Insecurity of position-based quantum-cryptography protocols against entanglement attacks

Hoi-Kwan Lau* and Hoi-Kwong Lo†

Center for Quantum Information and Quantum Control (CQIQC), Department of Physics and Department of Electrical and Computing Engineering, University of Toronto, 60 Saint George Street, Toronto, Ontario, Canada, M5S 1A7

(Received 21 September 2010; published 27 January 2011)

Recently, position-based quantum cryptography has been claimed to be unconditionally secure. On the contrary, here we show that the existing proposals for position-based quantum cryptography are, in fact, insecure if entanglement is shared among two adversaries. Specifically, we demonstrate how the adversaries can incorporate ideas of quantum teleportation and quantum secret sharing to compromise the security with certainty. The common flaw to all current protocols is that the Pauli operators always map a codeword to a codeword (up to an irrelevant overall phase). We propose a modified scheme lacking this property in which the same cheating strategy used to undermine the previous protocols can succeed with a rate of at most 85%. We prove the modified protocol is secure when the shared quantum resource between the adversaries is a two- or three-level system.

DOI: 10.1103/PhysRevA.83.012322 PACS number(s): 03.67.Dd

I. INTRODUCTION

Quantum cryptography has both power and limitations. Whereas quantum cryptography can offer unconditional communication security [1–3] through quantum key distribution (QKD) [4,5] and multiparty quantum secret sharing [6,7], it cannot protect private information in secure two-party computations due to standard no-go theorems in quantum bit commitment [8,9] and quantum oblivious transfer [10]. So what are the exact limits on the power of quantum cryptography?

In this article, we help shed light on this question by focusing on another proposed application of quantum cryptography. It is called position-based cryptography (PBC) [11]. The goal of position-based cryptography is for a prover to prove to a set of cooperating spatially separated verifiers that he or she is at (or in the small neighborhood of) a particular spatial location.

Why is position-based cryptography interesting? In everyday life, we constantly place trust on spatial locations. For instance, when using a bank to deposit some money, we seldom ask the teller to prove that he or she is indeed a bank employee rather than an imposter. Why? Presumably we have used this bank before (at this particular location), and thus the teller occupying this same physical space convinces us that he or she can be trusted as a bank employee.

Position-based cryptography might also be of interest in, for example, automatic road tolling in vehicular communication systems [12]. Instead of collecting road tolls manually or installing many automatic collection stations in each highway entrance and exit, perhaps satellites could track all vehicles in a highway and charge them road tolls automatically, according to the paths taken. For such a road toll system to be foolproof, it is important to ensure that a cheater cannot fool the verifiers (satellites) as to his or her whereabouts.

Unfortunately, in the classical world, unconditionally secure position-based cryptography has been proven to be impossible [11,13]. The reason is that classical messages can be perfectly cloned by cheaters before forwarding them to the authorized receiver. Consequently, neither senders nor receivers are able to detect an intercept-and-broadcast attack.

Quantum cryptography has a fundamental advantage over classical cryptography due to the quantum no-cloning theorem [14,15]. In view of the success in quantum key distribution, it is an interesting question to ask whether PBC can be implemented with unconditional security in the quantum setting. As far as we know, the possibility of position-based quantum cryptography (PBQC) was first studied by Kent under the name of "quantum tagging" as early as 2002. Based on the idea, a patent of a quantum tagging system introduced by Kent *et al.* was granted in 2006 [16]. However, their results did not appear in the academic literature until 2010 [17]. Recently, before the appearance of Ref. [17], two PBQC protocols have been independently proposed by Chandran *et al.* [13] (hereafter denoted as Protocol A) and Malaney [18,19] (hereafter denoted as Protocol B). Protocol A is claimed to be unconditionally secure with a detailed proof of security based on a complementary information trade-off argument. Protocol B is also claimed to be unconditionally secure due to the quantum no-cloning theorem, but no detailed security proof has been given.

Contrary to the claims of unconditional security, both protocols are, in fact, insecure. Cheaters can make use of entanglement to conduct nonlocal operations to produce the same response as in the honest case. Independent of our present work, Kent, Munro, and Spiller [17] have discussed some conditions required for a secure PBQC protocol. They report that several types of PBQC scheme are insecure against teleportation-based attacks, and they describe the attacks if the locations of reference stations and authorized receiver are collinear. Their attack applies to Protocols A and B for the case of one spatial dimension.

There are two objectives in this article. First, we show how existing PBQC protocols (Protocols A and B) can be cheated by using entangled resources and discuss why the protocols are insecure. We discuss not only the case of one spatial dimension but also higher dimensions. Second, we propose a modified protocol and discuss its security. Our article is organized as follows. In Sec. II, we outline the procedure of both Protocol A and Protocol B. In Sec. III, we consider the case where the number of reference stations $N = 2$. Similarly to Ref. [17]

*kero.lau@utoronto.ca

†hklo@comm.utoronto.ca

but, more explicitly and in a step-by-step manner, we show how the protocols can be cheated with certainty. In Sec. IV, we consider the cases where $N > 2$, which can be cheated by techniques of quantum secret sharing and cluster state quantum computation. The reason for the insecurity of both protocols and the loophole of the claimed security proof are discussed in Sec. V. In Sec. VI, we give our modified protocol and examine its security under our cheating scheme. Our protocol is proved to be secure in Sec. VII if cheaters share entangled qubits or qutrits only. Finally, we summarize our article in Sec. VIII with brief discussions.

II. PBQC PROTOCOLS

Here, for simplicity, we assume that all honest parties have synchronized clocks and work with a flat Minkowski space time. The idea of position-based quantum cryptography is to divide encoded quantum information into several parts (but possibly entangled) and distribute to N reference stations $V_1,\dots,V_N$ at various separated locations. The divided pieces are then sent from different directions to an authorized receiver P, who is located at a preassumed position $\vec{x}_P$ surrounded by a finite secure region which no cheaters have access to. For simplicity, we hereafter assume $\vec{x}_P$ is located equidistant from all reference stations and that the divided information is sent simultaneously from the respective stations. Measurement is immediately conducted by P on the quantum system, and the result is broadcast for verification. The argument is as follows. Since perfect quantum measurement (learning the particle's state in a deterministic manner) can be achieved only with adequate knowledge about the system, such as its polarization, cheaters outside $\vec{x}_P$ must wait for a longer time than P to obtain enough information for perfect measurement. Otherwise, they are only able to conduct imperfect measurements. Therefore, references can authenticate receiver's position by checking the response time and error rate of broadcasted measurement results. Procedures of two existing proposals are outlined as follows.

A. Protocol A

The idea of Protocol A is to send the basis of measurement and the encoded qubit separately from different reference stations [13]. Security of this protocol was believed to rely on the idea that quantum system can be measured perfectly only if the correct measurement basis is obtained. Explicit procedures of Protocol A follows.

Step 1. Station V_1 encodes a message $u \in \{0,1\}$ as a qubit $|u\rangle$, where $|0\rangle$ and $|1\rangle$ are $+1$ and -1 eigenstates of Pauli Z operator, respectively. Inspired by the well-known Bennett-Brassard 1984 (BB84) QKD protocol, V_1 encrypts the message by applying the transformation H^q on the qubit, where H is the Hadamard gate and q is a random bit valued 0 or 1.

Step 2. V_1 generates $N-2$ random bits $q_2,q_3,\dots,q_{N-1}$, and decide a bit q_N by the relation

$$q = q_2 + q_3 + \cdots + q_N \bmod 2. \tag{1}$$

The bits $q_2,q_3,\dots,q_N$ are distributed to the reference stations $V_2,\dots,V_N$, respectively. The encoded message u is also sent to other stations. We assume the communication between reference stations are secure, for example, the QKD system is employed.

Step 3. The reference stations $V_1,\dots,V_N$ agree a time t_0 when the PBQC scheme starts. At $t = t_0$, V_1 sends the encoded qubit to P, while V_i sends the classical bit q_i for $i = 2,3,\dots,N$.

Step 4. On receiving all information, P adds up all bits to obtain q. The qubit can be decrypted by applying H^q and measured in the Z basis to obtain the encoded message. P broadcasts the results immediately to all reference stations. We assume all operations of P cost negligible time.

Step 5. If q's are random enough, missing any one classical bit would cause half a chance of a wrong measurement basis. Reference stations can validate the identity of P by checking if the response is consistent with the encoded message. By checking the arrival time of the response at different reference stations, the location of P is also verified.

B. Protocol B

The idea of Protocol B [18] is to encode information into maximally entangled states and then perform encryption by local transformations. Classical information about transformations are sent from different reference stations. Security of this protocol was believed to rely on the fact that correct measurement cannot be conducted without decrypting all qubits, as well as the idea that local measurement must disturb an entangled state. The explicit procedure of Protocol B follows.

Step 1. N bits of message is encoded as a N qubit GHZ state

$$|\text{GHZ}\rangle = \frac{1}{\sqrt{2}}(|a_1\rangle|a_2\rangle\cdots|a_N\rangle \pm |1\oplus a_1\rangle|1\oplus a_2\rangle\cdots|1\oplus a_N\rangle), \tag{2}$$

where $a_1,\dots,a_N \in \{1,0\}$; $\oplus$ denotes addition with modular 2. Each reference station picks a qubit from the entangled state.

Step 2. Each qubit is encrypted by the local transformation U_i and sent to an authorized receiver P. P will store the entangled state in his quantum memory.

Step 3. The PBQC scheme starts at an agreed time $t = t_0$. Every reference station sends the classical information about the transformation U_i to P at the same time.

Step 4. P immediately decrypts the state after receiving the classical information. He then conducts an N-qubit GHZ state measurement to decode the message and announces his result at once.

