Finite-key security against coherent attacks in quantum key distribution

Lana Sheridan\(^1\), Thinh Phuc Le\(^1\) and Valerio Scarani\(^2\)

\(^1\) Centre for Quantum Technologies, National University of Singapore, Singapore, Singapore
\(^2\) Department of Physics, National University of Singapore, Singapore, Singapore
E-mail: cqtlss@nus.edu.sg

*New Journal of Physics* **12** (2010) 123019 (12pp)
Received 25 August 2010
Published 9 December 2010
Online at [http://www.njp.org/](http://www.njp.org/)
doi:10.1088/1367-2630/12/12/123019

**Abstract.** Christandl *et al* (2009 *Phys. Rev. Lett.* **102** 020504) provide, in particular, the possibility of studying unconditional security in the finite-key regime for all discrete-variable protocols. We spell out this bound from their general formalism. Then, we apply it in the analysis of a recently proposed protocol (Laing *et al* 2010 *Phys. Rev. A* **82** 012304). This protocol is meaningful when the alignment of Alice’s and Bob’s reference frames is not monitored and may vary with time. In this scenario, the notion of asymptotic key rate has hardly any operational meaning, because if one waits too long a time, the average correlations are smeared out and no security can be inferred. Therefore, finite-key analysis is necessary for finding the maximal achievable secret key rate and the corresponding optimal number of signals.
Quantum key distribution (QKD) provides a way of distributing secret keys for use in secure communication [1, 2]. Started by Bennett and Brassard in 1984 (BB84; [3]) and by Ekert in 1991 [4], QKD has posed several challenges both theoretical and experimental, which have been met to a large extent. One of those challenges has been the derivation of security bounds that take into account the finite number $N$ of exchanged quantum signals, i.e. the finite size of the keys one has to work with. The tools for such a study were remarkably anticipated by Mayers in his very first unconditional security proof [5], but for several reasons the full solution was delayed by more than 10 years. Hayashi’s formalism [6] was tailored for the BB84 protocol. The approach by Renner and one of the authors [7]–[9] is in principle more flexible but is limited to collective attacks in general: unconditional security could be claimed only for BB84 and the other few protocols in which the bound for collective attacks is known to coincide with the one for the most general attacks [10]. Recently, Christandl et al [11] developed some very general mathematical tools, whose applications include the derivation of finite-key bounds for any discrete-variable protocol (for the status of the question in continuous-variable protocols, see [12]).

In this paper, we spell out explicitly the method for computing the finite-key QKD bound described in [11]. This new tool can be used to compute unconditional security bounds in the finite-key regime for protocols such as Bennett 1992 (B92 [13]), Scarani–Acín–Ribordy–Gisin 2004 (SARG04 [14, 15]) or protocols based on the violation of Bell’s inequalities [16, 17]. As an application, we have rather chosen the reference frame-independent protocol proposed by Laing et al [18]. This protocol is useful in situations in which the alignment of reference frames between Alice and Bob is not monitored and may vary in time. In this study, we consider the finite-key analysis of this protocol in light of the fact that the reference frame relations in these scenarios will not only be unknown, but may also be fluctuating over the course of the protocol. Under these assumptions, one finds that optimal secret key rates are reached for a finite number of signals: if Alice and Bob wait too long a time, their correlations will be smeared due to misalignment of the frames.
This paper is organized as follows. In section 2, we present a new method for finite-key analysis against coherent attacks. In section 3, we use this method to analyze the reference frame-independent protocol for two cases of drifting phase references: firstly, one frame rotating at constant speed relative to the other; secondly, the angle between the frames fluctuating according to a random walk. Lastly, in section 4, the implications of the results are considered.

2. The finite-key analysis method

We start by summarizing the notation and the bound for collective attacks, as discussed in detail in previous works [7]–[9], [17]. Then we present the new bound extracted from [11].

2.1. The notation and bound for collective attacks

Let $N$ be the number of signals sent by Alice that are received by Bob. In addition to the error rate in the raw key, denoted by $Q$, the protocol uses $n_{PE}$ parameters $V = \{v_1, \ldots, v_{n_{PE}}\}$ to bound Eve’s information. For simplicity, we consider asymmetric protocols [19], in which $n$ signals are used to create the raw key, while the other signals are used to estimate the other parameters (the secret key rate for the symmetric protocol is larger by $n_{PE} + 1$ at most and becomes the same in the asymptotic limit). The number of signals devoted to estimating $v_j$ is written as $m_j$.

