantum error detection is a *probabilistic* process; as a result, it takes time to inform the relevant parties, through a classical signal, about the outcome of the error detection, causing additional delay.

2. Heralded entanglement generation protocol (HEGP) A widely used error detection scheme is the heralded entanglement generation protocol (HEGP), which can generate entanglement on success and detect loss errors on failure. Since entanglement cannot be generated under LOCC, a party needs to generate an entangled state between a local qubit and a flying qubit locally and then to send the flying qubit over a quantum channel. A typical choice of flying qubit is a bosonic system, such as a photonic state; its quantum channel—a bosonic

channel—has loss as the dominant noise process. The goal of HEGP, then, is to generate high-quality entanglement between separated parties in a heralded manner, notwithstanding losses in the channel.

Depending on how the quantum information is encoded in the optical modes, or how the local stationary qubits are entangled with the optical modes, one ought to choose appropriate schemes to detect loss errors. For dual-rail (single-rail) discrete-variable encodings, one generates entanglement using two-photon (single-photon) interference of incoming optical modes from neighboring stations, while detecting loss errors according to click patterns of the photon detection (Azuma and Kato, 2012; Azuma *et al.*, 2012; Barrett and Kok, 2005; Childress *et al.*, 2006b; Duan *et al.*, 2001; Sangouard *et al.*, 2011) after the interference. For continuous-variable (e.g., GKP (Gottesman *et al.*, 2000)) encoding, one may generate entanglement by combining the two incoming optical modes from neighboring stations followed by homodyne measurements at the output ports. The outcomes from the homodyne measurements provide information about the likelihood of loss errors, which may be used to determine whether the entanglement generation is successful or not (Fukui *et al.*, 2021).

If loss errors are detected, the heralded entanglement generation procedure is simply repeated until the two adjacent stations receive the confirmation of certain successful detection patterns via *two-way* classical signaling. Instead of using this time multiplexing, we could also use spatial or frequency multiplexing to run the heralded entanglement generation protocol in parallel so that one of the multiplexed trials succeed with a high probability within a constant time (Sinclair *et al.*, 2014).

3. Two-way entanglement distillation protocol (2-EDP) The purpose of two-way entanglement distillation (2-EDP) is to produce an almost maximally entangled pair from noisier entangled pairs by applying two-way LOCC. 2-EDP allows both parties to communicate with each other using a classical channel, which enables them to compare measurement results or adaptively perform operations conditioned on the outcomes from the other party. For example, if the Bell states suffer from bit-flip errors, $\rho_{AB} = (1 - \epsilon) |\Phi^+\rangle\langle\Phi^+|_{AB} + \epsilon |\Psi^+\rangle\langle\Psi^+|_{AB}$, separated parties may use two copies of the states to obtain one pair with a suppressed error of $O(\epsilon^2)$ by comparing measurement outcomes of a parity-check measurement on their own halves (Bennett *et al.*, 1996c; Briegel *et al.*, 1998; Deutsch *et al.*, 1996). We may also extend the result to suppress dephasing errors. For general depolarization errors, we may use *twirling* (Bennett *et al.*, 1996a) or switching between phase and bit errors (Deutsch *et al.*, 1996) to further suppress errors.

For ideal operations, we can quickly converge to perfect Bell pairs. In principle, we can extract entanglement with a rate limited by the two-way distillable entangle-

	<i>Deterministic</i> error suppression	<i>Probabilistic</i> error suppression
	Quantum error correction	Quantum error detection
Schemes	One-way entanglement distillation	Two-way entanglement purification
Signaling	No delay	Delay
Threshold to work	$\eta > 1/2$ for loss of qubits or bosons	$\eta > 0$ for loss of qubits or bosons
	$p < 1/4$ at least for depolarization of qubits	$p < 1/2$ for depolarization of qubits

TABLE IV Comparison between deterministic and probabilistic error suppression protocols.

ment (Bennett *et al.*, 1996c). In practice, however, operation errors limit the ultimate fidelity of the distilled Bell pairs. Various protocols have been proposed to distill entanglement (Bennett *et al.*, 1996a; Deutsch *et al.*, 1996; Fujii and Yamamoto, 2009; Jiang *et al.*, 2007b; Krastanov *et al.*, 2019; Nickerson *et al.*, 2013; Riera-Sàbat *et al.*, 2021). For example, one can use multiple copies of imperfect Bell pairs to purify a Bell pair (Fujii and Yamamoto, 2009; Nickerson *et al.*, 2013). One can also use a genetic algorithm to find the optimal 2-EDP (Krastanov *et al.*, 2019). Existing entanglement can also enhance the performance of 2-EDP (Riera-Sàbat *et al.*, 2021). Since there is a direct mapping from 2-EDP to quantum error detection (Dür and Briegel, 2007), we may treat them as equivalent at the protocol level. In practice—just as in the relationship between QEC and 1-EDP—there may be subtle differences in error accumulation and resource counts between quantum error detection and 2-EDP.

For CV encoding, due to the Gaussian entanglement distillation no-go theorem (Eisert *et al.*, 2002; Fiurášek, 2002; Giedke and Cirac, 2002), the CV repeaters use non-Gaussian operations at the entanglement distillation protocols (Fiurášek, 2010; Ralph and Lund, 2009) to suppress loss errors. Instead, we may distill entanglement using nondeterministic noiseless linear amplification (NLA) with quantum scissors (Pegg *et al.*, 1998; Ralph and Lund, 2009) or other non-Gaussian filtering with single-photon addition and subtraction operations (Fiurášek, 2010).

c. Comparison of deterministic and probabilistic quantum error suppression Deterministic error suppression has no corresponding classical signaling delay. However, it imposes a threshold of 50% on the loss of qubits or bosonic systems (associated with the transmittance η as $\eta > 1/2$ if they are sent over a pure-loss channel, as in (13)) (Bennett *et al.*, 1997, 1996c; Giovannetti *et al.*, 2003a,b). Furthermore, this category of protocols will not work at

all for qubits sent over a depolarizing channel (12) with strength $p > 1/4$ (Bennett *et al.*, 1997, 1996c; Knill and Laflamme, 1997), although they work for $p \lesssim 0.18929$ with the hashing protocol (Bennett *et al.*, 1996c) and even for $p \lesssim 0.19130$ with a concatenated coding scheme (Fern and Whaley, 2008)). Probabilistic error suppression has an associated classical signaling delay, but it can tolerate larger errors. In principle, it works if the transmission probability of qubits or bosonic systems is nonzero (Bennett *et al.*, 1997; Pirandola, 2019) or if qubits are sent over a depolarizing channel with $p < 1/2$ (Bennett *et al.*, 1996c; Deutsch *et al.*, 1996). We summarize and compare the properties of deterministic and probabilistic error suppression protocols in Table IV.

B. Generations of quantum repeaters

There are two major challenges for fiber-based quantum communication over long distances. First, as pointed out in Sec. III.A.3, fiber attenuation during transmission leads to an exponential decrease in the entangled-pair generation rate. Second, several operational errors such as channel errors, gate errors, measurement errors, and quantum memory errors, severely degrade the quality of the obtained entanglement. Different from classical information, quantum information is encoded as quantum states that cannot be amplified or duplicated deterministically due to the quantum no-cloning theorem (see Sec. II.B).

To overcome these challenges, quantum repeaters (QRs) have been proposed for the faithful realization of long-distance quantum communication (Briegel *et al.*, 1998). As exemplified in Sec. III.A.3, the essence of QRs is to divide the total distance of communication into shorter intermediate segments connected by QR stations, in which loss errors from fiber attenuation can be corrected. Active error suppression schemes are also employed at every repeater station to correct operation errors, i.e., imperfections induced by the channel, measurements, and gate operations. In the following, we will classify quantum repeaters according to how one suppresses loss and operation errors—using *probabilistic* error suppression (Sec. III.A.4.b) or *deterministic* error suppression (Sec. III.A.4.a)—which will lead to a different scaling of quantum communication rates.

For probabilistic error suppression protocols, we need *two-way* classical signaling to inform relevant repeater nodes whether to proceed to the next step (if error suppression succeeds) or to make another attempt (if error suppression fails). A widely used error detection scheme to suppress loss errors is the heralded entanglement generation protocol (HEGP), as exemplified dual-rail photonic encoding in Sec. III.A.3. For single-rail or CV encoding, photon click patterns may not immediately identify loss events, but we may use other non-Gaussian op-

Error		1G	2G	3G
Errors	suppression			
Loss error	Probabilistic	✓	✓	
	Deterministic			✓
Operation error	Probabilistic	✓		
	Deterministic		✓	✓
Time scale		$\max(\frac{L}{c}, t_0)$	$\max(\frac{L_0}{c}, t_0)$	t_0
Cost coefficient		poly(L)	polylog(L)	polylog(L)

TABLE V Three generations of quantum repeaters classified according to probabilistic or deterministic suppression of loss and operation errors. The time scale (key generation rate) and cost coefficient scale differently with the total distance L , repeater spacing L_0 , and gate time t_0 .

erations (e.g., non-deterministic noiseless linear amplification (NLA) with quantum scissors (Pegg *et al.*, 1998; Ralph and Lund, 2009) to suppress loss errors. If loss errors are detected, one simply repeats the heralded entanglement generation procedure until the two adjacent stations receive the confirmation of certain successful detection patterns via *two-way* classical signaling. Similarly, to achieve *probabilistic* suppression of operation errors, a popular error detection scheme is the two-way entanglement distillation protocol (2-EDP), which consumes several low-fidelity Bell pairs to probabilistically generate a smaller number of higher-fidelity Bell pairs (Deutsch *et al.*, 1996; Dür *et al.*, 1999). Like HEGP, to confirm the success of purification, *two-way* classical signaling between repeater stations for exchanging measurement results is required. The time delays from the two-way classical signaling may decrease the communication rates.

To achieve *deterministic* error suppression of loss errors or operation errors, we may use quantum error correction (Azuma *et al.*, 2015a; Fowler *et al.*, 2010; Jiang *et al.*, 2009; Li *et al.*, 2013; Munro *et al.*, 2010; Muralidharan *et al.*, 2014b) or one-way entanglement distillation (Bennett *et al.*, 1996c; Zwerger *et al.*, 2018). The key idea is to encode a logical qubit into a block of physical qubits that are sent through the lossy channel, and then to use quantum error correction to restore the logical qubit. One may also include *one-way* classical signaling to assist the deterministic one-way entanglement distillation protocols (Bennett *et al.*, 1996a,c), but the additional one-way (forward) classical signaling from the sender does not affect the quantum channel capacity. Hence, all the deterministic error suppression (even when assisted by one-way signaling) can correct no more than 50% loss, which is consistent with the no-cloning theorem (Muralidharan *et al.*, 2014b; Stace *et al.*, 2009), and not more than 25% depolarizing errors (see Table IV). The existence of these finite thresholds itself implies the need

of quantum repeater nodes in the case of the use of deterministic error suppression, as such errors tend to depend on the communication distance (Briegel *et al.*, 1998).

Based on the methods adopted to suppress loss and operation errors, we can classify various QRs into three categories, as shown schematically in Table V. We refer to these as first, second, and third generations of QRs (Munro *et al.*, 2015; Muralidharan *et al.*, 2014b, 2016), to imply the increasing difficulty in technology with improved performance⁵. Note that the combination of *deterministic* suppression of loss errors and *probabilistic* suppression for operation errors, which only does not appear in Table V, is sub-optimal compared to the other three combinations.

Each generation of QRs performs best for a specific regime of operational parameters such as local gate speed, gate fidelity, and coupling efficiency. We consider both the temporal and physical resources consumed by the three generations of QRs and identify the most efficient architecture for different parameter regimes. The results can guide the design of efficient long-distance quantum communication links that act as elementary building blocks for future quantum networks.

1. First-generation repeaters

The first generation of QRs uses *probabilistic* error suppression to overcome practical imperfections—for example, HEGP can herald the successful entanglement generation while overcoming loss errors and 2-EDP can use two-way classical signaling to recognize successful entanglement distillation to suppress operation errors (Azuma *et al.*, 2012; Briegel *et al.*, 1998; Childress *et al.*, 2006b; Kok *et al.*, 2003; van Loock *et al.*, 2006; Munro *et al.*, 2008; Sangouard *et al.*, 2011; Zwerger *et al.*, 2012). Since we have explained the principle of QRs by exemplifying a simplified first-generation QR protocol in Sec. III.A.3, here we start by briefly summarizing how QRs from this generation can be used to correct losses with a simple example in which we assume there are no operation errors. Alice and Bob, separated by a distance L_{tot} , want to share a maximally-entangled qubit pair that they can use, e.g., to teleport a quantum state or to distill a private key. They are connected by a lossy medium such as a telecom fiber, having the typical loss of 0.2 dB/km (that is, an attenuation length $L_{\text{att}} \approx 22$ km). Supposing that $L_{\text{tot}} \gg L_{\text{att}}$, the direct transmission of a photon between Alice and Bob succeeds with a vanishingly small probability on the order of $e^{-L_{\text{tot}}/L_{\text{att}}} \ll 1$.

⁵ We may also classify QRs using other criteria, such as the physical platform, different operations, and so on. For instance, see Ref. (Razavi, 2018). We will discuss various physical platform and implementation in Sec. V.

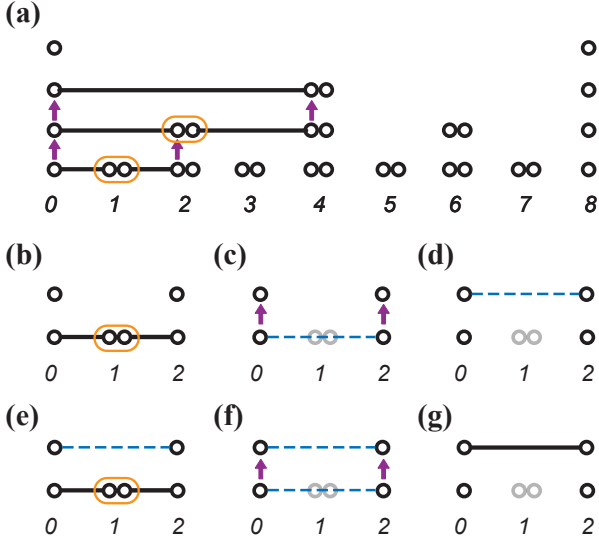


FIG. 5 The first generation repeater protocol (BDCZ scheme (Briegel *et al.*, 1998)). (a) In a realization based on the pumping protocol with $N + 1 = 9$ nodes, the number of qubits per node is bounded by $2 \log_2 2N = 8$. Each (orange) oval surrounding two vertices (or two qubits) describes application of Bell measurement to the two qubits for entanglement swapping. (b–d) Two entangled pairs with distance 1 are connected through entanglement swapping [(orange) oval] at node 1 to produce an entangled state with distance 2, which is stored in the qubits [as described by (purple) arrows] at higher level. (e–g) Another entangled state with distance 2 is produced to purify the entangled state [as described by (purple) arrows] stored in qubits at higher level. Similarly, entangled states with distance 2^n can be connected to produce entangled state with distance 2^{n+1} , which may be further purified, as indicated in (a). Figure from Ref. (Jiang *et al.*, 2007a). Copyright (2007) National Academy of Sciences.

The solution provided by first-generation QRs is to divide the total distance L between Alice and Bob into smaller lengths with the help of $N_{\text{QR}} = L_{\text{tot}}/L_0 - 1$ quantum repeater nodes. Here we assume that the nodes are evenly separated by an internodal distance L_0 and $L_0 = L_{\text{tot}}/2^n$ for simplicity. The role of each QR node is to share entanglement with its adjacent nodes: we use an HEGP strategy to create high-quality entanglement between a quantum memory and its counterpart to the immediate left, and between another memory and its counterpart in the adjacent QR node to the right. Each HEGP trial also takes a time $T_{\text{trial}} = t_{\text{op}} + t_c$, which depends on the total time t_{op} of operations and on the time $t_c = L_0/c$ for photons to arrive at the central measuring station and the classical signaling back to the QR node.

A typical HEGP procedure has success probability P_{ent} depending on the photon collection efficiency, fiber transmission efficiency, and photon detection efficiency. For the dual-rail encoding, without ancillary photons, the success probability $P_{\text{ent}} \leq 1/2$ even in the lossless limit,

limited by linear optics and by the photon loss probability (Calsamiglia and Lütkenhaus, 2001). However, we may use more advanced encoding to achieve a higher success probability $P_{\text{ent}} > 1/2$ (Azuma *et al.*, 2009, 2012; Martin and Whaley, 2019). In any case, if it succeeds, the HEGP tends to present high-quality entanglement between nearest neighbor nodes even under the existence of photon loss. Due to the probabilistic nature of HEGP, for the first-generation QR protocol to proceed, it is necessary to inform the adjacent nodes whether the HEGP has succeeded or not. In the case of a failure, the process is repeated until it succeeds. The entanglement generation procedure therefore succeeds in an average time $\langle T_{\text{ent}} \rangle = P_{\text{ent}}^{-1} T_{\text{trial}} = P_{\text{ent}}^{-1} (L_0/c + t_{\text{op}})$. In the case of a success, the entanglement can be stored in the quantum memories.

At each QR node, we can store entangled qubit pairs shared with an adjacent node, say the node on the immediate left, during the time required to produce an entangled pair with the adjacent QR node on the right. Thanks to this functionality of quantum memories, we see that not all the entanglement needs to be generated at the same time throughout the network; this is the reason that this strategy can outperform direct photon transmission and a quantum relay protocol (Jacobs *et al.*, 2002; de Riedmatten *et al.*, 2004; Waks *et al.*, 2002) (which uses repeater nodes but only distributes photonic Bell pairs from sending repeater nodes to their adjacent receiver nodes, in which Bell measurement is performed soon after receiving halves of the Bell pairs). When a QR node finally shares an entangled pair of qubits with each of its adjacent nodes, it performs entanglement swapping between its two quantum memories, such that if it succeeds, a maximally entangled pair is now shared between its two adjacent nodes. After repeating these entanglement swapping steps at each QR node, Alice and Bob end up with a maximally-entangled pair at a rate much higher than what is achievable with direct fiber transmission (see Sec. III.A.3 for detail).

So far, we have only considered loss errors and have thus assumed that information can be manipulated, transferred and stored faithfully. In practice, this is not the case; we ought to also handle operation errors, which eventually reduce the fidelity of the two qubits shared by Alice and Bob. This is achieved through an entanglement distillation scheme, which can be incorporated in first-generation QRs, for example, using a nested purification QR scheme, as introduced in the following paragraph.

As illustrated in Fig. 5, we start with distilled high-fidelity entangled pairs with separation $L_0 = L_{\text{tot}}/2^n$, created and stored in adjacent stations. At the k -th nesting level, two entangled pairs of distance $L_{k-1} = 2^{k-1}L_0$ are connected by entanglement swapping to extend entanglement to a distance $L_k = 2^k L_0$ (Zukowski *et al.*, 1993). As practical gate operations and entanglement swapping (Fig. 5 (b-d)) inevitably cause the fidelity of

entangled pairs to drop, 2-EDP may be incorporated at each level of entanglement extension (Fig. 5 (e-g)) (Deutsch *et al.*, 1996; Dür *et al.*, 1999). With n nesting levels of connection and distillation, a high-fidelity entangled pair over distance $L_n = L_{\text{tot}}$ can be obtained. Suppose T_{k-1} is the average time needed to prepare a distilled entangled pair over distance L_{k-1} , average time to prepare a distilled entangled pair over distance L_k is

$$T_k = \alpha_k T_{k-1} + \beta_k L_k / c = \alpha_k T_{k-1} + \beta_k 2^k t_c, \quad (34)$$

where $t_c = L_0/c$ is the communication time between neighboring repeater stations, α_k and β_k are dimensionless numbers capturing the time overhead associated with the entanglement swapping, distillation, and multiple rounds of classical communication. For simplicity, we assume each nesting level has similar overheads $\alpha_k \approx \alpha$ and $\beta_k \approx \beta$ for $k \geq 1$. The average time to generate distilled entangled pairs between neighboring repeaters is $T_0 = \beta_0 t_c$, with the time overhead β_0 associated with photon efficiency, entanglement generation and purification between neighboring repeater stations. From the recursive relation, we can obtain the average time to generate a distilled entangled pair over distance $L_n = L_{\text{tot}}$ is

$$T_{\text{tot}} = T_n \sim (L_{\text{tot}}/L_0)^{\log_2[\max(\alpha, 2)]} \max(\beta, \beta_0) t_c, \quad (35)$$

which increases polynomially with L_{tot} depending on the value of α .

For the simple mode of loss-only channel, $\alpha \approx \frac{3}{2} \frac{1}{P_{\text{swap}}}$, with prefactor $\frac{3}{2}$ for the time overhead associated with the requirement that two entangled pairs on both sides should be ready for entanglement swapping (Azuma *et al.*, 2021; Jiang *et al.*, 2007a; Sangouard *et al.*, 2011), and P_{swap} for the success probability of entanglement swapping. For example, $P_{\text{swap}} \leq 1/2$ for the Duan-Lukin-Cirac-Zoller quantum repeater protocol based on atomic ensembles and linear optics (Duan *et al.*, 2001). To overcome operation errors, we need entanglement distillation from at least two copies of entangled pairs, and hence $\alpha \geq 2$ for all entanglement distillation schemes (e.g., the Briegel-Dür-Cirac-Zoller (BDCZ) protocol (Briegel *et al.*, 1998) and the Childress-Taylor-Sørensen-Lukin (CTSL) protocol (Childress *et al.*, 2006b)), unless we use multiplexing in generating entangled pairs (Dür *et al.*, 1999).

The first generation of QRs reduces the exponential overhead in direct state transfer to only polynomial overhead, which is limited by the two-way classical signaling required by HEGP between non-adjacent repeater stations. The communication rate still decreases polynomially with distance and thus becomes very slow for long-distance quantum communication. The communication rate of first-generation QRs can be boosted using temporal, spatial, and/or frequency multiplexing associated with the internal degrees of freedom for the quantum memory (Bonarota *et al.*, 2011; Sangouard *et al.*, 2011).

The first generation of QRs can also be very efficient in entanglement resources. As shown in Fig. 5, the BDCZ protocol (Briegel *et al.*, 1998; Dür *et al.*, 1999) has a self-similar structure with $n = \log_2 \frac{L_{\text{tot}}}{L_0}$ nesting levels. We start with the elementary entangled pairs with initial fidelity⁶ F and distance L_0 between neighboring repeater nodes. In the j -th nesting level (with $j = 1, 2, \dots, n$), a repeater node performs entanglement swapping to convert two initial entangled pairs with fidelity F and the length $2^{j-1}L_0$ into an entangled pair with fidelity $F' (\leq F$ in general) and length of $2^j L_0$. The extended entangled pairs with fidelity F' are collected, and M pairs of them are used to distill a purified entangled pair with the initial fidelity F and the length of $2^j L_0$ through an entanglement distillation protocol. These imply that each purified entangled pair with fidelity F and with the length of $2^j L_0$ can be regarded as having been made from $2M$ entangled pairs with fidelity F and with the length of $2^{j-1}L_0$. Therefore, an entangled pair with fidelity F and with the length of $L_{\text{tot}} = 2^n L_0$ can be made up from $(2M)^n = (L_{\text{tot}}/L_0)^{1+\log_2 M}$ elementary entangled pairs.

In addition, the first generation of QRs can be highly efficient even in terms of quantum memory resources, if the purification of an unpurified entangled pair with the length of $2^j L_0$ ($j = n, n-1, \dots, 0$) can be done by a sequential application of the pumping protocol which “pumps” entanglement to the entangled pair out of a fixed unpurified auxiliary entangled pair with the same length of $2^j L_0$ (see Fig. 5) (Briegel *et al.*, 1998; Dür *et al.*, 1999). Here, how much entanglement is purified depends on both the initial fidelity and the shape of the fixed auxiliary pair. During the purification, we just need two pairs of memories, one for storing the entangled pair to be pumped and the other for storing the auxiliary entangled pair for each round, and the purification is regarded as having started from two unpurified pairs with the length of $2^j L_0$. One of these two unpurified pairs, as the auxiliary entangled pair, should be prepared repeatedly during the pumping purification, and it can be regarded as having been obtained by connecting two purified entangled pairs with the length of $2^{j-1}L_0$ through entanglement swapping. As a result, a purified entangled pair with the length of $2^j L_0$ can be regarded as having been made from an unpurified entangled pair (to be pumped at the j -th nesting level) with the length of $2^j L_0$ and from two purified pairs with the length of $2^{j-1}L_0$. By considering this recursively from $j = n$ to $j = 1$, a purified entangled pair with the length of $2^n L_0 (= L_{\text{tot}})$ is regarded as having been made from 1 unpurified entan-

⁶ A general definition of the fidelity between states ρ and σ is given by $F(\rho, \sigma) := \|\sqrt{\rho}\sqrt{\sigma}\|^2$, where $\|X\| := \text{Tr}\sqrt{X^\dagger X}$ is the trace norm (Jozsa, 1994). The “initial fidelity” here means the fidelity of an initial state ρ to a Bell state $|\Phi^+\rangle$, i.e., $F = F(\rho, |\Phi^+\rangle) = \langle \Phi^+ | \rho | \Phi^+ \rangle$.

gled pair (to be pumped at the n -th nesting level) with the length of $2^n L_0$, 2 unpurified pairs (to be pumped at the $n-1$ -th nesting level) with the length of $2^{n-1} L_0$, \dots , 2^{n-1} unpurified pairs (to be pumped at the 2nd nesting level) with the length of $2L_0$, and 2^n purified pairs with the length of L_0 . Since each of these entangled pairs needs two quantum memories, the maximum number N_{tot} of memories required during the protocol is $N_{\text{tot}} = 2 \sum_{j=0}^n 2^j = 2(2^{n+1} - 1) = 2(2L_{\text{tot}}/L_0 - 1) = 4L_{\text{tot}}/L_0 - 2$. For example, we have $n = 3$ in Fig. 5 (a), where 30 quantum memories are written, corresponding to N_{tot} memories.

There are different variations of the BDCZ protocol. Its measurement-based implementation using graph states is given in Ref. (Zwerger *et al.*, 2012). The DLCZ protocol simplifies it with the use of atomic ensembles and linear optics (Duan *et al.*, 2001). Room-temperature quantum repeaters have also been proposed using nitrogen-vacancy defect centers in diamond (Childress *et al.*, 2006b; Ji *et al.*, 2022). Reference (Sangouard *et al.*, 2011) provides a detailed review on various first-generation quantum repeaters based on atomic ensembles and linear optics, where HEGPs are based on Fock-state encoding, polarization encoding, and time-bin encoding. The concept of the nested purification in the BDCZ protocol, as well as the concatenation of quantum error-correcting codes (Knill and Laflamme, 1997), is generalized to distribute entangled pairs with fixed error to clients in a quantum network with arbitrary topology, regardless of their distance (Azuma, 2023).

We can further generalize the BDCZ protocol by introducing CV encoding. For example, we can take a hybrid CV-DV approach by interfering optical coherent-state signals to generate DV entanglement between repeater stations (Azuma *et al.*, 2012; Childress *et al.*, 2006b; van Loock *et al.*, 2006; Munro *et al.*, 2008). Moreover, we can design CV quantum repeaters to efficiently distribute CV entangled states with high fidelity over long distances (Dias and Ralph, 2017; Furrer and Munro, 2018; Shadreean *et al.*, 2020). Due to the Gaussian entanglement distillation no-go theorem (Eisert *et al.*, 2002; Fiurášek, 2002; Giedke and Cirac, 2002), the CV repeaters use non-Gaussian operations at the entanglement distillation protocols (Fiurášek, 2010; Ralph and Lund, 2009) to suppress loss errors.

2. Second-generation repeaters

The second generation of QRs uses *probabilistic* error suppression (see Sec. III.A.4.b) for loss errors and *deterministic* error suppression (see Sec. III.A.4.a) for operation errors (Jiang *et al.*, 2009; Li *et al.*, 2013; Mazurek *et al.*, 2014; Munro *et al.*, 2010). For example, we may first prepare the encoded states $|0\rangle_L$ and $|+\rangle_L$ using the Calderbank-Shor-Steane (CSS) codes and store them at

two adjacent stations. CSS codes are considered because of their fault-tolerant implementation of preparation, measurement, and encoded CNOT gates (Jiang *et al.*, 2009; Nielsen and Chuang, 2010). Then, an encoded Bell pair $|\Phi^+\rangle_L = \frac{1}{\sqrt{2}}(|0,0\rangle_L + |1,1\rangle_L)$ between adjacent stations can be created via teleportation-based non-local CNOT gates (Gottesman and Chuang, 1999; Jiang *et al.*, 2009) applied to each physical qubit in the encoded block using the entangled pairs generated through HEGP process. Finally, QEC is carried out when entanglement swapping at the encoded level is performed to extend the range of entanglement. Second-generation QRs use QEC to replace 2-EDP and therefore avoid the time-consuming two-way classical signaling between non-adjacent stations. The communication rate is then limited by the time delay associated with two-way classical signaling between adjacent stations and local gate operations. If the probability of accumulated operation errors over all repeater stations is sufficiently small, we can simply use the second generation of QRs *without* encoding. For instance, proposals based on single ion qubits, to which we can apply deterministic Bell measurement, fall into this category (Asadi *et al.*, 2020; Kimiaee Asadi *et al.*, 2018; Sangouard *et al.*, 2009).

We can generate entangled pairs through the HEGP process adapted for different photonic encoding schemes (see Sec. II.E). For dual-rail photonic encoding (time-bin, polarization, or path), we may use linear optics and photon detectors to herald the successful Bell measurement and also detect photon loss errors (e.g., Fig. 3 (a)). The potential limitation is that the success probability of the Bell measurement will be upper-bounded by 50% for dual-rail encoding. Alternatively, we may use bosonic encodings, such as GKP states, for HEGP (Fukui *et al.*, 2021). Different from the dual-rail encoding schemes, the GKP encoding can achieve deterministic Bell measurement with linear optics and homodyne detection (Gottesman *et al.*, 2000). In the presence of loss errors, there will be vacuum noise added to the system, which can be detected by the homodyne measurement. The GKP encoding can correct small added vacuum noise up to certain level, above which it is better to report the presence of large noise and restart the process.

Similar to the first-generation repeaters, we can also give bounds on the achievable communication rate for the second generation repeaters, which is limited by the HEGP and 2-EDP between neighboring repeater stations. For example, we have $R \leq \langle T_{\text{ent}} \rangle^{-1} \leq [2(L_0/c + t_{\text{op}})]^{-1}$. By reducing the distance L_0 to zero, and neglecting t_{op} , we see that this bound can, in principle, go to infinity. Yet, assuming $L_0 \rightarrow 0$ would require infinitely many QR nodes, $N_{\text{QR}} \rightarrow \infty$, and thus an infinite amount of resources (quantum memories).

The physical resources required for the second generation of QRs depend on the size of the CSS code, n_{code} . At each repeater station, we need at least $2n_{\text{code}}$ qubits

for storing the encoded states $|0\rangle_L$ and $|+\rangle_L$, and we also need additional memory qubits to store and purify entanglement between neighboring repeater stations (Jiang *et al.*, 2009). Hence, the total number of quantum memory qubits is $N_{\text{tot}} \sim n_{\text{code}} \frac{L_{\text{tot}}}{L_0}$.

The size of the encoding block, n_{code} , only needs to increase poly-logarithmically with the total distance L_{tot} . Asymptotically, there are CSS codes with $n_{\text{code}} \leq 19t$, which can correct up to t (bit-flip and dephasing) errors [obtained from the Gilbert-Varsharov bound, see Eq. (30) in (Calderbank and Shor, 1996)]. This implies that we only need $n_{\text{code}} \propto t \sim \ln \frac{L_{\text{tot}}}{L_0}$ that increases logarithmically with L_{tot} (Jiang *et al.*, 2009). In practice, however, it is might be challenging to initialize large CSS encoding block fault tolerantly with imperfect local operations. To avoid complicated initialization, we may construct larger CSS codes by concatenating smaller codes with r nesting levels, and the code size scales polynomially with the code distance, $n_{\text{code}} \propto t^r \sim (\ln \frac{L_{\text{tot}}}{L_0})^r$. Alternatively, we may consider the Bacon-Shor code (Bacon, 2006); the encoding block scales quadratically with the code distance $n_{\text{code}} = (2t + 1)^2 \sim (\ln \frac{L_{\text{tot}}}{L_0})^2$, and the initialization can be reduced to the preparation of $(2t + 1)$ -qubit Greenberger-Horne-Zeilinger (GHZ) states. For finite total distance L_{tot} , a more useful performance metric for comparing the QR protocols should quantify both the amount of physical resources, as well as the communication rate (see Sec. III.B.4).

3. Third-generation repeaters

The third generation of QRs relies on *deterministic* error suppression, such as QEC and one-way hashing (see Sec. III.A.4.a), to correct both loss and operation errors (Fowler *et al.*, 2010; Munro *et al.*, 2012; Muralidharan *et al.*, 2014b). The quantum information can be directly encoded in a block of physical qubits that are sent through the lossy channel. If the loss and operation errors are sufficiently small, the received physical qubits can be used to restore the whole encoding block, which is re-transmitted to the next repeater station. The third generation of QRs only needs *one-way* signaling and thus can achieve very high communication rates, just like classical repeaters only limited by local operation delays.

Various choices of quantum error-correcting codes can be used for the third generation of QRs (Knill and Laflamme, 1996). For qubit-based quantum error correction, we may use quantum parity codes (Ralph *et al.*, 2005) with moderate coding blocks (~ 200 qubits) to efficiently overcome both loss and operation errors (Munro *et al.*, 2012; Muralidharan *et al.*, 2014b). The surface code (Raussendorf *et al.*, 2007; Raussendorf and Harrington, 2007) or the tree-cluster code (Varnava *et al.*, 2006) can suppress more loss errors—up to 50%—with larger encoding blocks. For quantum codes based on d -level

quantum systems (e.g., based on time-bin encoding), we can implement quantum polynomial (Cleve *et al.*, 1999) codes to approach loss tolerances up to 50% (Muralidharan *et al.*, 2017) and quantum Reed-Solomon codes (Li *et al.*, 2008) to further improve the key generate rate (Muralidharan *et al.*, 2018). If we treat each optical mode as a continuous variable system, we may use bosonic quantum error-correcting codes (e.g., cat codes (Leghtas *et al.*, 2013; Mirrahimi *et al.*, 2014), binomial codes (Michael *et al.*, 2016), and GKP codes (Albert *et al.*, 2018; Gottesman *et al.*, 2000; Noh *et al.*, 2019)) to correct loss errors. The advantage of bosonic codes is that they can efficiently use the large Hilbert space of bosonic systems and reduce the number of bosonic modes, which might be advantageous to maximize the usage of our optical quantum channel bandwidth (Li *et al.*, 2017). To further suppress the residual errors from the first-level bosonic codes, we may concatenate it with a second-level DV encoding, which leads to a concatenated CV-DV encoding scheme. To reduce the resource cost with respect to an architecture for which all repeaters are the same, we may introduce two different types of repeaters, correcting errors at two different levels, respectively (Rozpędek *et al.*, 2021).

Note that the second and third generations of QRs can achieve communication rates much faster than the first generation over long distances, but they are technologically more demanding. For example, they require high-fidelity quantum gates, as QEC only works well when operation errors are below the fault-tolerance threshold. The repeater spacing for the third generation of QRs is smaller compared to the first two generations of QRs because error correction can only correct a finite amount of loss errors deterministically (only up to 50% loss error rates deterministically (Muralidharan *et al.*, 2014b; Stace *et al.*, 2009)).

Similar to the second generation of QRs, the physical resources required for the third generation of QRs depend on the size of the quantum error-correcting code. We may use n_{code} to characterize the size of the encoding blocks based on qubits or bosonic modes. At each repeater station, we need $O(n_{\text{code}})$ quantum memories to perform error correction suppressing not only operation errors, but loss errors as well. The total number of quantum memories (in terms of qubits or bosonic modes) needed is $N_{\text{tot}} \sim n_{\text{code}} \frac{L_{\text{tot}}}{L_0}$. In principle, we may use QEC over optical modes to fully replace the need of the traditional atomic or solid-state quantum memory, which inspires the design of all-photon quantum repeaters as discussed in. Sec III.C.

For the specific application of quantum key distribution, we may use QRs to generate random secret classical bits shared by remote parties. Since the ultimate goal is to generate secret keys, rather than the entangled states, we might slightly relax the requirement of quantum memories. In particular, in this case, even for first

and second generation repeaters, there is no need of long-lived quantum memories to store the entangled states at the *end* stations, because they can be measured simultaneously with all intermediate repeater stations (Jiang *et al.*, 2009) (see Sec. VI.A.2). However, notice that the first and second generation QRs still need quantum memories at repeater nodes, whose required memory time is longer than that of third generation QRs.

4. Comparison of three generation of QRs

To present a systematic comparison of different QRs in terms of efficiency, we need to consider both temporal and physical resources. The temporal resource depends on the rate, which is limited by the time delay from the two-way classical signaling (in first- and second-generation repeaters) and the local gate operation (in the second and third generations) (Jiang *et al.*, 2007a). The physical resources depend on the total number of qubits needed for HEGP (first and second generations) and QEC (second and third generations) (Bratzik *et al.*, 2014; Muralidharan *et al.*, 2014b). One may quantitatively compare the three generations of QRs using a cost function (Muralidharan *et al.*, 2014b) related to the required number of qubit memories to achieve a given transmission rate. If a total of N_{tot} qubits are needed to generate secure keys at R bits/second, a cost function is defined as

$$C(L_{\text{tot}}) = \frac{N_{\text{tot}}}{R} = \frac{N_s}{R} \times \frac{L_{\text{tot}}}{L_0}, \quad (36)$$

where N_s is the number of qubits needed per repeater station, L_{tot} is the total communication distance, and L_0 is the spacing between neighboring stations. Since the cost function scales at least linearly with L_{tot} , to demonstrate the additional overhead associated with L_{tot} , a *cost coefficient* can be introduced as

$$C'(L_{\text{tot}}) = \frac{C(L_{\text{tot}})}{L_{\text{tot}}}, \quad (37)$$

which can be interpreted as the resource overhead (qubits \times time) for the creation of one secret bit over 1 km (with target distance L_{tot}). Besides the fiber attenuation (with $L_{\text{att}} = 20$ km for telecom wavelengths), the cost coefficient also depends on other experimental parameters, in particular the coupling efficiency η_c , the gate error probability ϵ_G , and the gate time t_0 .

We may summarize the analysis of QRs based on the cost coefficient (Muralidharan *et al.*, 2016) using bubble and region plots in the three-dimensional parameter space, as shown in Fig. 6, which compares representative protocols from three generations of quantum repeaters (Briegel *et al.*, 1998; Jiang *et al.*, 2009; Muralidharan *et al.*, 2017).⁷ The bubble color indicates the associated

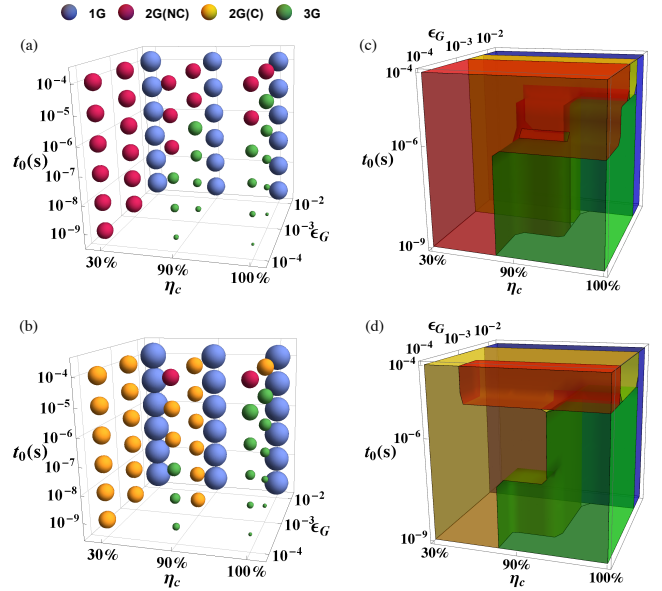


FIG. 6 The bubble plot comparing various QR protocols in the three-dimensional parameter space spanned by coupling efficiency η_c , gate error probability ϵ_G , and gate time t_0 , for a) $L_{\text{tot}} = 1000$ km and b) $L_{\text{tot}} = 10,000$ km. The bubble color indicates the associated optimized QR protocol, and the bubble diameter is proportional to the cost coefficient. The region plots (c) and (d) showing the distribution of different optimized QR protocol in the three dimensional parameter space for $L_{\text{tot}} = 1000$ km and $L_{\text{tot}} = 10,000$ km respectively. The region plot (c) contains a yellow region of second generation with encoding, which can be verified in a bubble plot with a finer discretization of ϵ_G . Figure from (Muralidharan *et al.*, 2016).

optimized QR protocol, and the bubble diameter is proportional to the cost coefficient. The parameter space can be divided into the following regions: (I) For high gate error probability ($\epsilon_G \gtrsim 1\%$), the first generation dominates; (II.A) For intermediate gate error probability, but poor coupling efficiency or slow local operation [$0.1 \frac{L_{\text{att}}}{L_{\text{tot}}} \lesssim \epsilon_G \lesssim 1\%$ and ($\eta_c \lesssim 90\%$ or $t_0 \gtrsim 1\mu\text{s}$)], the second generation *with* encoding is more favorable; (II.B) For low gate error probability, but low coupling efficiency or slow local operation [$\epsilon_G \lesssim 0.1 \frac{L_{\text{att}}}{L_{\text{tot}}}$ and ($\eta_c \lesssim 90\%$ or $t_0 \gtrsim 1\mu\text{s}$)], the second generation *without* encoding is more favorable; (III) For high coupling efficiency, fast local operation, and low gate error probability ($\eta_c \gtrsim 90\%$, $t_0 \lesssim 1\mu\text{s}$, $\epsilon_G \lesssim 1\%$), the third generation becomes the most favorable scheme in terms of the cost coefficient

⁷ The communication rate of the first generation of QRs can be

boosted using temporal, spatial, and/or frequency multiplexing associated with the internal degrees of freedom for the quantum memory (Afzelius *et al.*, 2009; Sangouard *et al.*, 2011).

C. All-optical repeaters

While the traditional repeater protocol necessitates physical memories—stationary quantum systems—to store quantum information during the long waits associated with long-distance entanglement generation, it is fairly nontrivial whether the protocol can be implemented all-optically just by replacing the memories with all-optical memories like ones in (Leung and Ralph, 2006). On the other hand, repeaters featuring QEC codes could preclude the necessity of such memories, as QEC codes can instead deterministically suppress the noise and loss affecting qubits. Indeed, error-corrected repeaters, which intersect with the second and third generations discussed above, are shown to be implementable all-optically; in this case, the significant differences in analysis and implementation compared to matter-based repeaters warrant special attention, which we provide in this subsection.

To better understand all-optical or all-photonics repeaters, we first review the operating principle of another quantum information protocol, *measurement-based quantum computation (MBQC)* (sometimes referred to as one-way computation⁸), especially relevant for optical implementations. In a measurement-based quantum computer (Raussendorf and Briegel, 2001), to be contrasted with a gate-based computer, an entangled resource state, namely a cluster (or graph) state (Sec. II.D.1), is prepared initially and the computation proceeds by way of adaptive *single-qubit* measurements on this state. For physical platforms suffering from probabilistic entangling gates, among them discrete-variable dual-rail photonics (see Sec. II.E), this type of computer has the advantage that such probabilistic gates are involved only in the preparation of the initial resource states and are not necessary during the computation. This circumvents the exponential decay of the computational success with the number of entangling operations and dramatically reduces the resource costs (Browne and Rudolph, 2005; Kok *et al.*, 2007; Nielsen, 2004) compared to the gate-based scheme (Knill *et al.*, 2001a). Furthermore, the measurement-based approach allows for fixed-depth circuits where a physical qubit only undergoes a finite (and generally small) amount of gate operations before being consumed by a single-qubit measurement. This approach therefore accords well with flying qubits; it helps overcome the weakness of probabilistic entangling gates for certain photonic encodings, and drastically cuts down on the amount of loss each photon experiences.

