Finite-key analysis of loss-tolerant quantum key distribution based on random sampling theory

Guillermo Currás-Lorenzo, Álvaro Navarrete, Margarida Pereira, and Kiyoshi Tamaki

Phys. Rev. A **104**, 012406 — Published 6 July 2021

DOI: 10.1103/PhysRevA.104.012406

Finite-key analysis of loss-tolerant quantum key distribution based on random sampling theory

Guillermo Currás-Lorenzo,[1, *] Álvaro Navarrete,[2] Margarida Pereira,[2] and Kiyoshi Tamaki[3]

[1]*School of Electronic and Electrical Engineering, University of Leeds, Leeds, United Kingdom*

[2]*Escuela de Ingeniería de Telecomunicación, Department of Signal*
Theory and Communications, University of Vigo, Vigo E-36310, Spain

[3]*Faculty of Engineering, University of Toyama, Gofuku 3190, Toyama 930-8555, Japan*

(Dated: June 11, 2021)

The core of security proofs of quantum key distribution (QKD) is the estimation of a parameter that determines the amount of privacy amplification that the users need to apply in order to distill a secret key. To estimate this parameter using the observed data, one needs to apply concentration inequalities, such as random sampling theory or Azuma's inequality. The latter can be straightforwardly employed in a wider class of QKD protocols, including those that do not rely on basis independent sources, such as the loss-tolerant (LT) protocol. However, when applied to real-life finite-length QKD experiments, Azuma's inequality typically results in substantially lower secret-key rates. Here, we propose an alternative security analysis of the LT protocol against general attacks, for both its prepare-and-measure and measurement-device-independent versions, that is based on random sampling theory. Consequently, our security proof provides considerably higher secret-key rates than the previous finite-key analysis based on Azuma's inequality. This work opens up the possibility of using random sampling theory to provide alternative security proofs for other QKD protocols.

Quantum key distribution (QKD) allows two distant users, Alice and Bob, to generate a shared secret key in the presence of an eavesdropper, Eve, with unbounded computational power [1, 2]. To prove the security of QKD, we often consider the error rate that Alice and Bob would have obtained in a fictitious scenario, known as the phase-error rate, which directly bounds the amount of sifted-key information that could have leaked to Eve, and determines the amount of privacy amplification that the users need to apply to distill a secret key [3–6]. Since Alice and Bob cannot directly observe the phase-error rate, they must estimate it using the data collected in the test rounds, i.e. the detected rounds which are not used to generate the sifted key. For this estimation, it is indispensable to employ statistical techniques. For example, in the case of the BB84 protocol [7] without source flaws, one can use the fact that Alice's source is basis independent to estimate the Z-basis phase-error rate from the X-basis bit-error rate, and vice-versa, using random sampling theory [8, 9]. In protocols where the user sources are basis dependent, the detection statistics of a particular round may depend on the basis choices made in previous rounds, and Azuma's inequality [10] has been typically applied to deal with this dependency [11–14]. However, recently, Maeda *et al.* [15] have successfully applied a non-trivial security analysis based on random sampling theory to a twin-field QKD variant in which the users do not employ a basis independent source. This work raises the obvious question of whether random sampling theory could also be applied to other protocols that do not use a basis independent source, and whose security proofs currently rely on Azuma's inequality. Since the estimation of Eve's side information is the core of QKD security proofs, investigating the possibility of using different estimation techniques deepens our understanding of QKD protocols and their security. Moreover, it has important experimental implications, in terms of the secret-key rate obtainable, since concentration bounds for *independent* random variables, such as the Chernoff bound, are typically tighter than those for *dependent* random variables, such as Azuma's inequality.

One obvious candidate to investigate is the loss-tolerant (LT) protocol [12], a three-state protocol that is resistant to losses in the presence of state preparation flaws (SPFs), which arise from the finite precision of modulation devices. Earlier attempts to address SPFs [16] resulted in a performance that degraded very quickly with moderate-to-high channel losses. Conversely, even in the presence of large SPFs and high losses, the performance of the LT protocol is close to that of a perfect four-state BB84 protocol, at least in the limit of infinitely-long keys [12]. Recent works [17–19] have shown that one can prove the security of the LT protocol in the presence of additional source imperfections, such as mode dependencies, Trojan horse attacks or pulse correlations, as long as one can ensure that their magnitude is sufficiently small. Also, the LT protocol can be combined with measurement-device-independent (MDI) QKD [20] to guarantee the security in the presence of arbitrarily flawed detectors. Moreover, the LT protocol is highly practical and can be implemented with off-the-shelf devices. In fact, several experiments have implemented the LT protocol [21, 22], and a variation of it [23] set a fibre QKD distance record. For these reasons, a deep un-

[*] g.j.curraslorenzo@leeds.ac.uk

derstanding of its security is of theoretical and practical interest.

Clearly, in the LT protocol, Alice's source is not basis independent. For starters, in its standard three-state formulation, Alice only emits one of the two X-basis states. However, even if one were to apply the LT idea to a four-state protocol, the source would still be basis dependent, due to the SPFs. Thus, Azuma's inequality has been used in both the asymptotic [12] and finite-key [13] security proofs of the LT protocol. In the asymptotic regime, the specific statistical technique employed does not affect the performance, since the deviation terms vanish in the limit of infinitely-long keys. However, choosing the tightest statistical technique available does have an impact on the key rate obtainable in (existing and future) real-life finite-length implementations of the LT protocol.

In this paper, we show how the finite-key security of the LT protocol against general attacks can be reduced to a random sampling problem, for both its original prepare-and-measure (P&M) version and its MDI version. This random sampling problem can be solved using concentration inequalities for sums of independent random variables, which results in tighter bounds than those of a previous analysis [13] based on Azuma's inequality. Our paper is structured as follows. In Section I, we present our general statistical analysis, inspired by that of Ref. [15], and apply it to a generic scenario. In Section II, we show how this analysis can be used to estimate the phase-error rate of the P&M LT protocol, and in Section III, we do the same for the MDI LT protocol. In Section IV, we give an expression for the secret-key rate obtainable in both protocols. In Section V, we simulate the secret-key rate obtainable for different values of the block size, and compare it with that of alternative analyses. Finally, in Section VI, we conclude our paper.

I. GENERAL STATISTICAL ANALYSIS

In this section, we present our general estimation procedure and apply it to a generic scenario, which we denote as the Tagged Virtual Protocol (TVP). Its name refers to the fact that, as we will see in Sections II and III, one can draw an equivalence between the TVP and the virtual protocols of both LT P&M QKD and LT MDI QKD, once the users probabilistically assign tags to their emissions.

In the TVP, the users emit, amongst others, the states $\rho_{\rm vir}$, $\rho_{\rm pos}$ and $\rho_{\rm neg}$, with probabilities $p_{\rm vir}$, $p_{\rm pos}$ and $p_{\rm neg}$. These may be states sent by Alice, in the P&M protocol, or joint states sent by Alice and Bob, in the MDI protocol. Also, $\rho_{\rm vir}$ is one of the virtual states, emitted only in the virtual protocol, while $\rho_{\rm pos}$ and $\rho_{\rm neg}$ are actual states, emitted also in the actual protocol. These states satisfy

$$\rho_{\rm vir} = c_{\rm pos}\rho_{\rm pos} - c_{\rm neg}\rho_{\rm neg} \tag{1}$$

where $c_{\rm pos}$ and $c_{\rm neg}$ are some non-negative coefficients such that $c_{\rm pos} - c_{\rm neg} = 1$. For reasons that will become clear later on, we assume that the users assign a tag of $t \in \{{\rm vir}, {\rm pos}, {\rm neg}\}$ to each emission of ρ_t. That is, each emission of $\rho_{\rm vir}$ is trivially assigned a tag $t = {\rm vir}$, and so on. In the quantum communication phase of the protocol, some of these emissions will be detected. Here, a "detection" refers to any process that depends on Eve's attack and distinguishes some emissions from others. For the P&M protocol, we will define a detection as an event in which Bob obtained a particular measurement result, and for the MDI protocol, as an event in which Charlie reports a projection to a particular Bell state. We denote by N_t the number of detected emissions with a tag of t, i.e., the number of detected emissions of ρ_t. In the actual protocol, the outcome of the random variables $N_{\rm pos}$ and $N_{\rm neg}$ can be directly observed by the users, but the outcome of $N_{\rm vir}$ cannot, and must be estimated. Thus, the objective of the analysis is to find a statistical relationship between $N_{\rm vir}$, $N_{\rm pos}$ and $N_{\rm neg}$; more specifically, we want to find a function f such that $\Pr[N_{\rm vir} > f(N_{\rm pos}, N_{\rm neg}; \varepsilon)] \leq \varepsilon$, where ε can be made arbitrarily small.

The starting point of the analysis is Eq. (1), which we now rewrite as

$$\rho_{\rm pos} = p_{\rho_{\rm vir}|{\rm pos}}\rho_{\rm vir} + p_{\rho_{\rm neg}|{\rm pos}}\rho_{\rm neg}, \tag{2}$$

where $p_{\rho_{\rm vir}|{\rm pos}} = 1/c_{\rm pos}$ and $p_{\rho_{\rm neg}|{\rm pos}} = c_{\rm neg}/c_{\rm pos}$. Equation (2) implies that sending $\rho_{\rm pos}$ is equivalent to sending $\rho_{\rm vir}$ with probability $p_{\rho_{\rm vir}|{\rm pos}}$ and $\rho_{\rm neg}$ with probability $p_{\rho_{\rm neg}|{\rm pos}}$. That is, the TVP is indistinguishable from the following scenario:

– The users select tag $t \in \{{\rm vir}, {\rm pos}, {\rm neg}\}$ with probability p_t.
– If $t = {\rm pos}$, the users emit $\rho_{\rm vir}$ with probability $p_{\rho_{\rm vir}|{\rm pos}}$, or $\rho_{\rm neg}$ with probability $p_{\rho_{\rm neg}|{\rm pos}}$.
– If $t \in \{{\rm vir}, {\rm neg}\}$, the users emit ρ_t.

In the above scenario, some emissions of $\rho_{\rm vir}$ will have a tag of "vir", and some will have a tag of "pos", but they are otherwise identical. The same is true for emissions of $\rho_{\rm neg}$ with tags of "neg" and "pos". Thus, one can go even further, and think of another equivalent scenario in which the users first decide the quantum state that they emit, and then probabilistically assign a tag to it. Namely:

Modified scenario

- The users select and emit the state $\rho_x \in \{\rho_{\rm vir}, \rho_{\rm neg}\}$ with probability $\tilde{p}_{\rho_x} := p_x + p_{\rm pos}p_{\rho_x|{\rm pos}}$.
- Next, they assign their emission the tag $t = x$ with probability $\tilde{p}_{x|\rho_x} := p_x/\tilde{p}_{\rho_x}$, or the tag $t = {\rm pos}$ with probability $\tilde{p}_{{\rm pos}|\rho_x} := 1 - \tilde{p}_{x|\rho_x}$.

This modified scenario is equivalent to the TVP in terms of tags, because:

1. The overall probability to assign a particular tag $t \in \{{\rm vir}, {\rm pos}, {\rm neg}\}$ is the same in both scenarios, i.e. p_t.

2. The quantum state emitted given a particular tag t is the same in both scenarios, i.e. ρ_t.

In the modified scenario, let $\tilde N_t^{\rho_x}$ be the number of detected emissions of ρ_x with a tag of t, $\tilde N^{\rho_x} = \sum_t \tilde N_t^{\rho_x}$ be the total number of detected emissions of ρ_x, and $\tilde N_t = \sum_x \tilde N_t^{\rho_x}$ be the total number of detected emissions with a tag of t. That is, $\tilde N_{\rm vir} = \tilde N_{\rm vir}^{\rho_{\rm vir}}$, $\tilde N_{\rm pos} = \tilde N_{\rm pos}^{\rho_{\rm vir}} + \tilde N_{\rm pos}^{\rho_{\rm neg}}$, and $\tilde N_{\rm neg} = \tilde N_{\rm neg}^{\rho_{\rm neg}}$. The equivalence above implies that, for any attack by Eve, the set of random variables $\{N_{\rm vir}, N_{\rm pos}, N_{\rm neg}\}$ in the TVP has an identical distribution as the set $\{\tilde N_{\rm vir}, \tilde N_{\rm pos}, \tilde N_{\rm neg}\}$ in the modified scenario. Hence, if we find a function f such that $\Pr\left[\tilde N_{\rm vir} > f(\tilde N_{\rm pos}, \tilde N_{\rm neg}; \varepsilon)\right] \le \varepsilon$ in an execution of the modified scenario, then it must also be the case that $\Pr\left[N_{\rm vir} > f(N_{\rm pos}, N_{\rm neg}; \varepsilon)\right] \le \varepsilon$ in an execution of the TVP. The equivalence between the two scenarios is shown in Fig. 1.

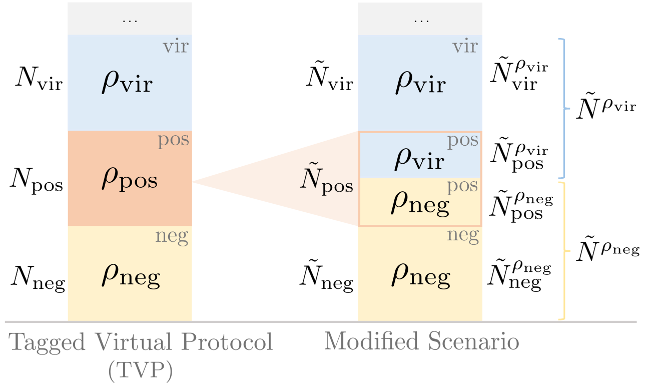

Figure 1. Relationship between the Tagged Virtual Protocol (TVP) and the modified scenario. In the modified scenario, each emission of $\rho_{\rm vir}$ ($\rho_{\rm neg}$) is assigned a tag of either "vir" ("neg") or "pos" with a fixed probability, in such a way that emissions with a tag of $t \in \{{\rm vir}, {\rm neg}, {\rm pos}\}$ are equivalent to emissions of ρ_t in the TVP. In the modified scenario, the detection statistics of each emission must be independent of the tag assigned to it, since Eve does not have any tag information. Hence, each of the $\tilde N^{\rho_{\rm vir}}$ ($\tilde N^{\rho_{\rm neg}}$) detected emissions of $\rho_{\rm vir}$ ($\rho_{\rm neg}$) is assigned a tag of either "vir" ("neg") or "pos" with the *a priori* fixed probability. This allows us to find a statistical relationship between the random variables $\tilde N_{\rm vir} := \tilde N_{\rm vir}^{\rho_{\rm vir}}$, $\tilde N_{\rm pos} := \tilde N_{\rm pos}^{\rho_{\rm vir}} + \tilde N_{\rm pos}^{\rho_{\rm neg}}$ and $\tilde N_{\rm neg} := \tilde N_{\rm neg}^{\rho_{\rm neg}}$ using a random sampling analysis, see Eq. (5). Since the TVP is equivalent to the modified scenario, the same relationship must hold for the random variables $N_{\rm vir}$, $N_{\rm pos}$ and $N_{\rm neg}$ in the TVP, see Eq. (6).