Let now $\epsilon_{PA}$ be the probability that privacy amplification fails and $\epsilon_{PE}$ the probability that the real value of a parameter lies outside of the chosen fluctuation range. There is a third error probability, denoted by $\tilde{\epsilon}$, which measures the accuracy of estimating the smooth min-entropy. Finally, there is a probability $\epsilon_{EC}$ that error correction fails, which is determined by the choice of the error correction code. Because of the composability of the bound, in the worst case, the probability $\epsilon_{col}$ that the quantum key distribution protocol fails does not exceed the sum of the probabilities of failure in different phases of the protocol:

$$\epsilon_{col} = \epsilon_{PA} + \tilde{\epsilon} + n_{PE} \epsilon_{PE} + \epsilon_{EC}. \quad (1)$$

The user can choose $\epsilon_{col}$ and $\epsilon_{EC}$; the other parameters can be optimized under the constraint (1).

If the key alphabet is made by $d$-valued symbols, the secret key fraction against collective attacks is given by

$$r_{N,\text{col}} = \frac{n}{N} \left[ \min_{E \in V \pm \Delta V(\text{typ})} H(A|E) - H(A|B) - \frac{1}{n} \log \frac{2}{\epsilon_{EC}} - \frac{2}{n} \log \frac{1}{\epsilon_{PA}} - \frac{2d + 3}{n} \sqrt{\frac{\log(2/\tilde{\epsilon})}{n}} \right], \quad (2)$$

where we are assuming that the yield of the error correction protocol is perfect, to reach the Shannon limit, $H(A|B)$.

2.2. Beyond collective attacks

Previous works [7]–[9] used the bound above to claim unconditional security for the BB84 and the six-state protocols, as well as for their natural high-dimensional generalizations, because for those protocols the bound for collective attacks coincides with the one for coherent attacks [10]. But for protocols using a less symmetric encoding, there is no guarantee that this is the case. The most general attacks are impossible to parameterize. Therefore, the generic recipe for
unconditional security consists, in a nutshell, of bounding the possible advantage of coherent attacks over the collective ones and then computing the bound for collective attacks with the suitable overhead terms.

The first such approach used the exponential de Finetti theorem [20, 21]. This theorem bounds the distance between any state $\rho_{AB}^{(n)}$ that leads to permutationally invariant statistics for Alice and Bob, and $n$-fold product states $\sigma_{AB}^{\otimes n}$ (or mixtures thereof), i.e. exactly the states that a collective attack would produce. The overhead obtained by this theorem turns out to be very heavy, so much so that it would make finite-key bounds unrealistically pessimistic (figure 2). This fact has been stressed already in [7], but the explicit expressions and results were not given, so we present them in appendix A.

The de Finetti theorem is tight if one wants to compare the attacks at the level of the states. Christandl et al [11] noted that, for the sake of QKD and other quantum information processing tasks, a much less refined comparison is actually sufficient.

They found that it suffices to consider the distance between two permutation invariant maps and how this distance changes when acting on states that result from a general attack rather than on states resulting from a collective attack. The maps are the one describing the QKD protocol being implemented and an idealized scheme that takes any quantum state as an input and distributes two classical perfectly correlated random strings to Alice and Bob. See figure 1.

**Figure 1.** Consider the distance, $\Delta$, between the permutation invariant maps $\mathcal{E}$, implementing the QKD protocol, and $\mathcal{F} = \mathcal{S} \circ \mathcal{E}$, where the map $\mathcal{S}$ is a hypothetical process that takes an imperfect key to a perfect one. This distance can be found when the maps act on the de Finetti–Hilbert–Schmidt state, which describes the case for collective attacks, and the increase in $\Delta$ can be bounded when the same two maps act on an arbitrary state, the case for coherent attacks. This model is from [11].
Figure 2. Secret key fraction for BB84 versus the number of signals $N$ for three different finite analysis bounds: (a) collective attacks, (b) the post-selection technique and (c) the exponential de Finetti theorem.

