Simple security proof of quantum key distribution based on complementarity

M Koashi\textsuperscript{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

New Journal of Physics 11 (2009) 045018 (12pp)
Received 30 November 2008
Published 30 April 2009
Online at http://www.njp.org/
doi:10.1088/1367-2630/11/4/045018

Abstract. We present an approach to the unconditional security of quantum key distribution protocols based on a complementarity argument. The approach is applicable to, but not limited to, every case that has been treated via the argument by Shor and Preskill based on entanglement distillation, with a benefit of decoupling of the error correction from the privacy amplification. It can also treat cases with uncharacterized apparatuses. We derive a secure key rate for the Bennett–Brassard-1984 protocol with an arbitrary source characterized only by a single parameter representing the basis dependence.

Contents

1. Introduction 2
2. Security proof based on complementarity 3
   2.1. Description of the actual protocol 3
   2.2. Basic idea of the security proof 3
   2.3. Main theorem 4
   2.4. Proof of the main theorem 6
3. Security of the BB84 protocol with uncharacterized sources 7
   3.1. BB84 with a basis-independent uncharacterized source 7
   3.2. BB84 with an arbitrary source 8
4. Security of the six-state protocol 10
5. Conclusion 11
Acknowledgments 11
References 12
1. Introduction

The aim of quantum key distribution (QKD) is to distribute a secret key between two distant parties, Alice and Bob, under the intervention by a third party, Eve. For any protocol of QKD, it is vital to have a proof of the unconditional security, which is the robustness against any kind of attack allowed by the law of physics, since it 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 us to choose a method for error correction and a method for privacy amplification carefully such that they correspond to a quantum code, which sometimes causes complication [8]. 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 beginning, and we can just use any conventional scheme for the error correction. The proof also has 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 error rates. 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.

In this paper, we present a general approach to the unconditional security based on a complementarity argument, extending the spirit initiated in the first proof by Mayers and applying tools developed in the proof by Lo and Chau [12] and the one by Shor and Preskill [1]. The new approach 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. As an example, we 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 the two bases. Our proof also provides an insight into the recently predicted phenomenon of secure key from bound entanglement [13].

This paper is organized as follows. In section 2, we describe our main result, a simple security proof based on complementarity. After the main idea is explained, we prove a security statement in terms of the fidelity and the trace distance to the ideal key. As an example of

---

3 The main idea was presented in the 12th Central European Workshop on Quantum Optics (Ankara, Turkey).
applications, we apply the proof to the BB84 protocol with uncharacterized sources in section 3.
In section 4, we reproduce the key rate for the six-state protocol. Then we conclude this paper in section 5.

2. Security proof based on complementarity

2.1. Description of the actual protocol

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 the parameter estimation via random sampling tests. (Here and henceforth, we refer to a quantum system by its Hilbert space.) The state $\rho_0$ of $\mathcal{H}_A \otimes \mathcal{H}_B$ at this point is not completely specified 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 the Shor–Preskill proof (we call it the Shor–Preskill case below), $\mathcal{H}_A \otimes \mathcal{H}_B$ 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 $n_{\text{bit}}$ of qubits showing the bit error ($\sigma_z \otimes \sigma_z = -1$) satisfies $n_{\text{bit}}/N \leq \delta_{\text{bit}}$, and the number $n_{\text{ph}}$ with the phase error ($\sigma_z \otimes \sigma_x = -1$) satisfies $n_{\text{ph}}/N \leq \delta_{\text{ph}}$. Here, $\delta_{\text{bit}}$ and $\delta_{\text{ph}}$ 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 $\mathcal{H}_B$, respectively. Through an encrypted classical communication consuming $r$ bits of secret key, they agree on an $N$-bit reconciled key $\kappa_{\text{rec}}$, except for a small failure probability $\zeta$. In the binary vector space on $N$ bits, one party chooses a linearly independent set $\{V_k\}_{k=1,...,N-m}$ of $N$-bit sequences randomly and announces it. The $k$th bit of the final key $\kappa_{\text{fin}}$ is defined as scalar product $\kappa_{\text{rec}} \cdot V_k$.

The definition of $\kappa_{\text{rec}}$ should be chosen depending on how the error correction is done. For example, if Bob’s $N$-bit sifted key $\kappa_{\text{Bsif}}$ is regarded as the correct one and Alice tries to correct the error in her key $\kappa_{\text{Asif}}$ relative to $\kappa_{\text{Bsif}}$, we may simply define $\kappa_{\text{rec}}$ to be Bob’s sifted key, $\kappa_{\text{rec}} = \kappa_{\text{Bsif}}$. In a more complicated case, $\kappa_{\text{rec}}$ may coincide neither with $\kappa_{\text{Asif}}$ nor $\kappa_{\text{Bsif}}$. After the error correction, Alice and Bob will obtain $N$-bit reconciled keys $\kappa_{\text{Arc}}$ and $\kappa_{\text{Brc}}$, respectively, where $\kappa_{\text{Arc}} = \kappa_{\text{Brc}} = \kappa_{\text{rec}}$ holds with probability no less than $1 - \zeta$. Then they proceed to the privacy amplification to shorten their key by $m$ bits. In the actual protocol above, we adopt a protocol of privacy amplification based on announcing random bit sequences $\{V_k\}_{k=1,...,N-m}$, which is simple in a theoretical point of view. Alice calculates $\{\kappa_{\text{Arc}} \cdot V_k\}_{k=1,...,N-m}$ to determine her $(N - m)$-bit final key $\kappa_A$, and Bob calculates $\{\kappa_{\text{Brc}} \cdot V_k\}_{k=1,...,N-m}$ to determine his final key $\kappa_B$. Note that $\kappa_A = \kappa_B = \kappa_{\text{fin}}$ holds except for probability $\zeta$. The net secret key gain of the actual protocol is $G = N - r - m$ bits, since it produces $(N - m)$ bits of new secret key by consuming $r$ bits of secret key.

