Applied Mathematics & Information Sciences
An International Journal

Two Novel and Secure Quantum ANDOS Schemes

Wei Yang[1,2], *Liusheng Huang*[2] *and Miaomiao Tian*[1]

[1]School of Computer Science and Technology, University of Science and Technology of China, Hefei 230026, China
[2]Suzhou Institute for Advanced Study, USTC, Suzhou, 215123, China

Received: 6 Apr. 2012; Revised 16 Sep. 2012; Accepted 22 Oct. 2012
Published online: 1 Mar. 2013

Abstract: A vendor has several secrets which he regards as of equal worth and importance. He is willing to sell any of these secrets to a buyer. The bargain is said to be secure when the following two conditions are satisfied: 1) the buyer can only obtain one secret if he pays for only one secret, and 2) the vendor will not be able to find out which secret the buyer picked. This cryptographic problem is customarily called all-or-nothing disclosure of secrets (ANDOS). Previous ANDOS schemes have a few defects: neither the number of the secrets is restricted within narrow limits, nor the security is desirable. In this paper, we propose two new and novel ANDOS protocols in quantum computing environment. The first protocol is shown to be as secure as a classical one. The second protocol is based on unambiguous state discrimination, which is proven to be secure in quantum world. Moreover, all our schemes have no limitation on the number of the secrets to be sold.

Keywords: Andos, unambiguous state discrimination, positive operator valued measure, qutrit

1. Introduction

All-or-nothing disclosure of secrets (ANDOS for short) describes the following cryptographic task [4]. A vendor has several secrets which he regards as of equal worth and importance. He is willing to sell any of these secrets to a buyer. The bargain is said to be secure when the following two conditions are satisfied: 1) the buyer can only obtain one secret if he pays for only one secret, and 2) the vendor will not be able to find out which secret the buyer picked. Of course, a basic assumption is that Alice will not send junk to Bob, otherwise the ANDOS is trivial.

Similar to those cryptographic tasks such as in Refs.[26, 23,7,25], ANDOS can be described by a black-box in the following. In the black–box, the inputs of Alice are n binary strings $s_0, s_1, \cdots, s_{n-1}$. She has no output. Bob's input is his choice n ($0 \leq c \leq n-1$). His output is the string s_c, the secret he wants to obtain. A typical ANDOS process is shown in Fig. 1.

The concept of ANDOS was first introduced in 1986 by Brassard, Crépeau and Robert in [4]. After that, a lot of various ANDOS schemes were proposed. However, previous ANDOS protocols in classical computing environment, even in quantum computing environment, have some defects that affect their practicability or availability. For example, in [24] the number of secrets is limited to no more than three. As a contrast, there is no limitation of the number of secrets in [21]. While [21] is vulnerable to collusion among the participants. Under cryptographic assumptions, the security obtained by [4] and [22] can complement each other: the former is computationally secure for Alice and unconditionally secure for Bob, the latter provides unconditional security to Alice and computational

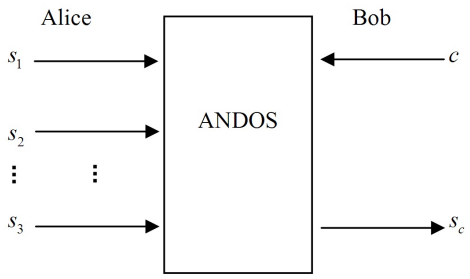


Figure 1 All-or-nothing disclosure of secrets.

* Corresponding author: e-mail: qubit@ustc.edu.cn

security to Bob. In [11], Adrian Kent claims that his protocol is unconditionally secure. However, he used a bit commitment protocol as a building block in his scheme. In fact, unconditionally secure bit commitment is known to be impossible in both the classical and quantum worlds [17, 15, 5, 16]. Thus the protocol given in [11] does not really have the property of unconditional security.

In this paper, we present two new and novel ANDOS protocols in quantum computing environment. The first protocol is shown to be as secure as a classical one. Namely, it does not gain an advantage over its classical counterparts. In contrast, the second quantum ANDOS protocol is based on unambiguous state discrimination, which is proven to be of unconditional security and has a performance that is superior to previous one, both in classical environment and in quantum world. Moreover, all our schemes have no limitation on the number of the secrets to be sold.

