Quantum dialogue by nonselective measurements

Ba An Nguyen

Institute of Physics, Vietnam Academy of Science and Technology (VAST), 18 Hoang Quoc Viet, Cau Giay, Hanoi, Vietnam
Thang Long Institute of Mathematics and Applied Sciences (TIMAS), Thang Long University (TLU), Nghiem Xuan Yem, Hoang Mai, Hanoi, Vietnam

E-mail: nban@iop.vast.vn

Received 19 February 2018
Accepted for publication 8 March 2018
Published 20 April 2018

Abstract
Unlike classical measurements, quantum measurements may be useful even without reading the outcome. Such so called nonselective measurements are exploited in this paper to design a quantum dialogue protocol that allows exchanging secret data without prior key distributions. The relevant data to be exchanged are in terms of the high-dimensional mutually unbiased bases of quantum measurements. Appropriate modes of bidirectional controlling are devised to ensure the protocol security which is asymptotic.

Keywords: quantum dialogue, mutually unbiased bases, nonselective measurement, quNit

Classification numbers: 3.00, 3.01

1. Introduction

Mankind would not be developed without communication which may be public or private. Private communication should be confidential. That is why cryptography appeared since the early period of civilization. Unconditionally secure communication can be achieved by means of the one-time pad encryption system [1], but it is inconvenient in practice. The public key encryption system [2] is practically convenient, but relies on mathematical difficulty of problems that cannot be solved efficiently within current resources, such as the hardness of discrete logarithm problems and the factorization of a large integer, so its security is unproven and seriously threatened by scalable quantum computers [3]. A potential solution is quantum cryptography [4] that relies on the laws of quantum mechanics to distribute secret keys. The essential point is the use of quantum states for cryptographic tasks. Since nature forbids perfectly duplicating data encoded in a quantum state and any attempt to read the data disturbs the quantum state, eavesdropping by an unauthorized party, if any, can be detected by the authorized parties.

Let Alice and Bob be two authorized communicating parties. If Alice wishes to securely send Bob a message she must, together with Bob, first run a quantum protocol (like BB84 [5] or E91 [6] or others) to generate a shared secret key. Then, Alice combines each character of her plaintext message with the corresponding character of the generated key to form the so-called ciphertext, which is sent to Bob. Bob is able to decrypt the ciphertext by the same shared key. If Alice and Bob wish to secretly exchange their messages, they need to generate and share two different secret keys, one is used for Alice-to-Bob communication while the other for Bob-to-Alice’s. Although it is absolutely secure, it requires establishing secret keys before actual encoding, sending and decoding messages. Here a question arises: can one still deliver confidential messages without a prior key distribution, as it is desirable in case of urgency? In fact, this can be done by the so-called quantum secure direct communication protocols (see, e.g., [7]). However, most of the proposed protocols for quantum secure direct communication allow only one-way communication, i.e., from a sender to a receiver. Later a quantum protocol was put forward [8, 9] that enables bidirectional communication, allowing two legitimate parties, Alice and Bob, to exchange their secret messages in a way much like a dialogue. Since then a great deal of improvements, modifications and extensions of the so-called quantum dialogue
have been made, including quantum dialogue using single photons [10, 11], quantum dialogue using entangled states and entanglement swapping [12], controlled quantum dialogue [13, 14], quantum dialogue using hyper-entanglement and Greenberger-Horne-Zeilinger states [15] against noises [16, 17], quantum dialogue with authenticated [18], quantum dialogue by continuous-variable states [19, 20], device-independent quantum dialogue [21], asymmetric quantum dialogue in noisy environment [22], semi-quantum dialogue [23] and so on.