The random tag assignments in the modified scenario allow us to find a bound on $\tilde N_{\rm vir}$ by using a random sampling analysis. The key idea is that the probability to assign a particular tag to a particular emission must be independent of whether the emission is detected or not, since the tag assignment does not change the emitted quantum state, and Eve does not have any tag information. Thus, each of the $\tilde N^{\rho_{\rm vir}}$ detected emissions of $\rho_{\rm vir}$ is assigned a random tag of "vir" or "pos" with probabilities $\tilde p_{{\rm vir}|\rho_{\rm vir}}$ and $\tilde p_{{\rm pos}|\rho_{\rm vir}} = 1 - \tilde p_{{\rm vir}|\rho_{\rm vir}}$, respectively. This implies that $\tilde N_{\rm vir}^{\rho_{\rm vir}}$ is a random sample of a population of $\tilde N^{\rho_{\rm vir}} = \tilde N_{\rm vir}^{\rho_{\rm vir}} + \tilde N_{\rm pos}^{\rho_{\rm vir}}$ elements, where each item is sampled with probability $\tilde p_{{\rm vir}|\rho_{\rm vir}}$. In Appendix A, we show that this implies that, except with probability $\varepsilon/2$,

$$\tilde N_{\rm vir}^{\rho_{\rm vir}} \le g_U\left(\tilde N_{\rm pos}^{\rho_{\rm vir}}, \tilde p_{{\rm vir}|\rho_{\rm vir}}, \varepsilon/2\right), \tag{3}$$

where g_U is defined in Eq. (A3). Similarly $\tilde N_{\rm pos}^{\rho_{\rm neg}}$ is the size of a random sample of a population of $\tilde N^{\rho_{\rm neg}} = \tilde N_{\rm pos}^{\rho_{\rm neg}} + \tilde N_{\rm neg}^{\rho_{\rm neg}}$ elements, where each item is sampled with probability $\tilde p_{{\rm pos}|\rho_{\rm neg}}$. This implies that, except with probability $\varepsilon/2$,

$$\tilde N_{\rm pos}^{\rho_{\rm neg}} \ge g_L\left(\tilde N_{\rm neg}, \tilde p_{{\rm pos}|\rho_{\rm neg}}, \varepsilon/2\right), \tag{4}$$

where g_L is defined in Eq. (A3).

Using the relations $\tilde N_{\rm vir} = \tilde N_{\rm vir}^{\rho_{\rm vir}}$, $\tilde N_{\rm pos} = \tilde N_{\rm pos}^{\rho_{\rm vir}} + \tilde N_{\rm pos}^{\rho_{\rm neg}}$, and $\tilde N_{\rm neg} = \tilde N_{\rm neg}^{\rho_{\rm neg}}$, in combination with Eqs. (3) and (4), we have that

$$\begin{aligned}\tilde N_{\rm vir} &\le g_U\left(\tilde N_{\rm pos} - \tilde N_{\rm pos}^{\rho_{\rm neg}}, \tilde p_{{\rm vir}|\rho_{\rm vir}}, \varepsilon/2\right)\\ &\le g_U\left(\tilde N_{\rm pos} - g_L\left(\tilde N_{\rm neg}, \tilde p_{{\rm pos}|\rho_{\rm neg}}, \varepsilon/2\right), \tilde p_{{\rm vir}|\rho_{\rm vir}}, \varepsilon/2\right),\end{aligned} \tag{5}$$

except with probability ε, where in the first inequality we have used Eq. (3), and in the second inequality we have used Eq. (4) and the fact that g_U is an increasing function with respect to its first argument.

As explained above, the random variables $\{N_{\rm vir}, N_{\rm pos}, N_{\rm neg}\}$ in the TVP are identically distributed as the random variables $\{\tilde N_{\rm vir}, \tilde N_{\rm pos}, \tilde N_{\rm neg}\}$ in the modified scenario. Thus, Eq. (5) implies that, in the virtual protocol

$$\begin{aligned}N_{\rm vir} &\le g_U\left(N_{\rm pos} - g_L\left(N_{\rm neg}, \tilde p_{{\rm pos}|\rho_{\rm neg}}, \varepsilon/2\right), \tilde p_{{\rm vir}|\rho_{\rm vir}}, \varepsilon/2\right)\\ &:= f(N_{\rm pos}, N_{\rm neg}; \varepsilon),\end{aligned} \tag{6}$$

except with probability ε, as required. Since $N_{\rm pos}$ and $N_{\rm neg}$ are observables of the actual protocol, Alice and Bob can use their observed values to obtain an upper bound on $N_{\rm vir}$.

In Sections II and III, we explain how to apply this statistical analysis to the LT protocol, for both its P&M and MDI versions. In this protocol, the virtual states and the actual states are all in the same qubit space. Because of this, each virtual state can be expressed as an operator-form linear function of the actual states. However, this linear function does not necessarily have one positive term and one negative term, as in Eq. (1). To apply the analysis above, the users will first probabilistically assign tags of "pos" and "neg" to some of their emissions, in such a way that the average state with a tag of $t \in \{\text{pos}, \text{neg}\}$ is ρ_t. After these tag assignments, the resulting *tagged* virtual protocol will be equivalent to the TVP, shown on the left side of Fig. 1.

II. PREPARE-AND-MEASURE PROTOCOL

In this section, we apply our analysis to the P&M LT protocol [12]. For each round, Alice sends Bob a pure state $|\psi_j\rangle_a$ with probability p_j, $j \in \{0_Z, 1_Z, 0_X\}$, where emissions of $|\psi_{0_X}\rangle_a$ ($|\psi_{0_Z}\rangle_a$ and $|\psi_{1_Z}\rangle_a$) are considered to belong to the X (Z) basis. The only assumption needed to apply our analysis is that Alice's states are characterised and linearly dependent, i.e. they are all in the same qubit space. For simplicity, in this discussion we assume that the states are in the XZ plane of the Bloch sphere; in Appendix B, we show how to apply our results in the general case. Bob measures the incoming signals in the Z or in the X basis, with probabilities p_{Z_B} and p_{X_B}, respectively. We do not need to assume that Bob's measurement bases are mutually unbiased, but we do assume that his choice of basis is fully random, and that the detection efficiency is the same for both bases. Afterwards, Bob reveals which rounds were detected, and both users reveal their basis choice in those rounds. The sifted key is generated from the detected events in which Alice and Bob both chose the Z basis. The detected rounds in which Bob chose the X basis are considered to be test rounds. In these, Bob will reveal his measurement result. The full protocol description is given in Appendix C.

The objective of the security analysis is to estimate the number of phase errors in the sifted key, using the test data. To define this quantity, we consider an equivalent entanglement-based virtual protocol, in which Alice replaces the key emissions by the generation of the entangled state

$$|\Psi_Z\rangle_{Aa} = \frac{1}{\sqrt{2}}\big(|0_Z\rangle_A |\psi_{0_Z}\rangle_a + |1_Z\rangle_A |\psi_{1_Z}\rangle_a\big), \tag{7}$$

where a is the photonic system sent to Bob and A is Alice's fictitious qubit ancilla, which she keeps in her lab. For simplicity, in Eq. (7), we have assumed that $p_{0_Z} = p_{1_Z}$. The key generated in the actual protocol is equivalent to the key that Alice and Bob would obtain by performing a Z-basis measurement on the systems A and a of the detected rounds in which Alice generated $|\Psi_Z\rangle_{Aa}$. The number of phase errors is defined as the number of errors that Alice and Bob would have observed if they had measured these systems A and a in the X basis instead. This is equivalent to a scenario in which, in the key rounds, Alice sends Bob the virtual states

$$|\psi_{\text{vir}_\alpha}\rangle_a = \frac{|\psi_{0_Z}\rangle_a + (-1)^\alpha |\psi_{1_Z}\rangle_a}{\sqrt{2(1-(-1)^\alpha \langle\psi_{0_Z}|\psi_{1_Z}\rangle_a)}}, \tag{8}$$

with probabilities

$$p_{\text{vir}_\alpha} = \frac{1}{2} p_{Z_A}(1-(-1)^\alpha \langle\psi_{0_Z}|\psi_{1_Z}\rangle_a), \tag{9}$$

and Bob measures these states in the X basis. Here, p_{Z_A} is the probability that Alice selects the Z basis, and $\alpha \in \{0,1\}$. Thus, Alice's choice of state in the virtual protocol can be equivalently described by assuming that she fictitiously prepares the entangled state

$$\begin{aligned}|\Psi_{\text{vir}}\rangle_{Sa} = {} & \sqrt{p_{\text{vir}_0} p_{Z_B}}\, |0\rangle_S |\psi_{\text{vir}_0}\rangle_a + \sqrt{p_{\text{vir}_1} p_{Z_B}}\, |1\rangle_S |\psi_{\text{vir}_1}\rangle_a \\ & + \sqrt{p_{0_Z} p_{X_B}}\, |2\rangle_S |\psi_{0_Z}\rangle_a + \sqrt{p_{1_Z} p_{X_B}}\, |3\rangle_S |\psi_{1_Z}\rangle_a \\ & + \sqrt{p_{0_X} p_{X_B}}\, |4\rangle_S |\psi_{0_X}\rangle_a + \sqrt{p_{0_X} p_{Z_B}}\, |5\rangle_S |\psi_{0_X}\rangle_a\,,\end{aligned} \tag{10}$$

and then performs a measurement on system S. Note that S holds information about Alice's and Bob's setting choices. For instance, $|2\rangle_S$ represents the events in which Alice selects the virtual state $|\psi_{0_Z}\rangle_a$ and Bob chooses the X basis. In the right-hand side of Eq. (10), the first two terms are associated with virtual events. That is, the events in which Alice and Bob select the Z basis in the actual protocol, but their basis choice is replaced by the X basis in the virtual protocol. All the other terms in Eq. (10) correspond to actual events that occur in the actual protocol.

In the virtual protocol that we have just defined, the occurrence of a phase error is defined as an event in which Alice measures system S, obtains the outcome 0 (1), and Bob's X-basis measurement outputs the bit value 1 (0). The measurement statistics associated with these events cannot be directly observed, since the virtual states are never sent in the actual protocol. However, as we show in Appendix B, one can exploit the fact that the virtual states and the actual states live in the same qubit space to find an operator-form linear relationship between the virtual states and the actual states. Namely,

$$\begin{aligned}\rho_{\text{vir}_0} &= c_{0_Z|\text{vir}_0}\rho_{0_Z} + c_{1_Z|\text{vir}_0}\rho_{1_Z} + c_{0_X|\text{vir}_0}\rho_{0_X}\,, \\ \rho_{\text{vir}_1} &= c_{0_Z|\text{vir}_1}\rho_{0_Z} + c_{1_Z|\text{vir}_1}\rho_{1_Z} + c_{0_X|\text{vir}_1}\rho_{0_X}\,,\end{aligned} \tag{11}$$

where $\rho_{\text{vir}_\alpha} \equiv |\psi_{\text{vir}_\alpha}\rangle\langle\psi_{\text{vir}_\alpha}|_a$, $\rho_j \equiv |\psi_j\rangle\langle\psi_j|_a$, and the coefficients $c_{j|\text{vir}_\alpha}$ can be positive, negative or zero depending on the form of the actual states $\{|\psi_j\rangle_a\}$. For example, when there are no SPFs, the emitted states are $|\psi_{0_Z}\rangle_a = |0_Z\rangle_a$, $|\psi_{1_Z}\rangle_a = |1_Z\rangle_a$ and $|\psi_{0_X}\rangle_a = |0_X\rangle_a$; and Eq. (11) becomes $\rho_{\text{vir}_0} = \rho_{0_X}$ and $\rho_{\text{vir}_1} = \rho_{0_Z} + \rho_{1_Z} - \rho_{0_X}$. Next, in order to employ the analysis in Section I, we rewrite Eq. (11) as

$$\rho_{\text{vir}_0} = c_{\text{pos}_0}\rho_{\text{pos}_0} - c_{\text{neg}_0}\rho_{\text{neg}_0}\,, \tag{12}$$

$$\rho_{\text{vir}_1} = c_{\text{pos}_1}\rho_{\text{pos}_1} - c_{\text{neg}_1}\rho_{\text{neg}_1}\,, \tag{13}$$

where, for $t \in \{\text{pos}, \text{neg}\}$ and $\alpha \in \{0,1\}$,

$$c_{t_\alpha} = \sum_{j \in \mathcal{S}_{t_\alpha}} |c_{j|\text{vir}_\alpha}|, \tag{14}$$

$$\rho_{t_\alpha} = \sum_{j \in \mathcal{S}_{t_\alpha}} p_{j|t_\alpha} |\psi_j\rangle\langle\psi_j|_a\,. \tag{15}$$

In Eq. (15), $\mathcal{S}_{\mathrm{pos}_\alpha}$ ($\mathcal{S}_{\mathrm{neg}_\alpha}$) is the set of indices j such that c_j^α is positive (negative), and

$$p_{j|t_\alpha} = \frac{|c_{j|\mathrm{vir}_\alpha}|}{c_{t_\alpha}}. \tag{16}$$

Now, each of Eqs. (12) and (13) is identical to Eq. (1), the starting point of the statistical fluctuation analysis introduced in Section I. We will apply this analysis to estimate the detection statistics of each virtual state, separately. Recall that, in the TVP defined in Section I, the states sent are ρ_{vir}, ρ_{pos} and ρ_{neg} (see Fig. 1). However, in the virtual protocol defined above, Alice does not emit the states ρ_{pos_0}, ρ_{pos_1}, ρ_{neg_0} and ρ_{neg_1}. Instead, Alice will probabilistically assign tags of $t_0 \in \{\mathrm{pos}_0, \mathrm{neg}_0\}$ and $t_1 \in \{\mathrm{pos}_1, \mathrm{neg}_1\}$ to some of her emissions, in such a way that the average state with a tag of t_0 (t_1) is ρ_{t_0} (ρ_{t_1}). After doing so, we can draw an equivalence between the virtual protocol and the TVP.

More concretely, let us consider the events in which Alice emits $|\psi_j\rangle_a$, $j \in \{0_Z, 1_Z, 0_X\}$, and Bob chooses the X basis, corresponding to measuring system S of Eq. (10) in 2, 3 or 4. Each of these events occurs with probability $p_{j,X_B} = p_j p_{X_B}$, and is assigned a tag of $t_\alpha \in \{\mathrm{pos}_\alpha, \mathrm{neg}_\alpha\}$ with probability

$$p_{t_\alpha|j,X_B} = \frac{p_{t_\alpha} p_{j|t_\alpha}}{p_j p_{X_B}}, \tag{17}$$

or a tag of $t_\alpha = \mathrm{junk}_\alpha$ otherwise; where $\alpha \in \{0,1\}$, $p_{j|t_\alpha}$ is given by Eq. (16), and p_{t_α} is the total probability of assigning tag t_α. Note that the assignment of tag t_0 and of tag t_1 is done independently: each of these emissions will have both a tag of t_0 and a tag of t_1. This is allowed because our key idea relies only on a probabilistic assignment of a tag, and even if multiple assignments are made for a single pulse, the argument still holds. In Eq. (17), the conditional probabilities $p_{t_\alpha|j,X_B}$ become fixed once one chooses the value of p_{t_α}, which must be such that $p_{t_\alpha} \leq p_j p_{X_B}/p_{j|t_\alpha}$ for all $j \in \{0_Z, 1_Z, 0_X\}$, since $p_{t_\alpha|j,X_B} \leq 1$. In order to waste as few test rounds as possible, and thus obtain a tight estimate of the number of phase errors, we assume that Alice chooses the largest possible value of p_{t_α}, given by

$$p_{t_\alpha} = \min_j \frac{p_j p_{X_B}}{p_{j|t_\alpha}}. \tag{18}$$

Moreover, in the virtual protocol, Alice assigns a deterministic tag of $t_0 = \mathrm{vir}_0$ ($t_1 = \mathrm{vir}_1$) to each emission of $|\psi_{\mathrm{vir}_0}\rangle_a$ ($|\psi_{\mathrm{vir}_1}\rangle_a$), corresponding to $S = 0$ ($S = 1$).

After these tag assignments, an emission with a tag of t_α is equivalent to an emission of ρ_{t_α}. Thus, if Alice disregards the outcome of her measurement of system S, and considers only the tags of t_α that she assigns, the virtual protocol becomes equivalent to a scenario in which Alice actually emits ρ_{t_α} with probability p_{t_α}, and then trivially assigns her emission a tag of t_α. This scenario, which we denote as the the Tagged Virtual Protocol α and depict on the right side of Fig. 2, is identical to the TVP defined in Section I and shown on the left side of Fig. 1.