Step 5. The measurement result is probably wrong if someone measures the state before getting all transformation information. Hence the identity of P can be authenticated from the announced result. Besides, the location of P can be verified by checking the total time spent on the whole process.

C. Dimensionality of PBQC scheme

In general, the reference stations lie on a one-dimensional straight line for $N = 2$ and a two-dimensional plane for $N = 3$, and they distribute in three-dimensional space for $N > 3$. We comment that the dimension of position of P that can be verified by the PBQC scheme is *independent* of the spatial

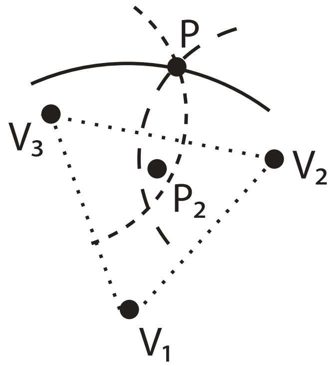

FIG. 1. At a particular time t_1, the front of signals sent from V_1, V_2, and V_3 are represented by solid, dashed, and short-dashed lines, respectively. While signals reach P at $t = t_1$, another position P_2 inside the triangle of three reference positions (framed by dotted lines) can obtain all information before t_1.

dimension of the reference station distribution. For example, even if there are two reference stations and they are collinear with P, all three components of $\vec{x}_p = (x_p, y_p, z_p)$ can be authenticated by the PBQC scheme. To illustrate this idea, assume V_1 and V_2 are lying on the x axis and $\vec{x}_p$ is some point in between. The signals are sent at a time designated by the PBQC protocols. It is easy to see that any position with $y \neq 0$ or $z \neq 0$ takes a longer time than P to receive both information from V_1 and V_2. Thus the *one*-dimensional PBQC actually confirms the *three*-dimensional position of P instead of the x coordinate only. Similarly, if P is located in the same plane as the three reference stations V_1, V_2, and V_3, the PBQC scheme also verifies the three-dimensional position of P. This argument, however, requires that the position of the reference stations are well chosen, i.e., V_1, V_2, P are collinear or V_1, V_2, V_3, P are coplanar. Four reference stations are necessary if their locations are constrained.

We also note that PBQC can be performed if and only if P is located inside a polyhedron formed by the positions of some reference stations. Otherwise, for all starting times chosen by the reference stations, there must be places inside the polyhedron such that shorter or equal time is required to receive all information. The idea is illustrated in Fig. 1.

III. CHEATING IN THE $N = 2$ CASE

Contrary to claim(s) of unconditional security, we find that both Protocols A and B are, in fact, insecure. We first demonstrate our cheating strategy for the two-reference-stations case (i.e., $N = 2$) for both protocols and generalize it to the more-reference-stations case (i.e., $N > 2$) in the next section. In the current case, we assume V_1 and V_2 are separated by distance $2d$ and P is located in the middle of the two reference stations so all systems lie on a one-dimensional straight line. PBQC requires P is surrounded by a finite restricted area, such as inside a big military base, with width $2l$ that no cheaters can get into. We assume either qubit or classical information are transmitted at the speed of light c, and the time for intermediate processing is negligible. If the PBQC scheme starts at $t = 0$, V_1 and V_2 expect to get the correct response at $t = 2d/c$.

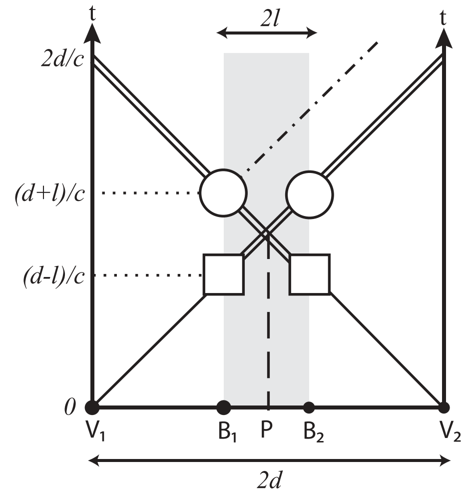

FIG. 2. Space-time diagram of the one-dimensional scenario. Solid lines denote space-time trajectory of information which is possibly quantum or classical, while double lines denote that of classical information only. In both Protocols A and B, all measurements ought to be conducted at $t = (d - l)/c$ (shown as squares) in order to give correct response to reference positions on the expected time $t = 2d/c$. An appropriate response is decided after information of another cheater is received at $t = (d + l)/c$ (shown as circles). If there is no entangled resources shared, B_1 has to wait for information from V_2 to conduct perfect measurement. Trajectory of the corresponding response is represented by the dot-dashed line, which shows the correct result cannot reach V_2 before $t = 2d/c$.

Successful cheating is to produce the correct response not slower than $t = 2d/c$ without entering the restricted area. We find that two cheaters are enough to cheat the protocols in this case. We assume cheaters B_1 and B_2 are sitting at $d - l$ and $d + l$, respectively, which are both just outside the restricted area. The layout of our scenario is shown in Fig. 2.

A. Flaw in claimed security proof

We remark that Protocol A was once believed to be unconditionally secure. In fact, a detailed claim of proof of security based on *complementary information trade-off* was given in Ref. [13]. The intuition behind the claimed proof is that any measurement on the encrypted qubit would inevitably disturb the state and hence yield a wrong outcome with nonzero probability.

Unfortunately, in the security proof of Protocol A [13], it was implicitly assumed that no prior entanglement is shared by the cheaters. Indeed, a *pure* state is assumed for the state consisting of only one cheater and one honest party. See, for example, the first sentence of the last paragraph of page 8 of Ref. [13].

We remark that such an assumption is incorrect. In fact, the cheaters can easily nullify the security proof by using shared entanglement. We note that with shared entangled resources, quantum teleportation can be conducted by measuring the qubit appropriately [20]. The main idea of our cheating scheme in the $N = 2$ case is to teleport the encrypted qubit from B_1 to B_2 for measurement in the correct basis. Detailed cheating strategy procedure is as follows.

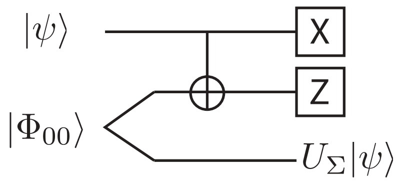

FIG. 3. The circuit for teleporting an unknown qubit $|\psi\rangle$ [20,21]. Measurement is denoted as squares; the measurement basis is represented by the character inside the squares. $U_\Sigma = X^{(1-s_2)/2}Z^{(1-s_1)/2}$ is the by-product of teleportation depending on random measurement outcome s_1 and s_2.

B. Cheating against Protocol A in the $N = 2$ case

Step 1. Before the cheaters move to the destination, they come together and each pick a particle from a Bell state

$$|\Phi_{00}\rangle \equiv \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \frac{1}{\sqrt{2}}(|++\rangle + |--\rangle). \quad (3)$$

We assume their quantum memory is perfect so the qubits remain coherent until measurement.

Step 2. When the PBQC scheme starts $t = 0$, V_1 sends a qubit $H^q|u\rangle$, and V_2 sends the bit $q_2 = q$ to P. At $t = (d - l)/c$, B_1 captures the qubit and B_2 obtains the basis information. To avoid suspicion of P, the cheaters can send a dummy qubit and basis information to him, and P's response thereafter is interfered or blocked by classical devices. We hereafter neglect the role of P.

Step 3. B_1 immediately perform a Bell measurement on this two qubits in order to teleport the state to B_2, the circuit of his measurement is given in Fig. 3. He sends the measurement outcomes of the encrypted qubit, s_1, and Bell state qubit, s_2, to B_2 at once. We note that measurement outcomes of Pauli operators are $+1$ or -1.

Step 4. At the same instance $t = (d - l)/c$, the teleported qubit of B_2 becomes

$$X^{(1-s_2)/2}Z^{(1-s_1)/2}H^q|u\rangle. \quad (4)$$

Consider if $q = 0$, B_2 has a state

$$X^{(1-s_2)/2}Z^{(1-s_1)/2}|u\rangle = (-1)^{u(1-s_1)/2}|u \oplus (1 - s_2)/2\rangle. \quad (5)$$

Since B_2 knows the basis is Z, and the state in Eq. (5) is an eigenstate of Pauli Z operator, he can conduct a perfect measurement with outcome $(-1)^u s_2$. If $q = 0$, B_2 has a state

$$HZ^{(1-s_2)/2}X^{(1-s_1)/2}|u\rangle = (-1)^{[u\oplus(1-s_1)/2](1-s_2)/2}H|u \oplus (1 - s_1)/2\rangle. \quad (6)$$

Since B_2 knows the basis is X, and the state in Eq. (6) is an eigenstate of Pauli X operator, he can conduct a perfect measurement with outcome $(-1)^u s_1$.

B_2 immediately sends the result to B_1. It must be noted that although the measurement outcome of B_2 contains information about outcome of B_1 our teleportation scheme does not permit superluminal communication because B_1 cannot choose the measurement result deterministically.

Step 5. Then at $t = (d + l)/c$, both B_1 and B_2 know each other's results, as well as the correct measurement basis. They can invert the value of u by multiplying the outcome of B_2 with the second outcome of B_1 for $q = 0$ or by multiplying the outcome of B_2 with first outcome of B_1 for $q = 0$. B_1 then sends u to V_1 while B_2 sends to V_2, and both reference stations will receive the correct signal at $t = 2d/c$. The whole process consumes the same amount of time to produce the same correct result as there are no cheaters; Protocol A is, therefore, insecure in 1D.