In existing quantum dialogue protocols signals to be exchanged are encoded in type of states (e.g., by means of  \( m, n \) in Einstein–Podolsky–Rosen states [24])
\[
|\Psi_{mn}\rangle = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} (-1)^{jn} |j, j \oplus n\rangle
\]
with \( \oplus \) denoting addition modulo \( N \) and \( j \) being a state in the computational basis by
\[
|\langle n\rangle = |n\rangle\]

Preliminaries

Therefore, nonselective measurements can be exploited for signalling [25]. The bases of measurement are concerned with mutually unbiased whose properties are briefly mentioned in section 2. Section 3 presents our quantum dialogue protocol with measurement bases as signals and nonselective measurement as a tool. We then analyse security of the protocol against typical eavesdropping attacks in section 4 and conclude in the last section 5.

2. Preliminaries

Consider a quNit in an \( N \)-dimensional Hilbert space spanned in the computational basis by \( N \) orthonormal basic states \( \{|l\rangle : l = 0, 1, \ldots, N - 1; N \gg 1\} \). Let the \( N \)-dimensional Heisenberg–Weyl operators, which are natural generalization of Pauli operators \( \sigma_x \) and \( \sigma_z \), be
\[
X = \sum_{l=0}^{N-1} |l+1\rangle \langle l|,
\]
\[
Z = \sum_{l=0}^{N-1} \Omega^{|l\rangle \langle l|},
\]
with ‘+’ inside the ket denoting addition modulo \( N \) and \( \Omega = \exp(2\pi i/N) \) the complex \( N \)th root of unity. It can be proved [26] that if \( N \) is an odd prime, then there exists a complete set of \( N + 1 \) mutually unbiased bases (MUBs), each is composed of \( N \) orthonormal states which are eigenstates of the \( N + 1 \) unitary operators \( \{XZ^d|, \beta = 0, 1, \ldots, N - 1\} \) and \( Z \).

Namely, a th state \( \langle k\rangle \) of a \( \beta \)th basis can be found to be
\[
|\beta; k\rangle = \frac{1}{\sqrt{N}} \sum_{l=0}^{N-1} \Omega^{(\beta+k)l - 2k^2} |l\rangle,
\]
with
\[
s_l = \sum_{j=1}^{N-1} j = \frac{1}{2} (N - 1)(N + L - 1),
\]
and a \( k \)th state \( \langle k\rangle \) of the \( (N + 1) \)th basis (which is the computational basis whose states are the eigenstates of the operator \( Z \)) is
\[
|N; k\rangle \equiv |k\rangle.
\]

Thus, there are \( N(N + 1) \) states in total which are grouped into \( N + 1 \) bases (labelled by \( \beta = 0, 1, \ldots, N - 1 \) for the first \( N \) bases and by \( N \) for the \( (N + 1) \)th basis) each \( N \) orthonormal states (labelled by \( k = 0, 1, \ldots, N - 1 \)). In this paper, for our convenience, we make use of the Fourier-Gauss structure and adopt the form
\[
|\beta; k\rangle = \frac{1}{\sqrt{N}} \sum_{l=0}^{N-1} \Omega^{N\beta + kl} |l\rangle,
\]
which are equivalent to (3) up to the indexing of bases. It can be shown that the \( N + 1 \) bases (5) and (6) mentioned above obey the mutual unbiasedness conditions
\[
|\langle \beta'; k'|\beta; k\rangle|^2 = |\langle k'|\beta\rangle|^2 = \frac{1}{N}
\]
for any \( k, k' \) and \( \beta \neq \beta' \), as must be due to definition of MUBs [27, 28].

