Secrecy of Bipartite Quantum Channels with Local Environment Assistance

Joonwoo Bae

School of Computational Sciences, Korea Institute for Advanced Study, Seoul 130-012, Korea
(Dated: March 3, 2008)

We investigate secrecy properties of bipartite quantum channels when local environment called shield system is assisted. Two honest parties apply either the classical distillation such as the standard one-way postprocessing followed by the advantage distillation (AD), or the quantum distillation applying the recurrence protocol. We then identify those entangled states that can be converted to secrecy by either the quantum or the classical distillation. Remarkably much wider range of bound entangled states are shown to be distilled to secrecy.

PACS numbers: 03.67.Dd, 03.65.Ud, 03.67.-a
where $\sigma_j$, $j = 1, 2, 3, 4$, are unnormalized shield states of systems $A'B'$ and $|\phi_i\rangle$, $j = 1, 2, 3, 4$ are Bell states, in terms of Pauli matrices, $|\phi_2\rangle = (\mathbb{1} \otimes Z)|\phi_1\rangle$, $|\phi_3\rangle = (\mathbb{1} \otimes X)|\phi_1\rangle$ and $|\phi_4\rangle = (\mathbb{1} \otimes iY)|\phi_1\rangle$. The state shared in the key part is denoted by, $\rho_{AB} = \sum_j \mu_j |\phi_j\rangle \langle \phi_j|$, where $\mu_j = \text{tr}(|\sigma_j\rangle \langle \sigma_j|)$, $j = 1, 2, 3, 4$. Here we restrict to that the key part shares Bell-diagonal states, and if it is not the case we suppose that two honest parties apply local filtering operations to the key part, to share bell-diagonal states. For $\rho_{ABA'B'}$ in (3), there exists a twisting $U$ such that $\rho_{ABA'B'} = U \sigma_{ABA'B'} U^\dagger$ in which, the shield part $A'B'$ being traced out,

\[
\sigma_{AB} = \lambda_1 |\phi_1\rangle \langle \phi_1| + \lambda_2 |\phi_2\rangle \langle \phi_2| + \lambda_3 |\phi_3\rangle \langle \phi_3| + \lambda_4 |\phi_4\rangle \langle \phi_4|,
\]

with

\[
\lambda_{1,2} = \frac{1}{2}(||\sigma_1 + \sigma_2|| + ||\sigma_1 - \sigma_2||),
\]
\[
\lambda_{3,4} = \frac{1}{2}(||\sigma_3 + \sigma_4|| + ||\sigma_3 - \sigma_4||).
\]

Here note that the $\sigma_{AB}$ has less phase errors than the $\rho_{AB}$ [17]. This means that not all errors from $\rho_{AB}$ have to be corrected for distilling a secret key, instead it suffices to correct the errors from $\sigma_{AB}$ since a secret key corresponds to a private state which also consists of phase errors due to the twisting effect on the $|\phi_i\rangle$. Then the question arises whether distillation steps to correct errors existing in $\sigma_{AB}$ commute with any twisting operation. The quantum and classical protocols to be considered throughout the paper are in fact the case [8 [21]. Therefore, identifying the untwisted state $\sigma_{AB}$, two honest parties will know the errors that should be corrected, from which they can quantify if $\rho_{ABA'B'}$ is key-distillable by the aforementioned distillation protocols. The precondition for key distillability is that $\sigma_{AB}$ is entangled, which holds if and only if $\lambda_1 > \lambda_2 + \lambda_3 + \lambda_4$ [18], and in terms of shield states

\[
||\sigma_1 - \sigma_2|| > ||\sigma_3 + \sigma_4||.
\]