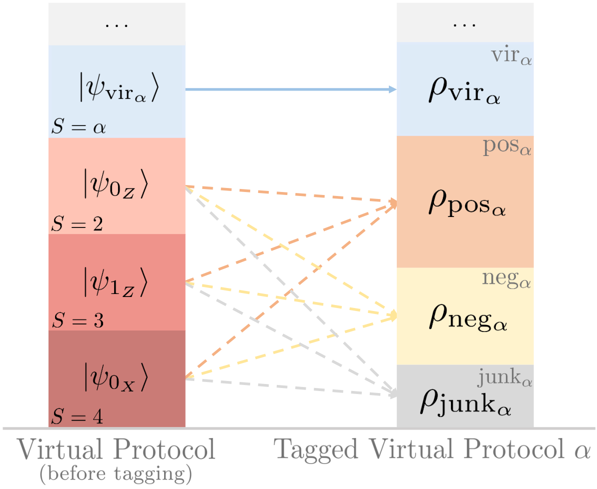

Figure 2. Relation between the virtual protocol and the Tagged Virtual Protocol α, where $\alpha \in \{0,1\}$, for the P&M scheme. In the virtual protocol, events for which $S \in \{2,3,4\}$ are probabilistically assigned a tag of $t_\alpha \in \{\mathrm{pos}_\alpha, \mathrm{neg}_\alpha, \mathrm{junk}_\alpha\}$ (dashed arrows), in such a way that the average state with a tag of t_α is ρ_{t_α}. Events for which $S = \alpha$ are deterministically assigned a tag of $t_\alpha = \mathrm{vir}_\alpha$ (solid arrow). If one considers only the tags of t_α that Alice has assigned, the virtual protocol becomes equivalent to the Tagged Virtual Protocol α. The ellipses at the top of the diagram represent events which are identical in both scenarios, but which are not relevant for the analysis.

Let $N_{t_0}^{1_X}$ ($N_{t_1}^{0_X}$) be the number of detected events with a tag of t_0 (t_1) in which Bob obtained measurement result 1_X (0_X). Equation (6) of Section I implies that, in the Tagged Virtual Protocol 0, it holds that, except with probability $\varepsilon/2$,

$$\begin{aligned} N_{\mathrm{vir}0}^{1_X} \leq g_U\Big(& N_{\mathrm{pos}0}^{1_X} - g_L\big(N_{\mathrm{neg}0}^{1_X}, \tilde{p}_{\mathrm{pos}0|\rho_{\mathrm{neg}0}}, \varepsilon/4\big), \\ & \tilde{p}_{\mathrm{vir}0|\rho_{\mathrm{vir}0}}, \varepsilon/4\Big), \end{aligned} \tag{19}$$

and in the Tagged Virtual Protocol 1, it holds that, except with probability $\varepsilon/2$,

$$\begin{aligned} N_{\mathrm{vir}1}^{0_X} \leq g_U\Big(& N_{\mathrm{pos}1}^{0_X} - g_L\big(N_{\mathrm{neg}1}^{0_X}, \tilde{p}_{\mathrm{pos}1|\rho_{\mathrm{neg}1}}, \varepsilon/4\big), \\ & \tilde{p}_{\mathrm{vir}1|\rho_{\mathrm{vir}1}}, \varepsilon/4\Big), \end{aligned} \tag{20}$$

where, for $\alpha \in \{0,1\}$, $\tilde{p}_{\mathrm{vir}\alpha|\rho_{\mathrm{vir}\alpha}} = p_{\mathrm{vir}\alpha}/(p_{\mathrm{vir}\alpha} + p_{\mathrm{pos}\alpha}/c_{\mathrm{pos}\alpha})$ and $\tilde{p}_{\mathrm{pos}\alpha|\rho_{\mathrm{neg}\alpha}} = 1 - p_{\mathrm{neg}\alpha}/(p_{\mathrm{neg}\alpha} + p_{\mathrm{pos}\alpha} c_{\mathrm{neg}\alpha}/c_{\mathrm{pos}\alpha})$. Moreover, since the virtual protocol is equivalent to the Tagged Virtual Protocol 0 (1), in terms of the assigned tags of t_0 (t_1), Eq. (19) (Eq. (20)) must also hold for the virtual protocol. Thus, combining Eqs. (19) and (20), we have that, in the virtual protocol, the number of phase errors $N_{\rm ph} := N^{1_X}_{\rm vir0} + N^{0_X}_{\rm vir1}$ satisfies

$$\begin{aligned} N_{\rm ph} \leq\, & g_U\Big(N^{1_X}_{\rm pos0} - g_L\big(N^{1_X}_{\rm neg0}, \tilde{p}_{{\rm pos0}|\rho_{\rm neg0}}, \varepsilon/4\big), \\ & \quad \tilde{p}_{{\rm vir0}|\rho_{\rm vir0}}, \varepsilon/4\Big) \\ & + g_U\Big(N^{0_X}_{\rm pos1} - g_L\big(N^{0_X}_{\rm neg1}, \tilde{p}_{{\rm pos1}|\rho_{\rm neg1}}, \varepsilon/4\big), \\ & \quad \tilde{p}_{{\rm vir1}|\rho_{\rm vir1}}, \varepsilon/4\Big), \end{aligned} \tag{21}$$

except with probability ε.

In order to use Eq. (21) to prove the security, the quantities $N^{1_X}_{t_0}$ and $N^{0_X}_{t_1}$, for $\alpha \in \{0, 1\}$ and $t_\alpha \in \{{\rm pos}_\alpha, {\rm neg}_\alpha\}$, must be observables in an actual implementation of the protocol. Thus, the probabilistic tag assignments defined in Eq. (17) must happen in the actual protocol too. However, note the following: (1) the tag assigned to a particular emission must be independent of Bob's measurement result, since the tag assignment does not change the emitted quantum state; and (2) the assignment of tag t_α is only relevant for the analysis if Bob happens to obtain a measurement outcome of $(\alpha \oplus 1)_X$ in that round. This implies that it is only necessary for Alice to probabilistically assign a tag of t_0 (t_1) to the events in which she sent $|\psi_j\rangle_a$, $j \in \{0_Z, 1_Z, 0_X\}$, and Bob obtained measurement result 1_X (0_X). For a full description of the protocol, including the tagging step, see Appendix C.

III. MEASUREMENT-DEVICE-INDEPENDENT PROTOCOL

In this section, we apply our analysis to the LT MDI QKD protocol. For each round, Alice (Bob) selects the state $|\psi_j\rangle_a$ ($|\psi'_s\rangle_b$) with probability p_j (p'_s), where j (s) $\in \{0, 1, \tau\}$, and sends it to an untrusted middle node Charlie. As in the P&M case, the only assumption required to apply our analysis is that all states emitted by Alice (Bob) are in the same qubit space. For simplicity, in this discussion we assume that all states lie in the XZ plane of the Bloch sphere; in Appendix D, we show how to treat the case in which they do not. Emissions for which $j \in \{0, 1\}$ ($s \in \{0, 1\}$) are considered to belong to the Z basis, and for simplicity their selection probability is assumed to be equal, i.e. $p_0 = p_1 = p_Z/2$ ($p'_0 = p'_1 = p'_Z/2$). We denote Alice and Bob's joint state by $|\psi_{j,s}\rangle_{ab} \equiv |\psi_j\rangle_a \otimes |\psi'_s\rangle_b$, and its associated probability by $p_{j,s} \equiv p_j p'_s$.

Alice and Bob expect Charlie to perform a Bell state measurement on each incoming joint pulse, and announce the result. In most MDI protocols, including the original MDI QKD proposal [20], Charlie may obtain a projection to one of two Bell states. However, for simplicity, for now we assume that Charlie attempts to obtain a projection to only one of the four Bell states, and that if he is successful (unsuccessful), he reports the round as "detected" ("undetected"). At the end of the section, we show how to generalise the analysis to the case in which Charlie may report a projection to two or more different Bell states. Also, note that Charlie is untrusted, and may even be fully controlled by Eve. Thus, in what follows, we directly assume that it is Eve who performs the measurements and announces the results. Importantly, Eve is not limited to measuring each round independently: if she performs a coherent attack, her full set of announcements may depend on an arbitrary general measurement acting jointly on the photonic systems of all the rounds in the protocol.

After Eve's announcements, Alice and Bob reveal, for each round, whether or not they used the Z basis, thus learning whether or not $(j, s) \in \mathcal{Z} := \{(0, 0), (0, 1), (1, 0), (1, 1)\}$. The rounds for which $(j, s) \notin \mathcal{Z}$ are automatically considered to belong to the set of test emissions, which we denote as $\mathcal{T}$. The rounds for which $(j, s) \in \mathcal{Z}$ receive a special treatment: with probability $p_{\mathcal{K}|\mathcal{Z}}$ they are considered key emissions, and with probability $p_{\mathcal{T}|\mathcal{Z}}$ they are considered test emissions, where $\mathcal{K}$ is the set of key emissions, and $p_{\mathcal{K}|\mathcal{Z}} + p_{\mathcal{T}|\mathcal{Z}} = 1$. This is needed because we want to use data from some $\mathcal{Z}$-rounds to estimate the phase-error rate. The resulting scenario is shown on the left-hand side of Fig. 3. For all rounds in $\mathcal{T}$, Alice and Bob reveal their choice of (j, s).

Alice (Bob) defines her (his) sifted key as her (his) choices of j (s) in the detected rounds in $\mathcal{K}$. The objective of the analysis is to use the detection statistics of the $\mathcal{T}$-rounds to estimate the number of phase errors in their sifted keys. This quantity is defined as the number of errors that Alice and Bob would have obtained if they had run a virtual scenario in which they replaced the $\mathcal{K}$-emissions by the generation of the virtual state $|\Psi_{\mathcal{K}}\rangle = \frac{1}{2}\sum_{j,s=0,1} |j_Z, s_Z\rangle_{AB} |\psi_{j,s}\rangle_{ab}$, followed by an X-basis measurement on their local ancillas A and B. Let $\Pi^{\rm ph}_{AB}$ be the projector onto the phase-error subspace in AB. Note that the definition of a phase error depends on the particular Bell state onto which Charlie is supposed to project the incoming pulses. The average state of a key emission may be written as

$$\rho_{\mathcal{K}} = \frac{1}{4}\sum_{j,s=0,1} |\psi_{j,s}\rangle\langle\psi_{j,s}|_{ab} = p_{{\rm ph}|\mathcal{K}}\rho_{\rm ph} + p_{\overline{\rm ph}|\mathcal{K}}\rho_{\overline{\rm ph}}. \tag{22}$$

where $\rho_{\rm ph}$ and $\rho_{\overline{\rm ph}}$ are quantum states such that $p_{{\rm ph}|\mathcal{K}}\rho_{\rm ph} = {\rm Tr}_{AB}[\Pi^{\rm ph}_{AB} |\Psi_{\mathcal{K}}\rangle\langle\Psi_{\mathcal{K}}|]$ and $p_{\overline{\rm ph}|\mathcal{K}}\rho_{\overline{\rm ph}} = {\rm Tr}_{AB}[(\mathbb{I} - \Pi^{\rm ph}_{AB}) |\Psi_{\mathcal{K}}\rangle\langle\Psi_{\mathcal{K}}|]$. Thus, the virtual protocol may be regarded as the following scenario: the users jointly select $\mathcal{K}$ or $\mathcal{T}$ with probabilities $p_{\mathcal{K}} = p_{\mathcal{Z}} p_{\mathcal{K}|\mathcal{Z}}$ and $p_{\mathcal{T}} = 1 - p_{\mathcal{K}}$, respectively, and

- If they select $\mathcal{K}$, they emit $\rho_{\rm ph}$ and $\rho_{\overline{\rm ph}}$ with probabilities $p_{{\rm ph}|\mathcal{K}}$ and $p_{\overline{\rm ph}|\mathcal{K}}$, respectively.
- If they select $\mathcal{T}$, they emit $|\psi_{j,s}\rangle_{ab}$ with probability $p_{j,s|\mathcal{T}} = p_{j,s}p_{\mathcal{T}|j,s}/p_{\mathcal{T}}$, where $p_{\mathcal{T}|j,s} = p_{\mathcal{T}|\mathcal{Z}}$ if $(j, s) \in \mathcal{Z}$ and $p_{\mathcal{T}|j,s} = 1$ if $(j, s) \notin \mathcal{Z}$.

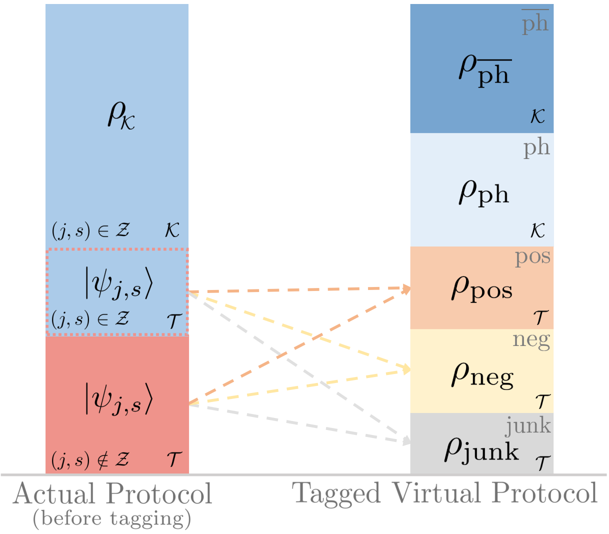

Figure 3. Relationship between the actual protocol and the Tagged Virtual Protocol in the MDI scenario. In the actual protocol, shown on the left, emissions such that $(j,s) \in \mathcal{Z}$ are probabilistically assigned to either $\mathcal{K}$ or $\mathcal{T}$, while emissions such that $(j,s) \notin \mathcal{Z}$ are always assigned to $\mathcal{T}$. In both the actual and virtual protocols, events in $\mathcal{T}$ are probabilistically assigned a tag of $t \in \{\text{pos}, \text{neg}, \text{junk}\}$, in such a way that the average state with a tag of t is ρ_t. The dashed arrows represent this tagging process. In the virtual protocol, $\mathcal{K}$-emissions are substituted by emissions of ρ_{ph} and $\rho_{\overline{\text{ph}}}$, and are assigned tags of "ph" and "$\overline{\text{ph}}$", respectively. If Alice and Bob consider only the tags that they have assigned, the virtual protocol becomes equivalent to the *tagged* virtual protocol, shown on the right.

The number of phase errors, N_{ph}, is defined as the number of detected emissions of ρ_{ph} that Alice and Bob would have observed if they had run this virtual protocol. To estimate this quantity, we use again the random sampling analysis of Section I. To apply this analysis, however, we need to first show that ρ_{ph} can be written in the form of Eq. (1), i.e.,

$$\rho_{\text{ph}} = c_{\text{pos}}\rho_{\text{pos}} - c_{\text{neg}}\rho_{\text{neg}}, \tag{23}$$

and then add a tagging step to the protocol, so that it becomes equivalent to a scenario in which the states ρ_{pos} and ρ_{neg} are actually emitted. In Appendix B, we show that ρ_{ph} can be expressed as an operator-form linear function of the actual states, that is

$$\rho_{\text{ph}} = \sum_{j,s} c_{j,s}\rho_{j,s}, \tag{24}$$

where $\rho_{j,s} \equiv |\psi_{j,s}\rangle\langle\psi_{j,s}|_{ab}$ and the coefficients $c_{j,s}$ are real and can be negative. Thus, if we denote by $\mathcal{S}_{\text{pos}}$ ($\mathcal{S}_{\text{neg}}$) the set of pairs (j,s) such that $c_{j,s}$ is positive (negative), and, for $t \in \{\text{pos}, \text{neg}\}$, we set

$$c_t = \sum_{j,s\in\mathcal{S}_t} |c_{j,s}|, \tag{25}$$

$$\rho_t = \sum_{j,s\in\mathcal{S}_t} p_{j,s|t}\rho_{j,s}, \tag{26}$$

where

$$p_{j,s|t} := \begin{cases} |c_{j,s}|/c_t & \text{if } (j,s) \in \mathcal{S}_t, \\ 0 & \text{otherwise,} \end{cases} \tag{27}$$

we obtain Eq. (23).

