Characterizing two-party correlations for quantum key distribution

Marcos Curty[1], Maciej Lewenstein[2], and Norbert Lütkenhaus[1]
[1] *Quantum Information Theory Group, Institut für Theoretische Physik, Universität Erlangen-Nürnberg, 91058 Erlangen, Germany*
[2] *Institut für Theoretische Physik, Universität Hannover, 30167 Hannover, Germany*

We show that a necessary precondition for unconditionally secure quantum key distribution is that sender and receiver can prove the presence of entanglement in an effectively distributed quantum state. One can therefore systematically search for entanglement using the class of entanglement witness operators that can be constructed from the observed data. We apply our analysis to two well-known quantum key distribution protocols, namely the 4-state protocol and the 6-state protocol. As a special case, we show that, for some asymmetric error patterns, the presence of entanglement can be proven even for error rates above 25% (4-state protocol) and 33% (6-state protocol).

PACS numbers:

Quantum key distribution (QKD) [1] allows two parties (Alice and Bob) to generate a secret key without assumptions on the computational and technological power of an eavesdropper (Eve) who interfers with the signals. Implementations of QKD schemes use two phases to establish a key. In the first one, quantum mechanical states are used to create correlations between the legitimate users. These correlations are described by a joint probability distribution $P(A,B)$. In a second phase, called *key distillation*, Alice and Bob use an authenticated public channel to process the correlated data in order to obtain a secret key.

We concentrate on the first phase, and we derive conditions on the correlations that are necessary for the second phase to succeed. To describe how the correlated data are created let us view two types of protocols separately. In *entanglement based schemes* a bi-partite state is distributed to Alice and Bob by an untrusted third party. This party may be an eavesdropper who is in possession of a third sub-system that may be entangled with those given to Alice and Bob. While the subsystems measured by Alice and Bob result in correlations described by $P(A,B)$, Eve can use her subsystem to obtain information about the future key. In *prepare&measure schemes* Alice prepares a random sequence of pre-defined non-orthogonal states that are sent to Bob through an untrusted channel (controlled by Eve). Generalizing the ideas of Bennett et al. [2], the signal preparation can be thought of as follows: Alice prepares an entangled bi-partite state of the form $|\Psi_{source}\rangle_{AB} = \sum_i \sqrt{p_i}|e_i\rangle|\varphi_i\rangle$. If she measures the first system in the canonical orthonormal basis $|e_i\rangle$, she effectively prepares the (non-orthogonal) signal states $|\varphi_i\rangle$ with probabilites p_i. The state $|\Psi_{source}\rangle_{AB}$ together with the action of the quantum channel leads to an effective distributed bi-partite state shared by Alice and Bob. One important characteristic of these schemes is that the reduced density matrix ρ_A of Alice is fixed.

A necessary condition for the success of the key distillation phase is that the performed measurements together with $P(A,B)$ suffice to prove that the (effective) bi-partite state is entangled.

Observation 1 *Assume that the observable joint probability distribution $P(A,B)$ together with the knowledge of the corresponding measurements can be interpreted as coming from a separable state σ_{AB}, then no secret key can be distilled via public communication from the correlated data.*

The question whether the effectively distributed bi-partite state is entangled or not can be addressed based on the ideas of entanglement witnesses operators [3, 4].

Theorem 1 *Given a set of local operations with POVM elements $F_a \otimes G_b$ together with the probability distribution of their occurrence, $P(A,B)$, then the correlations $P(A,B)$ cannot lead to a secret key via public communication unless one can prove the presence of entanglement in the (effectively) distributed state via an entanglement witness $W = \sum_{a,b} c_{a,b} F_a \otimes G_b$ with $c_{a,b}$ real such that $\mathrm{Tr} W\sigma \geq 0$ for all separable states σ and $\sum_{a,b} c_{a,b} P(a,b) < 0$.*

The problem of determining whether $P(A,B)$ might lead to a secure key is therefore reduced to a search over all optimal entanglement witnesses that can be constructed from the protocol and the collected data. We illustrate the consequences of this view for two well-known protocols: The 6-state protocol [5] and the 4-state protocol [1].

For the case of the 6-state protocol, Alice and Bob perform projection measurements onto the eigenstates of the three Pauli operators σ_x, σ_y, and σ_z in the entanglement based scheme where Eve distributes bi-partite qubit states. In the corresponding prepare&measure scheme, Alice prepares the eigenstates of those operators by performing the same measurements on a maximally entangled qubit state. This protocol allows Alice and Bob to construct any entanglement witness of the form

$$W = \sum_{i,j=\{0,x,y,z\}} c_{ij}\ \sigma_i \otimes \sigma_j, \qquad (1)$$

where $\sigma_0 = \mathbb{1}$ and c_{ij} are real numbers. This means that Alice and Bob can evaluate the class of optimal witnesses for two-qubits states. In this protocol all entangled states can be detected. Alternatively to the witness approach, Alice and Bob can employ quantum state tomography techniques to reconstruct the quantum state ρ_{AB} and to check its separability e.g. via the Peres-Horodecki criterion [3, 6].