In measurement-based computation, universality—the ability to approximate any unitary on any number of data

qubits arbitrarily well—is achieved through an appropriate choice of cluster state (Briegel and Raussendorf, 2001), as well as access to non-Clifford operations. Fault-tolerance—the exponential suppression of state preparation, gate and measurement errors—is obtained through an error-correcting code (Sec. III.A.4.a.1), which translates to a cluster state with a special shape and structure (the encoding); a prescription for implementing logical operations through adaptive single-qubit measurements; and a means of detecting and correcting the error, including an algorithm for extracting the outcomes of logical measurements (the decoding and recovery).

A common feature of recent architectures of all-optical repeaters is that they are realizable through measurement-based implementations of QEC codes. A measurement-based quantum repeater operates in much the same way as a measurement-based computer; however, there are a handful of salient distinctions, emblematic of the differences between computation and communication. First, gate-set universality is not necessary for communication, meaning Clifford operations suffice. Second, the dominant source of errors for the photonic states comprising optical repeaters—loss—is an even larger threat. Third, in contrast to computation, which can be done locally, the goal of communication is inherently nonlocal—to entangle spatially distant objects. Since noise for physical qubits generally increases with time, it is important to take the classical communication time into account.

With these general notions out of the way, in the next subsections we overview the workings of several protocols for all-optical repeaters and describe promising schemes for the preparation of repeater graph states. We begin with a summary of the first all-photonics repeater proposal (Azuma *et al.*, 2015a), as an instructive example.

1. Original all-photonics repeaters

Our review of the all-photonics repeaters introduced in (Azuma *et al.*, 2015a) begins with a description of the repeater graph state (RGS). The ideal RGS that the authors propose has two layers.

The inner or core layer is a *complete graph* or *clique* (Fig. 7), which is locally equivalent to a GHZ state of n qubits from Eq. (20). The qubits in the inner layer are tailored to play the same role as quantum memories in a second-generation quantum repeater protocol. Recall the assumption of the second-generation QR protocol about quantum memories which allow us to apply *deterministic* Bell measurements only on quantum memories which have successfully shared entanglement with adjacent repeater nodes (see III.B.2). To make photonic qubits play this role, the core qubits in the RGS of Fig. 8

⁸ “One-way” has a special meaning in quantum communication, so we forego this terminology.

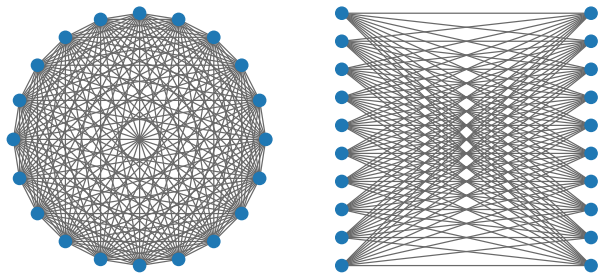


FIG. 7 A clique (left) and biclique (right). In the former, each vertex is connected with every other. In the latter, each vertex from the left set is connected with a vertex on the right, but the sets are internally disconnected. These graphs can underlie repeater graph states. See Sec. II.D.1 for more on graph states.

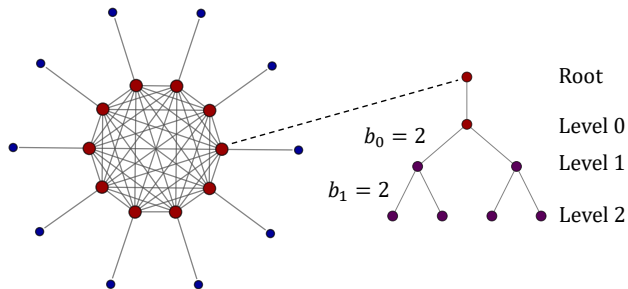


FIG. 8 Encoded repeater graph state (RGS) proposed in (Azuma *et al.*, 2015a). The RGS has two layers (left): the inner layer is composed of core qubits [big (red) vertices, closer to the center]; the outer layer is composed of outer qubits (or called leaves) [small (blue) vertices, further from the center]. Each vertex in the clique (left) is a logical qubit, which can be encoded in, e.g., the Varnava tree code (Varnava *et al.*, 2006) (right) to protect itself from loss (as well as general errors under the restriction of Pauli measurements). Displayed are the levels and branching parameters $\{b_0, b_1, \dots, b_{d-1}\}$ of the tree ($d = 2$ in this figure). Note the root and 0th-level qubits [two upper (red) qubits] in the tree will be measured out in the X basis, connecting the qubits in the first level with all of the neighbours of the root qubit. The inner logical qubits, conduits for the entanglement swapping, are connected to outer unencoded physical leaf qubits, which help effect the entanglement generation.

are prepared in a complete-graph state⁹ as in Fig. 7 (to overcome the probabilistic nature of the linear optical Bell measurements). In particular, if we apply X -basis measurements to two of them and Z -basis measurements

⁹ However, it was shown in (Russo *et al.*, 2018; Tzitrin, 2018; Tzitrin *et al.*, 2020) that some of the connections in the clique comprising the RGS are unnecessary, so that some variant, such as the biclique in Fig. 7, is sufficient as core qubits.

to the other qubits, it works as the Bell measurement on the two qubits and decouples the others (although we only use single-qubit measurements). To achieve these X -basis or Z -basis measurement deterministically even under photon loss, the qubits in the inner layer are encoded into a larger graph state with sufficient redundancy. In (Azuma *et al.*, 2015a), a tree-graph QEC code proposed by Varnava *et al.* (Varnava *et al.*, 2006) is considered for this purpose, as demonstrated schematically on the right panel of Fig. 8. This code places a qubit to be encoded at the root of a tree graph state composed of physical qubits. Then, it allows one to execute an arbitrary logical single-qubit measurement on the encoded qubit deterministically, even under loss, via single-qubit measurements on the physical qubits. Increasing the size of the tree graph state with increasing losses will ensure the correction succeeds, as long as the loss probability per physical qubit is less than 50%, a threshold consistent with the no-cloning theorem.

The other layer of the RGS consists of outer qubits or leaves appended to the vertices of the core graph; these are analogous to photons entangled with quantum memories for the purpose of HEGP in the second-generation QR protocol. In fact, a pair of outer qubits, each of which belongs to different RGSs, will be subject to a linear-optical Bell measurement in order to entangle their neighboring core qubits. Combining these layers of the RGS, the final state proposed by (Azuma *et al.*, 2015a) is shown in Fig. 8.

With an understanding of the RGS, we can now overview the precise operations required for Alice and Bob to establish an entangled pair in a given clock cycle of the all-photonic repeater protocol. The scheme is illustrated in Fig. 9. We use the notation from before: L is the total channel length; N is the number of repeater stations (sources or major nodes), not including Alice and Bob; m the number of parallel pulses. This means that there are $N + 1$ measurement stations (receivers or minor nodes), and $M = 2m$ is the size of the RGS, if it is symmetric.

Let us assume that an RGS is available at each source node (leaving the various preparation mechanisms for Sec. III.C.3). Then, each of the two nodes neighboring the source node receives half of photons in the RGS prepared and sent by the source. On arrival of the photons, every receiver first conducts simultaneous BSMs (Fig. 3 (a)) on m pairs of leaf photons of RGSs from different source nodes; this connects their adjacent inner qubits. Although each such BSM can only succeed with a probability of at most $1/2$ (and it is less than $1/2$ in practice, because of the losses experienced by the leaves), with m large enough, at least one BSM per station would be guaranteed to have succeeded. Then, depending on the outcomes of the BSMs, every receiver node applies X -basis measurements on a pair of the inner qubits whose adjacent leaves have been subject to a

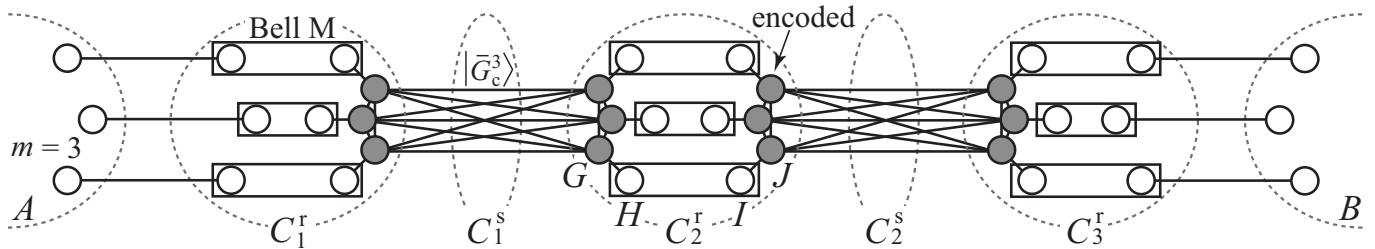


FIG. 9 Summary of original all-photonic repeater scheme (Azuma *et al.*, 2015a). Alice (A) and Bob (B) would like to establish one entangled pair; each prepares m Bell pairs ($m = 3$ in this figure) and sends them to a nearby receiver. Repeater graph states are created at C_1^s and C_2^s and their qubits are sent to adjacent receivers C_1^r and C_2^r , respectively. The receivers perform m simultaneous Bell state measurements on the outer qubits. In every receiver node, X -basis measurements is performed on a pair of inner qubits adjacent to outer qubits to which the Bell measurement is successfully applied, while Z -basis measurements are conducted on the other inner qubits. Figure from (Azuma *et al.*, 2015a).

successful BSM, and Z -basis measurements on the other inner qubits. Since inner qubits are encoded into the tree-graph code, these single-qubit measurements succeed almost deterministically (as long as the loss is below the threshold of 50%). As a result, the Z -basis measurements transform the total state into a linear cluster state between Alice and Bob, which is then converted into a Bell pair between them by the X -basis measurements, according to the effects detailed in Sec. II.D.1.

Importantly, the choice of the measurement on an inner encoded qubit, and accordingly on the physical qubits composing the tree cluster, depends on the measurement outcomes from the outer qubits. This means it is necessary to convey classical information from the outer qubits to the inner qubits. However, this can be done locally at each receiver node—that is, just by using a local active feedforward technique—as the inner qubits are transmitted together with their adjacent outer qubits. Therefore, the amount of necessary signalling is designed to be minimal, reducing time-dependent loss and errors for the photons.

Although loss is the dominant source of noise, one cannot dismiss other sources of error. Aided by a majority vote protocol, the tree-graph code of Varnava *et al.* is robust against general errors under the restriction of X -basis or Z -basis measurements on the encoded qubit, in contrast to other single-qubit measurements. In Sec. III.C.2, we overview an optical repeater protocol that instead makes use of parity codes (Ewert *et al.*, 2016). The existence of a better code specifically suited to an all-photonic repeater—in terms of error tolerance and overheads—is an important open question.

The all-optical protocol needs no quantum memories, including qubits held by Alice and Bob, for the applications in which entanglement for Alice and Bob, once generated, is consumed immediately to generate classical output strings, such as QKD (Bennett *et al.*, 1992; Koashi, 2009; Lo and Chau, 1999; Mayers, 2001; Portmann and Renner, 2022; Renner, 2008; Shor and Preskill, 2000), non-local measurements (Clerk *et al.*, 2010; Vaid-

man, 2003), and cheating strategies in position-based quantum cryptography (Buhrman *et al.*, 2011; Kent *et al.*, 2011; Lau and Lo, 2011). However, for applications that demand strictly a quantum output state to Alice and Bob, such as quantum teleportation and distributed quantum computation (Collins *et al.*, 2001; Eisert *et al.*, 2000; Gottesman, 1999), the applications themselves require Alice and Bob to have quantum memories with memory time on the order of classical communication time between Alice and Bob, because of the necessity of classical signaling. See Sec. VI.A.2 or Ref. (Azuma *et al.*, 2015a) for detail.

2. Other optical repeaters

a. Modified all-photonic repeaters. Although Ref. (Pant *et al.*, 2017) aims to analyze the performance of the all-photonic repeaters of Ref. (Azuma *et al.*, 2015a), the authors make several modifications that warrant discussion.

First, so-called *boosted* Bell state measurements (BBSMs) are employed in (Pant *et al.*, 2017). The previously cited maximal linear-optical Bell measurement success rate of $1/2$ can be increased with additional resources, such as ancillary photons in separable (Ewert and van Loock, 2014) or entangled (Grice, 2011) states, weak nonlinearities (Barrett *et al.*, 2005), and pre-detection squeezing (Kilmer and Guha, 2019; Zaidi *et al.*, 2015). However, BBSMs are no panacea: they increase experimental complexity and overhead, and infinite resources are still needed for unit probability, in line with a no-go theorem (Lütkenhaus *et al.*, 1999). The specific BBSMs (Ewert and van Loock, 2014) employed in (Pant *et al.*, 2017) succeed $3/4$ of the time. The analysis shows that they result in a net improvement to the overheads.

A more crucial design change is in the treatment of the inner qubits. In the original proposal, photons forming the clique of the RGS—the encoded inner qubits—are sent to neighbouring receiver nodes, together with their adjacent leaves, while Pant *et al.* assume they are stored

locally at the source nodes in fiber spools. In the original proposal, signalling from the leaves to the inner qubits can be done via local active feedforward; however, all the physical qubits in the encoding must be sent, necessitating a large number of fiber connections. While resulting in fewer fiber connections, the approach of Pant *et al.* comes at the expense of an increased loss, which stems from the necessity of signalling from the leaves to the inner qubits over the associated distance.

Finally, there is also a modification of the original scheme in Pant *et al.* with regards to the multiplexing strategy in state generation, which is discussed briefly in Sec. III.C.3.

b. Repeaters based on encoded Bell measurements. In (Ewert *et al.*, 2016; Lee *et al.*, 2019b), all-optical repeater protocols are presented based on *parity codes* (Ralph *et al.*, 2005). Specifically, the authors in (Ewert *et al.*, 2016) make use of Bell states with parity encoding. The graph states locally equivalent to the encoded Bell states look remarkably like the RGS from the original protocol: they are bicliques (complete bipartite graphs) with multiple leaves per node (Ewert and van Loock, 2017). However, the protocol of Ewert *et al.* itself is conceptually different from the all-photonic repeaters of (Azuma *et al.*, 2015a) (Zwenger *et al.*, 2016); it sends an encoded qubit from a sender to a receiver, directly, which makes it closer to the third-generation schemes of (Knill and Laflamme, 1996; Munro *et al.*, 2015; Muralidharan *et al.*, 2014a; Varnava *et al.*, 2007; Zwenger *et al.*, 2014) based on quantum error correction than the protocol of (Azuma *et al.*, 2015a), which can be regarded as a time-reversed version of a second-generation quantum repeater protocol. In their protocol (Ewert *et al.*, 2016), Bell measurement efficiency and loss tolerance improves as the size of the parity code increases. Furthermore, their scheme does not require active feedforward techniques, lowering local operation times, reducing losses, and facilitating on-chip integration. The concatenated Bell measurement scheme in (Lee *et al.*, 2019b) reaches the fundamental limits for Bell measurement efficiency and loss tolerance under the constraints of linear optics and the no-cloning theorem. Regarding loss-tolerance, this scheme also saturates the fundamental loss tolerance limits for logical Bell measurements based on adaptive linear-optical physical Bell measurements (Hilaire *et al.*, 2023). However, recent Bell measurement schemes (Bell *et al.*, 2022; Hilaire *et al.*, 2021b), based on an adaptive combination of physical two-photon Bell measurements and single-qubit measurements, exhibit an even stronger loss tolerance (saturating the no-cloning limit). So far, the performances of these new logical Bell measurement schemes remain to be evaluated in a quantum repeater scheme.

c. Bosonic repeaters. Certain repeaters based on continuous-variable states have been proposed (Fukui *et al.*, 2021; Rozpędek *et al.*, 2021). They leverage the inherent error-correction properties of bosonic encodings along with higher-level qubit codes to create what can be viewed as concatenated CV-DV error-correcting codes. Recall from Sec. II.E that there are several advantages to the GKP encoding in particular. First, it can tolerate small displacement errors; since any continuous error can be decomposed into displacements, it can natively treat loss errors as well. In fact, it was discovered that GKP states far better against loss errors in certain settings than codes tailored to handle losses (Albert *et al.*, 2018). Furthermore, for GKP states, entangling gates and Bell measurements are deterministic contingent on the availability of Gaussian resources, with the only probabilistic component being state generation. Finally, additional (analog) information obtained from the GKP-level error correction can be used to improve the logical error rates at the qubit code level (Fukui *et al.*, 2017; Noh and Chamberland, 2020).

The repeater architecture in (Rozpędek *et al.*, 2021) leverages the above advantages of GKP encodings and uses two types of repeaters: those consisting purely of GKP states, which can correct small displacement errors, and those comprised of GKP states concatenated with small qubit-level codes. In a related work, the authors in (Fukui *et al.*, 2021) compare using GKP encoding by itself, in a one- and two-way scheme, as well as with higher-level encodings.

3. Repeater graph state generation

Producing a large, high-quality optical graph state for measurement-based quantum information protocols is a tall order. In all-optical approaches, the stochasticity of entangling operations in some encodings (e.g., dual-rail) and of state preparation in others (e.g., GKP states) can result in large overheads; in matter-based approaches, effects like decoherence and inhomogeneity between emitters can result in significant decay of entanglement with the size of the target state. Nevertheless, there has been steady theoretical and experimental progress towards high-probability, high-fidelity cluster state generation. Let us discuss some promising ways of preparing optical graph states here.

a. General framework. Optical graph state generation can be understood in a general framework that involves the “stitching” of smaller resource states into iteratively larger states. Measurement-based entangling operations, such as those used for dual-rail encodings, are more formally referred to as *fusion gates* (Browne and Rudolph, 2005), introduced in (Pittman *et al.*, 2001). Fusion

gates on two optical modes, each of which may have a single photon, come in two varieties: *Type-I fusions*, which consume a single photon to create larger one-dimensional cluster states, and *type-II fusions* (essentially rotated Bell measurements) which consume two photons to grow cluster states in higher dimensions. As with BSMS, fusion probabilities may also be boosted with additional resources, a fact that has been exploited for RGS generation in (Pant *et al.*, 2017); as before, this introduces tradeoffs with experimental complexity and overheads (Gimeno-Segovia, 2016). For completeness, we also mention fusion-based quantum computation (FBQC) (Bartolucci *et al.*, 2023), a proposed alternative framework to MBQC where the fusion operations serve both to create entanglement and perform logical operations.

The schema for generating optical graph states is as follows:

1. *Unit resource production.* First, an optical circuit produces the smallest unit states. These can be single-qubit states or small entangled states, such as Bell pairs, n -partite GHZ states for $n \geq 3$, or few-qubit linear cluster states.
2. *Growth into meta-units.* As an optional intermediary step, the unit resources can be combined into larger meta-units. The utility of this extra step is to leave open the possibility, for example, of generating dual-rail n -partite GHZ states directly from single photons, or instead from photonic Bell pairs (see, for example, (Gimeno-Segovia, 2016)).
3. *Stitching.* Units or meta-units are entangled iteratively until the desired graph state is created. For dual-rail encodings, this can be achieved with type-II fusions; for GKP states, this can be done with continuous-variable CZ gates.

A few notes are in order. First, the framework accommodates matter-based optical graph state generation; in this case, the entanglement in the growth or stitching stages can be achieved either directly at the optical level, or assisted by the interaction between emitters. Second, each step carries an associated probability and fidelity that depends on the choice of encoding, the scheme for generating and entangling the resources, and the particular hardware implementation. Other considerations that will affect the architectural design include how much of the state can be made spatially (i.e., with the state sources arranged space) or temporally (i.e., with entanglement between states generated at different time steps). This is related to the question of how much of the graph state (e.g., how many layers in a regular cluster state) must exist at one time.

b. Dual-rail graph states. We review two different approaches to produce a graph state of dual-rail encoded qubits: one all-optical but probabilistic, the other relying on matter qubits but deterministic.

1. Probabilistic (optical) generation The original all-photonic repeater proposal (Azuma *et al.*, 2015a) relies on the approach taken in (Varnava *et al.*, 2007, 2008) for generating a tree graph state specified by a branching parameter $\{b_0, b_1, \dots, b_{d-1}\}$ (Fig. 8), where the root qubit of the tree graph state is connected to a 0th-level qubit, the 0th-level qubit is connected to b_0 1st-level qubits by edges and every i th-level qubit is connected to b_i $(i + 1)$ th-level qubits by edges ($i = 0, 1, \dots, d - 1$). As the encoding, the root and the 0th-level qubits are measured offline in the X basis. The tree graph state can be transformed into an RGS. The protocol of Varnava *et al.* proceeds as follows.

First, six single photons are prepared with single-photon sources. The photons are then sent to an optical circuit composed of beamsplitters, a type-I fusion gate and a type-II fusion gate, which produces a 3-partite GHZ state with probability $1/32$. Thanks to the design of this circuit, even if single-photon sources and detectors do not have unit efficiency, the generated 3-partite GHZ state is affected only by individual (uncorrelated) loss (Varnava *et al.*, 2008). This GHZ state then becomes the unit resource to produce the RGS. In particular, two 3-partite GHZ states are converted to a 4-partite GHZ state by a type-II fusion gate, and this 4-partite GHZ state corresponds to a three-qubit tree, i.e., $\{2\}$ -tree, with a redundant root qubit composed of two qubits. Then, from these elementary $\{2\}$ -trees, one can efficiently generate an arbitrary $\{b_0, b_1, \dots, b_{d-1}\}$ -tree from the bottom (d -th level) to the top (0-th level), with the help of type-II fusion gates.

Several generalizations or modifications are possible for this procedure. In (Pant *et al.*, 2017), the authors choose the more efficient generation scheme of (Li *et al.*, 2015), consider boosted fusion gates, improve the multiplexing strategy, and reorder the local measurements unconditioned on BSM outcomes. Furthermore, it is possible to create n -partite GHZ resource states with probability $1/2^{2n-1}$, and this number can theoretically be increased with Bell-state inputs rather than single-photon inputs, as well as boosted BSMS (Gimeno-Segovia, 2016; Joo *et al.*, 2007; Varnava *et al.*, 2008; Zhang *et al.*, 2008). For optical repeaters based on other error-correcting codes—which correspond to other graph states, these resource states can be stitched according to the different, tailored procedures.

2. Deterministic (matter-based) generation Unlike fusion-based approaches, which are fundamentally probabilistic, the protocol of Buterakos *et al.*

(Buterakos *et al.*, 2017), which uses emitter and ancilla qubits to generate the RGS, is—at least in principle—deterministic. The generation of linear cluster states from a single emitter was proposed by Schön *et al.* for atomic systems (Schön *et al.*, 2005) and by Lindner and Rudolph for quantum dots (QDs) (Lindner and Rudolph, 2009). More complex graph states, including a 2D square lattice cluster state, can be created by a linear chain of emitters with nearest-neighbor coupling (Economou *et al.*, 2010; Gimeno-Segovia *et al.*, 2019). Indeed, any graph state can be created with these ingredients (Russo *et al.*, 2019). In (Buterakos *et al.*, 2017), the key mechanism for generating the RGS is to entangle the emitter with an ancilla and pump it to produce one arm of the RGS, which emerges entangled to both the emitter and ancilla. The emitter is then measured and thus removed from the graph and the process is repeated until all the photonic arms are connected to the ancilla, which is assumed to have longer coherence time compared to the emitter. Measurement of the ancilla in the Y basis disentangles it from the graph and connects all the inner photons to each other, completing the RGS.

An attractive feature of the protocol of Ref. (Buterakos *et al.*, 2017) is that it is quite economical in terms of resources, which are quantified by the number of required matter qubits: To generate the unencoded version of the RGS, only one emitter and one ancilla are needed, irrespective of the size of the graph. In addition to the unencoded version, Buterakos *et al.* provide a recipe for the deterministic creation of arbitrarily large *encoded* RGSs in which the inner qubits are encoded using trees of depth 2 or 3. These protocols only require three matter qubits, including two emitters and one ancilla. Hilaire *et al.* (Hilaire *et al.*, 2021a) give a more general recipe for generating RGSs with arbitrarily deep tree encodings of the core photons in which the requisite number of matter qubits scales linearly with the tree depth d ($d-1$ emitters and 2 ancilla qubits). In this case, the number of required CZ gates is $2m \left(2 + \sum_{k=0}^{d-2} \prod_{j=0}^k b_j \right)$, where b_j denotes the branching vector component of the tree at level j and $2m$ is the number of arms in the RGS. These ideas for the deterministic generation of entangled photonic states were generalized in (Li *et al.*, 2021a), where a recipe for the generation of an arbitrary graph, using the minimal number of emitters, was provided.

Buterakos *et al.* also introduced a recipe for producing tree graphs of arbitrary depth d with k arms at each vertex using $d-1$ emitters and one ancilla. The number of CZ gates required in this case is $\frac{b^d + (-1)^{d+1}}{k+1} - 1$. This approach for creating tree-encoded photonic qubits is a powerful capability in its own right and can be applied to quantum repeaters of any generation. For example, Borregaard *et al.* (Borregaard *et al.*, 2020) employ this tree generation procedure in their proposed scheme to implement third-generation repeaters using SiV defects

in diamond as memory qubits.

The deterministic RGS protocol can be applied to any type of dual-rail encoding. Many of the proposals for graph state generation, especially with quantum dots, consider photon polarization encoding, but time-bin has also been proposed with these systems (Lee *et al.*, 2019a). In the case of time-bin, an alternative deterministic way of generating graph states is to use a single emitter and time-delayed feedback, as proposed by Pichler *et al.* (Pichler *et al.*, 2017), and adapted for RGS generation in (Zhan and Sun, 2020). In order to implement a maximally entangling gate, however, these approaches require the experimentally challenging capability of strong coupling between the emitter and the photonic waveguide where the photons propagate.

For the physical implementation of deterministic RGS generation schemes, modest-sized registers of well-controlled emitters and ancilla qubits are needed. The emitters need to be of high quality, especially in terms of brightness, so that the photon is emitted in the desired mode and successfully collected. This is critical for the protocol to be classified as deterministic. The register should also feature ancilla qubits with long coherence times, albeit not as long as what is required for quantum memories in first- and second-generation repeaters, along with the ability to perform high-fidelity gates between emitters and ancillae.

Self-assembled QDs are leading contenders for RGS generation. Indeed, the first experimental demonstration of an emitter-based cluster state generation protocol (Schwartz *et al.*, 2016) employed exciton-biexciton transitions in these systems. QDs are excellent photon emitters. They have a very efficient optical (excitonic) transition with a timescale of 1 ns (100 ps) without (with) coupling to a cavity. The QD community has made rapid progress over the last several years to improve the brightness, indistinguishability, and purity of QD photon sources (Senellart *et al.*, 2017). On the other hand, QDs have relatively low coherence times compared to point defects and atomic qubits and lack a long-lived quantum memory to act as the ancilla. Nevertheless, promising recent work (Gangloff *et al.*, 2019; Jackson *et al.*, 2021) suggests that the dense nuclear spin environment (more than 10^4 spinful nuclei) could potentially be cooled and controlled enough to play this role.

Other candidates for deterministic RGS generation are optically active point defects in wide bandgap materials, such as the nitrogen-vacancy or silicon-vacancy centers in diamond and the silicon-carbon divacancy or silicon vacancy in silicon carbide. These systems have longer coherence times than quantum dots and feature a small number of nuclear spins (natural abundance $\sim 1\%$ in C and $\sim 4\%$ in Si), which can be isolated and controlled well and are thus already being explored as memory registers for quantum repeater nodes (Bourassa *et al.*, 2020; Nguyen *et al.*, 2019a; Taminiou *et al.*, 2012). On the

other hand, defects are not as efficient and bright as QDs, and they tend to emit into unwanted modes a large fraction of the time. Atomic systems, such as trapped ions and atoms in optical lattices or cavities, have long coherence times and can be controlled with high fidelity. While their photon emission is not as fast, their other attractive properties could possibly compensate for the lower rates (Thomas *et al.*, 2022). Interestingly, hybrid strategies combining deterministic generation based on quantum emitters and linear-optical fusion are particularly appealing when quantum emitters cannot interact with each others (Herrera-Martí *et al.*, 2010; Hilaire *et al.*, 2022). In that setting, we can use quantum emitters to generate one dimensional clusters and GHZ states deterministically and fuse them probabilistically using linear-optical boosted fusion gates to generate graph states of arbitrarily complex topologies.

c. GKP-encoded graph states. While entangling gates for GKP encodings are deterministic and readily accessible experimentally, state preparation is a bigger challenge. There are several existing proposals to this end, with a recent focus on modified Gaussian Boson Sampling (GBS) devices, which use Gaussian optics combined with photon-number-resolving (PNR) detection (Quezada *et al.*, 2019; Sabapathy *et al.*, 2019; Su *et al.*, 2019; Tzitrin *et al.*, 2020). Once the GKP states are produced, they may be stitched together deterministically with passive and static optical resources, namely beamsplitters, phase shifters, and delay lines (Tzitrin *et al.*, 2021).

d. Performance and overheads. The overheads of the various optical repeater protocols are highly sensitive to the chosen state generation scheme. In this section we review the resource requirements and performances of the repeaters discussed in this section.

In the original all-photonic repeater protocol (Azuma *et al.*, 2015a), the total number of photons consumed to produce an entangled pair between Alice and Bob scales polynomially with the total distance. The average rate to produce an entangled pair with a single-repeater system is on the order of the repetition rate of the slowest device among single-photon sources, photon detectors, and active-feedforward techniques. The resource costs for the repeaters in (Ewert *et al.*, 2016) and (Ewert and van Loock, 2017) scale linearly or less-than-quadratically per the number of photons per encoded qubit.

Hilaire *et al.* (Hilaire *et al.*, 2021a) analyze the performance of repeaters based on the deterministic RGS generation of (Buterakos *et al.*, 2017) by calculating a bound on the secret key rate per matter qubit and comparing it to direct transmission and to “memory-based” (i.e., first- and second-generation) repeaters. To compare to the latter, the figure of merit is defined as the rate of

a Bell state generation between the end nodes (Alice and Bob) divided by the number of matter qubits per node. In the case of memory-based repeaters, there is an upper bound on this quantity that originates from the need for classical heralding between nodes and which is given by $c/(4L)$. This bound is used throughout Ref. (Hilaire *et al.*, 2021a) for memory-based repeaters; further reductions in the rate, originating from swap gates between the emitter and memory qubits, are ignored.

The deterministic RGS generation based on matter qubits in (Buterakos *et al.*, 2017) relies on entangling CZ gates between emitter and ancilla qubits, which enable us to create complicated photonic graph states. For realistic systems, the longest timescale in the deterministic RGS generation is the duration of these gates, T_{CZ} , compared to which the photon generation and single-qubit gate times are negligible. It is therefore T_{CZ} that sets the bound for the secret key rate for repeaters based on deterministic RGS generation. In Ref. (Hilaire *et al.*, 2021a), the authors fix the tree encoding depth to 2 for the inner RGS photons and optimize over the RGS size (number of arms), the branching vector b_0, b_1 of the tree encoding, and the number of nodes to maximize the key rate for a total distance of 10^3 km. For these distances, it is found that for $T_{CZ} \leq 60$ ns the RGS approach always outperforms memory-based repeaters. In this case, the distance between adjacent nodes is approximately 3.5 km. These are most likely conservative estimates, since memory-based repeaters also require entangling gates between matter qubits, which will further lower their rates. More research into quantifying the performance of deterministic RGS protocols is needed. For example, Hilaire *et al.* kept the tree encoding depth fixed throughout their treatment ($d = 2$). While deeper trees offer higher protection against photon loss, contributing to an increase of the rate, they also require a larger number of emitter-ancilla CZ gates, thus decreasing the rate. An analysis of optimal encoding depths is an open problem with deterministic RGS generation.

Sometimes, one is not limited by the number of photons, but rather by the number of optical modes available for communicating between neighboring repeater stations (i.e., by the optical channel bandwidth, as in classical communication). Then, it is important to choose good mode-efficient encoding schemes. In the low-loss regime, we may use continuous variable codes to encode multiple qubits per bosonic mode; for example, the GKP encoding can almost approach the quantum channel capacity of the one-way pure loss channel (Noh *et al.*, 2020). In addition, other CV codes, like cat codes, can also boost the secure communication rate per mode when compared to DV encodings (Li *et al.*, 2017). Moreover, for CV-DV concatenated encoding, we may further reduce the resource overhead by optimizing the distribution of two different types of repeaters associated with CV and DV error correction, respectively (Rozpędek *et al.*, 2021).

IV. MILESTONES: OUTPERFORMING POINT-TO-POINT OPTICAL COMMUNICATION

Point-to-point communication schemes allow for quantum communication over intracity distances even with the use of a standard optical fiber and they are ready for practical use (see, e.g., (Lo *et al.*, 2014; Xu *et al.*, 2020)). However, those schemes have a fundamental limitation on their achievable distances [which are about 400 km in practice, i.e., in the case of the use of a standard optical fiber (Boaron *et al.*, 2018) (see Sec. III.A.3)]. This limitation is now explicitly given as the form of upper bounds (Pirandola *et al.*, 2017; Takeoka *et al.*, 2014a) on the two-way private capacity of a lossy bosonic channel, which are proportional to the transmittance η of the channel for small η . The two-way private capacity represents how many private bits can be obtained per use of a given channel, in an asymptotically faithful manner, with the free use of LOCC. In the case of the lossy bosonic channel of Eq. (13), this quantity is given by the PLOB bound (Pirandola *et al.*, 2017), $-\log_2(1 - \eta)$ (see Sec. VI).

On the other hand, as one can see from Sec. III, a quantum repeater scheme has no fundamental limitation on their achievable distances. Indeed, it enables us to perform quantum communication efficiently even over intercontinental distances, but its realization is still challenging. Therefore, there is a technological gap between quantum repeater schemes for intercontinental distances and point-to-point communication schemes for intracity distances.

To bridge the gap, intermediate quantum communication schemes, especially for the application to QKD, for intercity distances have been proposed (Abruzzo *et al.*, 2014; Azuma *et al.*, 2015b; Lucamarini *et al.*, 2018; Luong *et al.*, 2016; Panayi *et al.*, 2014; Rozpędek *et al.*, 2019; Xie *et al.*, 2022; Zeng *et al.*, 2022). In particular, the schemes use only a single node C which is located at the center between a sender, Alice, and a receiver, Bob, and is connected to them with optical fibers. The goal of the schemes is basically to double the achievable distances of point-to-point QKD schemes, by making the secret key rate proportional to $\sqrt{\eta}$, outperforming the two-way private/quantum capacities proportional to η (for small η), where η is the transmittance of a pure-loss channel between Alice and Bob (see also Ref. (Curty *et al.*, 2021) which contextualizes this approach from the viewpoint of security for QKD). This expected secret key rate has the same scaling of the private capacity of single-repeater communication schemes with the use of pure-loss channels (Azuma and Kato, 2017; Azuma *et al.*, 2016; Pirandola, 2019; Rigovacca *et al.*, 2018) (see Sec. VI for detail). The schemes are divided into three categories: one is based on two-photon interference with dual-rail encoded qubits (Secs. IV.A and IV.D) at the central node C , another is based on single-photon interference with single-

rail encoded qubits (Sec. IV.B), while the third one is a time-reversed version of these (Sec. IV.C) to work without optical Bell measurements. In this section, we review these schemes, whose realizations are regarded as good and natural milestones towards quantum repeaters.

A. Adaptive measurement-device-independent QKD

To double the communication distance by utilizing a central node C between communicators, an adaptive measurement-device-independent (MDI) QKD scheme has been proposed with matter quantum memories (Abruzzo *et al.*, 2014; Panayi *et al.*, 2014) or with all-optical quantum non-demolition (QND) measurements (Azuma *et al.*, 2015b), based on a dual-rail encoding. Although these schemes have originally been proposed to perform QKD, its use as an entanglement generation protocol (or, a coherent version) can be summarized as follows (Figs. 10 and 12): (i) Each of Alice and Bob sends m optical polarization qubits (by using $2m$ bosonic modes), each of which is maximally entangled with a local qubit, to the central node C . (ii) On receiving the pulses, the node C essentially performs QND measurements to the pulses to confirm the arrival of single photons over lossy channels. (iii) Then, qubits of single photons that have successfully arrived from Alice are paired with ones from Bob at the node C . (iv) The node C then performs a linear-optical Bell measurement of Fig. 3 (a) relying on two-photon interference on each of these pairs. (v) Node C then announces the pairings and the measurement outcomes of the Bell measurements. (vi) Finally, Alice and Bob keep their local qubits which are supposed to be entangled with each other from the announcement of step (v). The essence of this protocol is to perform the Bell measurement *only* on pairs of pulses which still have single photons even after the travel over the lossy optical channels.

If the protocol is used for QKD like the original proposals (Abruzzo *et al.*, 2014; Azuma *et al.*, 2015b; Panayi *et al.*, 2014), Alice and Bob perform at random Z -basis or X -basis measurement on each of their local qubits just after step (i), and their measurement outcomes are regarded as their choice of random bits in QKD. Then, the step (i) is replaced by the random preparation of BB84 signals $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ (Bennett and Brassard, 1984). This would also imply that Alice and Bob could use phase-randomized weak coherent states emitted by lasers, instead of single-photon sources, by using the decoy-state method (Hwang, 2003; Lo *et al.*, 2005; Wang, 2005). The security simply follows from that for the original MDI QKD (Curty *et al.*, 2014; Lo *et al.*, 2012), because it relies only on the trust for Alice and Bob.

The communication efficiency of the above protocol scales with $\sqrt{\eta}$, rather than η , where η is the transmittance of a direct lossy bosonic channel between Alice and

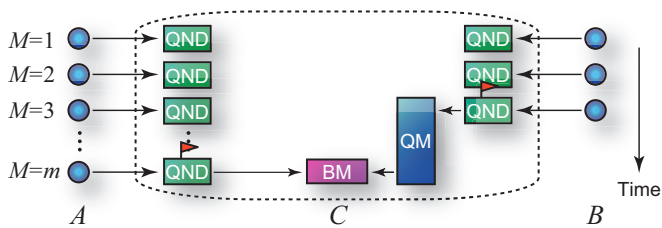


FIG. 10 The concept of memory-assisted MDI QKD. In this protocol, once the node C confirms the arrival of an optical polarization qubit either from Alice’s side or from Bob’s side with QND measurement [which is described by a (red) flag on a box labeled “QND” in the figure], it keeps it in a quantum memory (QM) until an optical polarization qubit arrives at the node C from the other side, followed by its release to be subjected to Bell measurement (BM).

Bob. This can be understood as follows. First notice that the success probability of the QND measurement in step (ii) is proportional to $\sqrt{\eta}$, because the polarization qubit emitted by Alice (or Bob) just travels over a lossy bosonic channel connecting between the central node C and Alice (between the central node C and Bob), rather than between Alice and Bob. This means that if the number m of multiplexing, defined in step (i), is on the order of $(\sqrt{\eta})^{-1}$, the probability with which the QND measurement in step (ii) finds the arrival of non-zero single photons from Alice and from Bob is pretty high. Then, the node C can have nonzero pairs in step (iii), to which the Bell measurements are applied in step (iv). Thus, as long as the inherent success probabilities of the QND measurement and the Bell measurement are constant (or, precisely, independent of the transmittance $\sqrt{\eta}$ of the channels), Alice and Bob would have an entangled pair with a finite probability, through steps (v) and (vi). Therefore, $m \sim (\sqrt{\eta})^{-1}$ is enough to present an entangled pair to Alice and Bob, implying that the communication efficiency, that is, the secret key rate per pulse¹⁰, of the protocol scales with $\sqrt{\eta}$.

1. Memory-assisted implementation

The memory-assisted MDI QKD protocol (Abruzzo *et al.*, 2014; Panayi *et al.*, 2014) corresponds to an implementation of the above protocol (in Sec. IV.A) by utilizing the functionality of matter quantum memories (Fig. 10). In particular, the protocol assumes that the

central node C uses matter quantum memories to achieve steps (ii)-(iv), and m optical polarization qubits in step (i) are sent by Alice and Bob in a time-multiplexing manner. If we can use a matter quantum memory that heralds the successful storing of a received optical polarization qubit, this heralding signal is regarded as the signal of the success of the QND measurement in step (ii). To achieve step (iii), the node C just uses one memory for Alice and one memory for Bob. Each of these memories receives optical pulses from Alice or from Bob until it successfully stores a single photon. Once this storage succeeds, each memory keeps the qubit information until the other memory heralds the successful storage. If both memories herald the successful storage of a single photon, they load the stored photons to perform the linear-optics-based Bell measurement of Fig. 3 (a) on them as step (iv). The secret key rate of this protocol is exemplified in Fig. 11, which shows $\sqrt{\eta}$ -scaling when the required memory time in the protocol is shorter than the coherence time of quantum memories.

Although we have assumed that the matter quantum memories have a function of heralding the storage, this method works even with a matter quantum memory which can just compose a Bell state with an optical polarization qubit. In particular, in this case, as step (ii), the node C just needs to perform the linear-optical Bell measurement of Fig. 3 (a) on this polarization qubit emitted by a quantum memory and a received pulse from Alice (or Bob). Since this Bell measurement provides the signal of the success only when it receives two (or more) photons, the signal of the success of this Bell measurement implies that the qubit information held by the pulse from Alice (or Bob) is successfully teleported into the other half of the Bell state, i.e., into the matter quantum memory. That is, this is essentially the success of the QND measurement required in step (ii). Hence, a matter quantum memory which can compose a Bell state with an optical polarization qubit allows the node C to implement the QND measurement in an indirect manner, which is also enough to implement the memory-assisted MDI QKD protocol.

This memory-assisted implementation uses time multiplexing by utilizing matter quantum memories. The dominant noise of matter quantum memories is dephasing and/or amplitude damping (which is sometimes treated as a depolarizing channel to simplify theoretical treatment), any of which increases exponentially with time. Therefore, the noise would significantly limit the allowed number m of time multiplexing in the memory-assisted MDI QKD protocols.

In fact, the secret key rate of a memory-assisted MDI QKD protocol using matter quantum memories with dephasing is limited by the allowed number m of multiplexing, that is, by T_2/T in Fig. 11 which corresponds to how many attempts, each of which needs time T , are possible for the matter quantum memory to successfully

¹⁰ Notice that an optical pulse here is regarded as being composed of two bosonic modes, i.e., a mode for horizontally polarized photons and a mode for vertically polarized photons. Hence, for this optical pulse, the PLOB (upper) bound on achievable secret key rates of point-to-point QKD between Alice and Bob per pulse (composed of the two bosonic modes) is $-2 \log_2(1 - \eta)$, which is approximated to $2\eta / \ln 2 \approx 2.89\eta$ for very small η .

store a single photon within its coherence time T_2 . In the graph, as η decreases, the secret key rate scales linearly with $\sqrt{\eta}$ as long as $T_2/T \geq (\sqrt{\eta})^{-1}$, but it then converges to η . This implies that the required coherence time T_2 is on the order of $(\sqrt{\eta})^{-1}T = e^{L/(2L_{\text{att}})}T$ with $\eta = e^{-L/L_{\text{att}}}$ ($L_{\text{att}} = 22$ km), and thus, it scales exponentially with $L/2$. However, as long as the period T of Alice's and Bob's pulse generation can be taken to be small, the required coherence time could be smaller (Panayi *et al.*, 2014) than even the minimum coherence time L/c required by multiplexed first generation quantum repeaters (Razavi *et al.*, 2008).

2. All-optical implementation

The all-photon adaptive MDI QKD protocol could be understood as an all-optical implementation of the above protocol in Sec. IV.A (Azuma *et al.*, 2015b) (Fig. 12). In the protocol, the QND measurement in step (ii) is assumed to be performed by using a quantum teleportation, similar to the memory-assisted MDI QKD protocol,

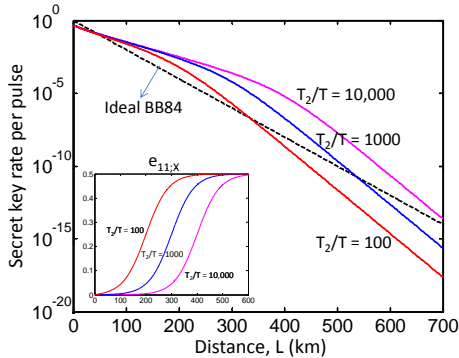


FIG. 11 Secret key rate (per pulse) of an adaptive MDI QKD protocol based on matter quantum memories with heralding storage and on Alice's and Bob's use of ideal single-photon sources. The secret key rate of the ideal BB84, which scales linearly with $\eta = e^{-L/L_{\text{att}}}$ ($L_{\text{att}} = 22$ km), is also shown as a reference. T_2 is the dephasing time for the matter quantum memories, $1/T$ is the pulse generation rate of Alice and Bob, and $e_{11;x}$ is the phase error rate for Alice's and Bob's raw key. T_2/T corresponds to how many attempts, each of which needs time T , are possible for the matter quantum memory to successfully store a single photon within its coherence time T_2 , that is, the allowed number m of time multiplexing in the protocol. The secret key rate scales linearly with $\sqrt{\eta}$ as long as $T_2/T \geq (\sqrt{\eta})^{-1}$, but it then converges to η as η decreases. This is because the increase of phase error $e_{11;x}$ for the case of $T_2/T \leq (\sqrt{\eta})^{-1}$ nullifies the benefit of time multiplexing from the use of matter quantum memories, as shown in the panel. Figure adapted from (Panayi *et al.*, 2014).