In the tagging step, Alice and Bob need to probabilistically assign tags of "pos" and "neg" to their emissions in $\mathcal{T}$, in such a way that the average state with a tag of t is ρ_t. To achieve this, in the actual protocol, Alice and Bob must assign a tag of $t \in \{\text{pos}, \text{neg}\}$ to each emission of $|\psi_{j,s}\rangle_{ab}$ in $\mathcal{T}$ with probability

$$p_{t|j,s,\mathcal{T}} = \frac{p_{t|\mathcal{T}}\,p_{j,s|t}}{p_{j,s|\mathcal{T}}}, \tag{28}$$

where $p_{j,s|t}$ is given by Eq. (27), and $p_{t|\mathcal{T}}$ is the probability that a round in $\mathcal{T}$ is assigned a tag of t. Note that the assignment probabilities $p_{t|j,s,\mathcal{T}}$ become fixed once one chooses $p_{t|\mathcal{T}}$. From Eq. (28), it follows that the value of $p_{t|\mathcal{T}}$ must be such that $p_{t|\mathcal{T}} \leq p_{j,s|\mathcal{T}}/p_{j,s|t}$, $\forall (j,s) \in \mathcal{S}_t$. Hence, its maximum possible value is

$$p_{t|\mathcal{T}} = \min_{j,s\in\mathcal{S}_t} \frac{p_{j,s|\mathcal{T}}}{p_{j,s|t}}, \tag{29}$$

and we assume that Alice and Bob choose this value, in order to waste as few $\mathcal{T}$-rounds as possible and thus obtain a tight estimate of the phase-error rate. Finally, Alice and Bob assign the tag "junk" to all the remaining rounds in $\mathcal{T}$ that have not been tagged as "pos" or "neg".

Since $\mathcal{T}$-emissions are identical in the actual and virtual protocols, the previous tag assignments can be regarded as taking place in both protocols. Besides, let us further assume that, in the virtual protocol, Alice and Bob assign trivial tags of "ph" and "$\overline{\text{ph}}$" to each emission of ρ_{ph} and $\rho_{\overline{\text{ph}}}$, respectively. Then, if Alice and Bob disregard their choice of state, and consider only the tags that they have assigned, the resulting *tagged* virtual protocol becomes equivalent to the scenario depicted in the right-hand side of Fig. 3, in which Alice and Bob emit ρ_t, $t \in \{\text{ph}, \overline{\text{ph}}, \text{pos}, \text{neg}, \text{junk}\}$, with probability p_t; where $p_t = p_{\mathcal{K}}p_{t|\mathcal{K}}$ for $t \in \{\text{ph}, \overline{\text{ph}}\}$, and $p_t = p_{\mathcal{T}}p_{t|\mathcal{T}}$ for $t \in \{\text{pos}, \text{neg}, \text{junk}\}$. This scenario is identical to the starting point of the random sampling analysis in Section I, the TVP shown on the left side of Fig. 1. The only differences are that here we have denoted the virtual state of interest as ρ_{ph}, not ρ_{vir}; and that we have some extra emissions of $\rho_{\overline{\text{ph}}}$ and ρ_{junk}, which we simply ignore in the analysis. Using Eq. (6), we have that, except with probability ε, the number of phase errors N_{ph}

satisfies

$$N_{\rm ph} \leq g_U\left(N_{\rm pos} - g_L\left(N_{\rm neg}, \tilde{p}_{{\rm pos}|\rho_{\rm neg}}, \varepsilon/2\right), \tilde{p}_{{\rm ph}|\rho_{\rm ph}}, \varepsilon/2\right), \tag{30}$$

where N_t is the number of detected events with a tag of t, $\tilde{p}_{{\rm ph}|\rho_{\rm ph}} = p_{\rm ph}/(p_{\rm ph} + p_{\rm pos}/c_{\rm pos})$ and $\tilde{p}_{{\rm pos}|\rho_{\rm neg}} = 1 - p_{\rm neg}/(p_{\rm neg} + p_{\rm pos}c_{\rm neg}/c_{\rm pos})$.

In the analysis above, we have assumed that Alice and Bob reveal their choice of basis for all rounds, and then probabilistically assign all events such that $(j,s) \in \mathcal{Z}$ to either $\mathcal{T}$ or $\mathcal{K}$ with probabilities $p_{\mathcal{T}|\mathcal{Z}}$ and $p_{\mathcal{K}|\mathcal{Z}}$. However, note the following: (1) the probability to assign a particular emission to $\mathcal{T}$ or $\mathcal{K}$ must be independent of whether or not it is detected, since Eve has no information about this assignment when she makes her announcements; and (2) the set assigned to the undetected rounds is irrelevant, since their data is not used at any point in the analysis. This implies that it is only necessary for Alice and Bob to reveal their choice of basis in the detected rounds, and then assign each detected event such that $(j,s) \in \mathcal{Z}$ to either $\mathcal{T}_{\rm d}$ or $\mathcal{K}_{\rm d}$ with probabilities $p_{\mathcal{T}|\mathcal{Z}}$ and $p_{\mathcal{K}|\mathcal{Z}}$, respectively, where $\mathcal{T}_{\rm d}$ ($\mathcal{K}_{\rm d}$) is the set of detected test (key) rounds. By a similar argument, we conclude that Alice and Bob only need to reveal their choice of (j,s) for the emissions in $\mathcal{T}_{\rm d}$, and then assign each of them a tag of $t \in \{{\rm pos}, {\rm neg}\}$ with probability $p_{t|j,s,\mathcal{T}}$. For a full description of the protocol, including these assignments, see Appendix D.

Case in which Charlie reports several projections

The analysis above can be easily generalised to the case in which Charlie may report a projection to two or more Bell states. Essentially, the procedure is simply repeated separately for each successful projection announcement Ω. Note that, because the definition of a phase error depends on Ω, so does the operator associated with a phase error, which we now denote as $\rho_{{\rm ph}_\Omega}$. By repeating the procedure in Eqs. (23) to (27), we define the operators $\rho_{{\rm pos}_\Omega}$ and $\rho_{{\rm neg}_\Omega}$, and the coefficients $c_{{\rm pos}_\Omega}$ and $c_{{\rm neg}_\Omega}$, for each Ω. Then, we imagine that, for all Ω, Alice and Bob assign a tag $t_\Omega \in \{{\rm pos}_\Omega, {\rm neg}_\Omega\}$ to each emission in $\mathcal{T}$ with probability $p_{t_\Omega|j,s,\mathcal{T}}$, defined similarly to Eq. (29), in such a way that the average state with a tag of t_Ω is ρ_{t_Ω}. In the virtual protocol, we also imagine that Alice and Bob assign a tag $t_\Omega = {\rm ph}_\Omega$ to each emission of $\rho_{{\rm ph}_\Omega}$. Then, if Alice and Bob look only at the assigned tag of t_Ω, the scenario becomes equivalent to the "Tagged Virtual Protocol Ω", in which Alice and Bob emit ρ_{t_Ω} with probability p_{t_Ω}. Let N_{t_Ω} be the number of events with a tag of t_Ω in which Charlie announced Ω. Applying the results of Section I to the "Tagged Virtual Protocol Ω", we have that, except with probability ε_Ω,

$$\begin{aligned} N_{{\rm ph}_\Omega} \leq & g_U\Big(N_{{\rm pos}_\Omega} - g_L\big(N_{{\rm neg}_\Omega}, \tilde{p}_{{\rm pos}_\Omega|\rho_{{\rm neg}_\Omega}}, \varepsilon_\Omega/2\big), \\ & \tilde{p}_{{\rm ph}_\Omega|\rho_{{\rm ph}_\Omega}}, \varepsilon_\Omega/2\Big) := N^{\rm U}_{{\rm ph}_\Omega}, \end{aligned} \tag{31}$$

and because of the equivalence between the "Tagged Virtual Protocol Ω" and the virtual protocol, Eq. (31) must also hold for the latter, for all Ω. Thus, the total number of phase errors is upper bounded by

$$N_{\rm ph} \leq \sum_\Omega N^{\rm U}_{{\rm ph}_\Omega}, \tag{32}$$

except with probability $\varepsilon = \sum_\Omega \varepsilon_\Omega$. By a similar argument as in the main analysis above, we deduce that, in the actual protocol: (1) Alice and Bob only need to reveal their choice of basis in the detected rounds, and then assign each detected event such that $(j,s) \in \mathcal{Z}$ to either $\mathcal{T}_{\rm d}$ or $\mathcal{K}_{\rm d}$ with probabilities $p_{\mathcal{T}|\mathcal{Z}}$ and $p_{\mathcal{K}|\mathcal{Z}}$, respectively, where $\mathcal{T}_{\rm d}$ ($\mathcal{K}_{\rm d}$) is the set of detected test (key) rounds; and (2) Alice and Bob only need to reveal their choice of (j,s) for the emissions in $\mathcal{T}_{\rm d}$, and then assign each of them a tag of $t_\Omega \in \{{\rm pos}_\Omega, {\rm neg}_\Omega\}$ with probability $p_{t_\Omega|j,s,\mathcal{T}}$, where Ω is Charlie's announcement on that round.

IV. SECRET-KEY RATE AND SECURITY PARAMETER

In Sections II and III, we have shown how to obtain an upper bound $N^{\rm U}_{\rm ph}$ on the number of phase errors $N_{\rm ph}$ such that

$$\Pr\left[N^{\rm U}_{\rm ph} > N_{\rm ph}\right] \leq \varepsilon. \tag{33}$$

After calculating this bound, Alice and Bob perform error correction, error verification, and privacy amplification. They obtain a secret key of length

$$K = N_{\rm s}(1 - h(N_{\rm ph}/N_{\rm s})) - \lambda_{\rm EC} - \log_2\frac{1}{\epsilon_{\rm c}} - \log_2\frac{1}{\xi}, \tag{34}$$

where $N_{\rm s}$ is the length of the sifted key, $\lambda_{\rm EC}$ is the number of bits revealed in the error correction step, and $\epsilon_{\rm c}$ is the probability that Alice and Bob's keys will not be identical after the error verification step. It is known [5, 15] that, if the number of phase errors is bounded as in Eq. (33) and the secret-key length is set as in Eq. (34), then the protocol is $\epsilon_{\rm s}$-secret, with $\epsilon_s = \sqrt{2}\sqrt{\varepsilon + \xi}$. Since the protocol is also $\epsilon_{\rm c}$-correct, then it is $\epsilon_{\rm sec}$-secure, with $\epsilon_{\rm sec} = \epsilon_{\rm c} + \epsilon_{\rm s}$.

V. NUMERICAL RESULTS

In this section, we simulate the secret key obtainable for both the P&M and MDI LT protocols, using the analysis introduced in the previous sections. As usual, we assume the nominal scenario in which no eavesdropper is present. Moreover, we assume that the users' sources emit three different imperfectly-encoded single-photon states in the form

$$|\psi_j\rangle = \cos(\theta_j)\,|0_Z\rangle + \sin(\theta_j)\,|1_Z\rangle\,, \tag{35}$$

where $\{|0_Z\rangle, |1_Z\rangle\}$ forms a qubit basis, and $\theta_j \in [0, 2\pi)$ is the encoded phase. For the P&M scheme, we assume that Alice's states satisfy $\theta_{0Z} = 0$, $\theta_{1Z} = \kappa\pi/2$, and $\theta_{0X} = \kappa\pi/4$, where $\kappa = 1 + \delta/\pi$ and δ quantifies the magnitude of the SPFs. For the MDI setup, we assume that Alice's and Bob's states satisfy $\theta_0 = \theta'_0 = 0$, $\theta_1 = \theta'_1 = \kappa\pi/2$, $\theta_\tau = \kappa\pi/4$ and $\theta'_\tau = -\kappa\pi/4$, where θ_j (θ'_s) denotes the angle of Alice's (Bob's) state when she (he) emits state j (s).

To simulate the data that would be obtained in an experiment, we use the channel model in Ref. [17] for the P&M protocol, and the channel model in Appendix E for the MDI protocol. For simplicity, in the latter we assume that Charlie only announces a detection if he obtains a projection to the Bell state Ψ^-. The experimental parameters considered are: SPF's parameter $\delta = 0.126$, error correction inefficiency $f = 1.16$, dark count probability of the detectors $p_d = 10^{-8}$ and fiber loss coefficient $\alpha = 0.2$ dB/km. Moreover, we select the correctness and secrecy parameters to be $\epsilon_c = 10^{-8}$ and $\epsilon_\mathrm{s} = 10^{-8}$, respectively, and for simplicity we set $\xi = \varepsilon$ in Eq. (34), which means that $\varepsilon = \epsilon_\mathrm{s}^2/4$. In our simulations, we optimise over Alice and Bob's basis selection probabilities, and in the MDI protocol, we also optimise over the value of $p_{\mathcal{T}|\mathcal{Z}}$. Also, we consider different values of the block size N_tot, which represents the total number of rounds in the protocol. Finally, we assume an error-correction leakage of $\lambda_\mathrm{EC} = fh(e_Z)$ bits, where e_Z is the bit-error rate of the sifted key. The results for the P&M and the MDI LT protocols are shown in Fig. 4(a) and Fig. 4(b), respectively.

For completeness, we compare our results with those of an alternative analysis based on the application of Azuma's inequality. This alternative analysis, presented in Appendix F, is essentially a simplified version of the security proof in Ref. [13], which considers the emission of weak coherent pulses rather than single photons. The results in Fig. 4 show that our analysis based on random sampling offers significantly higher performances for both the P&M and MDI LT protocols. The difference in performance is larger for lower values of N_tot, while as N_tot increases, the two analyses slowly converge. In the case $N_\mathrm{tot} \to \infty$, both analyses provide a perfect estimation of the phase-error rate, and thus offer the same secret-key rate.

We note that a novel concentration inequality for sums of dependent random variables has been recently uploaded to a preprint server by Kato [24]. This result can be regarded as an improved version of Azuma's inequality that is much tighter when the success probability of the random variables is low. In Appendix F, we give a statement of the result, and use it to substitute Azuma's inequality in the alternative finite-key analysis of the LT protocol. However, it must be said that, when applied to QKD protocols, Kato's inequality requires an extra condition that is not needed in either our analysis based on random sampling or analyses based on Azuma's inequality. Namely, it requires users to attempt to predict the results that they expect to obtain in the experiment, before they actually run the experiment. This is an important step, since the inequality is only tight when the actual experimental data was reasonable close to their predictions [25].

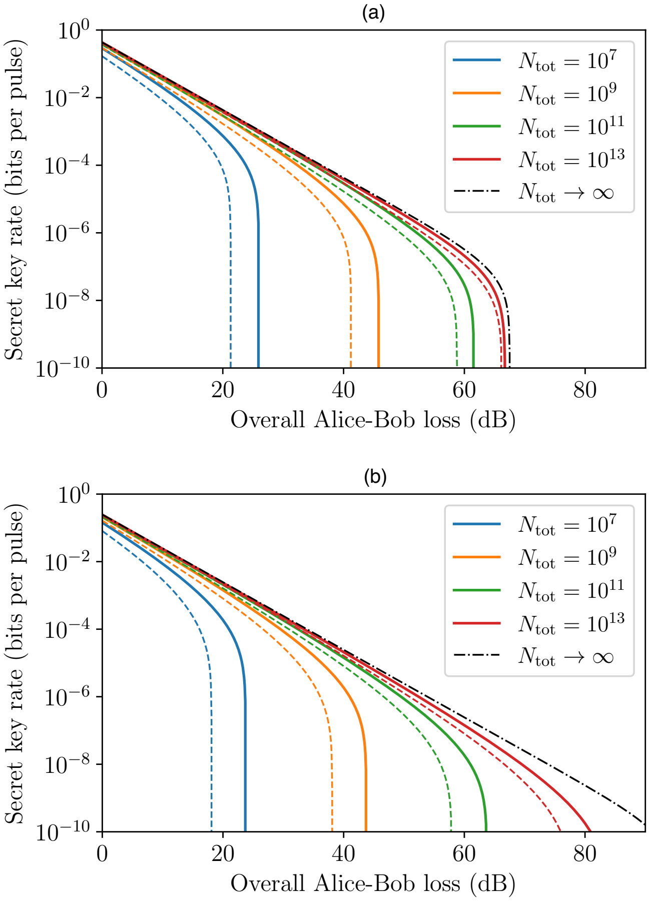

Figure 4. Secret-key rate obtainable using our analysis based on random sampling theory (solid lines), for the P&M (a) and MDI (b) LT protocols, as a function of the overall channel loss and for different values of the block size N_tot. For comparison, we include the secret-key rate obtainable using an alternative analysis based on Azuma's inequality (dashed lines), similar to that of Ref. [13]. For both LT protocols, our analysis clearly outperforms the alternative analysis based on Azuma's inequality.