To prove the general security, in fact one should go through the analysis of the most general attack by Eve. In the case, two honest parties share general $N$ symmetric states, $\rho^{(N)}_{ABA'B'}$, which is invariant under any permutations of copies such that each single state is identical: $\text{tr}_N - 1 \rho^{(N)}_{ABA'B'} = \rho_{ABA'B'}$. There could exist correlations among $N$ symmetric states [14], to which the analysis is in general a hard task. Recently, Renner has proven the quantum de Finetti theorem in the exponential form, which leads a huge simplification in the analysis. The theorem tells that whenever the shared state $\rho^{(N)}_{ABA'B'}$ is symmetric for arbitrarily large $N$, not necessarily going through the most general attack [15] instead two honest parties can safely assume the so-called collective attacks $\rho^{(N)}_{ABA'B'}$, for the general security.

We now consider key distillation from $\rho^{\otimes N}_{ABA'B'}$. The state $\rho_{ABA'B'}$ is simply key-distillable if $\rho_{AB}$ is entangled since all two-qubit entangled states are distillable. To avoid the overlap with distillable entanglement, we here assume that $\rho_{ABA'B'}$ is bound entangled. In what follows, we derive the key-distillability condition when two honest parties apply the recurrence protocol, which works as follows [3]. Taking two copies of $\rho_{ABA'B'}$, two honest parties first apply the CNOT operation to their first(controlled bit) and second(target bit) key systems and measure the second key systems. Their measurement outcomes are announced, and if both measurement outcomes are the same they repeat the procedure again to the remaining pair with another pair, otherwise they start again with another two pairs. A remaining state after passing $m$ repetitions is denoted by $\sigma_m$ [16]. Key distillability can be answered by the useful formula [18],

\[
||\langle 00|\sigma_m|11\rangle|| = \sqrt{p_{AB}(0,0)p_{AB}(1,1)F(p_E, \rho_E^1)},
\]

where $F(p_E^0, \rho_E^1)$ is the fidelity between two states $\rho_E^j$, $j = 0, 1$, after two honest parties share both the same value $j$. The property of secret key tells that the rhs of (7) is arbitrarily close to $1/2$ if and only if two honest parties share a secret key [1]. Therefore, a secret key can be distilled from $\sigma_m$ if and only if

\[
||\langle 00|\sigma_m|11\rangle|| = \frac{1}{2}||\sigma_1 - \sigma_2||^m + 2 ||\sigma_3 + \sigma_4||^m
\]

(8)

can be arbitrarily close to $1/2$ as repetitions $m$ become very large. For such a convergence the shield states should fulfill that

\[
||\sigma_1 - \sigma_2|| = ||\sigma_1 - \sigma_2||,
\]

since $||\sigma_1 + \sigma_2||$ is the most dominant in (8) from the condition in [10]. The condition [10] can be expressed equivalently as their orthogonality $\text{tr}[\sigma_1 \sigma_2] = 0$ [16]. Here note that correlations existing in shield states do not contribute the security condition, and the global property of them, orthogonality, matters. One can also relax the condition [10] to an $\epsilon$-neighborhood of private states: if $\text{tr}[\sigma_1 \sigma_2] < \delta$ for $\delta > 0$ then there exists $\epsilon > 0$ a function of $\delta$ such that $||\sigma_m - \gamma_{ABA'B'}|| < \epsilon$, by the recurrence protocol.

**Proposition 1.** A bound entangled states $\rho_{ABA'B'}$ is key-distillable by the recurrence protocol if and only if i) $\sigma_{AB}$ is entangled (3) and ii) shield states $\sigma_1$ and $\sigma_2$ are orthogonal [1].

