

# Quantum Oblivious Transfer Based on POVM Measurements

Wei Yang , Liusheng Huang , Yonglong Luo , Mingjun Xiao  
Anhui Province—MOST Co-Key Laboratory of High Performance Computing and Its Application,  
University of Science and Technology of China, Hefei 230027, China

**Abstract** - Oblivious transfer (OT) is an important primitive in cryptography. In chosen one-out-of-two OT, Alice offers two bits, one of which Bob can choose to read, not learning any information about the other bit. Alice on the other hand does not obtain any information about Bob's choice. We present a new technique for the same task in quantum environment, based on POVM measurements. It is shown that our method has two important advantages over the previous approaches. First, it is unconditionally secure without invoking a commitment scheme, and second, it is more efficient in terms of communication complexity.

**Key words:** Oblivious transfer, POVM measurements, Unconditional security

## 1 Introduction

Generally speaking , Oblivious transfer (OT) describes such a kind of primitive in cryptography that the receiver can get only one message from a secret message set owned by the sender without revealing his choice. We can, without loss of generality, assume the content of each message to be a single bit. OT is an important primitive in cryptography and can be used to construct many cryptographic protocols such as Zero Knowledge Proof (ZKP), Verifiable Secret Sharing (VSS) and Secure Multi-party Computation (SMC). OT is also the cornerstone of Private Information Retrieval (PIR).

The concept of OT was first introduced by Rabin in [1]. Subsequently, the related notion of “chosen one-out-of-two oblivious transfer” ( $\binom{2}{1}$ -OT) was proposed by Even, Goldreich and Lempel in [2]. Crépeau [3] presented a proof that the two notions are equivalent in the sense that either one can be achieved from another by reduction. So, from a theoretical point of view, it does not matter which of these two protocols we achieve. Because  $\binom{2}{1}$ -OT is most accepted and widely used model of OT so far, the quantum OT (QOT) protocol described in this paper implements  $\binom{2}{1}$ -OT. The following is a general definition of  $\binom{2}{1}$ -OT.

*Definition 1.*  $\binom{2}{1}$ -OT

Alice has two bits, named  $b_0$  and  $b_1$ . Bob can choose to get either one of them, noted as  $b_c (c \in \{0,1\})$ . At the end of the transmission, it requires that:

- ① Bob gets  $b_c$  only and gets no information about  $b_{1-c}$ .
- ② Alice does not know which bit Bob got.

After [1] and [2], some new OT models such as  $\binom{n}{1}$ -OT, All-or-nothing Disclosure of Secrets (ANDOS) and Generalized OT (GOT) were proposed [4~6]. They can all be reduced to  $\binom{2}{1}$ -OT. Universal OT or short for UOT was proposed in [7] which proved that  $\binom{2}{1}$ -OT can be reduced to UOT.

However, previous OT protocols in classical environment all have some defects. For example, most of previous OT protocols relied either on public-key cryptography [1~2] or on additional assumptions [8~11] which will be very vulnerable under quantum mechanics. [9] employed a third party named *Trusted Initializer* to finish part of the communicational and computational tasks. However, it is quite hard to get a trusted even an oblivious third party in practice.

The troubles with classical OT protocols can be fairly well solved in quantum computational environment. Compared to OT protocols in classical

environment, Quantum OT (QOT) protocols have a few advantages:

① *Higher security.* Both Alice and Bob have no limitation on their computing power.

② *More efficient wire-tapping detecting.* According to *Heisengberg Uncertainty Principle* and *quantum no-cloning theorem*, no eavesdropper can escape being detected. Obviously, this is impossible in classical environment.

③ *Stronger soundness.* There is no necessity to make any assumption on transmission channel. Also any trusted or oblivious third party is not needed at all.

First practical QOT protocol was presented by Bennett, Brassard, Crépeau and Skubiszewska in [12]. But they used a bit commitment protocol as a sub protocol in their scheme. In fact, unconditionally secure bit commitment is known to be impossible in both the classical and quantum worlds ([13]~[14]). Thus the protocol given in [12] does not have the property of unconditional security.

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

① It need not invoke a bit commitment scheme as a building block and thus has the property of unconditional security.

