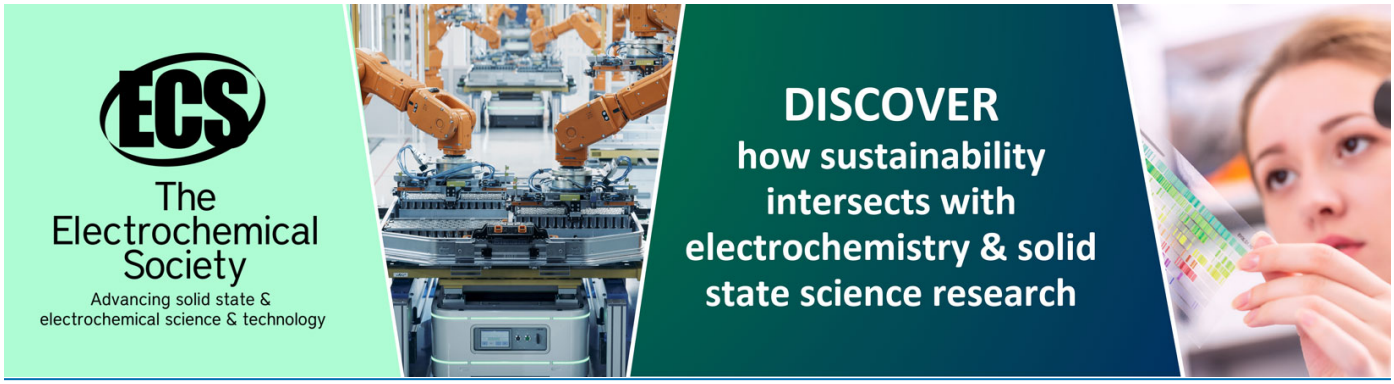
Unconditional security of quantum key distribution and the uncertainty principle



Institute of Physics Publishing
doi:10.1088/1742-6596/36/1/016
Journal of Physics: Conference Series **36** (2006) 98–102
The 12th Central European Workshop on Quantum Optics

Unconditional security of quantum key distribution and the uncertainty principle

Masato Koashi[1,2]

[1] Division of Materials Physics, Graduate School of Engineering Science, Osaka University, 1-3 Machikaneyama, Toyonaka, Osaka 560-8531, Japan
[2] CREST Photonic Quantum Information Project, 4-1-8 Honmachi, Kawaguchi, Saitama 331-0012, Japan

E-mail: koashi@mp.es.osaka-u.ac.jp

Abstract. An approach to the unconditional security of quantum key distribution protocols is presented, which is based on the uncertainty principle. The approach applies to every case that has been treated via the argument by Shor and Preskill, but it is not necessary to find quantum error correcting codes. It can also treat the cases with uncharacterized apparatuses. The proof can be applied to cases where the secret key rate is larger than the distillable entanglement.

1. Introduction

One of the aims of the cryptography is to allow two legitimate parties, Alice and Bob, to exchange messages secretly without leak to a third party, Eve, who tries to eavesdrop. It is well known that once Alice and Bob share a secret key, which is a common random bit sequence unknown to Eve, they can communicate a secret message of the same length as the key. The task of quantum key distribution (QKD) is a way to produce or to amplify the secret key using the properties of quantum mechanics. For any protocol of QKD, it is vital to have a proof of the unconditional security because the robustness against any kind of attack allowed by the law of physics is the main advantage of QKD over classical schemes aiming at the same task. One of the well-known strategies for the security proof is the argument [1] given by Shor and Preskill, in which a reduction to an entanglement distillation protocol (EDP) based on Calderbank-Shor-Steane (CSS) quantum error correcting codes (QECC) [2, 3] is used to show that the information leak on the final key is negligible. This approach has turned out to be quite versatile due to the simplicity of the idea: for example, the original proof for the BB84 protocol [4] has been extended [5, 6] to cover the B92 protocol [7]. On the other hand, invoking the CSS-QECC in the proof requires the actual users to find a quantum code satisfying a certain property, which is not always an easy task. Even the innocent-looking formula [(1) below] for the asymptotic key gain needs a complicated argument [8] for strict derivation. Decoupling of the error correction and the privacy amplification can be made by encrypting the former [9], but only when it satisfies a constraint coming from the CSS-QECC.

If we look back to the first proof [10] of unconditional security by Mayers, we notice that it also has its own merits. One disadvantage, the complexity of the proof, was recently remedied by a simple proof [11] by Koashi and Preskill based on the same spirit, namely, reduction to a two-party protocol by omitting one of the legitimate users by a symmetry argument. In this line

of approach, the error correction and the privacy amplification are decoupled from the start, and we can just use any conventional scheme for the error correction. The proof also shows a peculiar and useful property, which allows the use of basis-independent uncharacterized sources or detectors. For example, if we use an ideal detector, the source can be anything as long as it does not reveal which basis is used in the BB84 protocol. We can still use the same formula for the key rate, indicating that any fault in the source can be automatically caught in the form of an increase in the observed bit errors. Unfortunately, the argument of omitting one party relies heavily on the symmetry of the BB84 protocol, and it cannot be applied to the protocols with no such symmetry.

Here we present an approach to the unconditional security based on uncertainty principle. This argument has the same advantages in the Mayers-Koashi-Preskill argument, while retaining the versatility of the Shor-Preskill argument. In fact, in any protocol having a proof that relies on the Shor-Preskill argument, we can decouple the error correction and the privacy amplification just by encrypting the former, thereby relieve it from the constraint of CSS-QECC. The new approach allows us to solve security problems with imperfect devices that were beyond either of the previous arguments. For example, we can derive a key rate formula for the BB84 protocol with an arbitrary source, the properties of which are unknown except for a bound on the fidelity between the averaged states for two bases [12]. Our proof also provides an insight into the recently predicted phenomenon of secure key from bound entanglement [13].

2. Basic ideas in the security proof

Most of the QKD protocols can be equivalently described by an entanglement-based protocol, in which Alice and Bob share a pair of quantum systems $\mathcal{H}_A \otimes \mathcal{H}_B$ after discarding other systems used for random sampling tests. The state ρ_0 of $\mathcal{H}_A \otimes \mathcal{H}_B$ at this point is not fixed and may be highly correlated among subsystems due to Eve's intervention, but the results of the tests may give a set of promises on the possible state. For example, in the case of Shor-Preskill proof, $\mathcal{H}_A \otimes \mathcal{H}_B$ is composed of N pairs of shared qubits, and there is a promise that the following statements hold except for an exponentially small probability: Suppose that each qubit is measured on z or x basis. Then the number $n_{\rm bit}$ of qubits showing the bit error ($\sigma_z \otimes \sigma_z = -1$) satisfies $n_{\rm bit}/N \leq \delta_{\rm bit}$, and the number $n_{\rm ph}$ with the phase error ($\sigma_x \otimes \sigma_x = -1$) satisfies $n_{\rm ph}/N \leq \delta_{\rm ph}$. Here $\delta_{\rm bit}$ and $\delta_{\rm ph}$ are determined from the results of the test. Here we consider more general cases, in which the size of $\mathcal{H}_A \otimes \mathcal{H}_B$ is arbitrary. We give a proof for the unconditional security of the protocols having the following form:

Actual Protocol — Alice and Bob make measurements on $\mathcal{H}_A$ and on $\mathcal{H}_B$, respectively. Through an encrypted classical communication consuming r bits of secret key, they agree on an N-bit reconciled key $\boldsymbol{\kappa}_{\rm rec}$, except for a negligible failure probability. In the binary vector space on N bits, one party chooses a linearly-independent set $\{\boldsymbol{V}_k\}_{k=1,\ldots,N-m}$ of N-bit sequences randomly and announce it. The k-th bit of the final key $\boldsymbol{\kappa}_{\rm fin}$ is defined as scalar product $\boldsymbol{\kappa}_{\rm rec} \cdot \boldsymbol{V}_k$.

