CHOOSING T-OUT-OF-N SECRETS BY OBLIVIOUS TRANSFER

Jung-San LEE and Chin-Chen CHANG

Abstract: Oblivious Transfer (OT) has been regarded as one of the most significant cryptography tools in recent decades. Since the mechanism of OT is widely used in many applications such as e-commerce, secret information exchange, and games, various OT schemes have been proposed to improve its functionality and efficiency. In 2001, Naor and Pinkas proposed a secure 1-out-of-n OT protocol, in which the sender has n messages and the chooser can get one of these n messages in each protocol run. What is more, the sender cannot find which message has been chosen by the chooser and the chooser knows only the correct message. In 2004, Wakaha and Ryota proposed a secure t-out-of-n OT protocol, which is an extension of the 1-out-of-n OT protocol proposed by Naor and Pinkas. Wakaha and Ryota's t-out-of-n OT protocol allows the chooser to get t messages from the sender simultaneously in each protocol run. Besides, the sender cannot know what the chooser has chosen and the chooser can only know the exact t messages. However, getting deep understanding of Wakaha and Ryota's protocol, it could be concluded that it still lacks efficiency such that it is hard to be applied in real-world applications. In this article, a secure and efficient t-out-of-n OT protocol based on the Generalized Chinese Remainder Theorem is proposed, in which the chooser can securely get t messages from the sender simultaneously in each protocol run. The efficiency of the proposed t-out-of-n OT protocol is higher than that of Wakaha and Ryota's protocol in terms of practical application.

Keywords: Oblivious Transfer, Generalized Chinese Remainder Theorem, Communications, Secrets Exchange.

Introduction

Recently, numerous Oblivious Transfer (OT) protocols have been applied in many applications such as e-commerce, secret information exchange, games, and others. Therefore, OT has become an important cryptography tool. In 1981, Rabin first proposed the concept of oblivious transfer.[1] People can think of Rabin's OT protocol as a game between two participants, Alice and Bob, where Alice is the sender and Bob is the chooser. Alice sends one bit to Bob, and Bob will get either nothing with probability 1/2 or the same bit with the same probability. What is more, Alice cannot know which event has happened to Bob. Rabin's idea of OT has attracted a lot of attention; it has become a popular research topic since it was proposed.

An extended concept is one-out-of-two OT protocol, denoted as (OT_1^2), in which Alice sends two bits to Bob, b_1 and b_2. Besides, Bob can choose to get either b_1 or b_2 and can receive one of the two bits with the same probability 1/2. However, Alice cannot know which bit Bob has chosen in this protocol run. Later, a more significant version *1*-out-of-*n* OT protocol, denoted as (OT_1^n), was proposed, in which Alice possesses *n* messages and Bob can get one of them in each protocol run. Similarly to the OT_1^2-protocol, Alice cannot know which message Bob has received, and Bob can get nothing else than the correct message.[2,3,4,5,6]

In general, many OT protocols have been proposed with the objective to improve efficiency or functionality. The most recent research on OT protocols is the *t*-out-of-*n* version, denoted as (OT_t^n), in which Alice possesses *n* messages and Bob can get *t* out of these *n* messages simultaneously in each protocol run. Besides, Alice cannot find out which messages Bob has received, and Bob can know nothing other than the correct *t* messages. However, the majority of these improvements are either based on parallel computing or need heavy computation.[7,8,9,10,11,12,13,14] In 2004, Wakaha and Ryota proposed a secure *t*-out-of-*n* OT protocol, which is an extension of the 1-out-of-*n* OT protocol proposed by Naor and Pinkas. Although Wakaha and Ryota's *t*-out-of-*n* OT protocol allows the chooser to get *t* messages from the sender simultaneously in each protocol run, getting understanding of Wakaha and Ryota's *t*-out-of-*n* OT protocol shows that it still lacks efficiency.[15,16]

In this article, the authors propose a secure and more efficient version of the *t*-out-of-*n* OT protocol based on the Generalized Chinese Remainder Theorem (GCRT).[17] The proposed OT protocol can meet the following requirements, which are considered as the most important ones for the general OT protocols.[18,19,20]

- *Requirement 1*: *Correctness* – If both the sender and the chooser follow the *t*-out-of-*n* OT protocol, the chooser will receive the correct *t* messages after executing the protocol with the sender.
- *Requirement 2*: *Privacy of the chooser* – After the OT protocol is performed with the chooser the sender cannot know which messages are chosen by the chooser.
- *Requirement 3*: *Privacy of the sender* – After the OT protocol is performed with the sender the chooser can get nothing else except these *t* messages.