In Fig. 5, we compare the performance of our analysis based on random sampling theory with that of our alternative analysis based on Kato's inequality. For simplicity, in the alternative analysis, we assume that the users could perfectly predict the experimental data that they obtain in the experiment, which maximises the secret-key rate obtainable. Fig. 5(a) shows that, in the case of the P&M protocol, the difference between the two analyses vanishes almost completely. Conversely, Fig. 5(b) shows that, in the case of the MDI protocol, our analysis based on random sampling still retains an advantage, although significantly smaller than that observed in Fig. 4(b). We emphasise that, unlike the alternative analysis based on Kato's inequality, our analysis based on random sampling does not require the users to make any prediction before running the experiment.

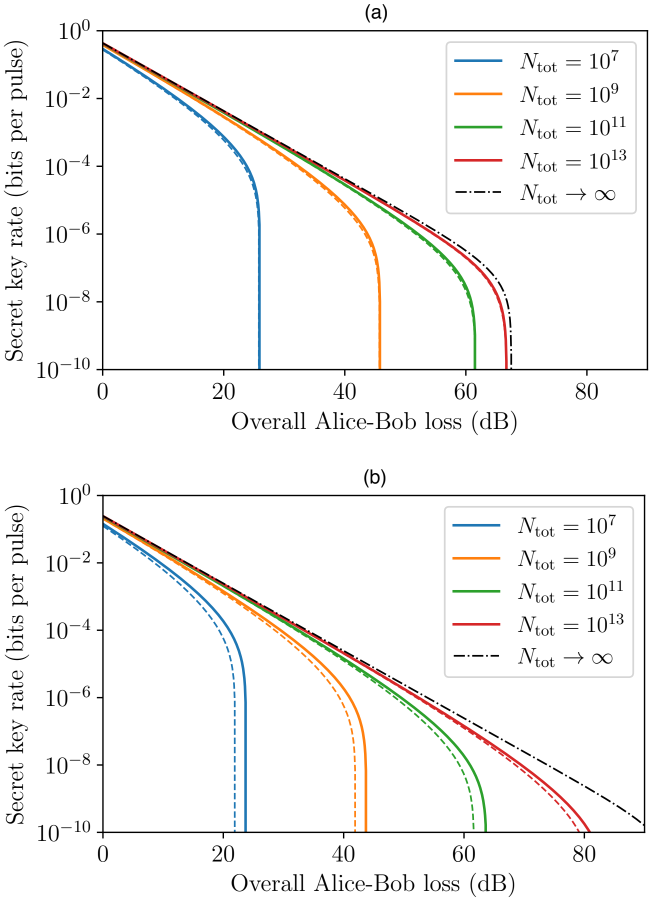

Figure 5. Comparison between the secret-key rate obtainable using our random sampling analysis (solid lines) and our alternative analysis based on the application of a novel concentration inequality for dependent random variables (dashed lines), for both the P&M (a) and MDI (b) versions of the LT protocol and different values of the block size $N_{\rm tot}$. For the P&M protocol, the performance of the two security proofs is almost identical, while for the MDI protocol, our analysis based on random sampling provides slightly better secret-key rates.

VI. DISCUSSION

In this work, we have proved the finite-key security of the loss-tolerant (LT) QKD protocol against general attacks, for both its prepare-and-measure and measurement-device-independent versions. Our security analysis reduces the parameter estimation task to a classical random sampling problem, which can be solved using Chernoff bounds, and provides higher secret-key rates than previous results based on the application of Azuma's inequality [13].

Although we have assumed single-photon sources, we believe that our analysis can be extended to the case in which the users employ weak coherent sources, as long as the single-photon components of the three encoded pulses satisfy the requirements of our proof, i.e. they are characterised and belong to the same qubit space. In that case, the users should assign tags to their emissions in such a way that Eq. (1) holds for their single-photon components; i.e. $\rho_{\rm vir}^{(1)} = c_{\rm pos}\rho_{\rm pos}^{(1)} - c_{\rm neg}\rho_{\rm neg}^{(1)}$, where $\rho_t^{(1)}$ is the average quantum state of a single-photon pulse with a tag of t. If so, Eq. (6) holds, although it now has the form $N_{\rm vir}^{(1)} \leq f(N_{\rm pos}^{(1)}, N_{\rm neg}^{(1)}; \varepsilon)$, where $N_t^{(1)}$ denotes the number of detected single-photon pulses with a tag of t. Note that now $N_{\rm pos}^{(1)}$ and $N_{\rm neg}^{(1)}$ are not directly observable, since the users do not know the photon number of their emissions. However, by using different laser intensities μ, they are able to observe the values $\{N_{\rm pos}^{\mu}\}$ and $\{N_{\rm neg}^{\mu}\}$ for all μ, where N_t^{μ} is the number of detected emissions with a tag of t that originated from intensity μ. Thus, they can apply the decoy-state method [26–29] to obtain an upper (lower) bound on $N_{\rm pos}^{(1)}$ ($N_{\rm neg}^{(1)}$), using for example the numerical techniques introduced in Ref. [30].

Also, in our random sampling analysis, we have assumed that the three encoded states live in the same qubit space. In a future work, it would be interesting to consider if our security proof can be extended to the case in which the qubit assumption is not satisfied, due to additional imperfections such as mode dependencies [17] or correlations between different rounds of the protocol [18, 19]. In that case, one can no longer derive an operator equality between the virtual and the actual states, such as e.g. Eq. (11). Instead, one needs to find an operator dominance condition [15] between them, which is non-trivial if the side-channel states are not characterised, as assumed by Refs. [17–19].

VII. ACKNOWLEDGEMENTS

We thank Mohsen Razavi and Marcos Curty for valuable discussions. G.C.-L. and M.P. acknowledge support from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement number 675662 (project QCALL). A.N. acknowledges support from a FPU scholarship (FPU 15/03668) from the Spanish Ministry of Science, Innovation and Universities (MCIU). K.T. acknowledges support from JSPS KAKENHI Grant Numbers JP18H05237 18H05237 and JST-CREST JPMJCR 1671. All data generated can be reproduced by the equations and the methodology introduced in this paper.

[1] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, The security of practical quantum key distribution, Rev. Mod. Phys. **81**, 1301 (2009).

[2] H.-K. Lo, M. Curty, and K. Tamaki, Secure quantum key distribution, Nat. Photonics **8**, 595 (2014).

[3] M. Koashi, Complementarity, distillable secret key, and distillable entanglement, arXiv:0704.3661 (2007).

[4] M. Koashi, Simple security proof of quantum key distribution based on complementarity, New J. Phys. **11**, 045018 (2009).

[5] M. Hayashi and T. Tsurumaru, Concise and tight security analysis of the Bennett–Brassard 1984 protocol with finite key lengths, New J. Phys. **14**, 093014 (2012).

[6] T. Tsurumaru, Leftover hashing from quantum error correction: Unifying the two approaches to the security proof of quantum key distribution, IEEE Trans. Inf. Theory **66**, 3465 (2020).

[7] C. H. Bennett and G. Brassard, Quantum cryptography: Public key distribution and coin tossing, in *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing* (1984) pp. 175–179.

[8] C.-H. F. Fung, X. Ma, and H. Chau, Practical issues in quantum-key-distribution postprocessing, Phys. Rev. A **81**, 012318 (2010).

[9] M. Tomamichel, C. C. W. Lim, N. Gisin, and R. Renner, Tight finite-key analysis for quantum cryptography, Nat. Commun. **3**, 634 (2012).

[10] K. Azuma, Weighted sums of certain dependent random variables, Tohoku Math. J. **19**, 357 (1967).

[11] J.-C. Boileau, K. Tamaki, J. Batuwantudawe, R. Laflamme, and J. M. Renes, Unconditional security of a three state quantum key distribution protocol, Phys. Rev. Lett. **94**, 040503 (2005).

[12] K. Tamaki, M. Curty, G. Kato, H.-K. Lo, and K. Azuma, Loss-tolerant quantum cryptography with imperfect sources, Phys. Rev. A **90**, 052314 (2014).

[13] A. Mizutani, M. Curty, C. C. W. Lim, N. Imoto, and K. Tamaki, Finite-key security analysis of quantum key distribution with imperfect light sources, New J. Phys. **17**, 093011 (2015).

[14] A. Mizutani, G. Kato, K. Azuma, M. Curty, R. Ikuta, T. Yamamoto, N. Imoto, H.-K. Lo, and K. Tamaki, Quantum key distribution with setting-choice-independently correlated light sources, npj Quantum Inf. **5**, 1 (2019).

[15] K. Maeda, T. Sasaki, and M. Koashi, Repeaterless quantum key distribution with efficient finite-key analysis overcoming the rate-distance limit, Nat. Commun. **10**, 1 (2019).

[16] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, Security of quantum key distribution with imperfect devices, Quantum Inf. Comput. **4**, 325 (2004).

[17] M. Pereira, M. Curty, and K. Tamaki, Quantum key distribution with flawed and leaky sources, npj Quantum Inf. **5**, 62 (2019).

[18] M. Pereira, G. Kato, A. Mizutani, M. Curty, and K. Tamaki, Quantum key distribution with correlated sources, Sci. Adv. **6**, eaaz4487 (2020).

[19] Á. Navarrete, M. Pereira, M. Curty, and K. Tamaki, Practical Quantum Key Distribution That is Secure Against Side Channels, Phys. Rev. Applied **15**, 034072 (2021).

[20] H.-K. Lo, M. Curty, and B. Qi, Measurement-device-independent quantum key distribution, Phys. Rev. Lett. **108**, 130503 (2012).

[21] F. Xu, K. Wei, S. Sajeed, S. Kaiser, S. Sun, Z. Tang, L. Qian, V. Makarov, and H.-K. Lo, Experimental quantum key distribution with source flaws, Phys. Rev. A **92**, 032305 (2015).

[22] Z. Tang, K. Wei, O. Bedroya, L. Qian, and H.-K. Lo, Experimental measurement-device-independent quantum key distribution with imperfect sources, Phys. Rev. A **93**, 042308 (2016).

[23] A. Boaron, G. Boso, D. Rusca, C. Vulliez, C. Autebert, M. Caloz, M. Perrenoud, G. Gras, F. Bussières, M.-J. Li, D. Nolan, A. Martin, and H. Zbinden, Secure quantum key distribution over 421 km of optical fiber, Phys. Rev. Lett. **121**, 190502 (2018).

[24] G. Kato, Concentration inequality using unconfirmed knowledge, arXiv:2002.04357 (2020).

[25] G. Currás-Lorenzo, Á. Navarrete, K. Azuma, G. Kato, M. Curty, and M. Razavi, Tight finite-key security for twin-field quantum key distribution, npj Quantum Information **7**, 1 (2021).

[26] W.-Y. Hwang, Quantum key distribution with high loss: Toward global secure communication, Phys. Rev. Lett. **91**, 057901 (2003).

[27] H.-K. Lo, X. Ma, and K. Chen, Decoy state quantum key distribution, Phys. Rev. Lett. **94**, 230504 (2005).

[28] X.-B. Wang, Beating the photon-number-splitting attack in practical quantum cryptography, Phys. Rev. Lett. **94**, 230503 (2005).

[29] X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, Practical decoy state for quantum key distribution, Phys. Rev. A **72**, 012326 (2005).

[30] M. Curty, F. Xu, W. Cui, C. C. W. Lim, K. Tamaki, and H.-K. Lo, Finite-key analysis for measurement-device-independent quantum key distribution, Nat. Commun. **5**, 1 (2014).

[31] Z. Zhang, Q. Zhao, M. Razavi, and X. Ma, Improved key-rate bounds for practical decoy-state quantum-key-distribution systems, Phys. Rev. A **95**, 012333 (2017).

[32] S. Bahrani, O. Elmabrok, G. Currás Lorenzo, and M. Razavi, Wavelength assignment in quantum access networks with hybrid wireless-fiber links, J. Opt. Soc. Am. B **36**, B99 (2019).

Appendix A: Random sampling analysis

Here, we prove the statements in Eqs. (3) and (4), and give an expression for the functions g_L and g_U. Let us assume that we have a population of n items, where n is unknown. Each item is assigned to either $\mathcal{K}_1$ with probability p or to $\mathcal{K}_2$ with probability $1-p$. We know the value of $K_2 = |\mathcal{K}_2|$ and we would like to obtain bounds on $K_1 = |\mathcal{K}_1|$.

Let $\xi_i = 1$ if the i-th trial is assigned to $\mathcal{K}_2$ and $\xi_i = 0$ otherwise. We have that

$$\sum_{i=1}^{n} \xi_i = K_2. \tag{A1}$$

Clearly, $\mathbb{E}[K_2] = (1-p)n$, and therefore $n = \mathbb{E}[K_2]/(1-p)$. Using the inverse multiplicative Chernoff bound [25, 31, 32], we have that

$$\begin{aligned} \mathbb{E}[K_2] &\geq -K_2 W_0 \left(-e^{\frac{\ln\varepsilon - K_2}{K_2}}\right) \\ \mathbb{E}[K_2] &\leq -K_2 W_{-1} \left(-e^{\frac{\ln\varepsilon - K_2}{K_2}}\right) \end{aligned} \tag{A2}$$

where W_0 and W_{-1} are branches of the Lambert W function, and each of the bounds fails with probability at most ε. From this and the fact that $n = K_1 + K_2$, we have that

$$\begin{aligned} K_1 = n - K_2 = \frac{\mathbb{E}[K_2]}{1-p} - K_2 &\geq \max\left(-\frac{K_2 W_0\left(-e^{\frac{\ln\varepsilon - K_2}{K_2}}\right)}{1-p} - K_2,\, 0\right) =: g_L(K_2, p, \varepsilon), \\ K_1 = n - K_2 = \frac{\mathbb{E}[K_2]}{1-p} - K_2 &\leq -\frac{K_2 W_{-1}\left(-e^{\frac{\ln\varepsilon - K_2}{K_2}}\right)}{1-p} - K_2 =: g_U(K_2, p, \varepsilon), \end{aligned} \tag{A3}$$

where each of the bounds fails with probability ε. It can be shown that g_U is an increasing function of K_2. Note that Eq. (A3) is only valid for $K_2 > 0$. In the special case $K_2 = 0$, we have that [31]

$$\begin{aligned} g_L(0, p, \varepsilon) &:= 0 \\ g_U(0, p, \varepsilon) &:= -\frac{\ln\varepsilon}{1-p}. \end{aligned} \tag{A4}$$

We note that this random sampling problem can also be solved using the method introduced in Ref. [15].

Appendix B: Operator-form linear relationship between the virtual and actual states

In this Appendix, we show how to find an operator-form linear relationship between the virtual states and the actual states, see Eq. (11) and Eq. (24). For simplicity, we provide first the procedure for the P&M protocol; then, at the end of this Appendix, we show how to extend it to the MDI case. The only assumption on Alice's emitted states, $\left|\psi_j\right\rangle_a$ for $j \in \{0_Z, 1_Z, 0_X\}$, is that they are linearly dependent, i.e. all three states live in the same qubit space. However, the analysis simplifies significantly if they are all in the same standard basis plane of the Bloch sphere, such as the XZ, XY or ZY plane. First, we consider this simpler case, and then provide the analysis for the general case.