In summary, let us fix $\epsilon_{\text{coh}}$ as the tolerable failure probability of the secret key against coherent attacks. Then, the resulting expression for the secret key rate is

$$r_N = r_{N,\text{col}} - \frac{2(d^4 - 1) \log(N + 1)}{N},$$

where the bound for collective attacks (2) is computed under the constraint (1) for the security parameter

$$\epsilon_{\text{col}} = \epsilon_{\text{coh}} (N + 1)^{-1}.$$

The improvement that this technique gives over the use of the exponential de Finetti theorem is illustrated in figure 2. For the BB84 protocol the optimal coherent attack is a collective attack and therefore the line (a) is the best bound for security. However, if that were not known to be the case, the post-selection technique gives a bound close to the optimal one, whereas the bound obtained using the de Finetti is substantially worse and would imply the practical impossibility of obtaining a key in QKD.

3. Case study: reference frame-independent protocol

3.1. Review of the protocol

We briefly describe the reference frame-independent protocol [18]. In the prepare and measure scenario, Alice sends to Bob a qubit prepared in an eigenstate of three mutually unbiased bases $\{X_A, Y_A, Z_A\}$ chosen at random but not necessarily with the same probability. Bob then receives a qubit that may be tampered by Eve and measures in his own basis chosen among a possibly different set of mutually unbiased bases $\{X_B, Y_B, Z_B\}$. The equivalent entanglement-based version is that Alice and Bob receive a pair of entangled qubits in a state $\rho_{AB}$, which is $|\Phi^+\rangle$ in the ideal case, and perform the local measurements defined by the above-mentioned bases on them. The measurements can be described by a vector in the Bloch sphere, which we...
will refer to by direction. Unlike usual protocols, where the reference frames orientations are actively monitored using the classical channel, this protocol requires one well-defined direction $Z_A = Z_B$, while the other two directions are related by an unknown transformation

$$X_B = \cos \beta X_A + \sin \beta Y_A, \quad Y_B = \cos \beta Y_A - \sin \beta X_A.$$  \hfill (5)

At the end of the signal exchange phase, they reveal their bases. This protocol is intrinsically asymmetric, in that the different bases play different roles. The raw key consists of the cases where both have measured in the $Z$-basis, and is characterized by the quantum bit error rate

$$Q = \frac{1 - \langle Z_A Z_B \rangle}{2}. \hfill (6)$$

Eve’s information is quantified by the parameter

$$C = \langle X_A X_B \rangle^2 + \langle X_A Y_B \rangle^2 + \langle Y_A X_B \rangle^2 + \langle Y_A Y_B \rangle^2 \leq 2,$$ \hfill (7)

where $C = 2$ guarantees maximal entanglement. Note that four measurements are needed to estimate $C$, so the actual parameters that are measured are

$$v_1 = \langle X_A X_B \rangle, \quad v_2 = \langle X_A Y_B \rangle, \quad v_3 = \langle Y_A X_B \rangle, \quad v_4 = \langle Y_A Y_B \rangle.$$ \hfill (8)

Expression (7) has been chosen because it is independent of $\beta$: it retains its value even if Alice’s and Bob’s frames are misaligned. In the asymptotic limit, the information that Eve can gain from coherent attacks is upper bounded by

$$I_E(Q, C) = (1 - Q) h \left( \frac{1 + u_{\text{max}}}{2} \right) + Q h \left( \frac{1 + v(u_{\text{max}})}{2} \right), \hfill (9)$$

where

$$u_{\text{max}} = \min \left[ \sqrt{\frac{C}{2}} - \frac{1}{1 - Q}, 1 \right], \quad v(u_{\text{max}}) = \frac{1}{Q} \sqrt{C/2 - (1 - Q)^2 u_{\text{max}}^2}$$ \hfill (10)

and $h(x)$ is the binary entropy. This result holds in the range $0 \leq Q \lesssim 15.9\%$, which is perfectly reasonable for the quality of optical lines.

Obviously, this protocol becomes of interest if $\beta$ varies in time: if the frames are possibly misaligned but are guaranteed to be fixed in time, one would just align them once and for all. However, it takes time to collect enough data to estimate the four average values that enter the expression of $C$: the misalignment of the frames during this time leads to a smearing of the correlations and the consequent decrease of $C$. In particular, if one waits to accumulate a very large number of signals, $C$ will ultimately drop so much that no security can be inferred: in other words, the asymptotic rate (9) somehow assumes not only that infinitely many signals can be collected, but also that $\beta$ is fixed. In all meaningful situations, not only the realistic secret key rate, but also the optimal one must be determined by finite-key analysis. This is the aim of what follows.