② In our QOT protocol, Alice need not reveal her random bit sequence (or the transmission bases she used) to Bob. As a result, it reduces the interactive cost and communication complexity.

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 t-OT protocol based on POVM constructed as a sub protocol in our QOT scheme is presented in section 3. The t-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 t-OT protocol to construct our QOT scheme. We also prove that the QOT protocol presented in this paper cannot be cheated by either party. 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:

$$|\varphi\rangle = a|0\rangle + b|1\rangle \quad (1)$$

where  $a$  and  $b$  are complex numbers and satisfy

$$|a|^2 + |b|^2 = 1 \quad (2)$$

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  $|\varphi\rangle$  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  $|\varphi\rangle$  immediately before the measurement then the probability that result  $m$  occurs is given by

$$p(m) = \langle \varphi | M_m^+ M_m | \varphi \rangle \quad (3)$$

where  $M_m^+$  denotes the complex conjugate transpose of  $M_m$ , and the state of the system after the measurement collapses to

$$\frac{M_m |\varphi\rangle}{\sqrt{\langle \varphi | M_m^+ M_m | \varphi \rangle}} \quad (4)$$

The measurement operators satisfy the completeness equation,

$$\sum_m M_m^+ M_m = I \quad (5)$$

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

$$1 = \sum_m p(m) = \sum_m \langle \varphi | M_m^+ M_m | \varphi \rangle \quad (6)$$

This equation is satisfied for all  $|\varphi\rangle$ .

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

### 2.2 POVM Measurements [15]

POVM is a special case of the general measurement formalism. POVMs have a very elegant nature that

they can distinguish non-orthogonal states reliably.

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

$$E_m \equiv M_m^\dagger M_m \quad (7)$$

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

$p(m) = \langle \varphi | E_m | \varphi \rangle$ . 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 t-OT sub protocol based on POVM measurements

First let us define two constant that will be used later:

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

In order to distinguish two non-orthogonal states  $|\varphi_1\rangle = \frac{-|0\rangle + |1\rangle}{\sqrt{2}}$  and  $|\varphi_2\rangle = |1\rangle$  reliably with successful probability of some constant, let us consider a POVM containing three elements,

$$E_1 = \alpha \cdot \left( \frac{|0\rangle + |1\rangle}{\sqrt{2}} \right) \left( \frac{\langle 0| + \langle 1|}{\sqrt{2}} \right) = \frac{\alpha}{2} \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \quad (8)$$

$$E_2 = \beta \cdot |0\rangle\langle 0| = \beta \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \quad (9)$$

$$E_3 = \gamma \cdot (-\nu|0\rangle + \mu|1\rangle)(-\nu\langle 0| + \mu\langle 1|) \\ = \gamma \begin{pmatrix} \nu^2 & -\mu\nu \\ -\mu\nu & \mu^2 \end{pmatrix} \quad (10)$$

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:

$$E_1 + E_2 + E_3 = I \quad (11)$$

By equation (3) and (7) we can get that, for 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 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 to 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

$$\frac{\beta}{2} = \frac{\alpha}{2} \quad (12)$$

Combine (8) ~ (12) we can get

$$\alpha = \beta = \frac{\sqrt{2}}{\sqrt{2}+1} \quad (13)$$

$$\gamma = \frac{2}{\sqrt{2}+1} \quad (14)$$

$$\text{Let } t = \frac{\alpha}{2} = \frac{1}{2} \cdot \frac{\sqrt{2}}{\sqrt{2}+1} = \frac{1}{2+\sqrt{2}} \approx 0.292895.$$

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 successful probability of  $t$ .

Below we present the t-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.  $E_1 \sim E_3$  are defined as (8)~(10), and  $\alpha$ ,  $\beta$  and  $\gamma$  are defined as (13) ~ (14).

*Protocol 1 t-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. Bob receives the state and performs the POVM measurements with  $\{E_1, E_2, E_3\}$ .*

It is easy to know that protocol 1 satisfy:

- ① Alice knows  $b=0$  or  $b=1$ .
- ② Bob gets bit  $b$  from Alice with probability  $t$ .
- ③ Alice does not know whether Bob got  $b$  rightly or not.