1. Case in which all states are in a standard basis plane

Without loss of generality, we assume that the three states are in the XZ plane of the Bloch sphere, i.e. they can be expressed as

$$\left|\psi_j\right\rangle_a = \cos(\theta_j)\left|0_Z\right\rangle_a + \sin(\theta_j)\left|1_Z\right\rangle_a, \tag{B1}$$

where $\theta_j = (-\pi, \pi]$. Alice generates her sifted key from the detected emissions of $\left|\psi_{0_Z}\right\rangle_a$ and $\left|\psi_{1_Z}\right\rangle_a$. To prove the security of the sifted key, we consider an entanglement-based virtual protocol in which Alice prepares the state

$$\left|\Psi_Z\right\rangle_{Aa} = \frac{1}{\sqrt{2}}\left(\left|0_Z\right\rangle_A \left|\psi_{0_Z}\right\rangle_a + \left|1_Z\right\rangle_A \left|\psi_{1_Z}\right\rangle_a\right). \tag{B2}$$

In this virtual protocol, Alice measures her local ancilla A in the complementary basis $\{\left|0_X\right\rangle_A, \left|1_X\right\rangle_A\}$, where $\left|\alpha_X\right\rangle_A = 1/\sqrt{2}\left[\left|0_Z\right\rangle_A + (-1)^\alpha \left|1_Z\right\rangle_A\right]$ for $\alpha \in \{0, 1\}$. If Alice obtains $\left|\alpha_X\right\rangle_A$, she effectively emits the virtual state

$$\left|\psi_{\mathrm{vir}_\alpha}\right\rangle_a = \frac{1}{\sqrt{p_{\mathrm{vir}_\alpha|Z}}}\big(\left|\psi_{0_Z}\right\rangle_a + (-1)^\alpha \left|\psi_{1_Z}\right\rangle_a\big), \tag{B3}$$

where $p_{\mathrm{vir}_\alpha|Z} = \left\| \left|\psi_{0_Z}\right\rangle_a + (-1)^\alpha \left|\psi_{1_Z}\right\rangle_a \right\|^2/4 = (1 + (-1)^\alpha \cos(\theta_{0_Z} - \theta_{1_Z}))/2$ is the probability that Alice obtains $\left|\alpha_X\right\rangle_A$. Since $\left|\psi_{0_Z}\right\rangle_a$ and $\left|\psi_{1_Z}\right\rangle_a$ are in the XZ plane, $\left|\psi_{\mathrm{vir}_\alpha}\right\rangle_a$ is also in the XZ plane.

Let $[S_j^Z,\, S_j^X,\, S_j^Y]$ be the Bloch vector of the state $\left|\psi_j\right\rangle_a$. We have that $S_j^Z = \cos(2\theta_j)$, $S_j^X = \sin(2\theta_j)$ and $S_j^Y = 0$. Thus, in operator form, the state $\left|\psi_j\right\rangle_a$ can be expressed as

$$\rho_j \equiv \left|\psi_j\right\rangle\!\left\langle\psi_j\right|_a = \frac{1}{2}\big(\sigma_I + S_j^Z\sigma_Z + S_j^X\sigma_X\big), \qquad \text{(B4)}$$

where σ_I is the identity operator and σ_K, for $K \in \{Z, X, Y\}$, is a Pauli operator. It is useful to see Eq. (B4) as a system of linear equations, with three unknowns (σ_I, σ_Z, σ_X) and three equations (one for each $\left|\psi_j\right\rangle_a$). We can write this system in matrix form:

$$\boldsymbol{\rho} = \boldsymbol{S}\boldsymbol{\sigma}, \qquad \text{(B5)}$$

where $\boldsymbol{\rho} = [\rho_{0_Z},\, \rho_{1_Z},\, \rho_{0_X}]^{\mathrm{T}}$, $\boldsymbol{\sigma} = [\sigma_I,\, \sigma_Z,\, \sigma_X]^{\mathrm{T}}$, and

$$\boldsymbol{S} := \frac{1}{2}\begin{bmatrix} 1 & S_{0_Z}^Z & S_{0_Z}^X \\ 1 & S_{1_Z}^Z & S_{1_Z}^X \\ 1 & S_{0_X}^Z & S_{0_X}^X \end{bmatrix}; \qquad \text{(B6)}$$

and express its solution as

$$\boldsymbol{\sigma} = \boldsymbol{S}^{-1}\boldsymbol{\rho}. \qquad \text{(B7)}$$

Equation (B7) essentially says that the operators σ_I, σ_Z, σ_X can be expressed as a linear combination of the actual states ρ_j. This implies that every state that can be expressed as a linear combination of σ_I, σ_Z, σ_X (i.e., every state in the XZ plane) can also be expressed as a linear combination of ρ_j. In particular, the virtual states $\left|\psi_{\mathrm{vir}_\alpha}\right\rangle_a$ are in the XZ plane, and in operator form they can be expressed as

$$\rho_{\mathrm{vir}_\alpha} \equiv \left|\psi_{\mathrm{vir}_\alpha}\right\rangle\!\left\langle\psi_{\mathrm{vir}_\alpha}\right|_a = \frac{1}{2}\big(\sigma_I + S_{\mathrm{vir}_\alpha}^Z\sigma_Z + S_{\mathrm{vir}_\alpha}^X\sigma_X\big), \qquad \text{(B8)}$$

where $S_{\mathrm{vir}_0}^Z = -S_{\mathrm{vir}_1}^Z = \cos(\theta_{0_Z} + \theta_{1_Z})$ and $S_{\mathrm{vir}_0}^X = -S_{\mathrm{vir}_1}^X = \sin(\theta_{0_Z} + \theta_{1_Z})$. Or equivalently,

$$\rho_{\mathrm{vir}_\alpha} = \boldsymbol{S}_{\mathrm{vir}_\alpha}\boldsymbol{\sigma}, \qquad \text{(B9)}$$

where $\boldsymbol{S}_{\mathrm{vir}_\alpha} = \frac{1}{2}\left[1,\, S_{\mathrm{vir}_\alpha}^Z,\, S_{\mathrm{vir}_\alpha}^X\right]^{\mathrm{T}}$. Combining Eqs. (B7) and (B9), we have that

$$\rho_{\mathrm{vir}_\alpha} = \boldsymbol{S}_{\mathrm{vir}_\alpha}\boldsymbol{S}^{-1}\boldsymbol{\rho} = \boldsymbol{f}_\alpha\boldsymbol{\rho}, \qquad \text{(B10)}$$

where $\boldsymbol{f}_\alpha := \boldsymbol{S}_{\mathrm{vir}_\alpha}\boldsymbol{S}^{-1}$ is a row vector. If we express $\boldsymbol{f}_\alpha$ as $\boldsymbol{f}_\alpha = [c_{0_Z|\alpha},\, c_{1_Z|\alpha},\, c_{0_X|\alpha}]$, we obtain Eq. (11), i.e.

$$\rho_{\mathrm{vir}_\alpha} = c_{0_Z|\mathrm{vir}_\alpha}\rho_{0_Z} + c_{1_Z|\mathrm{vir}_\alpha}\rho_{1_Z} + c_{0_X|\mathrm{vir}_\alpha}\rho_{0_Z}, \qquad \text{(B11)}$$

for $\alpha \in \{0, 1\}$, as required.

In our numerical simulations, we assume that the three states emitted by Alice are in the XZ plane, and that when written as in Eq. (B1), their phases satisfy $\theta_{0_Z} = 0$, $\theta_{1_Z} = \kappa\pi/2$ and $\kappa\pi/4$, for some κ. For this particular case, an analytical expression for the coefficients is given by

$$\begin{aligned} &c_{0_Z|\mathrm{vir}_0} = c_{1_Z|\mathrm{vir}_0} = 0, \\ &c_{0_X|\mathrm{vir}_0} = 1, \\ &c_{0_Z|\mathrm{vir}_1} = c_{1_Z|\mathrm{vir}_1} = \csc^2(\kappa\pi/4))/2, \\ &c_{0_X|\mathrm{vir}_1} = -\cot^2(\kappa\pi/4)). \end{aligned}$$

2. General case

Here, we consider the case in which the three states are not all in the same standard basis plane. Formally, we assume that for all $K \in \{Z, X, Y\}$, there is at least one j such that $S_j^K \neq 0$. Therefore Eq. (B4) becomes

$$\rho_j \equiv \left|\psi_j\right\rangle\!\left\langle\psi_j\right|_a = \frac{1}{2}\big(\sigma_I + S_j^Z\sigma_Z + S_j^X\sigma_X + S_j^Y\sigma_Y\big), \qquad \text{(B12)}$$

and now we have a system of three equations with four unknowns. We have to find a way to modify Eq. (B12) such that it becomes a system with three unknowns.

For any basis $\{\left|0_U\right\rangle_a, \left|1_U\right\rangle_a\}$ of the qubit space, Alice's emitted states can be expressed as

$$\left|\psi_j\right\rangle_a = e^{i\gamma_j}\left(\sqrt{u_j}\left|0_U\right\rangle_a + e^{i\phi_j}\sqrt{1-u_j}\left|1_U\right\rangle_a\right). \qquad \text{(B13)}$$

where $0 \leq u_j \leq 1$, $\gamma_j \in [0, 2\pi)$, $\phi_j \in [0, 2\pi)$. Since the end points of the three Bloch vectors associated to Alice's emitted states form a plane, there must be a basis U such that u_j has the same value $\forall j$. Expressed in this basis, which we denote as $\tilde{Y}$, the states are

$$\left|\psi_j\right\rangle_a = e^{i\gamma_j}\left(\sqrt{\tilde{y}}\left|0_{\tilde{Y}}\right\rangle_a + e^{i\phi_j}\sqrt{1-\tilde{y}}\left|1_{\tilde{Y}}\right\rangle_a\right), \qquad \text{(B14)}$$

for some $0 \leq \tilde{y} \leq 1$. Let V be a unitary operator such that $V\left|0_Y\right\rangle_a = \left|0_{\tilde{Y}}\right\rangle_a$ and $V\left|1_Y\right\rangle_a = \left|1_{\tilde{Y}}\right\rangle_a$. V can be regarded as a transformation from the set of mutually unbiased bases Z, X, Y to the set of mutually unbiased bases $\tilde{Z}$, $\tilde{X}$, $\tilde{Y}$. Let us define the modified Pauli operators $\tilde{\sigma}_K = V\sigma_K V^\dagger$, for $K \in \{Z, X, Y\}$, and express the actual states in terms of these, i.e.

$$\rho_j = \frac{1}{2}\big(\sigma_I + \tilde{S}_Z^j\tilde{\sigma}_Z + \tilde{S}_X^j\tilde{\sigma}_X + \tilde{S}_Y^j\tilde{\sigma}_Y\big). \qquad \text{(B15)}$$

Note that the three states have the same $\tilde{Y}$ component, i.e. $\tilde{S}_Y^j = \tilde{S}_Y := 2\tilde{y} - 1$, $\forall j$. This allows us to define the operator $\tilde{\sigma}_O = \sigma_I + \tilde{S}_Y\tilde{\sigma}_Y$, and rewrite Eq. (B15) as

$$\left|\psi_j\right\rangle\!\left\langle\psi_j\right|_a = \frac{1}{2}\big(\tilde{\sigma}_O + \tilde{S}_Z^j\tilde{\sigma}_Z + \tilde{S}_X^j\tilde{\sigma}_X\big), \qquad \text{(B16)}$$

which has a similar form as Eq. (B4), i.e. it can be regarded as a linear system of three equations and three unknowns. If we define $\boldsymbol{\rho} = [\rho_{0_Z},\, \rho_{1_Z},\, \rho_{0_X}]^{\mathrm{T}}$, $\boldsymbol{\sigma} = [\tilde{\sigma}_O,\, \tilde{\sigma}_Z,\, \tilde{\sigma}_X]^{\mathrm{T}}$, and

$$\boldsymbol{S} := \frac{1}{2}\begin{bmatrix} 1 & \tilde{S}_{0_Z}^Z & \tilde{S}_{0_Z}^X \\ 1 & \tilde{S}_{1_Z}^Z & \tilde{S}_{1_Z}^X \\ 1 & \tilde{S}_{0_X}^Z & \tilde{S}_{0_X}^X \end{bmatrix}; \qquad \text{(B17)}$$

we have that $\boldsymbol{\rho} = \boldsymbol{S}\boldsymbol{\sigma}$, and therefore,

$$\boldsymbol{\sigma} = \boldsymbol{S}^{-1}\boldsymbol{\rho}. \tag{B18}$$

The previous equation implies that the modified Pauli operators $\tilde{\sigma}_O$, $\tilde{\sigma}_Z$, $\tilde{\sigma}_X$ can be expressed as a linear combination of the actual states ρ_j. Therefore, any state that can be expressed as a linear combination of $\tilde{\sigma}_O$, $\tilde{\sigma}_Z$, $\tilde{\sigma}_X$ (i.e. any state whose $\tilde{Y}$-component is $\tilde{S}_Y$) can also be expressed as a linear combination of the ρ_j.

If we define the virtual states as in Eq. (B3), it is likely that they will not satisfy the condition that their $\tilde{Y}$-component is $\tilde{S}_Y$. However, note that to obtain Eq. (B3), we have assumed that Alice measures the ancilla A of the entangled state in Eq. (B2) in the X basis. In reality, Alice could have decided to measure it in any other basis that is mutually unbiased with Z. Equivalently, we can express this degree of freedom by assuming that Alice does measure in the X basis, but defines the entangled state as

$$\left|\Psi_Z\right\rangle_{Aa} = \frac{1}{\sqrt{2}}\left(\left|0_Z\right\rangle_A \left|\psi_0\right\rangle_a + e^{i\phi}\left|1_Z\right\rangle_A \left|\psi_1\right\rangle_a\right), \tag{B19}$$

for some $\phi \in [0, 2\pi)$. Thus, the virtual states now become

$$\left|\psi_{\mathrm{vir}_\alpha}\right\rangle_a = \frac{1}{\sqrt{p_{\mathrm{vir}_\alpha|Z}}}\left(\left|\psi_0\right\rangle_a + (-1)^\alpha e^{i\phi}\left|\psi_1\right\rangle_a\right), \tag{B20}$$

where $p_{\mathrm{vir}_\alpha|Z} = \left\|\left|\psi_0\right\rangle_a + (-1)^\alpha e^{i\phi}\left|\psi_1\right\rangle_a\right\|^2/4$ is the probability that Alice obtains $\left|\alpha_X\right\rangle_A$. Substituting Eq. (B14) in Eq. (B20), one can easily show that if Alice chooses $\phi = \gamma_{0_Z} - \gamma_{1_Z} + (\phi_{0_Z} - \phi_{1_Z})/2$, then the modified Bloch vector of the virtual state $\left|\psi_{\mathrm{vir}_\alpha}\right\rangle_a$, $[\tilde{S}^Z_{\mathrm{vir}_\alpha}, \tilde{S}^X_{\mathrm{vir}_\alpha}, \tilde{S}^{\mathrm{vir}_\alpha}_Y]$, satisfies $\tilde{S}^{\mathrm{vir}_\alpha}_Y = \tilde{S}_Y$ for both $\alpha \in \{0,1\}$. Therefore

$$\rho_{\mathrm{vir}_\alpha} = \frac{1}{2}\left(\tilde{\sigma}_O + \tilde{S}^Z_{\mathrm{vir}_\alpha}\tilde{\sigma}_Z + \tilde{S}^X_{\mathrm{vir}_\alpha}\tilde{\sigma}_X\right), \tag{B21}$$

or equivalently,

$$\rho_{\mathrm{vir}_\alpha} = \boldsymbol{S}_{\mathrm{vir}_\alpha}\boldsymbol{\sigma}, \tag{B22}$$

where $\boldsymbol{S}_{\mathrm{vir}_\alpha} = \frac{1}{2}\left[1, \tilde{S}^Z_{\mathrm{vir}_\alpha}, \tilde{S}^X_{\mathrm{vir}_\alpha}\right]^{\mathrm{T}}$. Combining Eqs. (B18) and (B22), we have that

$$\rho_{\mathrm{vir}_\alpha} = \boldsymbol{S}_{\mathrm{vir}_\alpha}\boldsymbol{S}^{-1}\boldsymbol{\rho} := \boldsymbol{f}_\alpha\boldsymbol{\rho}, \tag{B23}$$

where $\boldsymbol{f}_\alpha := \boldsymbol{S}_{\mathrm{vir}_\alpha}\boldsymbol{S}^{-1}$ is a row vector. If we express $\boldsymbol{f}_\alpha$ as $\boldsymbol{f}_\alpha = [c_{0_Z|\alpha}, c_{1_Z|\alpha}, c_{0_X|\alpha}]$, we obtain Eq. (11), i.e.

$$\begin{aligned}\left|\psi_{\mathrm{vir}_\alpha}\middle\rangle\middle\langle\psi_{\mathrm{vir}_\alpha}\right|_a = c_{0_Z|\alpha}\left|\psi_{0_Z}\middle\rangle\middle\langle\psi_{0_Z}\right|_a + c_{1_Z|\alpha}\left|\psi_{1_Z}\middle\rangle\middle\langle\psi_{1_Z}\right|_a \\ + c_{0_X|\alpha}\left|\psi_{0_X}\middle\rangle\middle\langle\psi_{0_X}\right|_a,\end{aligned} \tag{B24}$$

for $\alpha \in \{0,1\}$, as required.