Remark. Let us explain Step 3 (the teleportation step). The teleported state received by B_2 will be acted on by one of the four operators, I, X, Z, or XZ. Since the original state is an eigenstate of either X and Z, we note that the four resulting states are either orthogonal to each other or the same (up to an irrelevant overall phase). Therefore, B_2 with the basis information can simply measure the qubit in that basis without disturbing the state at all. Subsequently, after hearing the actual Bell measurement, outcomes by B_1 and B_2 will be able to tell what the original state is. For this reason, B_1 and B_2 can cheat successfully with certainty. Therefore, Protocol A is insecure.

Remark. Let us explain this from another angle. Since the measurements by B_1 and B_2 commute with each other, we can also interpret the result from the viewpoint where B_2 performs a measurement before B_1 does. In this case, B_2, with the basis information will measure a qubit in the correct basis. Using the Einstein-Podolsky-Rosen effect, the qubit held by B_1 will be projected to either the same state or the opposite state to the qubit sent by V_1. So the task of B_1 is to perform a parity check of the states of the two qubits. While a general parity check is impossible for all bases, we note that in Protocol A, we consider only the two bases X and Z. So, in this case, as the operator XX commutes with ZZ, indeed B_1 can perform a parity check by simply doing a Bell measurement. For this reason, B_1 and B_2 can cheat successfully with certainty.

C. Cheating against Protocol B in the $N = 2$ case

In the current case, 2 bits of information, $ab = \{00,01,10,11\}$, can be encoded into one of the four Bell states $|\Phi_{ab}\rangle$ [18] in Eq. (3) and

$$|\Phi_{01}\rangle \equiv \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) = \frac{1}{\sqrt{2}}(|+-\rangle + |-+\rangle) \quad (7)$$

$$|\Phi_{10}\rangle \equiv \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) = \frac{1}{\sqrt{2}}(|++\rangle - |--\rangle) \quad (8)$$

$$|\Phi_{11}\rangle \equiv \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) = \frac{-1}{\sqrt{2}}(|+-\rangle - |-+\rangle). \quad (9)$$

The qubits are then encrypted by random local transformation U_1 and U_2 and sent to P. The PBQC scheme starts at $t = 0$ when reference stations broadcast U_i and is expected to end at $t = 2d/c$ in the honest case. The idea of the cheating is to first capture and store the qubits until decryption information. One of the cheaters then teleports the qubit so the other cheater possesses two entangled qubits to do Bell measurement. The step-by-step procedure is as follows.

Step 1. Before the process, the cheaters share a Bell state in Eq. (3) and store it in good quantum memory.

Step 2. The cheaters break into the quantum channels connecting P with reference stations, they capture the qubits sent by V_1 and V_2 in a good quantum memory to preserve the coherence until measurement.

Step 3. At $t = (d - l)/c$, both cheaters receive the U_i form references, $U_i^\dagger$ is applied respectively on the qubits to recover the encoded state $|\Phi_{ab}\rangle$.

Step 4. B_2 teleports the incoming qubit to B_1. We call the encoded state qubit captured by $B_1(B_2)$ as qubit 1(2), and the Bell state qubit of $B_1(B_2)$ as qubit 4(3). We analyze the teleportation by stabilizer formalism [22] as follows. B_2 apply a controlled-NOT gate on his qubits, the state is then stabilized by

$$K_1 = (-1)^a Z_1 Z_2, \quad K_2 = (-1)^b X_1 X_2 X_3,$$
$$K_4 = Z_2 Z_3 Z_4, \quad K_3 = X_3 X_4. \tag{10}$$

Qubit 2 is then measured in the X basis and qubit 3 is measured in the Z basis. The outcomes s_2 and s_3 are sent to B_1 immediately. The new set of stabilizers after the measurement is

$$K_1' = (-1)^a s_3 Z_1 Z_4, \quad K_2' = (-1)^b s_2 X_1 X_4,$$
$$K_3' = s_3 Z_3, \quad K_4' = s_2 X_2. \tag{11}$$

Qubits 2 and 3 are obviously no longer entangled as they are measured. K_1' and K_2' show that qubits 1 and 4 are left as a Bell state $|\Phi_{a'b'}\rangle$, where $a' = a + (1 - s_3)/2$ and $b' = b + (1 - s_2)/2$. So B_1 can measure the state perfectly by Bell measurement, the outcomes a' and b' are sent to B_2 immediately.

Step 5. At $t = (d + l)/c$, both cheaters obtain information from each other. a and b are deduced from a', b', s_2, and s_3, and they are sent to and eventually received by reference stations at $t = 2d/c$. Hence correct results are extracted by cheaters using the same time as in honest case and PBQC is hacked.

IV. CHEATING IN $N > 2$ CASE

We first consider the $N = 3$ case in which the reference stations lie on the same plane, and then we discuss how the scheme can be generalized to three-dimensional cases with $N > 3$. For simplicity, we assume the three reference stations V_1, V_2, and V_3 are located at the vertex of an equilateral triangle. The receiver P sits in the center of the triangle, which is distance d from each references and surrounded by a restricted area with radius l. We find that three cheaters are enough to cheat both protocol perfectly. We assume cheaters B_1, B_2, and B_3 locate at distance l from P and $d - l$ from V_1, V_2, and V_3, respectively. A layout of their position is shown as Fig. 4.

A. Cheating against Protocol A in $N > 2$ case

In this protocol, V_1 encrypts the encoded state in $H^q|u\rangle$ and distributes q_2 and q_3 to V_2 and V_3. The physical meaning of q_2 and q_3 are the number of H gates such that progressively applying $H^{q_2} H^{q_3}$ is equal to H^q. In this case, the cheaters are not going to teleport the qubit as there is only one qubit but two separate pieces of information. Instead, they need methods to share the rotation information, so the quantum secret-sharing scheme is employed [6,7]. The steps of the cheating scheme are as follows.

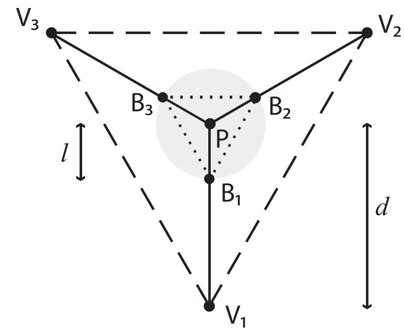

FIG. 4. Positions of reference stations, cheaters, and the authorized receiver of our three-station scenario are shown as black dots. The shaded region represents the restricted area surrounding P. Without the cheating, information flows along solid lines; if cheating presents, information flows along solid lines outside the restricted area and follows dotted lines in the restricted area. As the path of $V_2 \to P \to V_1$ is longer than $V_2 \to B_2 \to B_1 \to V_1$, the process of cheating takes a shorter amount of time than does the honest case.

Step 1. Before the PBQC scheme starts, the cheaters construct a three-particle GHZ state

$$\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle). \tag{12}$$

They then travel to the desired position before the PBQC starts at $t = 0$.

Step 2. At $t = (d - l)/c$, B_2 and B_3 gets q_2 and q_3. If $q_i = 0$, cheater B_i measures his qubit in the X basis; otherwise he measures in the Y basis. According to the idea of quantum secret sharing, if both B_2 and B_3 measure in the same basis, the GHZ qubit holding by B_1 becomes an eigenstate of the Pauli X operator; otherwise, it is an eigenstate of the Y operator. As an example, let us consider the case where $q_2 = 0$ and $q_3 = 1$. It can be shown that the GHZ states before measurement are stabilized by

$$K_1 = -Y_1 X_2 Y_3, \quad K_2 = Z_1 Z_2, \quad K_3 = Z_1 Z_3. \tag{13}$$

Entanglement is broken after measurement, and the stabilizers then become single-particle operators. It can be easily obtained that B_1's qubit is then stabilized by $-s_2 s_3 Y$, where s_2 and s_3 are measurement outcomes of B_2 and B_3. Results of other combination of q's are presented in Table I.

Step 3. Immediately after the measurement, B_1 applies a Hadamard transformation H followed by a $\pi/4$ gate S on the GHZ state qubit in order to transform the eigenstates of X to that of Z and eigenstates of Y to that of X, with the same

TABLE I. Tables of stabilizers in different cases of q_i's. K_1 is the stabilizer of the GHZ state compatible with the measurement basis. K_1'', K_2'', and K_3'' are stabilizers after the measurement according to the cheating scheme.

q_2	q_3	K_1	K_2''	K_3''	K_1''
0	0	$X_1 X_2 X_3$	$s_2 X_2$	$s_3 X_3$	$s_2 s_3 X_1$
0	1	$-Y_1 X_2 Y_3$	$s_2 X_2$	$s_3 Y_3$	$-s_2 s_3 Y_1$
1	0	$-Y_1 Y_2 X_3$	$s_2 Y_2$	$s_3 X_3$	$-s_2 s_3 Y_1$
1	1	$-X_1 Y_2 Y_3$	$s_2 Y_2$	$s_3 Y_3$	$-s_2 s_3 X_1$

eigenvalues. Now it can be observed that if $q_2 + q_3$ is even, B_1 will have a qubit in the Z basis; otherwise, he will have a qubit in the X basis. At the same time $t = (d - l)/c$, and B_1 also receives the encoded qubit sent from V_1, so he has two qubits on hand that are parallel or antiparallel, i.e., the two qubits are simultaneous eigenstates of either the Pauli X or Z operator. B_1 performs a Bell measurement and obtains one of the four outcomes in Eqs. (3) and (7)–(9).

Step 4. The cheaters share their measurement outcome and basis information with others. Since the mutual distance among B_1, B_2, and B_3 is $\sqrt{3}l$, the cheaters can obtain all the information at $t = [d + (\sqrt{3} - 1)l]/c$. From the information of B_2 and B_3, the actual state of the GHZ state qubit of B_1 is known from Table I. The outcome of the Bell measurement can tell the parity of the two qubits of B_1, and the state of the encoded qubit is obtained.

Step 5. The correct result is then sent by the cheaters and reaches the reference stations at $t = [2d + (\sqrt{3} - 2)l]/c$. When compared to the case without cheaters that the whole PBQC process is expected to finish at $t = 2d/c$, our cheating scheme eventually requires less time to produce the correct result. Cheaters can simply delay for a while before broadcasting their final outcomes in order to match the time consumption in the honest case. Hence the protocol is cheated.

We note that the time is shortened because information takes $2l/c$ time to travel from B_1's position to B_2's position in the honest case, while only $\sqrt{3}l/c$ is needed if there are cheaters. In general, if the geometry is not an equilateral triangle, our cheating scheme may still process faster than in the honest case, provided that P is not on the same straight line as any two reference stations. This is because honest information has to be sent from a vertex to the center of the triangle where P locates and then be rebroadcast to another vertex, while information of cheaters is transmitted along edges of the triangle.

Our cheating scheme can be generalized to cases with $N > 3$ reference stations; we need at most N cheaters in each case. Before the PBQC starts, the cheaters create a N-particle GHZ state which is stabilized by

$$K_1 = X_1 X_2 \cdots X_N, \quad K_i = Z_{i-1} Z_i, \tag{14}$$

for $i = 2,3,\ldots,N$; the subscripts of Pauli operators denote the order of qubits. Each cheater B_i picks a qubit and travels to a position between P and V_i. When $B_2,\ldots,B_N$ receives the basis information, they measure their qubit in the X basis if $q_i = 0$ or the Y basis if $q_i = 1$ and broadcast the results. If even number of q's are equal to 1, the qubit of B_1 is in the X basis; otherwise, it changes to the eigenstate of the Y basis. In the former case, the Y measurement must be performed in pairs. Consider $q_i = 1$ at position m and n; we must be able to construct a stabilizer $K_1' = K_1 K_{m+1} K_{m+2} \cdots K_n = -X_1 \cdots Y_m \cdots Y_n \cdots$ which is compatible to the measurements such that the qubit of B_1 remains at the X basis after the measurement. Otherwise, there is one single Y measurement at position r; the compatible stabilizer becomes $K_1' = K_1 K_2 \cdots K_r = -Y_1 \cdots Y_r \cdots$, and the qubit of B_1 has changed to the eigenstate of the Y basis.

Identical to the $N = 3$ case, B_1 applies an SH gate onto his cluster state qubit; he then obtains an eigenstate of the X operator if q is odd or an eigenstate of the Z operator if q is even. He then measures the cluster state qubit and encoded qubit sent from V_1 by the Bell measurement and broadcasts the measurement outcome. In the present case of $N > 3$, cheaters do not receive all the information at the same time, but it is easy to check that even the slowest piece of information should arrive as late as in the honest case. The information provided by $B_2,\ldots,B_N$ determines the actual state of the GHZ state qubit of B_1, and the measurement of B_1 reveals the parity between his two qubits. Hence the value of the encoded qubit is obtained and the cheaters have sent the results to reference stations. The whole process takes less time than or the same amount of time as does the honest case.

B. Cheating against Protocol B in $N > 2$ case

In this protocol, 3 bits of information are encoded as one of the eight tripartite GHZ-type states [18] characterized by parameters b_1,b_2,b_3

$$\left|\Phi_{b_1 b_2 b_3}\right\rangle = \frac{1}{\sqrt{2}}(|a_1\rangle|a_2\rangle|a_3\rangle \pm |1 \oplus a_1\rangle|1 \oplus a_2\rangle|1 \oplus a_3\rangle), \tag{15}$$

where $a_1,a_2,a_3,b_1,b_2,b_3 \in \{0,1\}$; $(-1)^{b_1} = \pm 1$ is the phase between two superposition states, $b_2 = a_1 \oplus a_2$ and $b_3 = a_1 \oplus a_3$. The qubits are then distributed to reference stations, and we denote the qubit held by V_i as qubit i. Qubit i is encrypted by the arbitrary local transformation U_i and sent to P subsequently. The PBQC scheme starts at $t = 0$ when reference stations send information of U_i to P; the correct response should return at $t = 2d/c$. We find that three cheaters are enough to cheat perfectly in this case. The idea is the same as in the $N = 2$ case, which is to teleport all qubits to one cheater so he can conduct an N-particle GHZ-type state measurement. The cheating strategy is as follows.

Step 1. Before they have traveled to their desired positions, $B_2(B_1)$ picks qubit 4 (5), and $B_3(B_1)$ picks qubit 6(7), where qubits 4, 5, 6, and 7 are Bell states in Eq. (3).

Step 2. The cheaters break into the quantum channel connecting V_i and P and capture the encrypted qubits. We call the qubit captured by B_1 qubit i. At $t = (d - l)/c$, cheaters receive information of U_i and a corresponding decryption procedure is made to obtain the original encoded state.

Step 3. Immediately after the decryption, B_2 and B_3 conduct a Bell measurement for teleportation. Afterward, the state is stabilized by

$$\begin{gathered} K_1' = (-1)^{b_1} s_2 s_3 X_1 X_5 X_7, \\ K_2' = (-1)^{b_2} s_4 Z_1 Z_5, \quad K_3' = (-1)^{b_3} s_6 Z_1 Z_7, \\ K_4' = s_2 X_2, \quad K_5' = s_4 X_4 \\ K_6' = s_3 X_3, \quad K_7' = s_6 X_6. \end{gathered} \tag{16}$$

It is easy to verify from Eq. (16) that qubits 1, 5, and 7 become a GHZ-type state $|\Phi_{b_1' a_2' a_3'}\rangle$, where $b_1' = b_1 \oplus (1 - s_2 s_3)/2$, $b_2' = b_2 \oplus (1 - s_4)/2$, and $b_3' = b_3 \oplus (1 - s_5)/2$. So B_1 can conduct a GHZ-state measurement to reveal the residual state exactly. The result is sent to other cheaters.

Step 4. In our equilateral triangle case, information exchange among cheaters is finished at $t = [d + (\sqrt{3} - 1)l]/c$. The encoded message b_1, b_2, b_3 can easily be inferred from the measuring outcomes. Correct results are sent to reference stations, and the whole process can be finished as early as $t = [2d + (\sqrt{3} - 2)l]/c$, which is even shorter than in the honest case. If the three stations do not form an equilateral triangle, the time required by cheating is longer. But the time consumption is in general less than $2d/c$ for any three-station scenario; PBQC is hence cheated.

V. PRINCIPLE OF THE CHEATING SCHEMES

A. Protocol A

We have verified that our cheating strategy works not only for qubits encoded in BB84 states (eigenstates of X and Z operators) but also if eigenstates of both Pauli X, Y, and Z can be chosen for encoding. In the one-dimensional case, the same cheating scheme can be applied as described in Sec. III B. What are the ideas here? An idea is that the teleported state will be transformed by one of the four operators I, X, Z, and XZ. Now, if the input state is an eigenstate of the X, Y, or Z operator, then the output state will be either the same as or opposite to the input state (up to an irrelevant overall phase). Another idea is that a Bell measurement by B_1 allows him to check the parity of the operators XX, YY, and ZZ simultaneously as the three operators commute with each other.

In the case of more than two reference stations, we have to modify our quantum secret-sharing cheating strategy. It is because quantum secret sharing can only allow conversion between two basis, while we need switching between the three basis in this six states protocol. Cheating can be achieved by cluster state quantum computation (CSQC) [23]. Instead of an N-particle GHZ state, the cheaters shares a $(4N-3)$-particle chain cluster state. B_1 picks a qubit on the end of the chain, while other cheaters pick four consecutive qubits from the chain. As stated in Ref. [23], each cheater can conduct a general rotation by measuring three qubits in the appropriate direction, while the last qubit is measured in the X basis to teleport the state to the next cheater. Finally, the cluster-state qubit of B_1 lies in the same basis as the incoming qubit, and he can conduct Bell measurement as before. It is noted that all cluster-state qubit measurements can be conducted at the same time; the sequence of the measurement among cheaters is unimportant. It is because all measurements are local operations and obviously independent of each other. We also note that the quantum secret sharing and quantum teleportation mentioned before are special cases of CSQC. In fact, CSQC is a more general concept, so we will analyze our cheating scheme under this formalism.

We find that two characteristics of eigenstates in the X, Y, and Z basis leave the possibility for our cheating. First, the conversion between them (H is the transformation between X states and Z states; S is the transformation between X states and Y states) are Clifford operators. Recall in the $N = 2$ case that we have pulled the H gate from Eq. (4) to the front in Eq. (6), and let the Pauli operators applying on the Z states before the gate. Since the basis of Pauli states are not changed by Pauli operators, the action of the transformation gate is not altered and hence the teleported state is in the same basis as the original qubit. In $N > 2$ cases, we refer to the general rotation operation of CSQC [23],

$$|\psi_{\text{out}}\rangle = \prod_{i=2}^{N} U_{\Sigma_i} U_i |\psi_{\text{in}}\rangle, \quad (17)$$

where $|\psi_{\text{out}}\rangle$ is the cluster-state qubit held by B_1; $|\psi_{\text{in}}\rangle$ can be treated as $|0\rangle$ in our case; U_i is the rotation induced by the cluster-state measurement (in our case it is performed by B_i to conduct rotation hinted by the message of V_i); and $U_{\Sigma_i} = X^i Z^i$ is the by-product of the random measurement outcome of the i-th qubit. It is transparent that if all U_i are Clifford operators, Eq. (17) becomes

$$|\psi_{\text{out}}\rangle = U U_{\Sigma} |0\rangle = e^{i\phi} U |0 \text{ or } 1\rangle, \quad (18)$$

where U is the product of all U_i, which is the complete encoding transformation separated beforehand in this protocol. U_Σ is a product of Pauli operators; its form depends on U_{Σ_i} as well as on the commutating relation between U_{Σ_i} and U_i. $e^{i\phi} = \{\pm 1, \pm i\}$ is the phase generated by $U_\Sigma|0\rangle$, and the state $|0\rangle$ can only flip to $|1\rangle$ or remain unchanged upon U_Σ.

