Unconditionally Secure All-or-Nothing Disclosure of Secrets
Based on POVM Measurements*

YANG WEI, LIUSHENG HUANG
Department of Computer Science and Technology
University of Science and Technology of China
National High Performance Computing Center (Hefei)
Hefei, 230027, P. R. CHINA

Abstract: Secure two-party protocols are of significant research and application value. All-or-Nothing Disclosure of Secrets (ANDOS) is such a kind of cryptographic task. It involves two parties, a vendor and a buyer. The vendor, say Alice, who disposes of several secrets and is willing to sell any of them to the buyer, say Bob, with the guarantee that no information about the other secrets will be obtained. Furthermore, Bob can freely choose his secret and wants to ensure that Alice can obtain no information about which of her secrets he has picked. In this paper, we present a new quantum ANDOS scheme which achieves the same functionality, but which is of unconditional security.

Key-Words: ANDOS, POVM Measurements, Unconditionally Secure, k-OT, Quantum Information, Non-orthogonal States

1 Introduction

All-or-Nothing Disclosure of Secrets (ANDOS) is an interesting cryptographic task. It involves two parties, a vendor and a buyer. The vendor, say Alice, who disposes of several secrets and is willing to sell any of them to the buyer, say Bob, with the guarantee that no information about the other secrets will be obtained. Furthermore, Bob can freely choose his secret and wants to ensure that Alice can obtain no information about which of her secrets he has picked.

The first ANDOS protocol was introduced in 1986 by Brassard, Crépeau and Robert in [1]. Indeed, the first case known as one-out-of-\(t\) string Oblivious Transfer for \(t = 3\) was addressed and solved in [2]. After [1] and [2], several other schemes were proposed. Salomaa and Santean [3] designed an efficient ANDOS protocol that can distribute secrets to any number of people greater than one. Adrian Kent [4] gave a novel solution to this problem using the exchange of quantum information. In [5], Stern proposed a very efficient algorithm for real-life applications.

However, previous ANDOS protocols all have some drawbacks. In [2] the number of secrets is limited to no more than three. [3] is vulnerable to collusion among the participants. Under cryptographic assumptions, the security obtained by [1] and [5] 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 security to Bob. In [4], Adrian Kent claims that his protocol is unconditionally secure. However, he used a bit commitment protocol as a sub protocol in his scheme. In fact, unconditionally secure bit commitment is known to be impossible in both the classical and quantum worlds ([6]–[7]). Thus the protocol given in [4] does not really have the property of unconditional security.

This paper gives a new ANDOS protocol by virtue of the elegant nature of quantum POVM (Positive Operator-Valued Measure) measurements. Compared to previous ANDOS protocols, the major contributions of this work are:

1. Both Alice and Bob have no limitation on their computing power, so it is unconditionally secure for each participants. (Comparing to [4], it need not invoke a bit commitment scheme as a building block in our scheme.)

2. According to Heisenberg Uncertainty Principle and quantum no-cloning theorem, no eavesdropper can escape being detected. Obviously, this is impossible in a classical environment.

The paper is organized as follows. Section 2 contains the material necessary for understanding the protocols of this paper as well as their context. The k-OT protocol based on POVM constructed as a sub protocol in our ANDOS scheme is presented...
in section 3. The k-OT protocol ensures that Bob can reliably get the right information of each bit sent by Alice with probability about 0.3. In section 4, we use k-OT protocol to construct our ANDOS scheme. We also prove that the ANDOS protocal presented in this paper cannot be cheated by either party, except with arbitrarily small probability. Section 5 concludes the paper with some open questions.

2 Preliminaries

2.1 Quantum Measurement

In a classical environment, all digital information is processed and stored as bits, taking on the values of either 0 or 1. In quantum information theory, the concept of a bit is replaced by its quantum-mechanical counterpart, the quantum bit or qubit.

A qubit state is a unit vector in a two-dimensional complex vector space. Contrary to a classical bit, the state of a qubit is not restricted to the basic states \( |0 \rangle \) and \( |1 \rangle \), but can take on any superposition of these two states:

\[
|\phi\rangle = a|0\rangle + b|1\rangle
\]

where \( a \) and \( b \) are complex numbers and satisfy

\[
|a|^2 + |b|^2 = 1
\]

The ability of qubits to be in superposition states is fundamental to quantum information theory, offering the prospect of solving certain problems much more efficiently than classical computers.