3. MDI protocol

In the MDI scenario, we essentially perform the above procedure separately for Alice's and Bob's states. Let $\left|\psi_j\right\rangle_a$ ($\left|\psi'_s\right\rangle_b$), with j $(s) \in \{0,1,\tau\}$, denote Alice's (Bob's) states, and let $\rho_j \equiv |\psi_j\rangle\langle\psi_j|$ ($\rho'_s \equiv |\psi'_s\rangle\langle\psi'_s|$) denote their operator form. Using the analysis in the previous sections, we have that

$$\begin{aligned}\rho_{\mathrm{vir}_\alpha} &= c_{0|\mathrm{vir}_\alpha}\rho_0 + c_{1|\mathrm{vir}_\alpha}\rho_1 + c_{0|\mathrm{vir}_\alpha}\rho_\tau, \\ \rho'_{\mathrm{vir}_\beta} &= c'_{0|\mathrm{vir}_\beta}\rho'_0 + c'_{1|\mathrm{vir}_\beta}\rho'_1 + c'_{0|\mathrm{vir}_\beta}\rho'_\tau;\end{aligned} \tag{B25}$$

where $\alpha, \beta \in \{0,1\}$, and $\rho_{\mathrm{vir}_\alpha}$ ($\rho'_{\mathrm{vir}_\beta}$) denotes one of Alice's (Bob's) virtual states, emitted with probability $p_{\mathrm{vir}_\alpha|\mathcal{K}}$ ($p'_{\mathrm{vir}_\beta|\mathcal{K}}$). We can define Alice and Bob's joint virtual states as

$$\rho_{\mathrm{vir}_{\alpha,\beta}} = \rho_{\mathrm{vir}_\alpha} \otimes \rho'_{\mathrm{vir}_\beta} = \sum_{j,s} c_{j,s|\mathrm{vir}_{\alpha,\beta}}\rho_{j,s}, \tag{B26}$$

emitted with probability $p_{\mathrm{vir}_{\alpha,\beta}|\mathcal{K}} = p_{\mathrm{vir}_\alpha|\mathcal{K}}p'_{\mathrm{vir}_\alpha|\mathcal{K}}$; where $c_{j,s|\mathrm{vir}_{\alpha,\beta}} = c_{j|\mathrm{vir}_\alpha}c'_{s|\mathrm{vir}_\beta}$. Depending on Charlie's Bell state report, the definition of a phase error will change. If Charlie reports a projection to either Ψ^- or Φ^-, the phase-error operator is defined as

$$\rho_{\mathrm{ph}} = (p_{\mathrm{vir}_{0,0}}\rho_{\mathrm{vir}_{0,0}} + p_{\mathrm{vir}_{1,1}}\rho_{\mathrm{vir}_{1,1}})/p_{\mathrm{ph}}, \tag{B27}$$

where $p_{\mathrm{ph}} = p_{\mathrm{vir}_{0,0}} + p_{\mathrm{vir}_{1,1}}$. Conversely, if he reports a projection to either Ψ^+ or Φ^+, the phase-error operator is defined as

$$\rho_{\mathrm{ph}} = (p_{\mathrm{vir}_{0,1}}\rho_{\mathrm{vir}_{0,1}} + p_{\mathrm{vir}_{1,0}}\rho_{\mathrm{vir}_{1,0}})/p_{\mathrm{ph}}, \tag{B28}$$

where $p_{\mathrm{ph}} = p_{\mathrm{vir}_{0,1}} + p_{\mathrm{vir}_{1,0}}$. In any case, one can express the phase-error operator as

$$\rho_{\mathrm{ph}} = \sum_{j,s} c_{j,s}\rho_{j,s}, \tag{B29}$$

where the coefficients $c_{j,s}$ are a linear function of the coefficients $c_{j,s|\alpha,\beta}$, and can be obtained by substituting Eq. (B26) in either Eq. (B27) or Eq. (B28).

In our numerical simulations we assume that Alice and Bob's states are in the XZ plane, and that when written as in Eq. (B1), their phases satisfy $\theta_0 = \theta'_0 = 0$, $\theta_1 = \theta'_1 = \kappa\pi/2$, $\theta_\tau = -\theta'_\tau = \kappa\pi/4$. For this particular case, we have that Alice's virtual states satisfy

$$\begin{aligned}&c_{0|\mathrm{vir}_0} = c_{1|\mathrm{vir}_0} = 0, \\ &c_{0|\mathrm{vir}_0} = 1, \\ &c_{0|\mathrm{vir}_1} = c_{1|\mathrm{vir}_1} = \csc^2(\kappa\pi/4))/2, \\ &c_{\tau|\mathrm{vir}_1} = -\cot^2(\kappa\pi/4);\end{aligned} \tag{B30}$$

while Bob's virtual states satisfy

$$\begin{aligned}
c'_{0|\mathrm{vir}_0} &= 1,\\
c'_{1|\mathrm{vir}_0} &= -c'_{\tau|\mathrm{vir}_0} = \frac{1}{1+2\cos(\kappa\pi/2)},\\
c'_{0|\mathrm{vir}_1} &= -\frac{\cos(\kappa\pi/2)\csc^2(\kappa\pi/4)}{2},\\
c'_{1|\mathrm{vir}_1} &= \frac{\cos(\kappa/2)\csc(\kappa\pi/4)\csc(3\kappa\pi/4)}{2},\\
c'_{\tau|\mathrm{vir}_1} &= \frac{\cot^2(\kappa\pi/4)}{1+2\cos(\kappa\pi/2)}.
\end{aligned} \tag{B31}$$

Appendix C: Description of the P&M protocol

(1) *Preparation*

For each round, Alice chooses a pure state $|\psi_j\rangle_a$ with probability p_j, where $j \in \{0_Z, 1_Z, 0_X\}$, and sends it to Bob through the quantum channel. Emissions of $|\psi_{0_X}\rangle_a$ ($|\psi_{0_Z}\rangle_a$ and $|\psi_{1_Z}\rangle_a$) are considered to belong to the X (Z) basis.

(2) *Detection*

Bob measures the incoming signals in either the Z or the X basis, which he chooses with probabilities p_Z and $p_X = 1 - p_Z$, respectively.

(3) *Sifting*

Bob announces which rounds were detected, and Alice and Bob reveal their basis choices in those rounds. Let $\mathcal{K}_Z$ be the set of detected rounds in which both users employed the Z basis, and let $\mathcal{T}_X$ be the set of detected rounds in which Bob employed the X basis. Then,

(3.1) Alice (Bob) defines her (his) sifted key as the bit values associated with her emissions (his measurement results) in the rounds in $\mathcal{K}_Z$.

(3.2) For all rounds in $\mathcal{T}_X$, Bob announces his measurement result.

(4) *Tag assignment*

Alice probabilistically assigns a tag to all rounds in $\mathcal{T}_X$, depending on her choice of state and Bob's measurement result. Namely, if she chose the state $|\psi_j\rangle_a$ and Bob obtained measurement result $(\alpha \oplus 1)_X$, for $\alpha \in \{0,1\}$, she assigns a tag of $t_\alpha \in \{\mathrm{pos}_\alpha, \mathrm{neg}_\alpha\}$ with probability $p_{t_\alpha|j,X_B}$, given by Eq. (17). Then, she calculates $N_{t_\alpha}^{(\alpha\oplus 1)_X}$, the number of detected events with a tag of t_α in which Bob obtained measurement result $(\alpha \oplus 1)_X$.

(5) *Parameter estimation*

Alice uses the values of $\{N_{t_\alpha}^{(\alpha\oplus 1)_X}\}$ to obtain an upper bound $N_{\mathrm{ph}}^{\mathrm{U}}$ on N_{ph}, the number of phase errors in her sifted key, using Eq. (21).

(6) *Postprocessing*

(6.1) *Error correction*: Alice sends Bob a prefixed amount λ_{EC} of syndrome information bits through an authenticated public channel, which Bob uses to correct errors in his sifted key.

(6.2) *Error verification*: Alice and Bob compute a hash of their error-corrected keys using a random universal hash function, and check whether they are equal. If so, they continue to the next step; otherwise, they abort the protocol.

(6.3) *Privacy amplification:* Alice and Bob extract a secret key pair (S_A, S_B) of length $|S_A| = |S_B| = \ell$ from their error-corrected keys using a random two-universal hash function.

Appendix D: Description of the MDI protocol

(1) *Quantum communication*

For each round, Alice (Bob) selects the state $|\psi_j\rangle_a$ ($|\psi'_s\rangle_b$) with probability p_j (p'_s), where j (s) $\in \{0, 1, \tau\}$, and sends it to an untrusted middle node Charlie, who announces whether or not he obtained a successful projection to a Bell state. Emissions for which $j \in \{0,1\}$ ($s \in \{0,1\}$) are considered to belong to the Z basis.

(2) *Sifting*

Alice and Bob announce their basis choices in the detected rounds. Then, they assign all detected rounds in which at least one of them used the X basis to set $\mathcal{T}_{\mathrm{d}}$. Also, for each detected round in which both chose the Z basis, they assign it to set $\mathcal{K}_{\mathrm{d}}$ with probability $p_{\mathcal{K}|\mathcal{Z}}$, or to set $\mathcal{T}_{\mathrm{d}}$ with probability $p_{\mathcal{T}|\mathcal{Z}} = 1 - p_{\mathcal{K}|\mathcal{Z}}$. Then, they announce these assignments, and

(2.1) Alice (Bob) defines her (his) sifted key as her (his) choices of j (s) in the rounds in $\mathcal{K}_{\mathrm{d}}$.

(2.2) For all rounds in $\mathcal{T}_{\mathrm{d}}$, Alice and Bob announce their choice of j and s.

(3) *Tag assignment*

Alice and Bob assign a tag $t \in \{\mathrm{pos}, \mathrm{neg}\}$ to each round in $\mathcal{T}_{\mathrm{d}}$ with probability $p_{t|j,s,\mathcal{T}}$, give by Eq. (29). Then, they calculate N_t, the number of detected events with a tag of t.

(4) *Parameter estimation*

Alice and Bob substitute the values of N_{pos} and N_{neg} in Eq. (30) to obtain an upper bound $N_{\mathrm{ph}}^{\mathrm{U}}$ on N_{ph}, the number of errors in the sifted key.

(5) *Postprocessing*

(5.1) *Error correction*: Alice sends Bob a prefixed amount λ_{EC} of syndrome information bits through an authenticated public channel, which Bob uses to correct errors in his sifted key.

(5.2) *Error verification*: Alice and Bob compute a hash of their error-corrected keys using a random universal hash function, and check whether they are equal. If so, they continue to the next step; otherwise, they abort the protocol.

(5.3) *Privacy amplification:* Alice and Bob extract a secret key pair (S_A, S_B) of length $|S_A| = |S_B| = \ell$ from their error-corrected keys using a random two-universal hash function.

Appendix E: Channel model for the MDI protocol

In this Appendix, we present the channel model used in our simulations of the MDI LT protocol, which is based on the single-photon version of the original MDI QKD scheme [20]. Specifically, we assume that Alice and Bob prepare polarised single-photon states in the form of Eq. (35), where here $|0_Z\rangle$ and $|1_Z\rangle$ denote the horizontally and vertically polarised single-photon states, respectively. After the preparation, Alice (Bob) sends the transmitted states to the intermediate party Charlie through a lossy quantum channel of transmittance η_A (η_B), who interferes the two incoming signals in a 50:50 beamsplitter, which has on each output port a polarising beamsplitter (PBS) that separates the horizontal and vertical modes. Now, let h_1 and v_1 (h_2 and v_2) be the threshold detectors placed at horizontal and vertical output port of the first (second) PBS, respectively, and let p_d be the dark-count probability of each detector. After the measurement, Charlie announces the Bell state Ψ^+ (Ψ^-) if he observes clicks in h_1 and v_1, or h_2 and v_2 (h_1 and v_2, or h_1 and v_2). Then, it is easy to prove that the conditional probability that Charles announces the Bell state $\Psi^{\pm}$ given that Alice and Bob selected the states $|\psi_j\rangle_a$ and $|\psi_s\rangle_b$, respectively, is

$$\begin{aligned}\mathrm{P}^{\Psi^{\pm}}_{j,s} &= (1-p_d)^2\Bigg[\frac{\eta_A\eta_B}{2}\sin^2(\kappa(\theta_j \pm \theta'_s)) \\ &+ p_d\frac{\eta_A\eta_B}{2}(1+\cos(2\kappa\theta_j)\cos(2\kappa\theta'_s)) \\ &+ p_d(1-\eta_A)\eta_B + p_d\eta_A(1-\eta_B) \\ &+ 2p_d^2(1-\eta_a)(1-\eta_b)\Bigg].\end{aligned} \tag{E1}$$

Appendix F: Alternative analysis using concentration inequalities for dependent random variables

In this Appendix, we present an alternative analysis that requires the application of a concentration inequality for sums of dependent Bernoulli random variables. This alternative analysis is a simplified version of that of Ref. [13], which considers the emission of weak coherent pulses rather than single photons. In Ref. [13], Azuma's inequality [10] is the concentration inequality applied. Here, we also present a new security proof based on the application of the recently proposed Kato's inequality [24]. First, we introduce the concentration inequalities that we consider, and then we provide the analysis.

