

Symmetric extension and its application in QKD

G. O. Myhr (1) (2), N. Lütkenhaus (1) (2), A. C. Doherty (3) and J. M. Renes (4)

1: Inst. for Quantum Computing, University of Waterloo, 200 University Ave. W., Waterloo ON N2L 3G1, Canada

2: Universität Erlangen-Nürnberg, Staudtstr. 7/B2, 91058 Erlangen, Germany

3: School of Physical Sciences, The University of Queensland, Queensland 4072, Australia

4: Institut für Angewandte Physik, Technische Universität Darmstadt, Hochschulstraße 4a,
D-64289 Darmstadt, Germany

(gomyhr@iqc.ca)

Abstract

We investigate from which quantum correlations it is at all possible to distill a secret key. States with a so-called symmetric extension can never lead to a secret key unless it is processed further. We show that if a symmetric extension can be broken by LOCC operations, it is also possible to break it with a single filter. For Bell-diagonal and some other two-qubit states we characterize the states with symmetric extension, and give a conjectured formula for the general two-qubit case. This is then used to show that beyond current noise thresholds, the best known postprocessing procedures always output states with symmetric extension.

QKD and symmetric extension

Any implementation of quantum key distribution consists of two parts. First the hardware distributes and measures quantum particles, producing correlated data. Then the software subjects the generated data to various tests and, if it passes, creates a secret key from it. Whether the implementation is entanglement-based or an equivalent prepare and measure scheme, the data must show evidence of effective entanglement for the output to be a secret key [1]. However, the converse is not known, that is, whether the data can be fashioned into a secret key given proof of effective entanglement.

Certainly this is not always possible if the key distillation protocol is restricted to one way communication. In this case there exist entangled states with a so-called symmetric extension [2], meaning that an eavesdropper will be in at least as good a position as one party to guess the other party's data. Formally, a bipartite state ρ_{AB} has a symmetric extension if there exists a state on the extended system $\rho_{ABB'}$ which is invariant under exchange of B and B' and reduces to ρ_{AB} when B' is traced out. The system B' is then a copy of B and for QKD purposes is assumed to be in the hands of an eavesdropper along with the rest of the purifying system.

We argue that symmetric extensions are also relevant in the general context of QKD with two-way postprocessing. Any such protocol consists of a finite number of rounds of one-way communication in alternating directions, and since the protocol must eventually terminate, the effective state shared prior to the final round must have no symmetric extension in order for

the protocol to succeed. If the effective state prior to the postprocessing had a symmetric extension, it must be broken at some point along the way.

Reduction to two communication rounds

By concerning ourselves only with the question of whether a key can be distilled or not, and not with the rate of distillation, the problem can be simplified further. Assume that each round of one-way postprocessing is done on blocks with a finite number of systems. We may then limit ourselves to filtering operations, general quantum operations which can succeed or fail. If more than one outcome of Bob's generalized filtering measurement succeeds, we could as well pre-select one of them and only consider this a successful outcome. Moreover, the number of rounds in the protocol can be reduced to two, as follows. For each block that Bob operates on in his last round, he can guess Alice's announcements relating to the quantum systems in that block ahead of time and start immediately with his last round. Alice will notice if this guess was wrong and tell Bob to discard that block. For the tiny fraction of blocks where Bob was right, Alice can proceed with her last round. This means that if a QKD protocol succeeds in distilling secret key from an underlying quantum state with symmetric extension, it must be possible to break the symmetric extension only with a filter on a block of copies of the state. [3]

Which states have symmetric extension?

To identify strategies for breaking a symmetric extension, we need to describe states with symmetric extension. We show that these states can be written as convex combinations of states with a *pure* symmetric

extension. For states with pure symmetric extension, the spectrum of the density operator has to be equal to the spectrum of the density operator on system B ,

$$\vec{\lambda}(\rho_{AB}) = \vec{\lambda}(\rho_B).$$

We can prove that in the special case when A and B are both qubits—but never otherwise—this condition is also sufficient for having a pure symmetric extension.

Using this condition and other techniques we have found necessary and sufficient conditions for special classes of two-qubit states to have a general symmetric extension. These classes are Bell-diagonal states, rank-2 states and states where only one of the off-diagonal terms in the density matrix is non-zero (in the latter case the state is either separable or the non-zero element can be chosen to be $\rho_{00,11} = \rho_{11,00}$ by a local change of basis). In all these cases the conditions can be shown to be equivalent to [4]

$$\text{tr}(\rho_B^2) \geq \text{tr}(\rho_{AB}^2) - 4\sqrt{\det(\rho_{AB})}.$$

We conjecture that this also is a necessary and sufficient condition for all other two-qubit states. This is also supported by numerical evidence.

BB84 and 6-state protocols

In the BB84 and 6-state protocols with standard sifting, the states from which the correlations arise can be taken to be Bell-diagonal without loss of generality. Moreover, most postprocessing schemes preserve this property throughout the postprocessing. It is therefore

possible to check for which states a given postprocessing breaks a symmetric extension. The currently best known procedure in terms of distilling key from more states is by Chau [5] and can distill key for up to an error rate of 20.0 % for BB84 and 27.6 % for the 6-state protocol. This works by starting out with so-called B-steps or advantage distillation, which detects and discards blocks with bit errors, followed by techniques which only involve one-way communication. We show that whenever the state is too noisy for the protocol to generate a secret key, it is because the first step fails to break a symmetric extension [3]. Therefore, no further processing using only one-way communication can generate a secret key. This reproduces the result by Acín et al. [6] without explicitly considering any actions by the eavesdropper.

References

- [1] M. Curty, M. Lewenstein, and N. Lütkenhaus, Phys. Rev. Lett. **92**, 217903 (2004).
- [2] A. C. Doherty, P. A. Parrilo, and F. Spedalieri, Phys. Rev. Lett. **88**, 187904 (2002).
- [3] G. O. Myhr, J. M. Renes, A. C. Doherty, and N. Lütkenhaus, in preparation.
- [4] G. O. Myhr and N. Lütkenhaus, in preparation.
- [5] H. F. Chau, Phys. Rev. A **66**, 060302 (2002).
- [6] A. Acín, J. Bae, E. Bagan, M. Baig, L. Masanes, and R. Muñoz-Tapia, Phys. Rev. A **73**, 012327 (2006).