**Example.** We reconsider the example in Ref. [8] which takes the followings as shield states in [3],

\[
\sigma_1 = p(\rho_s + \rho_a) \otimes I, \quad \sigma_2 = p\rho_s^I,
\]
\[
\sigma_{3,4} = (1 - p)(\rho_s + \rho_a) \otimes I,
\]

(10)
\[
\Psi_{ABAB'E}^{(N)} \xrightarrow{\text{Quantum Distillation}} U\Phi_1 \otimes \rho_{ABAB'E} U^+ \\
\xrightarrow{\text{Measurement}} P(A, B|\psi_E) \xrightarrow{\text{Classical Distillation}} \text{Secret Key}
\]

FIG. 1: Key distillation from quantum states follows either measurement followed by quantum distillation of a private state, or classical distillation followed by measurement. The \(U\) is a twisting operation in the

where \(\rho_{u(s)}\) is the normalized \(d\)-dimensional projection operator onto asymmetric (symmetric) space. The state \(\rho_{ABAB'A'B'}\) is bound entangled if and only if \(p \in (0, 1/3)\) and \(p \leq (1 + (d/(d-1))^2)^{-1}\). Applying the key distillability condition to this state, one obtains \(\text{tr}[\sigma_1 \sigma_2] = O(2^{-l})\), which means that two shield states can be made arbitrarily orthogonal to satisfy the orthogonality as \(l\) increases. The chosen shield states in fact play the role of increasing the orthogonality of themselves, while \(\rho_{ABAB'A'B'}\) is bound entangled for sufficiently large \(l\), a certain range of \(p\), and the projector’s dimension \(d\). Note that the shield states should be of large dimension to satisfy the orthogonality.

We now move to the classical key distillation method, that applies the standard one-way postprocessing followed by the AD [19]. This is an alternative to the quantum protocol (see, Fig. 1), but realistic in the sense that it only applies currently feasible technology such as single-copy level measurement plus classical processing. After identifying the shared state in a single-copy level in [3], two honest parties analyze the errors that should be corrected. As we have discussed before, it suffices to correct only the errors arisen from the untwisted state \(\sigma_{AB}\) in [3] but not all: phase errors are less in the \(\sigma_{AB}\) than in the \(\rho_{AB}\). Note that parameters identifying the \(\sigma_{AB}\) in [5] can also be directly estimated by LOCC protocols [20]. After the parameter estimation, two honest parties measure the key part of \(\rho_{ABAB'B'}^{\otimes N}\) in the computational basis and share secret correlations through measurement outcomes, called raw keys of the probability distribution \(p_{AB}\). Then, the key distillation protocol proceeds with the raw keys, to correct errors existing in \(p_{AB}\) that originated from the \(\sigma_{AB}\) rather than the \(\rho_{AB}\). We here remind that the classical distillation protocol commutes with a twisting operation [21].

In what follows, we describe the classical distillation protocol, which is known as the most tolerant to date. Sharing secret correlations \(p_{AB}\), two honest parties apply the AD that involves two-way classical communication [10], which works as follows. Alice first generates a secret bit \(s_A\) and computes a list \(x_i = s_A + a_i\), with her measurement outcomes \(a_i\), \(i = 1, \cdots, N\), and then announces \(x_i\) through a public and authenticated channel so that Bob can also compute \(b_i + x_i = y_i\). Bob will see that his resulting values are either all the same or not, and reply to Alice with acceptance or rejection, depending on the computation result. He says acceptance if all \(y_i\) are the same, and proceeds to apply one-way error correction and privacy amplification to the accepted values. Otherwise, two honest parties leave from the failed values and perform the protocol with another values again.

The AD is a post-selection processing to take stronger bit-correlations \(p'_{AB}\) from the initial ones \(p_{AB}\). Then, the security can be ensured if the one-way postprocessing converts \(p'_{AB}\) to secrecy, i.e. the lower bound of one-way secret key rate, \(K_{\text{se}} \geq I(A:B) - I(A:E)\), is positive [14, 15, 22]. To summarize, the classical distillation incorporates the AD before the one-way postprocessing.

The key distillability of the protocol has been completely analyzed in Refs. [23, 24]: \(\sigma_{AB}\) is distillable if the parameters \(\lambda_j\) in [5] satisfy \((\lambda_1 - \lambda_2)^2 > (\lambda_3 + \lambda_4)(\lambda_1 + \lambda_2)\). Then, straightforwardly from the relation in [5], we arrive at the following proposition.

