

The quantum one-time pad and superactivation

Fernando G.S.L. Brandão and Jonathan Oppenheim

I. MAIN CONTRIBUTIONS IN A NUTSHELL

Before we turn to a more detailed exposition of our contributions, we outline the main results from [1], [2] below.

- We solve the *quantum one-time pad* in the presence of an eavesdropper. We find, in surprising analogy with the classical case, that the rate Q that Alice can send encrypted quantum states to Bob using the state ψ_{AB} with purification $|\psi\rangle_{ABE}$ (with the E system held by the eavesdropper) is

$$Q(\psi_{ABE}) = \sup_{A \rightarrow a\alpha} \frac{1}{2}(I(a : B|\alpha) - I(a : E|\alpha)), \quad (1)$$

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 which maps ψ_A to $\rho_{a\alpha}$. This is the quantum analog of the famous Csiszar & Korner quantity [4], [6] from classical information theory. It gives the rate at which we can perform privacy amplification and error correction on a quantum state using an insecure quantum channel.

- The optimal rate given in Eq. (1) is *additive* and *single-letter*, something extremely rare in quantum information theory, where regularisation over infinitely many uses of the channel/state is almost always required (to our knowledge the only other example is entanglement-assisted classical capacity of a quantum channel).
- In the optimal protocol for the quantum one-time pad we find that the insecure channel is only used to simulate a *symmetric-side* channel [3], a channel which maps the quantum information symmetrically to the receiver and the environment. Moreover the optimal rate formula Eq. (1) turns out to be equal to the distillable entanglement assisted by symmetric-side channel [3]. This had been introduced before as a calculational tool and was instrumental in proving superactivation of the quantum channel capacity [5]. Our work gives an *operational interpretation* to this quantity.
- We find the symmetric-side channel to be the quantum analogue of *public communication*, in the sense that both in the classical and in the quantum case of privacy amplification and error correction, public communication makes the theory simple and elegant, with the classical and quantum optimal rates having remarkable similarities. Conversely, in both classical and quantum cases the theory becomes much more complicated if public communication is not available.
- Smith and Yard's example of superactivation of the quantum capacity [5] were constructed by showing that the symmetric-side channel assisted capacity is at least half the private capacity of the channel. This suggested a connection of privacy and distillable entanglement under

public quantum communication. We show that such a relation indeed holds, in a relaxed sense: we prove that when assisted by a symmetric-side channel, the distillable entanglement becomes equal to two recent fully quantum notions of privacy, the mutual independence rate [7] and its weak variant [2], defined as the maximal mutual information attainable by Alice and Bob which is inaccessible to the environment. Thus we can understand the role of the symmetric-side channel in superactivation as making the conversion of private but noisy correlation, in the form of mutual independence, into private and perfect correlations, in the form of EPR pairs.

In conclusion, insights from cryptography are invaluable in gaining a further understanding of quantum information theory, in a number of ways. In fact, the similarity between entanglement and private correlations was used in constructing the first entanglement distillation protocols, and has been used to conjecture new types of classical distributions. However, the insight had previously been that from an informational perspective, quantum states were like private distributions while classical communication acted like public communication. However, we now see that the more accurate analogue is that instead of a classical channel, we should consider the quantum public channel. As soon as we do so, we recover a capacity formula which is equivalent to its classical counterpart, and which, remarkably is additive and single-letter. What is more, the capacity of the one-time pad is equal to the superactivation rate of the symmetric side channel, which had previously been a surprising phenomena, but in this context has a natural explanation. We thus see that as soon as we introduce the notion of quantum public communication, quantum information theory becomes far more tractable and closer to the classical theory. We believe that this is such a natural setting, that it will enable us to better understand other previously intractable aspects of information carried by quantum systems.

II. BACKGROUND

Suppose two trusted parties, Alice and Bob, and a malicious third party, Eve, share noisy classical correlations given by a joint probability distribution P_{XYZ} and Alice and Bob would like to extract key from their common randomness. A key resource in this paradigm is *public communication*, which is conveniently represented by a symmetric broadcast channel which delivers the same information to Bob and Eve

In the *one-way* public communication scenario, only Alice is able to send public messages to Bob and Eve. In this case the distillable secret-key rate of the distribution P_{XYZ} (when the parties are given infinitely many independent realizations of it) is given by the celebrated formula [6], [4], [9]

$$C(P_{XYZ}) = \sup_{X \rightarrow V \rightarrow U} I(V : Y|U) - I(V : Z|U), \quad (2)$$

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 $X \rightarrow V \rightarrow U$.

