Quantum One-Time Pad in the Presence of an Eavesdropper

Fernando G. S. L. Brandão and Jonathan Oppenheim

Phys. Rev. Lett. **108**, 040504 — Published 27 January 2012

DOI: 10.1103/PhysRevLett.108.040504

The quantum one-time pad in the presence of an eavesdropper

Fernando G.S.L. Brandão[1] and Jonathan Oppenheim[2]

[1]*Departamento de Física, Universidade Federal de Minas Gerais, Belo Horizonte, Caixa Postal 702, 30123-970, MG, Brazil*

[2]*Department of Applied Mathematics and Theoretical Physics, University of Cambridge U.K.*

A classical one-time pad allows two parties to send private messages over a public classical channel – an eavesdropper who intercepts the communication learns nothing about the message. A quantum one-time pad is a shared quantum state which allows two parties to send private messages or private quantum states over a public quantum channel. If the eavesdropper intercepts the quantum communication she learns nothing about the message. In the classical case, a one-time pad can be created using shared and partially private correlations. Here we consider the quantum case in the presence of an eavesdropper, and find the single letter formula for the rate at which the two parties can send messages using a general quantum state as a quantum one-time pad. Surprisingly, the formula coincides with the distillable entanglement assisted by a symmetric channel, an important quantity in quantum information theory, but which lacked a clear operational meaning.

PACS numbers:

If two parties wish to send private messages over a public channel, then they need to share a *one-time pad* or *key* – perfectly correlated and private strings which are as long as the messages they want to send. Often, the strings they share are not perfectly correlated or not completely secure e.g. if produced through a channel subject to wire-tapping. However, they can perform a protocol over the public channel to reconcile the errors in their strings, and amplify the privacy, so that they share a shorter string which is perfectly correlated and private. Given access to many independent realizations of some distribution P_{XYZ} shared between the two parties, Alice (X) and Bob (Y), and an eavesdropper Eve (Z), the rate $C(P_{XYZ})$ at which Alice can send private messages to Bob was derived in [1], based on a celebrated result due to Wyner and Csiszar & Korner [2, 3]. It reads [29]

$$C(P_{XYZ}) = \sup_{X\to V\to U} I(V:Y|U) - I(V:Z|U), \qquad (1)$$

with the conditional mutual information $I(V:Y|U) := H(VU) + H(YU) - H(VYU) - H(U)$, the Shannon entropy $H(X) := -\sum_x P_{X=x}\log P_{X=x}$ and the supremum taken over the Markov chain $X \to V \to U$.

As Equation (1) play such a central role in classical information theory, understanding it in the quantum case would be an important step. Even just defining the quantum version of this scenario is important conceptually, as there are several possibilities, and indeed, it was not even clear that a quantum version existed which would be closely analogous to the classical case. Given that privacy is such a key property of shared quantum states, understanding it from an information-theoretic point of view analogous to Eqn. (1) has been desirable. Indeed, privacy considerations have historically laid the foundations of quantum information theory – quantum key distribution [4] was one of the big motivations for the field, and the first entanglement distillation protocols [5] were inspired by the same classical privacy amplification protocols which attain Eqn. (1).

Here, we consider the quantum analog of the classical scenario: three parties, Alice, Bob and Eve, who instead of sharing a classical distribution, share a quantum state ψ_{ABE}. Alice then wishes to send private messages or private quantum states to Bob over a quantum public channel i.e. an insecure quantum channel where the eavesdropper might intercept the sent states. The question of how many private messages can be sent using a shared state was posed and answered by Schumacher and Westmoreland [6] in the case where initially the eavesdropper is uncorrelated with the two parties ($\psi_{ABE} = \psi_{AB}\otimes\psi_E$), and the sent messages are classical. They proved that the rate of classical private messages which can be sent is given by the quantum mutual information $I(A:B) := S(A) + S(B) - S(AB)$, with $S(A) = -\operatorname{Tr}(\rho_A\log\rho_A)$ the von Neumann entropy.

