Secure Quantum Key Distribution with an Uncharacterized Source

Masato Koashi[1] and John Preskill[2]

[1]*CREST Research Team for Interacting Carrier Electronics, School of Advanced Sciences,
The Graduate University for Advanced Studies (SOKENDAI), Hayama, Kanagawa, 240-0193, Japan*
[2]*Institute for Quantum Information, California Institute of Technology, Pasadena, California 91125*

We prove the security of the Bennett-Brassard (BB84) quantum key distribution protocol for an arbitrary source whose averaged states are basis independent, a condition that is automatically satisfied if the source is suitably designed. The proof is based on the observation that, to an adversary, the key extraction process is equivalent to a measurement in the $\hat{\sigma}_x$ basis performed on a pure $\hat{\sigma}_z$-basis eigenstate. The dependence of the achievable key length on the bit error rate is the same as that established by Shor and Preskill [Phys. Rev. Lett. **85**, 441 (2000)] for a perfect source, indicating that the defects in the source are efficiently detected by the protocol.

Quantum key distribution is an ingenious application of quantum mechanics, in which two remote parties (Alice and Bob) establish a shared secret key through the transmission of quantum signals. In the Bennett-Brassard (BB84) protocol [1], Alice sends a key bit to Bob by preparing a qubit in one of two conjugate bases and Bob measures the qubit in one of the two bases; the eavesdropper Eve, who does not know the basis chosen by Alice or by Bob, cannot collect information about the key without producing a detectable disturbance. This protocol, when suitably augmented by classical error correction and privacy amplification, is provably secure against any attack by Eve [2–5].

Though security can be proven without imposing any restriction on Eve's attack (other than the requirement that she has no *a priori* information about the basis used), it is necessary to place conditions on the performance of the source and detector employed in the protocol. In the Shor-Preskill proof [5], it is assumed that any flaws in the source and detector can be absorbed into Eve's basis-independent attack. The proof by Mayers [2], however, applies to a more general setting: although the source is perfect, the detector has never been tested and is completely *uncharacterized*. Indeed, the detector could be under the control of Eve's collaborator Fred. Fred is unable to send messages to Eve, but he knows Bob's basis and can adjust the measurement performed by the detector accordingly. Still, as Mayers showed, Fred cannot fool Alice and Bob into accepting a key that Eve knows, as long as the efficiency of the detector is basis independent. Since a real device could have an indefinite number of degrees of freedom, no test can fully characterize it; therefore, proving security in the case of an uncharacterized apparatus provides comfort to a highly suspicious user of the key distribution scheme.

In this Letter, we present a simple proof of the security of the BB84 protocol that applies to a setting opposite to that considered by Mayers: the detector is perfect and

Fred controls the *source*. We, however, place one important restriction on Fred's attack—the source must not leak any information to Eve about the basis chosen by Alice. That is, the state emitted by the source, averaged over the values of Alice's key bit, is required to be independent of Alice's basis. Our proof applies to faulty sources that are notably more general than those encompassed by the Shor-Preskill proof; to give just one example, it applies to a source that performs perfectly when Alice chooses the $\hat{\sigma}_x$ basis but that rotates the qubit when Alice chooses the $\hat{\sigma}_z$ basis. Nevertheless, our proof shows that a secure key can be extracted from a sifted key at the same rate established by Shor and Preskill.

Our proof combines insights gleaned from both the Mayers proof and the Shor-Preskill proof. Following Mayers, we analyze the information about (Bob's) key collected by Eve in the case where Alice and Bob are using *different* bases. Following Shor and Preskill, we bound Eve's information by observing that Bob *could have* performed an error correction to remove any entanglement with Eve's probe before executing the measurement that extracts his final key. The core of our proof is the observation that a single quantum circuit computes Bob's final key in the $\hat{\sigma}_x$ basis and reverses the damage inflicted by Eve if the error rate is small in the $\hat{\sigma}_z$ basis. Using the same method, we can also prove security for the case of an uncharacterized detector.