The formula in Eq. (2) is so-called *single-letter*, meaning that an optimization over a single copy of the probability distribution gives the asymptotic rate. Moreover it is *additive*, i.e. for two probability distributions P_{XYZ} and $Q_{X'Y'Z'}$, $C(P_{XYZ} \otimes Q_{X'Y'Z'}) = C(P_{XYZ}) + C(Q_{X'Y'Z'})$ [6]. We can then say that Eq. (2) completely characterizes how to optimally distill secret-key in the one-way scenario.

In quantum information theory, the paradigm described above has two natural analogues, and both have been extensively analysed [10], [11], [12]. The first is to distill a secret-key from a tripartite quantum state $|\psi_{ABE}\rangle$ shared by Alice, Bob and Eve [12]. Alice and Bob can perform any operation allowed by quantum mechanics on their shares of the state, while (in the one-way setting considered here) Alice can communicate public *classical* messages to Bob and Eve. The second is entanglement distillation [10], in which Alice and Bob wish to distill Einstein-Podolsky-Rosen (EPR) pairs from a shared state ψ_{AB} by local quantum operations and, again, *classical* communication from Alice to Bob (here too, although not needed, one can consider that an eavesdropper has a purification of ψ_{AB} i.e. a pure state ψ_{ABE} such that $\psi_{AB} = \text{tr}_E \psi_{AB}$, and Eve learns all the classical communication that Alice sends to Bob).

In both paradigms, the shared randomness is extended from the original classical probability distribution to a quantum state. The public communication, however, remains the same; even in the quantum case only classical messages can be publicly communicated. A natural question then emerges: is there a meaningful notion of *public quantum communication*?

III. THE QUANTUM ONE-TIME PAD IN THE PRESENCE OF AN EAVESDROPPER

We consider now the quantum *one-time pad* problem [1] in the presence of an eavesdropper. The setting is as follows: Alice would like to send to Bob secret classical or quantum messages, using an ideal, but insecure, quantum channel which might be intercepted by an eavesdropper, who should not be able to learn anything about the message being sent.

Alice and Bob can make use of the insecure channel for secure communication if they share in addition a *secret-key*. Then using their secret correlations Alice can encode the message in a way that (i) Bob can decode it in the case that Eve does not intercept the states sent down the insecure quantum channel and (ii) Eve cannot distinguish the different messages if she intercepts the sent states. The raw key may initially be noisy and correlated with an eavesdropper – i.e. we assume that the raw key is given by (several copies of) a quantum state $|\psi_{ABE}\rangle$ shared by Alice, Bob and Eve and the question is to find out what is the optimal rate at which the state can be used to encrypt classical or quantum messages.

This problem was first considered in the noiseless case, in which Alice and Bob share perfect classical key or EPR pairs [15], [16], [17]. In Ref. [18], in turn, Schumacher and

Westmoreland analysed the case in which Alice and Bob shared a mixed bipartite quantum state ψ_{AB} , which is not correlated with the eavesdropper. Interestingly, they found the optimal rate at which the state can be used as a one-time-pad for classical messages to be given by the quantum mutual information of ψ_{AB} : $I(A : B)_\psi = S(A)_\psi + S(B)_\psi - S(AB)_\psi$.

In [1] we considered the general case, in which Alice and Bob have an arbitrary quantum state, in general correlated with Eve. We found that the optimal rate at which the state can be used as a one-time-pad for quantum information turns out to be given by the single-letter, additive expression of Eq. (1) This expression is formally equivalent to the classical expression given by Eq. (2).

A. Symmetric-side Channels

The rate given by Eq. (1) has appeared in the literature before – as the quantum capacity assisted by symmetric side-channels [3].

$$D_{ss}(\psi_{AB}) = \sup_{A \rightarrow a\alpha} \frac{1}{2} (I(a : B|\alpha) - I(a : E|\alpha)), \quad (3)$$

with the supremum taken over all channels which maps A to $a\alpha$. It is intriguing that it is the symmetric-side channel assisted distillable entanglement that appears as the optimal rate in our setting, even though the problem makes no mention in any way of the symmetric-side channel.