The rest of this paper is organized as follows. The next section will review the 1-out-of-*n* OT protocol proposed by Naor and Pinkas and the *t*-out-of-*n* OT protocol proposed by Wakaha and Ryota. Some preliminaries are described afterwards, followed by description of the proposed protocol. Some discussions and analyses of the proposed protocol and comparisons between the proposed OT_t^n protocol and other related works are given next. Finally, the last section gives some conclusions.

Review of Related Work

This section introduces the 1-out-of-*n* OT protocol proposed by Naor and Pinkas and the *t*-out-of-*n* OT protocol proposed by Wakaha and Ryota.

Review of Naor and Pinkas's 1-out-of-n OT Protocol

Prior to describing Naor and Pinkas's 1-out-of-*n* OT protocol, the authors define some notations used in their protocol. Let g be a generator of a multiplicative group with a prime order q. Alice is the sender, while Bob is the chooser. $M_1, M_2, \ldots, M_n \in < g >$ are the *n* messages kept by the sender Alice. G is a large prime. M_c is the choice of the chooser Bob, where *c* is the serial number of the chosen message and $1 \le c \le n$. The details of the protocol proposed by Naor and Pinkas are given below.

Step 1: Bob constructs a polynomial $f(x)$ as follows

$$f(x) = x - c,$$

and then he chooses a and b randomly from Z_q. Next, Bob generates

$$f'(x) = f(x) + ab = x + (ab - c),$$

and sets

$$e = ab - c.$$

Finally, Bob computes

$$A = g^a \bmod G,$$

$$B = g^b \bmod G, \text{ and}$$

$$E = g^{e} \bmod G,$$

and sends the messages $\{A, B, E\}$ to Alice.

Step 2: After receiving the messages sent by Bob, Alice computes

$$Y_i = E\, g^{i} \bmod G, \text{ for } i = 1, 2, \ldots, n\,.$$

Then, for $i = 1, 2, \ldots, n$, Alice selects s_i and r_i randomly from Z_q and computes

$$H_i = A^{s_i} g^{r_i} \bmod G,$$

$$K_i = Y_i^{s_i} B^{r_i} \bmod G, \text{ and}$$

$$F_i = K_i * M_i \bmod G.$$

Finally, Alice sends all pairs of (H_i , F_i) to Bob, where $i = 1, 2, \ldots, n$.

Step 3: When Bob receives the messages sent by Alice, he computes

$$K_c = H_c^{b} \bmod G,$$

and then reveals the demanded message as follows

$$M'_c = F_c / K_c \bmod G.$$

Review of Wakaha and Ryota's t-out-of-n OT Protocol

In this subsection, the authors introduce Wakaha and Ryota's OT_t^n protocol which is an extension of Naor and Pinkas's 1-out-of-*n* OT protocol. The authors begin with definition of the notations used in the OT_t^n protocol proposed by Naor and Pinkas. Let g be a generator of a multiplicative group with a prime order q . G is a large prime number. The sender Alice possesses *n* messages M_1, M_2, …, and M_n , where M_1, M_2, …, $M_n \in <g>$. M_{c_1} , M_{c_2} , …, and M_{c_t} are the t choices of the chooser Bob, where M_{c_1} , M_{c_2} , …, and $M_{c_t} \in \{ M_1, M_2, \ldots, M_n \}$ and $1 \le c_1, c_2, \ldots, c_t \le n$. M_{c_t} denotes the c_t -th message chosen by Bob. The details of the proposed by Wakaha and Ryota *t*-out-of-*n* OT protocol are presented below.

Step 1: Bob constructs a polynomial $f(x)$, where

$$f(x) = (x - c_1)(x - c_2)\ldots(x - c_t).$$

Then, Bob chooses a, b_0, b_1, …, and b_{t-1} randomly from Z_q, and generates another polynomial $f'(x)$, where

$$f'(x) = f(x) + a(b_0 + b_1 x + \cdots + b_{t-1} x^{t-1}).$$

Let e_0, e_1, …, e_t denote the coefficients of $f'(x)$, that is,

$$e_0 = (-c_1)(-c_2)\ldots(-c_t) + ab_0,$$

$$\vdots$$

$$e_{t-1} = (-c_1 - c_2 - \cdots - c_t) + ab_{t-1,} \text{ and}$$

$$f'(x) = e_0 + e_1 x + \cdots + e_{t-1} x^{t-1} + x^t.$$

Next, Bob computes

$$A = g^a \bmod G,$$

$$B_j = g^{b_j} \bmod G, \text{ where } 0 \le j \le t, \text{ and}$$

$$E_j = g^{e_j} \bmod G, \text{ where } 0 \le j \le t,$$

and then sends the messages $\{A, B_0, B_1, \ldots, B_{t-1}, E_0, E_1, \ldots, E_{t-1}\}$ to Alice.