If we measure \( |\phi\rangle \) in the \( \{|0\rangle, |1\rangle\} \) basis, then we will get \( |0\rangle \) with probability \( |a|^2 \) or \( |1\rangle \) with probability \( |b|^2 \).

To describe formally, quantum measurements are described by a collection \( \{M_m\} \) of measurements operators. These operators act on the state space of the system being measured. The index \( m \) refers to the measurement outcomes that may occur in the experiment. If the state of the quantum system is \( |\phi\rangle \) immediately before the measurement then the probability that result \( m \) occurs is given by

\[
p(m) = \langle \phi | M_m^* M_m | \phi \rangle
\]

where \( M_m^* \) denotes the complex conjugate transpose of \( M_m \), and the state of the system after the measurement collapses to

\[
\frac{M_m | \phi \rangle}{\sqrt{\langle \phi | M_m^* M_m | \phi \rangle}}
\]

The measurement operators satisfy the completeness equation,

\[
\sum_m M_m^* M_m = I
\]

Equation (5) expresses the fact that probabilities sum to one:

\[
1 = \sum_m p(m) = \sum_m \langle \phi | M_m^* M_m | \phi \rangle
\]

This equation is satisfied for all \( |\phi\rangle \).

Moreover, according to the laws of quantum physics, non-orthogonal states can’t be reliably distinguished by any quantum measurement.

2.2 POVM Measurements [8]

POVM is a special case of the general measurement formalism. POVMs have a very elegant nature that they can distinguish non-orthogonal states reliably with success probability of some constant.

Suppose a measurement described by measurement operators \( M_m \) is performed on a quantum system in the state \( |\phi\rangle \). Then the probability of outcome \( m \) occurs is given by equation (3). Suppose we define

\[
E_m = M_m^* M_m
\]

Then from section 2.1 and elementary linear algebra, \( E_m \) is a positive operator such that \( \sum_m E_m = I \) and

\[
p(m) = \langle \phi | E_m | \phi \rangle
\]

Thus the set of operators \( E_m \) are sufficient to determine the probabilities of the different measurement outcomes. The operators \( E_m \) are known as the POVM elements associated with the measurement. The complete set \( \{E_m\} \) is known as a POVM.

3 k-OT sub protocol based on POVM measurements

First let us define two constant to be used later:

\[
\mu = \cos \frac{\pi}{8}, \quad \nu = \sin \frac{\pi}{8}.
\]

In order to distinguish two non-orthogonal states \( |\phi_1\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \) and \( |\phi_2\rangle = |1\rangle \) reliably with success probability of some constant, let us consider a POVM containing three elements,
\[ E_i = \alpha \cdot \left( \frac{|0\rangle + |1\rangle}{\sqrt{2}} \right) \left( \frac{|0\rangle + |1\rangle}{\sqrt{2}} \right) = \alpha \left( \begin{array}{c} 1 \\ 1 \end{array} \right) \] (8)

\[ E_2 = \beta \cdot \frac{|0\rangle \langle 0|}{\sqrt{2}} = \beta \left( \begin{array}{c} 1 \\ 0 \\ 0 \\ 0 \end{array} \right) \] (9)

\[ E_3 = \gamma \cdot \left(-\nu |0\rangle + \mu |1\rangle \right) \left(-\nu |0\rangle + \mu |1\rangle \right) = \gamma \left( \begin{array}{c} \nu^2 & -\mu \nu \\ -\mu \nu & \mu^2 \end{array} \right) \] (10)

where \( \alpha \), \( \beta \) and \( \gamma \) are constants to be later determined.

Because operators \( E_1 \), \( E_2 \) and \( E_3 \) constitute a POVM, they satisfy:

\[ E_1 + E_2 + E_3 = I \] (11)

By equation (3) and (7) we can get that, for the state \( |\varphi_1\rangle \), if Bob performs the measurement described by the POVM \( \{E_1, E_2, E_3\} \), the probabilities of outcomes of \( E_1 \) and \( E_2 \) are 0 and \( \frac{\beta}{2} \) respectively. Similarly, for the state \( |\varphi_2\rangle \), the probabilities of outcomes of \( E_1 \) and \( E_2 \) are \( \frac{\alpha}{2} \) and 0 respectively.

Therefore, suppose Alice sends Bob a photon with the state \( |\varphi_1\rangle \) or \( |\varphi_2\rangle \), Bob measures it by the POVM \( \{E_1, E_2, E_3\} \), if the result of his measurement is \( E_1 \) then Bob can safely conclude that the state he received must have been \( |\varphi_2\rangle \). A similar line of reasoning shows that if the measurement outcome \( E_2 \) occurs then it must have been the state \( |\varphi_1\rangle \) that Bob received. Some of the time, however, Bob will obtain the measurement outcome \( E_3 \), then he will infer nothing about the identity of the state he was given.

