PHYSICAL REVIEW A **79**, 020303(R) (2009)

Optimal ratio between phase basis and bit basis in quantum key distributions

Masahito Hayashi[*]
Graduate School of Information Sciences, Tohoku University, Aoba-ku, Sendai, 980-8579, Japan

(Received 4 June 2008; published 5 February 2009)

In the original Bennett-Brassard 1984 protocol, the bit basis and the phase basis are used with equal probability. Lo *et al.* [J. Cryptology **18**, 133 (2005)] proposed modifying the ratio between the two bases by increasing the final key generation rate. However, the optimum ratio has not yet been derived. In this Rapid Communication, in order to examine this problem, the ratio between the two bases is optimized for exponential constraints, given Eve's information distinguishability and the final error probability.

DOI: 10.1103/PhysRevA.79.020303 PACS number(s): 03.67.Dd, 03.67.Hk

Bennett and Brassard in 1984 (BB84) [1] proposed a protocol for quantum key distribution (QKD). Recently, several researchers have reported the generation of a single-photon source with telecommunication wavelength 1.3 μm [2] (with economical instruments) and 1.5 μm [3], which has the lowest transmission loss. Also, as a single-photon source for free space communication, single nitrogen-vacancy centers in diamond have been developed [4]. Therefore, a quantum key distribution system with a single-photon source is close to becoming realistic. Indeed, it has been shown that this protocol generates secret random bits between two distinct parties, even if the quantum channel is noisy [5,6]. Since a proof of security was established for this protocol, many researchers [7] have improved the key generation rate. Lo *et al.* [8] proposed to improve the key generation rate by modifying the ratio between the bit $(+)$ basis and the phase $(\times)$ basis. In the original BB84 protocol, the sender Alice and the receiver Bob choose the $+$ basis and the $\times$ basis with equal probabilities. However, this one-to-one ratio is not essential, because the purpose of a random basis choice is to estimate the phase error rate in the channel of qubits on a coincidence basis. That is, in order to generate secure keys from raw keys in the $+$ basis, it is sufficient to estimate the error rates in both bases precisely. The aim of the present Rapid Communication is to improve the key generation rate by modifying the ratio between the two bases.

For example, the following protocol improves the key generation rate. When Alice and Bob communicate N qubits, Alice and Bob use the $\times$ basis only for the randomly chosen $\sqrt{N}$ qubits and use the $+$ basis for the remaining $N-\sqrt{N}$ qubits. For this protocol, when the length of the code N is sufficiently large, Alice and Bob can estimate the phase error rate precisely. Since $\sqrt{N}/N$ approaches zero, the rate of discarded qubits approaches zero. That is, it is possible that the generation rate of the raw keys with transmitted qubits is almost 100%. Hence, in order to optimize this ratio, we have to choose a suitable formulation. Due to the difficulty of such a formulation, this optimization has not been dealt with in existing research. As a possible formulation, one may consider optimization of the final key generation rate with a constant constraint on Eve's information in the finite length code. However, as has been discussed by Lo *et al.* [8], Hayashi [9], and Scarani and Renner [10], the formula for a finite-length code is not simple. Furthermore, its analysis depends on the length of the code. Hayashi [11] treats security of an imperfect source and channel. Indeed, while [11] treats the case of an imperfect source, it contains the case of a single photon with a lossy channel as a special case.

This Rapid Communication focuses on exponential constraint as an intermediate criterion between the finite- and the infinite-length cases. The exponential rate is a common measure in information theory [12], and it has been discussed in the QKD context in several papers [9,13,14]. Here, we treat exponential constraints on the block error probability for final keys and for Eve's information distinguishability for final keys [15]. This Rapid Communication optimizes the final key generation rate based on the key distillation protocol given by Hayashi [9,11]. In this key distillation protocol, first, a classical error correction is made. Next, privacy amplification using a Toeplitz matrix, which is an economical random matrix [16,17], is carried out. Hence, Eve's information distinguishability can be characterized by the phase error probability of the corresponding Calderbank-Shor-Steane (CSS) code.