2.2. Basic idea of the security proof

Here, we give an overview of our security proof, taking the Shor–Preskill case as an example. The core of our approach is to regard $\kappa_{\text{rec}}$ as the outcome of $z$-basis measurements on $N$ virtual
qubits $K^{\otimes N}$. In the Shor–Preskill case, we may just identify $H_B$ with $K^{\otimes N}$. Next, we ask how we could have predicted the $N$-bit outcome $X$ if the $N$ qubits had been measured in the $x$ basis. In the Shor–Preskill case, we could have measured $H_A$ on the $x$ basis to obtain an $N$-bit outcome $\mu$. The random sampling tests assure that this outcome coincides with $X$ within $\sim N\delta_{ph}$-bit errors, namely, the conditional entropy is bounded as $H(X|\mu) \leq N\xi$ with $\xi \sim h(\delta_{ph})$, where

$$h(y) \equiv -y \log_2 y - (1 - y) \log_2(1 - y).$$  \hspace{1cm} (1)

The fact that Alice can predict $X$ well means that the $z$-basis outcome $\kappa_{rec}$, which is an observable complementary to $X$, should be hard to predict due to the uncertainty principle.

If we were allowed to use the entropic uncertainty relation [15] here, we could say $H(\kappa_{rec}) \geq N - N\xi \sim N - Nh(\delta_{ph})$ holds for the uncertainty of $\kappa_{rec}$ from Eve’s point of view. Then, Eve will have negligible information on the final key $k_{fin}$ after the privacy amplification with $m = N[h(\delta_{ph}) + \epsilon]$. Since the error correction consumes $r = N[h(\delta_{bit}) + \epsilon]$ bits of secret key, we will arrive at the familiar asymptotic net key gain

$$G = N[1 - h(\delta_{bit}) - h(\delta_{ph})].$$  \hspace{1cm} (2)

Of course, we cannot use the entropic uncertainty relation in the security proof, since it does not necessarily apply to every possible attack made by Eve. Instead, we use simple properties of the vector binary space to derive the same key rate in the security proof in section 2.4.

2.3. Main theorem

In this subsection, we state a general security statement applicable to the actual protocol. In order to include the cases other than the Shor–Preskill case, we generalize the meaning of the statement in section 2.2 that Alice has a good prediction of $X$, which is an observable complementary to $\kappa_{rec}$. First, we choose a kind of squashing [16] operation, such as a quantum operation $\Lambda$ that converts state $\rho$ on $H_A \otimes H_B$ to state $\Lambda(\rho)$ on $H_R \otimes K^{\otimes N}$, where $H_R$ stands for a virtual ancillary system. Let $X$ be the $N$-bit sequence obtained as the outcome of $x$-basis measurements on $K^{\otimes N}$. We further consider a measurement $M_R$ on $H_R$, and define $\mu$ to be its outcome. As we have seen, in the Shor–Preskill case we may choose $\Lambda$ to be a trivial operation $\Lambda_0$ that just changes the definition as $H_A \cong H_R$ and $H_B \cong K^{\otimes N}$, and take $M_R$ to be the $x$-basis measurement. But the security proof here allows almost free choices of $\Lambda$ and $M_R$, except for the following requirement:

**Assumption 1.** The application of $\Lambda$ followed by the standard $z$-basis measurement on $K^{\otimes N}$ is equivalent to the measurement of $\kappa_{rec}$ on $H_A \otimes H_B$ in the actual protocol.

Within this constraint, it is even allowed to take $\Lambda$ involving collective operations over $H_A$ and $H_B$. That is to say, Alice is allowed to communicate with Bob freely over a quantum channel when we ask how well they can predict the value of $X$, as long as the observable $X$ and the reconciled key $\kappa_{rec}$ in the actual protocol form a pair of complementary observables.

The next step is to rephrase the condition $H(X|\mu) \leq N\xi$ appearing in the rough sketch in section 2.2 into a more rigorous and flexible form:

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

Now, we can state the main theorem about the security of the actual protocol. Let $p(\kappa)$ be the probability that the $(N - m)$-bit final key $k_{fin}$ in the actual protocol takes a specific value $\kappa$,
and \( \rho_E(\kappa) \) be the quantum state of Eve’s system when \( \kappa_{fin} = \kappa \). The property of the final key in relation to Eve is then completely described by the quantum state

\[
\rho_{fin} = \sum_{\kappa} p(\kappa) |\kappa\rangle \langle \kappa| \otimes \rho_E(\kappa),
\]

where we have assumed that the final key \( \kappa_{fin} \) has been written on a quantum system with a Hilbert space of dimension \( 2^{N-m} \) with an orthonormal basis \( \{|\kappa\rangle_c\}_\kappa \). The theorem will be stated on how this state is close to a quantum state for the ideal key

\[
\rho_{ideal} = \left( \sum_\kappa 2^{-\kappa} \langle \kappa| \langle \kappa| \otimes \rho_E(\kappa) \right)
\]

in terms of fidelity \([17, 18]\)

\[
F(\rho, \rho') \equiv (\text{tr} |\sqrt{\rho} \sqrt{\rho'}|)^2, \quad |O| \equiv \sqrt{O^\dagger O}.
\]

