Unconditionally Secure Key Distribution Based on Two Nonorthogonal States

Kiyoshi Tamaki, Masato Koashi, and Nobuyuki Imoto
CREST Research Team for Interacting Carrier Electronics, School of Advanced Sciences,
The Graduate University for Advanced Studies (SOKENDAI), Hayama, Kanagawa, 240-0193, Japan
(Received 28 December 2002; published 24 April 2003)

We prove the unconditional security of the Bennett 1992 protocol, by using a reduction to an entanglement distillation protocol initiated by a local filtering process. The bit errors and the phase errors are correlated after the filtering, and we can bound the amount of phase errors from the observed bit errors by an estimation method involving nonorthogonal measurements. The angle between the two states shows a trade-off between accuracy of the estimation and robustness to noises.

DOI: 10.1103/PhysRevLett.90.167904 PACS numbers: 03.67.Dd, 03.67.Hk

Quantum key distribution (QKD) provides a way to share a secret key between two parties (Alice and Bob) with negligibly small leakage of information to an eavesdropper (Eve). One of the simplest of such protocols is called B92 [1], which is based on the transmission of only two nonorthogonal states. For a qubit channel between Alice and Bob, this protocol proceeds as follows. Alice randomly chooses a bit value j and prepares a qubit in state $|\varphi_j\rangle \equiv \beta|0_x\rangle + (-1)^j\alpha|1_x\rangle$, where $0 < \alpha < 1/\sqrt{2}$, $\beta \equiv \sqrt{1-\alpha^2}$, and $\{|0_x\rangle, |1_x\rangle\}$ is a basis (X basis) of the qubit. She sends the qubit through the channel to Bob, who performs a measurement $\mathcal{M}_{\rm B92}$ with three outcomes $j' = 0$, 1, "null." The measurement $\mathcal{M}_{\rm B92}$ involves the projection measurement on the basis $\{|\varphi_j\rangle, |\overline{\varphi}_j\rangle\}$ with randomly chosen j and is defined by the POVM (positive operator valued measure) $F_0 = |\overline{\varphi}_1\rangle\langle\overline{\varphi}_1|/2$, $F_1 = |\overline{\varphi}_0\rangle\langle\overline{\varphi}_0|/2$, and $F_{\rm null} = 1 - F_0 - F_1$, where $|\overline{\varphi}_j\rangle \equiv \alpha|0_x\rangle - (-1)^j\beta|1_x\rangle$ is the state orthogonal to $|\varphi_j\rangle$. When the outcome is $j' =$ null, Bob announces that to Alice and they discard the event. Otherwise, they take notes of their bit values j and j', which should coincide in the absence of channel noises and Eve's intervention. Repeating this procedure many times, Alice and Bob each obtain a sequence of bits. Then they convert the sequences into a shared secret key through public discussions. Intuitively, the security of this protocol is based on the fact that Eve cannot discriminate two nonorthogonal states deterministically.

Although the QKD protocols themselves are simple, it is quite hard to prove the unconditional security, i.e., security against an adversary able to perform any operation allowed by quantum mechanics such as interacting all of the transmitted qubits jointly to a big probe system. This task has been accomplished [2] for the BB84 protocol [3], which involves four states forming two conjugate bases. Subsequent proofs [4–6] have provided us more than a basic claim of security, including a beautiful interplay [5,6] between QKD and other important protocols in quantum information, such as the entanglement distillation protocol (EDP) [7] and the Calderbank-Shor-Steane (CSS) quantum error correcting codes [8]. It is natural to ask about the unconditional security of the B92 protocol, which is conceptually the simplest of the QKD protocols. In contrast to BB84, it involves a free parameter α representing the nonorthogonality. The analyses of the B92 protocol are hence expected to give us an idea about how the nonorthogonality is related to the ability to convey secret information. Since the security proofs of BB84 rely on the symmetry of the protocol which is not shared in B92, it is not a trivial task to modify it for B92, except for the limiting case of $|\langle\varphi_0|\varphi_1\rangle|^2 = 1/2$ [9].