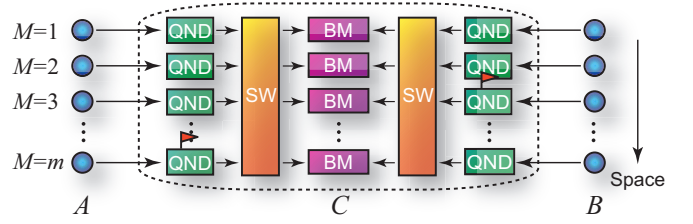


FIG. 12 The concept of all-photon adaptive MDI QKD. In this protocol, the node C first performs QND measurements to confirm the successful arrival of single photons [which is described by a red flag on a box labeled “QND” in the figure], followed by optical switches (SW) to send the surviving photons to Bell measurement (BM) modules. Figure adapted from (Azuma *et al.*, 2015b).

but it is implemented by using only optical devices¹¹. In particular, to achieve the QND measurement in step (ii), the node C first prepares optical polarization qubits in a Bell state locally, and applies the linear-optical Bell measurement of Fig. 3 (a) on the half of this Bell pair and the optical pulse sent by Alice or Bob. The success of this Bell measurement teleports the qubit information of the surviving single photon into the other half of the Bell pair, corresponding to the success of the QND measurement. Since this protocol does not assume to use matter quantum memories, m optical polarization qubits in step (i) of this protocol are assumed to be sent by Alice and Bob simultaneously in a spatial-multiplexing manner. Thus, the above all-optical QND measurements in step (ii) are performed at the same time on all the pulses sent by Alice and Bob, and then the pairing in step (iii) is made by using an optical switch. The performance of this protocol is exemplified in Fig. 13, which shows $\sqrt{\eta}$ -scaling of the secret key rate.

This all-optical implementation uses spatial multiplexing by utilizing optical switches. The dominant noise of optical switches is the photon loss. However, in contrast to memory-assisted implementation, this loss increases only logarithmically with the number m of spatial multiplexing (Azuma *et al.*, 2015b). Note that the all-optical protocol can achieve the $\sqrt{\eta}$ -scaling even if it uses only an $m \times 1$ optical switch and a Bell measurement module at the middle node C . Thus, if we implement an $m \times 1$ optical switch by concatenating 2×1 optical switches with transmittance η_{sw} in a knockout tournament manner with depth $\lceil \log_2 m \rceil$, the transmittance of the $m \times 1$ optical switch decreases as $\eta_{\text{sw}}^{\lceil \log_2 m \rceil}$, and it thus scales only logarithmically with the number m . This is a merit to use the spatial multiplexing, rather than time multi-

¹¹ An idea similar to this, called a qubit amplifier, is also used in the context of the device-independent QKD in order to close the detection loophole problem (Curty and Moroder, 2011; Gisin *et al.*, 2010).

plexing. Such combination of an $m \times 1$ optical switch and a Bell measurement module is also implementable without using such a large-scale optical switch, that is, by using only single-mode on/off switches, a passive Hadamard linear optical circuit and single-photon detectors (Azuma *et al.*, 2015b). The performance in this case is also described in Fig. 13.

3. Challenges

The question of whether a two-mode squeezed state, which can be produced with practical systems, can directly be used as the Bell state to implement the teleportation-based QND measurement in step (ii) has been answered to be negative, so far. For instance, if we use atomic-ensemble quantum memories for the memory-assisted MDI QKD protocol, the memory can naturally

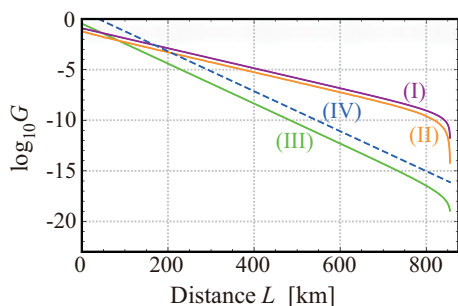


FIG. 13 Secret key rate (per pulse) G of an all-photon adaptive MDI QKD protocol. η is rephrased by the distance L between Alice and Bob, with $\eta = e^{-L/L_{\text{att}}}$ ($L_{\text{att}} = 22$ km), and $c = 2.0 \times 10^8$ m/s. Lines (I)–(IV) represent the performance of the protocol with active optical switches, that of the protocol with a passive Hadamard linear optical circuit, that of the original MDI QKD protocol (Lo *et al.*, 2012), and the TGW bound (Takeoka *et al.*, 2014a), respectively. This graph is described under the following assumptions (Azuma *et al.*, 2015b): a single active feedforward can be completed within time τ_a , during which photons run in optical fibers, being subject to the corresponding photon loss; heralded single-photon sources emit pulses with duration τ_s , with efficiency η_s , and they are multiplexed (Bonneau *et al.*, 2015; Christ and Silberhorn, 2012; Collins *et al.*, 2013; Ma *et al.*, 2011; Migdall *et al.*, 2002) to produce high-fidelity telecom single photons with the repetition rate of the slowest optical device at the expense of the use of (at least) one active feedforward; single-photon detectors have quantum efficiency η_d and dark count rate ν_d ; Bell pairs for the all-photon QND measurements can be generated in constant time τ_a with single-photon sources rather than a Bell-pair photon source, by paralleling a probabilistic procedure (Browne and Rudolph, 2005) with the active feedforward technique. In particular, they are assumed to be $\eta_s = 0.90$ (Christensen *et al.*, 2013; Giustina *et al.*, 2013; Migdall *et al.*, 2002), $\tau_s = 100$ ps (Shibata *et al.*, 2014), $\eta_d = 0.93$ (Marsili *et al.*, 2013), $\nu_d = 1$ s $^{-1}$ (Marsili *et al.*, 2013; Shibata *et al.*, 2010), and $\tau_a = 67$ ns (Ma *et al.*, 2011). Figure from (Azuma *et al.*, 2015b).

compose a two-mode squeezed state with an optical pulse (Duan *et al.*, 2001; Sangouard *et al.*, 2011). However, this entanglement cannot directly be used as a resource to implement the teleportation-based QND measurement in step (ii) (Piparo *et al.*, 2014), because the multi-photon component of the two-mode squeezed state makes the success probability of the QND measurement depend on the transmittance $\sqrt{\eta}$ of the channels. This result is made stronger by assuming that the node C is allowed to use photon number-resolving detectors (Trényi *et al.*, 2019), rather than threshold detectors assumed in (Piparo *et al.*, 2014). In particular, the paper shows that the polarization entanglement produced by a spontaneous parametric down-conversion (SPDC) process cannot directly be used to implement the QND measurement in step (ii) of the all-photon adaptive MDI QKD protocol, by deriving necessary conditions on photon-number statistics of the entanglement photon sources.

As a result, a single matter qubit, such as a single ion, a quantum dot or a nitrogen-vacancy center in a diamond, inside a cavity is proposed as a candidate for the memory to realize the memory-assisted MDI QKD protocol (Piparo *et al.*, 2017a,b), while a source emitting an entangled photon pair with a low multi-photon component, such as one assumed in the original paper (Azuma *et al.*, 2015b) (see the caption of Fig. 13) or an entanglement photon source (Eisaman *et al.*, 2011), is needed to implement the all-photon adaptive MDI QKD protocol. In the case where multi-photon emission is highly suppressed, threshold detectors without having the function of photon-number resolving are sufficient for implementing the teleportation-based QND measurement.

As for the all-photon adaptive MDI QKD protocol, since it needs only QND measurements on the photon number, it could adopt different types of QND measurements, such as one in (Imoto *et al.*, 1985) based on an optical Kerr effect and one in (Brune *et al.*, 1990) based on a dispersive atom-field coupling (see textbooks (Scully and Zubairy, 1997; Walls and Milburn, 2007)). It is thus an important open question whether the all-photon adaptive MDI QKD keeps their merit on communication efficiency even if we replace the teleportation-based QND measurement with an alternative one. As for the memory-assisted MDI QKD, a proof-of-principle experiment of the key element has been performed with a single solid-state spin memory integrated in a nanophotonic diamond resonator (Bhaskar *et al.*, 2020), based on an encoding on the phase difference between sequential two pulses (like one used in a differential phase shift QKD (Inoue *et al.*, 2002)) (see also Sec. V.H.2).

B. Twin-field QKD

To double the communication distance by utilizing a central node C between communicators, another idea is

also focused on especially in the field of QKD, thanks to the proposal of a twin-field (TF) QKD protocol based on a single-rail encoding (Lucamarini *et al.*, 2018). The scaling improvement of the TF QKD protocol is essentially brought by the following point: like entanglement generation processes in quantum repeater protocols (Azuma *et al.*, 2012; Childress *et al.*, 2006b; Duan *et al.*, 2001), the protocol makes the node C use a simple linear-optical Bell measurement of Fig. 3 (b) based on single-photon interference, rather than two-photon interference used in the original MDI QKD (Lo *et al.*, 2012), and Alice and Bob encode their qubit information into a *single* optical mode (i.e., a single-rail encoding), rather than two modes (i.e., a dual-rail encoding, such as polarizations and time bins). This aims to utilize the feature that this Bell measurement—to project a given state into a Bell state $(|0\rangle|1\rangle \pm |1\rangle|0\rangle)/\sqrt{2}$ with the vacuum state $|0\rangle$ and the single-photon state $|1\rangle$ as shown in Fig. 3 (b)—succeeds if a single photon reaches node C either from Alice or from Bob. For instance, in the case of the DLCZ protocol (Duan *et al.*, 2001), states of each local memory of Alice and Bob are entangled with the number states (i.e., the Fock states) of a single optical mode, while in the case of hybrid quantum repeater protocols (Azuma *et al.*, 2012; Childress *et al.*, 2006b), the computational basis states of each of Alice and Bob’s local qubits are entangled with two coherent states of a single optical mode (corresponding to a cat-state encoding). As a result, the efficiency of this type of entanglement generation schemes (Azuma *et al.*, 2012; Childress *et al.*, 2006b; Duan *et al.*, 2001) scales with $\sqrt{\eta}$, rather than η , without requiring any challenging devices at the node C , thanks to the use of single-photon interference. This scaling improvement in the entanglement generation might be reasonable because it relies on the following technical challenges:

- (a) those entanglement generation schemes need intense phase stabilization regarding the channels between Alice and the node C and between Bob and the node C , in contrast to ones based on two-photon interference at the node C ;
- (b) those schemes require Alice and Bob to use matter quantum memories which could be used to prepare nontrivial optical states, such as number states (Duan *et al.*, 2001) and cat states (Azuma *et al.*, 2012; Childress *et al.*, 2006b).

A bold claim was given in the original proposal of the TF QKD protocol (Lucamarini *et al.*, 2018): it had argued that if we borrow the idea of the decoy-state method (Hwang, 2003; Lo *et al.*, 2005; Wang, 2005), coherent states are enough to achieve QKD with $\sqrt{\eta}$ scaling, without the necessity of any device which has a potential to prepare nontrivial optical states (in contrast to the entanglement generation schemes with requirement (b) above). The idea was stemmed (Lucamarini *et al.*, 2018) from

making a decoy-state phase-encoding BB84 protocol be in the form of an MDI QKD setup, namely, attaching the decoy-state method to a phase-encoding MDI QKD protocol (Tamaki *et al.*, 2012). However, despite the extremely appealing claim, a rigorous security proof against the most general type of eavesdropping strategies was missing in the original proposal (Lucamarini *et al.*, 2018): only security over restricted eavesdropping was proven. This triggered a lot of interest to develop variants of the TF QKD protocol, as well as their security proofs over arbitrary eavesdropping attacks in asymptotic scenarios (Cui *et al.*, 2019; Curty *et al.*, 2019; Lin and Lütkenhaus, 2018; Ma *et al.*, 2018; Tamaki *et al.*, 2018; Wang *et al.*, 2018) and in finite-size scenarios (Currás-Lorenzo *et al.*, 2021; Jiang *et al.*, 2019; Maeda *et al.*, 2019; Xu *et al.*, 2020; Yu *et al.*, 2019). Here we focus on a variant (Curty *et al.*, 2019) of the TF QKD protocol, as it is explicitly related with entanglement generation protocols in quantum repeaters, to see why coherent states are enough to achieve QKD.

Before introducing the variant protocol, let us introduce its coherent version, which is essentially equivalent to an entanglement generation protocol (Azuma *et al.*, 2012). The coherent version is described as follows. (i) Each of Alice and Bob prepares an optical pulse entangled with a local qubit, whose state is described as $(|0\rangle|\alpha\rangle + |1\rangle|-\alpha\rangle)/\sqrt{2}$, where $|0\rangle$ and $|1\rangle$ are orthogonal states of the local qubit and $|\pm\alpha\rangle$ are coherent states of the optical pulse with an amplitude $\alpha > 0$. (ii) Each of them sends the prepared optical pulse to the node C over a lossy bosonic channel (13) with the transmittance $\sqrt{\eta}$. (iii) On receiving the pulse a in coherent state $|\pm\sqrt[4]{\eta}\alpha\rangle_a$ from Alice and the pulse b in coherent state $|\pm\sqrt[4]{\eta}\alpha\rangle_b$ from Bob, the node C performs a linear-optical Bell measurement of Fig. 3 (b) relying on single-photon interference on them. (iv) The node C then announces the measurement outcome of the Bell measurement. (v) Finally, Alice and Bob keep their local qubits if they know that one of two detectors for the Bell measurement announces arrival of photons, through the announcement in step (iv).

Notice that the 50:50 beamsplitter of the Bell measurement in step (iii) (Fig. 3 (b)) converts received states $|\pm\sqrt[4]{\eta}\alpha\rangle_a|\pm\sqrt[4]{\eta}\alpha\rangle_b$ into coherent states $|\pm\sqrt{2}\sqrt[4]{\eta}\alpha\rangle_c|0\rangle_d$ and $|\pm\sqrt[4]{\eta}\alpha\rangle_a|\mp\sqrt[4]{\eta}\alpha\rangle_b$ into coherent states $|0\rangle_c|\pm\sqrt{2}\sqrt[4]{\eta}\alpha\rangle_d$, respectively, where c and d are the outputs having received constructive interference and destructive interference, respectively. Since the detection of photons in the number basis erases the phase information \pm of the coherent states $|\pm\sqrt{2}\sqrt[4]{\eta}\alpha\rangle$, the successful detection of photons defined in step (v) works as nondestructive parity measurement, i.e., projection measurement $|00\rangle\langle 00| + |11\rangle\langle 11|$ or $|01\rangle\langle 01| + |10\rangle\langle 10|$ on Alice and Bob’s local qubits (Azuma *et al.*, 2012), which entangles their local qubits in the protocol.

To see the scaling, suppose that the Bell measurement is performed by using ideal threshold detectors, for simplicity. Then, the success probability of the Bell measurement is $r = 1 - e^{-2\sqrt{\eta}\alpha^2}$, while the Bell pair obtained at step (iv) includes only the phase error with probability $e_Z = (1 - e^{-2\alpha^2(2-\sqrt{\eta})})/2$ (Azuma *et al.*, 2012). This performance as entanglement generation is shown to be optimal in various scenarios (Azuma *et al.*, 2022; Azuma and Kato, 2012; Azuma *et al.*, 2010, 2009). If we maximize an asymptotic key rate formula $G = r(1 - h(e_Z))$ with the binary entropy function h over α , we can easily confirm that G scales with $\sqrt{\eta}$. However, this merely means that the key rate G could scale $\sqrt{\eta}$ when Alice and Bob use matter quantum memories to realize their local qubits, as considered in Ref. (Azuma *et al.*, 2012).

To make the protocol composed of steps (i)-(iv) a prepare-and-measure scheme, Alice and Bob are supposed to perform Z -basis or X -basis measurement randomly on each of their local qubits just after step (i) and before step (ii). Here, the Z -basis measurement prepares the optical pulse in coherent state $|\alpha\rangle$ or $|\alpha\rangle$ at random, while the X -basis measurement prepares it in cat state $|C_+\rangle := (|\alpha\rangle + |-\alpha\rangle)/(2\sqrt{p_+})$ with probability p_+ or $|C_-\rangle := (|\alpha\rangle - |-\alpha\rangle)/(2\sqrt{p_-})$ with probability p_- , where $p_{\pm} = (1 \pm \langle -\alpha|\alpha\rangle)/2$. The preparation of coherent states $|\pm\alpha\rangle$ regarding the Z -basis measurement can be done easily. In contrast, the preparation of cat states $|C_{\pm}\rangle$ regarding the X -basis measurement is problematic, because it requires a challenging device in practice. However, this preparation is not necessary, if Alice and Bob will distill a key only from the outcomes of the Z -basis measurements. In particular, in the case of this QKD, the X -basis measurements are used only to

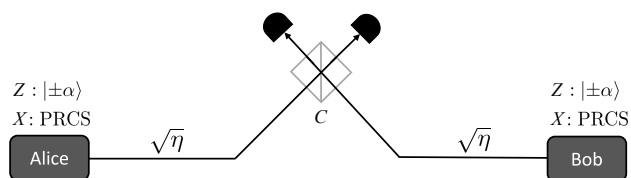


FIG. 14 Schematic of TF-type QKD protocol (Curty *et al.*, 2019). Each of Alice and Bob chooses Z basis or X basis, randomly. If Z basis is selected, Alice and Bob prepare coherent state $|\alpha\rangle$ or $|\alpha\rangle$ at random, and send it to the central node C . If X basis is selected, Alice and Bob prepare a phase-randomized coherent state (PRCS) whose intensity is chosen randomly from a predefined set (so as to be able to use the decoy-state method (Hwang, 2003; Lo *et al.*, 2005; Wang, 2005)), and send it to the central node C . On receiving pulses from Alice and Bob, the central node C performs the Bell measurement based on single-photon interference (Fig. 3 (b)). The secret key is distilled only from instances where both of Alice and Bob choose Z basis and the Bell measurement at the node C succeeds. Figure adapted from (Currás-Lorenzo *et al.*, 2021).

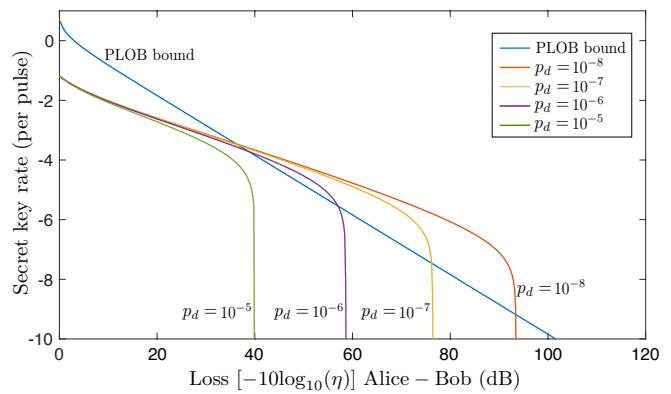


FIG. 15 Secret key rates (per pulse) of a TF-type QKD protocol for different dark count rates, p_d , in logarithmic scale as a function of the overall loss between Alice and Bob. The PLOB bound is the private capacity of a lossy bosonic channel (Pirandola *et al.*, 2017). This figure is described by assuming a misalignment of 2% in each channel Alice- C and Bob- C , and the inefficiency function for the error correction process $f = 1.16$. Figure adapted from (Curty *et al.*, 2019).

estimate the actual phase error rate e_Z for privacy amplification, and estimation of its upper bound by Alice and Bob through a protocol is enough to prove the security (Bennett *et al.*, 1992; Koashi, 2009; Lo and Chau, 1999; Mayers, 2001; Portmann and Renner, 2022; Renner, 2008; Shor and Preskill, 2000). In fact, it turns out that the estimation of an upper bound on the phase error e_Z can be done just by sending phase-randomized coherent states in the case of the choice of X basis and by invoking a decoy-state method, without preparing the cat states $|C_{\pm}\rangle$ (Curty *et al.*, 2019). As a result, the protocol is described as in Fig. 14, and the conjecture in the original proposal that the coherent states (and their phase-randomized ones) are enough to achieve QKD with $\sqrt{\eta}$ -scaling is concluded to be true, as shown by the performance in Fig. 15.

The TF QKD protocol and its secure variants omit technical challenge (b) as unnecessary for QKD, but they still include technical challenge (a). Nonetheless, various experiments (Chen *et al.*, 2021a, 2020; Clivati *et al.*, 2022; Minder *et al.*, 2019; Pittaluga *et al.*, 2021; Wang *et al.*, 2019b, 2022; Zhong *et al.*, 2019, 2022, 2021) to overcome this have already been performed, towards the full implementation of the TF-type QKD protocols in practical scenarios. These trials are important even for quantum repeaters, because they represent a good milestone towards the realization of a quantum repeater protocol based on single-photon interference, which involves the same technical challenge (a) (like Refs. (Azuma *et al.*, 2012; Childress *et al.*, 2006b; Duan *et al.*, 2001)).

In TF QKD, to achieve the phase stability required for single-photon detection based entanglement swapping, there are two general strategies. The first strategy is to use only one laser and employ auto-compensation with a

Sagnac loop where optical signals go through the same path either clockwise or counter-clockwise (Zhong *et al.*, 2019, 2022, 2021). The second strategy allows two independent lasers to be used, but may require a combination of techniques including, for example, frequency locking, using a reference pulse for compensation and ensuring that the optical path lengths of the two optical fibers do not differ too drastically (Chen *et al.*, 2021a, 2020; Clivati *et al.*, 2022; Li *et al.*, 2023; Minder *et al.*, 2019; Pittaluga *et al.*, 2021; Wang *et al.*, 2019b, 2022).

C. The single sequential quantum repeater

A third alternative is to invert the previous schemes and place a quantum device with a quantum memory in the central node and two detectors in the end nodes. This scheme was proposed by (Luong *et al.*, 2016).

In this scheme, the central node sends a photon entangled with a memory qubit to one of the end nodes until the end node confirms successful detection of the photon. Then, the central node repeats the same process with the other end node and thus emits a photon entangled with a memory qubit until success. Once the second end node confirms the successful detection of a photon, the central node performs a Bell measurement and heralds the measurement outcome to the two end nodes.

The advantage of this scheme is the simplicity of the setup, requiring a single node holding two memory qubits and no optical Bell measurement. On the other hand, this setup is not measurement-device independent and it requires qualitatively long coherence times when compared with memory-based adaptive MDI QKD. In particular, the coherence time should be large when compared with the sum of the travel time of a photon from the center node to an end node plus the corresponding heralding signal, multiplied by the average number of times required for a successful event.

The feasibility of this setup for outperforming the point-to-point limits was analyzed for different hardware parameters in (Luong *et al.*, 2016), (Rozpędek *et al.*, 2018) and (Rozpędek *et al.*, 2019). An experimental demonstration of the setup was recently reported in (Langefeld *et al.*, 2021) with Rubidium atoms in an optical cavity. While below the fundamental limit for direct transmission, the scaling of the key rate in the experiment was shown to be proportional to the square root of the transmittance of an optical fiber connecting two end parties.

D. Post-pairing measurement-device-independent QKD

Recently, Xie *et al.* and Zeng *et al.* have proposed a variant of MDI QKD protocol (Xie *et al.*, 2022; Zeng *et al.*, 2022) which may be conceptually intermediate be-

tween adaptive MDI QKD and TF QKD and whose secret key rate can scale with $\sqrt{\eta}$, rather than η , where η is the transmittance of a pure-loss channel between Alice and Bob. In this protocol (Fig. 16), the middle node C still uses linear-optical Bell measurement of Fig. 3 (b) based on single-photon interference like TF QKD, while Alice and Bob send N optical pulses in coherent states to the middle node sequentially, that is, in a time-multiplexing manner, like adaptive MDI QKD. The main aim here is to make a protocol rely on the application of a Bell measurement to project into Bell states $(|01\rangle_{a_i a_j} |10\rangle_{b_i b_j} \pm |10\rangle_{a_i a_j} |01\rangle_{b_i b_j})/\sqrt{2}$, based on *two-photon interference* between i th and j th time bins ($i, j = 1, 2, \dots, N$ and $i \neq j$) at the middle node C , where a_i and b_i are i th time bins sent by Alice and Bob, respectively. This is implemented by postselecting time slots i and j to which the Bell measurements based on single-photon interference at the node C are successfully applied, under the assumption that the phase correlation between such possibly long time separated i th and j th time bins is kept in the implementation. This keeping of the phase correlation is a technological challenging part if the number N of multiplexing is large. Nonetheless, since this protocol can be regarded as relying on two-photon interference at the middle node C , rather than single-photon interference, like adaptive MDI QKD, an intense phase stabilization regarding the channels between Alice and the node C and between Bob and the node C could be unnecessary in contrast to the TF QKD. In the protocol, Alice and Bob send Charlie optical pulses in coherent states whose phases are chosen randomly from $[0, 2\pi)$ and whose intensities are chosen randomly from a predefined set. This is designed so that time bins $a_i a_j$ and $b_i b_j$, postselected by the middle node C , can be regarded as a BB84 signal and a decoy state, that is, a signal used in the normal MDI QKD with time-bin encoding (Ma and Razavi, 2012). This postselection includes the matching between Alice's and Bob's random choices of phases in some cases (although, in contrast, it was shown to be unnecessary in the case of TF QKD (Cui *et al.*, 2019; Currás-Lorenzo *et al.*, 2021; Curty *et al.*, 2019; Lin and Lütkenhaus, 2018; Maeda *et al.*, 2019)).

For a large number N of the multiplexing, $n = \mathcal{O}(N\sqrt{\eta})$ Bell measurements based on *single-photon interference* would succeed, where $\sqrt{\eta}$ represents the transmittance of pure-loss channels between Alice and the middle node C and between the middle node C and Bob. Hence, there would be $\mathcal{O}(n/2) = \mathcal{O}(N\sqrt{\eta}/2)$ instances to which the target Bell measurements based on *two-photon interference* are successfully applied. Since the success of the target Bell measurement could produce an entangled state between Alice's virtual qubit and Bob's virtual qubit, the secret key rate of the protocol could scale with $\sqrt{\eta}$.

According to the proposals, called mode-pairing QKD (Zeng *et al.*, 2022) and asynchronous MDI-QKD (Xie

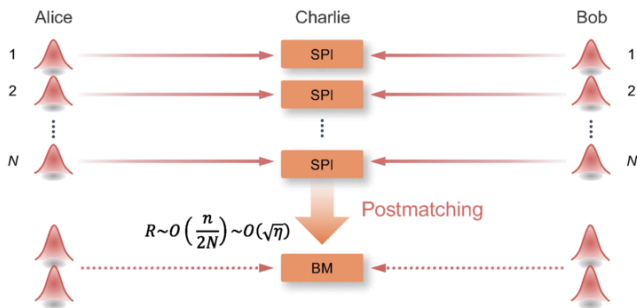


FIG. 16 Post-encoding measurement-device-independent QKD. In this protocol, Alice and Bob send N pulses to the middle node C , Charlie, to perform the linear-optical Bell measurement of Fig. 3 (b) based on single-photon interference (SPI), and a two-photon Bell state is obtained by postmatching two successful SPI events. Here n represents the number of successes of the Bell measurement based on SPI and $\sqrt{\eta}$ represents the transmittance of pure-loss channels between Alice and Charlie and between Charlie and Bob. Figure adapted from (Xie *et al.*, 2022).

et al., 2022), experimental demonstrations have been performed in Refs. (Zhu *et al.*, 2023) and (Zhou *et al.*, 2023), respectively.

V. EXPERIMENTAL PROGRESS TOWARDS REPEATERS

Long-distance quantum communication is enabled by low-loss media for photon transfer. Free-space communication (Ursin *et al.*, 2007) and satellite-based communication (Liao *et al.*, 2017; Yin *et al.*, 2017) have unique experimental challenges; in this section, we chiefly describe the practical advances towards optical-fiber-based quantum communication schemes featuring quantum repeaters. We organize our discussion roughly according to the requirements of each generation of repeaters from Sec. III.B and of memoryless repeaters from Sec. III.C.

Almost all quantum repeater architectures require the implementation of efficient interfaces between quantum memories and photons. In first-generation repeaters, a quantum memory must be capable of storing quantum information for a long time (Sec. V.A) and emitting photons that are entangled with the memory degrees of freedom (Sec. V.B). These photons are then coupled into optical fibers that connect distant repeater nodes. The intermediate entanglement between distant quantum memories (Sec. V.C) is finally used to create end-to-end entanglement links between Alice and Bob with a rate ideally much higher than direct transmission over fibers.

In first-generation repeaters, unavoidable memory errors are dealt with through entanglement distillation (Sec. V.D). In the second generation of quantum repeaters, memory errors are corrected through quantum error correction. Therefore, quantum registers of many quantum memories are required at each repeater node

to encode logical memory qubits (Sec. V.E). In the third generation of repeaters, loss errors are also dealt with through QEC. Since any QEC code can only tolerate a probability of erasure (a common model for loss) of 50% (see Sec. II.B and V.E), advanced engineering is required to obtain high transmissivities as well as collection, coupling, and detection efficiencies for the photons (Sec. V.F). In addition to the experimental progress aligning with the three generations, we review the headway that has been made towards memoryless repeaters (Sec. V.G), whose all-photonic implementations require the efficient generation of highly-entangled states of many photons. Finally, we overview the experimental demonstrations of trusted QKD networks and small quantum networks (Sec. V.H) that exist as important milestones on the way to a quantum internet.

A. Long-lived quantum memories

The success of most quantum repeater schemes critically relies on the performance of their quantum memories. The *coherence time*, T_2 , of the memory (sometimes called the *memory time*) is the relevant figure-of-merit: it characterizes the time during which quantum information can be stored in the memory before being degraded by the environment. For example, when generating entanglement between two quantum memories at nodes separated by a distance L_0 in a heralded manner (Sec. III.A.4.b.2), high entanglement fidelities can only be achieved if $L_0 \ll cT_2$, with c the speed of light in fiber. A quantum memory needs also to have characteristics beyond the coherence time, namely fast, efficient and high-fidelity initialization, gate application, and photon retrieval and read-out. For brevity, we restrict our discussion to the coherence time, and refer interested readers to Refs. (Heshami *et al.*, 2016; Lvovsky *et al.*, 2009; Simon *et al.*, 2010) for the other important features of quantum memories.

Several candidate quantum memories are under development, among them atomic ensembles ($T_2 = 0.2$ - 16 s (Dudin *et al.*, 2013; Yang *et al.*, 2016)) including Bose-Einstein condensates (Riedl *et al.*, 2012), and single natural or artificial atomic systems such as cold atoms, trapped ions ($T_2 = 4$ ms for $^{128}\text{Ba}^+$ (Inlek *et al.*, 2017)), colour centres in diamond ($T_2 = 1$ s (Abobeih *et al.*, 2018; Bar-Gill *et al.*, 2013)), and quantum dots ($T_2 = 3$ μs (Grelich *et al.*, 2007)). All of these platforms are also quantum emitters, making them suitable candidates for atom-photon interfaces; other systems may have superior coherence times but cannot emit photons. To benefit from these extremely long-lived memories, hybrid strategies can be chosen in which the quantum memory is indirectly interfaced with photons through its coupling to an efficient quantum emitter. This occurs naturally in NV centers, for example, where the electron

Quantum emitter		Quantum memory			Quantum register		Emitting properties						Refs.
		T_2	T_2^*	F (gate)	N	T_2	T_1	η_{eff}	ι	η_{DW}	F (atom-phot.)	λ_{QE} (nm)	
Atomic ensemble	^{87}Rb	16 s									$\geq 93.3\%$	780	a
Single atoms / trapped ions	^{87}Rb	2.6 ms	400 μs	$\geq 97.5\%$			300 ns	60%			89%	780	b
	$^{171}\text{Yb}^+$	> 1 h										369	c
	$^{128}\text{Ba}^+$	4 ms			≥ 4 ($^{171}\text{Yb}^+$)	> 1 h					$\geq 86\%$	493	d
Quantum dot		3 μs	39 ns	95%	1	1 μs	0.6-0.8 ns	57%	99.5%	90%	$\geq 80\%$	900-1565	e
Defects (diamond)	NV	0.6 s	5-36 μs	> 99%	9	75 s	13 ns	37%	98.6%	4%	96%	637	f
	SiV	10 ms	115 ns		1	100 ms	1.6 ns	85%	72%	75%	94%	737	g
	GeV						5.5 ns	0.72%		60%		602	h
	SnV		540 ns				4.5 ns			57%		620	i
Defects (in SiC)	V_{Si}	0.8-20 ms					37 ns		69%	6 – 9%		862-917	j
	$\text{V}_{\text{Si}}\text{V}_{\text{C}}$	64 ms	375 μs	99.98%	≥ 1		91 ns			7%		1078-1132	
	V^{4+}						45 ns			50%		1278-1388	
	NV		1 μs				13ns					1180-1468	
Defects (in Si)	G						34 ns			15%		1269	k
	T						802 ns			23%		1326	l
Rare-earth ions	Eu^{3+}	8.1 ms			≥ 1	6 h	0.8-1.2 ms					579	m
	Er^{3+}				≥ 1	1.2 s	1.5-8.7 ms					1532	n
	Pr^{3+}	880 μs			≥ 1		140 μs					606	o
	Nd^{3+}				≥ 1						80%*	883	p

^a (Dudin *et al.*, 2013; Hosseini *et al.*, 2011; Park *et al.*, 2019; Xu *et al.*, 2013)

^b (Daiss *et al.*, 2021; Ebert *et al.*, 2015; Langenfeld *et al.*, 2020; van Leent *et al.*, 2020; Levine *et al.*, 2019)

^c (Wang *et al.*, 2021)

^d (Inlek *et al.*, 2017)

^e (Bechtold *et al.*, 2015; De Greve *et al.*, 2011; Éthier-Majcher *et al.*, 2017; Gangloff *et al.*, 2019; Jackson *et al.*, 2021; Matthiesen *et al.*, 2013; Olbrich *et al.*, 2017; Somaschi *et al.*, 2016; Tomm *et al.*, 2021)

^f (Aharonovich *et al.*, 2011; Arroyo-Camejo *et al.*, 2014; Bar-Gill *et al.*, 2013; Bauch *et al.*, 2018; Bradley *et al.*, 2019; Hensen *et al.*, 2015; Pompili *et al.*, 2021; Ruf *et al.*, 2021)

^g (Becker *et al.*, 2018; Bhaskar *et al.*, 2020; Neu *et al.*, 2011a,b; Nguyen *et al.*, 2019a; Pingault *et al.*, 2017; Ruf *et al.*, 2021; Sipahigil *et al.*, 2014; Sukachev *et al.*, 2017)

^h (Iwasaki *et al.*, 2015; Palyanov *et al.*, 2015; Ruf *et al.*, 2021; Wan *et al.*, 2020)

ⁱ (Görlitz *et al.*, 2020; Ruf *et al.*, 2021; Trusheim *et al.*, 2020)

^j (Lukin *et al.*, 2020) and references therein

^k (Durand *et al.*, 2021)

^l (Bergeron *et al.*, 2020; Kurkjian *et al.*, 2021)

^m (Zhong *et al.*, 2015a; Zhong and Goldner, 2019)

ⁿ (Rančić *et al.*, 2018; Zhong and Goldner, 2019)

^o (Lago-Rivera *et al.*, 2021; Zhong and Goldner, 2019)

^p (Liu *et al.*, 2021; Zhong *et al.*, 2015b)

TABLE VI Properties of selected memory qubits for quantum repeater applications. Results for most systems were generally obtained in separate experiments. We distinguish the properties of the qubit emitters with those of the potential N -qubit registers they are coupled to. Also included are the properties of the systems as single-photon emitters, including the emission time T_1 , the end-to-end collection efficiency η_{eff} , the photon indistinguishability ι , the Debye-Waller factor η_{DW} , the fidelity F of the atom-photon entanglement, and the emission wavelength λ_{QE} . * Heralded entanglement generation fidelity between two quantum memories.

spin is coupled via hyperfine interaction with nearby ^{13}C nuclear spins ($T_2 = 75$ s) (Bradley *et al.*, 2019). The same strategy is also taken with trapped ions, where ionic species with good emission properties, such as $^{128}\text{Ba}^+$, are interfaced at the same quantum node with $^{171}\text{Yb}^+$, the latter of which have much longer coherence times ($T_2 > 1$ h (Wang *et al.*, 2021, 2017)). Using these ions, (Hucul *et al.*, 2015) showed two-ion entanglement which persists over more than 1 s. Recent results also show that a typically short-lived quantum dot spin can be efficiently coupled to a single magnon excitation of its nuclear environment, which consists of $10^4 - 10^5$ nuclear spins that behave as a long-lived memory ($T_2^* \approx \mu\text{s}$ (Gangloff *et al.*, 2019; Jackson *et al.*, 2021), compared to the $T_2^* = 39$ ns for the electron spin (Éthier-Majcher *et al.*,

2017)). Rare-earth Eu^{3+} ions in Y_2SiO_5 crystals have the longest coherence time experimentally observed with $T_2 = 6$ h (Zhong *et al.*, 2015a). This platform has an optical memory which can store a time-bin encoded photonic qubit for 1 h (Ma *et al.*, 2021).

Another important criterion for these platforms is the temperature at which they operate. It implies potentially the use of different cooling strategies that can be technologically demanding, from dilution refrigerator or liquid helium temperature cryostats to laser cooling. Interestingly, several studies propose to soften this requirement through the use of “room temperature” quantum repeaters based on either hybrid optomechanical systems with NV centers (Ji *et al.*, 2022) or warm atomic vapors (Borregaard *et al.*, 2016; Dideriksen *et al.*, 2021;

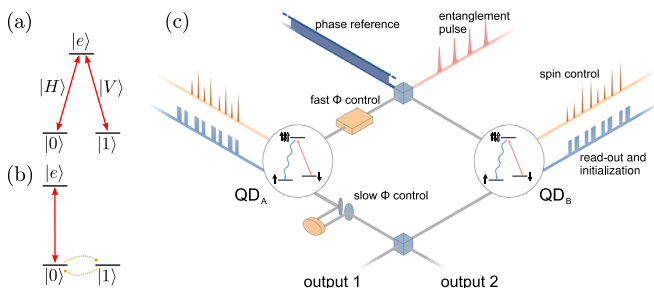


FIG. 17 Level structure and heralded entanglement generation. In (a), a Lambda level structure with states $|e\rangle$ (excited), $|0\rangle$ (connected to $|e\rangle$ by horizontally polarized light, $|H\rangle$) and $|1\rangle$ (connected to $|e\rangle$ by vertically polarized light, $|V\rangle$). In (b), a level structure for time-bin entanglement. $|e\rangle$ only connected to $|0\rangle$; control of the qubit states is required. In (c), a setup for spin-spin heralded entanglement generation. Figure from Ref. (Stockill *et al.*, 2017).

Katz and Firstenberg, 2018; Li *et al.*, 2021b; Pang *et al.*, 2020; Shaham *et al.*, 2021).

In Table VI, we summarize the experimental performance of long-lived quantum memories together with their emission properties. In addition to the coherence time, several other figures of merit are also important for quantum repeater applications. These include the quantum emitter control gate fidelity (F) and dephasing and relaxation times (T_2^* , T_1), and the availability of an additional quantum register and its properties. The photonic properties of the quantum emitters are also important, namely the photon collection efficiency (η_{eff}), the Debye-Waller factor in the case of solid-state defect qubits (i.e., probability of emitting photon into the zero-phonon line) η_{DW} , the indistinguishability ι and the quality of the spin-photon entanglement (F (atom-phot.)). The photon wavelength also plays a crucial role in quantum communication since the best transmission rates are achieved for telecom wavelengths. We include well-established quantum emitters alongside more recent but promising systems, such as rare-earth ions and new defects in diamond and silicon.

B. Emission of photons entangled with the quantum memory

Quantum memories should have—or should be coupled to quantum emitters which have—optical transitions that allow the emission of photons entangled with the memory qubits. The emitted photonic qubits are to be encoded in one of the degrees of freedom discussed in Sec. II.E. The emission of spin-entangled qubits encoded into photonic frequency, polarization, emission time bin, and spatial modes has already been experimentally demonstrated with the help of trapped ions, NV centers, and quantum dots. Many schemes exist for the production of photons entangled with the memory’s degrees of freedom, varying in details depending on the photonic encoding and

the energy level structure of the emitter. For concreteness, we will review two of the most common examples of such schemes.

Polarization-entangled photons can be produced in a system with a Λ -shaped level structure (that is, a Λ system), where the qubit ground states $|0\rangle$ and $|1\rangle$ are both optically coupled to a single excited state $|e\rangle$ by orthogonally-polarized transitions (say, horizontally-polarized and vertically-polarized photons, respectively). This type of level structure is present in most quantum emitters, including some species of trapped ions (Blinov *et al.*, 2004) and atoms (Volz *et al.*, 2006), in atomic ensembles (Chen *et al.*, 2007), NV centers (Togan *et al.*, 2010), and in quantum dots when a transverse magnetic field is applied (De Greve *et al.*, 2012; Gao *et al.*, 2012; Schaibley *et al.*, 2013). A quantum memory prepared in the excited state will spontaneously emit a single photon with either horizontal or vertical polarization ($|H\rangle$ or $|V\rangle$), as shown in Fig. 17 (a). After this emission, the total memory–photon system is in the entangled state $|0, H\rangle + |1, V\rangle$. For this scheme to successfully produce such a maximally entangled state, the coupling strength of the two optical transitions ought to be the same. If the transitions differ in energy ($E_H \neq E_V$), as in quantum dots, the final state might instead be $|0, (H, E_H)\rangle + |1, (V, E_V)\rangle$, where $|A, E_A\rangle$ for $A = H, V$ denotes the redundant encoding of the photonic qubit on its polarization and frequency degrees of freedom. The demonstration of bipartite entanglement is therefore challenging in this case, since it requires that this redundancy be erased, but such a quantum erasure of the photon frequency has been for example demonstrated in (Yu *et al.*, 2015).

Despite its relative simplicity, the previous scheme may not be available for all quantum memories, as it requires a Lambda-level structure. There is an alternative approach (Hensen *et al.*, 2015; Lee *et al.*, 2019a; Tchegotareva *et al.*, 2019; Vasconcelos *et al.*, 2020), which requires only one strong optical transition, that results in a photon whose emission time bin is entangled with the memory qubit. The minimal level structure required for this scheme is illustrated in Fig. 17 (b); it corresponds to a three-level system ($|0\rangle$, $|1\rangle$, $|e\rangle$), where only one state of the qubit states, e.g., $|0\rangle$, is optically coupled to the excited state $|e\rangle$. The memory is initialized in a superposition state $|0\rangle + |1\rangle$, and then the optical transition $0 \leftrightarrow e$ is excited by a π -pulse such that the system ends up in $|e\rangle + |1\rangle$. If in the excited state, the memory emits a photon in the early time bin $|t_1\rangle$; otherwise, it emits no photons, resulting in the state $|\text{vac}\rangle$: $|0, t_1\rangle + |1, \text{vac}\rangle$. The memory qubit is then flipped in its qubit subspace (yielding $|1, t_1\rangle + |0, \text{vac}\rangle$) and the $0 \leftrightarrow e$ transition is excited again, leading to the emission of a photon in the time bin t_0 if the excited state was populated: $|1, t_1\rangle + |0, t_0\rangle$. We see that a single photon is always emitted, and that its emission time bin is indeed

entangled with the quantum memory. This strategy requires the preparation of the memory in a superposition state and more control pulses; however, it has the advantage of operating with only a single optical transition, making it particularly convenient in the case of, e.g., NV centers (Bernien *et al.*, 2013), when one specific optical transition has better properties than the others. This approach has also been demonstrated in quantum dots, when a certain transition is made more favorable through cavity (Purcell) enhancement (Lee *et al.*, 2018).