Here, we consider the general case where the two parties want to protect themselves against an eavesdropper who might be correlated with their state. We also extend the result to the case where the parties wish to send encrypted quantum states to each other, i.e. any d-dimensional input state ψ_K is encrypted so that during transmission it is indistinguishable from the maximally mixed state (I/d). This makes the scenario a more fully quantum version of the classical situation. We show, in surprising analogy with the classical case, that the rate Q that Alice can send encrypted messages to Bob using the state ψ_{ABE} is

$$C(\psi_{ABE}) = \sup_{A\to a\alpha} (I(a:B|\alpha) - I(a:E|\alpha)), \qquad (2)$$

with the conditional mutual information $I(a:B|\alpha) := S(a\alpha) + S(B\alpha) - S(aB\alpha) - S(\alpha)$ and the supremum taken over channels with input space A and output space $a\alpha$. The rate for sending encrypted quantum states, in turn, is given by $Q(\psi_{ABE}) = C(\psi_{ABE})/2$. Note that this optimisation is over single copies of the state ψ_{ABE}

making the result of Equation (2) *single-letter*. This is rare in quantum information theory, where usually the solutions are intractable, requiring optimisation over arbitrary many copies of the state [30].

Using simple entropic identities, one sees that the right hand side of Eq. (2) (divided by half) is equal to $\frac{1}{2}(I(a:B\alpha) - I(a:E\alpha))$, a quantity which has made an early appearance in Ref. [7] as the distillable entanglement assisted by *symmetric-side channels*. The identification of the optimal rates in the quantum one-time pad problem and in entanglement distillation assisted by a symmetric channel is not merely coincidental: to prove Eq. (2) we will show how an insecure quantum channel can, in a precise sense, *simulate* the action of a symmetric channel.

Statement of the problem. The scenario is as follows: Alice and Bob share many copies of a quantum system in a (generally mixed) state ψ_{AB} and since we want to protect against an arbitrary eavesdropper, we should imagine that Eve might have any state such that $\mathrm{Tr}_E\, |\psi\rangle_{ABE}\langle\psi|_{ABE} = \psi_{AB}$, i.e. the eavesdropper might hold a *purification* of Alice and Bob's state. Alice is given a message, either classical or quantum, which she should communicate to Bob. She is able to implement arbitrary quantum operations on her share $\psi_A^{\otimes n}$ of the state and any local ancillas, and she then sends a quantum system in state ρ_α to Bob down an insecure quantum channel, which might be intercepted by Eve. In the case where Eve intercepts ρ_α, she should learn an arbitrarily small amount of information about the message. In the case where Bob receives the state, he should be able to recover the message with probability converging to one in the limit of large n. More formally:

Definition 1 (private state transfer) *Consider the message state Ψ_{KR} shared between the sender Alice and a reference. Let Alice, Bob and Eve share the state $|\psi_{ABE}\rangle^{\otimes n}$ and have further registers a, α and b for Alice and Bob, respectively. Consider Alice's local operation (a completely positive trace preserving map) $\mathcal{M}_{\mathcal{A}} : AK \longrightarrow a\alpha$ and Bob's local operation $\mathcal{M}_{\mathcal{B}} : B\alpha \longrightarrow b$. Then a* private state transfer protocol *for Ψ_{KR} has error δ and security parameter ϵ, if*

$$\|\rho_{bR} - \Psi_{KR}\|_1 \leq \delta, \tag{3}$$

and

$$\|\tilde{\rho}_{RE\alpha} - \tilde{\rho}_R \otimes \tilde{\rho}_{E\alpha}\|_1 \leq \epsilon, \tag{4}$$

where

$$\rho_{Ra\alpha BE} := \mathcal{M}_A(\Psi_{KR} \otimes \psi_{ABE}^{\otimes n}), \tag{5}$$

and

$$\tilde{\rho}_{RabE} := \mathcal{M}_B \circ \mathcal{M}_A(\Psi_{KR} \otimes \psi_{ABE}^{\otimes n}). \tag{6}$$

For classical messages we let $\Psi_{KR} = \frac{1}{d}\sum_k |kk\rangle\langle kk|_{KR}$ and define the optimal rate $C(\rho_{AB})$ as the ratio of $\log(d)$ per n, for the largest d for which a private state transfer protocol is possible, with negligible error for asymptotic large n. For the optimal rate of quantum messages, in turn, we set $|\Psi_{KR}\rangle = \frac{1}{\sqrt{d}}\sum_k |k,k\rangle_{KR}$ and define $Q(\rho_{AB})$ as the asymptotic optimal ratio of $\log(d)/n$, over all private state transfer protocols.