The present paper is organized as follows. Section 2 contains the material necessary for understanding the protocols of this paper as well as their context. In Section 3, we propose two quantum ANDOS protocols, where Protocol 1 has the property that it is as secure as previous classical ones, and Protocol 2 is superior to classical ones in a quantum computing environment. We provide detailed analysis of efficiency and proof of security of Protocol 2 (also in contrast with Protocol 1) in Section 4. Section 5 concludes the paper with some remarks.

2. Preliminaries

Readers are supposed to have fundamental knowledge about quantum computation and quantum information. In this section, we only briefly review the quantum concepts and techniques that are closely relevant to our quantum ANDOS protocols.

2.1. Unambiguous State Discrimination

In quantum information theory and quantum computing, a fundamental task is to determine the quantum state [27, 28]. Given a mix of quantum states, can we distinguish between them without any confusion? It is well known that if the quantum states are all orthogonal, then we can discriminate among these states with certainty. For example, assume that we are given an ensemble of Bell states, then we can easily distinguish between these four states via a Bell State Measurement.

However, if a set of quantum states are not orthogonal with each other, the discrimination task seems not so optimistic. Fortunately, we do have some techniques to discriminate among them, but at the cost of losing all the information of the state if an inconclusive result is got. Customarily, we call the technique to distinguish between mix states with some probability to get a conclusive result unambiguous state discrimination (USD) [20]. A simple instance is positive operator valued measure (POVM measurements) [19, 18], also known as probability operator measure (POM), can provide the most general physically measurement by quantum laws. POVM has a few elegant properties, one of which is that it can be used to perform unambiguous measurements and thus discriminate between non-orthogonal states reliably if we allow for the probability of an inconclusive result. Now we give a concrete example of USD using POVM measurement.

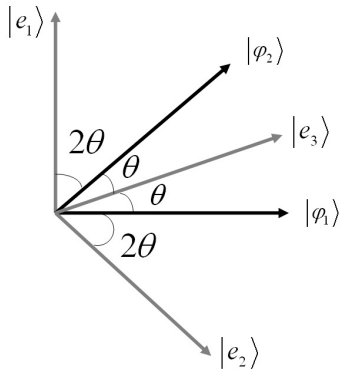


Figure 2 Non-orthogonal states and POVM elements, where $\theta = \frac{1}{8}\pi$.

Suppose that the task we are given is to distinguish between two non-orthogonal states $|\psi_1\rangle = |0\rangle$ and $|\psi_2\rangle = \cos(\frac{1}{4}\pi)|0\rangle + \sin(\frac{1}{4}\pi)|1\rangle$ reliably with certain success probability. Can we accomplish it? Let $|e_1\rangle = |1\rangle$, $|e_2\rangle = \cos(\frac{1}{4}\pi)|0\rangle - \sin(\frac{1}{4}\pi)|1\rangle$, and $|e_3\rangle = \cos(\frac{1}{8}\pi)|0\rangle + \sin(\frac{1}{8}\pi)|1\rangle$. Consider a POVM containing three elements

$$\begin{cases} E_1 = 2\eta \cdot |e_1\rangle \cdot \langle e_1| \\ E_2 = 2\eta \cdot |e_2\rangle \cdot \langle e_2| \\ E_3 = 2\sqrt{2}\eta \cdot |e_3\rangle \cdot \langle e_3| \end{cases} \quad (1)$$

where $\eta = \frac{1}{2+\sqrt{2}}$.

If we describe $|\psi_1\rangle$, $|\psi_2\rangle$, $|e_1\rangle$, $|e_2\rangle$ and $|e_3\rangle$ in a complex plane, then $|\psi_1\rangle$ is vertical to $|e_1\rangle$ and $|\psi_2\rangle$ is vertical to $|e_2\rangle$, as shown in Fig. 2. It is not hard to verify that E_1, E_2 and E_3 obey the conditions: $E_1 \geq 0$, $\sum_i E_i = I$.

Therefore we know that they constitute a complete quantum measurement. If the result of his measurement is E_1 then one can safely conclude that the state must be $|\psi_2\rangle$. A similar line of reasoning shows that if the measurement outcome E_2 occurs then it must be the state $|\psi_1\rangle$. Some of the time, however, we will obtain the measurement outcome E_3, and then we will infer nothing about the identity of the original state.

In this paper, we construct a USD with qutrit measurement, which will be shown in next section.