3.2. Computing the finite-key bound

Let us particularize the parameters that enter the finite-key bound (3) to the protocol under study. We denote by $p_Z$ the probability that Alice and Bob choose the key basis $Z$; we assume that the other two bases are chosen with equal probability $p_X = p_Y = 1 - 2p_Z \equiv p$. Hence, the raw key consists of $n = Np_Z^2$ signals, while each of the correlators $v_j$ is estimated using $m = Np^2$ signals.
The frames drift apart at a constant angular velocity \( \dot{\beta}(t) = \omega t \). Then

\[
\bar{c}_N + i\bar{s}_N = \frac{1}{N} \frac{1 - e^{i\theta N}}{1 - e^{i\theta}} \quad \text{with} \quad \theta = \omega \tau .
\]
Figure 3. Secret key fraction for (a) the frames drifting apart at constant angular velocity with $\theta = \frac{\pi}{180} \times 10^{-10}$ and (b) fixed frames, (c) one frame drifting relative to the other according to a random walk with the different rate of $\theta = \frac{\pi}{180} \times 10^{-5}$ per step. Then for both plots the security parameter is $\epsilon = 10^{-5}$, $C(0) = 1.72$ and $Q = 5\%$.

This leads in particular to

$$C(T_N) = C(0) \frac{1 - \cos(\theta N)}{N^2(1 - \cos \theta)}. \tag{17}$$

As $\theta \to 0$, the continuous sampling limit is recovered from $C(T_N) = C(0) \frac{2(1 - \cos(\theta N))}{(N\theta)^2}$.

• The relative angle is following a random walk behavior: $\beta$ changes by $\pm \theta$ randomly in the time $\tau$. One is led to compute the average value of the sine and cosine of a random walk, i.e.

$$\bar{c}_N + i\bar{s}_N = \sum_{k=-N/2}^{N/2} e^{i(2k)} P_N(2k) = \cos(\theta)^N, \tag{18}$$

where $P_N(d) = \frac{1}{2N} \binom{N}{(N+d)/2}$ is the probability of traveling a distance $d \in \{-N, \ldots, N\}$ in $N$ steps. This leads to

$$C(T_N) = C(0) (\cos \theta)^{2N}. \tag{19}$$

In both cases, of course, $C(T_N)$ goes to zero for large $N$. The effect of this smearing on the finite-key secret key rate is shown in figure 3.

4. Conclusion

We have studied the application of the post-selection technique of [11] to QKD protocols in finite-key scenarios to extend the security bounds for collective attacks to bounds for coherent attacks. We have compared it explicitly to the bounds recovered for finite keys using the de Finetti theorem. We demonstrate how to compute this new bound by applying it to the
reference frame-independent protocol of [18]. In addition, we have considered two physically plausible scenarios for the case of unaligned reference frames: that one frame may be rotating relative to the other or that one frame may be executing a random-walk-type drift relative to the other.

The most prominent feature of these two cases is that the asymptotic limit does not give the best key fraction. This can be seen in figure 3. The reason is that the longer we collect the signals, the lower the value of the security parameter $C$ becomes. For a fixed $\omega$ or $\theta$, there exists an optimal block of size $N$ to obtain the best secret key fraction. If more key is required, the protocol should be terminated and restarted after each block. Hence, any practical application of the reference frame-independent protocol should aim for this optimal number of signals to be exchanged in a run of key distribution.

Acknowledgments

We thank Matthias Christandl and Renato Renner for helpful discussions. This work was supported by the National Research Foundation and the Ministry of Education, Singapore.

Appendix A. de Finetti

Here we consider the bound which can be derived from using the de Finetti bound when using $d$-dimensional systems following the results of [20].

Now, of the sifted signals $N_s$, $m$ will be used for parameter estimation and $k$ systems are traced over to make use of the de Finetti theorem by bounding the remaining systems to have been very close to a mixture of product states $\sigma \otimes \cdots \otimes \sigma$. Thus, $n = N_s - m - k$ is the number of remaining systems that can be put towards the key, but since it is not yet secure, this is the raw key.