While the analysis of the 6-state protocol is quite simple, the 4-state protocol, however, needs a deeper examination since it turns out that the optimal witnesses cannot be evaluated with the given correlations. As a result, there can be entangled states that give rise to correlations $P(A, B)$ that are not sufficient to prove the presence of entanglement. In this protocol, Alice and Bob perform projection measurements in two qubit bases, say x and z. In the corresponding prepare&measure scheme Alice uses the same set of measurements on a maximally entangled state to prepare the eigenstates of these operators as signals. For the entanglement scheme we obtain the set of entanglement witnesses, which we shall denote as EW_4, that can be evaluated with the resulting correlations as

$$W = \sum_{i,j=\{0,x,z\}} c_{ij}\ \sigma_i \otimes \sigma_j\ . \tag{2}$$

In this class, one can characterise the family of witness operators that are optimal.

Theorem 2 *Consider the family of operators* $W = \frac{1}{2}(Q + Q^{T_P})$, *where* $Q = |\phi_e\rangle\langle\phi_e|$ *and* $|\phi_e\rangle$ *denotes a real entangled state. The elements of this family are witness operators that are optimal in* EW_4 *and detect all the entangled states that can be detected within* EW_4.

This set of witness operators, $W = \frac{1}{2}(Q + Q^{T_P})$, provides an infinite number of necessary and sufficient conditions for the presence of entanglement in the observable correlations $P(A, B)$. Each condition is characterized by a real entangled state $|\phi_e\rangle$, and therefore the whole set of them can be easily parametrized as a function of only three real parameters. From a practical point of view, this means that Alice and Bob can easily checked this set of conditions just with the help of a simple computer program.

The corresponding 4-state prepare&measure scheme allows additionally the use of the component $\sigma_y \otimes \mathbb{1}_B$. The entanglement witnesses EW_4 are therefore contained in those that can be constructed in this case.

Finally, let us briefly analyze the implications of our results for the relationship between the bit error rate e in the protocols and the presence of correlations of quantum mechanical nature. Here error rate refers to the sifted key, that is, those events where signal preparation and detection employ the same polarization basis. An entanglement breaking channel gives rise to $e \geq 25\%$ (4-state protocol) and $e \geq 33\%$ (6-state protocol), respectively [5, 7]. This means that if the error rate is below these values, this is already sufficient to prove that the joint probability distribution $P(A, B)$ contains quantum mechanical correlations. However, for some asymmetric error patterns, it is possible to detect the presence of quantum correlations even for error rates above 25% (33%). Let us illustrated this fact with an example motivated by the propagation of polarized light in an optical fiber. This channel can be described by a unitary transformation. Consider, for instance,

$$U(\theta) = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \tag{3}$$

The resulting bit error rate is given by $e = \sin^2\theta$ and $e = \frac{2}{3}\sin^2\theta$ for the 4-state and the 6-state protocols, respectively. Nevertheless, in both cases the existence of quantum correlations can be detected for all angles θ. The case of the 6-state protocol is clear, since a unitary transformation preserves the entanglement and all entanglement can be verified in this protocol. With respect to the 4-state protocol, it can also be shown that there is always an entanglement witness $W \in \mathrm{EW}_4$ that detects quantum correlations in $P(A, B)$.

To conclude, we have that a necessary condition for QKD is that the legitimate users can prove the presence of entanglement in the effectively distributed quantum state. We have analyzed the 4-state and 6-state QKD protocols, and we have derived necessary and sufficient conditions for the existence of quantum correlations in both protocols. As a special case, we have demonstrated that, for some asymmetric error patterns, the presence of this type of correlations can be detected even for error rates above 25% and 33%, respectively.

[1] C. H. Bennett and G. Brassard, in *Proc. IEEE Int. Conference on Computers, Systems and Signal Processing* (IEEE Press, New York, 1984), p. 175.

[2] C. H. Bennett, G. Brassard, and N. D. Mermin, Rev. Pev. Lett. **68**, 557 (1992).

[3] M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Lett. A **223**, 1 (1996).

[4] B. M. Terhal, Phys. Lett. A **271**, 319 (2000).

[5] D. Bruß, Phys. Rev. Lett. **81**, 3018 (1998).

[6] A. Peres, Phys. Rev. Lett. **77**, 1413 (1996).

[7] A. Ekert and B. Huttner, J. Mod. Opt. **41**, 2455 (1994).