2.2. Qutrit

A qutrit is the quantum information analogue of the classical trit. It is also the natural extension of qubit and the special case of *qudit* with $d = 3$ [1]. Typically, a qutrit takes the state

$$|\psi\rangle = \alpha|a\rangle + \beta|b\rangle + \gamma|c\rangle \tag{2}$$

where $|a\rangle$, $|b\rangle$, $|c\rangle$ are three-dimensional column vectors with the values

$$|a\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}, |b\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, |c\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \tag{3}$$

and α, β and γ are complex numbers that satisfy the normalization condition

$$|\alpha|^2 + |\beta|^2 + |\gamma|^2 = 1 \tag{4}$$

Qutrits have some advantages that outperform qubits. For example, qutrits provide better security than qubits in quantum bit commitment [13]. Another instance is their possible implementation in the fundamental tests of quantum mechanics, which are strongly resistant to noise [6]. Experimental realization of arbitrary qutrit states has been studied by Klimov *et al.* [12] and Bogdanov *et al.* [3]. These implementations open up a bright prospect for qutrits in quantum information area.

Like that of qubit, two non-orthogonal qutrit states cannot be reliably distinguished.

3. Quantum ANDOS Protocols

3.1. Quantum ANDOS Protocol Being Equivalent to Its Classical Counterpart

Enlightened by the fact that two non-orthogonal qubit states cannot be distinguished with certainty and the famous quantum key distribution scheme BB84 [2], readers may think that it is not hard to realize ANDOS scheme within the domain of quantum mechanics. A typical protocol is described in the following box.

Suppose that before the protocol, Alice and Bob come to an agreement that polarizations horizontal (0°) and 45° represent classical bit 0, and vertical (90°) and 135° represent classical bit 1. The parameters n and s denote the number of Alice's secrets and the length of each secret, respectively.

Protocol 1 *Quantum ANDOS Protocol Being Equivalent to Its Classical Counterpart*

1. Alice prepares randomly and uniformly 2ns photons, each of which is independently in one of the four possible polarizations: 0°, 90°, 45°, and 135°. She then sends these photons to Bob sequentially.
2. For each photon, Bob randomly selects between rectilinear base ($\{|0\rangle, |1\rangle\}$) and diagonal base ($\{|+\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}, |-\rangle = \frac{|0\rangle-|1\rangle}{\sqrt{2}}\}$) to perform a measurement. He records every outcome sequentially.
3. Alice announces her encryption bases to Bob and demands that Bob declare about $\frac{n-1}{n}$ of the outcomes that Bob measured with determinate results.
4. If Bob passes Alice's verification, he will get about s measurement outcomes with certainty from the remaining photons which were not declared to Alice. Bob now pick *ns* photons from this set and divided them into n subsets with the cardinality of each subset is equal to *s*, where one of the subset contains the photons he measured with determinate results. He is thus able to hide the number of the secret he wanted and sends these subsets to Alice.
5. For each subset, Alice performs a bitwise exclusive or operation with her corresponding secret. She sends Bob the *n* encrypted secret strings.
6. Bob decodes his secret with his "secret key".

It is not hard to see that if both Alice and Bob carry out Protocol 1 honestly, they will accomplish an ANDOS transaction in the end, with the guarantee that Alice cannot learn which secret Bob has picked and no information about the other secrets is obtained by Bob. However, consider that a dishonest Bob may attempt to get other secrets without paying more. He can initiate the following attack strategy: in Step 2 of Protocol 1, he just stores the photons sent by Alice without any operation instead of measuring these photons. He waits until Alice announces her encryption bases and then performs his measurements according to the encryption information. Thus he will get all the information of Alice's 2*ns* photons and further he will obtain all the *n* secrets form Alice. The only setup that Bob needs to perform this kind of attack strategy is a photon storage device. Namely, he needs a quantum computer. Therefore, similar to those classical ANDOS schemes, Protocol 1 will be insecure in the future when a quantum computer is available. Or in other words, Protocol 1 does not gain an advantage of previous classical ones.

3.2. Quantum ANDOS Protocol Based on Unambiguous State Discrimination

Similar to those of Protocol 1, the parameters *n* and *s* in the following represent the number of Alice's secrets and the length of each secret, respectively.