We can generate any state \( |\beta; k\rangle \) from a state in the computational basis \( |k\rangle \) as follows. To generate the state \( |0; k\rangle \), we apply on \( |k\rangle \) the unitary operator
\[
F = \frac{1}{\sqrt{N}} \sum_{l=0}^{N-1} \sum_{m=0}^{N-1} \Omega^{ml} |l\rangle \langle m|,
\]
which is the discrete quantum Fourier transformation [29]. In fact,
\[
F |k\rangle = \frac{1}{\sqrt{N}} \sum_{l=0}^{N-1} \sum_{m=0}^{N-1} \Omega^{ml} |l\rangle \langle m|k\rangle
= \frac{1}{\sqrt{N}} \sum_{l=0}^{N-1} \Omega^{kl} |l\rangle = |0; k\rangle,
\]
where the last equality holds thanks to equation (5). As for the \( N - 1 \) other states \( |\beta; k\rangle \) with \( \beta = 1, \ldots, N - 1 \), we apply the unitary operator [28]
\[
U = \frac{1}{\sqrt{N}} \sum_{m=0}^{N-1} \Omega^{km} |m\rangle \langle m|
\]
\( \beta \) times on the previously generated state \( |0; k\rangle \) to obtain
\[
U^\beta |0; k\rangle = \frac{1}{\sqrt{N}} \sum_{l=0}^{N-1} \sum_{m=0}^{N-1} \Omega^{2m^2 + kl} |m\rangle \langle l|
= \frac{1}{\sqrt{N}} \sum_{l=0}^{N-1} \Omega^{2\beta + kl} |l\rangle = |\beta; k\rangle,
\]
where the last equality holds thanks to equation (6) too.
We now deal with bipartite entanglement in MUSs. Consider two quNits 1 and 2. QuNit 1 is prepared in the state \(|\beta; k\rangle_1\) with fixed \(\beta\) and \(k\), while quNit 2 in the state \(|N; q\rangle_2 \equiv |q\rangle_2\) with a fixed \(q\). Let \(CS_{12}\) and \(CS'_{12}\),

\[
CS_{12}[m|n]_2 = |m|_1 [n + m]_2
\]

and

\[
CS'_{12}[m|n]_2 = |m|_1 [n - m]_2,
\]

with algebra inside the kets modulo \(N\) and \(|-l\rangle \equiv |N - l\rangle\), be two-quNit controlled-shift-forward and controlled-shift-backward gates, with quNit 1 the control quNit and quNit 2 the target one. Then,

\[
|\beta; k, q\rangle_2 = CS_{12}[\beta; k]\langle q\rangle_2 = \frac{1}{\sqrt{N}} \sum_{l=0}^{N-1} \Omega^{\beta k} |l\rangle_1 |g + l\rangle_2
\]

is a two-quNit entangled state. The entanglement of state (14) is ensured by the property that if quNit 1 and quNit 2 are measured separately in their computational bases then the outcome \(a\) corresponding to finding \(|a\rangle\) and the outcome \(b\) corresponding to finding \(|b\rangle\) satisfy the equality

\[
b = q + a,
\]

independent of concrete sequence of the two measurements, revealing a nonclassical correlation (entanglement) between the two quNits. In total there are \(N^3\) entangled states of the form (14) which are characterized by three parameters \(\beta, k, q \in \{0, 1, \ldots, N - 1\}\). On the other hand, having two quNits of such a state in the same place with unknown \(k, q\) and known \(\beta\) we can easily identify it by first performing \(CS'_{12}\) on it and then measuring the first quNit in the basis \(\beta\) and the second quNit in the computational basis (i.e., basis \(N\)). Namely, because

\[
CS'_{12}[\beta; k, q]_2 = \left(\frac{1}{\sqrt{N}} \sum_{l=0}^{N-1} \Omega^{\beta k} |l\rangle_1 \right) |q\rangle_2 = |\beta; k\rangle_1 |q\rangle_2,
\]

the subsequent single-quNit measurements will determine the values of \(k\) and \(q\), thus identifying the two-quNit entangled state under question. Yet, if the two quNits are separated spatially so that the two-quNit gate \(CS'_{12}\) cannot be performed, then a unknown two-quNit entangled state remains unknown. In passing we note a couple of formulae, namely

\[
\langle \beta'; p|\beta; k\rangle_2 = \frac{1}{N} \sum_{l=0}^{N-1} \Omega^{\beta' - \beta} |l\rangle_1 |g + l\rangle_2,
\]

and

\[
\langle p|\beta; k, q\rangle_2 = \frac{1}{\sqrt{N}} \Omega^{\beta k} |q + p\rangle_2
\]

which prove to be useful later.