Schumacher-Westmoreland scheme. To prove Eq. (2), we will make use of the result from [6] for the one-time-pad in the case where the message is classical and the state ρ_{AB} shared by Alice and Bob is not correlated with Eve. The main point of the argument is the construction of a set of quantum operations $\{\mathcal{E}_{k,n}\}$ on Alice's system and a probability distribution $\{p_{k,n}\}$ such that in the limit of large n,

$$\frac{1}{n}\chi(\{p_{k,n}, \mathcal{E}_{k,n} \otimes \mathrm{I}_B(\psi_{AB}^{\otimes n})\}) \to I(A:B)_\rho, \tag{7}$$

and

$$\frac{1}{n}\chi(\{p_{k,n}, \mathcal{E}_{k,n}(\psi_A^{\otimes n})\} \to 0, \tag{8}$$

where $\chi(\{q_k, \sigma_k\}) := S(\sum_k q_k\sigma_k) - \sum_k q_k S(\sigma_k)$ is the Holevo information [8]. By the HSW theorem [9] Alice can then send secret classical messages to Bob at a rate $I(A:B)$ by applying one of the $\mathcal{E}_{k,n}$ operations to her part of the state and sending it down the insecure channel. Eq. (7) guarantees that Bob is able to decode Alice's message in the case the channel is not tampered, while Eq. (8) ensures that Eve does not learn anything from the message being sent by intercepting the channel.

Mutual independence. A natural quantity which will arise in our discussion is the so-called *mutual independence* I_Λ [10], which we now define. Consider some sequence of maps $\Lambda^{(n)}$, from a restricted class of operations Λ, applied to subsystem AB with the property that

$$\rho_{ABE}^{(n)} := \Lambda^{(n)} \otimes \mathrm{I}_E(\psi_{ABE}^{\otimes n}) \tag{9}$$

is such that

$$\|\rho_{ABE}^{(n)} - \rho_{AB}^{(n)} \otimes \rho_E^{(n)}\|_1 \to 0. \tag{10}$$

Then

Definition 2 (mutual independence) *Given a state ψ_{AB}, consider a protocol from a class of operations Λ for extracting mutual independence $\mathcal{P} = \Lambda^{(n)}$. Define the rate*

$$R(\mathcal{P}, \rho_{AB}) := \liminf_{n\to\infty} \frac{1}{2} I(A:B)_{\Lambda^n(\psi_{AB}^{\otimes n})}. \tag{11}$$

Then we define the mutual independence rate of ψ_{AB} as

$$I_\Lambda(\rho_{AB}) := \sup_{\mathcal{P}} R(\mathcal{P}, \psi_{AB}). \tag{12}$$

The quantity I_Λ can be thought of as the rate of private mutual information that can be extracted from a state under the class of operations Λ. As an immediate consequence of Schumacher-Westmoreland construction and Definition 2, we find that $C(\psi_{AB})$ is lower bounded by $I_{\rm LO}(\psi_{AB})$, where LO is the class of local operations on Alice and Bob systems. It turns out, perhaps surprisingly, that local operations are not the right class of operations to be considered here.

As we show, the rate of private messages that can be sent is given by $I_{ss}(\psi_{AB})$, the mutual independence when Λ is the class of local operations assisted by a *symmetric-side channel*. This is a channel given by an isometry followed by partial trace $\psi_A \to {\rm Tr}_E\, \rho_{BE}$ such that ρ_{BE} is unchanged after interchanging system E with system B. In [11], it is shown that

$$I_{ss}(\psi_{AB}) = \sup_{A\to a\alpha} \frac{1}{2}(I(a:B|\alpha) - I(a:E|\alpha)) \qquad (13)$$

where the supremum is taken over channels $A \to a\alpha$.