Protocol 2 *Quantum ANDOS via USD*

1. For $k = 1$ to *ns*, Alice selects randomly and uniformly a bit b_k. If $b_k = 0$, she prepares and sends a qutrit in state $|\phi_1\rangle = p|c\rangle + q|b\rangle$ to Bob. Otherwise, she prepares and sends Bob a qutrit in state $|\phi_2\rangle = u|c\rangle + v|a\rangle$. ($p$, q, u and v are real numbers that will be determined later.)

2.Bob receives each qutrit and performs the quantum measurements with basis $\{M_1, M_2, M_3\}$, where

$$M_1 = |a\rangle\langle a| = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \tag{5}$$

$$M_2 = |b\rangle\langle b| = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix} \tag{6}$$

$$M_3 = |c\rangle\langle c| = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \tag{7}$$

The probability p_i of obtaining a measurement outcome M_i on system in state ρ is given by

$$p_i = Tr(M_i\rho) \tag{8}$$

Bob then records each measurement outcome sequentially. (In the next section, we will show that by Eq. (10), for some qutrits he can get definite conclusions, while for other ones he just cannot determine which state Alice prepared.)

3.For the qutrit states determined with certainty in step 2, Bob divides them into two sets R_i and R_j, where the cardinality of R_j is given by

$$|R_j| = [\frac{0.5}{n}] \cdot ns \tag{9}$$

(The value of $|R_j|$ will be explained in the next section.) Then he sends R_j to Alice via a public channel. Meanwhile, R_i is kept secret against Alice.

4.Alice verifies that, each state in R_j was rightly obtained by Bob. If all the states pass the test Alice can safely conclude that: *i*) there was no eavesdropper on the quantum channel, and *ii*) Bob is honest. Thus she informs Bob to continue. Otherwise, if an eavesdropper Eve is detected, Alice tells Bob about it and they abort the scheme.

5.If Bob is told that the quantum channel is secure, then he constitutes $(n-1)$ sets form the qutrits which he did not get conclusive results. He then announces an n-tuple $\mathbb{Z} = \{\mathbb{R}_1, \mathbb{R}_2, \cdots, \mathbb{R}_i, \cdots, \mathbb{R}_n\}$ to Alice, where $\mathbb{R}_i = R_i$ and the subscript i indicates the index of the secret that Bob wants to get.

6.For each element in $\mathbb{Z}$, Alice performs a bitwise exclusive or operation with her corresponding secret. Namely, she will sends Bob an n-tuple $\mathbb{Z} = \{\mathbb{R}_1 \oplus s_1, \mathbb{R}_2 \oplus s_2, \cdots, \mathbb{R}_i \oplus s_i, \cdots, \mathbb{R}_n \oplus s_n\}$.

7.Bob decodes his secret with his "secret key", namely, $\mathbb{R}_i$.

Detailed analysis of efficiency and proof of security of Protocol 2 (also in contrast with Protocol 1) are provided in Sec. 4.

4. Analysis and Proof

4.1. Analysis of efficiency

In protocol 2, Bob performs qutrit measurement on each state he received from Alice. If there is no eavesdropper on the channel, then for states $|\phi_1\rangle = p|c\rangle + q|b\rangle$ and $|\phi_2\rangle = u|c\rangle + v|a\rangle$, his probability of measurement outcomes M_1, M_2 and M_3 are shown in Tab. 1.

Table 1 Probabilities of qutrit measurement outcomes.

Probability	M_1	M_2	M_3
$\|\phi_1\rangle$	0	q^2	p^2
$\|\phi_2\rangle$	v^2	0	u^2

In order for Bob to get unbiased measurement probabilities, p, q, u and v should satisfy that

$$q^2 = v^2 \tag{10}$$

and

$$p^2 + q^2 = 1 \tag{11}$$

$$u^2 + v^2 = 1 \tag{12}$$

Because p, q, u and v are all real numbers, from Eqs. (4.1)∼(4.3) we get that

$$q = v \tag{13}$$

$$p = u \tag{14}$$

$$p = \sqrt{1-q^2} \tag{15}$$

Note that the qutrit states $|\phi_1\rangle$ and $|\phi_2\rangle$ are non-orthogonal, so we also have

$$p > 0 \tag{16}$$

In Protocol 2, we let

$$p = \sqrt{1 - [\frac{1.6}{n}]} \tag{17}$$

then the probability Bob obtains each state sent by Alice definitely is given by

$$P_{def} = q^2 = 1 - p^2 = [\frac{1.6}{n}] \tag{18}$$

By Eq. (18), we now understand that in Eq. (9), about $0.5s$ measurement results are used for eavesdropping purpose. If no eavesdropper is detected and the channel is error-free, then Alice and Bob can secretly share, on average, $1.1s$ classical bits when ns qutrits are transmitted. While in Protocol 1, Alice and Bob share s qubits via an initial amount of $2ns$ qubits.