The proof of our result reveals an interesting aspect of this task: the insecure quantum channel is only ever used to simulate a symmetric-side channel, meaning that in the optimal protocol Alice first locally simulates a symmetric-side channel, sends through the insecure channel the part of the symmetric-side channel's output which would go to Bob, and traces out the part that would go to Eve. It thus follows that there is no difference if Alice and Bob are connected by an insecure ideal channel or a symmetric-side channel!

We can therefore consider the quantum one-time-pad as an operational setting where the idea of a symmetric-side channel as public quantum communication naturally appears. In the same way a broadcast channel (which sends the same information to the two receivers) is employed as a model of a classical public communication channel, the quantum *symmetric-side* channel appears to be a model of quantum public communication.

Symmetric-side channels were introduced by Smith, Smolin and Winter [3] with the goal of obtaining a more tractable upper bound on the quantum capacity of quantum channels. They analysed how assistance by a symmetric-side channel could improve the quantum channel capacity and the (one-way) distillable entanglement. Here we see that assistance by symmetric side-channels is far more than a tool for computing upper-bounds on the capacity.

IV. SUPERACTIVATION OF THE CHANNEL CAPACITY

There is another line of investigation in which symmetric-side channels have been shown very useful: in exhibiting examples of non-additivity of the quantum channel capacity [5]. By the no-cloning theorem [13], [14], the symmetric-side

channel can be seen to have zero quantum capacity. However, in [5] Smith and Yard noted that a consequence of Eq. (3) and the formula of [11] for the one-way distillable secret-key rate (K_{\rightarrow}) is

$$D_{ss}(\psi_{AB}) \geq K_{\rightarrow}(\psi_{AB})/2, \quad (4)$$

for all bipartite states ψ_{AB} . The equation above is striking because there are examples of states for which the distillable entanglement is zero, but the distillable secret-key is not [19], [20], [12]. In this way we find an example of two quantum channels each with zero quantum capacity, but whose tensor product has positive quantum capacity. This effect has been termed the *superactivation* of the quantum capacity.

Equation (4) shows a curious property of the symmetric-side channel: it allows the conversion of secret-key into EPR pairs (at half the rate). An interesting question, raised already in [5] and further explored in [21], [22], [23], asks whether there is a more fundamental relation between entanglement and secrecy in the presence of symmetric-side channels. For instance, might the distillable entanglement and distillable secret-key, when assisted by symmetric-side channels, become the same? Although it is rather unlikely that this is the case it turns out that a relaxed version of the statement *is* true.

In order to formalize this result, we consider a recently introduced version of quantum privacy. The usual definition of secret-key consists of two requirements: (i) Alice and Bob systems should be classical, and perfectly correlated and (ii) their state should not be correlated in any way with the eavesdropper. A relaxed and fully quantum definition of private correlations has been introduced [7], in which only the second requirement is kept. Then given a bipartite quantum state ψ_{AB} , the degree of (potentially noisy) private correlations of Alice and Bob, termed *mutual independence* ($I_{\text{ind}}(\psi_{AB})$), is given by (half) the mutual information of a state extracted by Alice and Bob which is product with Eve's state, who is assumed to hold a purifying state for ψ_{AB} .

In [2] we introduced an even more relaxed notion of private correlations, which we call *weak mutual independence*. Its definition is almost the same as that of mutual independence, but here we only require that Alice's state is completely decoupled from Eve's. In the setting where no classical communication is allowed, the optimal protocol is just for Alice to split her system in two and trace out one of them, making herself product with Eve and at the same time trying to retain as much mutual information as possible with Bob. We can then see this quantity as a measure of Alice's ability to perform quantum privacy amplification against the eavesdropper.