C. Distant entanglement generation

It is possible to generate heralded entanglement between distant qubits mediated by the detection of photons. The implementation of these schemes is usually based on interference of photons within a linear-optical setup. To optimally interfere and hence create maximal entanglement, the photons emitted by two distant quantum memories should be perfectly indistinguishable (Aharonovich *et al.*, 2016; Senellart *et al.*, 2017).

The scheme of Cabrillo *et al.* (Cabrillo *et al.*, 1999) based on single-photon interference (see also (Bose *et al.*, 1999) for a similar proposal) for distant entanglement generation has been demonstrated with trapped ions (Slodička *et al.*, 2013), quantum dots (Delteil *et al.*, 2015; Stockill *et al.*, 2017), NV centers in diamond (Humphreys *et al.*, 2018) and atomic ensembles (Chou *et al.*, 2007). The experiment in (Stockill *et al.*, 2017), based on two quantum dot spins separated by a few meters, resulted in a postselected entanglement generation rate of 7.3 kHz (Stockill *et al.*, 2017).

Let us illustrate how the scheme works experimentally. Two quantum dots, A and B , situated at two separated nodes are prepared in a Voigt configuration (in-plane magnetic field) to exhibit a Λ -level structure with similar optical transition energies. The two quantum dots are prepared initially in the state $|0_A, 0_B\rangle = |\downarrow_A, \downarrow_B\rangle$ and are excited by the same weak phase-stabilized laser so that a photon may be produced by each quantum dot through Raman scattering with a probability $p \ll 1$ (see Fig. 17 (c)). The photonic modes are then mixed on a 50:50 beamsplitter at a central node to erase the which-path information—that is, to make it impossible to tell which quantum dot emitted the photon (essentially to perform the Bell measurement of Fig. 3 (b)). The state before the photon detection is:

$$\begin{aligned}
 |\Psi\rangle = & (1-p) |\downarrow_A, \downarrow_B\rangle |0_1, 0_2\rangle \\
 & + \sqrt{p(1-p)/2} (e^{i\Phi_A} |\uparrow_A, \downarrow_B\rangle + e^{i\Phi_B} |\downarrow_A, \uparrow_B\rangle) |1_1, 0_2\rangle \\
 & + \sqrt{p(1-p)/2} (e^{i\Phi_A} |\uparrow_A, \downarrow_B\rangle - e^{i\Phi_B} |\downarrow_A, \uparrow_B\rangle) |0_1, 1_2\rangle \\
 & + p/\sqrt{2} e^{i(\Phi_A + \Phi_B)} |\uparrow_A, \uparrow_B\rangle (|0_1, 2_2\rangle - |2_1, 0_2\rangle),
 \end{aligned} \tag{38}$$

where $|i_1, j_2\rangle$ (with i, j integers) corresponds to the num-

ber of photons in the first and second output modes of the beamsplitter, and Φ_A and Φ_B are the optical phases along the different optical paths corresponding to qubit A and B . If a single photon is detected, the quantum dot system is projected with probability $\approx p$ into the maximally entangled state $e^{i\Phi_A} |\uparrow_A, \downarrow_B\rangle \pm e^{i\Phi_B} |\downarrow_A, \uparrow_B\rangle$, with the sign depending on the output mode of the beamsplitter in which the photon was detected. In practice, p cannot be as high as desired because the quantum dot spins undergo two spin flip processes with probability p^2 , resulting in the emission of two photons. In that case, if only one of the two photons is detected—either due to imperfect collection and detection efficiencies or transmission losses—the heralding single-photon process leads to a state with fidelity that decreases with higher p . Refs. (Lago-Rivera *et al.*, 2021; Pompili *et al.*, 2021; Stockill *et al.*, 2017; Yu *et al.*, 2020) used this methods to demonstrate heralded entanglement generation. Ref. (Stockill *et al.*, 2017) demonstrated the highest rate for distant spin-spin entanglement with postselection and Ref. (Yu *et al.*, 2020) demonstrated the longest fiber distance between two remotely entangled quantum memories using atomic ensembles. However, while the two memories were separated by 50 kilometers of fiber, this was achieved using a spooled fiber of that length, the actual distance between the systems was a meter.

Other methods for generating distant heralded entanglement exist, namely the *Barrett and Kok* scheme (Barrett *et al.*, 2005) based on two-photon detection. This scheme has been demonstrated with NV centers (Bernien *et al.*, 2013) and trapped ions (Moehring *et al.*, 2007). The longest-distance entanglement between separated systems reached using this approach, 1.3 km, was achieved also with NV centers, in a loophole-free Bell test experiment (Hensen *et al.*, 2015). In Ref. (Yu *et al.*, 2020), the authors have also demonstrated a field-deployed heralded entanglement generation between two atomic ensembles separated by 11 kilometer (22 km of fibers) using two-photon interference. The latter was achieved by increasing the collection and detection efficiencies of the photons as well as converting the optical photons to the telecommunication frequency, which enjoys the highest transmissivity in optical fibers (see Sec. V.F for more details).

Cabrillo *et al.*'s scheme is required to operate in the low photon emission probability regime to obtain high fidelity heralded entanglement. In comparison, Barrett and Kok's scheme can operate in the high fidelity regime even with high emission probability. Therefore, it should be better suited for efficient quantum emitters and short distance between the nodes. However, for longer distances, the fiber losses becomes dominant and having a single-photon heralding like the Cabrillo *et al.* protocol leads to a better scaling with distance compared to the two-photon heralding of the Barrett and Kok scheme [similar to the relation between the TF QKD and the

original MDI QKD (see Sec. IV.B)].

D. Entanglement distillation

During the generation of entanglement between remote nodes, operation errors or the decoherence of quantum memories can lead to a reduced fidelity of Bell states shared between distant nodes. For first-generation quantum repeaters, the fidelity of Bell pairs can be increased through entanglement distillation (Sec. III.B.1). Starting with two imperfect copies of a Bell pair, it is possible to produce a single Bell pair with improved fidelity with a success probability of at best 50%. Entanglement distillation has been demonstrated with photonic Bell pairs (Pan *et al.*, 2003, 2001; Yamamoto *et al.*, 2001, 2003), atoms (Reichle *et al.*, 2006), and NV centers (Kalb *et al.*, 2017).

Photonic realizations differ in success rate because it is impossible to perform a deterministic CNOT gate with linear optics. Instead, the entanglement distillation protocols are performed using solely linear optics with a success rate limited to 25% at best (Pan *et al.*, 2001; Yamamoto *et al.*, 2001). Ref. (Reichle *et al.*, 2006) demonstrated the first experimental entanglement distillation with quantum memories. They distilled two Bell pairs of $^9\text{Be}^+$ ions, confined in the same Paul trap, with an overall success probability above 35%. Yet, because the pairs of entangled atoms were not spatially separated, this scheme is not particularly useful to enable long-distance quantum communication applications. Using two NV centers with two ^{13}C nuclear spins, Kalb *et al.* demonstrated entanglement distillation of a $65 \pm 3\%$ -fidelity Bell state in NV centers that were spatially separated by 2 meters. The highest reported heralded entanglement rate was 182Hz (Stephenson *et al.*, 2020) with trapped ions separated by 2 meters using a two-photon interference scheme. In this work, the authors expect a distilled Bell pair fidelity of 99% is within experimental reach.

E. Multi-qubit quantum registers and error correction

Multiple memory qubits will be required per repeater node, either for increasing the communication rate via multiplexing (Collins *et al.*, 2007), or for enabling error correction in repeaters beyond the first generation. A quantum register extends the architecture from Sec. V.A to a quantum emitter with good optical properties coupled to a large number of long-lived quantum memory qubits. This arrangement naturally occurs in colour centres in diamond, where the defect is coupled by hyperfine interaction to tens of ^{13}C nuclear spins (Bradley *et al.*, 2019), forming the register of qubits. There have been several advances in this line of research, e.g., in experi-

ments where the nuclear spins are individually controlled using the electron spin (Balasubramanian *et al.*, 2009; Bradley *et al.*, 2019; Childress *et al.*, 2006a; Fuchs *et al.*, 2011; Gurudev Dutt *et al.*, 2006; Taminiou *et al.*, 2012). Similarly, in the trapped ion setting, a quantum register of many qubits has been realized using one quantum emitter coupled to many memory qubits in the same optical trap. For example, dual species quantum nodes based on pairs of different ionic species such as $^{128}\text{Ba}^+ - ^{171}\text{Yb}^+$ (Inlek *et al.*, 2017) or $^{25}\text{Mg}^+ - ^9\text{Be}^+$ (Tan *et al.*, 2015) are being investigated. In a quantum dot, however, the spin is only coupled to one (potentially two) different magnon species (Jackson *et al.*, 2021), imposing limits on the size of the register. An alternative strategy for obtaining more qubits at each repeater node could be to vertically stack quantum dots (Stinaff *et al.*, 2006).

For repeaters from the second and third generation, a quantum register at each node can be seen as a quantum processor used to logically encode the quantum information transferred between nodes and to correct errors. A QEC code has recently been implemented in trapped ions (Egan *et al.*, 2020). Here, 9 physical $^{171}\text{Yb}^+$ qubits (with 4 additional qubits for stabilizer measurements) are associated with one logical qubit of the Bacon-Shor code in a fault-tolerant design. A recent experiment using superconducting qubits (Google, 2023) demonstrated experimentally a logical error rate reduction through increasing the size of the QEC code being used. There is also an effort to pursue error-corrected repeater nodes with solid-state spins (Cramer *et al.*, 2016; Waldherr *et al.*, 2014). In particular, with defects in diamond (Abobeih *et al.*, 2022), it has recently been shown the experimental fault-tolerant operation of a logical qubit using the 5-qubit code together with a flag protocol (Chamberland and Beverland, 2018; Chao and Reichardt, 2018) requiring a total of seven qubits. Yet, this proof-of-principle demonstration remains still above the break-even point for which logical qubit operations have higher fidelities than physical qubit operations.

Importantly, the logical qubits in error-corrected repeaters must be interfaced optically. For several platforms investigated for the realization of multi-qubit processors, such as superconducting circuits, a major challenge for quantum communication applications revolves around the emission of optical photons, which requires quantum transduction from microwave to optical energies (Ang *et al.*, 2022; Lauk *et al.*, 2020; Mirhosseini *et al.*, 2020).

The realization of logical photonic qubits is also being pursued; they are required in the third generation of repeaters and in all-photonic quantum repeaters in order to correct for loss errors. Error detection has been demonstrated on a photonic platform (Bell *et al.*, 2014), and recently a proof-of-concept photonic 9-qubit Shor code has been experimentally implemented together with an all-photonic quantum repeater proposal (Zhang *et al.*,

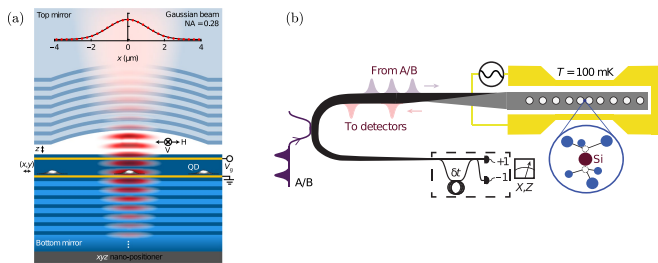


FIG. 18 State-of-the-art cavity-QED devices. In (a), a quantum dot coupled deterministically to an open Fabry-Pérot cavity. In (b), a silicon vacancy center in a photonic crystal cavity evanescently coupled to a fiber. Figure (a) from Ref. (Tomm *et al.*, 2021) and figure (b) from Ref. (Bhaskar *et al.*, 2020).

2022a).

F. Loss mitigation, quantum frequency conversion, and photonic source efficiency

A stringent requirement on correcting photonic errors is imposed by the no-cloning theorem (Sec. II.B), which implies that it is impossible to correct physical qubit losses of more than 50% with QEC. In light of this, reducing the photon losses throughout a quantum network is critical for the implementation of those repeaters where the loss is handled via QEC. Loss occurs at every optical component, with the main sources being propagation and coupling losses due to the intrinsic properties of fibers and photonic chips. Loss also occurs at the detectors and during the collection of photons produced by quantum emitters.

Losses in fibers are chiefly caused by infrared absorption and Rayleigh scattering, as well as imperfections introduced in manufacturing. Minimal loss is obtained at the telecom wavelength (1550 nm), where the loss coefficient is 0.2 dB per km, with few prospects of improvement. Even though there exist ultra-low-loss fibers with losses of 0.16 dB per km (Boaron *et al.*, 2018), they are not widely available, and would require complete modification of the existing infrastructure. It is therefore crucial to use quantum emitters that emit at the telecom wavelength, such as some engineered quantum dots (Benyoucef *et al.*, 2013) or rare-earth ions (Zhong *et al.*, 2019) and color centers in silicon (Bergeron *et al.*, 2020; Redjem *et al.*, 2020).

An alternative strategy consists of using a quantum frequency converter. The objective is to change the frequency of the photonic qubits while preserving the quantum information they encode (and the single-photon statistics if required for the scheme) (Ikuta *et al.*, 2011; McGuinness *et al.*, 2010; Tanzilli *et al.*, 2005). Frequency converters are generally based on a non-linear $\chi^{(2)}$ crystal (or possibly $\chi^{(3)}$) pumped by a laser pulse with frequency

ω_l chosen such that the frequency ω_i of an input photon is modified into $\omega_f = \omega_i - \omega_l$. This strategy has been used to convert the frequency to a telecom wavelength of photons emitted by NV centers (Tchebotareva *et al.*, 2019), quantum dots (De Greve *et al.*, 2012; Zaske *et al.*, 2012), single atoms (van Leent *et al.*, 2022, 2020), ions (Bock *et al.*, 2018; Krutyanskiy *et al.*, 2019, 2022), rare-earth-doped crystals (Maring *et al.*, 2017), and atomic ensembles (Dudin *et al.*, 2010; Ikuta *et al.*, 2018; Yu *et al.*, 2020).

The efficient collection of light produced by quantum emitters is another important technological challenge. Since spontaneous emission is non-directional, photon collection efficiencies tend to be quite low. To obtain a high efficiency source of single photons, the electromagnetic environment of the quantum emitter ought to be engineered to force its emission into one specific mode that can then be coupled into a fiber. This can be achieved using waveguides, which inhibit the emission outside of the waveguide mode (Arcari *et al.*, 2014), or with micro-cavities, which enhance the coupling between the quantum emitter and the electromagnetic mode confined in the cavity. In these two cases, the emission of a single photon is much more probable inside a particular mode (of the cavity or the waveguide) than in all the others. This photonic mode can then be efficiently coupled to the transmission fiber. Cavity enhancement also has the important advantage of increasing the probability of emission of indistinguishable coherent photons (Riedel *et al.*, 2017) as compared to incoherent phonon-assisted emission. Two examples of state-of-the-art cavity-QED devices are reviewed in Fig. 18. The single-photon collection efficiency has drastically improved over the years for all quantum emitters, through technological and material improvement of cavity-QED devices (Barros *et al.*, 2009; Bhaskar *et al.*, 2020; Maiwald *et al.*, 2012; Somaschi *et al.*, 2016; Tomm *et al.*, 2021; Uppu *et al.*, 2020; Wang *et al.*, 2019a); in quantum dots, trapped ions and defects in diamond, it has now risen above the 50% threshold.

While not making use of quantum emitters, it is also worth mentioning that spontaneous parametric downconversion sources have seen their effective collection efficiency increase to 67% through large-scale multiplexing and active switching (Kaneda and Kwiat, 2019). While it is not possible to use these sources to realize an efficient light-matter interface in quantum repeater protocol based on matter qubits, they nevertheless show great potential for all-photonic approaches, as detailed in the following section.

The single-photon detection efficiency (Hadfield, 2009) has also been significantly increased through the development of superconducting nanowire single-photon detectors (SNSPDs). Devices with detection efficiencies as high as 95% are now commercially available and superconducting nanowire detectors with efficiencies as high as 99 % have been demonstrated at telecom frequen-

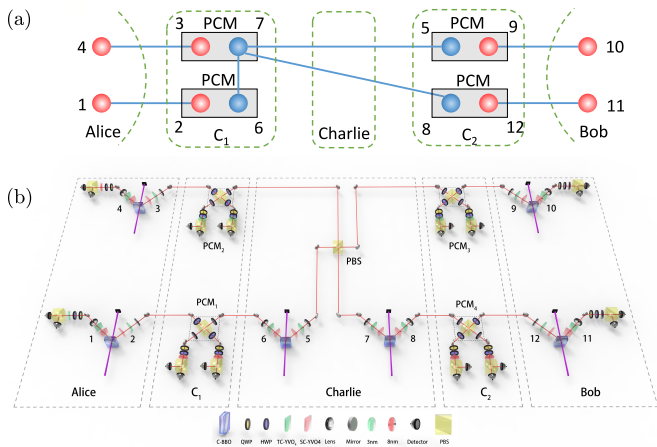


FIG. 19 A proof-of-principle experiment for an all-photonic quantum repeater. PCM stands for “passive choice measurement,” which automatically performs an entangling Bell measurement (in case of a coincidence detection) or a disentangling local X measurement (in case of a single-photon detection). Figures from (Li *et al.*, 2019).

cies (Chang *et al.*, 2021; Hu *et al.*, 2020a). Transition edge sensors also enjoy high detection efficiencies, with the bonus that they can resolve photon numbers (Lita *et al.*, 2008), which can be useful for some heralded entanglement schemes.

G. Progress towards memoryless quantum repeaters

In all-photonic quantum repeaters, error-correction and loss-tolerance are achieved through photonic codes, so that these protocols do not require quantum memories. The technological requirements of such repeaters are therefore considerably different from the other approaches. The primary challenge revolves around the creation of large, highly entangled photonic states, namely graph states.

Several different approaches have been suggested for photonic graph state generation. Until very recently, the largest entangled states of photons have been produced experimentally using spontaneous parametric downconversion sources and fusion gates (Browne and Rudolph, 2005). The probabilistic nature of the fusion gates is the main limitation to the number of photons in the graph state that can be produced with this approach, the current maximum being 12 (Zhong *et al.*, 2018).

Proof-of-principle experiments of all-photonic quantum repeaters have already been realized (Hasegawa *et al.*, 2019; Li *et al.*, 2019). In both cases, the original protocol in (Azuma *et al.*, 2015a) was replaced by a variant in order to facilitate its experimental realization. In this new all-photonic communication scheme, introduced in Ref. (Hasegawa *et al.*, 2019), Alice and Bob prepare n photonic Bell pairs each, sending one half of every one of

them through a lossy fiber to a central node (Charlie). Prior to the arrival of the photons, Charlie prepares a $2n$ -qubit GHZ state (equivalent to the complete graph state from Sec. III.C.1) and performs photonic Bell state measurements between the incoming photons and the corresponding photons in the GHZ state. The first key concept behind this scheme is a time-reversed adaptive Bell measurement, which Li *et al.* refer to as a passive choice measurement. If the photon a_i ($i = 1, 2, \dots, n$) emerging from Alice arrives at Charlie’s node, and the joint measurement with photon c_i from Charlie’s GHZ state is successful, then Charlie achieves a Bell state projection. However, if the photon a_i does not make it to Charlie’s node, or if the measurement is unsuccessful, the Bell state analyzer passively adapts to an X -basis measurement on c_i , which disconnects photon c_i from the GHZ state. This leads to the second important idea in (Hasegawa *et al.*, 2019): the outer qubits from the original repeater graph state in (Azuma *et al.*, 2015a) can be removed, leaving a bare GHZ state in its place.

In their work, Li *et al.* demonstrated the above scheme with a four-qubit GHZ state and $n = 2$ multiplexed communication channels. We illustrate the experiment in Fig. 19. Alice, Bob, and Charlie each prepare two Bell pairs using spontaneous parametric down-conversion sources. Alice and Bob send one qubit from each Bell pair—each corresponding to a communication channel—to Charlie’s node. Charlie mixes his two Bell pairs to produce a four-qubit GHZ state and the protocol proceeds as explained previously with $n = 2$. Although the experiment did not surpass the PLOB bound (Pirandola *et al.*, 2017), Li *et al.* demonstrated an enhancement in communication rates between Alice and Bob compared to the case where Charlie uses a Bell pair for each communication channel (that is, does not multiplex the channels). These results attested to the interest and experimental feasibility of all-photonic solutions for quantum communication.

In principle, the above modifications simplify the original all-photonic repeater, making it attainable with current technology. However, the protocol only works if a single QR node is used, consequently leading to a $\eta^{1/2}$ scaling, at best, and limiting the communication distances to, at most, about 800 km in practice¹² (in the sense explained in the footnote in Sec. III.A.3). Going beyond this limit would require cascading multiple QR nodes and using photonic states with much more photons, such as the RGS in original protocol

¹² For instance, with a twin-field-type QKD protocol which utilizes a single node between communicators, Wang *et al.* have successfully generated a secret key with 4.572×10^{-1} secret bits per second over 786.67 km of fiber and with 1.399×10^{-2} secret bits per second over 833.80 km of fiber (Wang *et al.*, 2022), experimentally.

(Sec. III.C.1). Furthermore, the protocol is particularly sensitive to local losses at Charlie’s node, as demonstrated in Ref. (Hasegawa *et al.*, 2019). Delaying the preparation of the GHZ state only goes part of the way to mitigate this issue, with a more complete scheme requiring loss-tolerant error correction. Recently, Ref. (Zhang *et al.*, 2022a) demonstrated a 9-qubit Shor code, with a new all-photonic quantum repeater approach which could be cascaded. They have also shown its tolerance to single-photon losses. Among the remaining steps to be fully operable, this Shor code should be generated in a heralded fashion rather than being postselected.

To move to higher photon numbers, the all-optical strategy requires probabilistic fusion gates combined with high-speed feedforward (Sec. III.C.3) to grow bigger and bigger graphs based on small graph resources. Having efficient feedforward techniques is thus crucial (Zanin *et al.*, 2021). This is achievable only with ultrafast optical switches and electronics.

The technological challenges of bosonic repeaters (Sec. III.C.2.c) are somewhat different than the discrete-variable repeater that we have focused on. For the particular case of encoding qubits into momentum-squeezed or GKP states, one can deterministically combine modes into large graph states with Gaussian operations (linear optics and squeezing). However, the production of photonic GKP states is challenging, and is not yet to be implemented on photonic platforms. On the other hand, Gaussian states of light are now a well-mastered technology (Asavanant *et al.*, 2019).

An alternative strategy for producing photonic graph states is to use light-matter interfaces in generation procedures such as (Buterakos *et al.*, 2017) or (Pichler *et al.*, 2017; Zhan *et al.*, 2023; Zhan and Sun, 2020), based on the initial work of Refs. (Economou *et al.*, 2010; Lindner and Rudolph, 2009; Schön *et al.*, 2005). This strategy is more demanding experimentally but has the advantage of being (in principle) deterministic. Indeed, with unity collection efficiency of the photons and perfect control of the quantum emitters, the generation procedure does become completely deterministic: the entanglement between photons is produced through the control of the quantum emitter rather than through probabilistic fusion gates. A proof-of-concept experiment has been realized by Schwartz *et al.* (Schwartz *et al.*, 2016) where a linear cluster state is produced by manipulating and optically pumping the spin of a quantum dot. The authors produced a three-qubit linear cluster state and showed that entanglement persists for up to five photons. More recently, this group showed that entanglement persists over 10 photons, with indistinguishability above 90 %, using also the deterministic generation from a hole spin quantum dot emitter (Cogan *et al.*, 2021). Quantum dot-based sources of entangled photons have also been inserted inside microcavities to generate linear-cluster states at much higher rates (Coste *et al.*, 2022). A similar

generation scheme using a single atom trapped in a cavity was used to demonstrate a 12-photon linear cluster state and a 14-photon GHZ state (Thomas *et al.*, 2022), which to date constitutes the record largest entangled photonic state demonstrated experimentally. In these experiments, the emitters produce polarization-entangled photons, but strategies involving time-bin entanglement have also been explored (Appel *et al.*, 2022; Lee *et al.*, 2018; Vasconcelos *et al.*, 2020; Vezvaei *et al.*, 2022).

To go beyond linear cluster state generation, one can either use multiple solid-state qubits or the strong non-linear interaction induced by atoms for light to effect entangling gates. For the generation procedures of Refs. (Pichler *et al.*, 2017; Zhan and Sun, 2020), one needs to implement spin-photon CZ gates, where a phase shift is induced onto a photon depending on the spin state. Cavity-QED devices increase the spin-photon interaction such that such spin-photon gates are within reach with many cavity-QED platforms (Androvitsaneas *et al.*, 2019; Arnold *et al.*, 2014; Bhaskar *et al.*, 2020; Javadi *et al.*, 2018; Reiserer *et al.*, 2014; Sun *et al.*, 2016; Wells *et al.*, 2019).

H. Experimental realization of quantum networks

In this section, we review experiments that go beyond two-node quantum communication to inch closer to the quantum internet. We first start by presenting the experimental realizations of trusted large-scale repeater networks for QKD applications based on trusted relays. We then discuss experimental progress towards the realization of quantum repeaters to actualize long-distance untrusted nodes. Finally, we discuss the experimental realization of untrusted quantum networks.

1. Trusted large-scale repeater networks

Several intercity QKD networks have already been realized, such as the SECOQC network (Peev *et al.*, 2009) in Austria, the Tokyo QKD network (Sasaki *et al.*, 2011) in Japan, the SwissQuantum network (Stucki *et al.*, 2011) in Switzerland, the Illinois Express Quantum network (Chung *et al.*, 2021) in the USA, and the Shanghai-Beijing QKD network (Chen *et al.*, 2021b) in China. In all of these networks, cryptographic keys are distributed between nodes separated by long distances using relay nodes. Assuming that the relay nodes are trusted, a secure key can be established at rates much higher than what is possible through direct fiber transmission (Pirandola *et al.*, 2017), thereby enabling efficient QKD over very long distances.

In Fig. 20 (a), we illustrate the Shanghai-Beijing QKD network, the largest QKD network to date. This network links four metropolitan areas—Shanghai, Hefei, Ji-

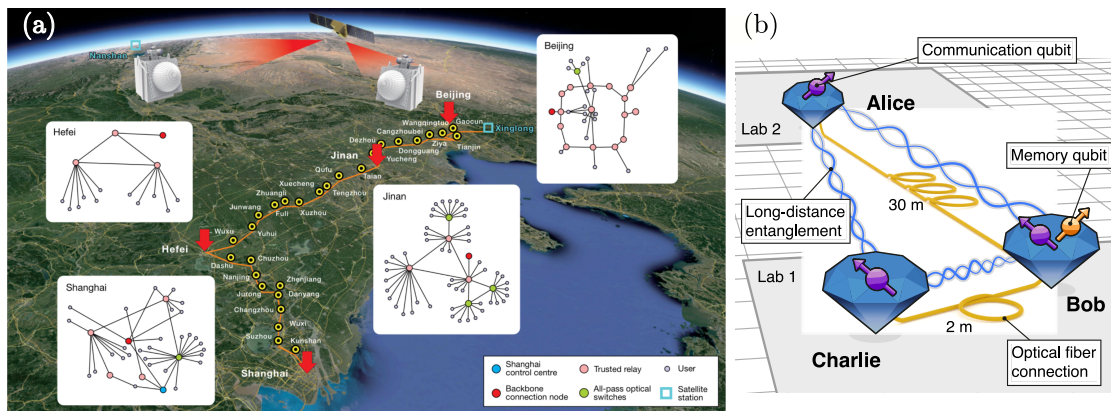


FIG. 20 Quantum networks. (a) Shanghai-Beijing QKD network. (b) Experimental quantum network composed of NV centers acting as quantum memories. Figure (a) from Ref. (Chen *et al.*, 2021b) and figure (b) from Ref. (Pompili *et al.*, 2021).

nan, and Beijing—using a backbone of 32 trusted relays in a linear topology. If any one of the 32 relay nodes is compromised, the generated key may be insecure. The trusted relays allow for efficient long-distance quantum communication between these metropolitan areas. Each of these cities is comprised of small QKD networks with different topologies, where end users with reduced capabilities (only requiring a QKD source) can connect to the network. This network incorporates both fiber- and satellite-based communication: the nodes at a Nanshan and Xinglong are separated by 2600 km, communicating through free-space via a satellite node that also acts as a trusted relay. A similar strategy has also been used to distribute a secret key over intercontinental distances—between Graz in Austria, and Nanshan and Xinglong in China, covering a total distance of 7600 km (Liao *et al.*, 2018). Thanks to this combination of fiber- and satellite-based quantum communication, the Shanghai-Beijing QKD network covers a total distance of 4600 km and provides a typical secret rate between each node of 50 kilobits per second (kbps) and a minimum inter-node secret key rate of 28 kbps in the entire network. Such large key rates achieved at such distances are completely out-of-reach for direct transmission over a fiber. Given its covered distance, complex topology, and the different quantum channels used, this QKD network can be considered as a genuine prototype of the quantum internet for QKD applications, albeit at the cost of having to trust the network provider.

2. Proof-of-concept of a quantum repeater

Improving on a trusted repeater network requires *device-independent* QKD, which can be realized through the distribution of Bell pairs to the end nodes. Recent experimental demonstrations of fibered device-independent QKD based on quantum memories (respectively single ^{87}Rb atoms (Zhang *et al.*, 2022b) and $^{88}\text{Sr}^+$

ions (Nadlinger *et al.*, 2022)) constitute significant improvements as they close the detection loophole in the violation of Bell’s inequality. In an experiment using an untrusted satellite node to share private keys with the help of the Ekert 91 protocol (Ekert, 1991), Yin *et al.* (Yin *et al.*, 2017) set the record distance of 1200 km for distribution of entangled photons. Realizing a long-distance device-independent multi-node network would also crucially require the practical implementation of efficient quantum repeaters in real networks. However, this major milestone is the subject of active research and remains to be demonstrated. Note, however, device-independent QKD still suffers¹³ from attacks such as memory attacks (Barrett *et al.*, 2013) and covert channels (Curty and Lo, 2019).

Bhaskar *et al.* (Bhaskar *et al.*, 2020) have demonstrated that the use of a single repeater node in an experiment increases the communication rate of *measurement-device-independent* (MDI)-QKD compared to repeaterless communication. Similar to Li *et al.* (Li *et al.*, 2019), they used a repeater scheme with a single repeater node; however, they were able to demonstrate an improvement over the PLOB bound in terms of a key rate in bits per channel use versus an effective channel transmission—a four-fold secret key rate increase over the original MDI QKD (Lo *et al.*, 2012). The repeater node consists of a single silicon-vacancy center embedded in a diamond photonic crystal cavity. The cavity mode of this device is efficiently evanescently coupled to a fiber to minimize the photonic

¹³ This is because once a key has been generated, it is classical, and as such is subject to copying. Therefore, if a QKD system is reused in future QKD sessions, then the key generated in a previous session might be stored in some memories and be leaked. Moreover, not only the QKD devices, but also the conventional computers used in the classical post-processing (e.g. error correction and privacy amplification) may leak key information via covert channels.

losses. A significant improvement toward the photon collection efficiency was also demonstrated, reaching 85%. The silicon-vacancy system is positioned in a dilution refrigerator to achieve a coherence time $T_2 = 0.2$ ms. In their experiment, the quantum memory at Charlie's node does not emit photons, but receives weak coherent time-bin-encoded pulses from Alice and Bob. Using electromagnetically-induced transparency of their cavity-QED device, these weak pulses are reflected or not depending on the electronic spin state. The reflected photonic pulses are then detected by superconducting single-photon detectors. If a photonic pulse coming from Bob is detected shortly after a pulse from Alice, a key bit can be distributed between Alice and Bob when Charlie communicates the two-photon and spin measurement results. With these experiments it is possible to achieve a $\sqrt{\eta}$ scaling because the two coherent pulses do not need to arrive simultaneously at the repeater node, thanks to the quantum memory (see Sec. IV for detail). The role of the memory is to store the information of the first pulse during the time it remains coherent while waiting for the second pulse to be detected. While operating with only one quantum memory per node for the moment, these results foresee a promising route toward long-distance quantum communication. Indeed, a silicon-vacancy color center can, in principle, make use of their ^{13}C neighbors to effect a quantum register of long-lived memories (Nguyen *et al.*, 2019b). This may increase the protocol's performance by enabling longer storage time as well as the concatenation of multiple repeater nodes, in principle paving the way to obtain a polynomial scaling of the rate with the communication distance.

In a more recent experiment, (Langenfeld *et al.*, 2021) demonstrated a memory-enhanced quantum repeater node based on two ^{87}Rb atoms in an atomic cavity. This node can in principle be cascaded can be at the core of a quantum repeater scheme that overcome the previous $\sqrt{\eta}$ limits of repeater nodes with a single memory such as (Bhaskar *et al.*, 2020). Moreover, the single-qubit error rate was below 11% ensuring that a secure key can indeed be transferred using this repeater node. Such a memory-enhanced repeater has also been demonstrated by performing entanglement swapping with two ^{87}Rb atomic ensemble memories (Pu *et al.*, 2021).

3. Untrusted quantum networks

Since a quantum internet for applications beyond QKD may look like a multi-node network where quantum information is stored and processed by quantum memories, a complementary route toward the development of long-distance multi-node networks is to create multi-qubit quantum networks at a small distance and to progressively increase their size when the quantum repeater technology becomes more mature. Pompili *et al.* (Pom-

pili *et al.*, 2021) is the first realization of such a small quantum network, where each node includes a quantum memory to process quantum information locally. This network is based on three nodes, with an inter-node distance of a maximum of seven meters (see Fig. 20 (b)). Each node includes one or two quantum memories based on a nitrogen-vacancy (NV) center electron spin, and potentially another proximal ^{13}C nuclear spin.

Pompili *et al.* used their network to perform non-trivial multi-node operations such as the generation of a 3-qubit GHZ state with a memory qubit at each node, and the generation of a Bell pair between quantum memories situated at nodes that were not directly connected. After the generation of heralded entanglement between an NV electron spin at Alice's node and the electron spin at Charlie's node, the information encoded in Charlie's electron spin qubit was swapped to a ^{13}C nuclear spin so that the electron spin could be used again to generate entanglement with Bob's NV center. This entanglement generation step could be realized with the strategies introduced in Sec. V.C. Then, the entanglement was swapped by performing a Bell measurement between the electron and the nuclear spins at Charlie's node. This was the first demonstration of entanglement swapping between distant nodes that were not originally connected. The work required the cooperation of a multitude of experimental components. In this work, they have used the single-photon detection scheme proposed by Cabrillo *et al.* to herald entanglement generation between distant spins with 80% fidelity and at rates of 7 and 9 Hz, using phase-stabilized links between the three nodes. The quantum information initially stored in Charlie's electron spin qubit needed to be swapped into one of its proximal nuclear spins, thereby requiring a nuclear spin register and a high level of control. In addition, since the entanglement ought to be stored for the time the three nodes were connected, dynamical decoupling sequences were used to further isolate the spins from their environment. Finally, an electron-nuclear spin Bell state was used to swap the entanglement at the central node and produce a Bell state between Alice's and Bob's spin qubits at a rate of 25 mHz. This protocol had an overall fidelity of 55%, which could potentially be improved by using better photonic interfaces, spin control, and read-out techniques, as well as reducing the infidelities and increasing the rate of the distant spin-spin entanglement generation. Such a network has also been used to teleport quantum information between two nodes that are not immediate neighbors (Hermans *et al.*, 2022).

The interest of these results is also to provide a testbed for real life applications and to prepare the other technological aspects of the implementation of a quantum network, such as the communication protocols. There is also a considerable development of quantum network simulator software (Coopmans *et al.*, 2021; Matsuo *et al.*, 2019; Wallnöfer *et al.*, 2022) to assist in this goal, for example,

to envision a city-scale network (Yehia *et al.*, 2022).

VI. QUANTUM INTERNET

The goal of this section is to look beyond linear networks, i.e., chains of quantum repeaters, and discuss how they blend into the vision of a future quantum internet. We first present a set of communication tasks that can be implemented over a quantum network and we link these sample communication tasks with experimental requirements and associate the tasks with a taxonomy of stages of the quantum internet which summarizes the discussion in (Wehner *et al.*, 2018). Second, we introduce the elements of a quantum networks and place repeaters in the larger context of a quantum network architecture. Finally, we investigate how to evaluate the usefulness of quantum networks for these different tasks. For this, we introduce a simplified model of a network in terms of a graph. The evaluation is phrased in the form of network capacities, quantities that can be achieved in an idealized situation. We observe that in spite of the apparent additional difficulty of dealing with a network, in this abstract setting many of the tools from point-to-point links carry to the network setting (see (Azuma *et al.*, 2021) for a review on tools for predicting quantum network performance).

A. Applications of the quantum internet

1. A set of representative communication tasks

Before we discuss how to quantify the usefulness of a quantum network, it is relevant to discuss the potential applications of quantum networks and more generally of the quantum internet. In the following we discuss a representative set of the applications that we know today divided by area. However, similar to the early days of the Internet, we should expect many new applications to be found as the number of users increases.

First of all, a quantum internet can be used for transmitting information. The nodes in the network might want to transmit classical information or quantum information. The latter is obviously not possible without a quantum network, but also for the former the quantum internet can offer an advantage with respect to a classical network. In particular, both entangled channel inputs (Hastings, 2009) and joint quantum measurements (Guha, 2011; Sasaki *et al.*, 1998) can enhance the transmission rate of classical communication. A quantum internet can also be used to transmit classical information between two parties that is secret to any third party (Devetak, 2005). In turn, this enables secret key distribution, a task that is possible with classical means only if the parties are willing to make assumptions on the communication channel, e.g., wireless physical layer security

relies on a model of the conditional probability distribution associated with the wireless channel (Bloch *et al.*, 2008), or on the capabilities of a potential eavesdropper, e.g., the security of the RSA cryptosystem (Rivest *et al.*, 1978) relies on the difficulty of the factoring problem.

Second, a quantum network can be used to implement several cryptographic tasks beyond private communication, with qualitative advantages with respect to classical networks. The best known one is QKD. Some other tasks are byzantine agreement (Ben-Or and Hassidim, 2005), certified deletion (Broadbent and Islam, 2020), conference key agreement (Augusiak and Horodecki, 2009; Chen and Lo, 2007; Murta *et al.*, 2020), distribution of money (Wiesner, 1983), leader election (Tani *et al.*, 2005), and secret sharing (Cleve *et al.*, 1999; Hillery *et al.*, 1999). Then there are some important cryptographic tasks which cannot be implemented neither with classical nor with quantum resources, such as information-theoretically secure quantum bit commitment and two-party secure computation (Lo, 1997; Lo and Chau, 1997, 1998; Mayers, 1997). But, if one is willing to make an assumption on the amount of storage (Damgård *et al.*, 2008) or on the quality (Konig *et al.*, 2012) of the storage of a potential attacker, then implementing these tasks with quantum resources is advantageous. In this category fall quantum protocols for bit commitment (Kent, 2011; Konig *et al.*, 2012), oblivious transfer (Schaffner, 2010; Wehner *et al.*, 2010) and secure identification (Damgård *et al.*, 2007; Dupuis *et al.*, 2014). Strikingly, quantum offers the possibility of implementing most of these cryptographic tasks without making any assumptions on the behavior of the devices held by the legitimate parties (Mayers and Yao, 1998). In consequence, these so-called device-independent implementations close by construction one of the most important sources of side channel attacks.

Third, as noted in the introduction (Sec. I), the study of quantum communication complexity tells us that by sending quantum information (qubits), we can dramatically lower the amount of communication required compared to sending classical information (bits). Quantum fingerprinting (Buhrman *et al.*, 2001) is an example of the quantum advantage in communication.

A fourth important application of quantum networks is computation. In its more direct sense, an alternative paradigm to the monolithic construction of a quantum computer is the so called modular or distributed quantum computer (Nickerson *et al.*, 2014). In this paradigm high quality small quantum computers are linked via entanglement to build a larger quantum computer. A quantum network can also be used to perform quantum computation on a remote quantum computer without revealing information about the computation or the underlying data (Aharonov *et al.*, 2017; Broadbent *et al.*, 2009; Childs, 2001), to perform multipartite computation (Cleve and Buhrman, 1997), or to obtain a computational advantage

in distributed computation tasks (Le Gall *et al.*, 2019).

Finally, the entanglement distributed by a quantum network can boost the performance of sensing applications (Degen *et al.*, 2017). Notable examples in this domain are in clock synchronization (Komar *et al.*, 2014) and in interferometry where entanglement can be used to extend the baseline of telescopes (Gottesman *et al.*, 2012; Khabiboulline *et al.*, 2019).

2. Stages of the quantum internet

The path to building the quantum internet will be long and difficult. The current standard viewpoint is that the quantum internet will probably develop in stages. There are different ways to divide it into stages. The classification proposed in (Wehner *et al.*, 2018) is based on the network functionality available to the end nodes.

Interestingly, quantum networks where nodes have very limited functionality are already useful for applications and new tasks can be implemented as the functionality of the end nodes increases. This means, that even at the early stages of development, we expect quantum networks to be useful. We will briefly recap the discussion in (Wehner *et al.*, 2018), linking the communication tasks introduced in VI.A.1 to development stages.

In the first stage *trusted repeater networks* are built. In this stage, the nodes can prepare and transmit quantum states to adjacent nodes in the network. This functionality allows to implement prepare-and-measure quantum key distribution protocols between adjacent nodes. In this way, it is possible, for instance, to construct a network of individual quantum key distribution links, but it is not a fully quantum network in the sense that quantum information cannot be transmitted to non-adjacent nodes. This very limited functionality is nonetheless useful: in such a network, if two end nodes trust the behavior of the nodes in a path connecting them, then they can exchange keys that are secure under this assumption (Salvail *et al.*, 2010). Existing quantum networks such as the Tokyo QKD network (Sasaki *et al.*, 2011), the SECOQC network (Peev *et al.*, 2009) and the Shanghai-Beijing network (Chen *et al.*, 2021b) are in this stage (see Sec. V.H.1).

In the second stage, end-to-end *prepare-and-measure networks* are built. In this stage, the nodes can prepare single qubits and transmit them to any other node in the network without any trust assumption and on the receiving side, nodes can measure incoming qubits. A potential price to pay is the post-selection of the transmitted signals. Nonetheless, prepare-and-measure networks can still be useful for various additional applications including secure identification in two-party cryptography with noisy quantum memories and key distribution. This includes protocols where entanglement is used to guarantee security but the nodes do not share an entangled state at

any moment. Instead, it is sufficient that the nodes can confirm whether entanglement could have been shared if the end nodes had run a coherent version of a prepare and measure protocol. For instance, communicators in a time-reversed entanglement distribution protocol (Biham *et al.*, 1996), measurement-device-independent quantum key distribution (MDI QKD) (Lo *et al.*, 2012), and twin-field quantum key distribution (TF QKD) (Lucamarini *et al.*, 2018) fall into this category, which remove assumptions about the measurement devices and highly limit the feasibility of side channel attacks (see, e.g., (Curty *et al.*, 2021)).

In the third stage, *entanglement distribution networks* are achieved where two users can obtain end-to-end quantum entanglement in either a deterministic or a heralded fashion. In this stage, the end nodes require no quantum memories. This added functionality enables, for example, device-independent QKD, when the loss is sufficiently low.

In the following we discuss the final three stages. These stages differ in the quality of the quantum computational capabilities of the nodes.

In the fourth stage, quantum memory networks are built. In this stage, the end users can store quantum information in their memories and teleport quantum information to each other. The minimum storage time is determined by the transit time between the two end nodes. Note that in this stage, the operations are done directly on the physical qubits. There is no fault tolerance. This functionality enables some blind quantum computation schemes, provided that there exists a remote quantum computer (Aharonov *et al.*, 2017; Broadbent *et al.*, 2009). It also enables protocols for extending the baseline of telescopes (Gottesman *et al.*, 2012; Khabiboulline *et al.*, 2019), protocols for cryptographic tasks such as anonymous quantum communication (Christandl and Wehner, 2005), secret sharing (Cleve *et al.*, 1999; Hillery *et al.*, 1999), simple leader election (Ambainis *et al.*, 2004), and some protocols for clock synchronization (Komar *et al.*, 2014).