3. Quantum dialogue by nonselective measurements

In this section we shall show in detail how Alice and Bob can ‘talk’ with each other in a quantum manner. Before that let us describe a simpler task of how Alice and Bob can exchange a pair of secret numbers. Let Alice have a number which is either \(\beta' \in \{0, 1, \ldots, N - 1\}\) or \(N\) with \(N\) being a large prime and Bob a number \(\beta \in \{0, 1, \ldots, N - 1\}\). Suppose they wish to exchange their numbers securely. Since classical communication is insecure they must do this quantumly. A way to do this is as follows.

To start with, Bob prepares a state \(|\beta; k, q\rangle_{AB}\) with known \(\beta, k, q\), then sends quNit A to Alice but keeps quNit B with himself. Alice, upon receiving A, measures it either in the basis \(\beta'\) (if she wishes to send number \(\beta'\) to Bob) or in the computational basis (if she wishes to send number \(N\) to Bob). After her measurement she returns A back to Bob without recording the outcome (that is, Alice’s measurement is nonselective).

For Alice’s measurement in basis \(\beta'\), she uses the projectors

\[
\Pi_A(\beta', p) = |\beta'; p\rangle_A \langle \beta'; p|,
\]

with \(p = 0, 1, \ldots, N - 1\). There are \(N\) measurement outcomes corresponding to finding \(A\) in state \(|\beta'; p\rangle_A\) with \(p \in \{0, 1, \ldots, N - 1\}\), each occurs with some probability. For whatever the outcome, if Alice records it then quNit A will be disentangled from quNit B. This scenario is not of our interest. Here, we are concerned with nonselective measurement so no outcomes are to be recorded: quNits A and B are not projected on a pure product state but become in a mixed state of the form

\[
\rho_{AB}(\beta, \beta', k, q) = \sum_{p=0}^{N-1} \Pi_A(\beta', p) \rho_{AB}(\beta, k, q) \Pi_A(\beta', p),
\]

where

\[
\rho_{AB}(\beta, k, q) = |\beta; k, q\rangle_{AB} \langle \beta; k, q|.
\]

Evidently, \(\rho_{AB}(\beta, \beta', k, q)\) depends explicitly not only on \(\beta, k, q\) but also on \(\beta'\) which is the very point of nonselective measurement that we exploit for our quantum dialogue protocol. Bob, upon getting back from Alice the quNit A, measures the two quNits A and B in the bases in which he prepared the initial two-quNit entangled state (14). Technically, this means that he makes use of \(CS'_{AB}\) defined in equation (13) to transform (20) to \(CS'_{AB}\rho_{AB}(\beta, \beta', k, q)\). Then he measures quNit A in the basis \(\beta\) and quNit B in the computational basis. In other words, we can say that Bob uses the following projectors

\[
\Pi_{AB}(\beta, k', q') = |\beta; k', q'\rangle_{AB} \langle \beta; k', q'|,
\]

with \(k', q' = 0, 1, \ldots, N - 1\). There are \(N^2\) measurement outcomes corresponding to finding \(A\) and \(B\) in state \(|\beta; k', q'\rangle_{AB}\) with some \(k', q' \in \{0, 1, \ldots, N - 1\}\), occurring with probability

\[
P_{AB}(\beta, \beta', k, q, k', q') = \langle AB | \beta; k', q'| \rho_{AB}(\beta, \beta', k, q) | \beta; k', q'\rangle_{AB}.
\]

Putting the right-hand-side of equation (20) into the right-hand-side of equation (22) and taking into account equation (17) yields

\[
P_{AB}(\beta, \beta', k, q, k', q') = \sum_{p=0}^{N-1} |\langle AB | \beta; k', q'| \Pi_A(\beta'; p) | \beta; k, q\rangle_{AB}|^2
\]

\[
= \frac{1}{N} \delta_{k-k',2(\beta-\beta')(q-q')}.
\]
with $\delta_{ab}$ the Kronecker delta equal to 1 if $a = b$ and to 0 if $a \neq b$.