One may think that, since Alice and Bob use an asymmetric ratio, Eve can improve her strategy by using the asymmetric property of the protocol. However, since the role of the $\times$ basis is only to estimate the error rate of the $\times$ basis in QKD, the disadvantage of the asymmetric protocol is that it decreases the precision of estimation of the error rate of the $\times$ basis. If estimation of the error rate of the $\times$ basis is not sufficiently precise, Eve can eavesdrop on Alice's information. Thus, the exponential constraint for Eve's information distinguishability for final keys reflects this disadvantage of the asymmetric protocol.

Thanks to recent advances in technology [2–4], it is natural to assume that a single-photon source with a lossy quantum channel is available. This Rapid Communication analyzes optimization under this assumption. Furthermore, for a simpler analysis, the random coding and the maximum likelihood decoding are assumed to be performed in the classical error correction procedure.

This paper focuses on the asymmetric protocol in which Alice and Bob use the $\times$ basis with ratio p_2, and they announce the check bits, which are randomly chosen with ratio p_1 among the bits for which Alice's and Bob's bases are the $+$ basis. (As will be shown later, the optimal case arises when the ratio of the $\times$ basis used by Alice is equal to that used by Bob.) The performance of the protocol is characterized by two quantities, i.e., the final error probability of the

[*] hayashi@math.is.tohoku.ac.jp

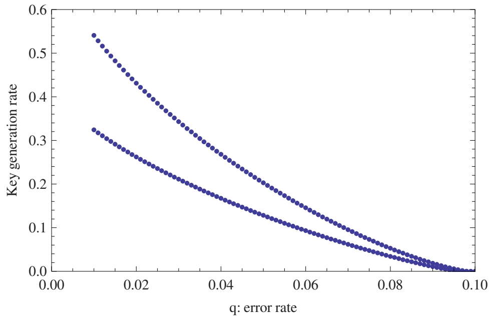

FIG. 1. (Color online) Asymptotic key generation rate: The upper line shows max R_A, while the lower line shows max R_S.

classical error correction and Eve's information distinguishability. The latter is equal to $\|\rho_{AE}-\rho_A\otimes\rho_E\|_1$ for Eve's final state ρ_E, Alice's final state ρ_A, and the final state ρ_{AE} of the joint system of the final keys.

The final error probability of the classical error correction depends on the number N of transmitted qubits, the observed error rates q_+ of the + basis. However, Eve's information distinguishability cannot be determined from the observed values because it depends on Eve's attack. Hence, we compute only the upper bounds, i.e., the upper bound $B_b(N,p_1,p_2,q_+)$ of the final error probability and the upper bound $B_p(N,p_1,p_2,q_\times)$ of Eve's information distinguishability [9,11], which depends on the observed error rates $q_\times$ of the × basis and does not depend on Eve's attack. For a given constant C, the following exponential constraint is considered:

$$\lim_{N\to\infty}\frac{-1}{N}\log B_b(N,p_1,p_2,q_+)\geq C, \qquad (1)$$

$$\lim_{N\to\infty}\frac{-1}{N}\log B_p(N,p_1,p_2,q_\times)\geq \frac{C}{2}. \qquad (2)$$

The reason for such an asymmetric constraint is that correctness for the final keys requires higher precision than secrecy.

Thus, our main target is the calculation of the rates p_1 and p_2 which optimize the final key generation rate $R_A(p_1,p_2,q_+,q_\times,C)$ under conditions (1) and (2), when $q := q_+ = q_\times$. These values are numerically calculated using logarithms to base 2 with $C=0.0001$. For example, when $N=100\,000$, $2^{-CN/2}=2^{-5}$. However, since the quantity $B_p(N,p_1,p_2,q_\times)$ has a polynomial factor, it is greater than 2^{-5}.