Another parameter to measure the performance an ANDOS scheme is the number of *ideal communication rounds*,

which considers the minimal number of ideal communication rounds that an error-free scheme needs. In our Protocol 2, there is no need for Alice to declare her encryption basis to Bob. This is because Bob's measurement method is a kind of unambiguous means. After his measurement on each qutrit, he knows whether he obtains the state of it at once. Thus Bob can get the right information of each qutrit with some success probability by himself, without the help of Alice. In contrast with Protocol 2, Protocol 1 is less efficient. It is because that in the latter, Alice has to declare her encryption basis to Bob. Therefore, the number of ideal communication rounds of our Protocol 2 is 5. By contrast, in Protocol 1, Bob cannot get the right result independently (he has to combine Alice's encryption basis and his measurement result to determine the information of each qubit). Therefore, the number of ideal communication rounds of Protocol 1 is 6.

4.2. Security proof

Let us first consider the attacking strategy that an eavesdropper Eve may adopt. Without loss of generality, we can assume that Eve can eavesdrop on both classical and quantum channel. In order to get secret information shared by Alice and Bob, Eve may intercept and forward the qutrits on the channel. By the above analysis, we know that Eve's best strategy is to perform the same measurements adopted by Bob. According Eq. (17), for each qutrit sent by Alice, the probability of Eve's failing to confirm its state is given by

$$P_{fail} = P_{def} = p^2 = 1 - [\frac{1.6}{n}] \tag{19}$$

Then Eve has to guess a significant number of states randomly. When Bob receives the states sent by Eve, his probability of getting the right information is a value less than P_{fail}. Therefore by comparing small quantities of their bits publicly, Alice and Bob can reach a conclusion. If they find more differences than can be attributed to known sources, they will know that there is an eavesdropper on the channel.

Another way Eve may adopt is to introduce an auxiliary qutrit. She then makes this auxiliary qutrit entangle with the qutrit she intercepted from Alice. After that, she sends the auxiliary qutrit Bob and keeps the qutrit she intercepted in her hands. Eve attempts to obtain the secret information generated between Alice and Bob by postponing the measurement of her qutrit until Bob has completed his operation. However, by computation we know that this strategy also cannot help Eve avoid being detected.

Thus any eavesdropping on the channel will always be detected by Alice and Bob and therefore our scheme is secure against any potential eavesdropper.

Now let us consider the security aspect of our ANDOS scheme. Namely, how can Protocol 2 satisfy the two properties: Alice cannot learn which secret Bob has picked, and Bob cannot learn more information than the secret he has paid for.

In order to investigate the privacy of Bob's choice, we have the following conclusion:

Theorem 4.1. Alice knows noting about Bob's choice i in Protocol 2.

Proof. In fact, Bob does not reveal anything that involves i until Step 5. Moreover, Bob's "secret key" $\mathbb{R}_i$ is purely random and information-theoretically hidden from Alice for that she is unable to distinguish which of Bob's set he had measured with affirmative outcomes. Therefore, sending n-tuple $\mathbb{Z} = \{\mathbb{R}_1, \mathbb{R}_2, \cdots, \mathbb{R}_i, \cdots, \mathbb{R}_n\}$ to Alice at Step 5 does not reveal anything about i either. Thus it is information-theoretically impossible for Alice to cheat, regardless of her computing power and available technology.

On the other hand, even if Alice deviates from Protocol 2 by sending entangled states to Bob, it will not help her to tell which secret Bob has obtained. Suppose Alice sends entangled states instead of $|\phi_1\rangle$ and $|\phi_2\rangle$. Bob receives it and performs USD measurement as usual. By Eqs. (13)$\sim$(15) we know that, the measurement outcomes no longer have the property of infallibility. This will render Bob unable to decide a state correctly. The subsequence is that Bob will obtain none of Alice's secrets. By the assumption mentioned in Sec. 1, the whole of the scheme will fall to the ground and have to abort. Obviously, this kind of attack is trivial and Alice will not take it. □

In order for Bob to get one and only one secret, the key issue is that the number of qutrits he get with certainty is actually less than $2s$ and more than $1s$. In fact, we have Theorem 4.2 and Theorem 4.4 to explain it.