Step 2: Receiving the messages sent by Bob, Alice computes

$$Y_i = E_0\, E_1^{i}\, E_2^{i^2} \ldots E_{t-1}^{i^{t-1}}\, g^{i^t} \bmod G, \text{ where } i = 1, 2, \ldots, n.$$

For $i = 1, 2, \ldots, n$, Alice chooses r_i and s_i randomly from Z_q and computes

$$H_i = A^{s_i} g^{r_i} \bmod G,$$

$$K_i = Y_i^{s_i}(B_0\ B_1^{i}\ B_2^{i^2} \ldots B_{t-1}^{i^{t-1}})^{r_i} \bmod G, \text{ and}$$

$$F_i = K_i * M_i \bmod G.$$

Next, Alice sends all pairs of (H_i , F_i) to Bob, where $i = 1, 2, \ldots, n$.

Step 3: Upon receiving the messages sent by Alice, for $i \in \{c_1, c_2, \ldots, c_t\}$ Bob computes K_i' as follows:

$$K_i' = H_i^{b_0 + b_1 i + \cdots + b_{t-1} i^{t-1}} \bmod G.$$

Finally, Bob can retrieve those t messages that he really wants to know as follows:

$$M_i' = F_i / K_i' \bmod G, \text{ for } i \in \{c_1, c_2, \ldots, c_t\}.$$

Preliminaries

This section introduces the exact definition of the proposed *t*-out-of-*n* OT protocol and the Generalized Chinese Remainder Theorem.

Definition of the t-out-of-n OT Protocol

The *t*-out-of-*n* OT protocol is a two-party protocol in which the sender has *n* messages, $\{a_1, a_2, \ldots, a_n\}$, and the chooser can securely get t of these messages simultaneously in each protocol run. Nevertheless, the sender cannot find which t messages are chosen by Bob, and the chooser knows only these t messages. In the following, the authors introduce the three essential properties of the general *t*-out-of-*n* OT protocol.

- *Property 1*: *Correctness* – If both the sender and the chooser follow the *t*-out-of-*n* OT protocol, the chooser will get the correct t messages after executing the protocol with the sender.
- *Property 2*: *The privacy of the chooser* – After the *t*-out-of-*n* OT protocol is executed with the chooser, the sender cannot find out which *t* messages are chosen by the chooser.
- *Property 3*: *The privacy of the sender* – After the *t*-out-of-*n* OT protocol is executed with the sender, the chooser cannot learn anything else but these t messages.

Generalized Chinese Remainder Theorem

This subsection presents the Generalized Chinese Remainder Theorem (GCRT) followed by an example.

Definition of the Generalized Chinese Remainder Theorem [21]

Let d_1, d_2, …, and d_n denote *n* positive integers and let form the modulus set, where d_i and d_j are relatively prime in pairs for $i, j = 1, 2, \ldots, n$ and $i \neq j$. a_1, a_2, …, a_n are any *n* positive integers. $D = k * d_1 * d_2 * \ldots * d_n$, where k is a positive integer that satisfies $\text{Max}\{a_1, a_2, \ldots, a_n\} < k < \text{Min}\{d_1, d_2, \ldots, d_n\}$. $D_i = k * d_1 * d_2 * \cdots * d_n / d_i$ for $i = 1, 2, \ldots, n$. $N_i = \lceil a_i * d_i / k \rceil$ for $i = 1, 2, \ldots, n$. Then the following congruences have the same unique solution,

$$\lfloor X / d_1 \rfloor \equiv a_1 (\text{mod}\, k),$$

$$\lfloor X / d_2 \rfloor \equiv a_2 (\text{mod}\, k),$$

$$\vdots$$

$$\lfloor X / d_n \rfloor \equiv a_n (\text{mod}\, k).$$

The reader may ask: how do we compute X from k, d_1, d_2, …, d_n, a_1, a_2, …, and a_n? Since d_1, d_2, …, and d_n are relatively prime in pairs, for $i = 1, 2, \ldots, n$ we have (d_i, D_i)=1. Therefore, there should exist an integer y_i such that $(D_i)\, y_i \equiv k\, (\text{mod}\ k * d_i)$ for $i = 1, 2, \ldots, n$. Besides, $(D_i)\, y_i \equiv 0\, (\text{mod}\, k * d_j)$, where $j \neq i$. This is due to the fact that (D/d_i) is h times of d_i, where $h \in N$. Let $X = (D_1) y_1 N_1 + (D_2) y_2 N_2 + \cdots + (D_n) y_n N_n \bmod D$. Then X is the unique solution of the above congruence system.