1. Concentration inequalities

Let $\xi_1, ..., \xi_N$ be a sequence of Bernoulli random variables, and let $\Lambda_l = \sum_{u=1}^{l}\xi_u$. Let $\mathcal{F}_l$ be its natural filtration, i.e. the σ-algebra generated by $\{\xi_1, ..., \xi_l\}$.

a. Azuma's inequality

According to Azuma's inequality [10],

$$\begin{aligned}\Pr\left[\Lambda_n - \sum_{u=1}^{N}\Pr(\xi_u = 1|\mathcal{F}_{u-1}) \geq b\sqrt{N}\right] &\leq \exp\left[-\frac{b^2}{2}\right], \\ \Pr\left[\sum_{u=1}^{N}\Pr(\xi_u = 1|\mathcal{F}_{u-1}) - \Lambda_n \geq b\sqrt{N}\right] &\leq \exp\left[-\frac{b^2}{2}\right].\end{aligned} \tag{F1}$$

Equating the right hand sides to to ε_{A} and solving for b, we have that

$$\begin{aligned}\sum_{u=1}^{N}\Pr\left(\xi_u = 1|\xi_1, ..., \xi_{u-1}\right) &\leq \Lambda_N + \Delta_{\mathrm{A}}, \\ \Lambda_N &\leq \sum_{u=1}^{N}\Pr\left(\xi_u = 1|\xi_1, ..., \xi_{u-1}\right) + \Delta_{\mathrm{A}},\end{aligned} \tag{F2}$$

except with probability at most ε_{A} for each of the bounds, where $\Delta_{\mathrm{A}} = \sqrt{2N\ln\varepsilon_{\mathrm{A}}^{-1}}$.

b. *Kato's inequality*

According to Kato's inequality [24], for any n, and any a, b such that $b \geq |a|$,

$$\Pr\left[\sum_{u=1}^{N} \Pr(\xi_u = 1|\mathcal{F}_{u-1}) - \Lambda_N \geq \left[b + a\left(\frac{2\Lambda_N}{N} - 1\right)\right]\sqrt{N}\right] \leq \exp\left[\frac{-2(b^2 - a^2)}{(1 + \frac{4a}{3\sqrt{N}})^2}\right]. \tag{F3}$$

By replacing $\xi_l \to 1 - \xi_l$ and $a \to -a$ in Eq. (F3), we also derive [25]

$$\Pr\left[\Lambda_N - \sum_{u=1}^{N} \Pr(\xi_u = 1|\mathcal{F}_{u-1}) \geq \left[b + a\left(\frac{2\Lambda_N}{N} - 1\right)\right]\sqrt{N}\right] \leq \exp\left[\frac{-2(b^2 - a^2)}{(1 - \frac{4a}{3\sqrt{N}})^2}\right]. \tag{F4}$$

By isolating Λ_N in Eq. (F4), we derive,

$$\Pr\left[\Lambda_N \geq \frac{N}{\sqrt{N} - 2a}\left(\frac{1}{\sqrt{N}}\sum_{u=1}^{N} \Pr(\xi_u = 1|\mathcal{F}_{u-1}) + b - a\right)\right] \leq \exp\left[\frac{-2(b^2 - a^2)}{(1 - \frac{4a}{3\sqrt{N}})^2}\right], \tag{F5}$$

which holds when $a \leq \sqrt{N}/2$.

In the following, we will use Eq. (F3) to obtain an upper bound on $\sum_{u=1}^{N} \Pr(\xi_u = 1|\mathcal{F}_{u-1})$, Eq. (F4) to obtain a lower bound on $\sum_{u=1}^{N} \Pr(\xi_u = 1|\mathcal{F}_{u-1})$, and Eq. (F5) to obtain an upper bound on Λ_N.

Upper bound on the sum of probabilities

Before running the protocol, one should use previous knowledge of the channel to come up with a prediction $\tilde{\Lambda}_N$ of the value of Λ_N that one expects to obtain. Then, one calculates the values of a and b that would minimise the deviation term in Eq. (F3) if the realisation of Λ_N equalled $\tilde{\Lambda}_N$, for a fixed failure probability ε_{K}. These are the solution of the optimisation problem

$$\begin{aligned} \min_{a,b} \quad & \left[b + a\left(\frac{2\tilde{\Lambda}_N}{N} - 1\right)\right]\sqrt{N} \\ \text{s.t.} \quad & \exp\left[\frac{-2(b^2 - a^2)}{(1 + \frac{4a}{3\sqrt{N}})^2}\right] = \varepsilon_{\mathrm{K}}, \\ & b \geq |a|, \end{aligned} \tag{F6}$$

which can be expressed as

$$\begin{aligned} a &= \frac{3\left(72\sqrt{n}\tilde{\Lambda}_N(n - \tilde{\Lambda}_N)\ln\varepsilon_{\mathrm{K}} - 16N^{3/2}\ln^2\varepsilon_{\mathrm{K}} + 9\sqrt{2}(N - 2\tilde{\Lambda}_N)\sqrt{-N^2\ln\varepsilon_{\mathrm{K}}(9\tilde{\Lambda}_N(n - \tilde{\Lambda}_N) - 2N\ln\varepsilon_{\mathrm{K}})}\right)}{4(9N - 8\ln\varepsilon_{\mathrm{K}})(9\tilde{\Lambda}_N(n - \tilde{\Lambda}_N) - 2N\ln\varepsilon_{\mathrm{K}})}, \\ b &= \frac{\sqrt{18a^2N - (16a^2 + 24a\sqrt{n} + 9N)\ln\varepsilon_{\mathrm{K}}}}{3\sqrt{2N}}. \end{aligned} \tag{F7}$$

Then, we have that

$$\sum_{u=1}^{N} \Pr\left(\xi_u = 1|\xi_1, ..., \xi_{u-1}\right) \leq \Lambda_N + \Delta_K^{\mathrm{U}}, \tag{F8}$$

except with probability ε_{K}, where

$$\Delta_K^{\mathrm{U}} = \left[b + a\left(\frac{2\Lambda_N}{N} - 1\right)\right]\sqrt{N}. \tag{F9}$$

Lower bound on the sum of probabilities

Similarly to the previous case, one should use previous knowledge of the channel to come up with a prediction $\tilde{\Lambda}_N$ of the value of Λ_N that one expects to obtain after running the protocol. Then, one calculates the values of a and b that would minimise the deviation term in Eq. (F4) if the realisation of Λ_N equalled $\tilde{\Lambda}_N$, for a fixed failure probability ε_{K}. These are the solution of the optimisation problem

$$\begin{aligned} \min_{a,b} \quad & \left[b + a\left(\frac{2\tilde{\Lambda}_N}{N} - 1\right)\right]\sqrt{N} \\ \text{s.t.} \quad & \exp\left[\frac{-2(b^2 - a^2)}{(1 - \frac{4a}{3\sqrt{N}})^2}\right] = \varepsilon_{\mathrm{K}}, \\ & b \geq |a|, \end{aligned} \tag{F10}$$

which can be expressed as

$$a=\frac{3\left(-72\sqrt{N}\tilde{\Lambda}_N(n-\tilde{\Lambda}_N)\ln\varepsilon_{\mathrm{K}}+16N^{3/2}\ln^2\varepsilon_{\mathrm{K}}+9\sqrt{2}(N-2\tilde{\Lambda}_N)\sqrt{-N^2\ln\varepsilon_{\mathrm{K}}(9\tilde{\Lambda}_N(n-\tilde{\Lambda}_N)-2N\ln\varepsilon_{\mathrm{K}})}\right)}{4(9N-8\ln\varepsilon_{\mathrm{K}})(9\tilde{\Lambda}_N(n-\tilde{\Lambda}_N)-2N\ln\varepsilon_{\mathrm{K}})},$$
$$b=\frac{\sqrt{18a^2N-(16a^2-24a\sqrt{n}+9N)\ln\varepsilon_{\mathrm{K}}}}{3\sqrt{2N}}. \tag{F11}$$

Then, we have that

$$\sum_{u=1}^{N}\Pr\left(\xi_u=1|\mathcal{F}_{u-1}\right)\geq\Lambda_N-\Delta_K^{\mathrm{L}}, \tag{F12}$$

except with probability ε_{K}, where

$$\Delta_K^{\mathrm{L}}=\left[b+a\left(\frac{2\Lambda_N}{N}-1\right)\right]\sqrt{N}. \tag{F13}$$

Upper bound on the actual value

In this case, we assume that we have an upper bound S_N on the sum of probabilities $\sum_{u=1}^{N}\Pr\left(\xi_u=1|\mathcal{F}_{u-1}\right)$, and we want to obtain an upper bound on Λ_N. Before running the protocol one should use previous knowledge to come up with a prediction $\tilde{S}_N$ of the value of the upper bound S_N that one expects to obtain. Then, one calculates the values of a and b that would minimise the deviation term in Eq. (F5) if the prediction comes true. These are the solution of the optimisation problem

$$\begin{aligned}\min_{a,b}\quad & \frac{N}{\sqrt{N}-2a}\left(\frac{1}{\sqrt{N}}\tilde{S}_N+b-a\right)\\ \text{s.t.}\quad & \exp\left[\frac{-2(b^2-a^2)}{(1-\frac{4a}{3\sqrt{N}})^2}\right]=\varepsilon_{\mathrm{K}},\\ & b\geq|a|,\end{aligned} \tag{F14}$$

whose analytical solution is

$$a=\frac{3\sqrt{N}\left(9\ln\varepsilon_{\mathrm{K}}\left(3N^2-8N\tilde{S}_N+8\tilde{S}_N^2\right)+9(N-2\tilde{S}_N)\sqrt{N\ln\varepsilon_{\mathrm{K}}(N\ln\varepsilon_{\mathrm{K}}+18\tilde{S}_N(\tilde{S}_N-N))}+4n\ln^2(\varepsilon_{\mathrm{K}})\right)}{4\left(36\ln\varepsilon_{\mathrm{K}}\left(N^2-2N\tilde{S}_N+2\tilde{S}_N^2\right)+4N\ln^2\varepsilon_{\mathrm{K}}+81N\tilde{S}_N(N-\tilde{S}_N)\right)},$$
$$b=\frac{\sqrt{18a^2N-\left(16a^2-24a\sqrt{N}+9N\right)\ln\varepsilon_a}}{3\sqrt{2N}}. \tag{F15}$$

Then, we have that,

$$\Lambda_N\geq\frac{N}{\sqrt{N}-2a}\left(\frac{1}{\sqrt{N}}S_N+b-a\right), \tag{F16}$$

except with probability ε_{K}.

2. Analysis

We assume a virtual protocol in which Alice prepares N_{tot} copies of the entangled state in Eq. (10), and sends all subsystems B to Bob through the untrusted quantum channel. Then, Bob performs a quantum non-demolition measurement on each system B, learning which rounds produce a click on his detectors, and saving the system B of these detected rounds in a quantum memory. Let N be the number of detected rounds. For each detected round $u=\{1,2,\dots,N\}$, Alice measures her ancilla S, and Bob measures B in the X basis; except if Alice obtained $S=5$, in which case Bob measures B in the Z basis. Let $\xi_u=(i,j)$ represent the event "Alice learns that she emitted i and Bob obtains measurement result j". More specifically, Alice learns that she emitted $i=\{\mathrm{vir}_0,\mathrm{vir}_1,0_Z,1_Z,0_X\}$ if she obtained $S=\{0,1,2,3,4\}$ in her measurement of system S, respectively. Events in which she obtained $S=5$ are ignored in the analysis. Then, using the fact that the virtual states can be written as an operator-form linear function of the actual states as in Eq. (11), one can show that

$$\begin{aligned}&\sum_{u=1}^{N}\Pr[\xi_u=(\mathrm{vir}_\alpha,\,\alpha\oplus1)|\mathcal{F}_{u-1}]\\ &=\sum_{i=\{0_Z,1_Z,0_X\}}\frac{p_{\mathrm{vir}_\alpha}p_{Z_B}c_{i|\mathrm{vir}_\alpha}}{p_ip_{X_B}}\sum_{u=1}^{N}\Pr[\xi_u=(i,\,\alpha\oplus1)|\mathcal{F}_{u-1}],\end{aligned} \tag{F17}$$

where $\mathcal{F}_{u-1}$ is the σ-algebra generated by $\{\xi_1,...,\xi_{u-1}\}$. Now one needs to apply a concentration bound for sums of dependent random variables to substitute the sums of probabilities in Eq. (F17) by the actual values.

a. Using Azuma's inequality

Applying Eq. (F2) to Eq. (F17), we have that

$$N_{\mathrm{vir}_\alpha}^{\alpha\oplus 1} \leq \sum_{i=\{0_Z,1_Z,0_X\}} \frac{p_{\mathrm{vir}_\alpha} p_{Z_B} c_{i|\mathrm{vir}_\alpha}}{p_i p_{X_B}} (N_i^{\alpha\oplus 1} + \delta_i) + \Delta_{\mathrm{A}} \\ := \overline{N}_{\mathrm{vir}_\alpha}^{\alpha\oplus 1}, \tag{F18}$$

except with probability $4\varepsilon_{\mathrm{A}}$, where ε_{A} is the failure probability of each aplication of Azuma's inequality, which has been applied four times; and $\delta_i = \Delta_{\mathrm{A}}$ ($\delta_i = -\Delta_{\mathrm{A}}$) if $c_{i|\mathrm{vir}_\alpha}$ is positive (negative). Then, the number of phase errors is upper bounded by

$$N_{\mathrm{ph}} \leq \overline{N}_{\mathrm{vir}_0}^{1} + \overline{N}_{\mathrm{vir}_1}^{0}, \tag{F19}$$

except with probability $\varepsilon = 8\varepsilon_{\mathrm{A}}$.

Using a similar analysis, for the MDI protocol, we have that

$$N_{\mathrm{ph}} \leq \sum_{j,s} \frac{p_{\mathrm{ph}} c_{j,s}}{p_{j,s,\mathcal{T}}} (N_{j,s,\mathcal{T}} + \delta_{j,s}) + \Delta_{\mathrm{A}} \tag{F20}$$

except with probability $\varepsilon = 9\varepsilon_{\mathrm{A}}$, where $N_{j,s,\mathcal{T}}$ is the number of detected test rounds in which the user emitted $\left|\psi_{j,s}\right\rangle_{a,b}$, and $\delta_{j,s} = \Delta_{\mathrm{A}}$ ($\delta_{j,s} = -\Delta_{\mathrm{A}}$) if $c_{j,s}$ is positive (negative).

b. Using Kato's inequality

Applying Eq. (F8) and Eq. (F12) to Eq. (F17), we have that

$$\sum_{u=1}^{N} \Pr[\xi_u = (\mathrm{vir}_\alpha, \, \alpha\oplus 1)|\mathcal{F}_{u-1}] \\ \leq \sum_{i=\{0_Z,1_Z,0_X\}} \frac{p_{\mathrm{vir}_\alpha} p_{Z_B} c_{i|\mathrm{vir}_\alpha}}{p_i p_{X_B}} (N_i^{\alpha\oplus 1} + \delta_i) := S_{\mathrm{vir}_\alpha}, \tag{F21}$$

except with probability $3\varepsilon_{\mathrm{K}}$, where $\delta_i = \Delta_{\mathrm{K}}^{\mathrm{U}}$ ($\delta_i = -\Delta_{\mathrm{K}}^{\mathrm{L}}$) if $c_{i|\mathrm{vir}_\alpha}$ is positive (negative). Substituting $S_n \to S_{\mathrm{vir}_\alpha}$ and $\Lambda_n \to N_{\mathrm{vir}_\alpha}^{\alpha\oplus 1}$ in Eq. (F16), we obtain an upper bound $\overline{N}_{\mathrm{vir}_\alpha}^{\alpha\oplus 1}$ which fails with probability $4\varepsilon_{\mathrm{K}}$. Then, the number of phase errors is upper bounded by

$$N_{\mathrm{ph}} \leq \overline{N}_{\mathrm{vir}_0}^{1} + \overline{N}_{\mathrm{vir}_1}^{0}, \tag{F22}$$

except with probability $\varepsilon = 8\varepsilon_{\mathrm{K}}$.

Similarly, for the MDI protocol, we have that

$$\sum_{u=1}^{N} \Pr[\xi_u = \mathrm{ph}|\mathcal{F}_{u-1}] \leq \sum_{j,s} \frac{p_{\mathrm{ph}} c_{j,s}}{p_{j,s,\mathcal{T}}} (N_{j,s,\mathcal{T}} + \delta_{j,s}) := S_{\mathrm{ph}} \tag{F23}$$

except with probability $\varepsilon = 8\varepsilon_{\mathrm{A}}$, where $\delta_{j,s} = \Delta_{\mathrm{K}}^{\mathrm{U}}$ ($\delta_{j,s} = -\Delta_{\mathrm{K}}^{\mathrm{L}}$) if $c_{j,s}$ is positive (negative). Then, substituting $S_n \to S_{\mathrm{ph}}$ and $\Lambda_n \to N_{\mathrm{ph}}$ in Eq. (F16), we obtain an upper bound on N_{ph} which fails with probability $9\varepsilon_{\mathrm{K}}$.