Let the state $\tilde{\rho}^{(\theta)}_n$ be the permutationally invariant output of a quantum key distribution protocol. Because the state $\tilde{\rho}^{(\theta)}_n$ is, in general, not exactly of product form, for any $|\theta\rangle$, it is a pure state of the symmetric subspace of $H^\otimes n$ such that $\tilde{\rho}^{(\theta)}_n = \sum_\pi |\theta\rangle^\otimes n-\pi \otimes |\phi\rangle_t$, where the sum is over all permutations, $\pi$, for some $t$ such that $0 \leq t \leq m/2$. In some sense, $t$ can be thought of as quantifying the distance that the state $\tilde{\rho}^{(\theta)}_n$ is from the perfect pure $n$-fold product state.

Hence, we can now introduce an error, $\varepsilon_{\text{deF}}$, that parameterizes $t$,

$$\varepsilon_{\text{coh}} = \varepsilon_{\text{PA}} + \tilde{\varepsilon} + n_{\text{PE}}\varepsilon_{\text{PE}} + \varepsilon_{\text{EC}} + \varepsilon_{\text{deF}}, \quad (A.1)$$

where $t = \frac{N_s}{k} (2 \ln(2/\varepsilon_{\text{deF}}) + d^4 \ln(k))$ [20].

The maximum error in the parameter estimation, assuming $m$ samples, is now

$$\delta(m) = \frac{1}{d-1} \sqrt{(1 + \ln 2) \frac{t}{m} + \frac{\ln(1/\varepsilon_{\text{PE}}) + d \ln(m/2+1)}{m}}, \quad (A.2)$$

where $k$ is optimized over. We see then that if $k$ is larger, $t$ can be smaller (the form of the raw key state can constrain Eve to collective attacks more closely); however, this reduces the size or the raw key, so there is a trade-off.
The term giving the privacy amplification correction is also modified [20], so that the final rate is given by

\[
\frac{r_{N,\text{coh}}}{N} = \frac{n}{N} \left[ \frac{\min_{E_{V_{min}}(\epsilon_p)}}{E_{V_{max}}(\epsilon_p)} H(A|E) - H(A|B) - \frac{1}{n} \log \frac{2}{\epsilon_{EC}} - \frac{2}{n} \log(1/\epsilon_{PA}) - \frac{2}{n} d + \frac{5}{2} d + 4 \sqrt{\frac{\log(2/\epsilon)}{n}} + h(t/n) \right].
\] (A.3)

These expressions can be used in equation (2) to obtain a bound for coherent attacks.

Appendix B. Derivation of our equations (3) and (4) from [11]

General coherent attacks can be bounded in terms of collective attacks for general permutation invariant protocols by using the method introduced in [11].

First, it is usually more easy to prove that a protocol is secure against collective attacks than coherent attacks, so the problem is approached for a particular state, the de Finetti–Hilbert–Schmidt state \( \tau_{A^N B^N} \), which represents the mixture of states that could be held by Alice and Bob after Eve makes a collective attack. This state is defined as

\[
\tau_{A^N B^N} = \int \sigma_{AB}^N d_{HS} \sigma_{AB},
\] (B.1)

where \( d_{HS} \) is the measure induced by the Hilbert–Schmidt metric, \( \Delta_{HS}(X - Y) = \| X - Y \|_{HS} \) and \( \| X \|_{HS}^2 = \text{Tr}(X^\dagger X) \).

Let \( \mathcal{E} \) be the actual protocol for which security is to be proven and \( \mathcal{F} \) be an ideal key-generation protocol composed of the actual protocol \( \mathcal{E} \) and a map \( \mathcal{S} \) that takes classical inputs, and outputs a perfectly random perfectly correlated key string, i.e. \( \mathcal{F} = \mathcal{S} \circ \mathcal{E} \) that for any inputs gives Alice and Bob the output of an ideal key (see figure 1). The main theorem of [11] guarantees the security of this protocol against any coherent attack

\[
\Delta(\mathcal{E}, \mathcal{F})_\rho \leq (N + 1)^{d - 1} \Delta(\mathcal{E}, \mathcal{F})_\tau,
\] (B.2)

where \( \Delta(\mathcal{E}, \mathcal{F})_\rho \) and \( \Delta(\mathcal{E}, \mathcal{F})_\tau \) are the diamond-norm distances between the protocols for arbitrary states \( \rho \) and the de Finetti–Hilbert–Schmidt state \( \tau \), respectively, and \( N \) is the number of signals or subsystems each with dimension \( d^2 \) (bipartite qudits shared by Alice and Bob). Since \( \rho \) is an arbitrary state it can correspond to an arbitrary quantum-mechanically allowed attack by Eve.