For the sake of symmetry of our protocol presented later, we let

\[ \frac{\beta}{2} = \frac{\alpha}{2} \] (12)

Combine (8) ~ (12) we can get

\[ \alpha = \beta = \frac{\sqrt{2}}{\sqrt{2} + 1} \] (13)

\[ \gamma = \frac{2}{\sqrt{2} + 1} \] (14)

Let \( k = \frac{\alpha}{2} = \frac{\sqrt{2}}{2(\sqrt{2} + 1)} = \frac{1}{2 + \sqrt{2}} \approx 0.292895 \).

Now we can conclude that no matter what state Alice sends to Bob, he will always confirm the identity of the state he received with success probability of \( k \).

Below we present the k-OT sub protocol.

Before the protocol, Alice and Bob agree on that \( |\varphi_1\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \) and \( |\varphi_2\rangle = |1\rangle \) represent the bit 0 and 1 respectively. \( E_i \) are defined as (8) ~ (10) , and \( \alpha \), \( \beta \) and \( \gamma \) are defined as (13) ~ (14).

**Protocol 1 k-OT_POVM (b)**

Step 1. Let \( b \) denotes the bit Alice wants to send. If \( b = 0 \), then she sends Bob \( |\varphi_1\rangle \). Otherwise she sends Bob \( |\varphi_2\rangle \).

Step 2. After received the state, Bob performs the POVM measurements with \( \{E_1, E_2, E_3\} \).

It is easy to know that protocol k-OT_POVM (b) satisfy:

- Alice knows \( b = 0 \) or \( b = 1 \).
- Bob gets bit \( b \) from Alice with probability \( k \).
- Alice does not know whether Bob got \( b \) rightly or not.

### 4 The new ANDOS Protocol

In this section we present a new ANDOS scheme based on protocol 1, then we discuss its correctness and security.

Before presenting our new scheme, we make the following assumption as in [1]: we assume that Alice is honest when she claims to be willing to disclose one secret, that is, she is not going to send junk to Bob.

**4.1 Quantum ANDOS protocol based on POVM measurements**

Let \( t \leq 5 \) be the number of Alice’s secrets, and \( s_1, s_2, \ldots, s_t \) be the secrets themselves. Let \( c \) be Bob’s choice (i.e. Bob wants to get \( s_c \)). In order for Alice to sell one secret to Bob, she uses protocol ANDOS_POVM(\( s_1, s_2, \ldots, s_t \)) (c) with Bob.

Before the protocol, Alice and Bob agree on a security parameter \( N \) used below.

**Protocol 2 ANDOS_POVM (s_1,s_2,…,s_t) (c)**

Step 1. Alice selects uniformly and randomly a N-bit sting \( R = \{r_1, r_2, \ldots, r_N\} \).

Step 2. For each bit in \( R \), Alice use the
k-OT_POVM (b) protocol to transmit the relevant state to Bob.

Step 3. Bob partitions his measurement outcomes into $t$ sets

$$B_i = \{a_{i(i-1)+1}, a_{i(i-1)+2}, \ldots, a_{i}\} \quad (i \in [1,t]),$$

where $\theta = [0.2N]$ and such that he knows every $r_{s_i}$ affirmatively for each $a_i \in B_j (j \in [\theta(c-1)+1, \theta c])$.

Step 4. Bob sends $t$-tuple $(X_1, X_2, \ldots, X_t) = (B_1, B_2, \ldots, B_t)$ to Alice.

Step 5. For each $i \in [1,t]$, Alice gets a binary string $m_i = r_{a_{i(i-1)+1}}r_{a_{i(i-1)+2}} \cdots r_{a_i}$. Then she sends Bob $t$-tuple $(Y_1, Y_2, \ldots, Y_t) = (s_1 \oplus m_1, s_2 \oplus m_2, \ldots, s_t \oplus m_t)$.

Step 6. Bob computes $Y_e \oplus m_e$ to get his secret string $s_e$.

### 4.2 Analysis and proofs

At the end of the above ANDOS protocol, Bob’s knowledge about Alice’s secrets can be divided into three cases:

- $A_i$: Bob obtains nothing about Alice’s secrets.
- $A_j$: Bob gets only one of Alice’s secrets.
- $A_k$: Bob gets more than one secret.