Next, we consider the symmetric protocol, in which the ratio of the × basis to the + basis is chosen to be the one-to-one ratio for both parties. In this case, it is possible to control only the ratio p_1 of the check bits. The original BB84 protocol is an example of this case where $p_1=1/2$. Then, we can numerically calculate the rate p_1 optimizing the final key generation rate $R_S(p_1,q_+,q_\times,C)$ under conditions (1) and (2), when $q := q_+ = q_\times$. The numerical results for $\max_{0\leq p_1,p_2\leq 1/2}R_A(p_1,p_2,q,q,0.0001)$ and $\max_{0\leq p_1\leq 1/2}R_S(p_1,q,q,0.0001)$ are shown in Fig. 1.

Using the above results, we obtain Fig. 2, which shows $\operatorname{argmax}_{0\leq p_1\leq 1/2}\max_{0\leq p_2\leq 1/2}R_A(p_1,p_2,q,q,0.0001)$ and $\operatorname{argmax}_{0\leq p_1\leq 1/2}R_S(p_1,q,q,0.0001)$. Figure 3 shows $\operatorname{argmax}_{0\leq p_2\leq 1/2}\max_{0\leq p_1\leq 1/2}R_A(p_1,p_2,q,q,0.0001)$.

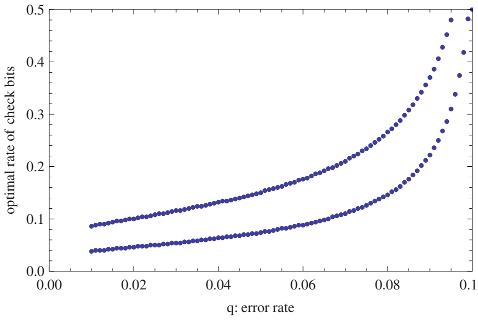

FIG. 2. (Color online) Optimal choice rate for the check bits: The upper line is argmax R_S, while the lower line is argmax R_A.

The above figures are derived by combining the type method [18] and the analysis by Hayashi [9,11] as follows. Here, we discuss security based on the key distillation protocol given by Hayashi [9,11], in which, after the generation of raw keys, classical error correction is performed using a pseudoclassical noisy channel, and random privacy amplification is carried out using the Toeplitz matrix. As was shown by Hayashi [9,11], application of a classical error correction via a pseudoclassical noisy channel is equivalent to combination of a classical error correction and discrete (partial) twirling. Hence, due to this kind of classical error correction, it is sufficient to concentrate on analysis of the security of the discrete-twirled channel. Indeed, it was proven by Hayashi ([11], that, Sec. V) when discrete twirling is applied, any lossy channel with a single-photon outcome becomes a Pauli channel, which can be described by a probabilistic application of Pauli matrices. Therefore, the following analysis deals with the case of a single-photon source with a lossy channel.

Let us calculate the probability that the estimated phase error rate is $q_\times$, and the phase error rate among raw keys is $q'_\times$. As discussed by Hayashi [9], this probability can be evaluated using the hypergeometric distribution, that is,

$$\frac{\left[\binom{Np_2^2}{Np_2^2q_\times}\binom{N(1-p_2)^2(1-p_1)}{N(1-p_2)^2(1-p_1)q'_\times}\right]}{\binom{N(p_2^2+(1-p_2)^2(1-p_1))}{Np_2^2q_\times+N(1-p_2)^2(1-p_1)q'_\times}}$$

where N is the total number of transmitted qubits. Since $\frac{1}{n+1}2^{nh(k/n)}\leq\binom{n}{k}\leq 2^{nh(k/n)}$, this probability is bounded by