In this Letter, we give a proof of the unconditional security of the B92 protocol for qubit channels, applicable to any amount of nonorthogonality α. We show that the B92 protocol is, from Eve's point of view, identical to an EDP initiated by a local filtering [10]. The security is then established by proving that the EDP is almost always successful. We also develop a method to estimate an error rate by measuring randomly chosen samples on a different basis, which plays an important role in the proof.

We first introduce a protocol involving EDP, which is then shown to be reduced to the B92 protocol. We assume that Alice initially prepares a pair of qubits AB in the state $|\Psi\rangle_{\rm AB} = (|0_z\rangle_{\rm A}|\varphi_0\rangle_{\rm B} + |1_z\rangle_{\rm A}|\varphi_1\rangle_{\rm B})/\sqrt{2}$, which is nonmaximally entangled. Here the Z basis $\{|0_z\rangle, |1_z\rangle\}$ of a qubit is related to the X basis by $|j_z\rangle = [|0_x\rangle + (-1)^j|1_x\rangle]/\sqrt{2}$. Alice sends Bob the qubit B through a quantum channel. Suppose that Bob performs a "local filtering operation" on qubit B, described by the Hermitian operator $F_{\rm fil} \equiv \alpha|0_x\rangle_{\rm B}\langle 0_x| + \beta|1_x\rangle_{\rm B}\langle 1_x|$. When the state of AB was ρ, the qubit B passes the filtering with probability $p = {\rm Tr}[\rho(\mathbf{1}_{\rm A} \otimes F_{\rm fil})^2]$, resulting in the filtered state $[(\mathbf{1}_{\rm A} \otimes F_{\rm fil})\rho(\mathbf{1}_{\rm A} \otimes F_{\rm fil})]/p$. When the channel is noiseless and Eve does nothing, this process is just the Procrustean method mentioned in [11]: the filtered state should be the maximally entangled state (EPR state) $|\Phi^+\rangle = (|0_x\rangle_{\rm A}|0_x\rangle_{\rm B} + |1_x\rangle_{\rm A}|1_x\rangle_{\rm B})/\sqrt{2}$, since the initial state is also written as $|\Psi\rangle_{\rm AB} = \beta|0_x\rangle_{\rm A}|0_x\rangle_{\rm B} + \alpha|1_x\rangle_{\rm A}|1_x\rangle_{\rm B}$. When noise is present, the filtered state may include a bit error, represented by the subspace spanned by $\{|0_z\rangle_{\rm A}|1_z\rangle_{\rm B}, |1_z\rangle_{\rm A}|0_z\rangle_{\rm B}\}$, and a phase error, represented by the subspace spanned by $\{|0_x\rangle_A|1_x\rangle_B, |1_x\rangle_A|0_x\rangle_B\}$. In parallel to the protocols for BB84 [5,6], we can consider the following protocol that will work in the presence of noise.

Protocol 1.—(1) Alice creates $2N$ pairs in the state $|\Psi\rangle_{AB}^{\otimes 2N}$, and she sends the second half of each pair to Bob over a quantum channel. (2) By public discussion, Alice and Bob randomly permute the position of $2N$ pairs of qubits. (3) For the first N pairs (check pairs), Alice measures her halves on the Z basis, and Bob performs measurement $\mathcal{M}_{B92}$ on his halves. By public discussion, they determine the number n_{err} of errors in which Alice found $|0_z\rangle$ and Bob's outcome was 1, or Alice found $|1_z\rangle$ with Bob's outcome 0. (4) For the second N pairs (data pairs), Bob performs the filtering F_{fil} on each of his qubits and announces the total number n_{fil} and the positions of the qubits that have passed the filtering. (5) From n_{err} and n_{fil}, they estimate an upper bound for the number of bit errors n_{bit}, and an upper bound for the number of phase errors n_{ph}, in the n_{fil} pairs. If these bounds are too large, they abort the protocol. (6) They run an EDP that can produce n_{key} nearly perfect EPR pairs if the estimation is correct. (7) Alice and Bob each measure the EPR pairs in the Z basis to obtain a shared secret key.