## 4 Quantum Oblivious Transfer

In this section we present a new Quantum Oblivious Transfer (QOT) scheme based on protocol 1 and discuss its correctness and security.

### 4.1 QOT protocol based on POVM measurements

Let  $b_0$  and  $b_1$  be Alice's bits and let  $c$  be Bob's choice (i.e. Bob wants to get  $b_c$ ). In order for Alice to effect an oblivious transfer of bit  $b$  to Bob, she uses protocol  $OT\_POVM(b_0, b_1)(c)$  with Bob.

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

*Protocol 2*  $OT\_POVM(b_0, b_1)(c)$

*Step 1.* Alice selects uniformly and randomly a  $N$ -bit string  $S = \{s_1, s_2, \dots, s_N\}$ .

*Step 2.* For each bit in  $S$ , Alice use the  $t$ - $OT\_POVM(b)$  protocol to transmit the relevant state to Bob.

*Step 3.* Bob partitions his measurement outcomes into two sets  $R_0 = \{i_1, i_2, \dots, i_\theta\}$  and  $R_1 = \{i_{\theta+1}, i_{\theta+2}, \dots, i_{2\theta}\}$ ,

where  $\theta = \left\lfloor \frac{3tN}{4} \right\rfloor$  and such that he knows every  $s_{i_j}$  affirmatively for each  $i_j \in R_0 (j \in [1, \theta])$ .

*Step 4.* Bob sends pairs  $(X, Y) = (R_c, R_{1-c})$  to Alice.

*Step 5.* Alice computes  $m_0 = \bigoplus_{x \in X} s_x$  and  $m_1 = \bigoplus_{y \in Y} s_y$ .

Then she sends Bob pairs  $(d_0, d_1) = (b_0 \oplus m_0, b_1 \oplus m_1)$ .

*Step 6.* Bob computes  $d_c \oplus m_c$  to get his secret bit  $b_c$ .

### 4.2 Analysis and proofs

At the end of the above QOT protocol, Bob's knowledge about  $b_0$  and  $b_1$  can be divided into three cases:

$A_1$  : Bob obtains none of  $b_0$  and  $b_1$ .

$A_2$  : Bob gets only one of  $b_0$  and  $b_1$ .

$A_3$  : Bob gets both bits.

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 bit of  $b_0$  and  $b_1$  with probability at least  $1 - \lambda^N$ .

In order to prove Theorem 1 we need an inequality named "Chernoff Bound"[16]. We present the inequality first, then come back to the proof.

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

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

*Proof of Theorem 1.* Let

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

By definition  $\Pr[x_i = 1] = t$ ,  $\Pr[x_i = 0] = 1 - t$ , and  $\sum_{i=1}^N x_i$  indexes the total number of the bits Bob reliably got from  $S = \{s_1, s_2, \dots, s_N\}$ .

If we let  $\varepsilon = \frac{t}{4}$ , then by inequality (15) we get

$$\Pr \left[ \left| \frac{\sum_{i=1}^N X_i}{N} - t \right| > \frac{t}{4} \right] < 2 \cdot e^{-\frac{(\frac{t}{4})^2}{2t(1-t)}N} \approx 2e^{-0.012944N} \quad (17)$$

Similarly, if we let  $\varepsilon = 0.140000$ , then we get

$$\Pr \left[ \left| \frac{\sum_{i=1}^N X_i}{N} - t \right| > 0.140000 \right] < 2 \cdot e^{-\frac{(0.140000)^2}{2t(1-t)}N} \approx 2e^{-0.047319N} \quad (18)$$