The cluster-state qubit of B_1 is hence parallel or antiparallel to the encoded qubit, and B_1 can obtain information of the unknown qubit by checking the parity of his qubits on hand, if such a parity-checking measurement exists. For eigenstates of Pauli operators, the parity of two qubits in the same basis can be checked by the Bell measurement, which is the second key point to our cheating scheme. We illustrate this idea using the BB84 states and leave interested readers to verify the Y states. If both qubits of B_1 are in the Z basis, only $|\Phi_{00}\rangle$ and $|\Phi_{01}\rangle$ contain even-parity states and odd-parity states appear in $|\Phi_{10}\rangle$ and $|\Phi_{11}\rangle$ only, whereas if they are in the X basis, only $|\Phi_{00}\rangle$ and $|\Phi_{10}\rangle$ contain even-parity states and odd-parity states appear in $|\Phi_{01}\rangle$ and $|\Phi_{11}\rangle$ only. It can be seen that even- and odd-parity states do not appear in the same Bell states, hence cheaters can infer the parity of qubits of B_1 by the Bell measurement result. Furthermore, cheaters know the exact form of cluster state qubit of B_1; the qubit is then revealed by the parity.

B. Protocol B

This protocol is once believed to be secure. The argument is based on the quantum no-cloning theorem [18]. But it is not necessary to clone the state perfectly in order to conduct a perfect measurement. The problem of Protocol B is that the message is encoded in GHZ states, where each code is related to every other by bit flips and an overall phase flip only. Since the random by-product of our teleportation scheme is single-particle X and Z operators, an encoded state must be mapped to another code state after teleportation. As a result, a standard decoding procedure can read out the teleported state perfectly.

VI. MODIFIED PBQC SCHEME

In Sec. V, we have discussed that Protocol A is insecure because the qubit is encoded as eigenstates of X or Z such that the basis of state does not change on teleportation or cluster-state manipulation. And we are able to reveal the parity of two particles if they are in the X or Z basis. Notice, however, that if one modifies a protocol to allow more general bases other than the X, Y, and Z bases, then our cheating strategy does not generally work, in the sense that B_1 may not be able to find an appropriate basis to measure the teleported qubits perfectly. This is because the by-product of random measurement outcomes of teleportation may map the encoded state into a state that is no longer a code. In fact, our cheating scheme fails if references encoded the 2-bit message as the states $\{|00\rangle,(|01\rangle \pm |10\rangle)/\sqrt{2},|11\rangle\}$ in the one-dimensional case. It is easy to check that the by-products of teleportation do not necessarily map a code state to a code state.

Another protocol that is resistant to our teleportation attack is a natural extension to Protocol A. A message is encoded as ± 1 eigenstates of $\hat{n}(\theta,\phi)\cdot\vec{\sigma}$

$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + \sin\frac{\theta}{2}e^{i\phi}|1\rangle, \tag{19}$$

$$|\bar{\psi}\rangle = \sin\frac{\theta}{2}|0\rangle - \cos\frac{\theta}{2}e^{i\phi}|1\rangle, \tag{20}$$

where $0 \leqslant \theta \leqslant \pi$ and $0 \leqslant \phi \leqslant 2\pi$, $\vec{\sigma} = X\hat{x} + Y\hat{y} + Z\hat{z}$ is the Pauli vector. Such a modified protocol was also proposed in Ref. [17].

In the $N = 2$ case, reference stations V_1 and V_2 are assumed to connect with a secret channel, such as a quantum channel for QKD. Although only finite bits can be communicated through QKD, random θ and ϕ can be generated by various methods. One example is to make use of the universality of quantum computation, where arbitrary qubits can be constructed by sequences of Clifford operators plus a $\pi/8$ gate [18,21]. A random sequence of "0" and "1" is generated by V_1 and sent to V_2. Each "0" represents an operation of Hadamard gate H, while a "1" represents an operation of $\pi/8$ gate T, applying on the state $|u\rangle$ encoded with a bit $u \in \{0,1\}$ [18]. For example, if the the sequence "01011" is sent, the encrypted state is given by $HTHTT|u\rangle$.

The idea can be generated to $N > 2$ cases. Each of the verifiers are connected to V_1 with QKD channels for communication of arbitrary rotation U_i. The encrypted qubit sent from V_1 to P is $U_2\cdots U_N|u\rangle$, while reference stations $V_2\cdots V_N$ send information of rotation U_i.

It is not difficult to check that our modified protocol is immune to our original cheating strategy demonstrated in Secs. III and IV. In the $N = 2$ case, B_1 captures the state $|\psi\rangle$ in Eq. (19) sent from V_1 at $t = (d - l)/c$ and teleports it to B_2 immediately. Although B_2 knows the basis from V_2, it can be shown that the teleported state can be neither parallel nor antiparallel with the original one, i.e., for s_1 and s_2 not equal to 1, the matrix element

$$\langle\psi|X^{(1-s_2)/2}Z^{(1-s_1)/2}|\psi\rangle \neq 0 \text{ or } 1. \tag{21}$$

Therefore B_2 cannot find a basis to measure the qubit always perfectly without knowing measurement outcomes from B_1. Message of B_1 arrives B_2 as soon as $t = (d + l)/c$. Even if B_2 measures the qubit immediately, correct feedback will reach V_1 no earlier than $t = 2(d + l)/c$, which costs more time than expected. Security of PBQC is hence enforced.

In the case of more reference stations, U_i's do not belong to the Clifford group; it precludes the encrypted state to transform from Eqs. (17) to (18). As in the one-dimensional case, B_1 cannot perform a perfect measurement until the random outcomes of cluster-state measurements are known. But the location where all information can reach each other in the shortest time is inside the restricted area of P; in other words, the cheaters need more time than in the honest case to get the correct result. Security of PBQC is hence enforced.

In practice, the quantum operations, quantum channel, and measurements are not noiseless; the incorrect response can be given even in the honest case. The total key rate of practical PBQC systems ought to be higher than the successful cheating rate, i.e., the probability of producing correct feedback by cheaters. Otherwise, failure of cheating may be regarded as error caused by noise, and the PBQC scheme hence becomes insecure.

We now discuss the successful cheating rate of our protocol under various cheating schemes in the one-dimensional case. First, we consider that B_1 simply measures the qubit and announces the result. It is equal to the average value of $|\langle 0|\psi\rangle|^2$ for any θ and ϕ. The successful rate is obviously 50%, as it does not differ from a random guess. Next, we consider that B_1 measures the qubit but announces until basis information from B_2 is obtained. The successful rate is 75%. It is more than a random guess, because for $\theta < \pi/2$, B_1's measurement outcome is more probably correct, while it is more probably wrong if $\theta > \pi/2$. B_1 can announce the inverse of his measurement outcome for $\theta > \pi/2$ case, successful rate is then increased. Finally, we consider our teleportation cheating scheme. B_2 measures the teleported state in Fig. 3 by basis states $\{|\psi\rangle,|\bar{\psi}\rangle\}$. Consider if the result is $|\psi\rangle$. After knowing s_2 and s_3, the cheaters announce the more probable correct result, i.e.,

$$|v\rangle = \{|\psi\rangle,|\bar{\psi}\rangle|\max(|\langle\psi|X^{(1-s_2)/2}Z^{(1-s_1)/2}|v\rangle|^2)\}. \tag{22}$$

The average successful rate is

$$\begin{aligned}\tfrac{1}{4}\int[1 &+ \max(|\langle\psi|X|\psi\rangle|^2,|\langle\psi|X|\bar{\psi}\rangle|^2)\\ &+ \max(|\langle\psi|Z|\psi\rangle|^2,|\langle\psi|Z|\bar{\psi}\rangle|^2)\\ &+ \max(|\langle\psi|XZ|\psi\rangle|^2,|\langle\psi|XZ|\bar{\psi}\rangle|^2)]d\Omega,\end{aligned} \tag{23}$$

which is about 85%. We have checked numerically that 85% is the highest successful rate that can be achieved for any measurement basis used by B_2. In the case of more reference stations, cluster-state quantum computation requires more measurements. So there are more random by-products and the successful rate is anticipated to be lower than $N = 2$ case.

It is noted that Chandran *et al.* suggests B_1 can entangle the encoded qubit with his quantum memory and then sends one to B_2 [13]. Since the quantum systems are entangled, any measurement of B_1 will leave B_2 a mixed state. B_1 has to announce a response before knowing measurement result of B_2; otherwise, the operation time must exceed that allowed by the PBQC scheme. But the measurement outcome of B_2 is probabilistic; if B_2 makes a response according to this, there is the probability that the response received by V_1 and V_2 will be inconsistent. This kind of inconsistency reveals there must be cheaters lying in between, because noisy operations in the honest case do not produce inconsistent results. So neither B_1 nor B_2 should do any measurement, because the cheaters are not benefited by the quantum memory.

VII. SECURITY OF MODIFIED PROTOCOL

So far we have demonstrated how our modified PBQC protocol remains secure against the teleportation-based cheating scheme. It is interesting to know whether the protocol is secure if other kinds of entangled qubits are shared among cheaters and if a strategy other than teleportation is employed.

Recall that in the $N = 2$ case, we first teleport the unknown encoded state from B_1 to B_2 for measurement, whereas in the $N > 2$ case we use secret sharing ideas to send a share of the basis information to B_1 through cluster state quantum computation, parity of the cluster state qubit and encoded qubit is then checked. Although seemingly different cheating strategy is taken in one dimensional and $N > 2$ cases, they are actually the same in principle. This is because the measurements of cheaters are local and thus independent of each other. Time order of the measurement is unimportant; all cheaters conduct their operation immediately after receiving information from reference stations. It is easy to see that measurement of a cluster state by B_2 in the $N = 2$ case actually uses secret sharing ideas to send a share of the basis information to B_1, while the entanglement operation and X basis measurement of B_1 is equivalent to some parity-checking procedure.

We first consider the $N = 2$ case. Suppose a general two-qubit entangled state is shared among cheaters, which would become any set of states containing basis information after measurements of B_2. If the encoded qubit is in the Z basis, we assume without loss of generality that B_2 makes an measurement to "send" states $|\tilde{0}\rangle$ and $|\tilde{1}\rangle$ to B_1. In general, the states B_1 obtained from B_2 are

$$\begin{aligned} |\tilde{\uparrow}\rangle &= g(\theta,\phi)|\tilde{0}\rangle + h(\theta,\phi)|\tilde{1}\rangle \\ |\tilde{\downarrow}\rangle &= h^*(\theta,\phi)|\tilde{0}\rangle - g^*(\theta,\phi)|\tilde{1}\rangle, \end{aligned} \tag{24}$$

where g,h are functions of basis information of B_2. Here we have assumed that $|\tilde{\uparrow}\rangle$ and $|\tilde{\downarrow}\rangle$ are orthogonal, and a successful rate of cheating decreases in the nonorthogonal case. It is noted that the probability of $|\tilde{\uparrow}\rangle$ or $|\tilde{\downarrow}\rangle$ appearing is the same as 0.5, otherwise causality is violated. After the measurement, B_2 transmits classical information on the basis of the encoded qubit, the basis of the measurement on the entangled state, and the measurement outcomes to B_1.

In the Z-basis case, in order to distinguish $|0\rangle$ and $|1\rangle$ after obtaining information from B_2, B_1 conducts a von Neumann measurement with basis

$$\begin{aligned} |M_1\rangle &= \alpha|0\rangle|\tilde{0}\rangle + \beta|1\rangle|\tilde{1}\rangle, |M_2\rangle = \beta^*|0\rangle|\tilde{0}\rangle - \alpha^*|1\rangle|\tilde{1}\rangle \\ |M_3\rangle &= \gamma|0\rangle|\tilde{1}\rangle + \delta|1\rangle|\tilde{0}\rangle, |M_4\rangle = \delta^*|0\rangle|\tilde{1}\rangle - \gamma^*|1\rangle|\tilde{0}\rangle, \end{aligned} \tag{25}$$

where the coefficients $\alpha,\beta,\gamma,\delta$ characterize the measurement. The states are set as above such that every $|\tilde{0}\rangle$ and $|\tilde{1}\rangle$ associate with either $|0\rangle$ or $|1\rangle$. Otherwise, if $|M_i\rangle$ contains terms like $(|0\rangle + |1\rangle)|\tilde{1}\rangle$, B_1 cannot reveal the identity of the encoded qubit after communicating with B_2.

Since B_1 knows nothing about the basis, he always conducts the same measurement in Eq. (25). For general θ and ϕ, B_1 gets one of the four states

$$\{|\psi\rangle|\tilde{\uparrow}\rangle, |\psi\rangle|\tilde{\downarrow}\rangle, |\bar{\psi}\rangle|\tilde{\uparrow}\rangle, |\bar{\psi}\rangle|\tilde{\downarrow}\rangle\}. \tag{26}$$

An important observation is that the cheaters are able to distinguish the encoded qubit, only if every measurement state $|M_i\rangle$ contains components of $|\tilde{\uparrow}\rangle$ and $|\tilde{\downarrow}\rangle$ associated with either $|\psi\rangle$ or $|\bar{\psi}\rangle$ only. This statement can be reformulated to say that each state in Eq. (26) is a superposition of at most two states in Eq. (25).

We expand $|\psi\rangle|\tilde{\uparrow}\rangle$ as

$$\begin{aligned} |\psi\rangle|\tilde{\uparrow}\rangle = {}& \cos\frac{\theta}{2}g(\theta,\phi)|0\rangle|\tilde{0}\rangle + \cos\frac{\theta}{2}h(\theta,\phi)|0\rangle|\tilde{1}\rangle \\ & + \sin\frac{\theta}{2}e^{i\phi}g(\theta,\phi)|1\rangle|\tilde{0}\rangle + \sin\frac{\theta}{2}e^{i\phi}h(\theta,\phi)|1\rangle|\tilde{1}\rangle. \end{aligned} \tag{27}$$

Without loss of generality, we assume it is a superposition of $|M_1\rangle$ and $|M_3\rangle$, imposing the relations

$$\cot\frac{\theta}{2}e^{-i\phi}\frac{g}{h} = \frac{\alpha}{\beta}, \quad \cot\frac{\theta}{2}e^{-i\phi}\frac{h}{g} = \frac{\gamma}{\delta}. \tag{28}$$

Similarly, we expand $|\bar{\psi}\rangle|\tilde{\downarrow}\rangle$

$$\begin{aligned} |\bar{\psi}\rangle|\tilde{\downarrow}\rangle = {}& \sin\frac{\theta}{2}h^*(\theta,\phi)|0\rangle|\tilde{0}\rangle - \sin\frac{\theta}{2}g^*(\theta,\phi)|0\rangle|\tilde{1}\rangle \\ & - \cos\frac{\theta}{2}e^{i\phi}h^*(\theta,\phi)|1\rangle|\tilde{0}\rangle + \cos\frac{\theta}{2}e^{i\phi}g^*(\theta,\phi)|1\rangle|\tilde{1}\rangle. \end{aligned} \tag{29}$$

It has to be the superposition of either $|M_1\rangle$ and $|M_3\rangle$ or $|M_2\rangle$ and $|M_4\rangle$; otherwise, an unphysical result $\langle\psi\tilde{\uparrow}|\bar{\psi}\tilde{\downarrow}\rangle \neq 0$ is yielded.

We first consider $|\bar{\psi}\tilde{\downarrow}\rangle$ is a superposition of $|M_2\rangle$ and $|M_4\rangle$. The following relations has to be satisfied

$$\cot\theta e^{-i\phi}\frac{g}{h} = -\frac{\alpha}{\beta}, \quad \cot\theta e^{-i\phi}\frac{h}{g} = -\frac{\gamma}{\delta}. \tag{30}$$

Together with Eq. (29), $\alpha,\delta,g(\theta,\phi)$ ought to be zero. This implies B_2 always sends $|\tilde{0}\rangle$ and $|\tilde{1}\rangle$ to B_1, and the basis of B_1 measurement is four untangled states, i.e., two single-qubit measurements. It can be readily seen that both $|\psi\rangle|\tilde{0}\rangle$ and $|\bar{\psi}\rangle|\tilde{0}\rangle$ contain components of $|M_2\rangle$, hence the cheaters cannot distinguish $|\psi\rangle$ and $|\bar{\psi}\rangle$ after communication.

Now we consider $|\bar{\psi}\tilde{\downarrow}\rangle$ is a superposition of $|M_1\rangle$ and $|M_3\rangle$, imposing the relations

$$\tan\frac{\theta}{2}e^{-i\phi}\frac{h^*}{g^*} = \frac{\alpha}{\beta}, \quad \tan\frac{\theta}{2}e^{-i\phi}\frac{g^*}{h^*} = \frac{\gamma}{\delta}. \tag{31}$$

Together with Eq. (29), we have

$$\frac{|g|^2}{|h|^2} = \tan^2\frac{\theta}{2}, \quad \frac{|h|^2}{|g|^2} = \tan^2\frac{\theta}{2}, \tag{32}$$

which can only be satisfied for $\theta = \pi/2$ but not for general θ. We therefore conclude that our protocol is unbreakable no matter what two-qubit state is shared among cheaters and what strategy the cheaters employ. We would like to comment on the case of $\theta = \pi/2$ case; it means that the basis for encoding is perpendicular in the Bloch sphere. There are only three mutually perpendicular directions in the Bloch sphere, which can be regarded as the X, Y, and Z directions. It explains why our cheating works for and only for states encoded in eigenstates of Pauli X,Y,Z operators.

In the case with $N > 2$ reference stations, we can prove by contradiction that our scheme is secure for any N-qubit states shared by the cheaters using any strategy. Let the maximum mutual distance between reference stations be $2d$, and we denote the two maximally separated reference stations as V_1 and V_2. Assume P lies in the middle such that the minimum time required for PBQC scheme is $t = 2d/c$ and further that the restricted area of P is so large that the N cheaters have to sit very close to each reference station. The minimum time required for information exchange among cheaters is $t = 2d/c$. Now suppose there exists a strategy to cheat successfully for any θ,ϕ with any U_i distributed to V_i. Consider the case that $U_3,\ldots,U_N$ are identity operators, in other words the basis information is contained in U_2 only. After measurement of $B_3,\ldots,B_N$, the situation reduces to the one-dimensional case, which cannot be cheated as proved above. Therefore a perfectly successful strategy for $N > 2$ reference stations does not exist.

In general, the cheaters can share more complicated quantum resources than entangled qubits. If two qubits belonging to an entangled network, such as a 2D cluster state, are possessed by each cheaters, it has to be treated as an entangled four-level system, which is not covered in our proof. A PBQC protocol is unconditionally secure if and only if cheating cannot succeed with certainty no matter what entangled resources is shared among cheaters, and what strategy they take. We provide in the appendix the proof that our protocol is still secure if the entangled three-level system is shared among cheaters.

VIII. SUMMARY

We have shown how entangled resources can help to cheat the two proposed PBQC protocols. The idea is to use teleportation, quantum secret sharing, or CSQC to share part of the quantum information among cheaters, whereby measurement can be conducted before all information is known. Subsequent exchange of classical information allows for correction due to the random measurement outcomes.

Our cheating scheme is successful because random by-products of teleportation, quantum secret sharing, or CSQC are Pauli operators. They do not map any code state out of the code space. The loophole can be fixed by using non-Clifford states to encode the message. Based on this idea, we propose a modified version of Protocol A in which the code space spans the Bloch sphere. Our protocol is proved to be secure if each cheater shares entangled qubits or qutrits (such as particle composites with effective spin 1). The highest average successful rate of cheating our protocol is 75% if no entangled resource is used, and 85% if our cheating scheme is employed.

In this article, we consider protocols only in which the verified receiver knows nothing except the publicly known method of decoding (i.e., rules of measuring incoming qubits according to incoming classical messages). An intriguing question is how PBQC becomes more secure if some resources are shared by the authorized receiver and reference stations, instead of communicating all information through public channels. Recently, Kent [24] has proposed a PBQC scheme that can be proved to be perfectly secure, provided that P and reference stations preshare a sequence of bits that cannot be obtained by cheaters. In addition, Malaney has also considered a protocol in which entangled pairs are shared beforehand among P and reference stations [19]. In that case, encoded qubits can be teleported to the authorized receiver, which eliminates the possibility that encoded qubits are captured by cheaters. We believe, in general, that an authorized receiver can make use of shared resources to set up secret keys with reference stations for message encoding. Cheaters without information of the keys cannot obtain any knowledge of the message, and thus this class of PBQC schemes should be secure.

Finally, we have assumed in the above consideration that all operations are performed extremely fast compared to the traveling time of signals. To verify the possibility of PBQC in practice, we consider the distance between reference stations at the order of 100 km and the size of the restricted area of P to be 1 km. A round trip of signals takes around 100 μs, and the presence of cheating will give a deviation for about 1% of time, which is microseconds in scale. Considering that recent experiments on optical quantum computation are operating on nanosecond scales [25], the assumption of fast operation is still valid.

Note added in proof Recently, Buhrman *et al.* [26] proposed a rather general cheating strategy based on the nonlocal measurement scheme of Vaidman [27]. By applying their strategy, all PBQC protocols without preshared resources, including our modified protocols described in Sec. VI of the current article, can be cheated with arbitrary accuracy. However, the required amount of entanglement and rounds of operations scale exponentially as the number of encoded qubits, n, involved in a PBQC protocol. In addition, the average entanglement consumption for exact cheating is infinite even for simple protocols involving one encoded qubit only. Although the efficiency of the general cheating strategy can be enhanced [26] by keeping track of the effect of the teleportation by-products on the encoding transformation U [28], the average entanglement required still depends exponentially on the parameters of the protocol. So, the next interesting open problem is to improve the efficiency of the general cheating strategy. The security proof in Sec. VII of the current article has put a lower bound on the required entanglement to be entanglment of four-level systems, e.g., two pairs of entangled qubits. We believe the bound is not tight. At the least, we cannot find a method to cheat our modified protocol with two shared EPR pairs only. Can we raise the lower bound by introducing some protocols that cannot be cheated by any entangled four-level system? Or is there any *efficient* general cheating strategy in the sense that it consumes only a polynominal number of e-bits as a function of the number of encoded qubits? We are currently working on answers to these questions.

ACKNOWLEDGMENTS

We thank Marcos Curty for bringing the subject of position-based quantum cryptography to our attention. His enlightening discussions started our investigation. We also thank numerous colleagues, including Harry Buhrman, Eric Chitambar, Serge Fehr, Andrian Kent, Robert Malaney, Bill Munro, Renato Renner, and Barry Sanders for useful conversations. We thank funding agencies and programs including NSERC, CIFAR, QuantumWorks, and Canada Research Chair program for financial support.

APPENDIX: SECURITY OF SHARED THREE-LEVEL SYSTEM

Here we outline the proof of security of our protocol if an entangled three-level system is shared among two cheaters in a one-dimensional case. This guarantees the security in cases involving $N > 2$ reference stations, of which the one dimensional case can always be regarded as a special case, as claimed in Sec. VII.

First, we investigate the properties of the entangled n-level system if the cheating is successful with certainty. We again assume B_2 can make a measurement such that B_1 will receive one of n orthogonal states with equal probability. The choice of orthogonal states incorporates information about the basis of encoded qubit. If the encoded qubit is an eigenstate of Z, we let B_1 receive a state belonging to $\{|\phi_1\rangle, \ldots, |\phi_n\rangle\}$. Define a vector $(|\vec{\phi}\rangle) \equiv (|\phi_1\rangle \cdots |\phi_n\rangle)^T$ such that if the encoded qubit is an eigenstate of $\hat{n}(\theta,\phi) \cdot \vec{\sigma}$, B_1 will receive an element of the vector $\hat{T}(\theta,\phi)(|\vec{\phi}\rangle)$, where $\hat{T}(\theta,\phi)$ is an $n \times n$ unitary matrix freely chosen by B_2.

Let the basis of B_1's measurement operator is $\{|M_1\rangle, \ldots, |M_n\rangle\}$. In order to distinguish the identity of encoded qubit after exchanging information with B_2, each state $|M_i\rangle$ should not contain components of both $|\phi_j\rangle|0\rangle$ and $|\phi_j\rangle|1\rangle$ for any j. Define a selection matrix $S^{(i)}$ which is an diagonal matrix with eigenvalues 1 and 0 only, such that $S^{(i)}_j j = 1$ if $|M_i\rangle$ contains component of $|\phi_j\rangle|0\rangle$; while $S^{(i)}_j j = 0$ if $|M_i\rangle$ contains component of $|\phi_j\rangle|1\rangle$. The states $|M_i\rangle$ can be written as

$$|M_i\rangle = \sum_{j,j'} \left(\alpha_{ij'} S^{(i)}_{j'j}|\phi_j\rangle|0\rangle + \alpha_{ij'}\left(I - S^{(i)}_{j'j}\right)|\phi_j\rangle|1\rangle\right), \quad \text{(A1)}$$

where $|\alpha_{i1}|^2 + \cdots + |\alpha_{in}|^2 = 1$; I is the $n \times n$ identity matrix. Since B_1 knows nothing about the basis, his measurement is always the same. Similar to the argument above, if B_1 is able to distinguish $|\psi\rangle$ and $|\bar{\psi}\rangle$ after information exchange, $|M_i\rangle$ has to be

$$|M_i\rangle = \sum_{k,k',j} \left(\beta_{ik}\tilde{S}^{(i)}_{kk'}\hat{T}_{k'j}|\phi_j\rangle|\psi\rangle + \beta_{ik}\left(I - \tilde{S}^{(i)}_{kk'}\right)\hat{T}_{k'j}|\phi_j\rangle|\bar{\psi}\rangle\right), \quad \text{(A2)}$$

where $|\beta_{i1}|^2 + \cdots + |\beta_{in}|^2 = 1$; $\tilde{S}^{(i)}$ are selection matrices. Comparing Eqs. (A1) and (A2), we get

$$\alpha_{ij}\left[\cos\frac{\theta}{2}S^{(i)}_{jj} + \sin\frac{\theta}{2}e^{i\phi}\left(I - S^{(i)}_{jj}\right)\right] = \beta_{ik}\tilde{S}^{(i)}_{kk}\hat{T}_{kj} \quad \text{(A3)}$$

$$\alpha_{ij}\left[\sin\frac{\theta}{2}S^{(i)}_{jj} - \cos\frac{\theta}{2}e^{i\phi}\left(I - S^{(i)}_{jj}\right)\right] = \beta_{ik}\left(I - \tilde{S}^{(i)}_{kk}\right)\hat{T}_{kj}. \quad \text{(A4)}$$

Summing the above two relations, and taking the scalar product of themselves, we have

$$\sum_j \alpha_{ij}\left[(1+\sin\theta)S^{(i)}_{jj} + (1-\sin\theta)\left(I - S^{(i)}_{jj}\right)\right]\alpha^*_{ij} = \sum_k \beta_{ik}\beta^*_{ik} = 1, \quad \text{(A5)}$$

where we have made use of the identities $S^2 = S$, $(I-S)^2 = (I-S)$, $S(I-S) = 0$. For $\sin\theta \neq 0$, above equation together with normalization of $|M_i\rangle$ imposes

$$\sum_j \alpha_{ij}S^{(i)}_{jj}\alpha^*_{ij} = \sum_j \alpha_{ij}\left(I - S^{(i)}_{jj}\right)\alpha^*_{ij} = \frac{1}{2}. \quad \text{(A6)}$$

This is an important relation to restrict the kind of measurement conducted by B_1. It is to say that if cheating is successful, the absolute square sum of coefficients associated with $|0\rangle$ of any state $|M_i\rangle$ has to be $\frac{1}{2}$.