Before proceeding to the proof, let us specify in more detail our models of the source and detector. Alice prepares a physical system with Hilbert space $\mathcal{H}_A$, which has an arbitrary size, in one of four states $\hat{\rho}(a, g)$ with probability $p_{a,g}$; $a = 0, 1$ labels Alice's basis choice and $g = 0, 1$ is the value of her key bit. The choice of a is assumed to be completely random: $p_{a,0} + p_{a,1} = 1/2$. We assume that the states satisfy

$$p_{0,0}\hat{\rho}(0, 0) + p_{0,1}\hat{\rho}(0, 1) = p_{1,0}\hat{\rho}(1, 0) + p_{1,1}\hat{\rho}(1, 1), \tag{1}$$

which is vital in the security proof. A convenient way to prepare such an ensemble is to introduce an auxiliary system A' with Hilbert space $\mathcal{H}_{A'}$. Alice first prepares $\mathcal{H}_A \otimes \mathcal{H}_{A'}$ in an entangled state $\hat{\rho}_{AA'}$ and then performs a measurement M_a on system A' alone. The measurement M_a gives a binary outcome, determining g. Equation (1) is then satisfied because the choice of the measurement, M_0 or M_1, does not affect the marginal state of $\mathcal{H}_A$. Hence, if the source is realized in this way, there is no need to test its performance.

As noted in [6], if A' is a qubit, M_0 is a measurement of $\hat{\sigma}_z$, and M_1 is a measurement of $\hat{\sigma}_x$, then security can be established by the method of Shor and Preskill. But our security proof invokes only the condition (1); no further properties of $\hat{\rho}_{AA'}$, M_0, or M_1 need be specified.

At the end of the transmission channel $\mathcal{H}_A \to \mathcal{H}_B$, Bob switches between two measurements on $\mathcal{H}_B$. We assume that the two measurements are modeled by a common quantum channel $\mathcal{H}_B \to \mathcal{H}_2$, where $\dim \mathcal{H}_2 = 2$, followed by the measurement of the Pauli operator $\hat{\sigma}_z$ or $\hat{\sigma}_x$. In the security proof, we include the common quantum channel in the transmission channel between Alice and Bob, so that Bob receives a qubit at the end of the channel.

The protocol that we shall prove to be secure is the following: Let $\Omega \equiv \{1, \ldots, 4N(1 + \epsilon)\}$. The variable denoted by $\bar{a}$ takes the value opposite to a.

Protocol 1 (BB84).—(1) Alice creates random bit sequences $\{a_i\}$ and $\{g_i\}$ for $i \in \Omega$. Alice randomly chooses a subset $R \subset \Omega$ with size $|R| = 2N(1 + \epsilon)$. (2) Bob creates a random bit sequence $\{b_i\}$. (3) When $i \in R$, Alice sends $\hat{\rho}(a_i, g_i)$. When $i \in \bar{R}(\equiv \Omega - R)$, Alice sends $\hat{\rho}(\bar{a}_i, g_i)$. (4) Bob measures $\hat{\sigma}_z$ when $b_i = 0$ and measures $\hat{\sigma}_x$ when $b_i = 1$. For either case, he sets bit h_i according to the outcome ($h_i = 0$ for outcome 1 and $h_i = 1$ for outcome -1). (5) Bob announces $\{b_i\}$. Alice announces $\{a_i\}$ and R. If the size of $T \equiv \{i \in R | a_i = b_i\}$ is less than N, the protocol aborts. Bob decides randomly on a subset $S \subset \{i \in \bar{R} | \bar{a}_i = b_i\}$ with $|S| = N$ and announces (if he cannot do this, the protocol aborts). (6) Alice and Bob compare g_i and h_i for $i \in T$ and determine the error rate δ. If δ is too large, the protocol aborts. (7) Bob randomizes the positions of the N qubits in S by a permutation π and announces π. Bob announces a linear code C with $|C| = 2^r$ that corrects $N(\delta + \epsilon)$ errors occurring in random positions with probability exponentially close to unity. (8) The sifted key κ_{sif} of length N is defined as the sequence $\{h_i\}_{i \in S}$. The final key is the coset $\kappa_{\text{sif}} + C^\perp$. (9) Alice obtains κ_{sif} by applying an error correction scheme to $\{g_i\}_{i \in S}$ via encrypted communication with Bob, consuming τ bits of the previously shared secret key. Then Alice obtains the final key.

Protocol 1 is the standard BB84 protocol, except for the use of $\bar{a}_i$ in place of a_i in steps (3) and (5), which we have adopted for later convenience in the proof. The random permutation π in step (7) is redundant, since it suffices to choose the code C randomly instead of doing the permu-

tation. In the limit of large N, the achievable r/N reaches $1 - h(\delta)$ [where $h(\delta) = -\delta\log_2\delta - (1 - \delta)\log_2(1 - \delta)$], and τ/N in step (9) approaches $h(\delta)$, resulting in the rate of key generation $1 - 2h(\delta)$.