By inequality (17) we get

$$\begin{aligned} & \Pr[\text{Bob gets at least one of } b_0 \text{ and } b_1] \\ &= 1 - \Pr[A_1] = 1 - \Pr \left[ \sum_{i=1}^N X_i < \theta \right] \\ &= 1 - \Pr \left[ \frac{\sum_{i=1}^N X_i}{N} > -\frac{\theta}{N} \right] = 1 - \Pr \left[ t - \frac{\sum_{i=1}^N X_i}{N} > \frac{t}{4} + \frac{3tN - \theta}{4N} \right] \end{aligned}$$

$$\geq 1 - \Pr \left[ t - \frac{\sum_{i=1}^N X_i}{N} > \frac{t}{4} \right] \geq 1 - \Pr \left[ \left| \frac{\sum_{i=1}^N X_i}{N} - t \right| > \frac{t}{4} \right]$$

$$> 1 - 2e^{-0.012944N}$$

As long as  $N$  is large enough

$$1 - 2e^{-0.012944N} > 1 - (e^{-0.012})^N$$

Therefore for any constant  $\lambda$ ,  $e^{-0.012} < \lambda < 1$ , Theorem 1 follows.  $\square$

Theorem 1 tells us that Bob can get at least one of Alice's two bits with a probability that can be made arbitrarily close to 1. Then, suppose Bob is semi-honest, will he obtain both bits sent by Alice? Or in other word, what is the probability that event  $A_3$  occurs? In fact, we have

*Theorem 3.* For sufficiently large  $N$ , there exist a constant  $\eta$  ( $0 < \eta < 1$ ) such that Bob can obtain both  $b_0$  and  $b_1$  with probability at most  $\eta^N$ .

*Proof.* Let  $x_i$  be defined as (16), we get

$$\Pr[\text{Bob gets both } b_0 \text{ and } b_1] = \Pr[A_3] = \Pr \left[ \sum_{i=1}^N X_i \geq 2\theta \right]$$

$$\leq \Pr \left[ \sum_{i=1}^N X_i > 2 \cdot \frac{3tN}{4} - 2 \right] = \Pr \left[ \frac{\sum_{i=1}^N X_i}{N} - t > \frac{t}{2} - \frac{2}{N} \right]$$

$$\leq \Pr \left[ \frac{\sum_{i=1}^N X_i}{N} - t > 0.140000 \right] \leq \Pr \left[ \left| \frac{\sum_{i=1}^N X_i}{N} - t \right| > 0.140000 \right]$$

$$< 2e^{-0.047319N}$$

where the last inequality uses (18).

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

Similarly, for any constant  $\eta$ ,  $e^{-0.047} < \eta < 1$ , Theorem 3 follows.  $\square$

Theorem 1 and 3 ensure that after protocol 2, an honest or semi-honest Bob can get only  $b_c$  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 both of  $b_0$  and  $b_1$ ?

*Theorem 4.* Even if cheating Bob performs other

measurements instead of POVM, it will help him little to get  $b_0$  and  $b_1$  at the same time.

*Proof.* Besides POVM measurement, Bob can do projective measurements which may maximize his information about each bit in *string*  $S$ .

Suppose the measurement basis Bob chooses is “+”, then for state  $|\varphi_1\rangle = \frac{-|0\rangle + |1\rangle}{\sqrt{2}}$ , the probabilities

of outcomes of  $|0\rangle$  and  $|1\rangle$  are both  $\frac{1}{2}$ . Similarly if the state Alice sent is  $|\varphi_2\rangle = |1\rangle$ , the probabilities of outcomes of  $|0\rangle$  and  $|1\rangle$  are 0 and 1 respectively. Therefore if  $S$  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  $t$  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  $|0\rangle$ . In this case, Bob can infer the state Alice sent must have been  $|\varphi_1\rangle$ . However, the probability of this case is only  $\frac{1}{4}$ , which is even worse than  $t$ .

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  $|\varphi_1\rangle$  or  $|\varphi_2\rangle$  all the measurement outcomes will large than 0, which will render Bob unsure of any state.  $\square$

Below we shall show that there is very little Alice can do in order to cheat in protocol 2. However, Alice can cheat at step 5 by sending Bob two bits randomly. We know that nothing can prevent Alice do this even if there exist unconditionally secure bit commitment scheme. But we need not worry about this condition, because it is a trivial event. Definition 1 itself implies that Alice *wants to* transmit Bob one of her two bits.

*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,  $R_c$  is purely random and information-theoretically hidden from Alice for that she is unable to distinguish which of Bob's set had been measured with affirmative

outcomes. Therefore, sending pairs  $(X, Y) = (R_c, R_{1-c})$  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 bit Bob has obtained.