Main result. We now show

Theorem 3

$$Q(\psi_{AB}) = C(\psi_{AB})/2 = I_{ss}(\psi_{AB}) \qquad (14)$$

Proof We begin by considering $C(\psi_{AB})$, i.e. Alice wishes to send Bob a private classical message, and will then prove the result for $Q(\psi_{AB})$. To see that $I_{ss}(\psi_{AB}) \geq C(\psi_{AB})/2$, consider an optimal protocol for $C(\psi_{AB})$, which can always be taken to be as follows: Alice applies the quantum operation $\mathcal{E}_{k,n} \otimes {\rm I}_{BE}$ with probability $p_{k,n}$, generating the ABE ensemble $\{p_{k,n}, \mathcal{E}_{k,n}(\psi_{ABE})\}$, with $\rho_\alpha = \mathcal{E}_{k,n}(\psi_A)$ being sent to Bob, and k the private message to be communicated. Then we have

$$C(\psi_{AB}) = \lim_{n\to\infty} \frac{1}{n} \chi(p_{k,n}, \mathcal{E}_{k,n} \otimes {\rm I}_B(\psi_{AB})). \qquad (15)$$

Consider the state after Alice's optimal local operation

$$\rho^n_{K\alpha BE} := \sum_{k=1}^{N} p_{k,n} |k\rangle_K\langle k| \otimes (\mathcal{E}_{k,n} \otimes {\rm I}_{BE})\,(\psi_{ABE}) \qquad (16)$$

Then, from Eq. (13) we get

$$I_{ss}(\psi_{AB}) \geq \frac{1}{2}\left(I(K:B\alpha)_\rho - I(K:E\alpha)_\rho\right). \qquad (17)$$

But $I(K:B\alpha)_\rho = \chi(p_{k,n}, \mathcal{E}_{k,n} \otimes {\rm I}_B(\psi_{AB}))$ and $I(K:E\alpha)_{\rho^n}/n \to 0$ with increasing n, since $\mathcal{E}_{k,n} \otimes {\rm I}_E(\psi_{AE})$ must satisfy Condition (4) and be asymptotically independent of k [31]. Therefore we get $I_{ss}(\psi_{AB}) \geq C(\psi_{AB})/2$.

Next we need to show that $I_{ss}(\psi_{AB}) \leq C(\psi_{AB})/2$. First, suppose that on top of the insecure ideal quantum channel Alice and Bob have access to a symmetric-side channel. Then they could distill $I_{ss}(\psi_{AB})$ of mutual independence, using the symmetric side-channel. They are now in the situation considered by Schumacher and Westmoreland, who showed that in the case where Alice and Bob are initially product with Eve, $C(\psi_{AB}) = I(A:B)$. Thus here we would get $C(\psi_{AB}) = 2I_{ss}(\psi_{AB})$ of secure classical communication.

Of course in the setting we are considering, they do not have access to the symmetric side-channel. However suppose Alice simulates locally the side-channel, sends the part that would go to Bob through the insecure quantum channel and traces out the part which would go to Eve. Then, on one hand, if Eve does not intercept the channel, Bob will get his share of what is send through the symmetric side-channel and they can distill at least $I_{ss}(\psi_{AB})$ of weak mutual independence and achieve the rate $C = 2I_{ss}(\psi_{AB})$. I.e. if Eve doesn't get her share of the output α' of the symmetric side-channel Alice and Bob can not be in a worse position than if she did receive it. On the other hand, if Eve intercepts the state sent through the insecure channel, then this is the same state she would get in the case they were connected by a symmetric side-channel (because what goes to Bob and Eve is symmetric), so Eve must still be decoupled from Alice's final state. This is so because Alice and Eve's state must be product in the end of the protocol for distilling mutual independence. Thus she gets no information about ρ_K.

This proves $C = 2I_{ss}(\psi_{AB})$. That $Q(\psi_{AB}) = C(\psi_{AB})/2$ comes from the fact that instead of using the quantum one-time pad to send private messages, Alice and Bob could just as well use it to share a classical private key $\sum |kk\rangle\langle kk|_{AB}/d^2$. This key can then be used to encrypt quantum states which can then be sent through the insecure quantum channel.

It is known [12–14] that the amount of key required to encrypt a state of dimension d is given by $2\log d$. In more detail, The procedure for encrypting a quantum state is for Alice to perform randomizing unitaries $\sum_k |k\rangle\langle k| \otimes U_k$ controlled on the classical key where U_k is a complete set of unitaries acting on the state she wants to encrypt. Bob can then decrypt the quantum state by performing $U_k^\dagger$. E.g. to encrypt a qubit, Alice acts one of the four Pauli operators ${\rm I}, \sigma_x, \sigma_y, \sigma_z$ with the choice of which operator to act decided by two bits of key. □

Note that when we are using the key to encrypt quantum states, we can modify the protocol slightly to include an authentication step [15, 16] so that if at some later point, Bob is allowed at least one bit of backwards communication, the key can be recycled [15, 17] and used to encrypt more quantum states. The bit of back-communication is required to signal to Alice that the protocol succeeded (i.e. that Eve didn't disturb the sent states too much) and is not part of the original scenario considered here. However, in such a case, one can prove that the one-time pad can be recycled in the case where we are using it to

send quantum states [17]!

A direct protocol. We can also construct a different protocol which encrypts quantum states directly using the one-time pad without first using it to create a classical key. This results in a saving of $\log d$ uses of the public quantum channel.

Recall that to create a classical key, Alice applies $\mathcal{E}_k \otimes \mathrm{I}_{BE}(\psi_{ABE}^{\otimes n})$ conditioned on a random classical variable k. To encrypt a quantum state directly, Alice applies $\mathcal{E}_k$ coherently, controlled on her half K of the entangled state $\psi_{KR} = \sum p_k |k\rangle_R |k\rangle_K$, i.e. she performs the operation $\sum |k\rangle\langle k|_K \otimes V_k$, where V_k is an isometric extension of the operation $\mathcal{E}_k$. This produces the total state $|\Psi\rangle = \sum p_k |k\rangle_R |k\rangle_K |\psi^k\rangle_{\alpha\alpha' BE}$ where $\rho^k_{\alpha'}$ is the local environment produced under the action of map $\mathcal{E}_k$ and ρ_α is its output. Alice then sends ρ_α to Bob, who can then coherently decode $\rho^k_{\alpha B}$ producing the state $\sum p_k |k\rangle_R |k\rangle_K |k\rangle_{B'} |\psi^0\rangle_{\alpha\alpha' BE}$. The protocol is thus far secure, because after tracing out system K, the state $\rho_{R\alpha E}$ is exactly the same as in the case of sending a classical message, and thus satisfies the privacy condition (4).

Since the state $\sum p_k |k\rangle_R |k\rangle_K |k\rangle_{B'}$ has $S(K|B') = 0$, Alice can *merge* [18] her share (K) of the state to Bob by performing a complete measurement in a random basis and communicating the result to Bob. In [18] it was shown that $S(K|B')$ is the amount of EPR pairs that is needed to send Alice's share K of $|\psi\rangle_{KB'R}$ by performing a measurement and if $S(K|B') = 0$, then no additional EPR pairs are needed. Alice's merging measurement completely decouples the K system from the reference, with the result that if Alice sends the remainder of her systems to Bob, the state must have been transmitted. She could also perform a measurement in the Fourier basis and communicate the result. Since the measurement is complete, the number of measurement outcomes is just $nH(K)$, and because we wish Eve to learn no information about the state, Alice needs to use an additional $nH(K)$ of the quantum one-time pad to encrypt the measurement result and send it.

Alice's measurement result is independent of the final state (as in teleportation [19]) so we can do the measuring and sending coherently, which will result in $nH(K)$ EPR pairs being created [20] in the case where Eve does not interfere with the channel. However, these EPR pairs can only be used at some later time if Bob verifies that he received them using an authentication scheme involving at least one bit of back-communication [16]. Note that if R is held by Alice, both protocols for sending quantum states can also be used to create secure EPR pairs between Alice and Bob.

The direct protocol for encrypting quantum states uses $\log d$ less uses of the channel than if we first create a classical key, and then send encrypted quantum states. As a result, $\log d$ less bits of key is left over if we are allowed back communication at some later point in time to recycle the key. This is in keeping with a fundamental law of privacy [17] relating sent qubits (δQ), the change in the amount of shared key (δK), and messages sent (δM) (whether they be classical or quantum):

$$\delta K \leq \delta Q - \delta M \ . \tag{18}$$

It is also worth noting the connection between merging, and encryption of the quantum states in this case. Encrypting the quantum state means that Alice's share of $|\Psi\rangle_{KR}$ should be *decoupled* from the reference R before being sent down the channel. At the same time, this decoupling of the reference from Alice's laboratory is the condition for Alice to succeed in sending her share [18, 21].

Approximate encryption with half key. As we have noted, the condition for decoupling system K from the reference R is that $2\log d$ unitaries are applied. It turns out there is a weaker form of quantum state encryption, where only slightly more than $\log d$ bits of key are used [22]. In such a case, the protocol is secure in the sense that if a measurement were to be performed on the reference system, then an eavesdropper would learn an arbitrary small amount about the measurement result. We say that the level of security we obtain is not *composable* [23, 24], meaning that if the reference system remains unmeasured, and the eavesdropper does not measure the parts of the quantum system she intercepted, then we may lose security if we use the encrypted state in another protocol.

We can easily construct an encryption scheme of this sort, by adapting the first protocol we presented, so that instead of choosing a complete set of $2\log d$ unitaries U_k which act on the state we are encrypting, we choose just over $\log d$ unitaries at random from the Haar measure [25]. Such a set is called *randomizing* rather than *completely randomizing*. It is unclear whether the direct protocol can be adapted in some way for approximate encryption. This is because the protocol uses merging, and thus the state to be sent must be completely decoupled from the reference system.

Discussion. There are essentially two ways we have used the quantum one-time pad. One way is to use ψ_{AB} to obtain a correlated and private key, and then use this key to encrypt messages (quantum or classical). The second, is a generalisation of Schumacher and Westmoreland [6] where the one-time pad is used directly to encrypt the message. This also holds true in the case of classical distributions.

Our results can also be applied to channel coding, where one has an authenticated noisy quantum channel, which produces the state ψ_{ABE}, and a public quantum channel. Here we have just taken ψ_{ABE} as a static resource, but we could have just imagined that it was produced by a channel from Alice to Bob and Eve. This

is perhaps closest to a quantum version of the Csiszar-Korner situation and gives a physical application to the results of [7, 11, 26], about state and channel capacities assisted by a symmetric-side channel.

We should thus think of a symmetric channel not as an exotic side-channel which can be used in conjunction with a standard quantum channel. Rather, results which make use of a symmetric channel can be applied to the situation where an eavesdropper might intercept the quantum systems that are sent down an insecure channel. This gives further motivation to the notion of the public quantum channel as emphasised in [11].

Acknowledgements. F.B. is supported by a fellowship "Conhecimento Novo" from Fundação de Amparo a Pesquisa do Estado de Minas Gerais (FAPEMIG). J.O. is supported by the Royal Society, and National Science Foundation under Grant No. PHY05-51164 during his stay at KITP.

[1] R. Ashlwede and A. Csiszar, IEEE Trans. Inf. Theory **39**, 1121 (1993).

[2] A. Wyner, Bell Sys. Tech. J **54**, 1355 (1975).

[3] I. Csiszar and J. Korner, IEEE Trans. Inf. Theory **24**, 339 (1978).

[4] C.H. Bennett and G. Brassard. Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, p. 175 (1984).