Theorem 4.2. For sufficiently large ns, there exist a constant ξ ($0 < \xi < 1$) such that Bob can obtain at least one secret with a probability at least $1 - \xi^{ns}$.

In order to prove Theorem 4.2 we need an inequality named "Chernoff Bound" [8]. We give the inequality first, and then come back to the proof.

Theorem 4.3. (Chernoff inequality) [19]: Let $p \leq 0.5$, and $X_1, X_2, \cdots, X_n$ be independent 0–1 random variables so that $Pr[X_i = 1] = p$ for each i. Then for all ε, $0 < \varepsilon \leq p(1-p)$, we have

$$Pr[|\frac{\sum_{i=1}^{n} X_i}{n} - p| > \varepsilon] \leq 2 \cdot e^{-\frac{\varepsilon^2}{2p(1-p)} \cdot n} \tag{20}$$

Now we continue to proving Theorem 4.2.

Proof. First we let

$$x_k = \begin{cases} 1 \text{ Bob got } r_k \text{ reliably} \\ 0 \text{ otherwise} \end{cases} \tag{21}$$

where $k \in [1, ns]$.

By (21), $Pr[X_k = 1] = [\frac{1.1}{n}]$, $Pr[X_k = 0] = 1 - [\frac{1.1}{n}]$ (note that here we omit the qutrits used for checking purpose), and $\sum_{k=1}^{ns} X_k$ indexes the total number of the bits Bob reliably got from Alice. Thus we have

$$\begin{aligned} &Pr[\text{Bob gets at least one secret}] \\ =&1 - Pr[\text{Bob gets none secret}] \\ =&1 - Pr[\sum_{k=1}^{ns} X_k < s] \end{aligned} \tag{22}$$

For $Pr[\sum_{k=1}^{ns} X_k < s]$, we have

$$\begin{aligned} & Pr[\sum_{k=1}^{ns} X_k < s] \\ =& Pr[-\sum_{k=1}^{ns} X_k > -s] \\ =& Pr[-\frac{\sum_{k=1}^{ns} X_k}{ns} > -\frac{1}{n}] \\ =& Pr[-\frac{\sum_{k=1}^{ns} X_k}{ns} + \frac{1.1}{n} > \frac{0.1}{n}] \\ \leq& Pr[|\frac{\sum_{k=1}^{ns} X_k}{ns} - \frac{1.1}{n}| > \frac{0.1}{n}] \\ <& 2 \cdot e^{-\frac{(\frac{0.1}{n})^2}{1 \cdot \frac{1.1}{n}(1-\frac{1.1}{n})} \cdot ns} \end{aligned} \tag{23}$$

In the last step of (23), we have used Lemma 3. Because

$$2 \cdot e^{-\frac{(\frac{0.1}{n})^2}{1 \cdot \frac{1.1}{n}(1-\frac{1.1}{n})} \cdot ns} < 2 \cdot e^{-0.0045 \cdot ns} \tag{24}$$

We now get that

$$Pr[\text{Bob gets at least one secret}] > 1 - 2 \cdot e^{-0.0045 \cdot ns} \tag{25}$$

Therefore as long as ns is large enough, for any constant ξ, $e^{-0.0045} < \xi < 1$, Theorem 34.2 follows. □

Theorem 4.2 tells us that Bob can get at least one of Alice's secrets with a probability that can be made arbitrarily close to 1. Then, suppose Bob is honest, will he obtain more than one secret sent by Alice? For this, we have

Theorem 4.4. For sufficiently large ns, there exist a constant η ($0 < \eta < 1$) such that Bob can obtain more than one secret with probability at most η^{ns}.