Our proof uses some basic properties of (classical) error-correcting codes. The linear code C appearing in step (7) is an r-dimensional subspace of the binary vector space $\mathbf{F}_2^N$. The code $C^\perp$ appearing in step (8) is the orthogonal complement of C, called the dual of C. We can specify a linear coding function $G : \mathbf{F}_2^r \to \mathbf{F}_2^N$, which assigns a distinct codeword of C to each binary sequence of length r. We have assumed in the protocol that C corrects $N(\delta + \epsilon)$ errors occurring in random positions with probability exponentially close to unity. More specifically, there exists a set of correctable errors $\mathcal{E} \subset \mathbf{F}_2^N$ and a decoding function $f : \mathbf{F}_2^N \to \mathbf{F}_2^r$, satisfying

$$f(G(y) + x) = y \qquad (2)$$

for any $y \in \mathbf{F}_2^r$ and any $x \in \mathcal{E}$. A random error with weight at most $N(\delta + \epsilon)$ belongs to $\mathcal{E}$ with probability exponentially close to unity. The function f is not necessarily linear and may be hard to compute, but we will need only its existence for the proof of security—Bob does not compute f in the actual protocol.

What Bob actually calculates is the coset $\kappa_{\text{sif}} + C^\perp$ in step (8). One way to do this is to use the function $G^T : \mathbf{F}_2^N \to \mathbf{F}_2^r$, which is the adjoint (matrix transpose) of G satisfying $G^T(x) \cdot y = x \cdot G(y) \pmod 2$ for any $x \in \mathbf{F}_2^N$ and $y \in \mathbf{F}_2^r$. Since the kernel of $G^T(x)$ is $C^\perp$, the final key is the r-bit sequence $G^T(\kappa_{\text{sif}})$. The duality between G and G^T will play an important role in the proof below.

In order to prove that protocol 1 is secure, we need to show that Eve's maximum knowledge I_1 about the final key is negligible. Note that Bob's final key is determined at step (8); step (9), which assures that Alice's key agrees with Bob's and leaks no information to Eve, is not relevant to I_1. Let us compare protocol 1 with a modified one.

Protocol 2.—(3)$'$ When $i \in R$, Alice sends $\hat{\rho}(a_i, g_i)$. When $i \in \bar{R}$, Alice also sends $\hat{\rho}(a_i, g_i)$. The other steps are the same as in protocol 1.

This modification follows Mayers's argument [2] except for the exchanged roles of the sender and the receiver. The only difference between protocols 1 and 2 is a flip in Alice's basis for $i \in \bar{R}$. But the bits $\{g_i\}$ for $i \in \bar{R}$ are kept secret by Alice. Hence, for Eve and Bob only the state averaged over $\{g_i\}$ is relevant, and this state is identical for the two protocols by the condition Eq. (1). Therefore, Eve's maximum knowledge I_2 about Bob's final key in protocol 2 is the same as I_1.

Next, let us further modify protocol 2 in favor of Eve, by allowing Eve to control Alice's source. Now Eve knows $\{a_i\}$ and $\{g_i\}$ and is free to prepare the states measured by Bob however she pleases. Since the states $\hat{\rho}(a_i, g_i)$ have been removed from the protocol and Bob's measurements are symmetric in b_i, the protocol is completely symmetric in $\{a_i\}$ and $\{g_i\}$. Therefore we may

assume $a_i = g_i = 0$ without loss of generality. The resulting protocol is as follows.

Protocol 3.—(1) Alice randomly chooses a subset $R \subset \Omega$ with size $|R| = 2N(1 + \epsilon)$. (2) Bob creates a random bit sequence $\{b_i\}$. (3) Eve prepares Bob's qubits and her ancilla system in a state. (4) Bob measures $\hat{\sigma}_z$ when $b_i = 0$ and measures $\hat{\sigma}_x$ when $b_i = 1$. For either case, he sets the bit h_i according to the outcome. (5) Bob announces $\{b_i\}$. Alice announces R. If the size of $T \equiv \{i \in R | b_i = 0\}$ is less than N, the protocol aborts. Bob decides randomly on a subset $S \subset \{i \in \bar{R} | b_i = 1\}$ with $|S| = N$ and announces (if he cannot do this, the protocol aborts). (6) Bob counts the number n of bits with $h_i = 1$ for $i \in T$ and determines the error rate $\delta = n/|T|$. If δ is too large, the protocol aborts. (7) Bob randomizes the positions of the N qubits in S by a permutation π and announces π. Bob announces a linear code C. (8) The sifted key κ_{sif} of length N is defined as $\{h_i\}_{i \in S}$. The final key is the coset $\kappa_{\text{sif}} + C^{\perp}$.