Suppose Alice sends  $|\phi_2\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$  instead of  $|\phi_2\rangle = |1\rangle$ . 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 confirm a state correctly. The subsequence is that Bob will get neither of the two bits and the whole of the scheme will fall to the ground. This, however, violates the original intention of Alice. Obviously, this kind of attack is trivial and Alice will not take it.  $\square$

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. She 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  $1-t$ . 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  $\left(t + \frac{1-t}{2}\right) \cdot t \approx 0.189341$ , which is a value much less than  $t$ . 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 QOT protocol.

## 5 Conclusion and Open Questions

We have described a complete protocol for  $\begin{pmatrix} 2 \\ 1 \end{pmatrix}$ -OT based on POVM measurements. We have shown that in the light of the laws of quantum mechanics, this protocol can not be cheated by either party except

with exponentially small probability. Moreover, the protocol in this paper does not invoke any bit commitment protocol as a building block and any eavesdropper can be detected efficiently. Therefore our QOT protocol is unconditionally secure.

In order to make the analysis easier, we present our QOT scheme without the consideration of transmission errors on the channel. In fact, it is impractical to some extent. How to construct a secure QOT protocol based on POVM measurements that can tolerate transmission errors? We will leave it as an open question.

## References

- [1] Rabin M O. How to exchange secrets by oblivious transfer. Technical Memo TR-81, Aiken Computation Laboratory, Harvard University, 1981.
- [2] Shimon Even, Oded Goldreich, and A. Lempel. A randomized protocol for signing contracts. Proc. CRYPTO '82, Plenum Press, 1983. 205-210
- [3] Claude Crépeau. Equivalence between two flavours of oblivious transfers. Lecture Notes In Computer Science, Vol. 293, 1987.
- [4] G. Brassard, C. Crépeau, and Jean-Marc Robert. Information theoretic reductions among disclosure problems. Proc the 27th IEEE Symposium on Foundations of Computer Science, 1986. 168-173
- [5] G. Brassard, C. Crépeau, and Jean-Marc Robert. All-or-nothing disclosure of secrets. In A.M. Odlyzko, editor, Proc. CRYPTO 86, pages 234-238. Springer-Verlag, 1987. Lecture Notes in Computer Science No. 263
- [6] M Naor, B Pinkas. Efficient oblivious transfer protocols. In Proceedings of the twelfth annual ACM-SIAM symposium on Discrete algorithms, 2001.
- [7] Christian Cachin. On the Foundations of Oblivious Transfer. In Proceedings of EUROCRYPT '98, Lecture Notes in Computer Science, Springer, 1998.
- [8] Claude Crépeau. Efficient cryptographic protocols based on noisy channels. In Proceedings of EUROCRYPT 97.
- [9] RL Rivest. Unconditionally Secure Commitment and Oblivious Transfer Schemes Using Private Channels and a Trusted Initializer. Manuscript, 1999.
- [10] G Brassard, C Crépeau, S Wolf. Oblivious Transfers and Privacy Amplification. Journal of Cryptology, 2003.
- [11] S Wolf, J Wullschleger. Zero-Error Information and Applications in Cryptography. Proceedings of 2004 IEEE Information Theory Workshop
- [12] Charles H. Bennett, Gilles Brassard, Claude Crépeau, and Marie Helene Skubiszewska. Practical quantum oblivious transfer. Advances in Cryptology

— Crypto '91 Proceedings, 1991, Springer - Verlag.  
351 - 366

[13] Hoi-Kwong Lo, H.F. Chau. "Is Quantum Bit Commitment Really Possible?". Los Alamos preprint archive quant-ph/9603004, 1996.

[14] Dominic Mayers. Unconditionally Secure Quantum Bit Commitment is Impossible. Fourth Workshop on Physics and Computation-PhysComp '96, 1996.

[15] MA Nielsen, IL Chuang. Quantum computation and quantum information. Cambridge University Press, 2000.

[16] Oded Goldreich. Foundation of Cryptography Basic Tools. Cambridge University Press, 2001.