An Example of GCRT

Task: Find a positive integer X for the RNS (2, 3, 4) with the moduli set (6, 7, 11) and the general modulus $k = 5$.

Solution: For the numbers D, D_1, D_2, D_3, we obtain

$$D = 5 * 6 * 7 * 11 = 2310,$$

$$D_1 = (D / d_1) = (2310/6) = 385,$$

$$D_2 = (D / d_2) = (2310/7) = 330, \text{ and}$$

$$D_3 = (D/d_3) = (2310/11) = 210.$$

Therefore solving $385\ y_1 \equiv 5\ (\bmod 6*5)$, we get $y_1 = 5$,

$330\ y_2 \equiv 5\ (\bmod 7*5)$, we have $y_2 = 5$, and

$210\ y_3 \equiv 5\ (\bmod 11*5)$, we have $y_3 = 5$.

Besides, N_1, N_2 and N_3 can be derived as follows

$$N_1 = \lceil 2*6/5 \rceil = 3,$$

$$N_2 = \lceil 3*7/5 \rceil = 5, \text{ and}$$

$$N_3 = \lceil 4*11/5 \rceil = 9.$$

Using the equation $X = (D_1)y_1N_1 + (D_2)y_2N_2 + \cdots + (D_n)y_nN_n \bmod D$, we obtain

$$X = 385*5*3 + 330*5*5 + 210*5*9 = 375 \bmod 2310.$$

Therefore, $X = 375$ is the solution of the example.

Verification:

$$\lfloor 375/6 \rfloor \bmod 5 = 62 \bmod 5 = 2,$$

$$\lfloor 375/7 \rfloor \bmod 5 = 53 \bmod 5 = 3,$$

$$\lfloor 375/11 \rfloor \bmod 5 = 34 \bmod 5 = 4.$$

The Proposed Protocol

This section presents the proposed *t*-out-of-*n* OT protocol based on the Generalized Chinese Remainder Theorem. The flowchart of the proposed OT protocol is shown in Figure 1. First, the authors summarize the notations used in their *t*-out-of-*n* OT protocol as follows.

- Alice is the sender;
- Bob is the chooser;
- e is the public key of the sender Alice;
- d is the private key of the sender Alice;
- G is a large prime number;

- a_1, a_2, …, a_n are the n messages held by Alice, where $a_i \in N$ and $i = 1, 2, \ldots, n$;
- d_1, d_2, …, d_n are n positive integers that are relatively prime in pairs, where $d_i > a_i$ for $i = 1, 2, \ldots, n$;
- k that satisfies $\text{Max}\{a_1, a_2, \ldots, a_n\} < k < \text{Min}\{d_1, d_2, \ldots, d_n\}$ is a positive integer;
- ID_i is the identity of the message a_i, where $i = 1, 2, \ldots, n$;
- T_1, T_2, …, T_n are the average values for the chooser enabling him/her to retrieve the demanded messages, where $T_i = d_i^e \bmod G$ for $i = 1, 2, \ldots, n$;
- D is the value of $k * d_1 * d_2 * \cdots * d_n$;
- D_i equals D / d_i for $i = 1,2,\ldots,n$;
- N_i equals $\lceil a_i * d_i / k \rceil$ for $i = 1,2,\ldots,n$;
- b_1, b_2, …, b_t are the t messages that Bob wants to know, where $b_j \in \{a_1, a_2, \ldots, a_n\}$ with the corresponding item (ID_j, T_j) for $j = 1, 2, \ldots, t$.

In what follows, the authors provide the details of the proposed *t*-out-of-*n* OT protocol based on GCRT.