For the same reason as in the proofs of BB84 [5,6], if the estimation in step (5) is correct except for a probability that becomes exponentially small as N increases, the final shared key is essentially secure. Intuitively, this comes from the fact that Eve has no clue on the outcomes of a measurement performed on an EPR pair, since it is in a pure state by definition. We will soon show how to estimate the upper bounds for the errors in step (5). Before that, we show that *Protocol 1* can be reduced to the B92 protocol.

According to the discussion by Shor and Preskill [6], we can use a one-way EDP based on CSS codes in step (6). Then, they have further shown that the whole extraction process of the n_{key}-bit final secret key from the noisy n_{fil} pairs in steps (6) and (7) can be equivalently accomplished by Z-basis measurements directly performed on Alice's and Bob's qubits of the n_{fil} noisy pairs, followed by a public discussion. Hence, without affecting the security, we can assume that Alice performs Z-basis measurements immediately after she has prepared the state $|\Psi\rangle_{AB}$ and that Bob performs Z-basis measurements immediately after he has performed the filtering. *Protocol 1* is thus reduced to a prepare-and-measure protocol. Now, note the following relation for $j' = 0, 1$, which is easily confirmed:

$$F_{fil}|j'_z\rangle_B\langle j'_z|F_{fil} = F_{j'}. \quad (1)$$

This implies that the filtering followed by the Z-basis measurement is, as a whole, equivalent to the measurement $\mathcal{M}_{B92}$. Hence in the reduced protocol Alice simply sends $|\varphi_0\rangle$ and $|\varphi_1\rangle$ randomly, and Bob performs $\mathcal{M}_{B92}$ on all of the received qubits, which completes the reduction to B92.

The estimation in step (5) can be done as follows. The number of bit errors n_{bit} could be determined if Alice and Bob exchange their measurement results in the Z basis. But this is the same process as the one performed on the first N pairs to obtain n_{err}, due to relation (1). Thanks to the random permutation in step (2), the check pairs are regarded as a classical random sample from the $2N$ pairs. Then, from a classical probability estimate, we may assume

$$|n_{bit} - n_{err}| \le N\epsilon_1. \quad (2)$$

For any strategy by Eve, the probability of violating this inequality is asymptotically less than $\exp(-N\epsilon_1^2)$.

The estimation of the phase errors is far more complicated. To do this, we derive several inequalities by assuming gedanken measurements that are not really done in the *Protocol 1*. The number of phase errors n_{ph} could be determined if Alice and Bob measure the n_{fil} pairs in the X basis just after step (4). Since the filtering operator F_{fil} is also diagonal in the X basis, n_{fil} and n_{ph} could also be determined by another measurement scheme, in which Alice and Bob perform X-basis measurements first, and then Bob applies the filtering F_{fil}. Note that this filtering can be done classically by Bernoulli trials since the outcomes of the X-basis measurements are available. This new scheme also produces the numbers $n_{ij}(i, j = 0, 1)$ of pairs found in state $|i_x\rangle_A|j_x\rangle_B$. Since n_{ij} and n_{fil} (n_{ph}) are related by Bernoulli trials, we have

$$|\alpha^2(n_{00} + n_{10}) + \beta^2(n_{01} + n_{11}) - n_{fil}| \le N\epsilon_2, \quad (3)$$

$$|\alpha^2 n_{10} + \beta^2 n_{01} - n_{ph}| \le N\epsilon_3, \quad (4)$$

which are violated with probability asymptotically less than $\exp(-2N\epsilon_2^2)$ and $\exp(-2N\epsilon_3^2)$, respectively.