Clearly, the above three mutually exclusive events constitute a complete event group. What is the probability that each event occurs? Indeed, we show that

**Theorem 1** For sufficiently large $N$, there exist a constant $\lambda (0 < \lambda < 1)$ such that Bob can obtain at least one secret with probability at least $1 - \lambda^N$.

In order to prove Theorem 1 we need an inequality named “Chernoff Bound”[9]. We present the inequality first, and then come back to the proof.

**Lemma 2 Chernoff Bound:** Let $p \leq \frac{1}{2}$, and let $X_1, X_2, \ldots, X_n$ be independent $0-1$ random variables, so that $\Pr[X_i = 1] = p$ for each $i$. Then for all $\epsilon$, $0 < \epsilon \leq p(1-p)$, we have

$$\Pr \left[ \frac{\sum_{i=1}^{n} X_i}{n} - p > \epsilon \right] < 2 \cdot e^{-\frac{\epsilon^2}{2p(1-p)}} \quad (15)$$

**Proof of Theorem 1.** Let

$$X_i = \begin{cases} 1 & \text{if Bob got } r_i \text{ reliably} \\ 0 & \text{otherwise} \end{cases} \quad (i \in [1,N]) \quad (16)$$

By definition $\Pr[X_i = 1] = k$, $\Pr[X_i = 0] = 1 - k$, and $\sum_{i=1}^{N} X_i$ indexes the total number of the bits Bob reliably got from $R = \{r_1, r_2, \ldots, r_N\}$.

If we let $\epsilon = k - 0.2 \approx 0.092895$, then by inequality (15) we get

$$\Pr \left[ \frac{\sum_{i=1}^{N} X_i}{N} - k > k - 0.2 \right] < 2 \cdot e^{-\frac{(k-0.2)^2}{2N(1-k)}} \quad (17)$$

Similarly, if we let $\epsilon = 0.392895 - k \approx 0.100000$, then we get

$$\Pr \left[ \frac{\sum_{i=1}^{N} X_i}{N} - k > 0.392895 - k \right] < 2 \cdot e^{-\frac{(0.392895-k)^2}{2N(1-k)}} \quad (18)$$

By inequality (17) we get

$$\Pr[Bob \ gets \ at \ least \ one \ secret] = 1 - \Pr[A_i] = 1 - \Pr \left[ \frac{\sum_{i=1}^{N} X_i}{N} < \theta \right]$$

$$= 1 - \Pr \left[ \frac{\sum_{i=1}^{N} X_i}{N} > \theta \right]$$

$$= 1 - \Pr \left[ k - \frac{\sum_{i=1}^{N} X_i}{N} > k - 0.2 + \frac{0.2N - \theta}{N} \right]$$

$$\geq 1 - \Pr \left[ k - \frac{\sum_{i=1}^{N} X_i}{N} > k - 0.2 \right] > 1 - 2e^{-0.020833N}$$

As long as $N$ is large enough

$$1 - 2e^{-0.020833N} > 1 - (e^{-0.020})^N$$

Therefore for any constant $\lambda$, $e^{-0.020} < \lambda < 1$, Theorem 1 follows. \(\square\)

Theorem 1 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
Theorem 3 For sufficiently large $N$, there exists a constant $\eta$ ($0 < \eta < 1$) such that Bob can obtain more than one secret with probability at most $\eta^N$.

Proof. Let $X_i$ be defined as (16), then

$$\Pr[ \text{Bob gets more than one secret} ] = \Pr[A_i]$$

$$= \Pr \left[ \sum_{i=1}^{N} X_i \geq 2\theta \right] \leq \Pr \left[ \sum_{i=1}^{N} X_i > 2 \cdot 0.2N - 2 \right]$$

$$= \Pr \left[ \frac{\sum_{i=1}^{N} X_i}{N} - k > 0.4 - \frac{2}{N} - k \right]$$

$$\leq \Pr \left[ \frac{\sum_{i=1}^{N} X_i}{N} - k > 0.392895 - k \right]$$

$$\leq \Pr \left[ \frac{\sum_{i=1}^{N} X_i}{N} - k > 0.392895 - k \right]$$

$$< 2e^{-0.024142N}$$

where the last inequality uses (18).

As long as $N$ is large enough, the probability that Bob will get more than one secret from Alice can be made arbitrarily small.

Similarly, for any constant $\eta$, $e^{-0.024} < \eta < 1$, Theorem 3 follows. \hfill $\blacksquare$

Theorem 1 and 3 ensure that after protocol 2, an honest or semi-honest Bob can get only $s_c$ from Alice. Now let us consider for a cheating Bob, if he cheats by measuring Alice’s states in bases other than $\{E_1,E_2,E_3\}$, will he successfully get more than one secret?