**Theorem.** If assumptions 1 and 2 hold for \( m = N(\xi + \epsilon) \) with \( \epsilon > 0 \), there exists a density operator \( \rho_E \) such that

\[
F(\rho_{fin}, \rho_{ideal}) \geq 1 - \eta'
\]

with

\[
\eta' \equiv \eta + 2^{-N\epsilon}.
\]

If we can further assume that Eve only has a classical variable \( E \), the mutual information satisfies

\[
I(\kappa_{fin}; E) \leq h(\eta') + N\eta'.
\]

The proof will be given in the next subsection, and here we make a few remarks. This theorem can be used as follows. First, we choose \( \Lambda \) and \( M_R \) under assumption 1. Next, combined with the promises obtained from the random sampling tests, we obtain a value of \( \xi \) with which assumption 2 holds. Then, the theorem assures that the secure key gain of at least \( G = N - r - N(\xi + \epsilon) \) is achievable. For a good key gain, \( \Lambda \) and \( M_R \) should be chosen such that \( \xi \) is as small as possible.

In our approach, the imperfection in the final key in the actual protocol is stated in terms of two parameters; \( \zeta \) for the disagreement between Alice’s and Bob’s key, and \( \eta' \) for the nonuniformity and the leak to Eve. Considering the feature of decoupling between the error correction and the privacy amplification, we believe it is best to leave as it is, but for convenience we also represent the imperfection in terms of a single parameter describing the closeness to an ideal \( (N - m) \)-bit secret key. Let \( |\kappa_A\rangle_a|\kappa_B\rangle_b|\kappa\rangle_c \) be the state where the value of Alice’s final key is \( \kappa_A \), Bob’s is \( \kappa_B \), and \( \kappa \) is the value of \( \kappa_{fin} = \kappa_{rec} \cdot V_k \) on which Alice and Bob tried to agree with failure probability \( \zeta \). Then we can write the final state of the actual protocol as

\[
\tau_{fin} = \sum_{\kappa_A, \kappa_B, \kappa} p(\kappa_A, \kappa_B, \kappa) |\kappa_A\kappa_B\kappa\rangle \langle \kappa_A\kappa_B\kappa|_{abc} \otimes \rho_E(\kappa_A, \kappa_B, \kappa),
\]

where

\[
\sum_{\kappa} p(\kappa, \kappa, \kappa) = 1 - \zeta.
\]

Let us define state \( \tau' \) as the one obtained after Alice’s and Bob’s keys in \( \tau_{fin} \) are replaced with \( \kappa \)

\[
\tau' \equiv \sum_{\kappa_A, \kappa_B, \kappa} p(\kappa_A, \kappa_B, \kappa) |\kappa\kappa\kappa\rangle \langle \kappa\kappa\kappa|_{abc} \otimes \rho_E(\kappa_A, \kappa_B, \kappa).
\]
From equation (8), we have
\[
\text{tr}|\tau_{\text{fin}} - \tau'| = 2\zeta.
\] (10)

On the other hand, since \(\text{tr}_{ab}(\tau') = \rho_{\text{fin}}\) by definition, we have
\[
\tau' = \sum_k p(k)|kkk\rangle\langle kkk|_{abc} \otimes \rho_E(k).
\] (11)

Let \(\tau_{\text{ideal}}\) be a state for the ideal secret key defined by
\[
\tau_{\text{ideal}} \equiv \sum_k 2^{-(N-m)}|kkk\rangle\langle kkk|_{abc} \otimes \rho_E.
\] (12)

Obviously, we have
\[
\text{tr}|\tau' - \tau_{\text{ideal}}| = \text{tr}|\rho_{\text{fin}} - \rho_{\text{ideal}}|.
\] (13)

Since the theorem gives \(\text{tr}|\rho_{\text{fin}} - \rho_{\text{ideal}}| \leq 2\sqrt{1 - F(\rho_{\text{fin}}, \rho_{\text{ideal}})} \leq 2\sqrt{\eta'}\), we have
\[
\text{tr}|\tau' - \tau_{\text{ideal}}| \leq 2\sqrt{\eta'}.
\] (14)

Combined with equation (10), we obtain
\[
\text{tr}[\text{tr}_c(\tau_{\text{fin}}) - \text{tr}_c(\tau_{\text{ideal}})] \leq \text{tr}|\tau_{\text{fin}} - \tau_{\text{ideal}}| \leq 2\zeta + 2\sqrt{\eta'}.
\] (15)

2.4. Proof of the main theorem

As an alternative to the actual protocol, let us introduce protocol 1 as follows:

**Protocol 1.** Apply operation \(\Lambda\) and discard \(\mathcal{H}_R\). For the \(N\) qubits \(\mathcal{K}^{\otimes N}\), measure each qubit on the \(z\) basis to determine the \(N\)-bit key \(k_{\text{rec}}\). Choose a linearly independent set \(\{V_k\}_{k=1,\ldots,N-m}\) randomly, and announce it to Eve. Let \(k_{\text{rec}}\cdot V_k\) be the \(k\)th bit of the final key \(k_{\text{fin}}\).

Thanks to assumption 1, Eve’s knowledge on \(k_{\text{fin}}\) in the actual protocol is the same as that on \(k_{\text{fin}}\) obtained from protocol 1. That is to say, if we begin with the same initial state, both procedures end up in the same state \(\rho_{\text{fin}}\) of equation (3).