Proposition 2. A bound entangled state \(\rho_{ABAB'A'B'}\) is key-distillable by the classical distillation if and only if i) its untwisted state \(\sigma_{AB}\) is entangled i.e. [9] and ii) shield states satisfy the following

\[
||\sigma_1 - \sigma_2||^2 > ||\sigma_3 + \sigma_4|| ||\sigma_1 + \sigma_2||. 
\]

Let us remind the bound entangled state in the example [10], which is key-distillable in a tiny range of bound entanglement. The following proposition tells that the more range would be key-distillable.

Proposition 3. Let \(S_R\) and \(S_C\) denote the sets of quantum states key-distillable by the recurrence protocol and by the considered classical protocol, respectively. Then, \(S_R \subset S_C\).

Proof. Suppose that \(\rho_{ABAB'A'B'} \in S_R\), so i) \(\sigma_{AB}\) is entangled and ii) it fulfills [9]. The classical distillation is applied to those key-distillable states. Since shield states fulfill [9], the security condition [11] becomes the same with the condition that \(\sigma_{AB}\) is entangled in [9]. This thus shows that \(S_R \subset S_C\). \(\Box\)

In addition, the proposition 3 shows that, for a particular choice of separable shield states such that [9] holds, entanglement itself means secrecy when its untwisted state \(\sigma_{AB}\) is entangled. This is because the entanglement condition [6] becomes the same with the security condition [11] by the orthogonality condition [9]. The gap between entanglement and secrecy then remains for bound entangled states \(\rho_{ABAB'A'B'}\) not satisfying [11]. All this can be seen more quantitatively in the following.

Example. Let us retake the shield states in [10]. Since shield states are separable the state \(\sigma_{AB}\) is entangled if \(p \leq p_1\) where

\[
p_j = \frac{1}{2}((1 - \frac{1}{2^j} + 1)^{-1},
\]
and $\rho_{ABA'B'}$ is of PPT for $p \leq 1/3$. From the key distillability condition (11), the state is key-distillable by the classical distillation protocol if $p > p_2$. This shows that the state $\rho_{ABA'B'}$ is key-distillable with small size of shield states i.e. $l \geq 1$, differently from the case of the recurrence protocol where $l$ should be large enough. Note that as $l$ goes very large, $p_2$ converges to $p_1$. From Fig. 2, the entanglement condition is generally weaker than the security bound, so the gap between and entanglement and secrecy still remains.

To summarize, we have identified those entangled states that are key-distillable by the known classical and quantum distillation protocols, while considering local environment in the security analysis. Then, much wider range of bound entangled states are turned out to be key-distillable, and for a particular choice of shield states, entanglement itself means the general security. It is also shown that, while local environment is considered in the key distillation scenario, the classical distillation could tolerate higher rates of errors than the quantum distillation. This is noteworthy for QKD protocols in long-distances, that work with high rates of errors in general. Notwithstanding, the result presented here is not mislead to that the classical is superior than any quantum protocols. Rather, there may exist a more general quantum key distillation protocol. That is, what we have shown implies that, when known distillation protocols apply to bound entangled states in considering local environment, it is optimal to measure the key part right after quantum states are shared. It still remains open if entanglement itself implies secrecy in general, and this is actually related to the existence of bipartite bound information.

Finally, we would like to mention that known security bounds of QKD protocols may be improved further by considering local environment of two honest parties. This holds true whenever the shared state is of the form in (3). In fact, earlier works presented in Refs. [14, 25, 26] apply local operations to create shield states in such a way that not all them are the same. Then, as we have discussed, not all errors have to be corrected. For instance, the bound 11% of the BB84 protocol has been improved up to 12.1% by considering distillation of a private state having a local and individual twisting i.e. in $U_{ij}^{AB} = U_i^A \otimes U_j^B$ [14, 22], and even up to 12.9% using a local and collective $n$-copy twisting [26] i.e. for $n$ copies, $U_{ABA'B'}^{(n)} = \sum_{\vec{i}, \vec{j}} |\vec{i}, \vec{j}\rangle \langle \vec{i}, \vec{j}| \otimes U_i^{A(n)} \otimes U_j^{B(n)}$ where $\vec{i} = (i_1, \ldots, i_n)$.