Next, recall the fact that neither the noisy channel nor Eve can touch the qubits held by Alice. This implies that the marginal state of Alice's data qubits before the measurements should be $\rho_A^{\otimes N}$, where $\rho_A \equiv \mathrm{Tr}_B(|\Psi\rangle_{AB}\langle\Psi|) = \beta^2|0_x\rangle_A\langle 0_x| + \alpha^2|1_x\rangle_A\langle 1_x|$. We can thus regard $n_{10} + n_{11}$ as a result of a Bernoulli trial, obtaining

$$|\alpha^2 N - (n_{10} + n_{11})| \le N\epsilon_4 \quad (5)$$

with probability of violation asymptotically less than $\exp(-2N\epsilon_4^2)$.

Let us switch to the measurement on the check pairs (the first N pairs). The element of POVM corresponding to the error in step (3) is given by $\Pi_{err} = (|\Gamma_{11}\rangle\langle\Gamma_{11}| + |\Gamma_{01}\rangle\langle\Gamma_{01}|)/2$, where $|\Gamma_{11}\rangle \equiv \alpha|0_x\rangle_A|0_x\rangle_B - \beta|1_x\rangle_A|1_x\rangle_B$ and $|\Gamma_{01}\rangle \equiv \beta|0_x\rangle_A|1_x\rangle_B - \alpha|1_x\rangle_A|0_x\rangle_B$. This is readily derived from the relation $\sqrt{2}|j_z\rangle_A|\overline{\varphi}_j\rangle_B = |\Gamma_{11}\rangle - (-1)^j|\Gamma_{01}\rangle$. Let us add two more states, $|\Gamma_{00}\rangle \equiv \beta|0_x\rangle_A|0_x\rangle_B + \alpha|1_x\rangle_A|1_x\rangle_B$ and $|\Gamma_{10}\rangle \equiv \alpha|0_x\rangle_A|1_x\rangle_B + \beta|1_x\rangle_A|0_x\rangle_B$, to form a basis. While n_{err} is determined from local measurements in step (3), the same outcome could be obtained by performing globally the complete measurement on the basis $\{|\Gamma_{ij}\rangle\}$, followed by a Bernoulli trial with probability 1/2. Let m_{ij} be the number of pairs found in $|\Gamma_{ij}\rangle$. Then we have

$$|(m_{11} + m_{01})/2 - n_{\rm err}| \leq N\epsilon_5, \quad (6)$$

which is violated with probability asymptotically less than $\exp(-2N\epsilon_5^2)$.

Since $\{|\Gamma_{01}\rangle, |\Gamma_{10}\rangle\}$ and $\{|0_x\rangle_{\rm A}|1_x\rangle_{\rm B}, |1_x\rangle_{\rm A}|0_x\rangle_{\rm B}\}$ span the same subspace, we can relate $m_{10} + m_{01}$ and $n_{10} + n_{01}$ by the classical probability estimate as in Eq. (2):

$$|(m_{10} + m_{01}) - (n_{10} + n_{01})| \leq N\epsilon_6, \quad (7)$$

which is violated with probability asymptotically less than $\exp(-N\epsilon_6^2)$. We further relate $m_{01}/(m_{01} + m_{10})$ to $n_{01}/(n_{01} + n_{10})$, but we can no longer apply classical arguments here, since $|\Gamma_{01}\rangle$ and $|0_x\rangle_{\rm A}|1_x\rangle_{\rm B}$ are nonorthogonal. We thus extend the classical probability estimate to the quantum case in the following.