Theorem 4 Even if cheating Bob performs other measurements instead of POVM, it will help him little to get more than one secret.

Proof. Besides POVM measurement, Bob can perform projective measurements that may maximize his information about each bit in string $R$.

Suppose the measurement basis Bob chooses is “+$”, then for state $\ket{\phi_1} = \frac{-\ket{0} + \ket{1}}{\sqrt{2}}$, the probabilities of outcomes of $\ket{0}$ and $\ket{1}$ are both $\frac{1}{2}$. Similarly, if the state Alice sent is $\ket{\phi_2} = \ket{1}$, the probabilities of outcomes of $\ket{0}$ and $\ket{1}$ are 0 and 1 respectively. Therefore if $R$ is uniformly distributed, Bob obtains each of Alice’s states with probability

$$\frac{1}{2} \times \frac{1}{2} + \frac{1}{2} \times 1 = 0.75$$

At a first glance, the result seems better than the success probability $k$ in POVM measurements. But notice that the probability 0.75 here does not convince Bob that he has got the state reliably. Indeed, there exist only one case that Bob believes he has obtained the state rightly, i.e. the result of Bob’s measurement is $\ket{0}$. In this case, Bob can infer the state Alice sent must have been $\ket{\phi_1}$. However, the probability of this case is only $\frac{1}{4}$, which is even worse than $k$.

If Bob chooses “$\times$” basis to perform the measurements, the result is similar. We omit the analysis for the sake of brevity.

However, if Bob’s choice is non-canonical bases, then for whether $\ket{\phi_1}$ or $\ket{\phi_2}$ all the measurement outcomes will large than 0, which will render Bob unsure of any state. \hfill $\blacksquare$

Below we shall show that there is very little Alice can do in order to cheat in protocol 2.

Theorem 5 Alice knows nothing about Bob’s choice $c$ in protocol 2.

Proof. In fact, Bob does not reveal anything that involves $c$ until Step 4. Moreover, $B_i$ 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 t-tuple $(X_1,X_2,\ldots,X_r) = (B_1,B_2,\ldots,B_r)$ to Alice at step 4 does not reveal anything about $c$ 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 deviated protocol 2 by sending entangled states to Bob, it will not help her to tell which secret Bob has
obtained. Suppose Alice sends $|ϕ_2^{'}) = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$ instead of $|ϕ_2\rangle = |1\rangle$. Bob receives it and performs POVM measurement as usual. By equation (2) and (6) we know that, the measurement outcomes no longer has 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 at the start of this section the whole of the scheme will fall to the ground. Obviously, this kind of attack is trivial and Alice will not take it.

Finally, we would like to discuss the wire-tapping detecting ability of protocol 2. Suppose there exists an eavesdropper, say Eve, on the channel, who tries to eavesdrop on the transmission. For each state, Eve will not be able to “read” it without altering it. Each state sent by Alice is converted to electrical energy as it is measured and destroyed, so Eve must generate a new state to send to Bob. By the proof of Theorem 4 it is clear that Eve’s best strategy is to perform the same POVM measurements adopted by Bob. For each photon sent by Alice, the probability of Eve’s failing to confirm its state is $1 - k$. 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 of each state is equal to $\left(k + \frac{1-k}{2}\right)^k \approx 0.189341$, which is a value much less than $k$. 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 and they will terminate the ANDOS protocol.

5 Conclusion and Open Questions
We have described a complete protocol for ANDOS based on POVM measurements. We have shown that in the light of the laws of quantum mechanics, this protocol cannot be cheated by either party except with exponentially small probability. The protocol in this paper does not invoke any bit commitment protocol and any eavesdropper can be detected efficiently. Moreover, both Alice and Bob have no limitation on their computing power in our scheme. Therefore our ANDOS protocol is unconditionally secure.

In order to make the analysis easier, we present our ANDOS scheme without the consideration of transmission errors on the channel. In fact, it is impractical to some extent.

In our new quantum ANDOS scheme, the upper bound of the number of Alice’s secrets is 5. In fact, we can let $\theta = \lceil 0.16N \rceil$ in step 3, then the upper bound can be improved to 6 without loss of security.

How to construct a secure ANDOS protocol based on POVM measurements that can tolerate transmission errors? Can the number of secrets be improved to greater than 6? We will leave them as open questions.

References: