Quantum-classical complexity-security tradeoff in secure multiparty computations

H. F. Chau*
Department of Physics, University of Hong Kong, Pokfulam Road, Hong Kong
(Received 31 December 1998; published 16 February 2000)

I construct a secure multiparty scheme to compute a classical function by a succinct use of a specially designed fault-tolerant random polynomial quantum error correction code. This scheme is secure provided that (asymptotically) strictly more than five-sixths of the players are honest. Moreover, the security of this scheme follows directly from the theory of quantum error correcting code, and hence is valid without any computational assumption. I also discuss the quantum-classical complexity-security tradeoff in secure multiparty computation schemes and argue why a full-blown quantum code is necessary in my scheme.

PACS number(s): 03.67.Dd, 03.67.Hk, 03.67.Lx, 89.70.+c

I. INTRODUCTION

Quantum computers are more powerful than classical computers in a number of applications such as integer factorization [1], database search [2] and secret key distribution [3,4]. In addition, careful use of entanglement reduces the multiparty communication complexity of certain functions [5] and allows secret sharing [6]. On the other hand, certain postmodern cryptographic applications, including bit commitment [7] and ideal two-party secure computation [8], are impossible if the cheater has a quantum computer. Thus, it is important to investigate the power and limitation of quantum computers. Moreover, the quantum versus classical and security versus complexity tradeoffs for certain multiparty computational tasks deserve in-depth study.

In this paper, I analyze the quantum versus classical and security versus complexity tradeoffs in secure multiparty computation. In secure multiparty computation, n players each with a private classical input x_i want to compute a commonly agreed classical function $z=f(x_1,x_2,\ldots,x_n)$ in such a way that (i) all players either know the value of z or abort after detecting a cheater or eavesdropper, (ii) no one can gain information on the private input of an honest player except those logically following z, and (iii) a limited number of cheating players cannot alter the final outcome z. Moreover, the above three conditions hold even if all cheaters and eavesdroppers cooperate.

Secure multiparty computation can be used as a basic building block for a number of extremely useful protocols including secure election and anonymous messages broadcast. Thus, it is important to devise a secure multiparty computation scheme that tolerates as many cheaters as possible on the one hand, and requires as few communications between the players as possible on the other.

Several classical secure multiparty computation schemes exist in the literature. The security of some of these schemes [9] is based on the security of either certain (classical) oblivious transfer or (classical) bit commitment protocols. Hence their methods are insecure if a cheating player has unlimited computational power. Ben-Or *et al.* [10] and Chaum *et al.* [11] independently proposed multiparty computation methods based on a distributed computing version of the so-called (k,n)-secret sharing scheme [12]. Their schemes are unconditionally secure provided that fewer than one-third of the players cheat. This is true even when the cheaters cooperate. The one-third cheating player bound is tight among all classical protocols that allow secret communications between any two players [10]. Later Rabin and Ben-Or showed that if each player can broadcast a message to all other players and each pair of players can communicate secretly, then there is an unconditionally secure way to compute z fewer if less than one-half of the players cheat [13]. The one-half cheating player bound is tight among all classical schemes that allow secret communications between any two players as well as in public broadcasting [13].

How many resources are required in classical conditionally secure multiparty computation? In all classical schemes known to date, the n players must communicate securely with others. Hence, $n(n-1)/2$ classical secure communication channels are required. Suppose each player has a private input of length k, then initially they have to distribute their private inputs via certain secret sharing schemes. To do so, each player has to send out $O(nk)$ bits. Thus, $O(n^2k)$ bits of (secret) classical communication are necessary for the initial setup in the whole system. To perform distributed computation, up to $O(n^2k)$ bits of (secret) communication and computation per arithmetical operation are required [10,13]. In addition, to verify that every player's secret input is correctly distributed in the secret sharing scheme, an extra $O(n^3k)$ bits of communications are needed [10,11,13]. Since the number of secret communication channels scales quadratically with the number of players, classical secure multiparty computation is rarely used in practice for more than, say, ten players [14]. In fact, the classical schemes by Ben-Or *et al.* and Chaum *et al.*, being generic, are designed primarily to point out the plausibility of secure multiparty computation.

II. QUANTUM SECURE MULTIPARTY COMPUTATION SCHEME

Now, let me report a quantum secure multiparty computation scheme that requires fewer communication channels and resources at the expense of tolerating fewer cheaters. Without lost of generality, I may assume that the private input for each player as well as the output of the function f

*Electronic address: hfchau@hkusua.hku.hk

are chosen from a finite field $\mathbb{F}_q$ for some prime q. My scheme goes as follows

(1) All players agree on a common computational basis for quantum computation, an exponentially small security parameter $e>0$, as well as two random polynomial quantum error correcting codes (QECC's) C_1 and C_2 [15]. In particular, they choose C_1 to be the $[[n,1,d]]_q$ code where the prime $q>n$, and $3d\leqslant n+2$. More precisely, C_1 encodes each $q$ary quantum register $|a_0\rangle$ into n $q$ary quantum registers $\Sigma_{a_1,a_2,\ldots,a_{d-1}=0}^{q-1}\otimes_{i=1}^{n}|a_0+a_1y_i+a_2y_i^2+\cdots+a_{d-1}y_i^{d-1}\rangle/q^{(d-1)/2}$ where y_i are distinct nonzero elements in $\mathbb{F}_q$. The distance of this code is d and hence it can correct up to $\delta\equiv[(d-1)/2]$ errors.[1] Furthermore, I denote the $[[n,1,d]]_q$ QECC $|a_0\rangle\mapsto\Sigma_{a_1,a_2,\ldots,a_{n-d+1}=0}^{q-1}\otimes_{i=1}^{n}|a_0+a_1y_i+a_2y_i^2+\cdots+a_{n-d+1}y_i^{n-d+1}\rangle/q^{(n-d+1)/2}$ by $\tilde{C}_1$. In addition, C_2 is chosen to be the $[[4d'+1,1,2d'+1]]_q$ random polynomial QECC [15] whose fidelity of quantum computation using imperfect devices is greater than $1-e$. (Since the random polynomial QECC C_2 has a fault-tolerant implementation [15], by concatenate coding, the threshold theorem in fault-tolerant quantum computation guarantees the existence of such a QECC C_2 [15–17].) As we shall see later on, the choice of the value of the distance d affects only the number of cheaters that can be tolerated by the scheme.

(2) Each player sets up a quantum channel with a central routing station. He or she may establish relay stations along each quantum channel in such a way that the noise level in each quantum channel segment is small enough to perform entanglement purification. (See Refs. [18–20] for details.) Furthermore, each player also has access to a classical public unjammable channel for broadcasting.

(3) The players, central routing channel and relay stations separately prepare a few copies of the state $|\Phi\rangle\equiv\Sigma_{k=0}^{q-1}|kk\rangle/\sqrt{q}$. They encode each copy using QECC C_2, and share these encoded states $|\Phi\rangle$ between the two ends of each quantum communication channel segment. Then, they perform a fault-tolerant entanglement purification procedure as discussed in Refs. [19,20] on these shared states. Next, these possibly impure encoded states $|\Phi\rangle$ shared between each channel segment from one player to another are connected together by quantum teleportation [4,18,21]. Finally, each pair of players tests the purity of their shared encoded states $|\Phi\rangle$ by a variation of the fault-tolerant random hashing technique described in Ref. [4]. (Readers may refer to Appendixes A and B for detailed descriptions of the teleportation and random hashing procedures, respectively.) They proceed to step (4) only if the random hashing test is passed for each pair of players. In this case, each pair of players will share a number of almost perfect encoded logical states $|\Phi\rangle$. The entanglement shared between each pair of players in this way can then be used to securely transport states among themselves in step (4). Clearly, shared $|\Phi\rangle$ is not the only possible way to establish such an entanglement. In fact, one may replace the state $|\Phi\rangle$ in this scheme by an Einstein-Podolsky-Rosen (EPR) pair. Nevertheless, the scheme will become slightly complicated after such a replacement for one has to teleport $q$ary instead of binary quantum registers in step (4).

(4) Let x_i be the private classical input of player i; then he or she prepares $s=O(\log(1/e))$ copies of the state $|x_i\rangle$. He or she also prepares a number of preset quantum registers $|0\rangle$ that will be used later on in the reversible quantum computation. Player i first encodes each of his or her prepared quantum registers using the QECC C_1. Then, player i further encodes the jth quantum register in each of his or her encoded states using C_2 and teleports the resultant quantum registers to player j using their previously shared encoded state $|\Phi\rangle$ from step (3) for all $j\neq i$. He or she also encodes each of the ith quantum registers by C_2 and keeps those quantum registers himself or herself. All players keep their received quantum registers private as well. In what follows, I use the subscript ''L'' to the state ket to denote a state that is encoded and distributed among the n players using this procedure. In addition, the players also prepare a number of preset quantum registers $|0\rangle$, encode it first by $\tilde{C}_1$, and then by C_2. The players then distribute these encoded preset registers among themselves in a similar way as in sharing their private inputs. I use the subscript ''$\tilde{\text{L}}$'' to the state ket to denote such an encoded and distributed state. States $|0\rangle_{\text{L}}$ and $|0\rangle_{\tilde{\text{L}}}$ will be used as preset registers during the reversible computation in step (6).

(5) In order to make sure that everyone follows step (4) honestly, a player j (the verifier) may challenge a randomly chosen player i (the prover) using a fault-tolerant random parity check method similar to that used in Ref. [4]. More precisely, player j publicly announces a sequence $\{c_k\}_{k=1}^{s}$ of integers in $\mathbb{F}_q$ such that $\Sigma_{k=1}^{s}c_k=0$. Then every player is required to help player j to compute the random parity $\Sigma_{k=1}^{s}c_kx_{ik}$ by distributed fault-tolerant quantum computation (FTQC), where x_{ik} denotes the state of the kth copy of the private input of player i. Clearly, the choice of QECC's C_1 and C_2 enables us to perform the above quantum computation in a fault-tolerant way *without* any measurement and ancilla [15]. Also, the method of distributing the private input state in step (4) allows the players to perform the above FTQC in a distributed manner *without* any communication between them.

To verify if the result computed (which I call the random parity) is equal to zero, all players measure and publicly announce their measurement outcome along their commonly agreed computational basis on their corresponding C_2 encoded quantum registers that encode the random parity. Because C_1 is an $[[n,1,d]]_q$ random polynomial QECC, the measurement results of the players correspond to the classical $[n,d,n-d+1]_q$ Reed-Solomon encoding of the random parity. Naturally, they continue only if the random parity inferred from this classical Reed-Solomon encoding is zero. This verification process has to repeat $O(\log(1/e))$ times for each proving player i so as to guarantee security.

In addition, all players use a similar distributed fault-

[1]The distance of this code is less than that reported in Ref. [15]. Nonetheless, I still call this a random polynomial code because this code closely resembles that reported in Ref. [15].

tolerant random parity checking technique to verify the purity of the distributed encoded preset quantum registers $|0\rangle_{\mathrm{L}}$ and $|0\rangle_{\tilde{\mathrm{L}}}$ among themselves. They proceed to step (6) only when all the measurement results are consistent with the assumption that there is no cheater or eavesdropper around. Thus, in order to establish the required security, $O(\log(1/e))$ private input states prepared and distributed in step (4) are wasted. (An alternative way to perform the random parity check measurement is to ask the players to teleport their shares of the encoded random parity quantum registers to the verifier. Then the verifier makes the appropriate measurement and publicly announces the outcome.)

(6) To compute the commonly agreed classical function $z=f(x_1,x_2,\ldots,x_n)$, the n players perform distributed FTQC on their received quantum particles. The players keep every quantum state private except the final result.

To be precise, they first decompose the classical function f into a commonly agreed composition of elementary operators. Each elementary operator is in the form of (i) registerwise addition $|x\rangle\mapsto|x+a\rangle$, (ii) registerwise multiplication $|x\rangle\mapsto|ax\rangle$, (iii) generalized controlled - NOT gate (C-NOT) $|x,y\rangle\mapsto|x,x+y\rangle$, and (iv) generalized Toffoli gate $|x,y,z\rangle\mapsto|x,y,z+xy\rangle$, for some fixed $a\neq 0$ [22].

At this point, each player should have $r=O(\log(1/e))<s$ remaining quantum registers distributed among themselves. Moreover, all the remaining distributed quantum states of an honest player, upon quantum error correction, should be identical. Clearly, the choice of the random polynomial QECC's C_1 and C_2 together with the private secure distribution method in step (4) allow, the players to perform the first three types of elementary operators without any measurement or communication between the players [15]. Thus, they can perform the fault-tolerant operation on the r remaining distributed quantum registers one by one. In this way, they end up with r identical resultant states if they are honest.

To perform the fourth type of elementary operator, namely, a generalized Toffoli gate on the r remaining distributed encoded states, the players do the following. First, they collectively synthesize the distributed state $\Sigma_{a,b=0}^{q-1}|a,b,ab\rangle_{\mathrm{L}}/q^{3/2}$ among themselves using their verified distributed states $|0\rangle_{\tilde{\mathrm{L}}}$ by a procedure based on that in Ref. [17] as follows:

$$|0,0,0,0\rangle_{\tilde{\mathrm{L}}}$$

$$\mapsto\frac{1}{q^2}\sum_{a,b,c,k=0}^{q-1}|a,b,c,k\rangle_{\mathrm{L}} \tag{1a}$$

$$\mapsto\frac{1}{q^2}\sum_{a,b,c,k=0}^{q-1}\omega_q^{-kc}|a,b,c,k\rangle_{\mathrm{L}} \tag{1b}$$

$$\mapsto\frac{1}{q^2}\sum_{a,b,c,k=0}^{q-1}\omega_q^{k(ab-c)}|a,b,c,k\rangle_{\mathrm{L}} \tag{1c}$$

$$\mapsto\frac{1}{q^{5/2}}\sum_{a,b,c,k,x=0}^{q-1}\omega_q^{k(ab-c+x)}|a,b,c\rangle_{\mathrm{L}}\otimes|x\rangle_{\tilde{\mathrm{L}}}, \tag{1d}$$

where ω_q is a primitive qth root of unity.

To arrive at Eq. (1a) in a fault-tolerant manner, each player i simply has to perform the local Fourier transformation $|a\rangle\mapsto\Sigma_{b=0}^{q-1}\omega_q^{m_iab}|b\rangle/\sqrt{q}$ on his or her corresponding quantum registers, where $m_i\in\mathbb{F}_q$ is a unique solution for the system of equations $\Sigma_{i=1}^{n}m_i=1$ and $\Sigma_{i=1}^{n}m_iy_i=\Sigma_{i=1}^{n}m_iy_i^2=\cdots=\Sigma_{i=1}^{n}m_iy_i^{n-1}=0$. I denote this fault-tolerant transformation by $\mathfrak{F}$. In fact, Appendix C shows that $\mathfrak{F}|0\rangle_{\mathrm{L}}=\Sigma_{k=0}^{q-1}|k\rangle_{\tilde{\mathrm{L}}}$ and $\mathfrak{F}|0\rangle_{\tilde{\mathrm{L}}}=\Sigma_{k=0}^{q-1}|k\rangle_{\mathrm{L}}$. Then Aharonov and Ben-Or tell us how to arrive at Eqs. (1b) by fault-tolerant controlled-phase-shift gate *without* any communication between the players [15]. More precisely, each player i applies $|a,b\rangle\mapsto\omega_q^{p_iab}|a,b\rangle$ to their share of the third and fourth quantum registers where $p_i\in\mathbb{F}_q$ satisfies $\Sigma_{i=1}^{n}p_i=-1$ and $\Sigma_{i=1}^{n}p_iy_i=\Sigma_{i=1}^{n}p_iy_i^2=\cdots=\Sigma_{i=1}^{n}p_iy_i^{2d}=0$. Subsequently, arriving at Eq. (1c) from Eq. (1b) requires the fault-tolerant controlled-controlled-phase-shift gate $|a,b,c\rangle_{\mathrm{L}}\mapsto\omega_q^{abc}|a,b,c\rangle_{\mathrm{L}}$. For the random polynomial code C_1 with $3d\leqslant n+2$, this operation is achieved when each player i applies the controlled-controlled-phase-shift gate $|a,b,c\rangle\mapsto\omega_q^{r_iabc}|a,b,c\rangle$ to his or her corresponding share of the encoded first, second, and third quantum registers, where $r_i\in\mathbb{F}_q$ is the solution (not necessarily unique unless $3d+1=n$) of the system of equations $\Sigma_{i=1}^{n}r_i=1$ and $\Sigma_{i=1}^{n}r_iy_i=\Sigma_{i=1}^{n}r_iy_i^2=\cdots=\Sigma_{i=1}^{n}r_iy_i^{3d}=0$. Finally, to arrive at Eq. (1d) from Eq. (1c) in a fault-tolerant way, the players simply apply the same local Fourier transform $\mathfrak{F}$ that creates Eq. (1a) to their share of the fourth quantum register. (Again, the proof can be found in Appendix C.) In summary, the players can evolve their share of quantum states to Eq. (1d) in a fault-tolerant manner *without* any measurement, communications or the use of ancillary particles.

After the players have evolved their quantum particles to the distributed state in Eq. (1d), they measure their share of the fourth encoded quantum register along the commonly agreed computational basis and then publicly announce their measurement results. In this way, they end up having a classical $[n,n-d+1,d]_q$ Reed-Solomon code and after error correction, they can infer the measurement outcome of the fourth encoded quantum register along the commonly agreed computational basis. Suppose the inferred measurement result is λ, then the state ket of the remaining three distributed encoded quantum registers becomes $\Sigma_{a,b,c,k=0}^{q-1}\omega_q^{k(ab-c+\lambda)}|a,b,c\rangle_{\mathrm{L}}/q^2=\Sigma_{a,b=0}^{q-1}|a,b,ab+\lambda\rangle_{\mathrm{L}}/q$. So, by applying a fault-tolerant generalized C-NOT gate depending on the measurement result λ, they eventually synthesize the state $\Sigma_{a,b=0}^{q-1}|a,b,ab\rangle_{\mathrm{L}}/q$ collectively.

At this point, using their newly synthesized distributed encoded state $\Sigma_{a,b=0}^{q-1}|a,b,ab\rangle_{\mathrm{L}}/q$ as ancilla, the n players implement the generalized Toffoli gate in a fault-tolerant manner using a variation of Gottesman's method in Ref. [23]. (See also Ref. [17] for details.) More precisely, they perform the following transformation using a number of fault-tolerant generalized C-NOT gates and a fault-tolerant $\mathfrak{F}$ gate:

$$\frac{1}{q^2}\sum_{a,b,c=0}^{q-1}|x,y,z,a,b,ab\rangle_{\mathrm{L}}$$

$$\mapsto\frac{1}{q^{3/2}}\sum_{a,b,c=0}^{q-1}\omega_q^{zc}|x-a,y-b\rangle_{\mathrm{L}}\otimes|c\rangle_{\tilde{\mathrm{L}}}\otimes|a,b,z+ab\rangle_{\mathrm{L}}. \tag{2}$$

Now the n players measure their shares of the first three encoded registers along the commonly agreed computational basis. Regarded as classical Reed-Solomon codes, their publicly announced measurement outcomes can then be used to infer the (quantum) measurement results of the first three registers along the commonly agreed computational basis. Suppose the inferred measurement results of the first three registers are λ_1,λ_2, and λ_3, respectively. Then, by adding λ_1 to the fourth register, λ_2 to the fifth register, and $\lambda_1 y+\lambda_2 x-\lambda_1\lambda_2$ to the sixth register, they get the state $\omega_q^{\lambda_3 z}|x,y,z+xy\rangle_{\mathrm{L}}$. Finally, they obtain the state $|x,y,z+xy\rangle_{\mathrm{L}}$, which is the result of a generalized Toffoli operation, by applying a suitable phase-shift gate in the sixth register then followed by another controlled-controlled-phase-shift operator to the first and second registers. (As I have discussed previously, players may perform these operations without any communication because of the choice of the QECC's C_1 and C_2 together with the fact that λ_1,λ_2, and λ_3 are classical data.)

To ensure accuracy, the players perform the above process r times to the r supposedly identical signal states. In this way, they end up by implementing r identical generalized Toffoli operators if all players are honest. [At this point, readers may wonder why I do not check the purity of ancillary state $\Sigma_{a,b=0}^{q-1}|a,b,ab\rangle_{\mathrm{L}}/q$ directly. The reason is that random parity checking does not work for this ancillary state because the state of the untested particles will be altered by the test itself. Readers may also ask why I do not apply the fault-tolerant Fourier transformation gate to obtain $\Sigma_{k=0}^{q-1}|k\rangle_{\mathrm{L}}$ from $|0\rangle_{\mathrm{L}}$. The reason is that all known fault-tolerant Fourier transformation gates for the $[[n,1,d]]_q$ QECC C_1 with $3d\leqslant n+2$ to date require collective measurements on the encoded quantum registers and hence are liable to error in the presence of cheaters. An alternative method to perform the required measurement is to assign once and for all a randomly chosen player for each of the $r=O(\log(1/e))$ supposedly identical signal states. Whenever it comes to a measurement, players teleport their states to be measured to the corresponding assigned player who then makes the necessary measurement and publicly announces the measurement outcome.

(7) In order to make sure that the players indeed follow the distributed FTQC in step (6) honestly, they carry out the random parity verification test $O(\log(1/e))$ times on their final state using the same method as described in step (5). Finally, to obtain the value of $z=f(x_1,x_2,\ldots,x_n)$, the n players separately measure their share of quantum registers that encode the value of z along the commonly agreed computational basis, and then publicly announce their measurement outcomes. They then infer the value of z using standard classical Reed-Solomon code error correction.

III. SECURITY OF THE QUANTUM SCHEME

Now, I claim that the above scheme correctly computes the classical function $z=f(x_1,x_2,\ldots,x_n)$ with a probability $1-\not e$ for some fixed constant $\not\geqslant 1$, provided that no more than δ players cheat. In addition, those $\delta\equiv[(d-1)/2]$ cheaters know nothing about the private inputs of every honest player and they cannot alter the final outcome z. These claims are true even if all cheaters cooperate and have unlimited computational power.

To prove the above claims, one observes that there are four possible ways for the above scheme to go wrong, namely, the presence of noise, bad instruments, eavesdroppers, and cheating players. Remember that a cheater may deliberately announce wrong measurement results and thereby mislead others. One must also make the most pessimistic assumption that all cheaters and eavesdroppers cooperate and control everything except the instruments in the laboratories of the honest players. The cheaters may even have unlimited computational power. Using the argument in Ref. [4], I first show that we can safely neglect the effect of noise and bad instruments. Since all steps in the above scheme are performed in a fault-tolerant manner, the theory of FTQC tells us that with probability $1-e$ we may assume that noise and bad instruments simply affect the error syndromes but not the quantum information encoded in the states [15–17]. The theory of QECC also tells us that learning error syndromes give no information about the quantum information encoded in the state [24,25]. Consequently, by restricting myself to the evolution of quantum information contained in the encoded quantum registers, I may analyze the behavior of the above scheme in a noiseless environment from now on.

Then it remains for me to show that no more than δ cheaters can obtain partial information on the private inputs of some honest players. In addition, these cheaters cannot alter the output of the classical function f. In order to do this, one first has to understand the function of each step in the scheme. Steps (2) and (3) are direct generalizations of the entanglement-based quantum key distribution protocol proposed by Lo and Chau in Ref. [4]. The aim of these two steps is to share the almost perfectly encoded state $|\Phi\rangle$ between any two pairs of players so that they can teleport quantum states in a fault-tolerant manner from one to another at a later time in step (4). Step (5) makes sure that every player follows step (4) to distribute his or her private input as well as the preset quantum registers using the QECC's C_1 and $\tilde{C}_1$. The actual computation is carried out in step (6), and finally, the computational result is varified and measured in step (7).

A. Private inputs of an honest player are secure up to step (5) of the quantum scheme

I have two cases to consider in order to show that the $\delta\equiv[(d-1)/2]$ cheaters obtain no information on the private inputs of the honest players up to the random parity verification in step (5) of the quantum scheme. The first case is when the proving player i in step (5) is honest. In this case, the encoded state $|\Phi\rangle$ sharing scheme in step (3) between the proving player i and all other honest players is a straightfor-

ward generalization of the quantum key distribution protocol of Lo and Chau in Ref. [4]. More important, as stated in Appendix B, the random parity test in step (5) maps the basis $\mathcal{B}=\{\Sigma_{k=0}^{q-1}\omega_q^{kb}|k,k+a\rangle/\sqrt{q}\}_{a,b\in\mathbb{F}_q}$ to basis $\mathcal{B}$ up to a global phase. Therefore the proof of Lo and Chau in Ref. [4] applies. In particular, they have already proved that the fidelity of every encoded state $|\Phi\rangle$ shared between any two honest players is at least $1-e$ even in the presence of eavesdroppers and cheaters [4]. Then in steps (4) and (5), eavesdroppers and cheaters can access only the public classical communications between the honest players. Fortunately, these classical messages contain no information about the teleported quantum state [21]. Hence, no one apart from the sender and the receiver knows the teleported state. Thus, these δ cheaters have access to at most their share of δ quantum registers of the distributed encoded state $|x_i\rangle_{\mathrm{L}}$. Since C_1 is a $[[n,1,d]]_q$ QECC, knowledge of the δ quantum registers in the hands of the cheaters contains no information on the private input x_i at all.

The second case is that the proving player i is dishonest. Clearly, the job of the dishonest player i is to somehow mislead the other players into believing that he or she is honest. More precisely, player i tries to devise a method (possibly with the help of the other $\delta-1$ cheaters in the system) so as to pass the verification test in step (5) with a probability greater than $1-\ell e$ for some fixed positive constant ℓ. Note that measuring every quantum register of an arbitrary quantum codeword of the $[[n,1,d]]_q$ random polynomial QECC C_1 along the commonly agreed computational basis gives a classical $[n,d,n-d+1]_q$ Reed-Solomon codeword. In addition, if the C_1 encoded quantum state $|\Psi\rangle$ contains δ erroneous quantum registers, then after measuring along the computational basis, we end up getting a classical Reed-Solomon codeword with at most δ erroneous registers. Since $\delta<n/4$ [25,26], if an error can be handled by the QECC C_1, the corresponding error after measurement can be handled by the corresponding classical Reed-Solomon code. Moreover, a coarse-grained measurement, that is, the process of measuring each quantum register along the computational basis together with the inference of the quantum state from the Reed-Solomon code, can be regarded as a projective measurement along the C_1 encoded computational basis on the quantum state. In the verification step (5), all the $n-\delta$ honest players indeed measure the quantum states along the commonly agreed computational basis. The random parity check does not alter the state of the unmeasured quantum particles. Therefore, the coarse-grained measurements performed by the honest players commute with each other; and hence each coarse-grained measurement result will in no way change the outcome of all subsequent measurements [4]. Thus, theoretically, the honest players may push their coarse-grained measurement forward to the time when the quantum states are just prepared. Consequently, the probability that cheating player i will pass the quantum verification test in step (5) cannot exceed the probability of passing a classical random parity verification test in which player i is allowed to prepare only a classical mixture of states [4]. Clearly, the probability that player i cheats and yet he or she passes the classical verification test is no greater than $1/q^r$ where r is the number of independent rounds of tests performed. Consequently, by repeating the quantum random parity test $\log_q(1/e)$ times, the probability that player i cheats and yet he or she passes the quantum verification test in step (5) is at most e. Once the quantum verification test is passed, the fidelity of the remaining untested quantum states as being a valid input $|x_i\rangle$ is equal to $1-\ell e$ for some constant ℓ independent of n and e. Thus, the entropy of each of the untested quantum states is equal to $\log_z q+\ell e$. Hence, the cheaters have an exponentially small amount information about the private inputs of every honest player [4]. Using a similar argument, I know that the fidelity of the distributed preset quantum registers $|0\rangle_{\mathrm{L}}$ and $|0\rangle_{\tilde{\mathrm{L}}}$ is also equal to $1-\ell e$.

Therefore, I conclude that if there are at most δ cheaters and they choose to perform measurements individually, then the probability that these cheaters can obtain partial information on the private inputs of the honest players is bounded from above by ℓe for some fixed constant $\ell>0$ up to step (5) of the quantum scheme.

In the event that the players choose to teleport their random parity state to the verifier who then makes the necessary measurement, the proof of security up to step (5) is similar. Note that if the verifier is honest, then the above proof applies. On the other hand, if the verifier cheats, two things may happen. First, the verifier may wrongly announce an inconsistent result. This leads to an immediate abortion of the scheme; hence, he or she cannot obtain any extra information on the private input of an honest player. Second, the verifier may turn a blind eye to a measurement result that is inconsistent with the no cheater or eavesdropper assumption. Since $\delta/n<1/6$, a nonzero fraction of the verifiers are honest. So, after $O(\log(1/e))$ rounds of random parity tests, the probability that the private input of an honest player leaks out is less than ℓe for some fixed constant $\ell>0$ up to step (5) of the quantum scheme.

Thus I conclude that if there are at most δ cheaters and the players choose to teleport the particles encoding the random parities to the verifiers before making measurements, then the probability that cheaters obtain partial information on the private input of an honest player is less than ℓe for some fixed constant $\ell>0$.

B. Cheater cannot alter the computation result

Now I proceed to show that these δ cheaters cannot alter the outcome of the function evaluation f with a probability greater than e in steps (6) and (7) of the quantum scheme. Since one may regard any illegal quantum manipulation by the δ cheaters as decoherence acting on up to δ quantum registers in the QECC C_1, the theory of FTQC implies that any *quantum* manipulation by these cheaters cannot alter the final outcome of the function f. Nevertheless, the theory of FTQC assumes that all measurements of the encoded quantum state and manipulation of classical data are error-free. So it remains for me to show that measurement and classical data manipulation by cheaters also cannot alter the outcome of the function f.

Because of the choice of C_1 and C_2, there are two possible operations in the scheme that require measurement or classical message communication, namely, the verification test and the generalized Toffoli gate. As I have discussed previously, incorrect measurement or classical message broadcasting in a verification test results in the immediate abortion of the scheme. Hence it cannot alter the final output of the function *f*. So it remains for me to consider the case of a generalized Toffoli gate. Recall that the generalized Toffoli gate is collectively synthesized by the n players from the verified distributed encoded state $|0\rangle_{\tilde{L}}$ in step (6). Fortunately, if the players choose to perform their measurements individually, then all measurement results in step (6) are in either the $[n,d,n-d+1]_q$ or the $[n,n-d,d]_q$ Reed-Solomon code forms. Hence the δ cheaters cannot alter the measurement outcome and the value of z.

On the other hand, if they choose to teleport their states to their corresponding randomly assigned player, then in order to pass the final random parity test in step (7) with a probability greater than e, the cheaters must arrange the state of the final outcome $z=f(x_1,x_2,\ldots,x_n)$ for each of the $r=O(\log(1/e))$ copies of quantum particles to be almost identical. This is possible only when all the r randomly assigned players who are responsible for measurement cheat, since the probability that all randomly assigned players cheat is equal to $(\delta/n)^r=O(e)$. Consequently, the probability that the δ cheaters can alter the final value of z without being detected is equal to $\mathscr{c}e$ for some fixed positive constant $\mathscr{c}$.

C. Cheater cannot obtain partial information during distributed computing of the function f

Although cheaters cannot alter the final outcome of the computation with a probability greater than $\mathscr{c}e$ for some fixed positive constant $\mathscr{c}$, readers may ask if these cheaters can obtain partial information on the private input of an honest player in steps (6) and (7). Now, I show that this is not possible. Using the same argument as in Sec. III B together with the choice of $[[n,1,d]]_q$ codes C_1 and C_2, the only possible place for information leakage is the measurement performed by the players during the implementation of a generalized Toffoli gate. As I have discussed in Sec. III B, if the players choose to measure individually, then the δ cheaters cannot alter the joint measurement result that is required during the collective and distributive synthesis of the ancillary state $\Sigma_{a,b=0}^{q-1}|a,b,ab\rangle_L/q$ as well as during the implementation of the generalized Toffoli gate. Moreover, the theory of QECC tells us that the value of these measurements contains no information on the distributed encoded state $|x,y,z\rangle_L$. Recall that the δ cheaters have access only to their shares of the entangled quantum state together with the classical information on the measurement results on the fault-tolerant generalized Toffoli gate. Since C_1 is an $[[n,1,d]]_q$ QECC, this information alone is not enough for the cheaters to obtain any information on $|x,y,z\rangle_L$ and hence the private inputs of an honest player.

On the other hand, if the players choose to teleport their corresponding states to the randomly assigned players before making measurements, then we cannot control the action of a cheating assigned player. Nonetheless, by looking into the synthesis scheme of the ancillary state $\Sigma_{a,b=0}^{q-1}|a,b,ab\rangle_L$ used in step (6), we see that the cheating assigned player can only alter the third encoded quantum register of this ancillary state. In other words, the cheating assigned player can only, after error correction, alter the state of the last quantum register in Eq. (2). Right after all players teleported their corresponding quantum registers to the cheating assigned player, the δ cheaters would control the first three encoded quantum registers together with shares of the distributed encoded fourth, fifth, and sixth registers. Consequently, the reduced density matrix of the quantum registers controlled by the cheating assigned players is independent of x,y, and z. Hence it is impossible for the δ cheaters to obtain partial information on the private input of an honest player.

In summary, using the results in Secs. III A–III C, I conclude that the quantum secure multiparty computation scheme in Sec. II is secure provided that no more than δ players cheat. Moreover, the security is unconditional for it does not rely on any computational assumption.

In the alternative scheme that the players teleport their quantum states to some randomly chosen players and let these assigned players make the measurement, the proof is similar that the δ cheaters cannot alter the final outcome z and that they cannot obtain extra information on the private input of an honest player.

IV. COMPLEXITY AND SECURITY TRADEOFF BETWEEN THE QUANTUM AND CLASSICAL SCHEMES

Clearly, the above quantum secure multiparty computation scheme requires $O(n)$ quantum channels, a public classical unjamable broadcasting channel, and $O(n^2k\log(1/e))$ bits of quantum and classical communication in order to distribute and compute the classical function f, where k is the length of each private input. Distributed FTQC of registerwise addition, registerwise multiplication, and generalized CNOT gate do not require any communication. Distributed FTQC of a generalized Toffoli gate requires $O(nk\log(1/e))$ bits of classical message broadcast, or equivalently, $O(n^2k\log(1/e))$ bits of classical communication between the players if they choose to perform their measurements individually. Distributed FTQC of a generalized Toffoli gate requires $O(nk\log(1/e))$ bits of classical communication should the choose to teleport the states and measure them collectively by the randomly assigned players. Moreover, if classically nondistributed computing f requires T time steps and S space, then the distributed quantum computing scheme in step (6) above requires $O(nT^{1+\epsilon})$ time steps and $O(nS\log T)$ space for any $\epsilon>0$ [27]. Hence, the amount of communication required for distributed FTQC of a classical function f is bounded from above by $O(n^2kT^{1+\epsilon}\log 1/e))$ should players use the alternative teleportation plus measurement method. In contrast, the best classical secure multiparty computation scheme known to date requires $O(n^2)$ communication channels and $O(n^3kT)$ bits of communication. Thus the quantum secure multiparty computation scheme requires fewer channels and less computation or communication than the best known classical algorithm to date.

Nevertheless, the improvement of the quantum scheme over the classical one comes with a price tag. Recall that the maximum number of cheaters tolerated by this quantum scheme is related to the maximum possible distance d of a QECC that maps one $q$ary quantum register to n $q$ary quantum registers. Since I am using the $[[n,1,d]]_q$ QECC with $3d \leqslant n+2$, my scheme can tolerate only asymptotically up to strictly fewer than 1/6 cheaters. On the other hand, the best known classical scheme is unconditionally secure provided that strictly more than one-half of the players are honest. In other words, the quantum scheme reported here trades security for communication complexity.

V. FULL-BLOWN QUANTUM CODE IS REQUIRED IN THE QUANTUM SCHEME

At this point, readers may question if a full-blown QECC is required in this quantum scheme because phase errors do not affect the final outcome z. Rather surprisingly, the answer is yes. In fact, I shall show that if C is a linear map sending one quantum register to n quantum registers, then any two of the three following conditions imply the third one: (1) C is a QECC correcting up to δ spin flip errors; (2) C is a QECC correcting up to δ phase shift errors; (3) the partial trace over any $n-\delta$ registers gives no information on the initial unencoded wave function.

The theory of QECC implies that (1) and (2) $\Rightarrow$ (3). Now I shall show that (1) and (3) $\Rightarrow$ (2). The remaining case that (2) and (3) $\Rightarrow$ (1) can be proven in a similar way. I divide the n players into two groups. Groups A and B have $n-\delta$ and δ players, respectively. By Schmidt polar decomposition, the encoded normalized state $\Sigma_k \alpha_k |k\rangle_{\mathrm{L}}$ can be written as $\rho = \Sigma_{i,j,k,k'} \alpha_k \overline{\alpha_{k'}} \sqrt{\lambda_i(k)\lambda_j(k')}\, |a_i(k)\rangle \otimes |b_i(k)\rangle\langle a_j(k')| \otimes \langle b_j(k')|$, where $|a_i(k)\rangle$ and $|b_i(k)\rangle$ are eigenvectors of the reduced density matrices as seen by groups A and B, respectively. Hence, taking a partial trace over group A, condition (3) above tells us that

$$\mathrm{Tr}_A(\rho) = \sum_{i,j,k,k'} \alpha_k \overline{\alpha_{k'}} \langle a_j(k')|a_i(k)\rangle |b_i(k)\rangle\langle b_j(k')| \quad (3)$$

is independent of α_k. This is possible only if $|b_i(k)\rangle \equiv |b_i\rangle$ and $\sqrt{\lambda_i(k)\lambda_j(k')}\langle a_j(k')|a_i(k)\rangle$ are independent of k for all i,j. Condition (1) implies that

$$\sum_{i,j} \sqrt{\lambda_i(k)\lambda_j(k')}\langle b_i|S^\dagger|b_j\rangle \langle a_i(k)|S'|a_j(k')\rangle = \delta_{k,k'}\Lambda_{S,S'}, \quad (4)$$

where S and S' are spin flip operators such that each acts on no more than δ quantum registers, and $\Lambda_{S,S'}$ is independent of k and k' [24,25]. Since $|b_i\rangle$ is independent of k, Eq. (4) holds if one replaces S by a general quantum error operator G which acts on no more than δ quantum registers. Since groups A and B are arbitrarily chosen, Eq. (4) is valid if one replaces S' by G. Once again, since $|b_i\rangle$ is independent of k, I conclude that Eq. (4) is true even if one replaces the two spin flip operators S and S' by general quantum error operators G and G' which act on no more than δ quantum registers. Consequently, C is a QECC correcting up to δ errors [24,25]. In particular, condition (2) is valid.

VI. OUTLOOK

In summary, I have reported and proved the security of a quantum secure multiparty scheme to compute classical functions. The scheme makes essential use of fault-tolerant quantum computation and a specially designed quantum error correcting code. While the quantum scheme tolerates only about one-third the number of cheaters as the best known classical scheme to date, it requires an asymptotically smaller amount of communication between the players.

This scheme also tells us that higher dimensional Calderbank Shor Steane (CSS)-like quantum error correcting codes with fault-tolerant implementation have far-reaching applications outside the context of quantum-mechanical computation. While quantum code is not the only possible way to protect quantum information during computation [28], cheating players may do all the nasty things that only full-blown quantum code can handle. Hence quantum code is an essential ingredient in this secure multiparty computation scheme. Moreover, no binary $[[n,1,d]]_2$ CSS code with $d > n/7$ is known to date. Thus higher dimensional quantum code [29] appears to be an essential ingredient in causing my scheme to tolerate strictly fewer than one-sixth of cheating players. Since fault-tolerant computation of a general non-CSS-like code requires collective measurements [23], it seems likely that C_1 should be a CSS-like code [30]. In addition, by replacing the random polynomial codes C_1 and C_2 by corresponding continuous quantum codes [31] of the form $|a_0\rangle \mapsto \int da_1\, da_2 \cdots da_{d-1} \otimes_{i=1}^{n} |a_0 + a_1 y_i + \cdots + a_{d-1} y_i^{d-1}\rangle$, my scheme also works for continuous quantum variables.

Rains showed that no binary $[[n,1,2\delta+1]]_2$ quantum code exists for $\delta > n+1$ [32] and a simple modification of the proof of the optimality of the five-quantum-register code in Refs. [25] and [26] shows that $[[n,1,d]]_q$ codes must satisfy $d/n < 1/4$. Thus, it may be possible to design a QECC based secure multiparty computation scheme that tolerates up to one-quarter cheaters. It would be instructive to find such scheme, if any.

It is also natural to ask if it is possible to extend this scheme to perform multiparty computation of a *quantum function*. That is, given a commonly agreed unitary operator U as well as n private quantum states $|x_i\rangle$, is it possible to compute $U \otimes_i |x_i\rangle$? Clearly, such a scheme exists if all the players are honest. The players may simply modify the scheme in this paper a little by dropping all the verification tests that check the identity of the private inputs, final output, and correct implementation of generalized Toffoli gates. Nevertheless, there is no obvious way to use the random parity test to check the validity of a general quantum state. Moreover, a player may cheat by using delay measurement tactics as in the proof of the impossibility of quantum bit commitment [7]. It is, therefore, of great interest to know if it is possible to achieve quantum multiparty computation of a quantum function in the presence of cheaters.

ACKNOWLEDGMENTS

I would like to thank Debbie Leung for her valuable discussions and H.-K. Lo for his useful suggestions on improving my presentation. Moreover, very useful discussions are gratefully acknowledged with C. Crépeau on the relation between random polynomial quantum code and classical Reed-Solomon code during the Quantum Computation Workshop at the Isaac Newton Institute, Cambridge. This work was supported by the Hong Kong Government RGC Grant Nos. HKU 7095/97P and HKU 7143/99P.

APPENDIX A: PROCEDURE FOR TELEPORTING A qARY STATE

The $q$ary state quantum teleportation process goes as follows: The sender and the receiver first share the state $|\Phi\rangle=\Sigma_{k=0}^{q-1}|kk\rangle/\sqrt{q}$ before the sender makes a joint measurement on the quantum state $|\Psi\rangle$ to be teleported and his or her share of the state $|\Phi\rangle$ along the basis $\{\Sigma_{k=0}^{q-1}\omega_q^{bk}|a,a+k\rangle/\sqrt{q}\}_{a,b\in\mathbb{F}_q}\}$ where ω_q is a primitive qth root of unity. Then, the sender informs the receiver of the measurement result. If the measurement outcome is $\Sigma_{k=0}^{q-1}\omega_q^{bk}|a,a+k\rangle/\sqrt{q}$, then the receiver may reconstruct the quantum state $|\Psi\rangle$ by applying the unitary transformation $|x\rangle\mapsto\omega_q^{b(x-a)}|x-a\rangle$ to his or her share of the original state $|\Phi\rangle$.

APPENDIX B: PROCEDURE FOR THE RANDOM PARITY–HASHING TEST

Let us consider the basis $\mathcal{B}=\{\Sigma_{k=0}^{q-1}\omega_q^{kb}|k,k+a\rangle/\sqrt{q}\}_{a,b\in\mathbb{F}_q}$. Clearly, one may transform from one basis state ket to another by local unitary operations alone. I denote the set of all such transformations by T. Furthermore, the registerwise generalized C-NOT operation maps the basis states $\mathcal{B}\otimes\mathcal{B}\equiv\{|A\rangle\otimes|B\rangle:|A\rangle,|B\rangle\in\mathcal{B}\}$ to $\mathcal{B}\otimes\mathcal{B}$ up to a global phase. Therefore the random parity–hashing test goes as follows: The two parties cooperate and randomly apply a transform $f_i\in T$ for each share of the entangled quantum state they obtain in step (3). Then they apply registerwise generalized C-NOT operations to a number of randomly selected pairs of their resultant entangled quantum states. Finally, they measure the outcome of their final target quantum register along the computational basis. They continue only if their measurement result is consistent with the hypothesis that their share of quantum particles are all in the state $|\Phi\rangle$. If they continue, they apply suitable transformations $g_i\in T$ on their remaining shares of quantum states so as to bring them back to the state $|\Phi\rangle$. Clearly, this random parity checking procedure is a direct generalization of that used in Ref. [4].

APPENDIX C: ACTION OF $\mathfrak{F}$

Here I show that $\mathfrak{F}|0\rangle_{\mathrm{L}}=\Sigma_{k=0}^{q-1}|k\rangle_{\tilde{\mathrm{L}}}$. The proof of $\mathfrak{F}|0\rangle_{\tilde{\mathrm{L}}}=\Sigma_{k=0}^{q-1}|k\rangle_{\mathrm{L}}$ is similar. Recall that $\mathfrak{F}$ denotes the collective action of $|a,b\rangle\mapsto\omega_q^{m_iab}|a,b\rangle$ by the ith player on their share of the encoded quantum registers, where $m_i\in\mathbb{F}_q$ satisfies the system of equations $\Sigma_{i=1}^n m_i=1$ and $\Sigma_{i=1}^n m_iy_i=\Sigma_{i=1}^n m_iy_i^2=\cdots=\Sigma_{i=1}^n m_iy_i^{n-1}=0$. Thus,

$$\mathfrak{F}|a_0\rangle_{\mathrm{L}}=\sum_{a_1,a_2,\ldots,a_{d-1},b_0,b_1,\ldots,b_{n-1}=0}^{q-1}\times\omega_q\sum_{i=1}^{n}\sum_{j=0}^{d-1}\sum_{k=0}^{n-1}m_ia_jb_ky_i^{j+k}\otimes_{i=1}^{n}|b_0+b_1y_i+\cdots+b_{n-1}y_i^{n-1}\rangle. \quad \text{(C1)}$$

Summing over a_1 in Eq. (C1) gives $b_{n-1}=0$; and then summing over a_2 gives $b_{n-2}=0$. Inductively, I conclude that Eq. (C1) becomes $\Sigma_{b_0,b_1,\ldots,b_{n-d}}\omega_q^{a_0b_0}\otimes_{i=1}^{n}|b_0+b_1y_i+\cdots+b_{n-d}y_i^{n-d}\rangle$. Hence, by putting $a_0=0$, I obtain $\mathfrak{F}|0\rangle_{\mathrm{L}}=\Sigma_{k=0}^{q-1}|k\rangle_{\tilde{\mathrm{L}}}$, which is our required result.