The problem to be considered is as follows: $M = M_0 + M_1$ qubits are prepared in a state, and the positions of qubits are then randomly permuted. Then, each of the first M_0 qubits is measured on an orthogonal basis $\{|0, 0\rangle, |0, 1\rangle\}$, and the rest of the M_1 qubits are measured on another basis $\{|1, 0\rangle, |1, 1\rangle\}$. What we ask is the bound for the probability $p(\delta_0, \delta_1)$, with which $M_0\delta_0$ qubits are found to be in $|0, 1\rangle$ and $M_1\delta_1$ qubits are found to be in $|1, 1\rangle$. Let ρ be the state after the permutation, and $|\chi\rangle \equiv \bigotimes_{b,j} |b, j\rangle^{\otimes n_{b,j}}$, where $n_{b,1} = M_b\delta_b$ and $n_{b,0} = M_b(1 - \delta_b)$. Then, the probability is given by

$$p(\delta_0, \delta_1) = \langle\chi|\rho|\chi\rangle \prod_{b=0,1} \frac{M_b!}{n_{b,0}!n_{b,1}!} \quad (8)$$

The technique used [12] for problems involving independently and identically distributed quantum sources is also useful here, although in our case the state ρ may be highly correlated. The Hilbert space for the M qubits, $\mathcal{H}^{\otimes M}$, can be decomposed as $\mathcal{H}^{\otimes M} \cong \bigoplus_\lambda \mathcal{U}_\lambda \otimes \mathcal{V}_\lambda$ such that any operator of the form $U^{\otimes M}$ with $U \in {\rm SU}(2)$ is decomposed as $U^{\otimes M} \cong \bigoplus_\lambda \pi_\lambda(U) \otimes \mathbf{1}$, and any unitary operator S_p corresponding to permutation $p \in S_M$ is decomposed as $S_p \cong \bigoplus_\lambda \mathbf{1} \otimes \tilde{\pi}_\lambda(p)$. Here the maps π_λ and $\tilde{\pi}_\lambda$ are irreducible representations of SU(2) and S_M, respectively. The index λ runs over all Young diagrams with two rows and M boxes, namely, $\lambda = (M - k, k)$ with $k = 0, 1, \ldots, \lfloor M/2 \rfloor$. We thus use k instead of λ below. For later use, we derive a convenient form of the projection P_k onto $\mathcal{U}_k \otimes \mathcal{V}_k$. Let us parametrize the pure states of a qubit as $|\mathbf{n}\rangle$, using the unit vector $\mathbf{n}$ in the Bloch sphere. Define a state on $\mathcal{H}^{\otimes M}$ as $|k, \mathbf{n}\rangle \equiv |\Psi\rangle^{\otimes k}|\mathbf{n}\rangle^{\otimes M-2k}$, where $|\Psi\rangle$ is the singlet state $(|0\rangle|1\rangle - |1\rangle|0\rangle)/\sqrt{2}$ of two qubits. The state $|k, \mathbf{n}\rangle$ is contained in subspace $\mathcal{U}_k \otimes \mathcal{V}_k$. Consider the operator with unit trace

$$\frac{1}{4\pi M!}\sum_p \int d\mathbf{n} S_p|k, \mathbf{n}\rangle\langle k, \mathbf{n}|S_p^\dagger. \quad (9)$$

Since it commutes with any S_p and any $U \in {\rm SU}(2)$, it should be equal to $(d_k^{\mathcal{U}}d_k^{\mathcal{V}})^{-1}P_k$, where $d_k^{\mathcal{U}} \equiv \dim\mathcal{U}_k$ and $d_k^{\mathcal{V}} \equiv \dim\mathcal{V}_k$.

Since ρ commutes with any S_p, it can be decomposed as $\rho \cong \bigoplus_k (p_k/d_k^{\mathcal{V}})\rho_k \otimes \mathbf{1}$, where $\sum p_k = 1$ and ${\rm Tr}\rho_k = 1$. Then, $\langle\chi|\rho|\chi\rangle \leq \sum_k (p_k/d_k^{\mathcal{V}})\langle\chi|P_k|\chi\rangle$. Substituting the form of (9) for P_k, we have

$$\langle\chi|\rho|\chi\rangle \leq \max_{k,\mathbf{n}} \frac{d_k^{\mathcal{U}}}{M!}\sum_p |\langle\chi|S_p|k, \mathbf{n}\rangle|^2. \quad (10)$$