Since the modifications in the protocol favor Eve, Eve's maximum knowledge I_3 about the final key in protocol 3 is no less than I_2: thus $I_1 = I_2 \leq I_3$. To complete the proof, we will show that I_3 is small—Eve cannot predict Bob's key accurately because Bob is measuring in the "wrong" basis.

Let us denote the Hilbert space of Eve's system as $\mathcal{H}_E$ and that of the N qubits belonging to S as $\mathcal{H}_S$. We may imagine that Bob's measurement on set S is delayed until step (8) and denote by $\hat{\rho}$ the state over $\mathcal{H}_S \otimes \mathcal{H}_E$ after the verification test on the set T is done, but before the qubits in S are measured. The test on T finds that the rate of error ($\hat{\sigma}_z = -1$) over N (or more) randomly chosen qubits is δ. If the qubits in the set S were also measured in the σ_z basis, then the joint probability of finding an error rate less than δ in T and finding more than $N(\delta + \epsilon)$ errors in S would be asymptotically less than $\exp[-\epsilon^2 N / 4(\delta - \delta^2)]$ for any strategy by Eve. Ignoring any inefficient strategy that has only an exponentially small probability of giving an error rate less than δ in T, we conclude that for the state $\hat{\rho}$, the probability of finding more than $N(\delta + \epsilon)$ errors in S is exponentially small.

Let $\{|v\rangle_Z, v \in \mathbf{F}_2^N\}$ denote the "Z basis" of $\mathcal{H}_S$, where the value of the jth bit of v corresponds to the eigenvalue of $\hat{\sigma}_z$ on the jth qubit, and let $\{|v\rangle_X = \hat{H}^N |v\rangle_Z\}$ denote the "X basis," where $\hat{H}^N$ is the Hadamard transformation acting on the N qubits. The announcement of π in step (7) can be described as the transmission from Bob to Eve of a particle J in one of $N!$ orthogonal states $\{|\pi\rangle_J\}$. The symmetrized state held by Bob and Eve after transmission of the particle is

$$\hat{\rho}_s = (N!)^{-1} \sum_{\pi} |\pi\rangle_J \langle \pi| \otimes (\hat{U}_{\pi} \otimes \hat{1}_E) \hat{\rho} (\hat{U}_{\pi}^{\dagger} \otimes \hat{1}_E). \quad (3)$$

Let $\hat{P}_{\mathcal{E}}$ be the projection of $\mathcal{H}_S$ onto the subspace spanned by the states $|e\rangle_Z$ such that $e \in \mathcal{E}$. The successful verification test ensures that the probability of finding an

error pattern that is not in $\mathcal{E}$ is exponentially small: $\text{Tr}[(\hat{P}_{\mathcal{E}} \otimes \hat{1}_E) \hat{\rho}_s] \geq 1 - \eta$, where η is an exponentially small number. (We are now regarding the particle J as part of Eve's system E.) If we define $\hat{\rho}'$ as

$$\hat{\rho}' \equiv \frac{(\hat{P}_{\mathcal{E}} \otimes \hat{1}_E) \hat{\rho}_s (\hat{P}_{\mathcal{E}} \otimes \hat{1}_E)}{\text{Tr}[(\hat{P}_{\mathcal{E}} \otimes \hat{1}_E) \hat{\rho}_s]}, \quad (4)$$

its fidelity [7] to $\hat{\rho}_s$, $F(\hat{\rho}', \hat{\rho}_s) \equiv [\text{Tr}(\sqrt{\sqrt{\hat{\rho}'} \hat{\rho}_s \sqrt{\hat{\rho}'}})^{1/2}]^2$, is given by

$$F(\hat{\rho}', \hat{\rho}_s) = \text{Tr}[(\hat{P}_{\mathcal{E}} \otimes \hat{1}_E) \hat{\rho}_s] \geq 1 - \eta. \quad (5)$$

In what follows, we will show that if the state $\hat{\rho}'$ instead of $\hat{\rho}_s$ were used, Eve would have no information about the final key ($I_3 = 0$). Then we will infer that any actual strategy by Eve (that passes the verification test with a probability that is not exponentially small) gives her exponentially small information.