This protocol newly produces $N - m$ bits of secret key, and the net secret key gain is $G = N - r - m$ bits. We first give an overview of our security proof, taking the Shor-Preskill (SP) case as an example. The core of our approach is to regard $\boldsymbol{\kappa}_{\rm rec}$ as the outcome of z-basis measurements on N virtual qubits $\mathcal{K}^{\otimes N}$. In the SP case, we may just identify $\mathcal{H}_B$ with $\mathcal{K}^{\otimes N}$. Next, we ask how we could have predicted the N-bit outcome $\boldsymbol{X}$ if the N qubits had been measured in the x-basis. In the SP case, we could have measured $\mathcal{H}_A$ on the x-basis to obtain an N-bit outcome μ. The random sampling tests assure that this outcome coincides with $\boldsymbol{X}$ within $\sim N\delta_{\rm ph}$-bit errors, namely, the conditional entropy is bounded as $H(\boldsymbol{X}|\mu) \leq N\xi$ with $\xi \sim h(\delta_{\rm ph})$, where $h(y) \equiv -y \log y - (1-y)\log(1-y)$. Then, the uncertainty of the complementary observable, namely, the z-basis outcome $\boldsymbol{\kappa}_{\rm rec}$, should satisfy $H(\boldsymbol{\kappa}_{\rm rec}) \geq N - N\xi$ according to the entropic uncertainty relation [14]. Hence, it is not surprising that Eve has negligible information on the final key $\boldsymbol{\kappa}_{\rm fin}$ when $m = N[h(\delta_{\rm ph}) + \epsilon]$. Since the error correction

consumes $r = N[h(\delta_{\rm bit}) + \epsilon]$ bits of secret key, we arrive at the familiar asymptotic net key gain

$$G = N[1 - h(\delta_{\rm bit}) - h(\delta_{\rm ph})]. \tag{1}$$

3. Main theorem

The rough sketch of the proof in the previous section can be made strict and generalized as follows. First we choose a quantum operation Λ that converts state ρ on $\mathcal{H}_A \otimes \mathcal{H}_B$ to state $\Lambda(\rho)$ on $\mathcal{H}_R \otimes \mathcal{K}^{\otimes N}$, where $\mathcal{H}_R$ stands for an ancillary system R. We further consider a measurement M_R on $\mathcal{H}_R$, and define μ to be its outcome. As we have seen, in the SP case we may choose Λ to be a trivial operation Λ_0 that just changes the definition as $\mathcal{H}_A \cong \mathcal{H}_R$ and $\mathcal{H}_B \cong \mathcal{K}^{\otimes N}$, and take M_R to be the x-basis measurement. But the security proof here allows almost free choices of Λ and M_R, except for the following requirement:

Assumption 1 — The application of Λ followed by the standard z-basis measurements on $\mathcal{K}^{\otimes N}$ is equivalent to the measurement of $\boldsymbol{\kappa}_{\rm rec}$ on $\mathcal{H}_A \otimes \mathcal{H}_B$ in Actual Protocol.

Note that within the constraint of Assumption 1, it is even allowed to take Λ involving collective operations over $\mathcal{H}_A$ and $\mathcal{H}_B$.

Let $\boldsymbol{X}$ be the outcome of x-basis measurements on $\mathcal{K}^{\otimes N}$. The next step is to rephrase the condition $H(\boldsymbol{X}|\mu) \leq N\xi$ in the rough sketch in a more rigorous and flexible form:

Assumption 2 — There exists a set T_μ of N-bit sequences with cardinality $|T_\mu| \leq 2^{N\xi}$ for each μ, such that the pair of measurement outcomes $(\mu, \boldsymbol{X})$ satisfies $\boldsymbol{X} \in T_\mu$ except for an exponentially small probability η.

Now we can state the main theorem about the security:

Theorem — If Assumptions 1 and 2 hold for $m = N(\xi + \epsilon)$ with $\epsilon > 0$, Eve's information on $\boldsymbol{\kappa}_{\rm fin}$ in Actual Protocol is at most $h(\eta') + N\eta'$ with $\eta' = \eta + 2^{-N\epsilon}$.

This theorem can be used as follows. First we choose Λ and M_R under Assumption 1. Next, combined with the promises obtained from the random sampling tests, we obtain a value of ξ with which Assumption 2 holds. Then, Theorem assures that the unconditionally secure key gain of at least $G = N - r - N(\xi + \epsilon)$ is achievable. For a good key gain, Λ and M_R should be chosen such that ξ is as large as possible.