Armed with these definitions we can state our main result concerning activation of the channel capacity and distillable entanglement: When assisted by a symmetric-side channel, the weak mutual independence rate ($W_{\text{ind},ss}$), the mutual independence rate ($I_{\text{ind},ss}$), and the distillable entanglement (D_{ss}) become the same, i.e. for every state ψ_{AB}

$$W_{\text{ind},ss}(\psi_{AB}) = I_{\text{ind},ss}(\psi_{AB}) = D_{ss}(\psi_{AB}). \quad (5)$$

The introduction of the symmetric side-channel makes the theory far more elegant. We note that an analogous equation holds true classically, if we replace distillable entanglement

by distillable secret-key and redefine the two mutual independence rates removing the half factor presented in the quantum case and using the correspondence quantum/classical public communication.

Eq. (5) also shows that when looking for more superactivation protocols with the symmetric-side channel, it suffices to focus on the rather indiscriminate task of making part of Alice's state product with the environment.

REFERENCES

- [1] F.G.S.L. Brandão and J. Oppenheim. The quantum one-time pad in the presence of an eavesdropper. arXiv:1004.3328.
- [2] F.G.S.L. Brandão and J. Oppenheim. Public Quantum Communication and Superactivation. arXiv:1005.1975.
- [3] G. Smith, J.A. Smolin, A. Winter. The quantum capacity with symmetric side channels. IEEE Trans. Info. Theory **54**, 9, 4208 (2008).
- [4] I. Csiszar and J. Korner. Broadcast Channels with Confidential Messages. IEEE Trans. Inf. Theory **24**, 339 (1978).
- [5] G. Smith and J. Yard. Quantum Communication With Zero-Capacity Channels. Science **321**, 1812 (2008).
- [6] R. Ahlswede and I. Csiszar. Common Randomness in Information Theory and Cryptography Part II. IEEE Trans. Inf. Theory **39**, 1121 (1993).
- [7] M. Horodecki, J. Oppenheim, A. Winter. Quantum Mutual Independence. arXiv:0902.0912v2 [quant-ph].
- [8] U.M. Maurer. Secret Key Agreement by Public Discussion from Common Information. IEEE Trans. Info. Theory **39**, 733 (1993).
- [9] A. D. Wyner. The wire-tap channel. Bell Sys. Tech. J. **54**, 1355 (1975).
- [10] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki. Quantum Entanglement. Rev. Mod. Phys. Vol. 81, No. 2, pp. 865-942 (2009).
- [11] I. Devetak and A. Winter. Distillation of secret key and entanglement from quantum states. Proc. R. Soc. Lond. A **461**, 207 (2005).
- [12] K. Horodecki, M. Horodecki, P. Horodecki, and J. Oppenheim. General paradigm for distilling classical key from quantum states. IEEE Trans. Inf. Theory **55**, 1898 (2009).
- [13] W.K. Wootters and W.H. Zurek. A Single Quantum Cannot be Cloned. Nature **299**, 802 (1982).
- [14] D. Dieks. Communication by EPR devices. Physics Letters A **92**, 271 (1982).
- [15] P.O. Boykin and V. Roychowdhury. Optimal encryption of quantum bits. Phys. Rev. A **67**, 042317 (2003).
- [16] A. Ambainis, M. Mosca, A. Tapp, R. de Wolf. Private quantum channels. Proc. IEEE Conf. on Found. Comp. Sci. (FOCS), 2000.
- [17] D.W. Leung. Quantum Vernam Cipher. quant-ph/0012077.
- [18] B. Schumacher and M.D. Westmoreland. Quantum mutual information and the one-time pad. Phys. Rev. A **74**, 042305 (2006).
- [19] K. Horodecki, M. Horodecki, P. Horodecki, and J. Oppenheim. Secure key from bound entanglement. Phys. Rev. Lett. **94**, 160502 (2005).
- [20] K. Horodecki, L. Pankowski, M. Horodecki, and P. Horodecki. Low dimensional bound entanglement with one-way distillable cryptographic key. IEEE Trans. Inf. Theory **54**, 2621 (2008).
- [21] G. Smith and J.A. Smolin. Can non-private channels transmit quantum information? Phys. Rev. Lett. **102**, 010501 (2009).
- [22] K. Li, A. Winter, X. Zou, and G. Guo. The private capacity of quantum channels is not additive. Phys. Rev. Lett. **103**, 120501 (2009).
- [23] G. Smith and J.A. Smolin. Extensive nonadditivity of privacy. Phys. Rev. Lett. **103**, 120503 (2009).