In order to show that Eve has negligible information on \(k_{\text{fin}}\), we consider yet another protocol, which carries out a phase error correction and will soon be shown to be equivalent to protocol 1. Define operator
\[
\Sigma_v(W_v) = \sigma_v^{b_1}\sigma_v^{b_2} \cdots \sigma_v^{b_N} (v = x, z)
\] (16)
acting on \(\mathcal{K}^{\otimes N}\) for \(N\)-bit sequence \(W = [b_1, b_2, \ldots, b_N]\). The new protocol is defined as follows:

**Protocol 2.** (a) Apply \(\Lambda\) and make measurement \(M_\mu\) on \(\mathcal{H}_R\) to obtain outcome \(\mu\). (b) Choose \(N\)-bit sequences \(W_j (j = 1, \ldots, m)\) randomly, and take an arbitrary linearly independent set \(\{V_k\}_{k=1,\ldots,N-m}\) of \(N\)-bit sequences satisfying \(V_k \cdot W_j = 0\) for any \((j, k)\). Announce \(\{V_k\}\) to Eve. (c) Measure \(m\) observables \(\{\Sigma_v(W_j)\}\) to determine an \(N\)-bit sequence \(X^*\) as we will explain later. (d) Apply unitary operation \(\Sigma_z(X^*)\). (e) Measure \(\Sigma_v(V_k)\) to determine the \((N-m)\)-bit final key \(k_{\text{fin}}\).

If we measured \(\mathcal{K}^{\otimes N}\) on the \(x\)-basis before step (c), the outcome \(X\) would be one of \(2^N\) candidates \(T_\mu\) except for probability \(\eta\) (assumption 2). Each measurement of \(\Sigma_v(W_j)\) in step (c) gives a random parity bit \(X \cdot W_j\), which intuitively works as a syndrome bit in a code for correcting phase errors. For every wrong candidate of \(X\), the probability of sharing the correct parity bit is exactly one half. As a result, one random parity bit almost halves the number of
candidates. Hence, as in the hushing method of EDP [19], by knowing \( m = N(\xi + \epsilon) \) random parity bits we can derive an estimate \( X^* \) of \( X \) with an exponentially small failure probability
\[
Pr(X^* \neq X) \leq \eta' \equiv \eta + 2^{-Ne}.
\]
Then, if we measured \( K^\otimes N \) on the \( x \) basis after the phase flip in step (d), the outcome would be \( X = X^* \), which is \( 0 \) except for probability \( \eta' \). This implies that the state \( \sigma \) of the qubits after step (d) is a nearly-pure state \( \sigma \) satisfying
\[
\langle 0_x^\otimes N | \sigma | 0_x^\otimes N \rangle = F(\sigma, | 0_x^\otimes N \rangle | 0_x^\otimes N \rangle) \geq 1 - \eta',
\]
where \( | 0_x^\otimes N \rangle \) is the \( x \)-basis eigenstate for \( X = 0 \).

The equivalence of the two protocols is easily seen. In protocol 2, the operators \( \{ \Sigma_z(V_k) \} \) commute with \( \Sigma_z(X^*) \) and with \( \Sigma_z(W_j) \) since \( V_k \cdot W_j = 0 \). 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 \( \{ V_k \} \) can be simplified to a random selection. Noting that \( \{ \Sigma_z(V_k) \} \) can also be obtained through a \( z \)-basis measurement on each qubit, we are lead to protocol 1.

Let \( \sigma_{\text{qubits,E}} \) be the state of the qubits and Eve’s system \( E \) after step (d). Since \( \text{tr}_E(\sigma_{\text{qubits,E}}) = \sigma \), we can pick a state \( \rho_E \) of Eve’s system such that
\[
F(\sigma_{\text{qubits,E}}, | 0_x^\otimes N \rangle | 0_x^\otimes N \rangle \otimes \rho_E) = F(\sigma, | 0_x^\otimes N \rangle | 0_x^\otimes N \rangle)
\]
holds. From equation (17), we have
\[
F(\sigma_{\text{qubits,E}}, | 0_x^\otimes N \rangle | 0_x^\otimes N \rangle \otimes \rho_E) \geq 1 - \eta'.
\]
When we proceed to step (e) with state \( \sigma_{\text{qubits,E}} \), we should obtain state \( \rho_{\text{fin}} \) due to the equivalence of the actual protocol, protocol 1 and protocol 2. Instead, if we apply step (e) to state \( | 0_x^\otimes N \rangle \otimes \rho_E \), the final state is easily calculated to be \( \rho_{\text{ideal}} \). Since the fidelity never decreases in step (e), we have \( F(\rho_{\text{fin}}, \rho_{\text{ideal}}) \geq 1 - \eta' \). On the other hand, the statement on the mutual information in the theorem immediately follows from \( S(\sigma) \leq h(\eta') + N\eta' \).

3. Security of the BB84 protocol with uncharacterized sources

In this section, we discuss the security of the BB84 protocol when the light source is uncharacterized except for a few promises, as an application of the security proof.

3.1. BB84 with a basis-independent uncharacterized source

This is the case where Alice uses a basis-independent uncharacterized source and Bob uses an ideal detector in the BB84 protocol, which was analyzed in [11]. Let \( \rho_{ab} \) acting on \( H_Q \) be the state of Alice’s source for the basis \( a = 0, 1 \) and the bit value \( b = 0, 1 \). Alice chooses basis \( a \) randomly, and then with probability \( p_{ab} \) (note that \( p_{ab} + p_{a\overline{b}} = 1 \), Alice sends out \( \rho_{ab} \) to a quantum channel, which may be tampered with by Eve. Bob receives a qubit state on \( K_B \) from the channel, on which he conducts the ideal \( z \)- or \( x \)-basis measurement depending on his random basis choice \( a' = 0, 1 \), respectively. Subsequently, they make \( a \) and \( a' \) public. After repeating this many times, they randomly sample events with \( a = a' \) to define \( k_{\text{rec}} \). Alice obtains \( k_{\text{rec}} \) with the help of a secret communication from Bob consuming \( r = N[h(\delta_0) + \epsilon] \) bits of secret key. (The portion with \( a = a' = 1 \) can be handled similarly.)