As for Alice’s measurement in the computational basis, the projectors to be used are

$$\Pi_A(N;p) = |N;p\rangle_A \langle N;p| \equiv |p\rangle_A \langle p| = \Pi_A(p),$$

(24)

with $p = 0, 1, \ldots, N - 1$. Alice would probabilistically obtain one of the $N$ outcomes corresponding to finding $A$ in state $|p\rangle_A$ with $p \in \{0, 1, \ldots, N-1\}$. Without reading the outcomes the two quNits $A$ and $B$ after Alice’s measurement are described by the density matrix

$$\rho_{AB}(\beta, N, k, q) = \sum_{p=0}^{N-1} \Pi_A(p) \rho_{AB}(\beta, k, q) \Pi_A(p),$$

with $\rho_{AB}(\beta, k, q)$ given by equation (21). Bob, in possession of both the quNits $A$ and $B$ at hand, measures them in the bases $\{|\beta';k',q'\rangle\}_{AB}$, as in the case of Alice’s measurement in basis $\beta'$. The probability of finding state $|\beta';k',q'\rangle_{AB}$ can be calculated by virtue of equations (18) and (24) as

$$P_{AB}(\beta, N, k, q, k', q') = \langle \beta';k',q'|\rho_{AB}(\beta, N, k, q)\langle \beta; k, q|\rangle_{AB} = \sum_{p=0}^{N-1} \langle \beta; k, q|p\rangle_A \langle p|\beta; k, q\rangle |_{AB}^2 = \frac{1}{N}\delta_{q'q}.\tag{25}$$

The expressions (23) and (25) indicate the following.

(i) If $q' = q$ and $k' = k$, then $P_{AB}(\beta, \beta', k, q, k', q') = P_{AB}(\beta, N, k, q, k', q') = 1/N$. So we are not able to know with certainty in which basis Alice measured her quNit $A$, as it may equally be in basis $\beta'$ or in the computational basis $N$.

(ii) If $q' = q$ and $k' \neq k$, then $P_{AB}(\beta, \beta', k, q, k', q') = 0$, but $P_{AB}(\beta, N, k, q, k', q') = 1/N$. So we know with certainty that Alice measured her quNit $A$ in the computational basis, the basis $N$.

(iii) If $q' \neq q$, then $P_{AB}(\beta, N, k, q, k', q') = 0$, but $P_{AB}(\beta, \beta', k, q, k', q') = 1/N$. So we know with certainty that Alice measured her quNit $A$ in the basis $\beta'$

$$\beta' = \beta + \frac{k'-k}{2(q'-q)}.\tag{26}$$

Particularly in this case, if $k' = k$, we know $\beta'$ with certainty $\beta' = \beta$. Thus, almost always Bob is able to know Alice’s secret number $\beta'$ or $N$. Bob fails just in the only case (i) with probability $1/N$ which is vanishing in the large-$N$ limit.

Now, to let Alice know his secret number $\beta$, Bob sends Alice (in fact, just public announcement suffices) the number $\gamma = \beta + \beta'$ or $\gamma = \beta + N$ depending on whether his outcome is $q' \neq q$ or $q' = q$ and $k' \neq k$. Obviously, Alice is able to determine with certainty what is $\beta$ by correspondingly subtracting $\beta'$ or $N$ from $\gamma$. Because here $N$ is large it is highly hard for anyone, who does not know $\beta'$ or $N$, to obtain the right value of $\beta$ from the announced value of $\gamma$.

As described by the above quantum procedure, the two people can at the same time exchange two numbers: $\beta' \in \{0, 1, \ldots, N-1\}$ or $N$ from Alice to Bob and $\beta \in \{0, 1, \ldots, N-1\}$ from Bob to Alice. It is alright if no eavesdropper, Eve, exists. In practical real-life conditions Eve is supposed to exist and, as a powerful person capable of doing anything allowed by nature, she can devise wise strategies of attack to steal partial or even full information if Alice and Bob ignore proper methods of control. In the rest part of this paper, we suggest a full protocol with suitable controls for Alice and Bob to talk with each other in front of Eve’s nose.