In the fifth stage, few-qubit fault-tolerant networks are built. Here, the end nodes can perform local quantum operations fault-tolerantly on a few logical qubits. This ability allows more complex protocols to be executed. More concretely, an end node can perform fault-tolerant execution of a universal gate set on q logical qubits such as the number $q \geq 1$ is small enough that the local quantum processors can still be simulated efficiently by a conventional computer. Since conventional computing power tends to increase exponentially with time, what value of q remains simulatable is a function of time and technology. This functionality enables the implementation of a distributed quantum computer by linking the end nodes.

In the sixth and final stage, quantum computing networks are built and large-scale fault-tolerant quantum computation can be performed. The end node can per-

form large-scale quantum computation that cannot be simulated efficiently by any conventional computer. This will be the ultimate quantum internet. With this functionality it is possible to implement protocols for leader election (Tani *et al.*, 2005), fast byzantine agreement (Ben-Or and Hassidim, 2005), quantum money (Gavinsky, 2012) and weak coin flipping with arbitrarily small bias (Chailloux and Kerenidis, 2009; Mochon, 2007).

We end the recap of the stages by noting that the placement of the tasks in a stage in (Wehner *et al.*, 2018) corresponds to the current theoretical state of the art. Future protocol proposals might allow to reduce the requirements to implement a given task. For a more thorough description of existing protocols and their relation to the development stages we point the reader to the quantum protocol zoo (qua, 2019).

B. Quantum networks

1. Elements of a quantum network

The Internet connects user devices that we call end-systems or hosts. These devices are linked by communication channels to other nodes in the network. However, the hosts are not directly linked. Instead, they are connected via intermediate devices that are called routers. Routers in the internet receive packets of information on incoming links and depending on the content of the packet forward it through one outgoing link. Devices situated in a communication link that passively amplify the signal and do not take routing decisions are called relays.

Similarly, a quantum network (Van Meter, 2014) connects end-systems linked by quantum channels. Intermediate nodes in quantum networks, in addition to taking routing decisions, participate in the generation of long-distance entanglement. The responsibilities associated with entanglement generation depend on the technology (see Sec. III.B). They might include generating entanglement with adjacent nodes, implementing a purification protocol, swapping entanglement or processing encoded quantum information. Moreover, quantum networks will also require classical nodes and links for their operation.

In this review, we have used the term quantum repeaters to denote all intermediate nodes in a quantum network. However, it is possible to make a finer classification. In analogy with classical networks, Munro *et al.* (Munro *et al.*, 2022) differentiate between quantum relays and quantum repeaters depending on whether they process quantum information passively or actively. Another distinction can be made depending on whether the intermediate nodes participate in network management and decide how to swap entanglement or not. The former are called quantum routers and the latter automated quantum nodes (Dahlberg *et al.*, 2019; Kozłowski *et al.*, 2020b).

2. Network architecture

The Internet provides an information-transmission service to the end-systems. To implement this service, most communication networks rely on a layered approach. Each layer of the so-called network stack uses the service from the layer below without requiring any knowledge about how it is implemented or what hardware components it relies upon and provides a more complex service to the layer above.

A priori, the main service of the quantum internet will be the delivery of remote bipartite entanglement, which can then be used as a resource for applications (Van Meter, 2014). Other proposals posit that the delivery of graph states will be the fundamental primitive of the quantum internet (Pirker and Dür, 2019). Independently of the main service, for the quantum internet we can expect a similar layered architecture (Cacciapuoti *et al.*, 2019; Dahlberg *et al.*, 2019; Kozłowski *et al.*, 2020a,b; Pirker and Dür, 2019; Van Meter *et al.*, 2008; Van Meter and Touch, 2013) to the Internet, see (Illiano *et al.*, 2022) for a survey on protocol stack proposals. Recently, Pompili *et al.* (Pompili *et al.*, 2022) demonstrated experimentally entanglement delivery using a network stack.

The quantum internet architecture will not be independent of the Internet since it is clear that the quantum internet will rely on classical communication for its functionality. However, the quantum internet could also support the functionality of the classical internet creating a complex interplay (Cacciapuoti *et al.*, 2022).

C. The fundamental limits of communications over network

In the following we discuss the usefulness of quantum networks from an information theoretic point of view. First, we introduce a model of a network in terms of a graph and the relevant notation. Then, we define the quantities that characterize the fundamental limits for communicating over quantum networks, i.e., the quantum network capacities. In the network setting, there is a richer set of quantities when compared with direct transmission depending, for instance, on how the communication rates are defined or whether several sets of users concurrently want to perform a communications task.

Second, we show how to bound the network capacities both from above and from below. These bounds take a particularly simple form in some relevant cases: e.g., for general linear networks (Pirandola, 2019) or for bounding the performance of DLCZ-like protocols (like the one in Sec. III.A.3) in the presence of noisy memories (Azuma *et al.*, 2016).

We end by discussing the computability of these bounds, and show that given bounds on the individual channel capacities, the bounds on the network capacities can be derived efficiently.

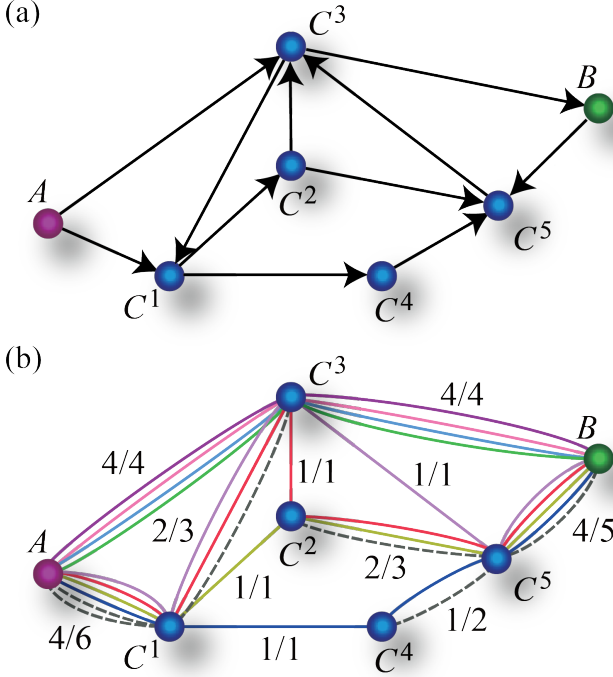


FIG. 21 Quantum network and a Bell-pair network. a) A quantum network as a graph. A quantum network can be abstracted by a directed graph, $G = (V, E)$ with V and E the sets of vertices and edges. However, if two-way classical communication is considered a free resource, edge directions play no role as quantum teleportation can be used to revert the direction of the channel. We associate with each vertex $v \in V$ a node in the quantum network and with each edge $e \in E$ a quantum channel \mathcal{N}_e . In this example, Alice's node A and Bob's node B are part of network with seven nodes also including intermediary nodes C^1, C^2, C^3, C^4 and C^5 . b) A network of maximally entangled states. One approach to entanglement distribution between distant parties in a quantum network is the aggregated repeater protocol (Azuma and Kato, 2017). In this protocol, adjacent nodes prepare maximally entangled states that then can be transformed into end-to-end entanglement between two distant parties by swapping the entanglement. In the figure, the graph from panel a) has been used to generate entanglement between adjacent nodes. Each edge is annotated with a fraction x/y , where the denominator y denotes the number of entangled pairs, while the numerator x denotes the number of entangled states used to establish entanglement between the end parties A and B . In this example, a total of eight Bell pairs could be distributed between A and B . Figure adapted from (Azuma and Kato, 2017).

1. An abstract depiction of networks

Similar to classical networks, quantum networks will consist of many different components: end nodes, communication channels, routers, switches, multiplexers, etc. However for analysis purposes it is more convenient to restrict networks to two different components: nodes and communication channels.

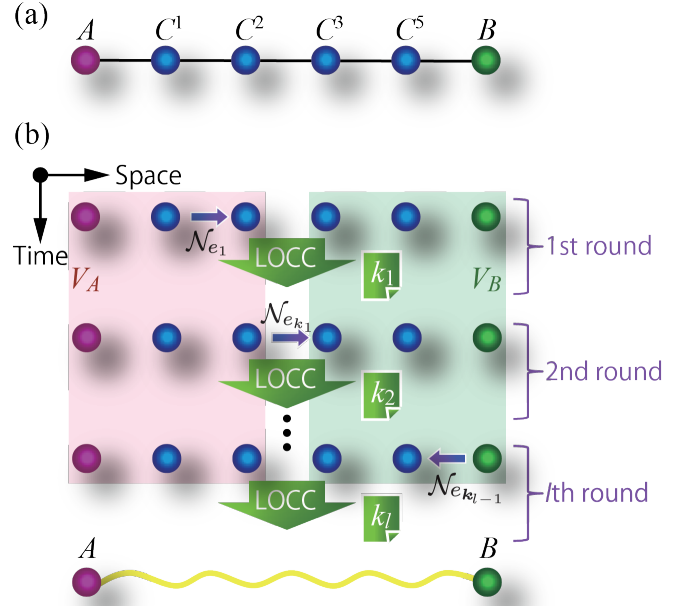


FIG. 22 Linear network and general protocol. a) A repeater chain or linear quantum network is associated with a linear graph, i.e., a graph that can be described by a sequence of edges connecting distinct nodes. The linear network in the panel may be a subnetwork of the network in panel a) from Fig. 21. b) The general adaptive protocol (Azuma *et al.*, 2016) illustrated over the linear network from panel a). The goal of the protocol is to distribute Bell pairs between A and B . The protocol begins with the network joint state represented by a separable state and proceeds iteratively until meeting a termination condition. On each round a node transmits a local subsystem through a quantum channel. Then all nodes perform an LOCC operation. The LOCC operation, the choice of a channel, and transmitted subsystem can depend on the history of the measurement outcomes of the protocol. The nodes of the linear network can be divided into two disjoint virtual nodes, V_A [nodes on the left (pink) box] including A and V_B [nodes on the right (green) box] including B . The intuition behind the capacity upper bounds in (47) and (49) is that distributing entanglement between these two virtual nodes is an easier task than distributing entanglement between A and B over the network. Figure adapted from (Azuma *et al.*, 2016).

We can represent this abstract network by $\mathcal{G} = (G, g)$, where $G = (V, E)$ is a directed graph (see Fig. 21 (a)) and g a map from edges in the graph to quantum channels, i.e., completely positive and trace-preserving maps.

We denote by V the set of nodes in the graph and by E the set of edges. Letting $e \in E$ be a directed edge from node u to node v , we say that the tail and head of the directed edge e are u and v , respectively. We will denote the edge by uv whenever it is useful to specify the tail and head of a node.

We associate with each node $v \in V$ a quantum information processing device. The capabilities of the

quantum information processing devices sitting at network nodes can range from a source that can prepare a predefined set of quantum states to a fully-fledged universal quantum computer. For the rest of the section, we assume that nodes can perform noiselessly arbitrary local operations (LO). Since classical communication is qualitatively cheaper than quantum communication, it is common to assume free classical communication between nodes connected by a quantum channel, and sometimes between any two nodes in the network. With this additional assumption, the nodes in the network can implement local operations and classical communication (LOCC) without cost.

Finally, we associate with each edge uv a quantum channel that receives a quantum system as the input from node u and outputs a quantum system to node v , via the map: $g(uv) = \mathcal{N}_{u \rightarrow v}$. To simplify notation, when possible we denote the channel at edge e by \mathcal{N}_e .

This abstract depiction of a network as a graph allows us to leverage tools from graph and network theory. One concept that will be useful for the following is a cut. Given a bipartition of the vertex set V , i.e., two sets $V' \subset V$ and $V'' = V \setminus V'$, the associated cut-set or cut $\Delta(V')$ is the set of edges connecting V' with V'' . In particular, the cut associated with V' is given by

$$\Delta(V') := \Delta^+(V') \cup \Delta^-(V') \quad (39)$$

with the output $\Delta^+(V')$ associated with V' ,

$$\Delta^+(V') := \{uv \in E : u \in V', v \in V \setminus V'\}, \quad (40)$$

and with the input $\Delta^-(V')$ associated with V' ,

$$\Delta^-(V') := \{uv \in E : u \in V \setminus V', v \in V'\}. \quad (41)$$

Given two different vertices $A, B \in V$, we denote by $V_{A;B}$ the set of all bipartitions of V separating A and B , i.e., the set of all the subsets of V that include node A but do not node B .

2. Quantum network capacities

While the applications of the quantum internet are very different, most of them can be implemented if the relevant nodes in the network share an appropriate entangled state. For instance, in order to transmit a d -dimensional quantum state it is sufficient to distribute a d -dimensional bipartite maximally entangled state,

$$|\Phi_d\rangle \equiv \frac{1}{\sqrt{d}} \sum_{i=1}^d |ii\rangle, \quad (42)$$

called an edit (called an ebit when $d = 2$), which then can be consumed to teleport the desired state (see Sec. III.A.1).

Similarly, to transmit secretly a message from a set of d possible messages, it suffices to distribute a d -dimensional bipartite private state (Horodecki *et al.*, 2005) or pdit (called pbit when $d = 2$). The family of private states consists of the states that can be used to generate a d -dimensional secret key, i.e., a uniform probability distribution over d values shared between two honest parties Alice and Bob and secret to any other user. The class of private states includes the class of maximally entangled states but is strictly larger. In fact, there exist states that cannot be distilled into a maximally entangled state but, nonetheless, can be used to distill a pdit (Horodecki *et al.*, 2005).

Formally, a pdit is a state shared between Alice who holds the systems $a_1 a_2$ and Bob who holds $b_1 b_2$ in the following form:

$$\gamma_d \equiv U_{\text{twist}} (|\Phi_d\rangle \langle \Phi_d|_{a_1 b_1} \otimes \sigma_{a_2 b_2}) U_{\text{twist}}^\dagger, \quad (43)$$

where $\sigma_{a_2 b_2}$ is an arbitrary bipartite state and $U_{\text{twist}} = \sum_{i,j=1}^d |ij\rangle \langle ij|_{a_1 b_1} \otimes U_{a_2 b_2}^{(ij)}$ is a so-called twisting controlled unitary: the systems $a_1 b_1$ control the application of $U_{a_2 b_2}^{(ij)}$, arbitrary unitary operators on the systems $a_2 b_2$.

GHZ states and multipartite private states (Augusiak and Horodecki, 2009) play a similar role as a resource for multiuser tasks such as secret sharing and conference key agreement. Hence, in order to study the usefulness of a quantum network for a given application, it suffices to study the rate at which the network can produce a desired resource state. In fact, for many tasks of interest both problems are equivalent.

For the sake of simplicity, we restrict the following discussion to bipartite target states, which we denote by $\theta_{AB}^{(d)}$. Typically the target state is a maximally entangled state or a private state: $\theta_{AB}^{(d)} = |\Phi_d\rangle \langle \Phi_d|_{AB}$ or $\theta_{AB}^{(d)} = \gamma_d$.

As mentioned earlier, we assume that the nodes can apply noiselessly any LOCC operation. Let us now discuss a general protocol for distributing entanglement in a quantum network between nodes A and B (see Fig. 22). Before the protocol, there is no entanglement between different nodes in the network. Therefore, the joint state is represented by a separable state as in Eq. (19). Iteratively, first a node transmits a local subsystem through a quantum channel and then all nodes perform an LOCC operation. The LOCC operation, the choice of a channel, and transmitted subsystem can depend on the history of the protocol, e.g., on measurement outcomes obtained through LOCC in previous rounds.

We denote the reduced state between A and B at the end of the protocol by σ_{AB} . It will be at trace distance $\epsilon (\geq 0)$ from a target state $\theta_{AB}^{(d)}$, i.e., $\|\sigma_{AB} - \theta_{AB}^{(d)}\|_1 = \epsilon$, where $\|X\|_1 = \text{Tr}(\sqrt{X^\dagger X})$. We say that a protocol is a $P_{\{n_e\}_{e \in E}, \epsilon}$ adaptive protocol if the average number of uses of channel \mathcal{N}^e is upper bounded by n_e for all edges and the protocol produces a state at most at a distance

ϵ from a target state $\theta_{AB}^{(d)}$, where $d(\geq 1)$ can depend on the outcome of the protocol.

The figure of merit of $P_{\{n_e\}_{e \in E}, \epsilon}$ protocols is the average amount of the target entanglement produced, which is quantified by $\log_2 d$ for the states mentioned. From an operational point of view, a d -dimensional maximally entangled state or private state enables respectively the transmission of $\log_2 d$ qubits or the private communication of $\log_2 d$ bits. We denote the average entanglement produced—it might vary from round to round—by $\langle \log_2 d \rangle$.

We obtain the rate at which the protocol produces the entanglement, by dividing the average entanglement by the appropriate quantity of resources used. In contrast with the single channel case, one can consider several metrics: the number of channels used, the number of full uses of the network or the number of times a path of channels connecting A with B was used. These metrics could be related to time which is for engineering purposes a more convenient figure of merit (see (Azuma and Kato, 2017), (Bäuml *et al.*, 2020), or (Azuma *et al.*, 2021) for detail).

The capacity of the quantum network is the optimal asymptotic rate for producing a target entangled state θ at which the error parameter ϵ can be made arbitrarily small. Following our previous discussion on the rate, each choice of rates gives rise to a different type of network capacity.

Let us denote by $n = \sum_e n_e$ an upper bound on the total number of channel uses and by $p_e = n_e/n$ the frequency that the protocol uses channel \mathcal{N}_e . Given a fixed set of frequencies, we define the capacity per channel use (Azuma *et al.*, 2016) as:

$$C_c^\theta(\mathcal{G}, \{p_e\}_{e \in E}) = \lim_{\epsilon \rightarrow 0} \lim_{n \rightarrow \infty} \frac{1}{n} \sup_{P_{\{n_e\}_{e \in E}, \epsilon}} \langle \log_2 d \rangle. \quad (44)$$

Depending on the network scenario, the usage frequencies of the channels in the network can be free parameters. In this case, Eq. (44) can be maximized over the set $\{p_e\}_{e \in E}$ of frequencies to give a unique network capacity per channel use (Bäuml *et al.*, 2020):

$$C_c^\theta(\mathcal{G}) = \max_{p_e \geq 0, \sum_e p_e = 1} C_c^\theta(\mathcal{G}, \{p_e\}_{e \in E}). \quad (45)$$

To capture the capacity per network use, which we denote by $C_n^\theta(\mathcal{G})$, we let all upper bounds on the average number of channel uses be equal $n_e = n_{e'}$ $e, e' \in E$ and let n denote the number of network uses, i.e., we let $n = n_e$, which then implies $p_e = 1, \forall e \in E$. This quantity corresponds to the notion introduced by Pirandola in (Pirandola, 2019) to capture the limits of so-called flooding protocols. A third important scenario is the single-path per network use capacity (Pirandola, 2019), where the goal is to maximize the rate per use of a single path, though it is unclear if it can be expressed in a form similar to Eq. (44).

If the target state θ is a maximally entangled state (see Eq. (42)), then these expressions represent a quantum capacity of the quantum network \mathcal{G} . If θ is a private state (see Eq. (43)) it represents a private capacity.

The distribution of entanglement between a single set of users is but one of many possible measures of usefulness of a quantum network. Networks typically serve many users and one might be interested in understanding the capacity of the network for distributing entanglement to multiple sets of users. Equation (44) can be adapted to capture multiuser setups by modifying appropriately the figure of merit of the protocol $\langle \log_2 d \rangle$ and the definition of $P_{\{n_e\}_{e \in E}, \epsilon}$ protocol (Bäuml *et al.*, 2020). For instance, given m sets of users and let $\langle \log_2 d^{(i)} \rangle$ be the average amount of entanglement that a $P_{\{n_e\}_{e \in E}, \epsilon}$ protocol produces for set i of users, then the maximization of $\min_{i=1}^m \langle \log_2 d^{(i)} \rangle$ leads to the maximum rate that can be guaranteed to all sets of users, called the worst-case network capacity, while the maximization of $\sum_{i=1}^m \langle \log_2 d^{(i)} \rangle$ leads to the maximum total rate, called the total network capacity.

3. Entanglement based upper bounds

While there is no known procedure for computing these capacities in general, there are several tools for bounding them both from above and from below leveraging the relation between the communication task and the distillation of the appropriate entangled state.

In the following, we present a formulation by (Rigovacca *et al.*, 2018) for abstract entanglement measures. This formulation generalizes earlier work by Pirandola (Pirandola, 2019) for quantum networks composed of a specific type of channels (called teleportation simulable channels, explained later) with the relative entropy of entanglement and by Azuma *et al.* (Azuma *et al.*, 2016) for arbitrary quantum networks with the squashed entanglement. In particular, these two results build respectively on the PLOB (Pirandola *et al.*, 2017) and TGW (Takeoka *et al.*, 2014a) bounds on the private capacity of an individual channel (see Sec. I and Sec. III.A.3).

In particular, let \mathcal{E} be a measure of bipartite entanglement. That is, \mathcal{E} is a function from the set of bipartite states into the positive real numbers that satisfy several requirements (Horodecki *et al.*, 2009). In particular, it is not increasing on average under LOCC. We define the entanglement of channel $\mathcal{N}_{A \rightarrow B}$ as

$$\mathcal{E}(\mathcal{N}_{A \rightarrow B}) \equiv \sup_{\rho_{AA'}} \mathcal{E}(\mathcal{N}_{A \rightarrow B}(\rho_{AA'})) , \quad (46)$$

where $\rho_{AA'}$ is a bipartite state with A' isomorphic to A .

Now, let \mathcal{E} be a bipartite entanglement measure that satisfies the following two inequalities:

P1 (Continuity) If a bipartite state ρ_{AB} is at epsilon distance from the target state $\theta_{AB}^{(d)}$, i.e., $\|\rho_{AB} -$

$\theta_{AB}^{(d)}\|_1 \leq \epsilon$, then $\mathcal{E}(\rho_{AB}) \geq g(\epsilon) \log d - f(\epsilon)$ with f and g two real valued continuous functions that verify $\lim_{\epsilon \rightarrow 0} f(\epsilon) = 0$ and $\lim_{\epsilon \rightarrow 0} g(\epsilon) = 1$.

P2 (Subadditivity) Given a bipartite state $\rho_{A_1 A_2 B_1}$, the entanglement in the AB -cut after sending the system A_2 through channel $\mathcal{N}_{A \rightarrow B}$ is not larger than the original entanglement in the AB -cut plus the entanglement of the channel: $\mathcal{E}(\sigma_{A_1 B_2 B_1}) \leq \mathcal{E}(\rho_{A_1 A_2 B_1}) + \mathcal{E}(\mathcal{N}_{A \rightarrow B})$, where $\sigma_{A_1 B_2 B_1} = \mathcal{N}_{A_2 \rightarrow B_2}(\rho_{A_1 A_2 B_1})$.

Then, the capacity of the network for distributing some target state θ between two nodes A and B can be bounded from above by the following optimization formulae (Rigovacca *et al.*, 2018):

$$C_c^\theta(\mathcal{G}, \{p_e\}_{e \in E}) \leq \min_{\mathcal{V} \in V_{A;B}} \sum_{e \in \Delta(\mathcal{V})} p_e \mathcal{E}(\mathcal{N}_e), \quad (47)$$

$$C_c^\theta(\mathcal{G}) \leq \max_{\substack{p_e \geq 0, \\ \sum_e p_e = 1}} \min_{\mathcal{V} \in V_{A;B}} \sum_{e \in \Delta(\mathcal{V})} p_e \mathcal{E}(\mathcal{N}_e), \quad (48)$$

$$C_n^\theta(\mathcal{G}) \leq \min_{\mathcal{V} \in V_{A;B}} \sum_{e \in \Delta(\mathcal{V})} \mathcal{E}(\mathcal{N}_e). \quad (49)$$

Note that Eqs. (47)-(49) do not depend on any functional of more than one channel: equations (47) and (48) depend only on the entanglement of each of the channels individually and the channel usage frequencies, while Eq. (49) depends only on the entanglement of the channels. The minimization is performed over $V_{A;B}$, the set of all cuts between A and B . The intuition for this formula is that we could join all the nodes of the network into two virtual nodes, one including A and one including B (see Fig. 22 (b)). Distributing entanglement between these two virtual nodes is an easier task and can be done at a rate no larger than the entanglement of all the channels connecting the two virtual nodes. Since this argument provides a valid upper bound for any bipartition, the minimum provides the best upper bound of this form.

Fortunately, there are several entanglement measures that verify P1 and P2 for private states (and in consequence also for maximally entangled states). In particular the squashed entanglement (Takeoka *et al.*, 2014a,b) and the max-relative entropy of entanglement (Christandl and Müller-Hermes, 2017) satisfy both properties for arbitrary channels, while the relative entropy of entanglement is only known to satisfy both properties for a family of channels known as teleportation simulable, Choi simulable or stretchable channels (Bennett *et al.*, 1996c; Gottesman and Chuang, 1999; Horodecki *et al.*, 1999; Pirandola *et al.*, 2017; Wolf *et al.*, 2007).

Leveraging an inequality from (Christandl and Müller-Hermes, 2017), Rigovacca *et al.* (Rigovacca *et al.*, 2018) proved a hybrid relative entropy upper bound, where the entanglement measure in the upper bounds in Eqs. (47),

(48) and (49) is the relative entropy of entanglement for teleportation simulable channels and the max-relative entropy of entanglement for the other channels. Therefore, the currently best option to give upper bounds in the form (47), (48) or (49) to a given arbitrary quantum network is to use this hybrid relative-entropy bound or the squashed-entanglement bound. Many relevant channels such as the amplitude damping channel are not teleportation simulable. However, several channels of particular interest are teleportation simulable; this includes the depolarizing and dephasing channels, more generally mixed Pauli channels, the erasure channel and lossy bosonic channels. Remarkably for the lossy bosonic channels, which model optical fibers, the relative entropy of entanglement based upper bound is tight (Pirandola *et al.*, 2017). In the following we define Choi-simulable channels and particularize the bounds for this case.

A channel $\mathcal{N}_{A \rightarrow B}$ is teleportation simulable if given a state ρ_A that one wants to transmit through channel $\mathcal{N}_{A \rightarrow B}$ and the Choi state of the channel $\Gamma_{A'B} = \mathcal{N}_{A \rightarrow B}(|\Phi_d\rangle\langle\Phi_d|_{A'A})$, there exists an LOCC protocol Λ that simulates the action of the channel on any input state ρ_A :

$$\mathcal{N}_{A \rightarrow B}(\rho_A) = \Lambda(\Gamma_{A'B} \otimes \rho_{A'}) . \quad (50)$$

To gain intuition on this equation one can think of the identity channel from A to B . Then simulation can be obtained by teleportation, i.e., Λ consists of a joint generalized Bell measurement on systems $A'A''$ and applying the appropriate correction to system B . More generally, this strategy works for any channel whose action commutes with the receiver's corrections of quantum teleportation (Bennett *et al.*, 1993), because, in this case, the correction to system B can be regarded as correction for system A before entering the channel $\mathcal{N}_{A \rightarrow B}$ and thus, this is merely a local teleportation to send a quantum state $\rho_{A''}$ to system A .

4. Application of the upper bounds to linear networks

In the following we focus on a particular use case: linear networks (see Fig. 22). This use case of the upper bounds is of particular relevance to quantum repeater protocols. In this case, the cut-sets are the individual channels, highly simplifying the upper bounds. The bounds on the capacities per channel (47), (48) and per network (49) use take the form:

$$C_c^\theta(\mathcal{G}, \{p_e\}_{e \in E}) \leq \min_{e \in E} p_e \mathcal{E}(\mathcal{N}_e), \quad (51)$$

$$C_c^\theta(\mathcal{G}) \leq \frac{1}{\sum_{e \in E} [\mathcal{E}(\mathcal{N}_e)]^{-1}}, \quad (52)$$

$$C_n^\theta(\mathcal{G}) \leq \min_{e \in E} \mathcal{E}(\mathcal{N}_e). \quad (53)$$

The upper bound on the network capacity per channel use (52) was derived in (Azuma *et al.*, 2016).

As a first example, let us consider a linear network connected by lossy bosonic channels. For these channels, the choice of the relative entropy of entanglement (i.e., $\mathcal{E} = E_{\text{R}}$) gives tight bounds. In particular, it was shown in (Pirandola *et al.*, 2017) that $E_{\text{R}}(\mathcal{N}_e) = -\log_2(1 - \eta_e)$, where η_e is the transmittance of the lossy bosonic channel \mathcal{N}_e of Eq. (13). Then, if we insert this relation into Eqs. (51), (52) and (53), we obtain the following expressions for the capacities of the network, including one derived in (Pirandola, 2019):

$$C_c^\theta(\mathcal{G}, \{p_e\}_{e \in E}) = \min_{e \in E} -p_e \log_2(1 - \eta_e), \quad (54)$$

$$C_c^\theta(\mathcal{G}) = \frac{1}{\sum_{e \in E} (-\log_2(1 - \eta_e))^{-1}}, \quad (55)$$

$$C_n^\theta(\mathcal{G}) = \min_{e \in E} -\log_2(1 - \eta_e). \quad (56)$$

As a second example, we consider the performance of a DLCZ-type quantum repeater protocol (Duan *et al.*, 2001) (like one in Sec. III.A.3) where the memory in the nodes is subject to decoherence and taking into account the time required to exchange classical communication between distant nodes. Razavi *et al.* (Razavi *et al.*, 2009) noticed that in contrast with the polynomial scaling with the total distance L predicted by the DLCZ protocol, the performance with finite coherence times of quantum memories degrades exponentially with \sqrt{L} . Azuma *et al.* (Azuma *et al.*, 2016) strengthened the results and showed that polynomial scalings for a large class of DLCZ-type protocols could be only possible above a threshold coherence time. In particular, see Fig. 23, the performance of any DLCZ-type repeater scheme with a memory coherence time below 1.0×10^{-4} s is upper-bounded by an exponential on the square root of the total distance, and this kind of performance is achievable as described in Sec. IV. The key idea to apply upper bound (52) is that the memory noise can be modeled by a noisy quantum channel between the memory at the time when it stores a state and the memory at the moment that it releases the state. In consequence, the performance of any protocol using the noisy memory is bounded by the performance of an induced linear network (i.e., by using Eq. (52)).

5. Capacity lower bounds via the aggregated repeater protocol

Now let us look at a general lower bound on the capacity of quantum networks (Azuma and Kato, 2017). This lower bound, based on aggregated quantum repeater protocol, matches the general upper bounds given in Eqs. (47) and (49) up to a prefactor. Moreover, the aggregation of even existing protocols (Duan *et al.*, 2001; Jiang *et al.*, 2009; Li *et al.*, 2013; Mazurek *et al.*, 2014; Sangouard *et al.*, 2011) matches the lower bound on the capacity up to another prefactor for the case of optical quantum networks composed of lossy bosonic channels. This implies that the upper bounds have no scaling

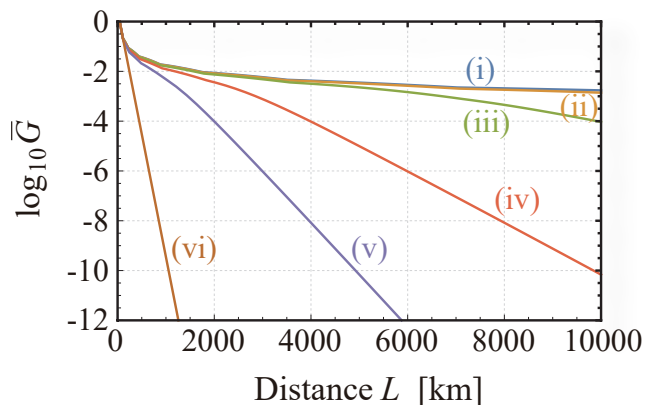


FIG. 23 Upper bound on the secret key rate achievable with a noisy linear network. In particular, the upper bound applies to a wide range of protocols including DLCZ (Duan *et al.*, 2001) and others (Azuma *et al.*, 2012; Kok *et al.*, 2003; Sangouard *et al.*, 2011) when implemented with matter quantum memories in the presence of dephasing noise. The linear network consists of a chain of repeaters equally separated and connected by an optical fiber with attenuation length 22 km and spanning a total distance of L km. The curves labeled by (i-vi) correspond respectively with the following coherence times: 1.0×10^{-2} s, 5.0×10^{-3} s, 2.5×10^{-3} s, 1.0×10^{-3} s, 5.0×10^{-4} s, 1.0×10^{-4} s. The upper bound in (vi) scales better than direct transmission, roughly proportional to the square root of the PLOB bound, but equivalent to the intercity QKD protocols in Sec. IV. In consequence, with a coherence time of 1.0×10^{-4} s there can be no advantage for a DLCZ-type repeater scheme compared with the simpler intercity QKD protocols. Figure from (Azuma *et al.*, 2016).

gap and yield good measures of the usefulness of a network. We note that, while we have exemplified the upper bounds with a linear network of repeaters in Sec. VI.C.4, they can be applied to any quantum network with arbitrary topology, including distributed quantum computation setups.

In the following, we discuss the lower bound which corresponds with the achievable rate of the aggregated quantum repeater protocol introduced by Azuma *et al.* (Azuma and Kato, 2017), see Fig. 21 (b). The goal of this protocol is to distribute entanglement between targeted nodes in the network which is later consumed to perform the appropriate communications task.

For each of the quantum channels in a given quantum network, let us consider a protocol that produces entangled states that are ϵ -close to a maximally entangled state at a rate R_e which can be different for each channel. This is possible for all channels provided that $R_e < Q(\mathcal{N}_e)$, i.e., provided that the rate is below the maximal rate of the channel for distributing maximally entangled states for a large enough number of channel uses (called the quantum capacity of the channel \mathcal{N}_e). Then, if each of the channels is used n_e times, the whole network will be in a tensor product of entangled states and the whole network can be regarded as a multi-graph with $n_e R_e$ edges

per edge in the original graph, where each edge in the multi-graph corresponds to a qubit maximally entangled state $|\Phi_2\rangle$.

We can use the resulting state to create maximally entangled states between Alice at node A and Bob at node B . For each state it is necessary to perform entanglement swapping over a path of maximally entangled states connecting Alice with Bob. The number of maximally entangled states that can be distributed between Alice and Bob is then equivalent to the maximum number of edge disjoint paths connecting Alice with Bob in the multi-graph. This maximum number of paths is by Menger's theorem (Jungnickel, 2005) equivalent to the value of the minimum cut of the graph:

$$M = \min_{\mathcal{V} \in V_{A;B}} \sum_{e \in \Delta(\mathcal{V})} n_e R_e. \quad (57)$$

This minimization can be solved in time proportional to a polynomial in the number of edges. However, since the number of edges grows with the number of uses, the full optimization is a priori intractable. Now, if we consider the achievable rate per channel use with the aggregated repeater protocol, Eq. (57) becomes $\min_{\mathcal{V} \in V_{A;B}} \sum_{e \in \Delta(\mathcal{V})} (n_e/n) R_e$. Moreover, for a number of uses n large enough, any rate below the capacity of each channel is achievable. Consequently, the right-hand side of the following expression is achievable:

$$C_c^\theta(\mathcal{G}, \{p_e\}_{e \in E}) \geq \min_{\mathcal{V} \in V_{A;B}} \sum_{e \in \Delta(\mathcal{V})} p_e Q(\mathcal{N}_e), \quad (58)$$

$$C_c^\theta(\mathcal{G}) \geq \max_{\substack{p_e \geq 0, \\ \sum_e p_e = 1}} \min_{\mathcal{V} \in V_{A;B}} \sum_{e \in \Delta(\mathcal{V})} p_e Q(\mathcal{N}_e), \quad (59)$$

$$C_n^\theta(\mathcal{G}) \geq \min_{\mathcal{V} \in V_{A;B}} \sum_{e \in \Delta(\mathcal{V})} Q(\mathcal{N}_e), \quad (60)$$

where $p_e = n_e/n$. We note that the lower bounds are of the same form of the respective upper bounds in Eqs. (47)-(49) where the entanglement of the channel is replaced by the quantum capacity. Therefore, if $\mathcal{E}(\mathcal{N}_e) = Q(\mathcal{N}_e)$ holds for any e , these lower bounds (58), (59) and (60) coincide with upper bounds (47), (48), and (49). For example, this is indeed the case for quantum networks composed only of lossy bosonic channels.

The aggregation of quantum repeaters is also possible with minimizing cost (Azuma, 2023). The cost here is a general notion like a price to pay for presenting ebits between two targeted nodes in a quantum network.

6. Computability of the network capacities

Let us now discuss how to compute both the lower and the upper bounds in Eqs. (47), (49), (58), and (60). This is indeed important in practice, for instance, to determine how a network provider should distribute entanglement

to clients according to their requests. All four equations depend only on the values of the entanglement of the individual channels. The four quantities are expressed as the solution of the minimum cut over an undirected graph. These optimization problems can be solved by a linear program in time polynomial in the number of nodes in the graph (Jungnickel, 2005). Similar arguments allow one to find efficiently lower and upper bounds not only on the capacities for two-party communication described above, but also on the worst-case and total quantum network capacities (see VI.C.2) and for distributing GHZ states (Bäumel *et al.*, 2020).

VII. CONCLUDING REMARKS

The quantum internet will have important applications in sensor networks, upscaling quantum computing and secure quantum communication (van Dam, 2020). To build the quantum internet, quantum repeaters have been proposed and studied extensively. This review has focused on the various generations of quantum repeaters as well as all-photon quantum repeaters; we have seen that quantum repeaters are essential to realize an efficient quantum internet. Nonetheless, our discussion has been largely limited to a fiber-optical setting connecting two end nodes, Alice and Bob.

In this concluding section, we take a step back to think some more about how to build a quantum internet. We will discuss a few alternative designs and important issues facing the quantum internet—not only its efficiency, but also its cost and the uncertainty in the technology it would leverage.

Cost can be a critical issue in realizing any technology. Although the conventional Internet is believed to contribute trillions of US dollars each year to the US economy, just upgrading the existing fiber optical network in the US to cover, say, 90 percent of households there would take an additional investment of over 100 billion US dollars (see, e.g., (Cartesian, 2021)). This figure is for a single country and for an upgrade to the existing, extensively developed, Internet. Therefore, it is not unreasonable to predict that the construction and operation of a global quantum internet would ultimately take decades and require investments of trillions of US dollars. This is an astonishing number. Such an enormous investment would almost certainly come not only from governments, but also from for-profit commercial corporations. For a comparison, the LIGO and LHC projects—endeavours admittedly more localized in scope—required only 1.1 billion and 4.75 billion dollars, respectively (Horgan, 2016; Roche, 2022). We have not even begun to estimate the cost of building various generations of quantum repeater structures on a global scale. Some detailed calculations, aided by a quantum network simulator, would be needed to address the cost issue more seriously.

On the other hand, as mentioned in the introductory section I, the Internet consumes a lot of energy through the transmission of optical signals. Furthermore, the sensing, monitoring and routing of the Internet require massive amounts of local computational power. As the Internet grows, scalability becomes a challenge. A quantum internet could operate at single-photon level. It may well be interesting to explore whether a quantum internet could lead to huge savings in energy consumption. Similarly, it may be worthwhile to investigate whether quantum computing and quantum information processing could contribute to the management of the internet.

Next, let us imagine a world—sometime in the distant future—where quantum memories with long-term stability become widely available at low cost. In this case, to distribute entanglement, one could simply ship those stable quantum memories all over the world, physically, in the same way that we currently dispatch hard drives and mail (see, e.g., (Devitt *et al.*, 2016)). The apparent drawback would be latency, which means the delay before a transfer of data begins following an instruction for its transfer; however, this shipment could be done off-line, and entanglement swapping could be used to connect users via intermediate nodes *instantaneously* in the same way that a telephone network can connect the users. In this way, the latency issue could be alleviated. With the physical shipment of quantum memory devices, the requirements of quantum repeaters could be reduced. This is just one way in which our design of the quantum internet is highly dependent on the available technology, in addition to cost.

Currently, quantum memories often operate at cryogenic temperatures and their lifetimes are often limited. If this is the case, quantum repeater nodes will need refrigerators. Notice that all-photon quantum repeaters may also require refrigerators (either in photonic graph state generation devices or measurement devices). Suppose we wanted to connect someone in New York with another person in Tokyo—10,845 km away—through undersea optical fibers. Then, optimistically, we would need to place a quantum repeater node every a few hundred kilometers under the sea. In this case, hundreds of repeater nodes would be needed. Placing cryogenic repeater nodes in undersea optical fibers, maintaining them, and providing the energy to operate them reliably are no easy feats, and would likely prove very costly.

As an alternative solution, ground-to-satellite quantum communication is a serious candidate. By preparing an entangled source of photons in a satellite, Charlie, and sending it to two ground stations, Alice and Bob, Charlie can act as an untrusted relay to connect two distant locations on the globe. Currently, line of sight is a serious restriction in ground-to-satellite communication. However, we can envision a future wherein space-grade long-lifetime quantum memories are available. By first sending one half of an entangled pair to Alice, storing the

second half in the quantum memory on a rapidly moving quantum satellite, and later sending it to Bob, Charlie can connect any two ground stations that have a line of sight to any point on the satellite’s orbit. Besides this, a constellation of orbiting satellites could provide a continuous, on-demand entanglement distribution service to ground stations (Khatri *et al.*, 2021). In principle, one could put quantum repeaters even on satellites to run a quantum repeater protocol (Liorni *et al.*, 2021). However, this may also be challenging if the repeaters need cryogenic environment.

As mentioned earlier (see Sec. III), the probabilistic nature of a Bell state measurement in linear optics (for certain photonic encodings) is a key limiting factor in the design of both matter-based and all-photon quantum repeaters. Indeed, without using additional ancillae or a different encoding, the success probability of a linear-optical Bell measurement is upper-bounded by $1/2$. A game changer for the efficiency of quantum repeaters would therefore be a near-deterministic, high-fidelity entangling gate on photons. This could be based on, for example, an enhancement by quantum memories (Bhaskar *et al.*, 2020; Borregaard *et al.*, 2020; Munro *et al.*, 2012).

For all-photon quantum repeaters in particular, a game-changer would be the deterministic generation of photonic graph states based on coupled quantum emitters such as quantum dots (see, e.g., (Li *et al.*, 2021a)). Alternatively, a hybrid approach with a single quantum emitter and subsequent fusions would also dramatically lower the resource requirements (Hilaire *et al.*, 2022). There exists another possibility of the development purely on all photonics: beginning with all-photon quantum key distribution (Sec. IV), proceeding to all-photon quantum repeaters (Sec. III.C), and ending with linking fault-tolerant photonic quantum computers (e.g., (Knill *et al.*, 2001b)).

Another important area of research is the quantum interconnect (see, e.g., (Awschalom *et al.*, 2021)). Indeed, the ability to convert and transfer quantum information across different platforms will enhance the interoperability of the future quantum internet.

In this review, we have focused on the distribution of bipartite entanglement. However, for many applications, including quantum sensing, it is often advantageous to use multipartite entangled states. Conceptually, we may build up multipartite states through successive teleportations. However, were we to do it with linear optics, the probabilistic nature of a Bell measurement would make the success probability of constructing an n -partite entangled state exponentially small. Therefore, there is value in further exploring the preparation and distribution of multipartite entanglement.

To conclude, we stress that a truly global quantum internet requires seamless operation across continents. As different countries are currently pursuing different approaches and strategies for the quantum internet, there will be a need for cooperation and standardization in the

design, construction and operation of this major technology.

ACKNOWLEDGMENTS

We thank Stefan Bäuml, Johannes Borregaard, Ronald Hanson, Tomoyuki Horikiri, Rikizo Ikuta, Jessica Iliano, Norbert Lütkenhaus, Mattia Montagna, William J. Munro, Shoichi Murakami, Fatih Ozaydin, Stefano Pirandola, John Preskill, Mohsen Razavi, Tim Taminiau, Wolfgang Tittel, Takashi Yamamoto, Qiang Zhou, and Val Zwiller for their helpful comments and suggestions on different versions of this manuscript. K.A. is thankful for the support, in part, from CREST, JST JP-MJCR1671, from PREST, JST JP-MJPR1861, from Moonshot R&D, JST JPMJMS2061, and from JSPS KAKENHI 21H05183 JP. S.E.E. was supported by the NSF (grant number 1741656), the EU Horizon 2020 programme (GA 862035 QLUSTER), and by ARO (MURI grant no. W911NF2120214). D.E. was supported by the Netherlands Organization for Scientific Research (NWO/OCW), as part of the Quantum Software Consortium program (project number 024.003.037 / 3368). L.J. was supported by the ARO (W911NF-18-1-0020, W911NF-18-1-0212), ARO MURI (W911NF-16-1-0349), AFOSR MURI (FA9550-19-1-0399, FA9550-21-1-0209), DoE Q-NEXT, NSF (EFMA-1640959, OMA-1936118, EEC-1941583), NTT Research, and the Packard Foundation (2013-39273). H.-K. Lo was supported by NSERC, Connaught Innovation, CFI, ORF, MITACS Accelerate, Huawei Canada, Royal Bank of Canada (RBC), the start-up grant by the University of Hong Kong, US Air Force, NRC-CSTIP program, and Innovative Solutions Canada program. I.T. was supported by the Ontario Graduate Scholarship.