Recall that $|\chi\rangle$ takes the form of $|\chi\rangle = \bigotimes_\nu |\nu\rangle^{\otimes n_\nu}$, where ν represents the double index (b, j). Then, $|\langle\chi|S_p|k, \mathbf{n}\rangle|^2$ becomes the product of $(S_{\nu\nu'})^{s_{\nu\nu'}}$ and $(T_\nu)^{t_\nu}$, where $S_{\nu\nu'} \equiv |\langle\nu|\langle\nu'||\Psi\rangle|^2$ and $T_\nu \equiv |\langle\nu|\mathbf{n}\rangle|^2$. The numbers $s_{\nu\nu'}$ and t_ν depend on the permutation p. Let $\mu(\{s_{\nu\nu'}\}, \{t_\nu\})$ be the number of different permutations that give the same values of $\{s_{\nu\nu'}\}, \{t_\nu\}$. Explicitly, this degeneracy factor is given by $\mu = (\prod_\nu n_\nu!)k!(M - 2k)!/(\prod_{\nu,\nu'} s_{\nu\nu'}!\prod_\nu t_\nu!)$. Using this factor, the summation over p can be replaced by the summation over $\{s_{\nu\nu'}\}, \{t_\nu\}$, which take at most poly(M) values. Since $d_k^{\mathcal{U}} = M - 2k + 1$ is also poly(M), we obtain $\langle\chi|\rho|\chi\rangle \leq {\rm poly}(M)\max_{k,\mathbf{n},\{s_{\nu\nu'}\},\{t_\nu\}}(\mu/M!)\prod_{\nu,\nu'}(S_{\nu\nu'})^{s_{\nu\nu'}} \times \prod_\nu (T_\nu)^{t_\nu}$. Combining this inequality and Eq. (8), and replacing the factorials by the entropy function $H(p_i) \equiv -\sum_i p_i \log_2 p_i$ using the formula ${\rm poly}(N)^{-1} \leq 2^{-NH(p_i)}N!/\prod(Np_i)! \leq 1$, we can cast the upper bound into the form $p(\delta_0, \delta_1) \leq {\rm poly}(M)2^{-M\min R}$, where the exponent R is given by

$$\begin{aligned} R = H(M_b/M) &+ (k/M)[D(s_{\nu\nu'}/k|S_{\nu\nu'}/4) - 2] \\ &+ (1 - 2k/M)[D(t_\nu/(M - 2k)|T_\nu/2) - 1], \end{aligned} \quad (11)$$

where D is the relative entropy defined by $D(p_i|q_i) = \sum_i p_i \log_2(p_i/q_i)$. The empirical probability $p_{bj} \equiv t_\nu/(M - 2k)$ appearing here can be regarded as a joint probability over the two variables b and j, and we can consider its marginal probability $p_j \equiv p_{0j} + p_{1j}$ and the conditional probability $p_{b|j} \equiv p_{bj}/p_j$. We use similar notations for other joint probabilities $q_{bb'jj'} \equiv s_{\nu\nu'}/k$, $\alpha_{bj} \equiv T_\nu/2$, and $\beta_{bb'jj'} \equiv S_{\nu\nu'}/4$. We further introduce a variable a, which takes three values $\{1, 2, 3\}$, define a probability ξ_a by $\xi_1 = 1 - 2k/M$ and $\xi_2 = \xi_3 = k/M$, and define a joint probability γ_{ab} over a and b, defined by $\gamma_{1b} = \xi_1 p_b$, $\gamma_{2b} = \xi_2 q_b$, and $\gamma_{3b'} = \xi_3 q_{b'}$. Then, it is a bit tedious but straightforward to rewrite Eq. (11) as

$$\begin{aligned} R = (k/M)[D(q_{bb'}|q_b q_{b'}) &+ \sum_{bb'} q_{bb'} D(q_{jj'|bb'}|\beta_{jj'|bb'})] \\ &+ (1 - 2k/M)\sum_b p_b D(p_{j|b}|\alpha_{j|b}) + D(\gamma_{ab}|\gamma_a\gamma_b), \end{aligned} \quad (12)$$