The basis-independent source satisfies \( \rho_0 = \rho_1 \), where \( \rho_0 \equiv p_{a0}\rho_{ab} + p_{a1}\rho_{a\overline{b}} \). Then, we can find a state \( \chi \) on \( H_S \otimes H_Q \) and measurements \( M_b \) on \( H_S \) with positive operator valued measure (POVM) elements \( \{ F_{ab}, F_{a\overline{b}} \} \), such that \( \text{tr}_S[(F_{ab} \otimes 1_Q)\chi] = p_{ab}\rho_{ab} \). We are thus allowed to
consider an equivalent protocol in which Alice prepares $\chi$ and conducts measurement $M_a$ on $\mathcal{H}_S$ to determine her bit value $b$. This new protocol takes the form of the actual protocol by defining $\mathcal{H}_A = \mathcal{H}_S^\otimes N$ and $\mathcal{H}_B = \mathcal{K}_B^\otimes N$. For the security proof, we choose $\Lambda = \Lambda_0$, and assume $M_R$ to be $M_1$ applied on each $\mathcal{H}_S$. In order to establish a statement like assumption 2, we need to know the relation between the outcome of $M_1$ and the outcome of the $x$-basis measurement on $\mathcal{K}_B$. Fortunately, this is exactly the same pair of measurements used in determining the error rate $\delta_1$. Hence, assumption 2 holds with $\xi = h(\delta_1) + \epsilon'$, and we obtain the asymptotic net key gain
\[ G = N[1 - h(\delta_0) - h(\delta_1)]. \] (20)

Note that everything we need in the actual protocol is $\delta_0$ and $\delta_1$. There is no need to know the identities of $\chi$ and $M_a$, and hence no need to characterize the source to determine $\rho_{ab}$, as long as it is guaranteed to be basis independent. We also note that a similar argument with the roles of Alice and Bob exchanged leads to a security proof with uncharacterized detectors with a basis-independent efficiency [20].

3.2. BB84 with an arbitrary source

The main theorem allows us to prove unconditional security in the general case of $\rho_0 \neq \rho_1$. Of course, we need to know something about the source states since the protocol is entirely insecure if $\rho_0$ and $\rho_1$ are orthogonal. A natural choice is to assume that we know a single parameter $\Delta$, which determines a lower bound on the fidelity between the two states
\[ 1 - 2\Delta \leq \sqrt{F(\rho_0, \rho_1)}. \] (21)

Note that for $F < 1$, we can still find two pure states $|\chi_0\rangle$ and $|\chi_1\rangle$ in $\mathcal{H}_S \otimes \mathcal{H}_Q$ satisfying $\langle \chi_0|\chi_1\rangle = 1 - 2\Delta$ such that for each value of $a$, there is a POVM measurement $M_a = \{|F_{a0}, F_{a1}\}$ on $\mathcal{H}_S$ satisfying $\text{tr}_S[(F_{ab} \otimes I_Q)|\chi_a\rangle\langle \chi_a|] = p_{ab}\rho_{ab}$. For a special case where $\mathcal{H}_S$ includes a qubit as a subsystem and $M_0$ and $M_1$ are the standard $x$- and $z$-basis measurements on that qubit, Gottesman et al [16] derived a secure key rate along the line of the Shor–Preskill argument, which allows a positive key gain up to $\Delta < 0.029$. Here, we can derive a better key rate formula for arbitrary states $\rho_{ab}$.

Let us consider an equivalent protocol in which Alice chooses the basis $a$ by measuring a ‘quantum coin’ [16] described by a qubit $\mathcal{K}_C$. If she prepares $\mathcal{H}_S \otimes \mathcal{H}_Q \otimes \mathcal{K}_C$ in state $|\Psi\rangle = (|\chi_0\rangle|0_z\rangle_C + |\chi_1\rangle|1_z\rangle_C)/\sqrt{2}$ and measures $\mathcal{K}_C$ on $z$ basis, the outcome $a$ is random and $\mathcal{H}_S \otimes \mathcal{H}_Q$ is prepared in state $|\chi_a\rangle$. Then she conducts measurement $M_a$ on $\mathcal{H}_S$ to prepare $\rho_{ab}$ with probability $p_{ab}$. In order to prove security, we follow the same argument as in the basis-independent case up to the point where we need to know the relation between the outcome of $M_1$ and that of $x$-basis measurement on $\mathcal{K}_B$. Unfortunately, we have no direct clue this time. The expected error rate $\delta_{ph}$ in this fictitious set of measurements is no longer equal to $\delta_1$, since the former is taken for $a = 0$ and the latter is for $a = 1$.

In order to determine upper bounds on $\delta_{ph}$, let us consider the following scenario. Alice starts from $|\Psi\rangle^\otimes L$, and she immediately sends the $L$ copies of system $\mathcal{H}_Q$ into the channel. After Eve’s attack, Bob receives the qubits $\mathcal{K}_B^\otimes L$. For every pair of systems $\mathcal{H}_S \otimes \mathcal{K}_B$, Bob may choose $a'$ randomly, but regardless of its value, measurement $M_1$ and $x$-basis measurement are applied to determine whether there is an error ($t = 1$) or not ($t = 0$). Finally, Alice measures the coin $\mathcal{K}_C$ on $z$ basis to determine $a$. Let us denote the empirical probability for the $L$ events by $r(\cdot)$. For example, $r(t = 1|a = 0)$ is the number of events with $(t = 1, a = 0)$ divided by that of events with $a = 0$.

