Numerical evidence for bound secrecy from two-way postprocessing in quantum key distribution

Sumeet Khatri and Norbert Lütkenhaus
Institute for Quantum Computing and the Department of Physics and Astronomy, University of Waterloo, Waterloo, ON
(Dated: April 26, 2017)

Given some set of data shared by two parties, Alice and Bob, are the correlations between them strong enough to allow them to execute some protocol to be able to create a secret key? Is it possible for Alice and Bob to be strongly correlated and still not create a secret key by any protocol? Interestingly, while the existence of such correlations has been proven to exist in the quantum case, where it is called *bound entanglement*, the existence of such correlations in the classical case, where is it called *bound secrecy* or *bound secret information*, has remained unproven for almost 17 years since it was first conjectured in 2000 [1] (see also [2–4]). Our work [5] provides a new framework for proving this fundamental conjecture in the context of two-way postprocessing in prepare-and-measure-based (PM-based) quantum key distribution (QKD). At the same time, we make progress on another long-standing question, namely, about the highest tolerable error-rate thresholds for qubit-based six-state QKD protocols [6], in which the classical data from which Alice and Bob wish to create a secret key arises from measurement of quantum states; see Fig. 1. Specifically, we conjecture based on strong analytical and numerical evidence that there does not exist a two-way postprocessing protocol distilling secret key in the gap of Fig. 1, meaning, therefore, that the gap is a domain of bound secrecy for the particular correlations shared by Alice and Bob in the protocol. The symmetric extendability of quantum states, another problem that has evaded a full solution for many years, plays a critical role in our investigation, and our work also provides an efficient numerical test for symmetric extendability that forms a large part of our numerical evidence. Our work thus lays the groundwork for a systematic investigation into the existence of two-way protocols and provides a concrete route to a potential proof of our conjecture. A positive answer to the question of the existence of bound secrecy would be a truly remarkable result and would be a stark contrast to what was previously believed about classical secret key creation. Furthermore, if our conjecture is true, then we would have a rare example of a scenario in which concepts from quantum information theory lead to new insights in classical information theory.

We assume in our work [5] that Alice and Bob share many copies of the state $\rho_Q^{AB} = (1-2Q)|\Phi^+\rangle\langle\Phi^+| + \frac{Q}{2}\mathbb{1}_{AB}$, where $Q \in \left[0, \frac{1}{2}\right]$ is the quantum bit-error rate (QBER) and $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|0,0\rangle + |1,1\rangle)$. They obtain their classical data by local measurement of each state in the standard basis $\{|0\rangle, |1\rangle\}$. As indicated in Fig. 1, it is known that ρ_Q^{AB} is separable for $Q \geq \frac{1}{3}$ and *symmetrically extendable* for $Q \geq \frac{1}{6}$ [7]. The latter means, by definition, that there exists a tripartite extension $\rho_Q^{ABB'}$ of ρ_Q^{AB} such that $\rho_Q^{AB'} = \rho_Q^{AB}$. In this situation, it is known that no one-way protocol involving communication from Alice to Bob can be used to distill a secret key because the system B' is effectively a copy of B and could belong to an eavesdropper (Eve), meaning that from Alice's point of view Bob and Eve are symmetric [7]. Distilling secret key beyond $\frac{1}{6}$ therefore requires a *two-way* postprocessing protocol.

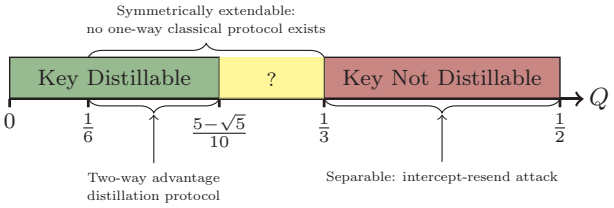

FIG. 1: Key distillability as a function of the quantum bit-error rate Q characterizing Alice and Bob's classical data in the six-state QKD protocol. The highest Q for which a protocol distilling secret key is known to exist is $\frac{5-\sqrt{5}}{10} \approx 27.6\%$. The existence of an intercept-resend attack for $Q \geq \frac{1}{3}$ immediately precludes the existence of a protocol, leaving open our question of interest, which is whether a secret key can be distilled in the *gap*, that is, the yellow region.