Let Alice have a set of secret numbers $\{\alpha_1, \alpha_2, \ldots, \alpha_L\}$ while Bob has a set of other secret numbers $\{\beta_1, \beta_2, \ldots, \beta_L\}$, where $L \geq 1$, $\alpha_j \in \{0, 1, \ldots, N\}$ and $\beta_j \in \{0, 1, \ldots, N-1\}$. Suppose that they want to securely exchange their numbers sequentially like in a conversation, i.e., for each $j$, from $j = 1$ until $j = L$, Alice ‘asks’ $\alpha_j$ and Bob ‘answers’ $\beta_j$. For that purpose they are suggested to proceed as follows (see figure 1).

1. $j = 0$.

2. $j = j + 1$. Bob entangles quNits $A_j$ and $B_j$ into state $|\beta_j; k_j, q_j\rangle_{AB_j}$ of equation (14), then sends $A_j$ to Alice and keeps $B_j$ in his lab.
S3. After receiving quNit $A_j$, Alice with probability $v_1$ performs a control mode of type 1 (CM1) or with probability $1 - v_1$ executes a message mode of type 1 (MM1).

CM1. Alice measures quNit $A_j$ in the computational basis and publicly publishes the measurement outcome $a_j$, which with a probability of $1/N$ takes on a value equal to $0, 1, 2, \ldots$ or $N - 1$ corresponding to finding $|0\rangle_{A_j}, |1\rangle_{A_j}, |2\rangle_{A_j}, \ldots$ or $|N - 1\rangle_{A_j}$, respectively. She also informs Bob of her choice and asks him to measure quNit $B_j$ in the computational basis. The outcome $b_j$ of Bob’s measurement corresponding to finding $|b_j\rangle_{B_j}$ also with a probability of $1/N$ takes on a value equal to $0, 1, 2, \ldots$ or $N - 1$. Then Bob checks the equality (15) which here reads $b_j = q_j + a_j$. If the equality holds, then he sets $j = j - 1$ and goes back to S2 to continue. Otherwise, i.e., the equality is violated, then protocol should be restarted from S1.

MM1. Alice encodes her number $a_j$ by measuring quNit $A_j$ in the basis $B_j = |\beta\rangle_{A_j}$. She creates her own entangled state $|\beta\rangle_{A_j} = |\beta\rangle_{A_j}^\prime$, with $\beta_j = \beta_j^\prime$ chosen at her will and, when Bob releases quNit $A_j$, captures it and stores it in a quantum memory, followed by replacing quNit $A_j$ by quNit $C_j$ to be sent to Alice. Alice would encode her number $\alpha_j$ on the state of quNit $C_j$ as in MM1, then send quNit $C_j$ to Bob without recording the measurement outcome as designed by the protocol. Eve again captures quNit $C_j$ and, as Bob would do in S4 with quNits $A_j$ and $B_j$, she measures quNits $C_j$ and $D_j$ in the basis $\{|\beta\rangle_{C_j}^\prime, |\gamma\rangle_{C_j}^\prime\}$. If $\gamma_j^\prime = \alpha_j$, Eve gets no information about $\alpha_j$ so she puts quNit $C_j$ aside but takes quNit $A_j$ intact from the quantum memory and sends it back to Bob. Bob’s measurement outcome in S4 must be $k_j^\prime = k_j^\prime = \gamma_j^\prime$ so that the protocol returns back to S2 to continue. Otherwise, i.e., if $\gamma_j^\prime = \alpha_j$, Eve determines $\alpha_j$ as in MM2. After having known $\alpha_j$, Eve uses the basis $B_j$ to nonselectively measure quNit $A_j$ he stored before in the memory, then sends this measured quNit $A_j$ back to Bob, who would execute S4 to obtain $\alpha_j$ and proceeds further to broadcast $\gamma_j = \alpha_j + \beta_j$. This broadcasting provides both Alice and Eve with the value of $\beta_j$. Thus, through the above described capture-and-replace attack, Eve is able to eavesdrop the whole dialogue between Alice and Bob. Unfortunately for Eve, there are control modes that help Alice and Bob to detect her presence. It is easy to observe that Eve is immune to CM2 but is not to CM1 because $B_j$ and $C_j$ are not correlated at all. Let us denote by $L$ the total number of the protocol run. Eve would be detected by a CM1 run with a probability $d = (1 - 1/N)v_1$ or, in other words, she would pass with a probability $1 - d$. If Eve is detected in the first run, $L = 1$, the detection probability is $P_{\text{Detected}}(1) = d$. If Eve passes the first run but is detected in the second run, $L = 2$, the detection probability is $P_{\text{Detected}}(2) = (1 - d)d$. If Eve passes the first two runs but is detected in the third run, $L = 3$, the detection probability is $P_{\text{Detected}}(3) = (1 - d)^2d$, and so on. The total detection probability for $L$ runs is therefore