In protocol 3, Bob measures in the Z basis for the verification test, and in the X basis to generate the key—we need to show that if the error rate is low in the Z basis, then the key is random and private. Our proof invokes a quantum circuit that outputs the same r-bit final key as Bob finds in protocol 3, and that also expunges Eve's entanglement with the key bits. Though Bob might not have actually executed this circuit, it would be all the same to Eve if he had, which is sufficient to ensure privacy.

The circuit, shown in Fig. 1, uses an auxiliary system Q of r qubits initially prepared in the state $|0\rangle_X$ and is a composition $\hat{U} \equiv \hat{U}_2 \hat{U}_1$ of two unitary operators $\hat{U}_1$ and $\hat{U}_2$. The operator $\hat{U}_1$, which calculates the final key, acts in the X basis as

$$\hat{U}_1 : |x\rangle_X \otimes |y\rangle_X \rightarrow |x\rangle_X \otimes |y + G^T(x)\rangle_X. \quad (6)$$

Using the duality between G and G^T, we easily see that U_1 acts in the Z basis as

$$\hat{U}_1 : |x\rangle_Z \otimes |y\rangle_Z \rightarrow |x + G(y)\rangle_Z \otimes |y\rangle_Z. \quad (7)$$

The operator $\hat{U}_2$ is defined in the Z basis as

$$\hat{U}_2 : |x\rangle_Z \otimes |y\rangle_Z \rightarrow |x\rangle_Z \otimes |y + f(x)\rangle_Z, \quad (8)$$

and in the X basis acts as

$$\hat{U}_2 : |x\rangle_X \otimes |y\rangle_X \rightarrow |\Psi_{x,y}\rangle_X \otimes |y\rangle_X. \quad (9)$$
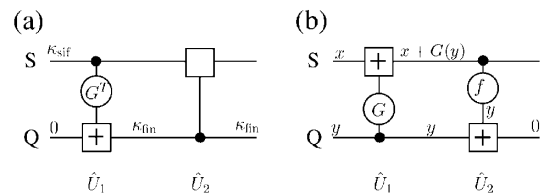

FIG. 1. (a) A quantum circuit calculating $\kappa_{\text{fin}} = G^T(\kappa_{\text{sif}})$ in the X basis. (b) The same circuit in the Z basis. When $x \in \mathcal{E}$, the final state of system Q is $|0\rangle_Z$.

Here $|\Psi_{x,y}\rangle$ is a rather complicated state of $\mathcal{H}_S$, but its exact form is not relevant here.

If the initial state of the ancilla Q is $|0\rangle_X$, then from Eqs. (6) and (9) we have

$$\hat{U}(|\kappa_{\mathrm{sif}}\rangle_X \otimes |0\rangle_X) = |\Psi_{x,\kappa_{\mathrm{fin}}}\rangle_X \otimes |G^T(\kappa_{\mathrm{sif}})\rangle_X; \qquad (10)$$

the final key $\kappa_{\mathrm{fin}} = G^T(\kappa_{\mathrm{sif}})$ is obtained by measuring the system Q in the X basis after execution of the circuit. Meanwhile, Eqs. (7) and (8) with $|0\rangle_X \propto \sum_y |y\rangle_Z$ lead to

$$\hat{U}(|x\rangle_Z \otimes |0\rangle_X) \propto \sum_y |x + G(y)\rangle_Z \otimes |y + f(x + G(y))\rangle_Z; \qquad (11)$$

if $x \in \mathcal{E}$, the final state of Q is $|0\rangle_Z$, due to Eq. (2). Then, Eq. (4) ensures that if the initial state of $\mathcal{H}_S \otimes \mathcal{H}_E$ is $\hat{\rho}'$, the final marginal state of Q is still $|0\rangle_Z$. Therefore, the final state $\hat{\rho}_Q$ of Q obtained when we start from the actual state $\hat{\rho}_s$ is exponentially close to $|0\rangle_Z$:

$$_Z\langle 0|\hat{\rho}_Q|0\rangle_Z \geq F(\hat{\rho}', \hat{\rho}_s) \geq 1 - \eta. \qquad (12)$$