Much work has been done on two-way postprocessing protocols for the PM-based six-state protocol considered here [8–11]. The highest QBER achieved in these works has been $\frac{5-\sqrt{5}}{10} \approx 27.6\%$, and efforts to increase this threshold have been unsuccessful (see, in particular, [10, 11]). Myhr et al. [12] then provided a different perspective on two-way protocols by shifting the goal from distilling a secret key to *breaking symmetric extendability*. Specifically, they argued that if Alice and Bob's initial data corresponds to a symmetrically extendable state, then any successful two-way protocol must first transform this state to one that is not symmetrically extendable. This is due to the fact that any two-way protocol necessarily ends with a final round of one-way communication, which cannot be successful in distilling a secret key unless Alice and Bob's correlations are not symmetrically extendable. To break symmetric extendability, they proved that it is sufficient to consider one announcement by Bob to Alice on a block of his data that can be de-

scribed by one Kraus operator on the quantum states. By considering protocols in which Alice and Bob postselect on some pre-chosen linear error correction code, they provided analytical and numerical evidence to suggest that such generalized protocols cannot break symmetric extendability beyond 27.6%. Since only postselection on linear codes was considered, their results left open the possibility that postselection on *nonlinear* codes might be able to break symmetric extendability beyond 27.6%.

We thus consider postselection on nonlinear codes using the single-Kraus-operator formulation from [12]. Specifically, we argue that it is sufficient to consider only postselection protocols and we provide an explicit form for the Kraus operator. This allows us to obtain the effective quantum state after postselection by Bob on *arbitrary* error correction codes, i.e., both linear and nonlinear codes. It can be shown (see [5] for details) that this effective state is of the form

$$\rho_{Q,\mathcal{C}}^{A^n\tilde{B}} = (\mathbb{1}_{A^n} \otimes K_{\mathcal{C}})(\rho_Q^{AB})^{\otimes n}(\mathbb{1}_{A^n} \otimes K_{\mathcal{C}})^\dagger, \qquad (1)$$

where

$$K_{\mathcal{C}} = \sum_{k=0}^{m-1} |k\rangle\langle C_k| \qquad (2)$$

is the single Kraus operator corresponding to Bob's postselection and $\mathcal{C} = \{C_k\}_{k=0}^{m-1}$ is the set of codewords defining the error correction code. Using arguments from [12], we argue that for the existence of a two-way postprocessing protocol distilling secret key it is sufficient to consider the symmetric extendability of the states (1). Specifically, we show that it is sufficient to determine for each code $\mathcal{C}$ the *updated threshold* $Q_{\mathcal{C}}^*$, which we define as the value of the QBER beyond which the state (1) is symmetrically extendable. (Note that without the Kraus operator the threshold is simply $\frac{1}{6}$ for all n.) We then provide numerical evidence that there does not exist a code $\mathcal{C}$ whose updated threshold $Q_{\mathcal{C}}^*$ exceeds 27.6%, hence there does not exist a two-way postprocessing protocol in the gap.

Specifically, after reducing the problem of determining the existence of a two-way protocol to the problem of finding a code for which the postselected state (1) is not symmetrically extendable in the gap (as described above), we reduce the problem further by showing that it is sufficient to search over *inequivalent codes*, and we exhaustively search over all inequivalent codes of small block lengths and number of codewords. Using semidefinite programming, we are able to numerically determine the thresholds $Q_{\mathcal{C}}^*$ of all of these codes, and the discovered trend is displayed in Fig. 2. Notably, we discover that the *repetition codes* $\mathcal{R}_n = \{00\cdots00, 11\cdots11\}$ have the highest threshold for each block length n of the codes, with a decreasing threshold with increasing number of codewords. Since we are able to show analytically that in the limit $n \to \infty$ the repetition code thresholds $Q_{\mathcal{R}_n}^*$ approach 27.6%, we conjecture that the repetition codes have the highest threshold for each block length n and therefore that there does not exist a code whose threshold exceeds 27.6%.