[5] C.H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J.A. Smolin, W.K. Wootters. Phys. Rev. Lett. **76**, 722 (1996).

[6] B. Schumacher and M. Westmoreland, Physical Review A **74**, 42305 (2006).

[7] G. Smith, J. A. Smolin, and A. Winter, IEEE Transactions on Information Theory **54**, 4208 (2008), quant-ph/0607039.

[8] A. S. Holevo, IEEE Trans. Inf. Theory **44**, 2818 (1998).

[9] B. Schumacher and M. Westmoreland, Phys. Rev. A **56**, 131 (1997).

[10] M. Horodecki, J. Oppenheim, and A. Winter (2009), arXiv:0902.0912.

[11] F.G.S.L. Brandão and J. Oppenheim. arXiv:1005:XXXX (2010).

[12] P. Boykin and V. Roychowdhury (2003), quant-ph/0003059.

[13] A. Ambainis, M. Mosca, A. Tapp, and R. de Wolf, in *FOCS '00: Proceedings of the 41st Annual Symposium on Foundations of Computer Science* (IEEE Computer Society, Washington, DC, USA, 2000), p. 547, ISBN 0-7695-0850-2, quant-ph/0003101.

[14] P. Hayden, D. Leung, P. W. Shor, and A. Winter, Commun. Math. Phys. **250**, 371 (2004), quant-ph/0307104.

[15] D. Leung, QIC **2**, 13 (2001).

[16] H. Barnum, C. Crepeau, D. Gottesman, A. Smith, and A. Tapp (2000), quant-ph/0205128.

[17] J. Oppenheim and M. Horodecki (2005), quant-ph/0306161.

[18] M. Horodecki, J. Oppenheim, and A. Winter, Nature **436**, 673 (2005), quant-ph/0505062.

[19] C. H. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres, and W. K. Wootters, Phys. Rev. Lett **70**, 1895 (1983).

[20] I. Devetak, A. Harrow, and A. Winter, Phys. Rev. Lett. **93**, 230504 (2004), quant-ph/0308044.

[21] M. Horodecki, J. Oppenheim, and A. Winter, Comm. Math. Phys. **269**, 107 (2006), quant-ph/0512247.

[22] P. Hayden, D. Leung, P. Shor, and A. Winter, Commun. Math. Phys. **250(2)**, 371 (2004).

[23] M. Ben-Or and D. Mayers, quant-ph/0409062.

[24] M. Ben-Or, M. Horodecki, D. W. Leung, D. Mayers, and J. Oppenheim, in *Theory of Cryptography: Second Theory of Cryptography Conference, TCC 2005* (2005), pp. 386–406, quant-ph/0409078.

[25] G. Aubrun, Communications in Mathematical Physics **288**, 1103 (2009).

[26] G. Smith, Physical Review A **78**, 22306 (2008).

[27] G. Smith, J.M. Renes, and J. Smolin. Phys. Rev. Lett. **100**, 170502 (2008).

[28] J. Renes and R. Renner. arXiv:1008.0452.

[29] In the case of one-way public communication from Alice to Bob and Eve. It is still an open question to determine a formula for the optimal rate in the case of two-way public communication.

[30] We note that the setting considered here is different from the standard setting considered e.g. in [27, 28]. There public communication is classical, while in our case it is quantum, in the form of an insecure (ideal) quantum channel. This is the reason why we can obtain a single-letter formula, while in the case of classical public communication, it is known that regularization is sometimes required [27].

[31] In more detail, Definition 1 gives $\|\rho^n_{\alpha E} - \rho^n_\alpha \otimes \rho^n_E\|_1 := \epsilon_n \to 0$. Then by Alicki-Fannes inequality [], $|I(K : E\alpha)_{\rho^n_{\alpha E}} - I(K : E\alpha)_{\rho^n_\alpha \otimes \rho^n_E}| \leq 4 \log |N| \epsilon_n$. Since $N = 2^{rn}$, for a $r \geq 0$, we find that $I(K : E\alpha)_{\rho^n}/n \to 0$.