REFERENCES

- (2019), “Quantum protocol zoo,” <https://wiki.veriqcloud.fr>.
- (2022), “The European Quantum Communication Infrastructure (EuroQCI) Initiative,” <https://digital-strategy.ec.europa.eu/en/policies/european-quantum-communication-infrastructure-euroqci>.
- Abobeih, M H, Y. Wang, J. Randall, S. J. H. Loenen, C. E. Bradley, M. Markham, D. J. Twitchen, B. M. Terhal, and T. H. Taminiau (2022), “Fault-tolerant operation of a logical qubit in a diamond quantum processor,” *Nature* **606**, 884–889.
- Abobeih, Mohamed H, Julia Cramer, Michiel A. Bakker, Norbert Kalb, Matthew Markham, Daniel J. Twitchen, and Tim H. Taminiau (2018), “One-second coherence for a single electron spin coupled to a multi-qubit nuclear-spin environment,” *Nature Communications* **9**, 2552.
- Abruzzo, Silvestre, Hermann Kampermann, and Dagmar Bruß (2014), “Measurement-device-independent quantum key distribution with quantum memories,” *Physical Review A* **89** (1), 012301.
- Afzelius, Mikael, Christoph Simon, Hugues de Riedmatten, and Nicolas Gisin (2009), “Multimode quantum memory based on atomic frequency combs,” *Physical Review A* **79** (5), 052329.
- Aharonov, Dorit, Michael Ben-Or, Elad Eban, and Urmila Mahadev (2017), “Interactive proofs for quantum computations,” arXiv preprint arXiv:1704.04487.
- Aharonovich, I, S. Castelletto, D. A. Simpson, C.-H. Su, A. D. Greentree, and S. Praver (2011), “Diamond-based single-photon emitters,” *Reports on progress in Physics* **74** (7), 076501.
- Aharonovich, Igor, Dirk Englund, and Milos Toth (2016), “Solid-state single-photon emitters,” *Nature Photonics* **10** (10), 631–641.
- Albert, Victor V, Kyungjoo Noh, Kasper Duivenvoorden, Dylan J Young, R T Brierley, Philip Reinhold, Christophe Vuillot, Linshu Li, Chao Shen, S M Girvin, Barbara M Terhal, and Liang Jiang (2018), “Performance and structure of single-mode bosonic codes,” *Physical Review A* **97** (3), 32346.
- Ambainis, Andris, Harry Buhrman, Yevgeniy Dodis, and Hein Rohrig (2004), “Multiparty quantum coin flipping,” in *Proceedings. 19th IEEE Annual Conference on Computational Complexity, 2004.* (IEEE) pp. 250–259.
- Androvsitanneas, Petros, A. B. Young, J. M. Lennon, Christian Schneider, Sebastian Maier, J. J. Hinchliff, G. S. Atkinson, Edmund Harbord, Martin Kamp, S. Hofling, *et al.* (2019), “Efficient quantum photonic phase shift in a low q-factor regime,” *ACS Photonics* **6** (2), 429–435.
- Ang, James, Gabriella Carini, Yanzhu Chen, Isaac Chuang, Michael Austin DeMarco, Sophia E Economou, Alec Eickbusch, Andrei Faraon, Kai-Mei Fu, Steven M Girvin, *et al.* (2022), “Architectures for multinode superconducting quantum computers,” arXiv preprint arXiv:2212.06167.
- Appel, Martin Hayhurst, Alexey Tiranov, Simon Pabst, Ming Lai Chan, Christian Starup, Ying Wang, Leonardo Midolo, Konstantin Tiurev, Sven Scholz, Andreas D Wieck, *et al.* (2022), “Entangling a hole spin with a time-bin photon: A waveguide approach for quantum dot sources of multiphoton entanglement,” *Phys. Rev. Lett.* **128** (23), 233602.
- Arcari, Marta, Immo Söllner, Alisa Javadi, S. Lindskov Hansen, Sahand Mahmoodian, Jin Liu, Henri Thyrestrup, Eun Hye Lee, Jin Dong Song, Søren Stobbe, *et al.* (2014), “Near-unity coupling efficiency of a quantum emitter to a photonic crystal waveguide,” *Phys. Rev. Lett.* **113** (9), 093603.
- Arnold, C, V. Loo, A. Lemaître, I. Sagnes, O. Krebs, P. Voisin, P. Senellart, and L. Lanco (2014), “Cavity-enhanced real-time monitoring of single-charge jumps at the microsecond time scale,” *Physical Review X* **4**, 021004.
- Arroyo-Camejo, Silvia, Andrii Lazariiev, Stefan W Hell, and Gopalakrishnan Balasubramanian (2014), “Room temperature high-fidelity holonomic single-qubit gate on a solid-state spin,” *Nature Communications* **5**, 4870.
- Asadi, F Kimiaee, S C Wein, and C Simon (2020), “Protocols for long-distance quantum communication with single 167er ions,” *Quantum Science and Technology* **5** (4), 045015.
- Asavanant, Warit, Yu Shiozawa, Shota Yokoyama, Baramee Charoensombutamon, Hiroki Emura, Rafael N. Alexander, Shuntaro Takeda, Jun ichi Yoshikawa, Nicolas C. Menicucci, Hidehiro Yonezawa, and Akira Furusawa (2019), “Generation of time-domain-multiplexed two-dimensional cluster state,” *Science* **366** (6463), 373–376.
- Atatüre, Mete, Dirk Englund, Nick Vamivakas, Sang-Yun Lee,

- and Joerg Wrachtrup (2018), “Material platforms for spin-based photonic quantum technologies,” *Nature Reviews Materials* **3** (5), 38–51.
- Augusiak, Remigiusz, and Paweł Horodecki (2009), “Multi-partite secret key distillation and bound entanglement,” *Physical Review A* **80** (4), 042307.
- Awschalom, David, Karl K. Berggren, Hannes Bernien, Sunil Bhave, Lincoln D. Carr, Paul Davids, Sophia E. Economou, Dirk Englund, Andrei Faraon, Martin Fejer, *et al.* (2021), “Development of quantum interconnects (quics) for next-generation information technologies,” *PRX Quantum* **2** (1), 017002.
- Awschalom, David D, Ronald Hanson, Jörg Wrachtrup, and Brian B. Zhou (2018), “Quantum technologies with optically interfaced solid-state spins,” *Nature Photonics* **12** (9), 516–527.
- Azuma, Koji (2023), “Networking quantum networks with minimum cost aggregation,” arXiv preprint arXiv:2304.08921.
- Azuma, Koji, Stefan Bäuml, Tim Coopmans, David Elkouss, and Boxi Li (2021), “Tools for quantum network design,” *AVS Quantum Science* **3** (1), 014101.
- Azuma, Koji, Nobuyuki Imoto, and Masato Koashi (2022), “Optimal supplier of single-error-type entanglement via coherent-state transmission,” *Phys. Rev. A* **105**, 062432.
- Azuma, Koji, and Go Kato (2012), “Optimal entanglement manipulation via coherent-state transmission,” *Physical Review A* **85** (6), 060303.
- Azuma, Koji, and Go Kato (2017), “Aggregating quantum repeaters for the quantum internet,” *Physical Review A* **96** (3), 032332.
- Azuma, Koji, Akihiro Mizutani, and Hoi-kwong Lo (2016), “Fundamental rate-loss trade-off for the quantum internet,” *Nature Communications* **7**, 13523.
- Azuma, Koji, Naoya Sota, Masato Koashi, and Nobuyuki Imoto (2010), “Tight bound on coherent-state-based entanglement generation over lossy channels,” *Physical Review A* **81** (2), 022325.
- Azuma, Koji, Naoya Sota, Ryo Namiki, Şahin Kaya Özdemir, Takashi Yamamoto, Masato Koashi, and Nobuyuki Imoto (2009), “Optimal entanglement generation for efficient hybrid quantum repeaters,” *Physical Review A* **80** (6), 060303.
- Azuma, Koji, Hitoshi Takeda, Masato Koashi, and Nobuyuki Imoto (2012), “Quantum repeaters and computation by a single module: Remote nondestructive parity measurement,” *Physical Review A* **85** (6), 062309.
- Azuma, Koji, Kiyoshi Tamaki, and Hoi-Kwong Lo (2015a), “All-photonic quantum repeaters,” *Nature Communications* **6** (1), 6787.
- Azuma, Koji, Kiyoshi Tamaki, and William J. Munro (2015b), “All-photonic intercity quantum key distribution,” *Nature Communications* **6**, 10171.
- Bacco, Davide, Jacob F. F. Bulmer, Manuel Erhard, Marcus Huber, and Stefano Paesani (2021), “Proposal for practical multidimensional quantum networks,” *Phys. Rev. A* **104**, 052618.
- Bacon, Dave (2006), “Operator quantum error-correcting subsystems for self-correcting quantum memories,” *Phys. Rev. A* **73**, 012340.
- Balasubramanian, Gopalakrishnan, Philipp Neumann, Daniel Twitchen, Matthew Markham, Roman Kolesov, Norikazu Mizuochi, Junichi Isoya, Jocelyn Achard, Johannes Beck, Julia Tissler, *et al.* (2009), “Ultralong spin coherence time in isotopically engineered diamond,” *Nature materials* **8** (5), 383–387.
- Bar-Gill, Nir, Linh M. Pham, Andrejs Jarmola, Dmitry Budker, and Ronald L. Walsworth (2013), “Solid-state electronic spin coherence time approaching one second,” *Nature Communications* **4**, 1743.
- Barnum, Howard, Carlton M Caves, Christopher A Fuchs, Richard Jozsa, and Benjamin Schumacher (1996), “Non-commuting mixed states cannot be broadcast,” *Phys. Rev. Lett.* **76** (15), 2818.
- Barrett, Jonathan, Roger Colbeck, and Adrian Kent (2013), “Memory attacks on device-independent quantum cryptography,” *Phys. Rev. Lett.* **110**, 010503.
- Barrett, S D, Pieter Kok, Kae Nemoto, R. G. Beausoleil, W. J. Munro, and T. P. Spiller (2005), “Symmetry analyzer for nondestructive bell-state detection using weak nonlinearities,” *Phys. Rev. A* **71**, 060302.
- Barrett, Sean D, and Pieter Kok (2005), “Efficient high-fidelity quantum computation using matter qubits and linear optics,” *Physical Review A* **71** (6), 060310.
- Barros, HG, A Stute, TE Northup, C Russo, PO Schmidt, and R Blatt (2009), “Deterministic single-photon source from a single ion,” *New Journal of Physics* **11** (10), 103004.
- Bartolucci, Sara, Patrick Birchall, Hector Bombin, Hugo Cable, Chris Dawson, Mercedes Gimeno-Segovia, Eric Johnston, Konrad Kieling, Naomi Nickerson, Mihir Pant, *et al.* (2023), “Fusion-based quantum computation,” *Nature Communications* **14** (1), 912.
- Bauch, Erik, Connor A Hart, Jennifer M Schloss, Matthew J Turner, John F Barry, Pauli Kehayias, Swati Singh, and Ronald L Walsworth (2018), “Ultralong dephasing times in solid-state spin ensembles via quantum control,” *Physical Review X* **8** (3), 031025.
- Bäuml, Stefan, Koji Azuma, Go Kato, and David Elkouss (2020), “Linear programs for entanglement and key distribution in the quantum internet,” *Communications Physics* **3**, 55.
- Bayrakci, Veysel, and Fatih Ozaydin (2022), “Quantum zeno repeaters,” *Scientific Reports* **12** (1), 15302.
- Bechtold, Alexander, Dominik Rauch, Fuxiang Li, Tobias Simmet, Per-Lennart Ardel, Armin Regler, Kai Müller, Nikolai A Sinitsyn, and Jonathan J Finley (2015), “Three-stage decoherence dynamics of an electron spin qubit in an optically active quantum dot,” *Nature Physics* **11** (12), 1005–1008.
- Becker, Jonas N, Benjamin Pingault, David Groß, Mustafa Gündoğan, Nadezhda Kukharchyk, Matthew Markham, Andrew Edmonds, Mete Atatüre, Pavel Bushev, and Christoph Becher (2018), “All-optical control of the silicon-vacancy spin in diamond at millikelvin temperatures,” *Phys. Rev. Lett.* **120** (5), 053603.
- Bell, B A, D. A. Herrera-Martí, M. S. Tame, D. Markham, W. J. Wadsworth, and J. G. Rarity (2014), “Experimental demonstration of a graph state quantum error-correction code,” *Nature Communications* **5**, 3658.
- Bell, J S (1964), “On the einstein podolsky rosen paradox,” *Physics Physique Fizika* **1**, 195–200.
- Bell, Tom J, Love A Pettersson, and Stefano Paesani (2022), “Optimising graph codes for measurement-based loss tolerance,” arXiv preprint arXiv:2212.04834.
- Ben-Or, Michael, and Avinatan Hassidim (2005), “Fast quantum byzantine agreement,” in *Proceedings of the thirty-seventh annual ACM symposium on Theory of computing*, pp. 481–485.

- Bennett, C H, and G. Brassard (1984), “Quantum cryptography: Public key distribution and coin tossing,” in *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing* (India) pp. 175–179.
- Bennett, C H, G. Brassard, C. Crepeau, R. Jozsa, A. Peres, and W. K. Wootters (1993), “Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels,” *Phys. Rev. Lett.* **70** (13), 1895.
- Bennett, C H, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters (1996a), “Purification of noisy entanglement and faithful teleportation via noisy channels,” *Phys. Rev. Lett.* **76** (5), 722–725.
- Bennett, Charles H, Herbert J. Bernstein, Sandu Popescu, and Benjamin Schumacher (1996b), “Concentrating partial entanglement by local operations,” *Physical Review A* **53** (4), 2046.
- Bennett, Charles H, and Gilles Brassard (2014), “Quantum cryptography: Public key distribution and coin tossing,” *Theoretical Computer Science* **560** (P1), 7–11.
- Bennett, Charles H, Gilles Brassard, and N. David Mermin (1992), “Quantum cryptography without Bell’s theorem,” *Phys. Rev. Lett.* **68** (5), 557–559.
- Bennett, Charles H, David P DiVincenzo, and John A Smolin (1997), “Capacities of quantum erasure channels,” *Phys. Rev. Lett.* **78** (16), 3217.
- Bennett, Charles H, David P. DiVincenzo, John A. Smolin, and William K. Wootters (1996c), “Mixed-state entanglement and quantum error correction,” *Phys. Rev. A* **54**, 3824–3851.
- Benyoucef, M, M. Yacob, J. P. Reithmaier, J. Kettler, and P. Michler (2013), “Telecom-wavelength (1.5 μ m) single-photon emission from inp-based quantum dots,” *Applied Physics Letters* **103** (16), 162101.
- Bergeron, L, C. Chartrand, A. T. K. Kurkjian, K. J. Morse, H. Riemann, N. V. Abrosimov, P. Becker, H.-J. Pohl, M. L. W. Thewalt, and S. Simmons (2020), “Silicon-integrated telecommunications photon-spin interface,” *PRX Quantum* **1** (2), 020301.
- Bernien, Hannes, Bas Hensen, Wolfgang Pfaff, Gerwin Koolstra, M. S. Blok, Lucio Robledo, T. H. Taminiau, Matthew Markham, D. J. Twitchen, Lilian Childress, *et al.* (2013), “Heralded entanglement between solid-state qubits separated by three metres,” *Nature* **497** (7447), 86–90.
- Berry, Michael (1998), *Introduction to Quantum Computation and Information*, edited by Hoi-Kwong Lo, Sandu Popescu, and Tim Spiller (World Scientific).
- Bhaskar, Mihir K, Ralf Riedinger, Bartholomeus Machielse, David S Levonian, Christian T Nguyen, Erik N Knall, Hongkun Park, Dirk Englund, Marko Lončar, Denis D Sukachev, *et al.* (2020), “Experimental demonstration of memory-enhanced quantum communication,” *Nature* **580** (7801), 60–64.
- Biham, Eli, Bruno Huttner, and Tal Mor (1996), “Quantum cryptographic network based on quantum memories,” *Physical Review A* **54** (4), 2651.
- Blinov, B B, D. L. Moehring, L.-M. Duan, and Chris Monroe (2004), “Observation of entanglement between a single trapped atom and a single photon,” *Nature* **428** (6979), 153–157.
- Bloch, Matthieu, João Barros, Miguel RD Rodrigues, and Steven W McLaughlin (2008), “Wireless information-theoretic security,” *IEEE Transactions on Information Theory* **54** (6), 2515–2534.
- Boaron, Alberto, Gianluca Boso, Davide Rusca, Cédric Vuliez, Claire Autebert, Misael Caloz, Matthieu Perrenoud, Gaëtan Gras, Félix Bussièeres, Ming-Jun Li, *et al.* (2018), “Secure quantum key distribution over 421 km of optical fiber,” *Phys. Rev. Lett.* **121** (19), 190502.
- Bock, Matthias, Pascal Eich, Stephan Kucera, Matthias Kreis, Andreas Lenhard, Christoph Becher, and Jürgen Eschner (2018), “High-fidelity entanglement between a trapped ion and a telecom photon via quantum frequency conversion,” *Nature communications* **9** (1), 1998.
- Bonarota, M, J. L. Le Gouët, and T. Chanelière (2011), “Highly multimode storage in a crystal,” *New Journal of Physics* **13** (1), 013013.
- Bonneau, Damien, Gabriel J Mendoza, Jeremy L O’Brien, and Mark G Thompson (2015), “Effect of loss on multiplexed single-photon sources,” *New Journal of Physics* **17** (4), 043057.
- Boone, K, J-P Bourgoin, E Meyer-Scott, K Heshami, T Jennewein, and C Simon (2015), “Entanglement over global distances via quantum repeaters with satellite links,” *Physical Review A* **91** (5), 052325.
- Borregaard, J, M. Zugenmaier, J. M. Petersen, H. Shen, G. Vasilakis, K. Jensen, E. S. Polzik, and A. S. Sørensen (2016), “Scalable photonic network architecture based on motional averaging in room temperature gas,” *Nature Communications* **7**, 11356.
- Borregaard, Johannes, Hannes Pichler, Tim Schröder, Mikhail D Lukin, Peter Lodahl, and Anders S Sørensen (2020), “One-way quantum repeater based on near-deterministic photon-emitter interfaces,” *Physical Review X* **10** (2), 021071.
- Bose, S, P. L. Knight, M. B. Plenio, and V. Vedral (1999), “Proposal for teleportation of an atomic state via cavity decay,” *Phys. Rev. Lett.* **83** (24), 5158.
- Bourassa, A, C. P. Anderson, K. C. Miao, M. Onizhuk, H. Ma, A. L. Crook, H. Abe, J. Ul-Hassan, T. Ohshima, N. T. Son, G. Galli, and D. D. Awschalom (2020), “Entanglement and control of single nuclear spins in isotopically engineered silicon carbide,” *Nature Materials* **19**, 1319.
- Bradley, C E, J. Randall, M. H. Abobeih, R. C. Berrevoets, M. J. Degen, M. A. Bakker, M. Markham, D. J. Twitchen, and T. H. Taminiau (2019), “A ten-qubit solid-state spin register with quantum memory up to one minute,” *Phys. Rev. X* **9**, 031045.
- Brassard, Gilles (2003), “Quantum communication complexity,” *Foundations of Physics* **33** (11), 1593–1616.
- Bratzik, S, H. Kampermann, and D. Bruss (2014), “Secret key rates for an encoded quantum repeater,” *Physical Review A (Atomic, Molecular, and Optical Physics)* **89**, 032335.
- Braunstein, Samuel L, and H Jeff Kimble (1998), “Teleportation of continuous quantum variables,” *Phys. Rev. Lett.* **80** (4), 869.
- Briegel, H J, W. Dur, J. I. Cirac, and P. Zoller (1998), “Quantum repeater: The role of imperfect local operations in quantum communication,” *Phys. Rev. Lett.* **81** (26), 5932–5935.
- Briegel, Hans J, and Robert Raussendorf (2001), “Persistent Entanglement in Arrays of Interacting Particles,” *Phys. Rev. Lett.* **86** (5), 910–913.
- Broadbent, Anne, Joseph Fitzsimons, and Elham Kashefi (2009), “Universal blind quantum computation,” in *2009 50th Annual IEEE Symposium on Foundations of Computer Science (IEEE)* pp. 517–526.
- Broadbent, Anne, and Rabib Islam (2020), “Quantum encryption with certified deletion,” in *Theory of Cryptography*

- Conference* (Springer) pp. 92–122.
- Broadbent, Anne, and Christian Schaffner (2016), “Quantum cryptography beyond quantum key distribution,” *Designs, Codes and Cryptography* **78** (1), 351–382.
- Browne, Daniel E, and Terry Rudolph (2005), “Resource-Efficient Linear Optical Quantum Computation,” *Phys. Rev. Lett.* **95** (1), 010501.
- Brune, M, S. Haroche, V. Lefevre, J. M. Raimond, and N. Zagury (1990), “Quantum nondemolition measurement of small photon numbers by rydberg-atom phase-sensitive detection,” *Phys. Rev. Lett.* **65** (8), 976.
- Brunner, Nicolas, Daniel Cavalcanti, Stefano Pironio, Valerio Scarani, and Stephanie Wehner (2014), “Bell nonlocality,” *Rev. Mod. Phys.* **86**, 419–478.
- Buhrman, Harry, Nishanth Chandran, Serge Fehr, Ran Gelles, Vipul Goyal, Rafail Ostrovsky, and Christian Schaffner (2011), “Position-based quantum cryptography: Impossibility and constructions,” in *Advances in Cryptology – CRYPTO 2011*, edited by Phillip Rogaway (Springer Berlin Heidelberg, Berlin, Heidelberg) pp. 429–446.
- Buhrman, Harry, Richard Cleve, John Watrous, and Ronald de Wolf (2001), “Quantum fingerprinting,” *Phys. Rev. Lett.* **87** (16), 167902.
- Buterakos, Donovan, Edwin Barnes, and Sophia E Economou (2017), “Deterministic Generation of All-Photonic Quantum Repeaters from Solid-State Emitters,” *Physical Review X* **7** (4), 041023.
- Cabrillo, C, J. I. Cirac, P. Garcia-Fernandez, and P. Zoller (1999), “Creation of entangled states of distant atoms by interference,” *Physical Review A* **59** (2), 1025.
- Cacciapuoti, Angela Sara, Marcello Caleffi, Francesco Tafuri, Francesco Saverio Cataliotti, Stefano Gherardini, and Giuseppe Bianchi (2019), “Quantum internet: networking challenges in distributed quantum computing,” *IEEE Network* **34** (1), 137–143.
- Cacciapuoti, Angela Sara, Jessica Illiano, Seid Koudia, Kyrylo Simonov, and Marcello Caleffi (2022), “The quantum internet: Enhancing classical internet services one qubit at a time,” *IEEE Network* **36** (5), 6–12.
- Calderbank, A R, and Peter W. Shor (1996), “Good quantum error-correcting codes exist,” *Physical Review A* **54** (2), 1098.
- Calsamiglia, John, and Norbert Lütkenhaus (2001), “Maximum efficiency of a linear-optical bell-state analyzer,” *Applied Physics B* **72** (1), 67–71.
- Cartesian, (2021), “Addressing Gaps in Broadband Infrastructure Availability and Service Adoption,” <https://www.cartesian.com/addressing-gaps-in-broadband-infrastructure-availability-and-service-adoption/>.
- Castelvecchi, Davide (2017), “IBM’s quantum cloud computer goes commercial,” <https://www.nature.com/news/ibm-s-quantum-cloud-computer-goes-commercial-1.21585>.
- Chailloux, André, and Iordanis Kerenidis (2009), “Optimal quantum strong coin flipping,” in *2009 50th Annual IEEE Symposium on Foundations of Computer Science (IEEE)* pp. 527–533.
- Chamberland, Christopher, and Michael E Beverland (2018), “Flag fault-tolerant error correction with arbitrary distance codes,” *Quantum* **2**, 53.
- Chang, J, JWN Los, JO Tenorio-Pearl, Niels Noordzij, R Gourgues, A Guardiani, JR Zichi, SF Pereira, HP Urbach, Val Zwiller, *et al.* (2021), “Detecting telecom single photons with 99.5- 2.07+ 0.5% system detection efficiency and high time resolution,” *APL Photonics* **6** (3), 036114.
- Chao, Rui, and Ben W Reichardt (2018), “Quantum error correction with only two extra qubits,” *Phys. Rev. Lett.* **121** (5), 050502.
- Chen, Jiu-Peng, Chi Zhang, Yang Liu, Cong Jiang, Wei-Jun Zhang, Zhi-Yong Han, Shi-Zhao Ma, Xiao-Long Hu, Yu-Huai Li, Hui Liu, *et al.* (2021a), “Twin-field quantum key distribution over a 511 km optical fibre linking two distant metropolitan areas,” *Nature Photonics* **15**, 570–575.
- Chen, Jiu-Peng, Chi Zhang, Yang Liu, Cong Jiang, Weijun Zhang, Xiao-Long Hu, Jian-Yu Guan, Zong-Wen Yu, Hai Xu, Jin Lin, *et al.* (2020), “Sending-or-not-sending with independent lasers: Secure twin-field quantum key distribution over 509 km,” *Phys. Rev. Lett.* **124** (7), 070501.
- Chen, Kai, and Hoi-Kwong Lo (2007), “Multi-partite quantum cryptographic protocols with noisy ghz states,” *Quantum Information & Computation* **7** (8), 689–715.
- Chen, Shuai, Yu-Ao Chen, Bo Zhao, Zhen-Sheng Yuan, Jörg Schmiedmayer, and Jian-Wei Pan (2007), “Demonstration of a stable atom-photon entanglement source for quantum repeaters,” *Phys. Rev. Lett.* **99** (18), 180505.
- Chen, Yu-Ao, Qiang Zhang, Teng-Yun Chen, Wen-Qi Cai, Sheng-Kai Liao, Jun Zhang, Kai Chen, Juan Yin, Ji-Gang Ren, Zhu Chen, *et al.* (2021b), “An integrated space-to-ground quantum communication network over 4,600 kilometres,” *Nature* **589** (7841), 214–219.
- Childress, L, M. V. Gurudev Dutt, J. M. Taylor, A. S. Zibrov, F. Jelezko, J. Wrachtrup, P. R. Hemmer, and M. D. Lukin (2006a), “Coherent dynamics of coupled electron and nuclear spin qubits in diamond,” *Science* **314** (5797), 281–285.
- Childress, Lilian, J. M. Taylor, Anders Søndberg Sørensen, and M. D. Lukin (2006b), “Fault-tolerant quantum communication based on solid-state photon emitters,” *Phys. Rev. Lett.* **96** (7), 070504.
- Childs, Andrew M (2001), “Secure assisted quantum computation,” arXiv preprint quant-ph/0111046.
- Chou, Chin-Wen, Julien Laurat, Hui Deng, Kyung Soo Choi, Hugues De Riedmatten, Daniel Felinto, and H Jeff Kimble (2007), “Functional quantum nodes for entanglement distribution over scalable quantum networks,” *Science* **316** (5829), 1316–1320.
- Christ, Andreas, and Christine Silberhorn (2012), “Limits on the deterministic creation of pure single-photon states using parametric down-conversion,” *Physical Review A* **85** (2), 023829.
- Christandl, Matthias, and Alexander Müller-Hermes (2017), “Relative entropy bounds on quantum, private and repeater capacities,” *Communications in Mathematical Physics* **353** (2), 821–852.
- Christandl, Matthias, and Stephanie Wehner (2005), “Quantum anonymous transmissions,” in *International Conference on the Theory and Application of Cryptology and Information Security* (Springer) pp. 217–235.
- Christensen, Brad G, Kevin T McCusker, Joseph B Altepeter, Brice Calkins, Thomas Gerrits, Adriana E Lita, Aaron Miller, Lynden K Shalm, Yanbao Zhang, Sae Woo Nam, *et al.* (2013), “Detection-loophole-free test of quantum nonlocality, and applications,” *Phys. Rev. Lett.* **111** (13), 130406.
- Chung, Joaquin, Gregory Kanter, Nikolai Lauk, Raju Valivarthi, Wenji Wu, Russell R Ceballos, Cristián Peña, Neil Sinclair, Jordan Thomas, Si Xie, *et al.* (2021), “Illinois express quantum network (ieqnet): metropolitan-scale exper-

- imental quantum networking over deployed optical fiber,” in *Quantum Information Science, Sensing, and Computation XIII*, Vol. 11726 (SPIE) p. 1172602.
- Clerk, A A, M. H. Devoret, S. M. Girvin, Florian Marquardt, and R. J. Schoelkopf (2010), “Introduction to quantum noise, measurement, and amplification,” *Rev. Mod. Phys.* **82**, 1155–1208.
- Cleve, Richard, and Harry Buhrman (1997), “Substituting quantum entanglement for communication,” *Physical Review A* **56** (2), 1201.
- Cleve, Richard, Daniel Gottesman, and Hoi-Kwong Lo (1999), “How to share a quantum secret,” *Phys. Rev. Lett.* **83** (3), 648.
- Clivati, Cecilia, Alice Meda, Simone Donadello, Salvatore Virzi, Marco Genovese, Filippo Levi, Alberto Mura, Mirko Pittaluga, Zhiliang Yuan, Andrew J Shields, *et al.* (2022), “Coherent phase transfer for real-world twin-field quantum key distribution,” *Nature Communications* **13**, 157.
- Cogan, Dan, Zu-En Su, Oded Kenneth, and David Gershoni (2021), “A deterministic source of indistinguishable photons in a cluster state,” arXiv preprint arXiv:2110.05908.
- Collins, Daniel, Noah Linden, and Sandu Popescu (2001), “Nonlocal content of quantum operations,” *Phys. Rev. A* **64**, 032302.
- Collins, Matthew J, Chunle Xiong, Isabella H Rey, Trung D Vo, Jiakun He, Shayan Shahnia, Christopher Reardon, Thomas F Krauss, MJ Steel, Alex S Clark, *et al.* (2013), “Integrated spatial multiplexing of heralded single-photon sources,” *Nature Communications* **4**, 2582.
- Collins, O A, S D Jenkins, A Kuzmich, and T A B Kennedy (2007), “Multiplexed Memory-Insensitive Quantum Repeaters,” *Phys. Rev. Lett.* **98** (6), 060502.
- Coopmans, Tim, Robert Knegjens, Axel Dahlberg, David Maier, Loek Nijsten, Julio Oliveira, Martijn Papendrecht, Julian Rabbie, Filip Rozpędek, Matthew Skrzypczyk, Leon Wubben, Walter de Jong, Damian Podareanu, Ariana Torres Knoop, David Elkouss, and Stephanie Wehner (2021), “Netsquid, a discrete-event simulation platform for quantum networks,” *Communications Physics* **4**, 164.
- Corning® (2021), “Corning® SMF-28® ULL Optical Fiber Portfolio,” <https://www.corning.com/optical-communications/worldwide/en/home/products/fiber/optical-fiber-products/smf-28-ull.html>.
- Coste, N, D Fioretto, N Belabas, SC Wein, P Hilaire, R Frantzeskakis, M Gundin, B Goes, N Somaschi, M Morassi, *et al.* (2022), “High-rate entanglement between a semiconductor spin and indistinguishable photons,” arXiv preprint arXiv:2207.09881.
- Cramer, J, N. Kalb, M. A. Rol, B. Hensen, M. S. Blok, M. Markham, D. J. Twitchen, R. Hanson, and T. H. Taminiau (2016), “Repeated quantum error correction on a continuously encoded qubit by real-time feedback,” *Nature Communications* **7**, 11526.
- Cui, Chaohan, Zhen-Qiang Yin, Rong Wang, Wei Chen, Shuang Wang, Guang-Can Guo, and Zheng-Fu Han (2019), “Twin-field quantum key distribution without phase post-selection,” *Physical Review Applied* **11** (3), 034053.
- Currás-Lorenzo, Guillermo, Álvaro Navarrete, Koji Azuma, Go Kato, Marcos Curty, and Mohsen Razavi (2021), “Tight finite-key security for twin-field quantum key distribution,” *npj Quantum Information* **7** (1), 10.1038/s41534-020-00345-3.
- Curty, Marcos, Koji Azuma, and Hoi-Kwong Lo (2019), “Simple security proof of twin-field type quantum key distribution protocol,” *npj Quantum Information* **5**, 64.
- Curty, Marcos, Koji Azuma, and Hoi-Kwong Lo (2021), “A quantum leap in security,” *Physics Today* **74** (3), 36.
- Curty, Marcos, and Hoi-Kwong Lo (2019), “Foiling covert channels and malicious classical post-processing units in quantum key distribution,” *npj Quantum Information* **5**, 14.
- Curty, Marcos, and Tobias Moroder (2011), “Heralded-qubit amplifiers for practical device-independent quantum key distribution,” *Phys. Rev. A* **84**, 010304.
- Curty, Marcos, Feihu Xu, Wei Cui, Charles Ci Wen Lim, Kiyoshi Tamaki, and Hoi-Kwong Lo (2014), “Finite-key analysis for measurement-device-independent quantum key distribution,” *Nature Communications* **5**, 3732.
- Dahlberg, Axel, Matthew Skrzypczyk, Tim Coopmans, Leon Wubben, Filip Rozpędek, Matteo Pompili, Arian Stolk, Przemysław Pawełczak, Robert Knegjens, Julio de Oliveira Filho, *et al.* (2019), “A link layer protocol for quantum networks,” in *Proceedings of the ACM Special Interest Group on Data Communication*, pp. 159–173.
- Daiss, Severin, Stefan Langenfeld, Stephan Welte, Emanuele Distanto, Philip Thomas, Lukas Hartung, Olivier Morin, and Gerhard Rempe (2021), “A quantum-logic gate between distant quantum-network modules,” *Science* **371** (6529), 614–617.
- van Dam, Kleese K (2020), *From Long-distance Entanglement to Building a Nationwide Quantum Internet: Report of the DOE Quantum Internet Blueprint Workshop*, Tech. Rep. (Brookhaven National Laboratory, Upton).
- Damgård, Ivan B, Serge Fehr, Louis Salvail, and Christian Schaffner (2007), “Secure identification and qkd in the bounded-quantum-storage model,” in *Annual International Cryptology Conference* (Springer) pp. 342–359.
- Damgård, Ivan B, Serge Fehr, Louis Salvail, and Christian Schaffner (2008), “Cryptography in the bounded-quantum-storage model,” *SIAM Journal on Computing* **37** (6), 1865–1890.
- De Greve, Kristiaan, Peter L McMahon, David Press, Thaddeus D Ladd, Dirk Bisping, Christian Schneider, Martin Kamp, Lukas Worschech, Sven Höfling, Alfred Forchel, *et al.* (2011), “Ultrafast coherent control and suppressed nuclear feedback of a single quantum dot hole qubit,” *Nature Physics* **7** (11), 872–878.
- De Greve, Kristiaan, Leo Yu, Peter L. McMahon, Jason S Pelc, Chandra M Natarajan, Na Young Kim, Eisuke Abe, Sebastian Maier, Christian Schneider, Martin Kamp, Sven Höfling, Robert H Hadfield, Alfred Forchel, M M Fejer, and Yoshihisa Yamamoto (2012), “Quantum-dot spin-photon entanglement via frequency downconversion to telecom wavelength,” *Nature* **491** (7424), 421–425.
- Degen, C L, F. Reinhard, and P. Cappellaro (2017), “Quantum sensing,” *Rev. Mod. Phys.* **89**, 035002.
- Delteil, Aymeric, Zhe Sun, Wei-bo Gao, Emre Togan, Stefan Faelt, and Atac Imamoglu (2015), “Generation of heralded entanglement between distant hole spins,” *Nature Physics* **12**, 218–223.
- Deutsch, David, Artur Ekert, Richard Jozsa, Chiara Macchiavello, Sandu Popescu, and Anna Sanpera (1996), “Quantum privacy amplification and the security of quantum cryptography over noisy channels,” *Phys. Rev. Lett.* **77** (13), 2818–2821.
- Devetak, Igor (2005), “The private classical capacity and quantum capacity of a quantum channel,” *IEEE Transactions on Information Theory* **51** (1), 44–55.

- Devitt, Simon J, Andrew D. Greentree, Ashley M. Stephens, and Rodney Van Meter (2016), “High-speed quantum networking by ship,” *Scientific Reports* **6**, 36163.
- Dias, Josephine, and T. C. Ralph (2017), “Quantum repeaters using continuous-variable teleportation,” *Physical Review A* **95** (2), 022312.
- Dideriksen, Karsten B, Rebecca Schmieg, Michael Zugemaier, and Eugene S. Polzik (2021), “Room-temperature single-photon source with near-millisecond built-in memory,” *Nature Communications* **12**, 3699.
- Dieks, D (1982), “Communication by EPR devices,” *Physics Letters A* **92** (6), 271–272.
- Dowling, Jonathan P, and Gerard J. Milburn (2003), “Quantum technology: the second quantum revolution,” *Philosophical Transactions of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences* **361** (1809), 1655–1674.
- Duan, L-M, M. D. Lukin, J. I. Cirac, and P. Zoller (2001), “Long-distance quantum communication with atomic ensembles and linear optics,” *Nature* **414** (6862), 413–418.
- Dudin, YO, L Li, and A Kuzmich (2013), “Light storage on the time scale of a minute,” *Physical Review A* **87** (3), 031801.
- Dudin, YO, AG Radnaev, Ran Zhao, JZ Blumoff, TAB Kennedy, and Alex Kuzmich (2010), “Entanglement of light-shift compensated atomic spin waves with telecom light,” *Phys. Rev. Lett.* **105** (26), 260502.
- Dupuis, Frederic, Omar Fawzi, and Stephanie Wehner (2014), “Entanglement sampling and applications,” *IEEE Transactions on Information Theory* **61** (2), 1093–1112.
- Dür, W, H.-J. Briegel, J. I. Cirac, and P. Zoller (1999), “Quantum repeaters based on entanglement purification,” *Phys. Rev. A* **59**, 169–181.
- Dür, W, G. Vidal, and J. I. Cirac (2000), “Three qubits can be entangled in two inequivalent ways,” *Phys. Rev. A* **62**, 062314.
- Durand, Alrik, Yoann Baron, Walid Redjem, T Herzig, A Benali, S Pezzagna, J Meijer, A Yu Kuznetsov, J-M Gérard, I Robert-Philip, *et al.* (2021), “Broad diversity of near-infrared single-photon emitters in silicon,” *Phys. Rev. Lett.* **126** (8), 083602.
- Dür, W, and H. J. Briegel (2007), “Entanglement purification and quantum error correction,” *Reports on Progress in Physics* **70** (8), 1381–1424.
- Eberhard, Phillippe H, and Ronald R. Ross (1989), “Quantum field theory cannot provide faster-than-light communication,” *Foundations of Physics Letters* **2** (2), 127–149.
- Ebert, M, M. Kwon, T. G. Walker, and M. Saffman (2015), “Coherence and rydberg blockade of atomic ensemble qubits,” *Phys. Rev. Lett.* **115** (9), 093601.
- Economou, Sophia E, Netanel Lindner, and Terry Rudolph (2010), “Optically Generated 2-Dimensional Photonic Cluster State from Coupled Quantum Dots,” *Phys. Rev. Lett.* **105** (9), 093601.
- Egan, Laird, Dripto M Debroy, Crystal Noel, Andrew Risinger, Daiwei Zhu, Debopriyo Biswas, Michael Newman, Muyuan Li, Kenneth R Brown, Marko Cetina, *et al.* (2020), “Fault-tolerant operation of a quantum error-correction code,” arXiv preprint arXiv:2009.11482.
- Einstein, A, B. Podolsky, and N. Rosen (1935), “Can quantum-mechanical description of physical reality be considered complete?” *Physical Review* **47** (10), 777–780.
- Eisaman, M D, J. Fan, A. Migdall, and S. V. Polyakov (2011), “Invited Review Article: Single-photon sources and detectors,” *Review of Scientific Instruments* **82** (7), 071101.
- Eisert, J, K. Jacobs, P. Papadopoulos, and M. B. Plenio (2000), “Optimal local implementation of nonlocal quantum gates,” *Phys. Rev. A* **62**, 052317.
- Eisert, J, S. Scheel, and M. B. Plenio (2002), “Distilling gaussian states with gaussian operations is impossible,” *Physical Review Letters* **89** (13), 137903.
- Ekert, Artur K (1991), “Quantum cryptography based on Bell’s theorem,” *Phys. Rev. Lett.* **67** (6), 661–663.
- Éthier-Majcher, G, D. Gangloff, R. Stockill, E. Clarke, M. Hugues, C. Le Gall, and M. Atatüre (2017), “Improving a solid-state qubit through an engineered mesoscopic environment,” *Phys. Rev. Lett.* **119** (13), 130503.
- Ewert, Fabian, Marcel Bergmann, and Peter van Loock (2016), “Ultrafast long-distance quantum communication with static linear optics,” *Phys. Rev. Lett.* **117** (21), 10.1103/PhysRevLett.117.210501.
- Ewert, Fabian, and Peter van Loock (2014), “3/4 -efficient bell measurement with passive linear optics and unentangled ancillae,” *Phys. Rev. Lett.* **113** (14), 10.1103/PhysRevLett.113.140403.
- Ewert, Fabian, and Peter van Loock (2017), “Ultrafast fault-tolerant long-distance quantum communication with static linear optics,” *Physical Review A* **95** (1), 12327.
- Fern, Jesse, and K Birgitta Whaley (2008), “Lower bounds on the nonzero capacity of pauli channels,” *Physical Review A* **78** (6), 062335.
- Fitzsimons, Joseph F (2017), “Private quantum computation: an introduction to blind quantum computing and related protocols,” *npj Quantum Information* **3**, 23.
- Fiurášek, Jaromír (2002), “Gaussian transformations and distillation of entangled gaussian states,” *Physical Review Letters* **89** (13), 137904.
- Fiurášek, Jaromír (2010), “Distillation and purification of symmetric entangled gaussian states,” *Physical Review A* **82** (4), 042331.
- Fowler, A G, D. S. Wang, C. D. Hill, T. D. Ladd, R. Van Meter, and L. C. L. Hollenberg (2010), “Surface code quantum communication,” *Phys. Rev. Lett.* **104** (18), 180503.
- Fuchs, G D, Guido Burkard, P. V. Klimov, and D. D. Awschalom (2011), “A quantum memory intrinsic to single nitrogen-vacancy centres in diamond,” *Nature Physics* **7** (10), 789–793.
- Fujii, Keisuke, and Katsuji Yamamoto (2009), “Entanglement purification with double selection,” *Physical Review A* **80** (4), 042308.
- Fukui, Kosuke, Rafael N. Alexander, and Peter van Loock (2021), “All-optical long-distance quantum communication with Gottesman-Kitaev-Preskill qubits,” *Phys. Rev. Research* **3**, 033118.
- Fukui, Kosuke, Akihisa Tomita, and Atsushi Okamoto (2017), “Analog Quantum Error Correction with Encoding a Qubit into an Oscillator,” *Phys. Rev. Lett.* **119** (18), 180507.
- Furrer, Fabian, and William J. Munro (2018), “Repeaters for continuous-variable quantum communication,” *Physical Review A* **98** (3), 032335.
- Gangloff, D A, G. Ethier-Majcher, C. Lang, E. V. Denning, J. H. Bodey, D. M. Jackson, E. Clarke, M. Hugues, C. Le Gall, and M. Atatüre (2019), “Quantum interface of an electron and a nuclear ensemble,” *Science* **364**, 62.
- Gao, WB, Parisa Fallahi, Emre Togan, Javier Miguel-Sánchez, and Atac Imamoglu (2012), “Observation of entanglement between a quantum dot spin and a single photon,” *Nature* **491** (7424), 426–430.