[1] P.W. Shor, in *Proceedings of the 35th Annual Symposium on the Foundation of Computer Science* (IEEE Computer Society, Los Alamitos, CA, 1994), p. 124.

[2] L. Grover, in *Proceedings of the 28th Annual ACM Symposium on the Theory of Computing* (ACM Press, New York, 1996), p. 212.

[3] C.H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing* (IEEE, New York, 1984), p. 175; A.K. Ekert, Phys. Rev. Lett. **67**, 661 (1991); D. Mayers, Los Alamos e-print quant-ph/9802025.

[4] H.-K. Lo and H.F. Chau, Science **283**, 2050 (1999); and the associated supplementary materials available at http://www.sciencemag.org/feature/data/984035.shl.

[5] R. Cleve and H. Buhrman, Phys. Rev. A **56**, 1201 (1997); W. van Dam, P. Hoyer, and A. Tapp, Los Alamos e-print quant-ph/9710054.

[6] A. Karlsson, M. Koashi, and N. Imoto, Phys. Rev. A **59**, 162 (1999); M. Hillery, V. Buzek, and A. Berthiaume, *ibid.* **59**, 1829 (1999); R. Cleve, D. Gottesman, and H.-K. Lo, Phys. Rev. Lett. **83**, 648 (1999).

[7] H.-K. Lo and H.F. Chau, Phys. Rev. Lett. **78**, 3410 (1997); D. Mayers, *ibid.* **78**, 3414 (1997); H.F. Chau and H.-K. Lo, Fortschr. Phys. **46**, 507 (1998).

[8] H.-K. Lo, Phys. Rev. A **56**, 1154 (1997).

[9] O. Goldreich, S. Micali, and A. Wigderson, in *Proceedings of the 19th Annual ACM Symposium on the Theory of Computing* (ACM Press, New York, 1987), p. 218.

[10] M. Ben-Or, S. Goldwasser, and A. Wigderson, in *Proceedings of the 20th Annual ACM Symposium on the Theory of Computing* (ACM Press, New York, 1998), p. 1.

[11] D. Chaum, C. Crépeau, and I. Damgard, in *Proceedings of the 20th Annual ACM Symposium on the Theory of Computing* Ref. [10], p. 11.

[12] A. Shamir, Commun Assoc. Comput Mach. **22**, 612 (1979).
[13] T. Rabin and M. Ben-Or, in *Proceedings of the 21st Annual ACM Symposium on the Theory of Computing* (ACM Press, New York, 1989), p. 73.
[14] B. Schneier, *Applied Cryptography*, 2nd ed. (Wiley, New York, 1996), Secs. 6.1 and 6.2.
[15] D. Aharonov and M. Ben-Or, in *Proceedings of the 29th Annual ACM Symposium on the Theory of Computation* (ACM, New York, 1998), p. 176.
[16] P. Shor, in *Proceedings of the 37th Annual Symposium on the Foundation of Computer Science* (IEEE Computer Society, Los Alamitos, CA, 1996), p. 56; A.Yu. Kitaev, Russ. Math. Surv. **52**, 1191 (1997); E. Knill, R. Laflamme, and W. Zurek, Science **279**, 342 (1998).
[17] J. Preskill, in *Introduction to Quantum Computation and Information*, edited by H.-K. Lo, S. Popescu, and T. Spiller (World Scientific, Singapore, 1998), p. 213.
[18] W. Dür, H.-J. Briegel, J.I. Cirac, and P. Zoller, Philos. Trans. R. Soc. London, Ser. A **356**, 1713 (1998); H.-J. Briegel, W. Dür, J.I. Cirac, and P. Zoller, Phys. Rev. Lett. **81**, 5932 (1998); W. Dür, H.-J. Briegel, J.I. Cirac, and P. Zoller, Phys. Rev. A **59**, 169 (1999).
[19] C.H. Bennett, D.P. DiVincenzo, J.A. Smolin, and W.K. Wootters, Phys. Rev. A **54**, 3824 (1996).
[20] M. Murao, M.B. Plenio, S. Popescu, V. Vedral, and P.L. Knight, Phys. Rev. A **57**, R4075 (1998).
[21] C.H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W.K. Wootters, Phys. Rev. Lett. **70**, 1895 (1993).
[22] A. Barenco, C.H. Bennett, R. Cleve, D.P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J.A. Smolin, and H. Weinfurter, Phys. Rev. A **52**, 3457 (1995).
[23] D. Gottesman, Los Alamos e-print quant-ph/9802007; in *Proceedings of the 1st NASA International Conference on Quantum Communications and Quantum Computing*, Springer-Verlag Lecture Notes in Computer Science Vol. 1509, edited by C.P. Williams (Springer-Verlag, Berlin, 1999), p. 302; Chaos Solitons and Fractals **10**, 1749 (1999).
[24] A.M. Steane, Phys. Rev. A **54**, 4741 (1996); D. Gottesman, Ph.D. thesis, Caltech, 1997, and references cited therein.
[25] E. Knill and R. Laflamme, Phys. Rev. A **55**, 900 (1997).
[26] H.F. Chau, Phys. Rev. A **56**, R1 (1997).
[27] C.H. Bennett, SIAM J. Comput. **18**, 766 (1989).
[28] A.Yu. Kitaev, Los Alamos e-print quant-ph/9707021 1997; A. Barenco, A. Berthiaume, D. Deutsch, A. Ekert, R. Jozsa and C. Macchiavello, SIAM J. Comput. **26**, 1541 (1997); P. Zanardi and M. Rasetti, Phys. Rev. Lett. **79**, 3306 (1997); D.A. Lidar, I.L. Chuang and K.B. Whaley, *ibid.* **81**, 2594 (1998).
[29] E. Knill, Los Alamos e-print quant-ph/9608048; e-print quant-ph/9608049; H.F. Chau, Phys. Rev. A **55**, R839 (1997); E. Rains, Los Alamos e-print quant-ph/9703048.
[30] A.R. Calderbank and P.W. Shor, Phys. Rev. A **54**, 1098 (1996); A.M. Steane, Proc. R. Soc. London, Ser. A **452**, 2551 (1996).
[31] S.L. Braunstein and H.J. Kimble, Phys. Rev. Lett. **80**, 4084 (1998); S. Lloyd and J.-J.E. Slotine, *ibid.* **80**, 4088 (1998).
[32] E. Rains, Los Alamos e-print quant-ph/9611001.