Proof. Let x_k be defined as in (21), then

$$\begin{aligned} & Pr[\text{Bob gets more than one secret}] \\ =& Pr[\sum_{k=1}^{ns} X_k > 2s] \\ =& Pr[\frac{\sum_{k=1}^{ns} X_k}{ns} > \frac{2}{n}] \\ =& Pr[\frac{\sum_{k=1}^{ns} X_k}{ns} - \frac{1.1}{n} > \frac{0.9}{n}] \\ \leq& Pr[|\frac{\sum_{k=1}^{ns} X_k}{ns} - \frac{1.1}{n}| > \frac{0.9}{n}] \\ <& 2 \cdot e^{-\frac{(\frac{0.9}{n})^2}{1 \cdot \frac{1.1}{n}(1-\frac{1.1}{n})} \cdot ns} \end{aligned} \tag{26}$$

where the last inequality uses inequality (20) once more.

Because

$$2 \cdot e^{-\frac{(\frac{0.9}{n})^2}{1 \cdot \frac{1.1}{n}(1-\frac{1.1}{n})} \cdot ns} < 2 \cdot e^{-0.3682 \cdot ns} \tag{27}$$

Similarly, combine (26) and (27), we now can safely get that

$$Pr[\text{Bob gets more than one secret}] < 2 \cdot e^{-0.3682 \cdot ns} \tag{28}$$

That is to say, for sufficiently large ns, the probability that Bob gets more than one secret at the same time can be made arbitrarily small. Therefore as long as ns is large enough, for any constant η, $e^{-0.3682} < \eta < 1$, Theorem 344 follows. □

Combine Theorems 4.1, 4.2 and 4.4, we know that a secure and fair quantum ANDOS protocol is achieved by Protocol 2.

5. Summary

In this paper, we have proposed two new quantum ANDOS protocols. Both of them have the property that the number of the secrets of Alice can be arbitrarily large. Moreover, Protocol 1 makes use of quantum laws to achieve ANDOS, but it does not embody the superiority over its classical counterparts. On the other hand, Protocol 2 is carefully constructed based on unambiguous state discrimination. This makes Alice be free of declaring her encryption bases and further result in an efficiency and security improvement. Detailed analysis and proof show that Bob will get the only secret he has paid for, and he cannot learn more information about other secret. Furthermore, Alice is not able to learn which secret Bob has picked.

In addition, there are already known physical implementations for quantum key distribution based on entangled qutrits using two-photon states from spontaneous parametric down-conversion, see for instance of Ref. [9]. Therefore, it is not hard to envisage an implementation based on single qutrits and heralded detection [14,10]. These achievements all suggest that our protocols in this paper will be feasible in the near future.

Acknowledgement

This work was supported by the National Natural Science Foundation of China (No. 60903217), the Natural Science Foundation of Jiangsu Province of China (No. BK2011357), the Fundamental Research Funds for the Central Universities (No. WK0110000027) and the Guangdong Province Strategic Cooperation Project with the Chinese Academy of Sciences (No. 2012B090400013).

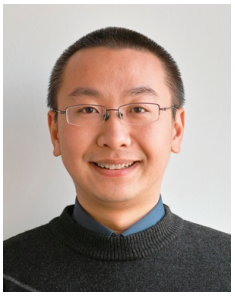
References

[1] A. Al-Rabadi. Qudits representations and computations of n-player many-valued quantum games. *Applied mathematics and computation*, **175**(1):691–714, 2006.

[2] C. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computers Systems and Signal Processing*, volume **175**, pages 175–179. Bangalore, India, 1984.

[3] Y. Bogdanov, M. Chekhova, S. Kulik, G. Maslennikov, A. Zhukov, C. Oh, and M. Tey. Qutrit state engineering with biphotons. *Physical review letters*, **93**(23):230503, 2004.