In order to find the secret key fraction for finite length keys, it is also necessary to consider the effect of Eve’s possession of the purification of \( \rho_{A^N B^N} \). This is already considered for collective attacks when the min-entropy of Alice’s information given Eve’s, \( H_{\text{min}}(A|E) \), is used to bound the secret key fraction. Let \( \mathcal{H}_E \) be the system Eve holds that purifies \( \sigma_{AB} \) (see figure B.1). Now it is necessary to include the extra information she may have as a result of holding the purification of the mixture of the state on \( N \) systems \( \tau_{A^N B^N E^N} \). Let the purification of this \( N \)-system state be on the Hilbert space \( \mathcal{H}_E \). Hence, now we must consider \( H_{\text{min}}(A^N|E^N E') \) in the equation for the secret key fraction. We use the entropy bound

\[
H_{\text{min}}^N(A^N|E^N E') \geq H_{\text{min}}^N(A^N|E^N) - 2H_0(E').
\] (B.3)
Figure B.1. Eve’s Hilbert space $E$ purifies each entangled system space held by Alice and Bob. The remainder of Eve’s space $E'$ purifies the state $\tau'$ on $N$ systems which is a mixture over the possible pure product states $\sigma_{ABE}$.

A space of dimension not more than $(N + 1)^{d - 1}$ is needed for constructing such a purification and so $\mathcal{H}_{E'}$ cannot contain more than $\log((N + 1)^{d - 1})$ bits of information. We therefore subtract twice this from the available entropy and divide by the number of signals $N$ to obtain equation (3).

Hence, the post-selection technique gives another way of relating a bound that can be shown for collective attacks to a bound for an unknown optimal coherent attack, provided that there is a bound on the dimension of the systems being exchanged $d$. In other words, this result, just like the de Finetti theorem, cannot be used as such for continuous variables.

References

[1] Gisin N, Ribordy G, Tittel W and Zbinden H 2002 Rev. Mod. Phys. 74 145
[2] Scarani V, Bechmann-Pasquinucci H, Cerf N J, Dusek M, Lutkenhaus N and Peev M 2009 Rev. Mod. Phys. 81 1301
[3] Bennett C H and Brassard G 1984 Proc. IEEE Int. Conf. on Computers, Systems and Signal Processing (Bangalore, India) (New York: IEEE) pp 175–9
[4] Ekert A K 1991 Phys. Rev. Lett. 67 661
[5] Mayers D 1996 Advances in Cryptology—Proc. Crypto ’96 (Berlin: Springer) p 343
[6] Hayashi M 2007 Phys. Rev. A 76 012329
[7] Scarani V and Renner R 2008 Phys. Rev. Lett. 100 200501
[8] Cai R Y and Scarani V 2009 New J. Phys. 11 045024
[9] Sheridan L and Scarani V 2010 Phys. Rev. A 82 030301
[10] Kraus B, Gisin N and Renner R 2005 Phys. Rev. Lett. 95 080501
[11] Christandl M, König R and Renner R 2009 Phys. Rev. Lett. 102 020504
[12] Leverrier A, Grosshans F and Grangier P 2010 Phys. Rev. A 81 062343
[13] Bennett C H 1992 Phys. Rev. Lett. 68 3121
[14] Scarani V, Acín A, Ribordy G and Gisin N 2004 Phys. Rev. Lett. 92 057901
[15] Branciard C, Gisin N, Kraus B and Scarani V 2005 Phys. Rev. A 72 032301
[16] Acín A, Massar S and Pironio S 2006 New J. Phys. 8 126

New Journal of Physics 12 (2010) 123019 (http://www.njp.org/)
[17] Scarani V and Renner R 2008 Proc. TQC2008 (Lecture Notes in Computer Science vol 5106) (Berlin: Springer) pp 83–95
[18] Laing A, Scarani V, Rarity J G and O’Brien J L 2010 Phys. Rev. A 82 012304
[19] Lo H-K, Chau H and Ardehali M 2005 J. Cryptol. 18 133
[20] Renner R 2008 Int. J. Quantum. Inf. 6 1
[21] Renner R 2007 Nat. Phys. 3 645
[22] Cover T M and Thomas J A 2006 Elements of Information Theory 2nd edn (New York: Wiley Interscience) ISBN 9780471241959
[23] Sano Y, Matsumoto R and Uyematsu T 2010 J. Phys. A: Math. Theor. 43 495302