- Gavinsky, Dmitry (2012), “Quantum money with classical verification,” in *2012 IEEE 27th Conference on Computational Complexity* (IEEE) pp. 42–52.
- Giedke, G, and J. I. Cirac (2002), “Characterization of gaussian operations and distillation of gaussian states,” *Physical Review A* **66** (3), 032316.
- Gimeno-Segovia, Mercedes (2016), *Towards practical linear optical quantum computing*, Ph.D. thesis.
- Gimeno-Segovia, Mercedes, Terry Rudolph, and Sophia E Economou (2019), “Deterministic Generation of Large-Scale Entangled Photonic Cluster State from Interacting Solid State Emitters,” *Phys. Rev. Lett.* **123** (7), 10.1103/PhysRevLett.123.070501.
- Giovannetti, Vittorio, Seth Lloyd, Lorenzo Maccone, and Peter W Shor (2003a), “Broadband channel capacities,” *Physical Review A* **68** (6), 062323.
- Giovannetti, Vittorio, Seth Lloyd, Lorenzo Maccone, and Peter W Shor (2003b), “Entanglement assisted capacity of the broadband lossy channel,” *Phys. Rev. Lett.* **91** (4), 047901.
- Gisin, Nicolas, Stefano Pironio, and Nicolas Sangouard (2010), “Proposal for implementing device-independent quantum key distribution based on a heralded qubit amplifier,” *Phys. Rev. Lett.* **105**, 070501.
- Giustina, Marissa, Alexandra Mech, Sven Ramelow, Bernhard Wittmann, Johannes Kofler, Jörn Beyer, Adriana Lita, Brice Calkins, Thomas Gerrits, Sae Woo Nam, *et al.* (2013), “Bell violation using entangled photons without the fair-sampling assumption,” *Nature* **497** (7448), 227–230.
- Google, Quantum AI (2023), “Suppressing quantum errors by scaling a surface code logical qubit,” *Nature* **614**, 676–681.
- Görlitz, Johannes, Dennis Herrmann, Gergő Thiering, Philipp Fuchs, Morgane Gandil, Takayuki Iwasaki, Takashi Taniguchi, Michael Kieschnick, Jan Meijer, Mutsuko Hatano, *et al.* (2020), “Spectroscopic investigations of negatively charged tin-vacancy centres in diamond,” *New Journal of Physics* **22** (1), 013048.
- Gottesman, Daniel (1997), *Stabilizer Codes and Quantum Error Correction*, Ph.D. thesis.
- Gottesman, Daniel (1999), “The heisenberg representation of quantum computers,” in *Group22: Proceedings of the XXII International Colloquium on Group Theoretical Methods in Physics*, edited by S. P. Corney, R. Delbourgo, and P. D. Jarvis (International Press, Cambridge, MA) pp. 32–43.
- Gottesman, Daniel, and Isaac L. Chuang (1999), “Demonstrating the viability of universal quantum computation using teleportation and single-qubit operations,” *Nature* **402**, 390.
- Gottesman, Daniel, Thomas Jennewein, and Sarah Croke (2012), “Longer-baseline telescopes using quantum repeaters,” *Phys. Rev. Lett.* **109** (7), 070503.
- Gottesman, Daniel, Alexei Kitaev, and John Preskill (2000), “Encoding a qubit in an oscillator,” *Physical Review A* **64** (1), 12310.
- Grelich, A, A. Shabaev, D. R. Yakovlev, Al. L. Efros, I. A. Yugova, D. Reuter, A. D. Wieck, and M. Bayer (2007), “Nuclei-induced frequency focusing of electron spin coherence,” *Science* **317** (5846), 1896–1899.
- Grice, W P (2011), “Arbitrarily complete Bell-state measurement using only linear optical elements,” *Physical Review A* **84** (4), 042331.
- Grosshans, Frederic, and Nicolas J. Cerf (2004), “Continuous-variable quantum cryptography is secure against non-gaussian attacks,” *Physical Review Letters* **92** (4), 047905–4.
- Guha, Saikat (2011), “Structured optical receivers to attain superadditive capacity and the holevo limit,” *Phys. Rev. Lett.* **106** (24), 240502.
- Gündoğan, Mustafa, Jasminder S Sidhu, Victoria Henderson, Luca Mazzarella, Janik Wolters, Daniel KL Oi, and Markus Krutzik (2021), “Proposal for space-borne quantum memories for global quantum networking,” *npj Quantum Information* **7** (1), 128.
- Gurudev Dutt, M V, Jun Cheng, Yanwen Wu, Xiaodong Xu, D. G. Steel, A. S. Bracker, D. Gammon, Sophia E. Economou, Ren-Bao Liu, and L. J. Sham (2006), “Ultrafast optical control of electron spin coherence in charged GaAs quantum dots,” *Phys. Rev. B* **74**, 125306.
- Hadfield, R H (2009), “Single-photon detectors for optical quantum information applications,” *Nature Photonics* **3** (12), 696–705.
- Hasegawa, Yasushi, Rikizo Ikuta, Nobuyuki Matsuda, Kiyoshi Tamaki, Hoi-Kwong Lo, Takashi Yamamoto, Koji Azuma, and Nobuyuki Imoto (2019), “Experimental time-reversed adaptive Bell measurement towards all-photonic quantum repeaters,” *Nature Communications* **10** (1), 378.
- Hastings, Matthew B (2009), “Superadditivity of communication capacity using entangled inputs,” *Nature Physics* **5** (4), 255–257.
- Hein, M, J. Eisert, and H. J. Briegel (2004), “Multiparty entanglement in graph states,” *Physical Review A* **69** (6), 062311.
- Hein, Marc, Wolfgang Dür, Jens Eisert, Robert Raussendorf, M. Nest, and H-J Briegel (2006), “Entanglement in graph states and its applications,” arXiv preprint quant-ph/0602096.
- Hensen, B, H. Bernien, A. E. Dreaú, A. Reiserer, N. Kalb, M. S. Blok, J. Ruitenbergh, R. F.L. Vermeulen, R. N. Schouten, C. Abellán, W. Amaya, V. Pruneri, M. W. Mitchell, M. Markham, D. J. Twitchen, D. Elkouss, S. Wehner, T. H. Taminiau, and R. Hanson (2015), “Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres,” *Nature* **526** (7575), 682–686.
- Hermans, S L N, M. Pompili, H. K. C. Beukers, S. Baier, J. Borregaard, and R. Hanson (2022), “Qubit teleportation between non-neighbouring nodes in a quantum network,” *Nature* **605** (7911), 663–668.
- Herrera-Martí, David A, Austin G. Fowler, David Jennings, and Terry Rudolph (2010), “Photonic implementation for the topological cluster-state quantum computer,” *Physical Review A* **82** (3), 032332.
- Heshami, Khabat, Duncan G. England, Peter C. Humphreys, Philip J. Bustard, Victor M. Acosta, Joshua Nunn, and Benjamin J. Sussman (2016), “Quantum memories: emerging applications and recent advances,” *Journal of Modern Optics* **63** (20), 2005–2028, pMID: 27695198, <https://doi.org/10.1080/09500340.2016.1148212>.
- Hilaire, Paul, Edwin Barnes, and Sophia E. Economou (2021a), “Resource requirements for efficient quantum communication using all-photonic graph states generated from a few matter qubits,” *Quantum* **5**, 397.
- Hilaire, Paul, Edwin Barnes, Sophia E Economou, and Frédéric Grosshans (2021b), “Error-correcting entanglement swapping using a practical logical photon encoding,” *Physical Review A* **104** (5), 052623.
- Hilaire, Paul, Yaron Castor, Edwin Barnes, Sophia E Economou, and Frédéric Grosshans (2023), “Linear optical logical bell state measurements with optimal loss-tolerance threshold,” arXiv preprint arXiv:2302.07908.

- Hilaire, Paul, Leonid Vidro, Hagai S. Eisenberg, and Sophia E. Economou (2022), “Near-deterministic hybrid generation of arbitrary photonic graph states using a single quantum emitter and linear optics,” arXiv preprint arXiv:2205.09750.
- Hillery, Mark, Vladimír Bužek, and André Berthiaume (1999), “Quantum secret sharing,” *Physical Review A* **59** (3), 1829.
- Horgan, John (2016), “Is the Gravitational-Wave Claim True? And Was It Worth the Cost?” <https://blogs.scientificamerican.com/cross-check/is-the-gravitational-wave-claim-true-and-was-it-worth-the-cost>.
- Horodecki, Karol, Michał Horodecki, Paweł Horodecki, and Jonathan Oppenheim (2005), “Secure key from bound entanglement,” *Phys. Rev. Lett.* **94** (16), 160502.
- Horodecki, Michał, Paweł Horodecki, and Ryszard Horodecki (1999), “General teleportation channel, singlet fraction, and quasidistillation,” *Physical Review A* **60** (3), 1888.
- Horodecki, Ryszard, Paweł Horodecki, Michał Horodecki, and Karol Horodecki (2009), “Quantum entanglement,” *Rev. Mod. Phys.* **81**, 865–942.
- Hosseini, Mahdi, Ben M. Sparkes, Geoff Campbell, Ping K. Lam, and Ben C. Buchler (2011), “High efficiency coherent optical memory with warm rubidium vapour,” *Nature Communications* **2**, 174.
- Howarth, Josh (2021), “80+ Amazing IoT Statistics (2022-2030),” <https://explodingtopics.com/blog/iot-stats>.
- Hu, Peng, Hao Li, Lixing You, Heqing Wang, You Xiao, Jia Huang, Xiaoyan Yang, Weijun Zhang, Zhen Wang, and Xiaoming Xie (2020a), “Detecting single infrared photons toward optimal system detection efficiency,” *Optics Express* **28** (24), 36884–36891.
- Hu, Xiao-Min, Chao Zhang, Bi-Heng Liu, Yu Cai, Xiang-Jun Ye, Yu Guo, Wen-Bo Xing, Cen-Xiao Huang, Yun-Feng Huang, Chuan-Feng Li, and Guang-Can Guo (2020b), “Experimental high-dimensional quantum teleportation,” *Phys. Rev. Lett.* **125**, 230501.
- Hucul, David, Ismail V Inlek, Grahame Vittorini, Clayton Crocker, Shantanu Debnath, Susan M Clark, and Christopher Monroe (2015), “Modular entanglement of atomic qubits using photons and phonons,” *Nature Physics* **11** (1), 37–42.
- Humphreys, Peter C, Norbert Kalb, Jaco PJ Morits, Raymond N Schouten, Raymond FL Vermeulen, Daniel J Twitchen, Matthew Markham, and Ronald Hanson (2018), “Deterministic delivery of remote entanglement on a quantum network,” *Nature* **558** (7709), 268–273.
- Hwang, Won-Young (2003), “Quantum key distribution with high loss: toward global secure communication,” *Phys. Rev. Lett.* **91** (5), 057901.
- Ikuta, Rikizo, Toshiki Kobayashi, Tetsuo Kawakami, Shigehito Miki, Masahiro Yabuno, Taro Yamashita, Hirohito Terai, Masato Koashi, Tetsuya Mukai, Takashi Yamamoto, *et al.* (2018), “Polarization insensitive frequency conversion for an atom-photon entanglement distribution via a telecom network,” *Nature Communications* **9**, 1997.
- Ikuta, Rikizo, Yoshiaki Kusaka, Tsuyoshi Kitano, Hiroshi Kato, Takashi Yamamoto, Masato Koashi, and Nobuyuki Imoto (2011), “Wide-band quantum interface for visible-to-telecommunication wavelength conversion,” *Nature Communications* **2**, 537.
- Illiano, Jessica, Marcello Caleffi, Antonio Manzalini, and Angela Sara Cacciapuoti (2022), “Quantum internet protocol stack: A comprehensive survey,” *Computer Networks*, 109092.
- Imoto, N, H. A. Haus, and Y. Yamamoto (1985), “Quantum nondemolition measurement of the photon number via the optical kerr effect,” *Physical Review A* **32** (4), 2287.
- Inlek, Ismail Volkan, Clayton Crocker, Martin Lichtman, Ksenia Sosnova, and Christopher Monroe (2017), “Multispecies trapped-ion node for quantum networking,” *Phys. Rev. Lett.* **118** (25), 250502.
- Inoue, Kyo, Edo Waks, and Yoshihisa Yamamoto (2002), “Differential phase shift quantum key distribution,” *Phys. Rev. Lett.* **89**, 037902.
- Iwasaki, Takayuki, Fumitaka Ishibashi, Yoshiyuki Miyamoto, Yuki Doi, Satoshi Kobayashi, Takehide Miyazaki, Kosuke Tahara, Kay D Jahnke, Lachlan J Rogers, Boris Naydenov, *et al.* (2015), “Germanium-vacancy single color centers in diamond,” *Scientific Reports* **5**, 12882.
- Jackson, Daniel M, Dorian A Gangloff, Jonathan H Bodey, Leon Zaporski, Clara Bachorz, Edmund Clarke, Maxime Hugues, Claire Le Gall, and Mete Atatüre (2021), “Quantum sensing of a coherent single spin excitation in a nuclear ensemble,” *Nature Physics* **17**, 585–590.
- Jacobs, BC, TB Pittman, and JD Franson (2002), “Quantum relays and noise suppression using linear optics,” *Physical Review A* **66** (5), 052307.
- Javadi, Alisa, Dapeng Ding, Martin Hayhurst Appel, Sa-hand Mahmoodian, Matthias Christian Löbl, Immo Söllner, Rüdiger Schott, Camille Papon, Tommaso Pregnolato, Søren Stobbe, *et al.* (2018), “Spin-photon interface and spin-controlled photon switching in a nanobeam waveguide,” *Nature Nanotechnology* **13** (5), 398–403.
- Ji, Jia-Wei, Yu-Feng Wu, Stephen C Wein, Faezeh Kimiaee Asadi, Roohollah Ghobadi, and Christoph Simon (2022), “Proposal for room-temperature quantum repeaters with nitrogen-vacancy centers and optomechanics,” *Quantum* **6**, 669.
- Jiang, Cong, Zong-Wen Yu, Xiao-Long Hu, and Xiang-Bin Wang (2019), “Unconditional security of sending or not sending twin-field quantum key distribution with finite pulses,” *Physical Review Applied* **12** (2), 024061.
- Jiang, L, J. M. Taylor, N. Khaneja, and M. D. Lukin (2007a), “Optimal approach to quantum communication algorithms using dynamic programming,” *Proceedings of the National Academy of Sciences of the United States of America* **104**, 17291–17296.
- Jiang, Liang, J. M. Taylor, Kae Nemoto, W. J. Munro, Rodney Van Meter, and M. D. Lukin (2009), “Quantum repeater with encoding,” *Phys. Rev. A* **79**, 032325.
- Jiang, Liang, Jacob M. Taylor, Anders S. Sørensen, and Mikhail D. Lukin (2007b), “Distributed quantum computation based on small quantum registers,” *Phys. Rev. A* **76**, 062323.
- Joo, Jaewoo, Peter L. Knight, Jeremy L. O’Brien, and Terry Rudolph (2007), “One-way quantum computation with four-dimensional photonic qudits,” *Phys. Rev. A* **76**, 052326.
- Jozsa, Richard (1994), “Fidelity for mixed quantum states,” *Journal of Modern Optics* **41** (12), 2315–2323.
- Jozsa, Richard, Daniel S. Abrams, Jonathan P. Dowling, and Colin P. Williams (2000), “Quantum Clock Synchronization Based on Shared Prior Entanglement,” *Phys. Rev. Lett.* **85** (9), 2010–2013.
- Jungnickel, Dieter (2005), *Graphs, networks and algorithms* (Springer).
- Kalb, Norbert, Andreas A. Reiserer, Peter C. Humphreys, Ja-

- cob J. W. Bakermans, Sten J. Kamberling, Naomi H. Nickerson, Simon C. Benjamin, Daniel J. Twitchen, Matthew Markham, and Ronald Hanson (2017), “Entanglement distillation between solid-state quantum network nodes,” *Science* **356** (6341), 928–932.
- Kaneda, Fumihito, and Paul G Kwiat (2019), “High-efficiency single-photon generation via large-scale active time multiplexing,” *Science advances* **5** (10), eaaw8586.
- Katz, Or, and Ofer Firstenberg (2018), “Light storage for one second in room-temperature alkali vapor,” *Nature Communications* **9**, 2074.
- Rozpędek, Filip, Raja Yehia, Kenneth Goodenough, Maximilian Ruf, Peter C. Humphreys, Ronald Hanson, Stephanie Wehner, and David Elkouss (2019), “Near-term quantum-repeater experiments with nitrogen-vacancy centers: Overcoming the limitations of direct transmission,” *Phys. Rev. A* **99**, 052330.
- Kent, Adrian (2011), “Unconditionally secure bit commitment with flying qudits,” *New Journal of Physics* **13** (11), 113015.
- Kent, Adrian, William J. Munro, and Timothy P. Spiller (2011), “Quantum tagging: Authenticating location via quantum information and relativistic signaling constraints,” *Phys. Rev. A* **84**, 012326.
- Khabiboulline, Emil T, Johannes Borregaard, Kristiaan De Greve, and Mikhail D. Lukin (2019), “Optical interferometry with quantum networks,” *Phys. Rev. Lett.* **123** (7), 070504.
- Khatri, Sumeet, Anthony J Brady, Renée A Desporte, Manon P Bart, and Jonathan P Dowling (2021), “Spooky action at a global distance: analysis of space-based entanglement distribution for the quantum internet,” *npj Quantum Information* **7** (1), 4.
- Kilmer, Thomas, and Saikat Guha (2019), “Boosting linear-optical Bell measurement success probability with pre-detection squeezing and imperfect photon-number-resolving detectors,” *Physical Review A* **99** (3), 32302.
- Kimble, H J (2008), “The quantum internet,” *Nature* **453** (7198), 1023–1030.
- Kimiaee Asadi, F, N. Lauk, S. Wein, N. Sinclair, C. O’Brien, and C. Simon (2018), “Quantum repeaters with individual rare-earth ions at telecommunication wavelengths,” *Quantum* **2**, 93.
- Knill, E, R. Laflamme, and G. J. Milburn (2001a), “A scheme for efficient quantum computation with linear optics,” *Nature* **409** (6816), 46–52.
- Knill, Emanuel, and Raymond Laflamme (1996), “Concatenated quantum codes,” arXiv preprint quant-ph/9608012.
- Knill, Emanuel, and Raymond Laflamme (1997), “Theory of quantum error-correcting codes,” *Physical Review A* **55** (2), 900.
- Knill, Emanuel, Raymond Laflamme, and Gerald J. Milburn (2001b), “A scheme for efficient quantum computation with linear optics,” *Nature* **409** (6816), 46–52.
- Koashi, M (2009), “Simple security proof of quantum key distribution based on complementarity,” *New Journal of Physics* **11** (4), 045018.
- Koashi, Masato, and Nobuyuki Imoto (1998), “No-cloning theorem of entangled states,” *Phys. Rev. Lett.* **81**, 4264–4267.
- Koashi, Masato, and Nobuyuki Imoto (2002), “Operations that do not disturb partially known quantum states,” *Phys. Rev. A* **66**, 022318.
- Kok, Pieter, W. J. Munro, Kae Nemoto, T. C. Ralph, Jonathan P. Dowling, and G. J. Milburn (2007), “Linear optical quantum computing with photonic qubits,” *Rev. Mod. Phys.* **79**, 135–174.
- Kok, Pieter, Colin P. Williams, and Jonathan P. Dowling (2003), “Construction of a quantum repeater with linear optics,” *Physical Review A* **68** (2), 022301.
- Komar, Peter, Eric M Kessler, Michael Bishof, Liang Jiang, Anders S Sørensen, Jun Ye, and Mikhail D Lukin (2014), “A quantum network of clocks,” *Nature Physics* **10** (8), 582–587.
- Konig, Robert, Stephanie Wehner, and Jürg Wullschlegler (2012), “Unconditional security from noisy quantum storage,” *IEEE Transactions on Information Theory* **58** (3), 1962–1984.
- Kozłowski, Wojciech, Axel Dahlberg, and Stephanie Wehner (2020a), “Designing a quantum network protocol,” in *Proceedings of the 16th international conference on emerging networking experiments and technologies*, pp. 1–16.
- Kozłowski, Wojciech, Stephanie Wehner, RV Meter, Bruno Rijsman, Angela Sara Cacciapuoti, Marcello Caleffi, and Shota Nagayama (2020b), “Architectural principles for a quantum internet,” Internet Engineering Task Force, Internet-Draft draft-irtfqing-principles-03.
- Krastanov, Stefan, Victor V. Albert, and Liang Jiang (2019), “Optimized entanglement purification,” *Quantum* **3**, 123.
- Krutyskiy, V, M Meraner, J Schupp, V Krcmarsky, H Hainzer, and BP Lanyon (2019), “Light-matter entanglement over 50 km of optical fibre,” *npj Quantum Information* **5** (1), 72.
- Krutyskiy, Victor, Marco Canteri, Martin Meraner, James Bate, Vojtech Krcmarsky, Josef Schupp, Nicolas Sangouard, and Ben P Lanyon (2022), “A telecom-wavelength quantum repeater node based on a trapped-ion processor,” arXiv preprint arXiv:2210.05418.
- Kurkjian, A T K, D. B. Higginbottom, C. Chartrand, E. R. MacQuarrie, J. R. Klein, N. R. Lee-Hone, J. Stacho, C. Bowness, L. Bergeron, A. DeAbreu, *et al.* (2021), “Optical observation of single spins in silicon,” arXiv preprint arXiv:2103.07580.
- Lago-Rivera, Dario, Samuele Grandi, Jelena V Rakonjac, Alessandro Seri, and Hugues de Riedmatten (2021), “Telecom-heralded entanglement between multimode solid-state quantum memories,” *Nature* **594** (7861), 37–40.
- Langenfeld, Stefan, Olivier Morin, Matthias Körber, and Gerhard Rempe (2020), “A network-ready random-access qubits memory,” *npj Quantum Information* **6**, 86.
- Langenfeld, Stefan, Philip Thomas, Olivier Morin, and Gerhard Rempe (2021), “Quantum repeater node demonstrating unconditionally secure key distribution,” *Phys. Rev. Lett.* **126** (23), 230506.
- Lau, Hoi-Kwan, and Hoi-Kwong Lo (2011), “Insecurity of position-based quantum-cryptography protocols against entanglement attacks,” *Phys. Rev. A* **83**, 012322.
- Lauk, Nikolai, Neil Sinclair, Shabir Barzanjeh, Jacob P. Covey, Mark Saffman, Maria Spiropulu, and Christoph Simon (2020), “Perspectives on quantum transduction,” *Quantum Science and Technology* **5** (2), 020501.
- Le Gall, François, Harumichi Nishimura, and Ansis Rosmanis (2019), “Quantum advantage for the local model in distributed computing,” in *36th International Symposium on Theoretical Aspects of Computer Science (STACS 2019)* (Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik).
- Lee, J P, B. Villa, A. J. Bennett, R. M. Stevenson, D. J. P. Ellis, I. Farrer, D. A. Ritchie, and A. J. Shields (2019a), “A quantum dot as a source of time-bin entangled multi-

- photon states,” *Quantum Science and Technology* **4** (2), 25011.
- Lee, J P, L. M. Wells, B. Villa, S. Kalliakos, R. M. Stevenson, D. J. P. Ellis, I. Farrer, D. A. Ritchie, A. J. Bennett, and A. J. Shields (2018), “Controllable photonic time-bin qubits from a quantum dot,” *Physical Review X* **8** (2), 021078.
- Lee, Seung-Woo, Timothy C. Ralph, and Hyunseok Jeong (2019b), “Fundamental building block for all-optical scalable quantum networks,” *Physical Review A* **100** (5), 052303.
- van Leent, Tim, Matthias Bock, Florian Fertig, Robert Garthoff, Sebastian Eppelt, Yiru Zhou, Pooja Malik, Matthias Seubert, Tobias Bauer, Wenjamin Rosenfeld, *et al.* (2022), “Entangling single atoms over 33 km telecom fibre,” *Nature* **607** (7917), 69–73.
- van Leent, Tim, Matthias Bock, Robert Garthoff, Kai Recker, Wei Zhang, Tobias Bauer, Wenjamin Rosenfeld, Christoph Becher, and Harald Weinfurter (2020), “Long-distance distribution of atom-photon entanglement at telecom wavelength,” *Phys. Rev. Lett.* **124** (1), 010510.
- Leghtas, Z, G. Kirchmair, B. Vlastakis, R. Schoelkopf, M. Devoret, and M. Mirrahimi (2013), “Hardware-efficient autonomous quantum error correction,” *Phys. Rev. Lett.* **111**, 120501.
- Leon-Garcia, Alberto, and Martha Steenstrup (2021), “The need for holistic network design,” *IEEE Communications Magazine* **59** (8), 4–5.
- Leung, Patrick M, and Timothy C. Ralph (2006), “Quantum memory scheme based on optical fibers and cavities,” *Phys. Rev. A* **74**, 022311.
- Levine, Harry, Alexander Keesling, Giulia Semeghini, Ahmed Omran, Tout T Wang, Sepehr Ebadi, Hannes Bernien, Markus Greiner, Vladan Vuletić, Hannes Pichler, *et al.* (2019), “Parallel implementation of high-fidelity multiqubit gates with neutral atoms,” *Phys. Rev. Lett.* **123** (17), 170503.
- Li, Bikun, Sophia E. Economou, and Edwin Barnes (2021a), “Entangled photon factory: How to generate quantum resource states from a minimal number of quantum emitters,” arXiv preprint arXiv:2108.12466.
- Li, Hang, Jian-Peng Dou, Xiao-Ling Pang, Tian-Huai Yang, Chao-Ni Zhang, Yuan Chen, Jia-Ming Li, Ian A. Walmsley, and Xian-Min Jin (2021b), “Heralding quantum entanglement between two room-temperature atomic ensembles,” *Optica* **8** (6), 925–929.
- Li, Linshu, Chang-Ling Zou, Victor V. Albert, Sreraman Muralidharan, S. M. Girvin, and Liang Jiang (2017), “Cat codes with optimal decoherence suppression for a lossy bosonic channel,” *Phys. Rev. Lett.* **119** (3), 030502.
- Li, Wei, Likang Zhang, Yichen Lu, Zheng-Ping Li, Cong Jiang, Yang Liu, Jia Huang, Hao Li, Zhen Wang, Xiang-Bin Wang, Qiang Zhang, Lixing You, Feihu Xu, and Jian-Wei Pan (2023), “Twin-field quantum key distribution without phase locking,” *Phys. Rev. Lett.* **130**, 250802.
- Li, Ying, Sean D. Barrett, Thomas M. Stace, and Simon C. Benjamin (2013), “Long range failure-tolerant entanglement distribution,” *New Journal of Physics* **15** (2), 023012.
- Li, Ying, Peter C. Humphreys, Gabriel J. Mendoza, and Simon C. Benjamin (2015), “Resource costs for fault-tolerant linear optical quantum computing,” *Physical Review X* **5** (4), 10.1103/PhysRevX.5.041007.
- Li, Zheng-Da, Rui Zhang, Xu-Fei Yin, Li-Zheng Liu, Yi Hu, Yu-Qiang Fang, Yue-Yang Fei, Xiao Jiang, Jun Zhang, Li Li, *et al.* (2019), “Experimental quantum repeater without quantum memory,” *Nature photonics* **13** (9), 644–648.
- Li, Zhuo, Li-Juan Xing, and Xin-Mei Wang (2008), “Quantum generalized reed-solomon codes: Unified framework for quantum maximum-distance-separable codes,” *Physical Review A* **77** (1), 012308.
- Liao, Sheng-Kai, Wen-Qi Cai, Johannes Handsteiner, Bo Liu, Juan Yin, Liang Zhang, Dominik Rauch, Matthias Fink, Ji-Gang Ren, Wei-Yue Liu, *et al.* (2018), “Satellite-relayed intercontinental quantum network,” *Phys. Rev. Lett.* **120** (3), 030501.
- Liao, Sheng-Kai, Wen-Qi Cai, Wei-Yue Liu, Liang Zhang, Yang Li, Ji-Gang Ren, Juan Yin, Qi Shen, Yuan Cao, Zheng-Ping Li, *et al.* (2017), “Satellite-to-ground quantum key distribution,” *Nature* **549** (7670), 43.
- Lidar, Daniel A, and eds. Todd A. Brun (2013), *Quantum Error Correction* (Cambridge University Press).
- Lin, Jie, and Norbert Lütkenhaus (2018), “Simple security analysis of phase-matching measurement-device-independent quantum key distribution,” *Physical Review A* **98** (4), 042332.
- Lindner, Netanel H, and Terry Rudolph (2009), “Proposal for Pulsed On-Demand Sources of Photonic Cluster State Strings,” *Phys. Rev. Lett.* **103** (11), 113602.
- Liorni, Carlo, Hermann Kampermann, and Dagmar Bruß (2021), “Quantum repeaters in space,” *New Journal of Physics* **23** (5), 053021.
- Lita, Adriana E, Aaron J. Miller, and Sae Woo Nam (2008), “Counting near-infrared single-photons with 95% efficiency,” *Optics express* **16** (5), 3032–3040.
- Liu, Xiao, Jun Hu, Zong-Feng Li, Xue Li, Pei-Yun Li, Peng-Jun Liang, Zong-Quan Zhou, Chuan-Feng Li, and Guang-Can Guo (2021), “Heralded entanglement distribution between two absorptive quantum memories,” *Nature* **594** (7861), 41–45.
- Lo, Hoi-Kwong (1997), “Insecurity of quantum secure computations,” *Physical Review A* **56** (2), 1154.
- Lo, Hoi-Kwong (2000), “Classical-communication cost in distributed quantum-information processing: A generalization of quantum-communication complexity,” *Phys. Rev. A* **62**, 012313.
- Lo, Hoi-Kwong, and H. F. Chau (1999), “Unconditional security of quantum key distribution over arbitrarily long distances,” *Science* **283** (5410), 2050–2056.
- Lo, Hoi-Kwong, and Hoi Fung Chau (1997), “Is quantum bit commitment really possible?” *Phys. Rev. Lett.* **78** (17), 3410.
- Lo, Hoi-Kwong, and Hoi Fung Chau (1998), “Why quantum bit commitment and ideal quantum coin tossing are impossible,” *Physica D: Nonlinear Phenomena* **120** (1-2), 177–187.
- Lo, Hoi-Kwong, Marcos Curty, and Bing Qi (2012), “Measurement-device-independent quantum key distribution,” *Phys. Rev. Lett.* **108**, 130503.
- Lo, Hoi-Kwong, Marcos Curty, and Kiyoshi Tamaki (2014), “Secure quantum key distribution,” *Nature Photonics* **8** (8), 595–604.
- Lo, Hoi-Kwong, Xiongfeng Ma, and Kai Chen (2005), “Decoy state quantum key distribution,” *Phys. Rev. Lett.* **94** (23), 230504.
- van Loock, P, T. D. Ladd, K. Sanaka, F. Yamaguchi, Kae Nemoto, W. J. Munro, and Y. Yamamoto (2006), “Hybrid quantum repeater using bright coherent light,” *Phys. Rev. Lett.* **96**, 240501.
- Lucamarini, M, Z. L. Yuan, J. F. Dynes, and A. J. Shields

- (2018), “Overcoming the rate-distance limit of quantum key distribution without quantum repeaters,” *Nature* **557** (7705), 400–403.
- Lukin, Daniil M, Melissa A. Guidry, and Jelena Vučković (2020), “Integrated quantum photonics with silicon carbide: challenges and prospects,” *PRX Quantum* **1** (2), 020102.
- Luo, Yi-Han, Han-Sen Zhong, Manuel Erhard, Xi-Lin Wang, Li-Chao Peng, Mario Krenn, Xiao Jiang, Li Li, Nai-Le Liu, Chao-Yang Lu, Anton Zeilinger, and Jian-Wei Pan (2019), “Quantum teleportation in high dimensions,” *Phys. Rev. Lett.* **123**, 070505.
- Luong, David, Liang Jiang, Jungsang Kim, and Norbert Lütkenhaus (2016), “Overcoming lossy channel bounds using a single quantum repeater node,” *Applied Physics B* **122** (4), 96.
- Lütkenhaus, N, J. Calsamiglia, and K.-A. Suominen (1999), “Bell measurements for teleportation,” *Physical Review A* **59** (5), 3295.
- Lvovsky, Alexander I, Barry C. Sanders, and Wolfgang Tittel (2009), “Optical quantum memory,” *Nature Photonics* **3** (12), 706–714.
- Ma, Xiao-song, Stefan Zotter, Johannes Kofler, Thomas Jennewein, and Anton Zeilinger (2011), “Experimental generation of single photons via active multiplexing,” *Physical Review A* **83** (4), 043814.
- Ma, Xiongfeng, and Mohsen Razavi (2012), “Alternative schemes for measurement-device-independent quantum key distribution,” *Phys. Rev. A* **86**, 062319.
- Ma, Xiongfeng, Pei Zeng, and Hongyi Zhou (2018), “Phase-matching quantum key distribution,” *Physical Review X* **8** (3), 031043.
- Ma, Yu, You-Zhi Ma, Zong-Quan Zhou, Chuan-Feng Li, and Guang-Can Guo (2021), “One-hour coherent optical storage in an atomic frequency comb memory,” *Nature Communications* **12**, 2381.
- Maeda, Kento, Toshihiko Sasaki, and Masato Koashi (2019), “Repeaterless quantum key distribution with efficient finite-key analysis overcoming the rate-distance limit,” *Nature Communications* **10**, 3140.
- Maiwald, Robert, Andrea Golla, Martin Fischer, Marianne Bader, Simon Heugel, Benoît Chalopin, Markus Sondermann, and Gerd Leuchs (2012), “Collecting more than half the fluorescence photons from a single ion,” *Physical Review A* **86** (4), 043431.
- Maring, Nicolas, Pau Farrera, Kutlu Kutluer, Margherita Mazzera, Georg Heinze, and Hugues de Riedmatten (2017), “Photonic quantum state transfer between a cold atomic gas and a crystal,” *Nature* **551** (7681), 485–488.
- Marsili, F, V. B. Verma, J. A. Stern, S. Harrington, A. E. Lita, T. Gerrits, I. Vayshenker, B. Baek, M. D. Shaw, R. P. Mirin, and S. W. Nam (2013), “Detecting single infrared photons with 93% system efficiency,” *Nature Photonics* **7** (3), 210–214.
- Martin, Leigh S, and K. Birgitta Whaley (2019), “Single-shot deterministic entanglement between non-interacting systems with linear optics,” arXiv preprint arXiv:1912.00067.
- Matsuo, Takaaki, Clément Durand, and Rodney Van Meter (2019), “Quantum link bootstrapping using a ruleset-based communication protocol,” *Physical Review A* **100** (5), 052320.
- Matthiesen, Clemens, Martin Geller, Carsten H. H. Schulte, Claire Le Gall, Jack Hansom, Zhengyong Li, Maxime Hugues, Edmund Clarke, and Mete Atatüre (2013), “Phase-locked indistinguishable photons with synthesized waveforms from a solid-state source,” *Nature Communications* **4**, 1600.
- Mayers, Dominic (1997), “Unconditionally secure quantum bit commitment is impossible,” *Phys. Rev. Lett.* **78** (17), 3414.
- Mayers, Dominic (2001), “Unconditional security in quantum cryptography,” *J. ACM* **48** (3), 351–406.
- Mayers, Dominic, and Andrew Yao (1998), “Quantum cryptography with imperfect apparatus,” in *Proceedings 39th Annual Symposium on Foundations of Computer Science (Cat. No. 98CB36280)* (IEEE) pp. 503–509.
- Mazurek, Paweł, Andrzej Grudka, Michał Horodecki, Paweł Horodecki, Justyna Łodyga, Łukasz Pankowski, and Anna Przysiężna (2014), “Long-distance quantum communication over noisy networks without long-time quantum memory,” *Phys. Rev. A* **90**, 062311.
- McGuinness, Hayden J, Michael G. Raymer, Colin J. McKinnis, and Stojan Radic (2010), “Quantum frequency translation of single-photon states in a photonic crystal fiber,” *Phys. Rev. Lett.* **105** (9), 093604.
- Menicucci, Nicolas C, Peter van Loock, Mile Gu, Christian Weedbrook, Timothy C. Ralph, and Michael A. Nielsen (2006), “Universal quantum computation with continuous-variable cluster states,” *Phys. Rev. Lett.* **97** (11), 10.1103/PhysRevLett.97.110501.
- Michael, Marios H, Matti Silveri, R. T. Brierley, Victor V. Albert, Juha Salmilehto, Liang Jiang, and S. M. Girvin (2016), “New class of quantum error-correcting codes for a bosonic mode,” *Physical Review X* **6** (3), 031006.
- Migdall, Alan L, D Branning, and Stefania Castelletto (2002), “Tailoring single-photon and multiphoton probabilities of a single-photon on-demand source,” *Physical Review A* **66** (5), 053805.
- Miller, Johanna L (2016), “Three groups close the loopholes in tests of bell’s theorem,” <https://physicstoday.scitation.org/doi/10.1063/PT.3.3039>.
- Minder, M, M. Pittaluga, G. L. Roberts, M Lucamarini, J. F. Dynes, Z. L. Yuan, and A. J. Shields (2019), “Experimental quantum key distribution beyond the repeaterless secret key capacity,” *Nature Photonics* **13** (5), 334–338.
- Mirhosseini, Mohammad, Alp Sipahigil, Mahmoud Kalaei, and Oskar Painter (2020), “Superconducting qubit to optical photon transduction,” *Nature* **588** (7839), 599–603.
- Mirrahimi, M, Z Leghtas, Victor V. Albert, S. Touzard, R. Schoelkopf, L. Jiang, and M. Devoret (2014), “Dynamically protected cat-qubits: a new paradigm for universal quantum computation,” *New Journal of Physics* **16**, 045014.
- Mochon, Carlos (2007), “Quantum weak coin flipping with arbitrarily small bias,” arXiv preprint arXiv:0711.4114.
- Moehring, David L, Peter Maunz, Steve Olmschenk, Kelly C. Younge, Dzmityry N. Matsukevich, L.-M. Duan, and Christopher Monroe (2007), “Entanglement of single-atom quantum bits at a distance,” *Nature* **449** (7158), 68–71.
- Munro, W J, K. A. Harrison, A. M. Stephens, S. J. Devitt, and Kae Nemoto (2010), “From quantum multiplexing to high-performance quantum networking,” *Nature Photonics* **4**, 792–796.
- Munro, W J, A. M. Stephens, S. J. Devitt, K. A. Harrison, and Kae Nemoto (2012), “Quantum communication without the necessity of quantum memories,” *Nature Photonics* **6** (11), 777–781.
- Munro, W J, R. Van Meter, Sebastien G. R. Louis, and Kae Nemoto (2008), “High-bandwidth hybrid quantum re-

- peater,” *Phys. Rev. Lett.* **101** (4), 040502.
- Munro, William J, Koji Azuma, Kiyoshi Tamaki, and Kae Nemoto (2015), “Inside quantum repeaters,” *IEEE Journal of Selected Topics in Quantum Electronics* **21** (3), 78–90.
- Munro, William J, Nicolo’Lo Piparo, Josephine Dias, Michael Hanks, and Kae Nemoto (2022), “Designing tomorrow’s quantum internet,” *AVS Quantum Science* **4** (2), 020503.
- Muralidharan, Sreraman, Jungsang Kim, Norbert Lütkenhaus, Mikhail D Lukin, and Liang Jiang (2014a), “Ultrafast and fault-tolerant quantum communication across long distances,” *Phys. Rev. Lett.* **112** (25), 250501.
- Muralidharan, Sreraman, Jungsang Kim, Norbert Lütkenhaus, Mikhail D. Lukin, and Liang Jiang (2014b), “Ultrafast and fault-tolerant quantum communication across long distances,” *Phys. Rev. Lett.* **112** (25), 250501.
- Muralidharan, Sreraman, Linshu Li, Jungsang Kim, Norbert Lütkenhaus, Mikhail D. Lukin, and Liang Jiang (2016), “Optimal architectures for long distance quantum communication,” *Scientific Reports* **6** (1), 20463.
- Muralidharan, Sreraman, Chang-Ling Zou, Linshu Li, and Liang Jiang (2018), “One-way quantum repeaters with quantum reed-solomon codes,” *Physical Review A* **97** (5), 052316.
- Muralidharan, Sreraman, Chang-Ling Zou, Linshu Li, Jianming Wen, and Liang Jiang (2017), “Overcoming erasure errors with multilevel systems,” *New Journal of Physics* **19**, 013026.
- Murta, Gláucia, Federico Grasselli, Hermann Kampermann, and Dagmar Bruß (2020), “Quantum conference key agreement: A review,” *Advanced Quantum Technologies* **3** (11), 2000025.
- Nadlinger, DP, P Drmota, BC Nichol, G Araneda, D Main, R Srinivas, DM Lucas, CJ Ballance, K Ivanov, EY-Z Tan, *et al.* (2022), “Experimental quantum key distribution certified by bell’s theorem,” *Nature* **607** (7920), 682–686.
- Neu, Elke, Martin Fischer, Stefan Gsell, Matthias Schreck, and Christoph Becher (2011a), “Fluorescence and polarization spectroscopy of single silicon vacancy centers in heteroepitaxial nanodiamonds on iridium,” *Physical Review B* **84** (20), 205211.
- Neu, Elke, David Steinmetz, Janine Riedrich-Möller, Stefan Gsell, Martin Fischer, Matthias Schreck, and Christoph Becher (2011b), “Single photon emission from silicon-vacancy colour centres in chemical vapour deposition nanodiamonds on iridium,” *New Journal of Physics* **13** (2), 025012.
- Nguyen, C T, D. D. Sukachev, M. K. Bhaskar, B. Machielse, D. S. Levonian, E. N. Knall, P. Stroganov, C. Chia, M. J. Burek, R. Riedinger, H. Park, M. Loncar, and M. D. Lukin (2019a), “An integrated nanophotonic quantum register based on silicon-vacancy spins in diamond,” *Physical Review B* **100**, 165428.
- Nguyen, C T, D. D. Sukachev, M. K. Bhaskar, B. Machielse, D. S. Levonian, E. N. Knall, P. Stroganov, R. Riedinger, H. Park, M. Lončar, *et al.* (2019b), “Quantum network nodes based on diamond qubits with an efficient nanophotonic interface,” *Phys. Rev. Lett.* **123** (18), 183602.
- Nickerson, Naomi H, Joseph F. Fitzsimons, and Simon C. Benjamin (2014), “Freely scalable quantum technologies using cells of 5-to-50 qubits with very lossy and noisy photonic links,” *Physical Review X* **4** (4), 041041.
- Nickerson, Naomi H, Ying Li, and Simon C. Benjamin (2013), “Topological quantum computing with a very noisy network and local error rates approaching one percent,” *Nature Communications* **4**, 1756.
- Nielsen, Michael A (2004), “Optical quantum computation using cluster states,” *Phys. Rev. Lett.* **93** (4), 040503–1.
- Nielsen, Michael A, and Isaac L. Chuang (2010), *Quantum Computation and Quantum Information: 10th Anniversary Edition* (Cambridge University Press).
- Niset, Julien, Jaromír Fiurášek, and Nicolas J Cerf (2009), “No-go theorem for Gaussian quantum error correction,” *Phys. Rev. Lett.* **102** (12), 10.1103/PhysRevLett.102.120501.
- NIST, (2021), “Post-Quantum Cryptography,” <https://csrc.nist.gov/projects/post-quantum-cryptography>.
- Noh, Kyungjoo, Victor V. Albert, and Liang Jiang (2019), “Quantum Capacity Bounds of Gaussian Thermal Loss Channels and Achievable Rates with Gottesman-Kitaev-Preskill Codes,” *IEEE Transactions on Information Theory* **65** (4), 2563–2582.
- Noh, Kyungjoo, and Christopher Chamberland (2020), “Fault-tolerant bosonic quantum error correction with the surface-gottesman-kitaev-preskill code,” *Phys. Rev. A* **101**, 012316.
- Noh, Kyungjoo, S. M. Girvin, and Liang Jiang (2020), “Encoding an oscillator into many oscillators,” *Phys. Rev. Lett.* **125**, 080503.
- Olbrich, Fabian, Jonatan Höschele, Markus Müller, Jan Kettler, Simone Luca Portalupi, Matthias Paul, Michael Jetter, and Peter Michler (2017), “Polarization-entangled photons from an ingaas-based quantum dot emitting in the telecom c-band,” *Applied Physics Letters* **111** (13), 133106.
- Palyanov, Yuri N, Igor N. Kupriyanov, Yuri M. Borzdov, and Nikolay V. Surovtsev (2015), “Germanium: a new catalyst for diamond synthesis and a new optically active impurity in diamond,” *Scientific Reports* **5**, 14789.
- Pan, Jian-Wei, Sara Gasparoni, Rupert Ursin, Gregor Weihs, and Anton Zeilinger (2003), “Experimental entanglement purification of arbitrary unknown states,” *Nature* **423** (6938), 417–422.
- Pan, Jian-Wei, Christoph Simon, Časlav Brukner, and Anton Zeilinger (2001), “Entanglement purification for quantum communication,” *Nature* **410** (6832), 1067.
- Panayi, Christiana, Mohsen Razavi, Xiongfeng Ma, and Norbert Lütkenhaus (2014), “Memory-assisted measurement-device-independent quantum key distribution,” *New Journal of Physics* **16** (4), 043005.
- Pang, Xiao-Ling, Ai-Lin Yang, Jian-Peng Dou, Hang Li, Chao-Ni Zhang, Eilon Poem, Dylan J Saunders, Hao Tang, Joshua Nunn, Ian A Walmsley, *et al.* (2020), “A hybrid quantum memory-enabled network at room temperature,” *Science advances* **6** (6), eaax1425.
- Pant, Mihir, Hari Krovi, Dirk Englund, and Saikat Guha (2017), “Rate-distance tradeoff and resource costs for all-optical quantum repeaters,” *Physical Review A* **95** (1), 1–15.
- Park, Jiho, Heonoh Kim, and Han Seb Moon (2019), “Polarization-entangled photons from a warm atomic ensemble using a sagnac interferometer,” *Phys. Rev. Lett.* **122** (14), 143601.
- Peev, Momtchil, Christoph Pacher, Romain Alléaume, Claudio Barreiro, Jan Bouda, W Boxleitner, Thierry Debuisschert, Eleni Diamanti, Mehrdad Dianati, JF Dynes, *et al.* (2009), “The SECOQC quantum key distribution network in vienna,” *New Journal of Physics* **11** (7), 075001.
- Pegg, David T, Lee S. Phillips, and Stephen M. Barnett (1998), “Optical state truncation by projection synthesis,”