where we have used $\gamma_b = M_b/M$, $\alpha_b = 1/2$ and $\beta_{bb'} = 1/4$. Since all terms are non-negative, R is zero only if each pair of probabilities in D is identical. This implies $p_{bj} = |\langle b, j|\mathbf{n}\rangle|^2(M_b/M)$, $q_{bj} = (1/2)(M_b/M)$, and $q_{b'j'} = (1/2)(M_{b'}/M)$. From the relation $n_{b,j} = M(\xi_1 p_{bj} + \xi_2 q_{bj} + \xi_3 q_{b'j'}|_{b'=b,j'=j})$ we conclude that, for $\min R$ to be zero, it is necessary that

$$\delta_b = \xi_1 |\langle b, 1|\mathbf{n}\rangle|^2 + (1 - \xi_1)/2 \tag{13}$$

for a choice of $|\mathbf{n}\rangle$ and $0 \leq \xi_1 \leq 1$, or equivalently, $\delta_b = \langle b, 1|\sigma|b, 1\rangle$ for a state σ of a single qubit. Otherwise, $p(\delta_0, \delta_1)$ is as exponentially small as $2^{-M\min R}$. Note that in the limit of $M \to \infty$, the result is consistent with what is expected from the quantum de Finetti theorem [13].

Now applying this general result to our case, we have

$$\sin^2(\theta_l - \theta) - \epsilon_7 \leq \sin^2\phi_l \leq \sin^2(\theta_l + \theta) + \epsilon_8 \tag{14}$$

for $l = 0, 1$, where all the angles are defined in $[0, \pi/2]$ by the relations $n_{11}/(n_{11} + n_{00}) = \sin^2\theta_0$, $n_{01}/(n_{01} + n_{10}) = \sin^2\theta_1$, $m_{11}/(m_{11} + m_{00}) = \sin^2\phi_0$, $m_{01}/(m_{01} + m_{10}) = \sin^2\phi_1$, and $\alpha^2 = \sin^2\theta$. Together with Eqs. (3)–(7), an exponentially reliable upper bound of $n_{\rm ph}$ can be found.

In the following, we calculate the final key length in the limit of large N, by setting all ϵ_j to be zero. From Eq. (2), $n_{\rm bit}$ is found to be equal to $n_{\rm err}$. Equations (3)–(7) are now linear equations, and together with the relation $\sum n_{ij} = \sum m_{ij} = N$, they can be used to eliminate n_{ij} and m_{ij}. Then, the inequalities (14) for $l = 0, 1$ are combined to give

$$|n_{\rm fil} - 2n_{\rm err}| \leq N\alpha\beta f(x), \tag{15}$$

where $f(x) \equiv \sqrt{x^2 - \Delta^2} + \sqrt{(1-x)^2 - (\beta^2 - \alpha^2 - \Delta)^2}$ with $\Delta \equiv (n_{\rm fil}/N - 2\alpha^2\beta^2)/(\beta^2 - \alpha^2)$ and $x \equiv 2n_{\rm ph}/N - (\beta^2 - \alpha^2)\Delta$. The positivity of n_{ij} requires that $|\Delta| \leq x \leq 1 - |\beta^2 - \alpha^2 - \Delta|$. Solving Eq. (15) gives an upper bound $\overline{n}_{\rm ph}$ on the number of phase errors $n_{\rm ph}$, as a function of the observed values $n_{\rm err}$ and $n_{\rm fil}$.