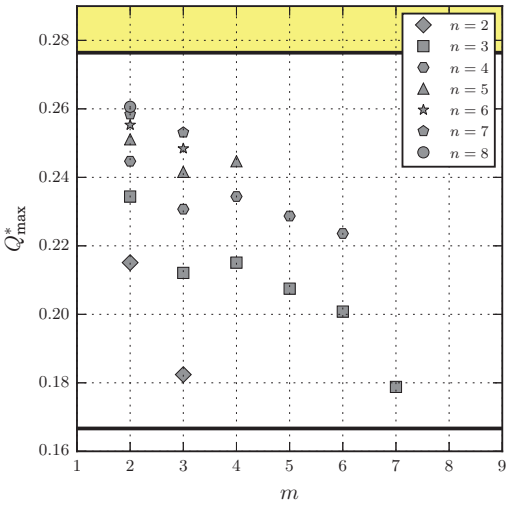

FIG. 2: For each class of codes with small block length n and small number of codewords m, we have determined the thresholds of all inequivalent codes in the class and plotted the highest threshold from each class.

Finally, we consider a more restricted class of protocols that involve postselection by Alice in addition to postselection by Bob. We determine analytically in this scenario that the class of *simplex* codes do not exceed 27.6%. We also numerically test over 540,000 codes of high block length and number of codewords, and none of them break symmetric extendability in the gap. This test is performed using the connection between symmetrically extendable states and antidegradable quantum channels. Specifically, for the CP maps corresponding to the states (1) via the Choi-Jamiolkowski correspondence, our test involves picking an ansatz for the degrading map and checking whether this map is completely positive and trace preserving. This test is more time- and resource-efficient than running semidefinite programs, and yields conclusive results for 99% of the codes we tested.

[1] N. Gisin and S. Wolf, *Linking Classical and Quantum Key Agreement: Is There "Bound Information"?* (Springer Berlin Heidelberg, Berlin, Heidelberg, 2000), pp. 482–500, ISBN 978-3-540-44598-2.

[2] N. Gisin, R. Renner, and S. Wolf, *Bound Information: The Classical Analog to Bound Quantum Entanglemen* (Birkhäuser Basel, Basel, 2001), pp. 439–447, ISBN 978-3-0348-8266-8.

[3] Gisin, Renner, and Wolf, Algorithmica **34**, 389 (2002), ISSN 1432-0541.

[4] R. Renner and S. Wolf, in *Advances in Cryptology — EUROCRYPT 2003*, edited by E. Biham (Springer-Verlag, 2003), vol. 2656 of *Lecture Notes in Computer Science*, pp. 562–577.
[5] S. Khatri and N. Lütkenhaus, Phys. Rev. A **95**, 042320 (2017), URL `https://link.aps.org/doi/10.1103/PhysRevA.95.042320`.
[6] D. Bruß, Phys. Rev. Lett. **81**, 3018 (1998).
[7] T. Moroder, M. Curty, and N. Lütkenhaus, Phys. Rev. A **74**, 052301 (2006).
[8] D. Gottesman and H.-K. Lo, IEEE Transactions on Information Theory **49**, 457 (2003).
[9] H. F. Chau, Phys. Rev. A **66**, 060302 (2002).
[10] A. Acín, J. Bae, E. Bagan, M. Baig, L. Masanes, and R. Muñoz Tapia, Phys. Rev. A **73**, 012327 (2006).
[11] J. Bae and A. Acín, Phys. Rev. A **75**, 012334 (2007).
[12] G. O. Myhr, J. M. Renes, A. C. Doherty, and N. Lütkenhaus, Phys. Rev. A **79**, 042329 (2009).