New Journal of Physics 11 (2009) 045018 (http://www.njp.org/)
The rate $\delta_{ph}$ can be regarded as an error rate in a fair sampling from the events with $a = a' = 0$. Since $a'$ has no effect in the above scenario, it can also be regarded as a fair sampling from the events with $a = 0$. We thus have $\delta_{ph} \cong r(t = 1|a = 0)$. Similarly, $\delta_1 \cong r(t = 1|a = 1)$. Since $r(a = 0) \cong 1/2$, we have
\[
\begin{align*}
  r(t = 1) & \cong (\delta_1 + \delta_{ph})/2, \\
  r(a = 1|t = 1) & \cong \delta_1/(\delta_1 + \delta_{ph}), \\
  r(a = 0|t = 0) & \cong (1 - \delta_{ph})/(2 - \delta_1 - \delta_{ph}).
\end{align*}
\]  

Now, we describe two methods of deriving bounds on $\delta_{ph}$. The first one is to apply the main theorem in section 2.3 formally to the coins, regarding $K_C^{\otimes L}$ as $K^{\otimes N}$ in the theorem. Since $\|c \langle 1_x|\Psi\rangle\|^2 = \Delta$, it is guaranteed that we can distill a secret key of length $L(1 - h(\Delta) - \epsilon)$ from the $z$-basis measurement results. This implies that even with the knowledge of each $t$, the entropy of the outcomes $a$ should be larger than $L(1 - h(\Delta) - \epsilon)$. Hence, in the asymptotic limit we have
\[
1 - h(\Delta) \leq \frac{\delta_1 + \delta_{ph}}{2} h\left(\frac{\delta_1}{\delta_1 + \delta_{ph}}\right) + \frac{2 - \delta_1 - \delta_{ph}}{2} h\left(\frac{1 - \delta_{ph}}{2 - \delta_1 - \delta_{ph}}\right)
\]
\[
\leq h\left(\frac{1 - |\delta_{ph} - \delta_1|}{2}\right),
\]  

which shows that $\delta_{ph} = \delta_1$ for $\Delta = 0$ and $\delta_{ph}$ becomes larger when $\Delta > 0$. If we write the maximum of $\delta_{ph}$ under the above first inequality as $f(\delta_1, \Delta)$, the key gain is given by
\[
G = N[1 - h(\delta_0) - h(\min[1/2, f(\delta_1, \Delta)])].
\]  

This key gain is positive only for $\Delta < 0.056$.

The second method is more complicated, but gives a better rate. We assume that for each event, Alice draws a random binary variable $s$ with a small probability of being $s = 1$. If $s = 0$, she just follows the above scenario, but if $s = 1$, she measures the coin $K_C$ in $x$ basis instead of $z$ basis. Let $\bar{a}$ be the outcome of this $x$-basis measurement, and define $r_{x,j} \equiv r(\bar{a} = 1|s = 1, t = j)$ and $r_{z,j} \equiv r(a = 0|s = 0, t = j)$ for $j = 0, 1$. Since $\|c \langle 1_x|\Psi\rangle\|^2 = \Delta$, we have
\[
r(t = 0)r_{x,0} + r(t = 1)r_{x,1} = r(\bar{a} = 1|s = 1) \cong \Delta.
\]  

Note that $r_{x,j}$ is determined from the outcomes of $x$-basis measurements applied to random samples from the qubits with $t = j$, and $r_{z,j}$ is from the $z$-basis outcomes for the rest of the qubits. This problem of random sampling was analyzed in [5], and it was shown that for all $\epsilon > 0$, except for an exponentially small probability, there exists a qubit state $\rho$ such that $|r_{z,j} - \langle 0_x|\rho|0_x\rangle| < \epsilon$ and $|r_{x,j} - \langle 1_x|\rho|1_x\rangle| < \epsilon$. We thus obtain the following relation in the asymptotic limit:
\[
(1 - 2r_{x,j})^2 + (1 - 2r_{z,j})^2 \leq 1.
\]  

Combining it with $r(t = 1) \cong (\delta_1 + \delta_{ph})/2$, $r_{z,1} \cong \delta_{ph}/(\delta_1 + \delta_{ph})$, $r_{z,0} \cong (1 - \delta_{ph})/(2 - \delta_1 - \delta_{ph})$, and equation (27), we obtain
\[
1 - 2\Delta \leq \sqrt{(1 - \delta_1)(1 - \delta_{ph})} + \sqrt{\delta_1 \delta_{ph}}.
\]  

We can now take $f(\delta_1, \Delta)$ to be the maximum of $\delta_{ph}$ under equation (29), and obtain a better key rate with equation (26). Now the region of positive key gain extends to $\Delta < 0.146$, or
\(F(\rho_0, \rho_1) > 1/2\). Since Alice and Bob do not use the outcome \(\tilde{a}\), this measurement can be omitted. Hence, in the actual BB84 protocol, they only have to discard a small portion of events. From Eve’s point of view, Alice could have measured \(\tilde{a}\) for the discarded events, and it is enough to apply the above security proof.

4. Security of the six-state protocol

In this section, we derive the well-known key rate for the six-state protocol \([21, 22]\) using our framework based on complementarity. The reason why we take up this example is the fact that the six-state protocol uses the correlation between the bit errors and the phase errors to improve the key rate. Since the complementarity argument treats the two kinds of errors separately, it may not be easy to see how it can incorporate such a correlation. The solution is, as we will see, to use the freedom of choosing a collective operation \(\Lambda\) satisfying assumption 1.