4. Proof of the main theorem

Thanks to Assumption 1, Eve's knowledge on $\boldsymbol{\kappa}_{\rm fin}$ in Actual Protocol is the same as that on $\boldsymbol{\kappa}_{\rm fin}$ obtained from $\mathcal{H}_A \otimes \mathcal{H}_B$ by the following procedure.

Protocol 1 — Apply Λ and discard $\mathcal{H}_R$. For the N qubits $\mathcal{K}^{\otimes N}$, measure each qubit on z-basis to determine the N-bit key $\boldsymbol{\kappa}_{\rm rec}$. Choose a linearly-independent set $\{\boldsymbol{V}_k\}_{k=1,\ldots N-m}$ randomly, and announce it to Eve. Let $\boldsymbol{\kappa}_{\rm rec} \cdot \boldsymbol{V}_k$ be the k-th bit of the final key $\boldsymbol{\kappa}_{\rm fin}$.

In order to show that Eve has negligible information on $\boldsymbol{\kappa}_{\rm fin}$, we consider yet another protocol, which is later shown to be equivalent to Protocol 1. Define operator $\Sigma_\nu(\boldsymbol{W}) \equiv \sigma_\nu^{b_1}\sigma_\nu^{b_2}\cdots\sigma_\nu^{b_N} (\nu = x, z)$ acting on $\mathcal{K}^{\otimes N}$ for N-bit sequence $\boldsymbol{W} = [b_1 b_2 \cdots b_N]$. The new protocol is defined as follows:

Protocol 2 — (a) Apply Λ and make measurement M_R on $\mathcal{H}_R$ to obtain outcome μ. (b) Choose N-bit sequences $\boldsymbol{W}_j (j = 1, \ldots m)$ randomly, and take an arbitrary linearly-independent set $\{\boldsymbol{V}_k\}_{k=1,\ldots N-m}$ of N-bit sequences satisfying $\boldsymbol{V}_k \cdot \boldsymbol{W}_j = 0$ for any j, k. Announce $\{\boldsymbol{V}_k\}$ to Eve. (c) Measure m observables $\{\Sigma_x(\boldsymbol{W}_j)\}$ to determine an N-bit sequence $\boldsymbol{X}^*$ as we will explain later. (d) Apply unitary operation $\Sigma_z(\boldsymbol{X^*})$. (e) Measure $\{\Sigma_z(\boldsymbol{V}_k)\}$ to determine the $(N-m)$-bit final key $\boldsymbol{\kappa}_{\rm fin}$.

If we measured $\mathcal{K}^{\otimes N}$ on the x-basis before step (c), the outcome $\boldsymbol{X}$ would be one of $2^{N\xi}$ candidates T_μ except for probability η (Assumption 2). Each measurement of $\Sigma_x(\boldsymbol{W}_j)$ in step (c) gives a random parity bit $\boldsymbol{X} \cdot \boldsymbol{W}_j$, which halves the number of candidates. Hence, as in the hushing method of EDP [15], by knowing $m = N(\xi + \epsilon)$ random parity bits we can derive an estimate $\boldsymbol{X}^*$ of $\boldsymbol{X}$ with an exponentially small failure probability $Pr(\boldsymbol{X}^* \neq \boldsymbol{X}) \leq \eta' \equiv \eta + 2^{-N\epsilon}$.

Then, if we measured $\mathcal{K}^{\otimes N}$ on the x-basis after the phase flip in step (d), the outcome would be $\boldsymbol{X}^* - \boldsymbol{X}$, which is $\mathbf{0}$ except for probability η'. This implies that the state σ of the qubits after step (d) is a nearly-pure state satisfying $\langle 0_x^{\otimes N}|\sigma|0_x^{\otimes N}\rangle \geq 1-\eta'$, where $|0_x^{\otimes N}\rangle$ is the x-basis eigenstate for $\boldsymbol{X} = \mathbf{0}$. Since the measurement in step (e) is applied on this nearly-pure state, Eve has only negligible (at most $S(\sigma) \leq [h(\eta') + N\eta']$-bit) information about $\boldsymbol{\kappa}_{\rm fin}$.