$$P_{\text{TotalDetected}} = \sum_{l=0}^{L-1} P_{\text{Detected}}(l) = \sum_{l=0}^{L-1} (1 - d)^ld$$

$$= 1 - \left(1 - \left(\frac{(N-1)v_1}{N}\right)^L\right). \tag{28}$$

As the total number of run $L$ is related to the length $L$ of the dialogue by $L = L/(1 - v_1 - v_2)$, the total detection probability can be reexpressed in terms of $L$ as
Clearly from equation (29), $P_{\text{TotalDetect}} \to 1$ in the limit of large $L$ and/or large $N$, for any possible values of $v_1$ and $v_2$.

We next consider another attack called measure-and-forward one. When quNit $A_j$ appears from Bob side, Eve measures it in the computational basis with an outcome $|a_j\rangle_A$ and forwards the measured quNit to Alice. As a result of entanglement, the state of quNit $B_j$ immediately collapses into $|q_j + a_j\rangle_{B_j}$, implying immunity of such an Eve’s action to CM1. Anyway, after Eve’s measurement, the state of the two quNits $A_j$ and $B_j$, up to a global phase factor, becomes

$$
|a_j\rangle_A |q_j + a_j\rangle_{B_j} = \sum_{v_j=0}^{N-1} \frac{1}{\sqrt{N}} \Omega^{-v_j|a_j\rangle} |\beta_{u_j,v_j}\rangle_{A,B_j} |q_j + a_j\rangle_{B_j}.
$$

which is a superposition of $N$ entangled states, of which only one, that with $u_j = k_j$, coincides (ignoring the weight coefficient) with the state prepared in S2. Without CM2, Eve’s action is hidden, Alice executes MM1 and Bob executes MM2, as designed. But, with a probability of $(N - 1)/N$ for $u_j \neq k_j$, they exchange totally wrong data. Unfortunately for Eve, there is CM2 that helps Alice and Bob to detect her presence. Namely, because the number Bob decodes in S4 differs from the number Alice encodes in MM1 in most of the cases, Eve’s action is exposed with CM2. The total detection probability for $L$ runs has the form of (28), but with $v_1$ in $d$ replaced by $v_2$.

Also, to prevent anyone from pretending Bob to get Alice’s secret numbers (so-called masquerading attack), it is assumed that the two parties always keep in touch with each other via phone/fax before as well as during the performance of the quantum dialogue. Such assumption is implicit in section 3.

Because both directions between Alice and Bob are controlled the protocol designed in section 3 proves to be secure against other typical attacks: Eve would be detected by CM1 or/and CM2.

5. Conclusion

We have designed a quantum protocol for two-way communication allowing two parties, Alice and Bob, to simultaneously exchange their data in a manner like in a dialogue. Many different protocols of this quantum dialogue kind have been proposed previously. Most of them rely on superdense coding [30]. Our protocol here, instead, makes use of nonselective measurements with choices of measurement bases as signals to exchange. Because the protocol is two-way, two-way should also be the control. In fact, our bidirectional controlling, one on the Bob-to-Alice direction and the other on the Alice-to-Bob direction, make the protocol secure against commonly encountered eavesdropping attacks. Our analysis shows that the security is not absolute but asymptotic in the sense that the eavesdropper’s detection probability approaches 1 if the dimension of the quantum carrier is high or/and the size of the to-be-exchanged data is large. Because of such kind of security, this (as well as other quantum dialogue protocols) is advised to apply only in urgent circumstances when top-secrecy is not prerequisite. Anyway, our protocol sheds some more insight into distinction between classical and quantum measurements and the idea of it may suggest novel applications based on still-less-explored features of quantum measurements.