In the six-state protocol, Alice and Bob can share \(N\) pairs of qubits with a promise that is stronger than the one in the BB84 protocol. Suppose that each qubit pair is measured on the Bell basis, which reveals the values of the pair of observables \(\sigma_z \otimes \sigma_z\) and \(\sigma_z \otimes \sigma_x\) at the same time. Let \(r_{jk}\) be the fraction among the \(N\) pairs that has resulted in \(\sigma_z \otimes \sigma_z = (-1)^j\) and \(\sigma_z \otimes \sigma_x = (-1)^k\). In the BB84 protocol, we only have good estimates for \(r_{00}\) and \(r_{11}\) (the bit error rate) and \(r_{01} \equiv r_{10} + r_{11}\) (the phase error rate). In the six-state protocol, the additional set of measurements on the \(y\) basis further give a good estimate of \(r_{00} + r_{11}\), and thus each of the four values \(\{r_{jk}\}\) is estimated. The asymptotic key rate is then given \([22]\) by

\[
G = N \left[ 1 - h(r_{bit}) - (1 - r_{bit}) h\left( \frac{r_{01}}{1 - r_{bit}} \right) - r_{bit} h\left( \frac{r_{11}}{r_{bit}} \right) \right],
\]

which is larger than the rate \(G = N[1 - h(r_{bit}) - h(r_{ph})]\) of the BB84 protocol whenever \(r_{ph} \neq r_{11}/r_{bit}\), namely, when there is a correlation between the bit errors and the phase errors.

The key rate of equation (30) is derived using the argument in section 2 by choosing the operation \(\Lambda\) and measurement \(M_R\) as follows. For each qubit pair (let us call them \(\mathcal{K}_A\) and \(\mathcal{K}_B\)), prepare an auxiliary qubit \(\mathcal{K}_C\) in state |0\>_C, and apply a controlled-NOT gate \(U_{\text{CNOT}}\) between \(\mathcal{K}_B\) (control) and \(\mathcal{K}_C\) (target), which effectively copies the \(z\)-basis value of \(\mathcal{K}_B\) onto \(\mathcal{K}_C\) since

\[
U_{\text{CNOT}}|0\>_C = |0\>_B|0\>_C, \quad U_{\text{CNOT}}|1\>_C = |1\>_B|1\>_C.
\]

The operation \(\Lambda\) is defined as this procedure followed by identifying \(\mathcal{K}_A^\otimes N \cong \mathcal{K}_B^\otimes N\) and \(\mathcal{K}_C^\otimes N \cong \mathcal{H}_B\). Since the controlled-NOT gates do not affect the \(z\)-basis outcomes of qubits \(\mathcal{K}_B^\otimes N\), assumption 1 is obviously satisfied by choosing Bob’s \(z\)-basis outcomes as \(\kappa_{\text{rec}}\). For measurement \(M_R\), we assume that each of the qubit pair \(\mathcal{K}_A \otimes \mathcal{K}_C\) is measured on the Bell basis.

Let us see how the outcome of the Bell measurement on \(\mathcal{K}_A \otimes \mathcal{K}_C\) is correlated to that of the \(x\)-basis measurement on \(\mathcal{K}_B\). When the initial state of \(\mathcal{K}_A \otimes \mathcal{K}_B\) is \(|\Theta\>_AB\), the state of \(\mathcal{K}_A \otimes \mathcal{K}_C\) after \(\mathcal{K}_B\) is projected to one of the \(x\)-basis eigenstates \(|0_x\>_B \equiv (|0_x\>_B + |1_x\>_B)/\sqrt{2}\) is calculated to be

\[
B\langle 0_x|U_{\text{CNOT}}|\Theta\>_AB|0_x\>_C = \frac{1}{\sqrt{2}}(|0_x\>_CB|0_z\>_C + |1_x\>_CB|1_z\>_C)|\Theta\>_AB.
\]

which means that the initial state \(|\Theta\>_AB\) is faithfully transferred to the qubit pair \(\mathcal{K}_A \otimes \mathcal{K}_C\). When \(\mathcal{K}_B\) is projected to \(|1_x\>_B \equiv (|0_x\>_B - |1_x\>_B)/\sqrt{2}\), we have

\[
B\langle 1_x|U_{\text{CNOT}}|\Theta\>_AB|1_x\>_C = \frac{1}{\sqrt{2}}(|0_x\>_CB|0_z\>_C - |1_x\>_CB|1_z\>_C)|\Theta\>_AB.
\]
which means that the phase-flipped state \((1 \otimes \sigma_z)|\Theta\rangle_{AB}\) is faithfully transferred to the qubit pair \(K_A \otimes K_C\) in this case. Hence, if the initial \(N\) pairs had no phase errors \((r_{ph} = 0)\), each measured value of \(\sigma_x \otimes \sigma_z\) in the Bell measurement on \(K_A \otimes K_C\) would have exactly told us the corresponding bit value in the sequence \(X\), namely, \(\sigma_z \otimes \sigma_z = 1\) and \(-1\) implies the bit values 0 and 1, respectively. But when we do have phase errors initially, for such \(Nr_{ph}\) pairs the correspondence is reversed, namely, \(\sigma_z \otimes \sigma_z = 1\) and \(-1\) implies the bit values 1 and 0, respectively. Since we do not exactly know which of the \(N\) pairs have phase errors initially, we have the candidates \(T_{ph}\) for the sequence \(X\) as many as the number of the phase-error patterns. Here, the measured value of \(\sigma_z \otimes \sigma_z\) in the Bell measurement on \(K_A \otimes K_C\) helps us to narrow down the possible phase-error patterns, combined with the values of \(r_{01}\) and \(r_{11}\) that are estimated through the \(y\)-basis measurements in the six-state protocol. There must be \(Nr_{11}\) pairs with phase errors among the \(Nr_{bit}\) pairs that have resulted in \(\sigma_z \otimes \sigma_z = -1\), and the rest of the \(N(1 - r_{bit})\) pairs should include \(Nr_{01}\) phase-error pairs. Hence, the number of the phase-error patterns is approximately given by \(2^{N\xi}\) with
\[
\xi = (1 - r_{bit})h \left( \frac{r_{01}}{1 - r_{bit}} \right) + r_{bit}h \left( \frac{r_{11}}{r_{bit}} \right),
\]
which reproduces the key rate of equation (30).