Here we show that a complete set of states satisfying Eq. (A6) does not exist in the entangled three-level system case. Assume $|M_1\rangle$ consists of $\{|0\rangle|\phi_1\rangle, |0\rangle|\phi_2\rangle, |1\rangle|\phi_3\rangle\}$ with a nonzero contribution. Other $|M\rangle$ cannot be formed by combination of two $|0\rangle$ and one $|1\rangle$; otherwise, the inner product with $|M_1\rangle$ is nonzero, unless coefficient of one $|0\rangle$ is zero. We ignore this case for a while and assume other $|M\rangle$'s has to be formed by one $|0\rangle$ and two $|1\rangle$. Consider $|M_2\rangle$ share two common components as $|M_1\rangle$, for example, it contains $\{|0\rangle|\phi_1\rangle, |1\rangle|\phi_2\rangle, |1\rangle|\phi_3\rangle\}$. By completeness of the measurement states, there must be a state $|M_3\rangle$ that contains $|1\rangle|\phi_1\rangle$. But there is no state containing $|1\rangle|\phi_1\rangle$ that can both be orthogonal to $|M_1\rangle$, $|M_2\rangle$ and satisfy Eq. (A6). So $|M_2\rangle$ must contain $\{|1\rangle|\phi_1\rangle, |1\rangle|\phi_2\rangle, |0\rangle|\phi_3\rangle\}$. Since there are six orthogonal states in total, at least three of them must share the same set of components.

Consider that $|M_1\rangle, |M_3\rangle, |M_5\rangle$ contain the terms $\{|0\rangle|\phi_1\rangle, |0\rangle|\phi_2\rangle, |1\rangle|\phi_3\rangle\}$. As they have to satisfy Eq. (A6), they can be expressed as

$$|M_i\rangle = \frac{1}{\sqrt{2}}(\cos\theta_i|0\rangle|\phi_1\rangle + \sin\theta_i e^{i\mu_i}|0\rangle|\phi_2\rangle + e^{i\nu_i}|1\rangle|\phi_3\rangle). \quad \text{(A7)}$$

Since the three states are orthogonal, we require the following:

$$\cos\theta_i\cos\theta_j + \sin\theta_i\sin\theta_j e^{i(\mu_i-\mu_j)} = -e^{i(\nu_i-\nu_j)} \quad \text{(A8)}$$

for $i \neq j$. The term on the right-hand side has norm 1, which imposes constraints on the left-hand side such that

$$|M_3\rangle = \frac{1}{\sqrt{2}}(\cos\theta_1|0\rangle|\phi_1\rangle + \sin\theta_1 e^{i\mu_1}|0\rangle|\phi_2\rangle - e^{i\nu_1}|1\rangle|\phi_3\rangle). \quad \text{(A9)}$$

But one cannot find (θ_5, μ_5, ν_5) that $|M_5\rangle$ is orthogonal to $|M_1\rangle$ and $|M_3\rangle$. So three states sharing the same components of states do not exist. We now return to the case that some $|M_i\rangle$ contains only two $|0\rangle$ and one $|1\rangle$ with coefficient of one $|0\rangle$ is zero. As the coefficient is zero, it is no different to treat the component as $|1\rangle$, it will then fall into paradigm of our proof.

We have assumed in the above argument that at least one state is a superposition of three components, we now consider all states contain only two components. We find the only possible choice of states is

$$\begin{aligned}|M_{1,2}\rangle &= \frac{1}{\sqrt{2}}(|0\rangle|\phi_1\rangle \pm e^{i\mu_1}|1\rangle|\phi_2\rangle)\\ &= \frac{1}{\sqrt{2}}|\psi\rangle\left(\cos\frac{\theta}{2}|\phi_1\rangle \pm \sin\frac{\theta}{2}e^{i(\mu_1-\phi)}|\phi_2\rangle\right)\\ &\quad + \frac{1}{\sqrt{2}}|\bar{\psi}\rangle\left(\sin\frac{\theta}{2}|\phi_1\rangle \mp \cos\frac{\theta}{2}e^{i(\mu_1-\phi)}|\phi_2\rangle\right) \quad \text{(A10)}\end{aligned}$$

$$|M_{3,4}\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle|\phi_2\rangle \pm e^{i\mu_2}|1\rangle|\phi_3\rangle\right)$$
$$= \frac{1}{\sqrt{2}}|\psi\rangle\left(\cos\frac{\theta}{2}|\phi_2\rangle \pm \sin\frac{\theta}{2}e^{i(\mu_2-\phi)}|\phi_3\rangle\right)$$
$$+\frac{1}{\sqrt{2}}|\bar{\psi}\rangle\left(\sin\frac{\theta}{2}|\phi_2\rangle \mp \cos\frac{\theta}{2}e^{i(\mu_2-\phi)}|\phi_3\rangle\right) \quad \text{(A11)}$$

$$|M_{5,6}\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle|\phi_3\rangle \pm e^{i\mu_3}|1\rangle|\phi_1\rangle\right)$$
$$= \frac{1}{\sqrt{2}}|\psi\rangle\left(\cos\frac{\theta}{2}|\phi_3\rangle \pm \sin\frac{\theta}{2}e^{i(\mu_3-\phi)}|\phi_1\rangle\right)$$
$$+\frac{1}{\sqrt{2}}|\bar{\psi}\rangle\left(\sin\frac{\theta}{2}|\phi_3\rangle \mp \cos\frac{\theta}{2}e^{i(\mu_3-\phi)}|\phi_1\rangle\right), \quad \text{(A12)}$$

or some cyclic permutation of $|\phi\rangle$. On the other hand, because we have proved $|M\rangle$ cannot contain three components, each $|M_i\rangle$ should be written as

$$|M_{1,2}\rangle = \frac{1}{\sqrt{2}}(|\psi\rangle(\hat{T}_{1i}|\phi_i\rangle) \pm e^{i\nu_1}|\bar{\psi}\rangle(\hat{T}_{2i}|\phi_i\rangle)) \quad \text{(A13)}$$
$$|M_{3,4}\rangle = \frac{1}{\sqrt{2}}(|\psi\rangle(\hat{T}_{2i}|\phi_i\rangle) \pm e^{i\nu_1}|\bar{\psi}\rangle(\hat{T}_{3i}|\phi_i\rangle)) \quad \text{(A14)}$$
$$|M_{5,6}\rangle = \frac{1}{\sqrt{2}}(|\psi\rangle(\hat{T}_{3i}|\phi_i\rangle) \pm e^{i\nu_1}|\bar{\psi}\rangle(\hat{T}_{1i}|\phi_i\rangle)). \quad \text{(A15)}$$

When comparing the state associated with $|\psi\rangle$ in $|M_1\rangle$ and $|M_3\rangle$, it is clear that the expressions in Eqs. (A10)–(A12) and (A13)–(A15) cannot be equivalent. Therefore, we now can claim that B_1 cannot find a measurement such as the states $|\psi\rangle$ and $|\bar{\psi}\rangle$ after exchanging information with B_2, no matter what set of three-level states is transmitted by B_2 through the entangled resources, which proves the security of our protocol in this case.

[1] D. Mayers, J. ACM **48**, 406 (2001).
[2] H. K. Lo and H. F. Chau, Science **283**, 2050 (1999).
[3] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).
[4] C. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, 1984* (IEEE Press, New York, 1984), p. 175.
[5] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
[6] M. Hillery, V. Buzek, and A. Berthiaume, Phys. Rev. A **59**, 1829 (1999).
[7] R. Cleve, D. Gottesman, and H. K. Lo, Phys. Rev. Lett. **83**, 648 (1999).
[8] H. K. Lo and H. F. Chau, Phys. Rev. Lett. **78**, 3410 (1997).
[9] D. Mayers, Phys. Rev. Lett. **78**, 3414 (1997).
[10] H. K. Lo, Phys. Rev. A **56**, 1154 (1997).
[11] N. Chandran, V. Goyal, R. Moriarty, and R. Ostrovsky, Lect. Notes Comput. Sci. **5677/2009**, 391 (2009).
[12] See, for example [http://bbcr.uwaterloo.ca/~rxlu/sevecombib.htm] and [http://en.wikipedia.org/wiki/Vehicular_communication_systems] and references therein.
[13] N. Chandran, S. Fehr, R. Gelles, V. Goyal, and R. Ostrovsky, e-print arXiv:1005.1750 [quant-ph].
[14] W. K. Wootters and W. H. Zurek, Nature **299**, 802 (1982).
[15] D. Dieks, Phys. Lett. A **92**, 271 (1982).
[16] A. P. Kent, W. J. Munro, T. P. Spiller, and R. G. Beausoleil, US Patent No. US20067075438 (July 11, 2006).
[17] A. Kent, B. Munro, and T. Spiller, e-print arXiv:1008.2147 [quant-ph].
[18] R. A. Malaney, Phys. Rev. A **81**, 042319 (2010).
[19] R. A. Malaney, e-print arXiv:1004.4689 [quant-ph].
[20] C. H. Bennett *et al.*, Phys. Rev. Lett. **70**, 1895 (1993).
[21] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, UK, 2000).
[22] D. Gottesman, Ph.D. thesis, Caltech, 1997.
[23] R. Raussendorf, D. E. Browne, and H. J. Briegel, Phys. Rev. A **68**, 022312 (2003).
[24] A. Kent, e-print arXiv:1008.5380 [quant-ph].
[25] R. Prevedel *et al.*, Nature **445**, 65 (2007).
[26] H. Buhrman *et al.*, e-print arXiv:1009.2490 [quant-ph].
[27] L. Vaidman, Phys. Rev. Lett. **90**, 010402 (2003).
[28] S. R. Clark, A. J. Connor, D. Jaksch, and S. Popescu, New J. Phys. **12**, 083034 (2010).