The achievable length of the final key is given [8,14] by $n_{\rm key} = n_{\rm fil}[1 - h(n_{\rm bit}/n_{\rm fil}) - h(\overline{n}_{\rm ph}/n_{\rm fil})]$, when $\overline{n}_{\rm ph}/n_{\rm fil} \leq 1/2$ [note that positions of errors are randomized in step (2)]. Here $h(p) \equiv H(p, 1-p)$. In order to show a quantitative example of the security, we assume that the channel is the depolarizing channel where the state ρ evolves as $\rho \to (1-p)\rho + p/3\sum_{a=x,y,z}\sigma_a\rho\sigma_a$, where σ_a is the Pauli operator for component a. In Fig. 1(a), we plot the key generation rate $G = n_{\rm key}/N$ optimized over the nonorthogonality $|\langle\varphi_0|\varphi_1\rangle|^2$. It is seen that our protocol is secure up to $p \sim 0.034$, which is smaller than in BB84 with one-way EDP ($p \sim 0.165$) [6]. In Fig. 1(b), it can be seen that when $|\langle\varphi_0|\varphi_1\rangle|^2$ becomes smaller, the estimation of the phase errors becomes poorer. On the other hand, larger values of $|\langle\varphi_0|\varphi_1\rangle|^2$ make the signal more vulnerable to noise, resulting in larger errors. This trade-off is in contrast to BB84, in which a good estimation and small errors are achieved at the same time by adding two more states in the protocol.

In summary, the B92 protocol can be regarded as an EDP with a filtering process, and the filtering makes the phase and bit errors related to each other, which enables us to estimate the phase errors from the amount of the bit errors. The estimation scheme involving nonorthogonal measurements developed here will also be useful in practical QKD schemes having lower symmetries due to imperfections in the apparatus.

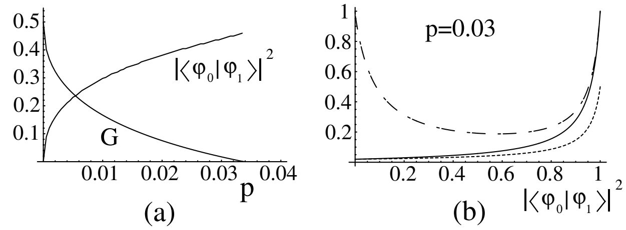

FIG. 1. (a) The optimum value of $|\langle\varphi_0|\varphi_1\rangle|^2$ and the key generation rate G in the depolarizing channel. (b) The error rates (normalized by $n_{\rm fil}$) in the data qubits for the depolarizing channel with $p = 0.03$. The estimated upper bound for phase errors (dot-dashed line), the actual phase errors (solid line), and the bit errors (dotted line).

We thank Hoi-Kwong Lo, John Preskill, and Takashi Yamamoto for helpful discussions.

[1] C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).
[2] D. Mayers, Lect. Notes Comput. Sci. **1109**, 343–357 (1996).
[3] C. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India* (IEEE, New York, 1984), pp. 175–179.
[4] E. Biham, M. Boyer, P. O. Boykin, T. Mor, and V. Roychowdhury, quant-ph/9912053; H. Inamori, N. Lütkenhaus, and D. Mayers, quant-ph/0107017; M. Koashi and J. Preskill, quant-ph/0208155.
[5] H.-K. Lo and H. F. Chau, Science **283**, 2050 (1999).
[6] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).
[7] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, Phys. Rev. A **54**, 3824 (1996).
[8] A. R. Calderbank and P. W. Shor, Phys. Rev. A **54**, 1098 (1996); A. M. Steane, Proc. R. Soc. London A **452**, 2551 (1996).
[9] Z. Quan and T. Chaojing, Phys. Rev. A **65**, 062301 (2002).
[10] N. Gisin, Phys. Lett. A **210**, 151 (1996); M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Rev. Lett. **78**, 574 (1997).
[11] C. H. Bennett, H. J. Bernstein, S. Popescu, and B. Schumacher, Phys. Rev. A **53**, 2046 (1996).
[12] M. Keyl and R. F. Werner, Phys. Rev. A **64**, 052311 (2001); M. Hayashi and K. Matsumoto, Phys. Rev. A **66**, 022311 (2002).
[13] C. M. Caves, C. A. Fuchs, and R. Schack, quant-ph/0104088.
[14] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, quant-ph/0212066.