The equivalence of the two protocols are easy to be seen. In Protocol 2, the operators $\{\Sigma_z(\boldsymbol{V}_k)\}$ commute with $\Sigma_z(\boldsymbol{X}^*)$ and with $\Sigma_x(\boldsymbol{W}_j)$ since $\boldsymbol{V}_k \cdot \boldsymbol{W}_j = 0$. Hence we can omit steps (c) and (d) and still obtain the same final key. We further notice that M_R is now redundant, and the choosing method of $\{\boldsymbol{V}_k\}$ can be simplified to a random selection. Noting that $\{\Sigma_z(\boldsymbol{V}_k)\}$ can be also obtained through a z-basis measurement on each qubit, we are lead to Protocol 1. This completes the proof.

5. Discussion

We have described a method of proving the unconditional security which unifies two major previous approaches and retains the advantages in both of them. The proof relies on the observation that Alice can guess the z-basis outcomes of virtual N qubits with r-bit uncertainty in the actual protocol, and Alice and Bob can guess the x-basis outcomes with m-bit uncertainty in a equivalent protocol. The "excess" over the uncertainty limit, $N - r - m$, amounts to the key gain. Note that if they share a maximally entangled state (MES), Alice alone can guess for both of the bases. The condition for the secrecy is weaker than that since it allows her to collaborate with Bob nonlocally for the x basis, through any operation Λ satisfying Assumption 1. This difference is considered to be a reason for the gap between distillable entanglement and secret key gain [13]. In fact, examples in [13] are constructed by applying a nonlocal "twisting" operation to $\rho_{AB} \otimes \rho_{A'B'}$, where ρ_{AB} is an MES. Their twisting operations do not change the outcome of z-basis measurement on $\mathcal{H}_B$, which can be regarded as $\boldsymbol{\kappa}_{\rm rec}$. Hence, we can define Λ to be the reverse of the twisting followed by Λ_0, which satisfies Assumption 1. This shows that the present method potentially gives a key rate exceeding the amount of distillable entanglement.

Acknowledgments

The author thanks N. Imoto, J. Preskill and H. -K. Lo for helpful discussions. This work was supported by a MEXT Grant-in-Aid for Young Scientists (B) 17740265.

References

[1] P. W. Shor and J. Preskill. Simple proof of security of the BB84 quantum key distribution protocol. *Phys. Rev. Lett.*, 85:441, 2000.

[2] A. R. Calderbank and P. W. Shor. Good quantum error-correcting codes exist. *Phys. Rev. A*, 54:1098, 1996.

[3] A. M. Steane. Multiple-particle interference and quantum error correction. *Proc. R. Soc. Lond. A*, 452:2551, 1996.

[4] C. H. Bennett and G. Brassard. Quantum cryptography: public key distribution and coin tossing. In *Proceeding of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India*, pages 175–179. IEEE, New York, 1984.

[5] K. Tamaki, M. Koashi, and N. Imoto. Unconditionally secure key distribution based on two nonorthogonal states. *Phys. Rev. Lett.*, 90:167904, 2003.

[6] M. Koashi. Unconditional security of coherent-state quantum key distribution with a strong phase-reference pulse. *Phys. Rev. Lett.*, 93:120501, 2004.

[7] C. H. Bennett. Quantum cryptography using any two nonorthogonal states. *Phys. Rev. Lett*, 68:3121, 1992.

[8] M. Hamada. Reliability of Calderbank-Shor-Steane codes and security of quantum key distribution, quant-ph/0308039.

[9] H. K. Lo. Method for decoupling error correction from privacy amplification. *New J. Phys.*, 5:36, 2003.

[10] D. Mayers. Quantum key distribution and string oblivious transfer in noisy channels. *Lect. Notes Comput. Sci.*, 1109:343, 1996.

[11] M. Koashi and J. Preskill. Secure quantum key distribution with an uncharacterized source. *Phys. Rev. Lett.*, 90:057902, 2003.

[12] M. Koashi. Simple security proof of quantum key distribution via uncertainty principle, quant-ph/0505108.
[13] K. Horodecki, M. Horodecki, P. Horodecki, and J. Oppenheim. Secure key from bound entanglement. *Phys. Rev. Lett.*, 94:160502, 2005.
[14] H. Maassen and J. B. M. Uffink. Generalized entropic uncertainty relations. *Phys. Rev. Lett.*, 60:1103, 1988.
[15] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters. Mixed-state entanglement and quantum error correction. *Phys. Rev. A*, 54:3824, 1996.