This work is supported by the IT R&D program of MIC/IITA [2005-Y-001-04 , Development of next generation security technology].

* Electronic address: bae.joonwoo@gmail.com

[1] The probability distribution of a secret key shows, i)perfect correlation between two honest parties, $p_{AB}(0,0) = p_{AB}(1,1) = 1/2$ and ii) independence against an eavesdropper, $p_{ABE} = p_{AB}p_E$.
[2] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, Phys. Rev. A 54, 3824 (1996)
[3] C. H. Bennett and G. Brassard, Proceedings of International Conference on Computer Systems and Signal Processing, p. 175 (1984).
[4] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. 74, 145 (2002).
[5] P. W. Shor and J. Preskill, Phys. Rev. Lett. 85, 441, (2000)
[6] A. Acín and N. Gisin Phys. Rev. Lett. 94, 020501 (2005).
[7] See problem 24 in http://www.imaph.tubs.de/qi/problems/.
[8] K. Horodecki, M. Horodecki, P. Horodecki, and J. Oppenheim, Phys. Rev. Lett. 94, 160502 (2005)
[9] C. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. Smolin, and W. Wootters, Phys. Rev. Lett. 76 722(1996).
[10] U. Maurer, IEEE Trans. Inf. Theory 39, 733 (1993).
[11] F. Verstraete, J. Dehaene, and B. DeMoor, Phys. Rev. A 64, 010101 (2001)
[12] M. Curty, M. Lewenstein and N. Luetkenhaus, Phys. Rev. Lett. 92, 217903 (2004).
[13] M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Lett. A 223, 1 (1996)
[14] B. Kraus, N. Gisin, and R. Renner, Phys. Rev. Lett. 95, 080501 (2005)
[15] R. Renner, PhD thesis.
[16] D. P. Chi, J. W. Choi, J. S. Kim, T. Kim, S. Lee, Phys. Rev. A 75, 032306 (2007)
[17] The following holds always true, $\text{tr}[\sigma_i - \sigma_j] \leq \text{tr}[|\sigma_i - \sigma_j|]$, from which it follows that $\lambda_1 \leq \mu_2$ and $\lambda_2 \leq \mu_4$.
[18] K. Horodecki, M. Horodecki, P. Horodecki, and J. Oppenheim, quant-ph/0506189
[19] J. Bae and A. Acín, Phys. Rev. A 75, 012334 (2007)
[20] K. Horodecki, M. Horodecki, P. Horodecki, D. Leung, and J. Oppenheim, to appear IEEE, arXiv:quant-ph/0608195
[21] All steps of the classical distillation commute with a twisting operation [20], and the AD does so since both $\rho_{AB}$ and $\sigma_{AB}$ exploit the same bit-correlation and the AD is only concerned with bit errors.
[22] I. Devetak and A. Winter, Phys. Rev. Lett. 93, 080501 (2004); R. Renner and R. Koenig, quant-ph/0403133
[23] A. Acín, J. Bae, E. Bagan, M. Baig, Ll. Masanes, and R. Muñoz-Tapia, Phys. Rev. A 73, 012327 (2006).
[24] B. Kraus, C. Branciard, and R. Renner Phys. Rev. A 75, 012316 (2007)
[25] J. Renes and G. Smith, Phys. Rev. Lett. 98 020502 (2007).
[26] G. Smith, J. Renes, and J. A. Smolin, arXiv:quant-ph/0607018