- Physical Review Letters **81** (8), 1604–1606.
- Pichler, Hannes, Soonwon Choi, Peter Zoller, and Mikhail D Lukin (2017), “Universal photonic quantum computation via time-delayed feedback,” Proceedings of the National Academy of Sciences of the United States of America **114** (43), 11362–11367.
- Pingault, Benjamin, David-Dominik Jarausch, Christian Hepp, Lina Klintberg, Jonas N Becker, Matthew Markham, Christoph Becher, and Mete Atatüre (2017), “Coherent control of the silicon-vacancy spin in diamond,” Nature Communications **8**, 15579.
- Piparo, Nicolás Lo, Mohsen Razavi, and William J Munro (2017a), “Measurement-device-independent quantum key distribution with nitrogen vacancy centers in diamond,” Physical Review A **95** (2), 022338.
- Piparo, Nicolás Lo, Mohsen Razavi, and William J Munro (2017b), “Memory-assisted quantum key distribution with a single nitrogen-vacancy center,” Physical Review A **96** (5), 052313.
- Piparo, Nicolás Lo, Mohsen Razavi, and Christiana Panayi (2014), “Measurement-device-independent quantum key distribution with ensemble-based memories,” IEEE Journal of selected topics in quantum electronics **21** (3), 138–147.
- Pirandola, S, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, J. L. Pereira, M. Razavi, J. Shamsul Shaari, M. Tomamichel, V. C. Usenko, G. Vallone, P. Villoresi, and P. Wallden (2020), “Advances in quantum cryptography,” Adv. Opt. Photon. **12** (4), 1012–1236.
- Pirandola, Stefano (2019), “End-to-end capacities of a quantum communication network,” Communications Physics **2**, 51.
- Pirandola, Stefano, Riccardo Laurenza, Carlo Ottaviani, and Leonardo Banchi (2017), “Fundamental limits of repeaterless quantum communications,” Nature Communications **8** (1), 15043.
- Pirker, Alexander, and Wolfgang Dür (2019), “A quantum network stack and protocols for reliable entanglement-based networks,” New Journal of Physics **21** (3), 033003.
- Pittaluga, Mirko, Mariella Minder, Marco Lucamarini, Mirko Sanzaro, Robert I Woodward, Ming-Jun Li, Zhiliang Yuan, and Andrew J Shields (2021), “600-km repeater-like quantum communications with dual-band stabilization,” Nature Photonics **15**, 530–535.
- Pittman, T B, B. C. Jacobs, and J. D. Franson (2001), “Probabilistic quantum logic operations using polarizing beam splitters,” Phys. Rev. A **64**, 062311.
- Plenio, Martin B, and Shashank Virmani (2005), “An introduction to entanglement measures,” Quant. Inf. Comput. **7** (1,2), 1–51.
- Pompili, M, S. L. N. Hermans, S. Baier, H. K. C. Beukers, P. C. Humphreys, R. N. Schouten, R. F. L. Vermeulen, M. J. Tiggeleman, L. dos Santos Martins, B. Dirkse, S. Wehner, and R. Hanson (2021), “Realization of a multinode quantum network of remote solid-state qubits,” Science **372** (6539), 259–264.
- Pompili, Matteo, Carlo Delle Donne, Ingmar te Raa, Bart van der Vecht, Matthew Skrzypczyk, Guilherme Ferreira, Lisa de Kluijver, Arian J Stolk, Sophie LN Hermans, Przemysław Pawełczak, *et al.* (2022), “Experimental demonstration of entanglement delivery using a quantum network stack,” npj Quantum Information **8** (1), 121.
- Portmann, Christopher, and Renato Renner (2022), “Security in quantum cryptography,” Rev. Mod. Phys. **94**, 025008.
- Pu, Yun-Fei, Sheng Zhang, Yu-Kai Wu, Nan Jiang, Wei Chang, Chang Li, and Lu-Ming Duan (2021), “Experimental demonstration of memory-enhanced scaling for entanglement connection of quantum repeater segments,” Nature Photonics **15** (5), 374–378.
- Quesada, N, L. G. Helt, J. Izaac, J. M. Arrazola, R. Shahrokhshahi, C. R. Myers, and K. K. Sabapathy (2019), “Simulating realistic non-gaussian state preparation,” Phys. Rev. A **100**, 022341.
- Ralph, T C, A. J. F. Hayes, and A. Gilchrist (2005), “Loss-tolerant optical qubits,” Phys. Rev. Lett. **95** (10), 100501.
- Ralph, Timothy C, and AP Lund (2009), “Nondeterministic noiseless linear amplification of quantum systems,” in *AIP Conference Proceedings*, Vol. 1110 (American Institute of Physics) pp. 155–160.
- Rančić, Miloš, Morgan P. Hedges, Rose L. Ahlefeldt, and Matthew J. Sellars (2018), “Coherence time of over a second in a telecom-compatible quantum memory storage material,” Nature Physics **14** (1), 50–54.
- Raussendorf, R, J. Harrington, and K. Goyal (2006), “A fault-tolerant one-way quantum computer,” Annals of Physics **321** (9), 2242–2270.
- Raussendorf, R, J. Harrington, and K. Goyal (2007), “Topological fault-tolerance in cluster state quantum computation,” New Journal of Physics **9**, 10.1088/1367-2630/9/6/199.
- Raussendorf, Robert, and Hans J Briegel (2001), “A one-way quantum computer,” Phys. Rev. Lett. **86** (22), 5188–5191.
- Raussendorf, Robert, and Jim Harrington (2007), “Fault-tolerant quantum computation with high threshold in two dimensions,” Phys. Rev. Lett. **98** (19), 10.1103/PhysRevLett.98.190504.
- Razavi, M, M. Piani, and N. Lutkenhaus (2008), “Quantum repeaters with imperfect memories: cost and scalability,” Physical Review A **80**, 1–8.
- Razavi, M, K. Thompson, H. Farmanbar, Ma. Piani, and Norbert Lütkenhaus (2009), “Physical and architectural considerations in quantum repeaters,” Proceedings of SPIE **7236**, 723603–723613.
- Razavi, Mohsen (2018), *An introduction to quantum communications networks* (Morgan & Claypool Publishers).
- Redjem, W, A. Durand, T. Herzig, A. Benali, S. Pezzagna, J. Meijer, A. Yu Kuznetsov, H. S. Nguyen, Sébastien Cuffe, J.-M. Gérard, *et al.* (2020), “Single artificial atoms in silicon emitting at telecom wavelengths,” Nature Electronics **3**, 738–743.
- Reichle, Rainer, Dietrich Leibfried, Emanuel Knill, Joseph Britton, RB Blakestad, John D Jost, Christopher Langer, R Ozeri, Signe Seidelin, and David J Wineland (2006), “Experimental purification of two-atom entanglement,” Nature **443** (7113), 838–841.
- Reiserer, Andreas, Norbert Kalb, Gerhard Rempe, and Stephan Ritter (2014), “A quantum gate between a flying optical photon and a single trapped atom,” Nature **508** (7495), 237–240.
- Reiserer, Andreas, and Gerhard Rempe (2015), “Cavity-based quantum networks with single atoms and optical photons,” Rev. Mod. Phys. **87**, 1379–1418.
- Renner, Renato (2008), “Security of quantum key distribution,” International Journal of Quantum Information **06** (01), 1–127, <https://doi.org/10.1142/S0219749908003256>.
- Riedel, Daniel, Immo Söllner, Brendan J. Shields, Sebastian Starosielec, Patrick Appel, Elke Neu, Patrick Maletinsky,

- and Richard J. Warburton (2017), “Deterministic enhancement of coherent photon generation from a nitrogen-vacancy center in ultrapure diamond,” *Physical Review X* **7** (3), 031040.
- Riedl, Stefan, Matthias Lettner, Christoph Vo, Simon Baur, Gerhard Rempe, and Stephan Dürr (2012), “Bose-einstein condensate as a quantum memory for a photonic polarization qubit,” *Physical Review A* **85** (2), 022318.
- de Riedmatten, Hugues, Ivan Marcikic, Wolfgang Tittel, Hugo Zbinden, Daniel Collins, and Nicolas Gisin (2004), “Long distance quantum teleportation in a quantum relay configuration,” *Phys. Rev. Lett.* **92** (4), 047904.
- Riera-Sabat, F, P. Sekatski, A. Pirker, and W. Dür (2021), “Entanglement-assisted entanglement purification,” *Phys. Rev. Lett.* **127** (4), 040502.
- Rigovacca, Luca, Go Kato, Stefan Bäuml, Myungshik S Kim, William J Munro, and Koji Azuma (2018), “Versatile relative entropy bounds for quantum networks,” *New Journal of Physics* **20** (1), 013033.
- Rivest, Ronald L, Adi Shamir, and Leonard Adleman (1978), “A method for obtaining digital signatures and public-key cryptosystems,” *Communications of the ACM* **21** (2), 120–126.
- Roche, Calum (2022), “How much money did CERN’s Large Hadron Collider cost to build and who paid for it?” https://en.as.com/latest_news/how-much-money-did-cerns-large-hadron-collider-cost-to-build-and-who-paid-for-it-n.
- Rozpędek, Filip, Kenneth Goodenough, Jeremy Ribeiro, Norbert Kalb, V Caprara Vivoli, Andreas Reiserer, Ronald Hanson, Stephanie Wehner, and David Elkouss (2018), “Parameter regimes for a single sequential quantum repeater,” *Quantum Science and Technology* **3** (3), 034002.
- Rozpędek, Filip, Kyungjoo Noh, Qian Xu, Saikat Guha, and Liang Jiang (2021), “Quantum repeaters based on concatenated bosonic and discrete-variable quantum codes,” *npj Quantum Information* **7**, 102.
- Rozpędek, Filip, Raja Yehia, Kenneth Goodenough, Maximilian Ruf, Peter C Humphreys, Ronald Hanson, Stephanie Wehner, and David Elkouss (2019), “Near-term quantum-repeater experiments with nitrogen-vacancy centers: Overcoming the limitations of direct transmission,” *Physical Review A* **99** (5), 052330.
- Ruf, Maximilian, Noel H. Wan, Hyeonrak Choi, Dirk Englund, and Ronald Hanson (2021), “Quantum networks based on color centers in diamond,” *Journal of Applied Physics* **130** (7), 070901, <https://doi.org/10.1063/5.0056534>.
- Russo, Antonio, Edwin Barnes, and Sophia E. Economou (2018), “Photonic graph state generation from quantum dots and color centers for quantum communications,” *Phys. Rev. B* **98**, 085303.
- Russo, Antonio, Edwin Barnes, and Sophia E. Economou (2019), “Generation of arbitrary all-photonic graph states from quantum emitters,” *New Journal of Physics* **21** (5), 055002.
- Sabapathy, Krishna Kumar, Haoyu Qi, Josh Izaac, and Christian Weedbrook (2019), “Production of photonic universal quantum gates enhanced by machine learning,” *Phys. Rev. A* **100**, 012326.
- Salvail, Louis, Momtchil Peev, Eleni Diamanti, Romain Alléaume, Norbert Lütkenhaus, and Thomas Länger (2010), “Security of trusted repeater quantum key distribution networks,” *Journal of Computer Security* **18** (1), 61–87.
- Sangouard, Nicolas, Romain Dubessy, and Christoph Simon (2009), “Quantum repeaters based on single trapped ions,” *Phys. Rev. A* **79**, 042340.
- Sangouard, Nicolas, Christoph Simon, Hugues de Riedmatten, and Nicolas Gisin (2011), “Quantum repeaters based on atomic ensembles and linear optics,” *Rev. Mod. Phys.* **83**, 33–80.
- Sasaki, M, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, S. Miki, T. Yamashita, Z. Wang, A. Tanaka, K. Yoshino, Y. Nambu, S. Takahashi, A. Tajima, A. Tomita, T. Domeki, T. Hasegawa, Y. Sakai, H. Kobayashi, T. Asai, K. Shimizu, T. Tokura, T. Tsurumaru, M. Matsui, T. Honjo, K. Tamaki, H. Takesue, Y. Tokura, J. F. Dynes, A. R. Dixon, A. W. Sharpe, Z. L. Yuan, A. J. Shields, S. Uchikoga, M. Legré, S. Robyr, P. Trinkler, L. Monat, J.-B. Page, G. Ribordy, A. Poppe, A. Allacher, O. Maurhart, T. Länger, M. Peev, and A. Zeilinger (2011), “Field test of quantum key distribution in the tokyo qkd network,” *Opt. Express* **19** (11), 10387–10409.
- Sasaki, Masahide, Kentaro Kato, Masayuki Izutsu, and Osamu Hirota (1998), “Quantum channels showing superadditivity in classical capacity,” *Physical Review A* **58** (1), 146.
- Schaffner, Christian (2010), “Simple protocols for oblivious transfer and secure identification in the noisy-quantum-storage model,” *Physical Review A* **82** (3), 032308.
- Schaibley, J R, A. P. Burgers, G. A. McCracken, L.-M. Duan, P. R. Berman, D. G. Steel, A. S. Bracker, D. Gammon, and L. J. Sham (2013), “Demonstration of quantum entanglement between a single electron spin confined to an inas quantum dot and a photon,” *Phys. Rev. Lett.* **110** (16), 167401.
- Schön, C, E. Solano, F. Verstraete, J. I. Cirac, and M. M. Wolf (2005), “Sequential generation of entangled multiqubit states,” *Phys. Rev. Lett.* **95**, 110503.
- Schrödinger, E (1935), “Discussion of Probability Relations between Separated Systems,” *Mathematical Proceedings of the Cambridge Philosophical Society* **31** (4), 555–563.
- Schwartz, Ido, Dan Cogan, Emma R Schmidgall, Yaroslav Don, Liron Gantz, Oded Kenneth, Netanel H Lindner, and David Gershoni (2016), “Deterministic generation of a cluster state of entangled photons,” *Science* **354**, 434–437.
- Scully, Marlan O, and M. Suhail Zubairy (1997), *Quantum optics* (Cambridge University Press).
- Senellart, Pascale, Glenn Solomon, and Andrew White (2017), “High-performance semiconductor quantum-dot single-photon sources,” *Nature Nanotechnology* **12** (11), 1026–1039.
- Seshadreesan, Kaushik P, Hari Krovi, and Saikat Guha (2020), “Continuous-variable quantum repeater based on quantum scissors and mode multiplexing,” *Physical Review Research* **2** (1), 013310.
- Shaham, Roy, Or Katz, and Ofer Firstenberg (2021), “Strong coupling of alkali spins to noble-gas spins with hour-long coherence time,” *arXiv preprint arXiv:2102.02797*.
- Shibata, H, H. Takesue, T. Honjo, T. Akazaki, and Y. Tokura (2010), “Single-photon detection using magnesium diboride superconducting nanowires,” *Applied Physics Letters* **97** (21), 212504.
- Shibata, Hiroyuki, Toshimori Honjo, and Kaoru Shimizu (2014), “Quantum key distribution over a 72 db channel loss using ultralow dark count superconducting single-photon detectors,” *Optics letters* **39** (17), 5078–5081.

- Shor, Peter W (1997), “Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer,” *SIAM Journal on Computing* **26** (5), 1484–1509, <https://doi.org/10.1137/S0097539795293172>.
- Shor, Peter W, and John Preskill (2000), “Simple proof of security of the BB84 quantum key distribution protocol,” *Phys. Rev. Lett.* **85** (2), 441–444.
- Simon, C, M. Afzelius, J. Appel, A. Boyer de la Giroday, S.J. Dewhurst, N. Gisin, C. Y. Hu, F. Jelezko, S. Kröll, J.H. Müller, J. Nunn, E. S. Polzik, J. G. Rarity, H. De Riedmaten, W. Rosenfeld, A. J. Shields, N. Sköld, R. M. Stevenson, R. Thew, I. A. Walmsley, M. C. Weber, Harald Weinfurter, J. Wrachtrup, and R. J. Young (2010), “Quantum memories: A review based on the European integrated project “Qubit Applications (QAP)”,” *European Physical Journal D* **58** (1), 1–22.
- Sinclair, Neil, Erhan Saglamyurek, Hassan Mallahzadeh, Joshua A. Slater, Mathew George, Raimund Ricken, Morgan P. Hedges, Daniel Oblak, Christoph Simon, Wolfgang Sohler, and Wolfgang Tittel (2014), “Spectral multiplexing for scalable quantum photonics using an atomic frequency comb quantum memory and feed-forward control,” *Phys. Rev. Lett.* **113**, 053603.
- Sipahigil, Alp, Kay D. Jahnke, Lachlan J. Rogers, Tokuyuki Teraji, Junichi Isoya, Alexander S. Zibrov, Fedor Jelezko, and Mikhail D. Lukin (2014), “Indistinguishable photons from separated silicon-vacancy centers in diamond,” *Phys. Rev. Lett.* **113** (11), 113602.
- Slodička, L, G. Hétet, N. Röck, P. Schindler, M. Hennrich, and R. Blatt (2013), “Atom-atom entanglement by single-photon detection,” *Phys. Rev. Lett.* **110** (8), 083603.
- Somaschi, N, V. Giesz, L. De Santis, J. C. Laredo, M. P. Almeida, G. Hornecker, S. L. Portalupi, T. Grange, C. Antón, J. Demory, C. Gómez, I. Sagnes, N. D. Lanzillotti-Kimura, A. Lemaître, A. Auffeves, A. G. White, L. Lanco, and P. Senellart (2016), “Near-optimal single-photon sources in the solid state,” *Nature Photonics* **10** (5), 340–345.
- Stace, Thomas M, Sean D. Barrett, and Andrew C. Doherty (2009), “Thresholds for topological codes in the presence of loss,” *Phys. Rev. Lett.* **102** (20), 10.1103/PhysRevLett.102.200501.
- Stephenson, L J, D. P. Nadlinger, B. C. Nichol, S. An, P. Dromota, T. G. Ballance, K. Thirumalai, J. F. Goodwin, D. M. Lucas, and C. J. Ballance (2020), “High-rate, high-fidelity entanglement of qubits across an elementary quantum network,” *Phys. Rev. Lett.* **124** (11), 110501.
- Stinaff, Eric A, Michael Scheibner, Allan S. Bracker, Ilya V. Ponomarev, Vladimir L. Korenev, Morgan E. Ware, Matt F. Doty, Thomas L. Reinecke, and Dan Gammon (2006), “Optical signatures of coupled quantum dots,” *Science* **311** (5761), 636–639.
- Stockill, Robert, M. J. Stanley, Lukas Huthmacher, E. Clarke, M. Hugues, A. J. Miller, C. Matthiesen, C. Le Gall, and Mete Atatüre (2017), “Phase-tuned entangled state generation between distant spin qubits,” *Phys. Rev. Lett.* **119** (1), 010503.
- Stucki, Damien, Matthieu Legre, Francois Buntschu, B Clausen, Nadine Felber, Nicolas Gisin, Luca Henzen, Pascal Junod, Gérald Litzistorf, Patrick Monbaron, *et al.* (2011), “Long-term performance of the swissquantum quantum key distribution network in a field environment,” *New Journal of Physics* **13** (12), 123001.
- Su, Daiqin, Casey R. Myers, and Krishna Kumar Sabapathy (2019), “Conversion of Gaussian states to non-Gaussian states using photon-number-resolving detectors,” *Physical Review A* **100** (5), 052301.
- Sukachev, Denis D, Alp Sipahigil, Christian T. Nguyen, Mihir K. Bhaskar, Ruffin E. Evans, Fedor Jelezko, and Mikhail D. Lukin (2017), “Silicon-vacancy spin qubit in diamond: a quantum memory exceeding 10 ms with single-shot state readout,” *Phys. Rev. Lett.* **119** (22), 223602.
- Sun, Shuo, Hyochul Kim, Glenn S Solomon, and Edo Waks (2016), “A quantum phase switch between a single solid-state spin and a photon,” *Nature Nanotechnology* **11** (6), 539–544.
- Takeoka, Masahiro, Saikat Guha, and Mark M. Wilde (2014a), “Fundamental rate-loss tradeoff for optical quantum key distribution,” *Nature Communications* **5**, 5235.
- Takeoka, Masahiro, Saikat Guha, and Mark M. Wilde (2014b), “The squashed entanglement of a quantum channel,” *IEEE Transactions on Information Theory* **60**, 4987–4998.
- Tamaki, Kiyoshi, Hoi-Kwong Lo, Chi-Hang Fred Fung, and Bing Qi (2012), “Phase encoding schemes for measurement-device-independent quantum key distribution with basis-dependent flaw,” *Physical Review A* **85** (4), 042307.
- Tamaki, Kiyoshi, Hoi-Kwong Lo, Wenyuan Wang, and Marco Lucamarini (2018), “Information theoretic security of quantum key distribution overcoming the repeaterless secret key capacity bound,” arXiv preprint arXiv:1805.05511.
- Taminiau, T H, J. J. T. Wagenaar, T. Van der Sar, Fedor Jelezko, Viatcheslav V. Dobrovitski, and R. Hanson (2012), “Detection and control of individual nuclear spins using a weakly coupled electron spin,” *Phys. Rev. Lett.* **109** (13), 137602.
- Tan, Ting Rei, John P. Gaebler, Yiheng Lin, Yong Wan, R. Bowler, D. Leibfried, and David J. Wineland (2015), “Multi-element logic gates for trapped-ion qubits,” *Nature* **528** (7582), 380–383.
- Tani, Seiichiro, Hirotada Kobayashi, and Keiji Matsumoto (2005), “Exact quantum algorithms for the leader election problem,” in *Annual Symposium on Theoretical Aspects of Computer Science* (Springer) pp. 581–592.
- Tanzilli, S, W. Tittel, M. Halder, O. Alibart, P. Baldi, N. Gisin, and H. Zbinden (2005), “A photonic quantum information interface,” *Nature* **437** (7055), 116–120.
- Tchebotareva, Anna, Sophie L. N. Hermans, Peter C. Humphreys, Dirk Voigt, Peter J. Harmsma, Lun K. Cheng, Ad L. Verlaan, Niels Dijkhuizen, Wim de Jong, Anaïs Dréau, and Ronald Hanson (2019), “Entanglement between a diamond spin qubit and a photonic time-bin qubit at telecom wavelength,” *Phys. Rev. Lett.* **123**, 063601.
- Terhal, Barbara M (2015), “Quantum error correction for quantum memories,” *Rev. Mod. Phys.* **87**, 307–346.
- The Fibre Optic Association, (2019), “FOA Reference Guide,” <https://www.thefoa.org/tech/ref/testing/test/loss.html>.
- Thomas, Philip, Leonardo Ruscio, Olivier Morin, and Gerhard Rempe (2022), “Efficient generation of entangled multi-photon graph states from a single atom,” arXiv preprint arXiv:2205.12736.
- Togan, E, Y. Chu, A. S. Trifonov, L. Jiang, J. Maze, L. Childress, M. V. G. Dutt, A. S. Sørensen, P. R. Hemmer, A. S. Zibrov, and M. D. Lukin (2010), “Quantum entanglement between an optical photon and a solid-state spin qubit,” *Nature* **466** (7307), 730–734.
- Tomm, Natasha, Alisa Javadi, Nadia Olympia Antoniadis, Daniel Najer, Matthias Christian Löbl, Alexander Rolf Ko-

- rsch, Rüdiger Schott, Sascha René Valentin, Andreas Dirk Wieck, Arne Ludwig, *et al.* (2021), “A bright and fast source of coherent single photons,” *Nature Nanotechnology* **16**, 399–403.
- Townsend, Kevin (2022), “NIST Post-Quantum Algorithm Finalist Cracked Using a Classical PC,” <https://www.securityweek.com/nist-post-quantum-algorithm-finalist-cracked-using-classical-pc>.
- Trényi, Róbert, Koji Azuma, and Marcos Curty (2019), “Beating the repeaterless bound with adaptive measurement-device-independent quantum key distribution,” *New Journal of Physics* **21** (11), 113052.
- Trusheim, Matthew E, Benjamin Pingault, Noel H. Wan, Mustafa Gündoğan, Lorenzo De Santis, Romain Debroux, Dorian Gangloff, Carola Purser, Kevin C. Chen, Michael Walsh, *et al.* (2020), “Transform-limited photons from a coherent tin-vacancy spin in diamond,” *Phys. Rev. Lett.* **124** (2), 023602.
- Tzitrin, Ilan (2018), “Local equivalence of complete bipartite and repeater graph states,” *Physical Review A* **98** (3), 32305.
- Tzitrin, Ilan, J. Eli Bourassa, Nicolas C. Menicucci, and Krishna Kumar Sabapathy (2020), “Progress towards practical qubit computation using approximate Gottesman-Kitaev-Preskill codes,” *Physical Review A* **101** (3), 32315.
- Tzitrin, Ilan, Takaya Matsuura, Rafael N. Alexander, Guillaume Dauphinais, J. Eli Bourassa, Krishna K. Sabapathy, Nicolas C. Menicucci, and Ish Dhand (2021), “Fault-tolerant quantum computation with static linear optics,” [arXiv:2104.03241 \[quant-ph\]](https://arxiv.org/abs/2104.03241).
- Uppu, Ravitej, Freja T. Pedersen, Ying Wang, Cecilie T. Olesen, Camille Papon, Xiaoyan Zhou, Leonardo Midolo, Sven Scholz, Andreas D. Wieck, Arne Ludwig, *et al.* (2020), “Scalable integrated single-photon source,” *Science advances* **6** (50), eabc8268.
- Ursin, Rupert, F. Tiefenbacher, T. Schmitt-Manderbach, H. Weier, Thomas Scheidl, M. Lindenthal, B. Blauensteiner, T. Jennewein, J. Perdigues, P. Trojek, *et al.* (2007), “Entanglement-based quantum communication over 144 km,” *Nature Physics* **3** (7), 481.
- Vaidman, Lev (2003), “Instantaneous measurement of nonlocal variables,” *Phys. Rev. Lett.* **90**, 010402.
- Van Meter, Rodney (2014), *Quantum networking* (John Wiley & Sons).
- Van Meter, Rodney, Thaddeus D Ladd, William J Munro, and Kae Nemoto (2008), “System design for a long-line quantum repeater,” *IEEE/ACM Transactions On Networking* **17** (3), 1002–1013.
- Van Meter, Rodney, and Joe Touch (2013), “Designing quantum repeater networks,” *IEEE Communications Magazine* **51** (8), 64–71.
- Varnava, Michael, Daniel E. Browne, and Terry Rudolph (2006), “Loss Tolerance in One-Way Quantum Computation via Counterfactual Error Correction,” *Phys. Rev. Lett.* **97** (12), 120501.
- Varnava, Michael, Daniel E. Browne, and Terry Rudolph (2007), “Loss tolerant linear optical quantum memory by measurement-based quantum computing,” *New Journal of Physics* **9** (6), 203–203.
- Varnava, Michael, Daniel E. Browne, and Terry Rudolph (2008), “How Good Must Single Photon Sources and Detectors Be for Efficient Linear Optical Quantum Computation?” *Phys. Rev. Lett.* **100** (6), 060502.
- Vasconcelos, Rui, Sarah Reisenbauer, Cameron Salter, Georg Wachter, Daniel Wirtitsch, Jörg Schmiedmayer, Philip Walther, and Michael Trupke (2020), “Scalable spin-photon entanglement by time-to-polarization conversion,” *npj Quantum Information* **6**, 9.
- Vezevae, Arian, Paul Hilaire, Matthew F Doty, and Sophia E Economou (2022), “Deterministic generation of entangled photonic cluster states from quantum dot molecules,” [arXiv preprint arXiv:2206.03647](https://arxiv.org/abs/2206.03647).
- Volz, Jürgen, Markus Weber, Daniel Schlenk, Wenjamin Rosenfeld, Johannes Vrana, Karen Saucke, Christian Kurtz, and Harald Weinfurter (2006), “Observation of entanglement of a single photon with a trapped atom,” *Phys. Rev. Lett.* **96** (3), 030404.
- Waks, Edo, Assaf Zeevi, and Yoshihisa Yamamoto (2002), “Security of quantum key distribution with entangled photons against individual attacks,” *Physical Review A* **65** (5), 052310.
- Waldherr, Gerald, Y. Wang, S. Zaiser, M. Jamali, T. Schulte-Herbrüggen, H. Abe, T. Ohshima, J. Isoya, J. F. Du, P. Neumann, *et al.* (2014), “Quantum error correction in a solid-state hybrid spin register,” *Nature* **506** (7487), 204–207.
- Wallnöfer, Julius, Frederik Hahn, Mustafa Gündoğan, Jasinder S Sidhu, Fabian Wiesner, Nathan Walk, Jens Eisert, and Janik Wolters (2022), “Simulating quantum repeater strategies for multiple satellites,” *Communications Physics* **5** (1), 169.
- Walls, Daniel F, and Gerard J. Milburn (2007), *Quantum optics* (Springer Science & Business Media).
- Wan, Noel H, Tsung-Ju Lu, Kevin C. Chen, Michael P. Walsh, Matthew E. Trusheim, Lorenzo De Santis, Eric A. Bersin, Isaac B. Harris, Sara L. Mouradian, Ian R. Christen, *et al.* (2020), “Large-scale integration of artificial atoms in hybrid photonic circuits,” *Nature* **583** (7815), 226–231.
- Wang, Hui, Yu-Ming He, T.-H. Chung, Hai Hu, Ying Yu, Si Chen, Xing Ding, M.-C. Chen, Jian Qin, Xiaoxia Yang, *et al.* (2019a), “Towards optimal single-photon sources from polarized microcavities,” *Nature Photonics* **13**, 770–775.
- Wang, Pengfei, Chun-Yang Luan, Mu Qiao, Mark Um, Junhua Zhang, Ye Wang, Xiao Yuan, Mile Gu, Jingning Zhang, and Kihwan Kim (2021), “Single ion qubit with estimated coherence time exceeding one hour,” *Nature Communications* **12**, 233.
- Wang, Shuang, De-Yong He, Zhen-Qiang Yin, Feng-Yu Lu, Chao-Han Cui, Wei Chen, Zheng Zhou, Guang-Can Guo, and Zheng-Fu Han (2019b), “Beating the fundamental rate-distance limit in a proof-of-principle quantum key distribution system,” *Physical Review X* **9** (2), 021046.
- Wang, Shuang, Zhen-Qiang Yin, De-Yong He, Wei Chen, Rui-Qiang Wang, Peng Ye, Yao Zhou, Guan-Jie Fan-Yuan, Fang-Xiang Wang, Yong-Gang Zhu, *et al.* (2022), “Twin-field quantum key distribution over 830-km fibre,” *Nature Photonics* **16** (2), 154–161.
- Wang, Xiang-Bin (2005), “Beating the photon-number-splitting attack in practical quantum cryptography,” *Phys. Rev. Lett.* **94** (23), 230503.
- Wang, Xiang-Bin, Zong-Wen Yu, and Xiao-Long Hu (2018), “Twin-field quantum key distribution with large misalignment error,” *Physical Review A* **98** (6), 062323.
- Wang, Ye, Mark Um, Junhua Zhang, Shuoming An, Ming Lyu, Jing-Ning Zhang, L.-M. Duan, Dahyun Yum, and Kihwan Kim (2017), “Single-qubit quantum memory exceeding ten-minute coherence time,” *Nature Photonics* **11** (10), 646.

- Wehner, Stephanie, Marcos Curty, Christian Schaffner, and Hoi-Kwong Lo (2010), “Implementation of two-party protocols in the noisy-storage model,” *Physical Review A* **81** (5), 052336.
- Wehner, Stephanie, David Elkouss, and Ronald Hanson (2018), “Quantum internet: A vision for the road ahead,” *Science* **362** (6412), 10.1126/science.aam9288.
- Wells, L M, Sokratis Kalliakos, Bruno Villa, D. J. P. Ellis, R. M. Stevenson, A. J. Bennett, Ian Farrer, D. A. Ritchie, and A. J. Shields (2019), “Photon phase shift at the few-photon level and optical switching by a quantum dot in a microcavity,” *Physical Review Applied* **11** (6), 061001.
- Werner, Reinhard F (2001), “All teleportation and dense coding schemes,” *Journal of Physics A: Mathematical and General* **34** (35), 7081.
- Wiesner, Stephen (1983), “Conjugate coding,” *ACM Sigact News* **15** (1), 78–88.
- Wolf, Michael M, David Pérez-García, and Geza Giedke (2007), “Quantum capacities of bosonic channels,” *Phys. Rev. Lett.* **98** (13), 130501.
- Wootters, W K, and W. H. Zurek (1982), “A single quantum cannot be cloned,” *Nature* **299**, 802–803.
- Wootters, William K (1998), “Entanglement of formation of an arbitrary state of two qubits,” *Phys. Rev. Lett.* **80** (10), 2245–2248.
- Xie, Yuan-Mei, Yu-Shuo Lu, Chen-Xun Weng, Xiao-Yu Cao, Zhao-Ying Jia, Yu Bao, Yang Wang, Yao Fu, Hua-Lei Yin, and Zeng-Bing Chen (2022), “Breaking the rate-loss bound of quantum key distribution with asynchronous two-photon interference,” *PRX Quantum* **3** (2), 020315.
- Xu, Feihu, Marcos Curty, Bing Qi, and Hoi-Kwong Lo (2015), “Measurement-device-independent quantum cryptography,” *IEEE Journal of Selected Topics in Quantum Electronics* **21** (3), 148–158.
- Xu, Feihu, Xiongfeng Ma, Qiang Zhang, Hoi-Kwong Lo, and Jian-Wei Pan (2020), “Secure quantum key distribution with realistic devices,” *Rev. Mod. Phys.* **92**, 025002.
- Xu, Zhongxiao, Yuelong Wu, Long Tian, Lirong Chen, Zhiying Zhang, Zhihui Yan, Shujing Li, Hai Wang, Changde Xie, and Kunchi Peng (2013), “Long lifetime and high-fidelity quantum memory of photonic polarization qubit by lifting zeeman degeneracy,” *Phys. Rev. Lett.* **111** (24), 240503.
- Yamamoto, Takashi, Masato Koashi, and Nobuyuki Imoto (2001), “Concentration and purification scheme for two partially entangled photon pairs,” *Physical Review A* **64** (1), 012304.
- Yamamoto, Takashi, Masato Koashi, Şahin Kaya Özdemir, and Nobuyuki Imoto (2003), “Experimental extraction of an entangled photon pair from two identically decohered pairs,” *Nature* **421** (6921), 343–346.
- Yang, Sheng-Jun, Xu-Jie Wang, Xiao-Hui Bao, and Jian-Wei Pan (2016), “An efficient quantum light–matter interface with sub-second lifetime,” *Nature Photonics* **10** (6), 381–384.
- Yehia, Raja, Simon Neves, Eleni Diamanti, and Iordanis Kerenidis (2022), “Quantum city: simulation of a practical near-term metropolitan quantum network,” arXiv preprint arXiv:2211.01190.
- Yin, Juan, Yuan Cao, Yu-Huai Li, Sheng-Kai Liao, Liang Zhang, Ji-Gang Ren, Wen-Qi Cai, Wei-Yue Liu, Bo Li, Hui Dai, *et al.* (2017), “Satellite-based entanglement distribution over 1200 kilometers,” *Science* **356** (6343), 1140–1144.
- Yu, Leo, Chandra M Natarajan, Tomoyuki Horikiri, Carsten Langrock, Jason S Pelc, Michael G Tanner, Eisuke Abe, Sebastian Maier, Christian Schneider, Sven Höfling, *et al.* (2015), “Two-photon interference at telecom wavelengths for time-bin-encoded single photons from quantum-dot spin qubits,” *Nature Communications* **6** (1), 8955.
- Yu, Yong, Fei Ma, Xi-Yu Luo, Bo Jing, Peng-Fei Sun, Ren-Zhou Fang, Chao-Wei Yang, Hui Liu, Ming-Yang Zheng, Xiu-Ping Xie, *et al.* (2020), “Entanglement of two quantum memories via fibres over dozens of kilometres,” *Nature* **578** (7794), 240–245.
- Yu, Zong-Wen, Xiao-Long Hu, Cong Jiang, Hai Xu, and Xiang-Bin Wang (2019), “Sending-or-not-sending twin-field quantum key distribution in practice,” *Scientific Reports* **9**, 3080.
- Zaidi, Hussain A, Chris Dawson, Peter van Loock, and Terry Rudolph (2015), “Near-deterministic creation of universal cluster states with probabilistic bell measurements and three-qubit resource states,” *Phys. Rev. A* **91**, 042301.
- Zanin, Guilherme Luiz, Maxime J Jacquet, Michele Spagnolo, Peter Schiansky, Irati Alonso Calafell, Lee A Rozema, and Philip Walther (2021), “Fiber-compatible photonic feed-forward with 99% fidelity,” *Optics Express* **29** (3), 3425–3437.
- Zaske, Sebastian, Andreas Lenhard, Christian A. Keßler, Jan Kettler, Christian Hepp, Carsten Arend, Roland Albrecht, Wolfgang-Michael Schulz, Michael Jetter, Peter Michler, and Christoph Becher (2012), “Visible-to-telecom quantum frequency conversion of light from a single quantum emitter,” *Phys. Rev. Lett.* **109**, 147404.
- Zeng, Pei, Hongyi Zhou, Weijie Wu, and Xiongfeng Ma (2022), “Mode-pairing quantum key distribution,” *Nature Communications* **13**, 3903.
- Zhan, Yuan, Paul Hilaire, Edwin Barnes, Sophia E Economou, and Shuo Sun (2023), “Performance analysis of quantum repeaters enabled by deterministically generated photonic graph states,” *Quantum* **7**, 924.
- Zhan, Yuan, and Shuo Sun (2020), “Deterministic generation of loss-tolerant photonic cluster states with a single quantum emitter,” *Phys. Rev. Lett.* **125**, 223601.
- Zhang, Qiang, Xiao-Hui Bao, Chao-Yang Lu, Xiao-Qi Zhou, Tao Yang, Terry Rudolph, and Jian-Wei Pan (2008), “Demonstration of a scheme for the generation of “event-ready” entangled photon pairs from a single-photon source,” *Phys. Rev. A* **77**, 062316.
- Zhang, Rui, Li-Zheng Liu, Zheng-Da Li, Yue-Yang Fei, Xu-Fei Yin, Li Li, Nai-Le Liu, Yingqiu Mao, Yu-Ao Chen, and Jian-Wei Pan (2022a), “Loss-tolerant all-photonic quantum repeater with generalized shor code,” *Optica* **9** (2), 152–158.
- Zhang, Wei, Tim van Leent, Kai Redeker, Robert Garthoff, René Schwonnek, Florian Fertig, Sebastian Eppelt, Wenjamin Rosenfeld, Valerio Scarani, Charles C-W Lim, *et al.* (2022b), “A device-independent quantum key distribution system for distant users,” *Nature* **607** (7920), 687–691.
- Zhong, Han-Sen, Yuan Li, Wei Li, Li-Chao Peng, Zu-En Su, Yi Hu, Yu-Ming He, Xing Ding, Weijun Zhang, Hao Li, *et al.* (2018), “12-photon entanglement and scalable scattershot boson sampling with optimal entangled-photon pairs from parametric down-conversion,” *Phys. Rev. Lett.* **121** (25), 250505.
- Zhong, Manjin, Morgan P. Hedges, Rose L. Ahlefeldt, John G. Bartholomew, Sarah E. Beavan, Sven M. Wittig, Jevon J. Longdell, and Matthew J. Sellars (2015a), “Optically addressable nuclear spins in a solid with a six-hour coherence time,” *Nature* **517** (7533), 177–180.

- Zhong, Tian, and Philippe Goldner (2019), “Emerging rare-earth doped material platforms for quantum nanophotonics,” *Nanophotonics* **8** (11), 2003–2015.
- Zhong, Tian, Jonathan M Kindem, Evan Miyazono, and Andrei Faraon (2015b), “Nanophotonic coherent light–matter interfaces based on rare-earth-doped crystals,” *Nature Communications* **6**, 8206.
- Zhong, Xiaoqing, Jianyong Hu, Marcos Curty, Li Qian, and Hoi-Kwong Lo (2019), “Proof-of-principle experimental demonstration of twin-field type quantum key distribution,” *Phys. Rev. Lett.* **123**, 100506.
- Zhong, Xiaoqing, Wenyuan Wang, Reem Mandil, Hoi-Kwong Lo, and Li Qian (2022), “Simple multiuser twin-field quantum key distribution network,” *Physical Review Applied* **17** (1), 014025.
- Zhong, Xiaoqing, Wenyuan Wang, Li Qian, and Hoi-Kwong Lo (2021), “Proof-of-principle experimental demonstration of twin-field quantum key distribution over optical channels with asymmetric losses,” *npj Quantum Information* **7**, 6.
- Zhou, Lai, Jinping Lin, Yuan-Mei Xie, Yu-Shuo Lu, Yumang Jing, Hua-Lei Yin, and Zhiliang Yuan (2023), “Experimental quantum communication overcomes the rate-loss limit without global phase tracking,” *Phys. Rev. Lett.* **130**, 250801.
- Zhu, Hao-Tao, Yizhi Huang, Hui Liu, Pei Zeng, Mi Zou, Yunqi Dai, Shibiao Tang, Hao Li, Lixing You, Zhen Wang, Yu-Ao Chen, Xiongfeng Ma, Teng-Yun Chen, and Jian-Wei Pan (2023), “Experimental mode-pairing measurement-device-independent quantum key distribution without global phase locking,” *Phys. Rev. Lett.* **130**, 030801.
- Zukowski, M, A. Zeilinger, M. A. Horne, and A. K. Ekert (1993), “Event-ready-detectors bell experiment via entanglement swapping,” *Phys. Rev. Lett.* **71**, 4287.
- Zwenger, M, H. J. Briegel, and W. Dür (2016), “Measurement-based quantum communication,” *Applied Physics B* **122** (3), 50.
- Zwenger, M, H. J. Briegel, and W. Dür (2014), “Hybrid architecture for encoded measurement-based quantum computation,” *Scientific Reports* **4**, 5364.
- Zwenger, M, W. Dür, and H. J. Briegel (2012), “Measurement-based quantum repeaters,” *Physical Review A* **85** (6), 062326.
- Zwenger, M, A. Pirker, V. Dunjko, H. J. Briegel, and W. Dür (2018), “Long-range big quantum-data transmission,” *Phys. Rev. Lett.* **120** (3), 030503.