Equation (12) establishes that the final key can be obtained from a complete X-basis measurement on the state $\hat{\rho}_Q$, whose fidelity to the Z-basis eigenstate $|0\rangle_Z$ is exponentially close to unity. From this, we conclude the following: (a) The mutual information I_3 between the final key and Eve, who may conduct any measurement on her system, is upper bounded by the von Neumann entropy $S(\hat{\rho}_Q)$ [8]. Since $\hat{\rho}_Q$ has an eigenvalue greater than or equal to $1 - \eta$, we have $I_1 \leq I_3 \leq S(\hat{\rho}_Q) \leq h(\eta) + \eta \log_2(2^r - 1) < h(\eta) + r\eta$. (b) The probability distribution p_y over the 2^r final keys is very close to uniform. In fact, the fidelity to the uniform distribution cannot be lower than the fidelity in Eq. (12). Thus we have $2^{-r}(\sum_y \sqrt{p_y})^2 \geq 1 - \eta$. Using the inequality $-2\log_2 x \leq r(1-x)^2 + (1-x^2)/(\ln 2)$ which holds for $x \geq 2^{-r/2}$ when r is large, the Shannon entropy of $\{p_y\}$ is bounded as $H(\{p_y\}) = r + 2\sum_y p_y \log_2(2^r p_y)^{-1/2} \geq r(2\sqrt{1-\eta} - 1) \geq r(1 - 2\eta)$.

The two imperfections of the final key derived in (a) and (b) can be combined into a single parameter by the following argument. Let us assume that Bob randomly chooses and announces a bit sequence $w \in \mathbf{F}_2^r$ and produces a new key $w + y$ which is truly uniformly distributed. If Eve's information about y is I_1, then her information about $w + y$ is

$$I = r - H(\{p_y\}) + I_1 < 3r\eta + h(\eta), \qquad (13)$$

which is also exponentially small, concluding the proof.

Finally, suppose that Bob uses a detector with imperfect efficiency, which has a "null" outcome (signifying a detection failure) in addition to the valid binary outcome. Our proof remains valid, provided that the efficiency (probability of obtaining a valid outcome) is the same for the two bases, and the size of Ω is increased.

Our proof of security applies to an uncharacterized source with basis-independent averaged states. By interchanging the roles of sender and receiver, the same proof can be applied to the case of an uncharacterized detector, considered by Mayers [2]. Indeed, in that case our proof allows a more general source (one triggered by a perfect measurement on half of an entangled state, as opposed to a perfect source) and a higher rate of key generation $[1 - 2h(\delta)$ rather than $1 - h(\delta) - h(2\delta)]$ than established by Mayers. In either case, by exploiting the duality between the operation that encodes a message using C and the operation that computes a $C^\perp$ coset, our proof illuminates the connection between a low error rate and successful privacy amplification.

It is also interesting to consider *characterized* imperfect sources and detectors that have limited basis-dependent flaws. One important case of a characterized defective source, recently analyzed in [9], is a source that occasionally emits two identical copies of a qubit, one of which can be intercepted by Eve. In this case, our proof does not apply because Eq. (1) is not satisfied. Security criteria for characterized sources and detectors are further discussed in [10].

[1] C. H. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India* (IEEE, New York, 1984), pp. 175–179.
[2] D. Mayers, in *Advances in Cryptography—Proceedings of Crypto '96* (Springer-Verlag, New York, 1996), pp. 343–357; J. Assoc. Comput. Mach. **48**, 351 (2001).
[3] H.-K. Lo and H. F. Chau, Science **283**, 2050 (1999).
[4] E. Biham, M. Boyer, P. O. Boykin, T. Mor, and V. Roychowdhury, in *Proceedings of the 32nd Annual ACM Symposium on Theory of Computing* (ACM Press, New York, 2000), pp. 715–724.
[5] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).
[6] D. Gottesman and J. Preskill, Phys. Rev. A **63**, 022309 (2001).
[7] A. Uhlmann, Rep. Math. Phys. **9**, 273 (1976); R. Jozsa, J. Mod. Opt. **41**, 2315 (1994).
[8] A. S. Holevo, Probl. Inf. Transm. (Engl. Transl.) **9**, 117 (1973).
[9] H. Inamori, N. Lütkenhaus, and D. Mayers, quant-ph/0107017.
[10] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, quant-pn/0212066.