5. Conclusion

We have described a method of proving unconditional security, which unifies two major previous approaches and retains the advantages in both of them. We have also shown that the new method can solve a problem which eluded the previous approaches. 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 an 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 \(\Lambda\) 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 \(\rho_{AB} \otimes \rho_{AB}'\), where \(\rho_{AB}\) is an MES. Their twisting operations do not change the outcome of \(z\)-basis measurement on \(H_B\), which can be regarded as \(\kappa_{rec}\). Hence, we can define \(\Lambda\) to be the reverse of the twisting followed by \(\Lambda_0\), which satisfies assumption 1. This shows that the present method potentially gives a key rate exceeding the amount of distillable entanglement. The exact relation of the present method to the distillable entanglement and the distillable secret key is discussed elsewhere [23]. The relation of our approach to other security approaches [24]–[26] is also an interesting issue.

Acknowledgments

I thank N Imoto, J Preskill, H-K Lo, K Azuma and V Scarani for helpful discussions. This work was supported by the JSPS Grant-in-aid for Scientific Research (C) 20540389.

New Journal of Physics 11 (2009) 045018 (http://www.njp.org/)
References

[1] Shor P W and Preskill J 2000 Simple proof of security of the BB84 quantum key distribution protocol Phys. Rev. Lett. 85 441
[2] Calderbank A R and Shor P W 1996 Good quantum error-correcting codes exist Phys. Rev. A 54 1098
[3] Steane A M 1996 Multiple-particle interference and quantum error correction Proc. R. Soc. Lond. A 452 2551
[4] Bennett C H and Brassard G 1984 Quantum cryptography: public key distribution and coin tossing Proc. IEEE Int. Conf. on Computers, Systems, and Signal Processing (Bangalore, India) (New York: IEEE) pp 175–9
[5] Tamaki K, Koashi M and Imoto N 2003 Unconditionally secure key distribution based on two nonorthogonal states Phys. Rev. Lett. 90 167904
[6] Koashi M 2004 Unconditional security of coherent-state quantum key distribution with a strong phase-reference pulse Phys. Rev. Lett. 93 120501
[7] Bennett C H 1992 Quantum cryptography using any two nonorthogonal states Phys. Rev. Lett. 68 3121
[8] Hamada M 2003 Reliability of Calderbank–Shor–Steane codes and security of quantum key distribution arXiv:quant-ph/0308039
[9] Lo H K 2003 Method for decoupling error correction from privacy amplification New J. Phys. 5 36
[10] Mayers D 1996 Quantum key distribution and string oblivious transfer in noisy channels Lecture Notes Comput. Sci. 1109 343
[11] Koashi M and Preskill J 2003 Secure quantum key distribution with an uncharacterized source Phys. Rev. Lett. 90 057902
[12] Lo H K and Chau H F 1999 Unconditional security of quantum key distribution over arbitrarily long distances Science 283 2050
[13] Horodecki K, Horodecki M, Horodecki P and Oppenheim J 2005 Secure key from bound entanglement Phys. Rev. Lett. 94 160502
[14] Koashi M 2005 Unconditional security of quantum key distribution and the uncertainty principle J. Phys.: Conf. Ser. 36 98
[15] Maassen H and Uffink J B M 1988 Generalized entropic uncertainty relations Phys. Rev. Lett. 60 1103
[16] Gottesman D, Lo H K, Lütkenhaus N and Preskill J 2004 Security of quantum key distribution with imperfect devices Quantum Inf. Comput. 5 325
[17] Uhlmann A 1976 The ‘transition probability’ in the state space of a *-algebra Rep. Math. Phys. 9 273
[18] Jozsa R 1994 Fidelity for mixed quantum states J. Mod. Opt. 41 2315
[19] Bennett C H, DiVincenzo D P, Smolin J A and Wootters W K 1996 Mixed-state entanglement and quantum error correction Phys. Rev. A 54 3824
[20] Koashi M 2006 Efficient quantum key distribution with practical sources and detectors arXiv:quant-ph/0609180
[21] Bruß D 1998 Optimal eavesdropping in quantum cryptography with six states Phys. Rev. Lett. 81 3018
[22] Lo H K 2001 Proof of unconditional security of six-state quantum key distribution scheme Quantum Inf. Comput. 1 81
[23] Koashi M 2007 Complementarity, distillable secret key, and distillable entanglement arXiv:0704.3661
[24] Christandl M, Ekert A and Renner R 2004 A generic security proof for quantum key distribution arXiv:quant-ph/0402131
[25] Renner R, Gisin N and Kraus B 2005 Information-theoretic security proof for quantum-key-distribution protocols Phys. Rev. A 72 012332
[26] Hayashi M 2006 Practical evaluation of security for quantum key distribution Phys. Rev. A 74 022307

New Journal of Physics 11 (2009) 045018 (http://www.njp.org/)