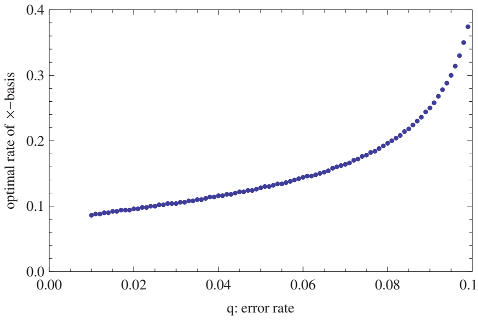

FIG. 3. (Color online) Optimal choice rate of × basis.

$$\frac{\left[\begin{pmatrix} Np_2^2 \\ Np_2^2 q_\times \end{pmatrix}\begin{pmatrix} N(1-p_2)^2(1-p_1) \\ N(1-p_2)^2(1-p_1)q'_\times \end{pmatrix}\right]}{\begin{pmatrix} N(p_2^2+(1-p_2)^2(1-p_1)) \\ Np_2^2 q_\times + N(1-p_2)^2(1-p_1)q'_\times \end{pmatrix}} \leqslant \epsilon_p(q'_\times)$$

$$:= [N(p_2^2+(1-p_2)^2(1-p_1))+1]2^{-ND_p(p_1,p_2,q_\times,q'_\times)},$$

where the exponentially decreasing rate is given by

$$\begin{aligned} D_p(p_1,p_2,q_\times,q'_\times) := {}& [p_2^2+(1-p_2)^2(1-p_1)] \\ & \times h\left(\frac{p_2^2 q_\times + (1-p_2)^2(1-p_1)q'_\times}{p_2^2+(1-p_2)^2(1-p_1)}\right) \\ & - p_2^2 h(q_\times) - (1-p_2)^2(1-p_1)h(q'_\times). \end{aligned}$$

When the phase error rate among raw keys is $q'_\times$, the random privacy amplification with the sacrificed bit rate S_2 reduces the block error probability of final keys in the × basis to $\delta_p(q'_\times) := 2^{-N[S_2-(1-p_2)^2(1-p_1)h(q'_\times)]_+}$ [9], where $[x]_+$ is x for a positive number x while $[x]_+$ is zero for a negative number x. Since $q'_\times$ takes values in $\{0,1/N,2/N,\ldots,1\}$, the (block) error probability of the final keys in the × basis is bounded above by $\Sigma_{k=0}^N \epsilon_p(k/N)\delta_p(k/N)$. Define the bound $B_p(N,p_1,p_2,q_\times)$ by $B_p(N,p_1,p_2,q_\times) := 2\sqrt{2}\sqrt{\Sigma_{k=0}^N \epsilon_p(k/N)\delta_p(k/N)}$. Then, Eve's distinguishability $\|\rho_{A,E}-\rho_A\otimes\rho_E\|_1$ is characterized by [11]

$$E\|\rho_{A,E}-\rho_A\otimes\rho_E\|_1 \leqslant E\max_X\|\rho_{E,X}-\rho_E\|_1 \leqslant B_p(N,p_1,p_2,q_\times),$$

where E denotes the average with respect to random privacy amplification, M denotes the length of the final keys, and $\rho_{E,X}$ is Eve's state when the final key is X. Hence, $B_p(N,p_1,p_2,q_\times)$ can be regarded as an upper bound for Eve's distinguishability.

Applying the type method to the parameter $q'_\times$ [18], we obtain its exponentially decreasing rate (see Hayashi [9]):

$$\begin{aligned} \lim_{N\to\infty}\frac{-1}{N}\log B_p(N,p_1,p_2,q_\times) \\ = \frac{1}{2}\min_{0\leqslant q'_\times\leqslant 1/2} & \{[S_2-(1-p_2)^2(1-p_1)h(q'_\times)]_+ \\ & + D_p(p_1,p_2,q_\times,q'_\times)\}. \end{aligned} \tag{3}$$

In the following discussion, $S_2(p_1,p_2,q_\times,C)$ represents the solution S_2 of (3), $C/2$. Thus, the quantity $S_2(p_1,p_2,q_\times,C)$ is the minimum sacrificed bit rate for random privacy under the condition that the exponentially decreasing rate of the upper bound of Eve's distinguishability is greater than $C/2$.