[4] G. Brassard, C. Crépeau, and J. Robert. All-or-nothing disclosure of secrets. In *Advances in CryptologyCRYPTO86*, pages 234–238. Springer, 1987.
[5] H. Chau and H. Lo. Making an empty promise with a quantum computer. *Fortschritte der Physik*, **46**(4-5):507–519, 1998.
[6] D. Collins, N. Gisin, N. Linden, S. Massar, and S. Popescu. Bell inequalities for arbitrarily high-dimensional systems. *Physical review letters*, **88**(4):40404, 2002.
[7] Y. FU and R. SHEN. Novel self-reference based image watermarking scheme. *Journal of Circuits, Systems, and Computers*, **19**(2):491Ŕ502, 2010.
[8] O. Goldreich. Foundations of cryptography basic tools. 2001.
[9] S. Gröblacher, T. Jennewein, A. Vaziri, G. Weihs, and A. Zeilinger. Experimental quantum cryptography with qutrits. *New Journal of Physics*, 8:75, 2006.
[10] R. Kaltenbaek, J. Lavoie, B. Zeng, S. Bartlett, and K. Resch. Optical one-way quantum computing with a simulated valence-bond solid. *Nature Physics*, **6**(11):850–854, 2010.
[11] A. Kent. Unconditionally secure all-or-nothing disclosure of secrets. *Arxiv preprint quant-ph/9711025*, 1997.
[12] A. Klimov, R. Guzman, J. Retamal, and C. Saavedra. Qutrit quantum computer with trapped ions. *Physical Review A*, **67**(6):062313, 2003.
[13] N. Langford, R. Dalton, M. Harvey, J. OBrien, G. Pryde, A. Gilchrist, S. Bartlett, and A. White. Measuring entangled qutrits and their use for quantum bit commitment. *Physical review letters*, **93**(5):53601, 2004.
[14] G. Lima, A. Vargas, L. Neves, R. Guzmßn, and C. Saavedra. Manipulating spatial qudit states with programmable optical devices. *Optics Express*, **17**(13):10688–10696, 2009.
[15] H. Lo and H. Chau. Is quantum bit commitment really possible? *Physical Review Letters*, **78**(17):3410–3413, 1997.
[16] H. Lo and H. Chau. Why quantum bit commitment and ideal quantum coin tossing are impossible. *Physica D: Nonlinear Phenomena*, **120**(1-2):177–187, 1998.
[17] D. Mayers. Unconditionally secure quantum bit commitment is impossible. *Physical review letters*, **78**(17):3414–3417, 1997.
[18] M. Nielsen, I. Chuang, and L. Grover. Quantum computation and quantum information. *American Journal of Physics*, 70:558, 2002.
[19] A. Peres. *Quantum theory: concepts and methods*, volume **57**. Kluwer Academic Publishers, 1993.
[20] M. Rezaei, M. Rezapour, and M. Fasihi. Optimal unambiguous discrimination of two finite-dimensional coherent states. *International Journal of Quantum Information*, **7**(2):517–528, 2009.
[21] A. Salomaa and L. Santean. Secret selling of secrets with several buyers. *Bulletin of the EATCS*, 42:178–186, 1990.
[22] J. Stern. A new and efficient all-or-nothing disclosure of secrets protocol. In *Advances in CryptologyASIACRYPT98*, pages 357–371. Springer, 1998.
[23] S. Tang and G. Wei. Id-based digital multisignature scheme. *JOURNAL OF CIRCUITS SYSTEMS AND COMPUTERS*, **9**(3/4):223–228, 1999.
[24] S. Wiesner. Conjugate coding. *ACM Sigact News*, **15**(1):78–88, 1983.
[25] S. Wolf and J. Wullschleger. Oblivious transfer is symmetric. *Advances in Cryptology-EUROCRYPT 2006*, pages 222–232, 2006.
[26] W. Yang, L. Huang, Y. Zhu, Y. Ye, P. Meng, F. Song, and Q. Wang. Incentive compatible quantum secure division. *The European Physical Journal D-Atomic, Molecular, Optical and Plasma Physics*, **60**(2):429–433, 2010.
[27] E. Yépez, A. Calles, and J. Castro. A simple algorithm for the group theoretical classification of quantum states. *Applied mathematics and computation*, **133**(1):119–130, 2002.
[28] E. Yépez, J. Soto, J. Castro, and A. Calles. A simple algorithm for the group theoretical classification of quantum states ii. the case of molecular electronic states. *Applied mathematics and computation*, **164**(3):719–729, 2005.



Wei Yang received the Ph.D degree from the Department of Computer Science and Technology, University of Science and Technology of China in 2007. He is currently a post doctorate in University of Science and Technology of China. His major research interest is information security and quantum information.

Liusheng Huang received the M.S. degree in computer science from University of Science and Technology of China in 1988. He is currently a professor and Ph.D supervisor of the Department of Computer Science and Technology at University of Science and Technology of China. He has published 6 books and more than 60 papers. His research interests are in the areas of information security, distributed computing and Wireless Sensor Networks.

Miaomiao Tian is a Ph.D. student in School of Computer Science and Technology at University of Science and Technology of China. His research interests include cryptography and information security.