Acknowledgments

The author dedicates this paper to his teacher, Professor Van Hieu Nguyen, on the occasion of the teacher’s 80th birthday. This work is supported by Vietnam National Foundation for Science and Technology Development (NAFOSTED) under project no. 103.01-2017.08.

References

[1] Bellovin S M 2011 Cryptologia 35 203
[2] Rivest R, Shamir A and Adleman L 1978 Commun. ACM 21 120
[3] Shor P W 1994 Proc. of the 35th Annual Symp. on Foundations of Computer Science (Santa Fe, USA) (IEEE) p 124
[4] Wiesner S J 1983 SIGACT News 15 7
[5] Bennett C H and Brassard G 1984 Proc. of IEEE Int. Conf. on Computers, Systems and Signal Processing (New York) vol 175 p 8
[6] Ekert A K 1991 Phys. Rev. Lett. 67 661
[7] Deng F G, Long G L and Liu X S 2003 Phys. Rev. A 68 042317
[8] Nguyen B A 2004 Phys. Lett. A 328 6
[9] Nguyen B A 2005 J. Kor. Phys. Soc. 47 562
[10] Lucamarini M and Mancini S 2005 Phys. Rev. Lett. 94 140501
[11] Shi G F, Xi X Q, Hu M L and Yue R H 2010 Opt. Commun. 283 1984
[12] Wang H, Zhang Y Q, Liu X F and Hu Y P 2016 Quantum Inf. Process. 15 2593
[13] Thapliyal K and Pathak A 2015 Quantum Inf. Process. 14 2599
[14] Kao S H and Hwang Z 2016 Quantum Inf. Process. 15 4313
[15] Greenberger D M, Horne M A and Zeilinger A 1989 Bell’s Theorem Quantum Theory and Conceptions of the Universe (Dordrecht: Kluwer)
[16] Wang R J, Li D F, Zhang F L, Qin Z, Baaguer E and Zhan H 2016 Int. J. Theor. Phys. 55 3607
[17] Chang C H, Yang C W, Hsu G R, Hwang T and Kao S H 2016 Quantum Inf. Process. 15 2971
[18] Abukasim H, Hamad S, Bahnsy K E and Rida S Z 2016 Phys. Scr. 91 085101
[19] Yu Z B, Gong L H, Zhu Q B, Cheng S and Zhou N R 2016 Int. J. Theor. Phys. 55 3147
[20] Zhou N R, Li J F, Yu Z B, Gong L H and Farouk A 2017 Quantum Inf. Process. 16 4
[21] Maitra A 2017 Quantum Inf. Process. 16 305
[22] Banerjee A, Shukla C, Thapliyal K, Pathak A and Panigrahi P K 2017 Quantum Inf. Process. 16 69
[23] Shukla C, Thapliyal K and Pathak A 2017 Quantum Inf. Process. 16 295
[24] Einstein A, Podolsky B and Rosen N 1935 Phys. Rev. 47 777
[25] Kalev A, Mann A and Revzen M 2013 Phys. Rev. Lett. 110 260502

[26] Bandyopadhyay S, Boykin P O, Roychowdhury V and Vatan F 2002 Algorithmica 34 512

[27] Durt T, Englert B G, Bengtsson I and Zyczkowski K 2013 Int. J. Quant. Inf. 8 535

[28] Wiesniak M, Paterek T and Zeilinger A 2011 New J. Phys. 13 053047

[29] Nielsen M and Chuang I 2000 Quantum Computation and Quantum Information (Cambridge: Cambridge University Press) p 216

[30] Bennett C and Wiesner S 1992 Phys. Rev. Lett. 69 2881