Now, it will be shown why the rate $p_{2,A}$ of the × basis of Alice can be assumed to be equal to the rate $p_{2,B}$ of the × basis of Bob. If different rates are chosen, then the performance is characterized by the coincidence probability for the + basis, $(1-p_{2,A})(1-p_{2,B}) = 1+p_{2,A}p_{2,B}-2(p_{2,A}+p_{2,B})$, and the coincidence probability for the × basis, $p_{2,A}p_{2,B}$. Hence, it is sufficient to maximize the coincidence probability for the + basis $(1-p_{2,A})(1-p_{2,B}) = 1+p_{2,A}p_{2,B}-2(p_{2,A}+p_{2,B})$ under the condition that the coincidence probability for the × basis $p_{2,A}p_{2,B}$ is equal to an arbitrary constant P. This maximum value occurs when $p_{2,A}=p_{2,B}=\sqrt{P}$. Thus, it is sufficient to consider only the case of $p_{2,A}=p_{2,B}$.

In order to express the rate of sacrificed bits $S_2(p_1,p_2,q_\times,C)$ as a function of the constraint C, we introduce two quantities $q'_{\times,1}$ and $q'_{\times,2}$ as solutions of the following equations in the range $[0,1/2]$:

$$D_p(p_1,p_2,q_\times,q'_{\times,1}) = C,$$

$$\frac{p_2^2 q_\times + (1-p_2)^2(1-p_1)q'_{\times,2}}{p_2^2(1-q_\times)+(1-p_2)^2(1-p_1)(1-q'_{\times,2})} = \left(\frac{q'_{\times,2}}{1-q'_{\times,2}}\right)^2.$$

Then, the rate of sacrificed bits $S_2(p_1,p_2,q_\times,C)$ is as follows:

$$S_2(p_1,p_2,q_\times,C) = (1-p_2)^2(1-p_1)h(q'_{\times,1})$$

when $q'_{\times,1}\leqslant q'_{\times,2}$. Otherwise,

$$S_2(p_1,p_2,q_\times,C) = D_p(p_1,p_2,q_\times,q'_{\times,2}) + C.$$

Next, we consider the (block) error probability of the final keys in the case when Gallager random coding and maximum likelihood decoding are applied [12]. When the bit error rate of the raw keys is q'_+ and the rate of sacrificed bits in classical error correction is S_1, the final error probability is bounded above by $\epsilon_b(q'_+) := 2^{-N[S_1-(1-p_2)^2(1-p_1)h(q'_+)]_+}$. We calculate the probability that the estimate of the bit error rate is q_+ and the phase error bit among raw keys is q'_+. Similar to the case of the bit error rate, by using the hypergeometric distribution, this probability is bounded above by $\delta_b(q'_+) := 2^{-ND_b(p_1,p_2,q_+,q'_+)}/[N(1-p_2)^2+1]$, where the exponentially decreasing rate is given by

$$\begin{aligned} & D_b(p_1,p_2,q_+,q'_+) \\ & \quad := (1-p_2)^2\{h[p_1q_+ + (1-p_1)q'_+] - p_1h(q_+) \\ & \quad - (1-p_1)h(q'_+)\}. \end{aligned}$$

Thus, the (block) error probability of the final keys in the + basis is bounded above by $B_b(N,p_1,p_2,q_+) := \Sigma_{k=0}^N \epsilon_b(k/N)\delta_b(k/N)$. Applying the type method to the parameter q'_+ [18], we obtain the exponentially decreasing rate:

$$\begin{aligned} \lim_{N\to\infty}\frac{-1}{N}\log B_b(N,p_1,p_2,q_+) \\ = \min_{0\leqslant q'_+\leqslant 1/2} & D_b(p_1,p_2,q_+,q'_+) + [S_1 \\ & - (1-p_2)^2(1-p_1)h(q'_+)]_+. \end{aligned} \tag{4}$$

In the following, $S_1(p_1,p_2,q_+,C)$ represents the solution S_1 of (4), C. Thus, the quantity, $S_1(p_1,p_2,q_+,C)$ is the minimum sacrificed bit rate in the classical error correction under the condition that the exponentially decreasing rate of the upper bound of error probability of the final keys is greater than C.

Following the discussion of $S_2(p_1,p_2,q_\times,C)$, in order to express the rate of sacrificed bits $S_1(p_1,p_2,q_\times,C)$ as a function of the constraint C, we introduce two quantities, $q'_{+,1}$ and $q'_{+,2}$ as solutions of the following in the range $[0,1/2]$:

$$D_b(p_1,p_2,q_+,q'_{+,1}) = C,$$

$$\frac{p_1 q_+ + (1-p_1)q'_{+,2}}{p_1(1-q_+) + (1-p_1)(1-q'_{+,2})} = \left(\frac{q'_{+,2}}{1-q'_{+,2}}\right)^2.$$

Therefore, $S_1(p_1,p_2,q_\times,C)$ is given as a function of the constraint C as follows. When $q'_{+,1} \leq q'_{+,2}$,

$$S_1(p_1,p_2,q_+,C) = (1-p_2)^2(1-p_1)h(q'_{+,1}).$$

Otherwise,

$$S_1(p_1,p_2,q_+,C) = D_b(p_1,p_2,q_+,q'_{+,2}) + C.$$

Hence, the final key generation rate $R_A(p_1,p_2,q_+,q_\times,C)$ is given by

$$R_A(p_1,p_2,q_+,q_\times,C) = (1-p_2)^2(1-p_1) - S_1(p_1,p_2,q_+,C) - S_2(p_1,p_2,q_\times,C).$$

Next, we consider the final key generation rate $R_S(p_1,q_+,q_\times,C)$ for the symmetric case. In this case, the exponential decreasing rate of the final error probability is given by substituting $1/2$ into p_2 in the formula $S_1(p_1,p_2,q_+,C)$. The exponentially decreasing rate of Eve's distinguishability is given by substituting $1/2$ into p_2 in the formula $S_1(p_1,p_2,q_\times,C)$. Thus, $R_S(p_1,q_+,q_\times,C)$ is calculated by

$$R_S(p_1,q_+,q_\times,C) = \frac{1-p_1}{2} - 2S_1(p_1,1/2,q_+,E) - 2S_1(p_1,1/2,q_\times,C).$$

Applying numerical analysis to these formulas, we obtain Figs. 1–3.

It has been shown that the asymmetric protocol improves the symmetric protocol under an exponential constraint condition based on the analysis of Hayashi [9]. This result suggests the importance of the choice of the ratio between the two bases when designing a QKD system. It would be interesting to attempt to implement a QKD system consisting of a single-photon source with a lossy quantum channel in the optimum ratio derived here using current technology [2–4]. A similar result can be expected based on the results of Lo *et al.* [8] and Scarani and Renner [10]. It is interesting to compare the results obtained here with those based on Lo *et al.* [8] and Scarani and Renner [10]. A similar result can also be expected for the decoy method [19–23]. Future work will investigate the same problem in a finite-length framework. In addition, it has been shown in this Rapid Communication that the exponential rate is a useful criterion for the case of limited coding length. It would be interesting to apply this criterion to other topics in QKD.

This research was partially supported by the SCOPE project of the MIC of Japan and a Grant-in-Aid for Scientific Research in the Priority Area "Deepening and Expansion of Statistical Mechanical Informatics (DEX-SMI)," No. 18079014 and a MEXT Grant-in-Aid for Young Scientists (A) No. 20686026. The author thanks Professor Keiichi Edamatsu and Professor Shigeki Takeuchi for explaining the current research on the development of a single-photon source.

[1] C. H. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India, 1984* (IEEE, New York, 1984), p. 175.

[2] M. B. Ward *et al.*, Appl. Phys. Lett. **90**, 063512 (2007).

[3] K. Takemoto *et al.*, J. Appl. Phys. **101**, 081720 (2007).

[4] C. Kurtsiefer *et al.*, Phys. Rev. Lett. **85**, 290 (2000); R. Brouri *et al.*, Opt. Lett. **25**, 1294 (2000); http://www.gizmag.com/quantum-computing-single-particle/8907/.

[5] D. Mayers, in *Advances in Cryptology—Proceedings of Crypto'96*, edited by N. Koblitz, Lecture Notes in Computer Science, Vol. 1109 (Springer-Verlag, New York, 1996), p. 343; J. ACM **48**, 351 (2001).

[6] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).

[7] R. Renner *et al.*, Phys. Rev. A **72**, 012332 (2005); G. Smith *et al.*, Phys. Rev. Lett. **100**, 170502 (2008); H. F. Chau, Phys. Rev. A **66**, 060302(R) (2002); J. Bae and A. Acín, *ibid.* **75**, 012334 (2007); S. Watanabe *et al.*, *ibid.* **76**, 032312 (2007); R. Renner, Ph.D thesis, ETH, Switzerland, 2005, e-print arXiv:quant-ph/0512258; D. Gottesman and H.-K. Lo, IEEE Trans. Inf. Theory **49**, 457 (2003); X. B. Wang, Phys. Rev. Lett. **92**, 077902 (2004); in *Quantum Computation and Information—From Theory To Experiment*, edited by H. Imai and M. Hayashi (Springer, Berlin, 2006), pp. 185–233; S. Watanabe *et al.*, Phys. Rev. A **78**, 042316 (2008).

[8] H.-K. Lo *et al.*, J. Cryptology **18**, 133 (2005).

[9] M. Hayashi, Phys. Rev. A **74**, 022307 (2006).

[10] V. Scarani and R. Renner, Phys. Rev. Lett. **100**, 200501 (2008).

[11] M. Hayashi, Phys. Rev. A **76**, 012329 (2007); **79**, 019901(E) (2009).

[12] R. G. Gallager, *Information Theory and Reliable Communication* (John Wiley & Sons, New York, 1968).

[13] M. Hamada, J. Phys. A **37**, 8303 (2004).

[14] S. Watanabe *et al.*, Int. J. Quantum Inf. **4**, 935 (2006).

[15] M. Ben-Or *et al.*, *Theory of Cryptography: Second Theory of Cryptography Conference, TCC 2005*, edited by J. Kilian Lecture Notes in Computer Science, Vol. 3378 (Springer, Berlin, 2005).

[16] L. Carter and M. Wegman, J. Comput. Syst. Sci. **18**, 143 (1979).

[17] H. Krawczyk, in *Advances in Cryptology—CRYPTO '94*, edited by Yuo Desmedt, Lecture Notes in Computer Science Vol. 839 (Springer-Verlag, Berlin, 1994), pp 129–139.

[18] I. Csiszár and J. Körner, *Information Theory: Coding Theorems for Discrete Memoryless Systems* (Akadémiai, Kiado, Budapest, 1981).

[19] W.-Y. Hwang, Phys. Rev. Lett. **91**, 057901 (2003).

[20] X.-B. Wang, Phys. Rev. Lett. **94**, 230503 (2005).

[21] H.-K. Lo *et al.*, Phys. Rev. Lett. **94**, 230504 (2005).

[22] M. Hayashi, New J. Phys. **9**, 284 (2007).

[23] J. Hasegawa *et al.*, e-print arXiv:0707.3541.