Step 1: Receiving the request sent by Bob, for all messages a_1, a_2, …, a_n, Alice selects n positive integers, d_1, d_2, …, d_n, that are relatively prime in pairs for this protocol run, where $d_1 > a_1$, $d_2 > a_2$, …, and $d_n > a_n$. Then Alice generates a positive integer k that satisfies $k > \text{Max}\{a_1, a_2, \ldots, a_n\}$ and $k < \text{Min}\{d_1, d_2, \ldots, d_n\}$ and computes

$$D = k * d_1 * d_2 * \cdots * d_n,$$

$$D_i = D / d_i, \text{ for } i = 1, 2, \ldots, n,$$

$$N_i = \lceil a_i * d_i / k \rceil, \text{ for } i = 1, 2, \ldots, n;$$

then she constructs the following congruence system:

$$\lfloor X / d_1 \rfloor \equiv a_1 (\text{mod } k),$$

$$\lfloor X / d_2 \rfloor \equiv a_2 (\text{mod } k),$$

$$\vdots$$

$$\lfloor X / d_n \rfloor \equiv a_n (\mathrm{mod}\, k).$$

Next, Alice computes X as follows:

$$X = (D_1) y_1 N_1 + (D_2) y_2 N_2 + \cdots + (D_n) y_n N_n \bmod D \text{ by GCRT,}$$

where $(D_i) y_i \equiv k (\mathrm{mod}\, d_i * k)$, for $i = 1, 2, \ldots, n$.

Afterwards, Alice computes

$$T_1 = d_1^e \bmod G,$$

$$T_2 = d_2^e \bmod G,$$

$$\vdots$$

$$T_n = d_n^e \bmod G,$$

by using the public key e. Next, Alice transmits X, k and all pairs of (ID_i, T_i) to Bob for $i = 1, 2, \ldots, n$.[22,23]

Step 2: Receiving the messages sent by Alice, Bob selects t pairs (ID'_j, T'_j), for $j = 1, 2, \ldots, t$, and generates t corresponding random numbers r_1, r_2, …, r_t, for each pair (ID'_j, T'_j). Next, Bob computes

$$\alpha_1 = r_1^e * T_1' \bmod G,$$

$$\alpha_2 = r_2^e * T_2' \bmod G,$$

$$\vdots$$

$$\alpha_t = r_t^e * T_t' \bmod G,$$

by using Alice's public key e. Then, Bob sends the computational result {α_1, α_2, …, α_t} to Alice.

Step 3: Upon receiving the messages sent by Bob, Alice computes

$$\rho_1 = \alpha_1^d \bmod G,$$

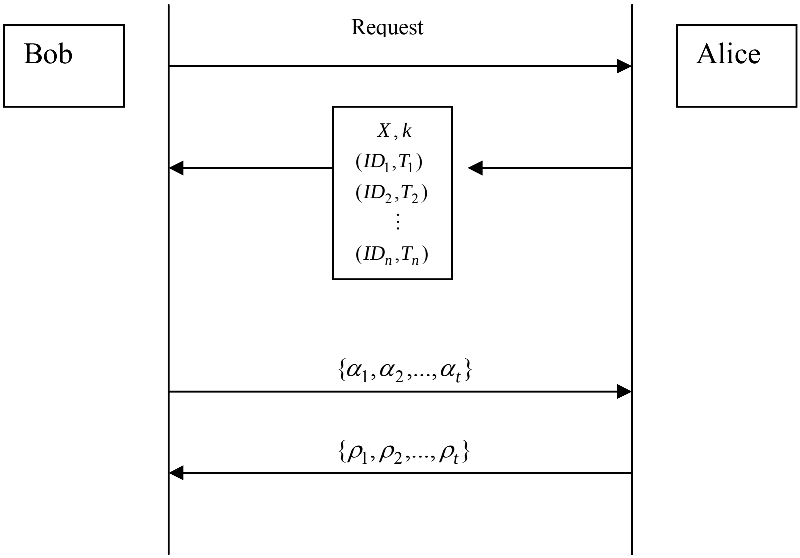

Figure 1: Flowchart of the Proposed *t*-out-of-*n* OT Protocol.

$$\rho_2 = \alpha_2^d \bmod G,$$

$$\vdots$$

$$\rho_t = \alpha_t^d \bmod G,$$

using her private key d, and then she sends the computational results $\{\rho_1, \rho_2, \ldots, \rho_t\}$ to Bob.

Step 4: Receiving the messages sent by Alice, Bob computes

$$d_1' = r_1^{-1} * \rho_1 \bmod G,$$

$$d_2' = r_2^{-1} * \rho_2 \bmod G,$$

$$\vdots$$

$$d_t' = r_t^{-1} * \rho_t \bmod G,$$

Finally, Bob can successfully use X and k to compute the required t messages as follows,

$$b_1 = \lfloor X / d_1' \rfloor \bmod k,$$

$$b_2 = \lfloor X / d_2' \rfloor \bmod k,$$

$$\vdots$$

$$b_t = \lfloor X / d_t' \rfloor \bmod k.$$

Discussion and Analysis

This section demonstrates that the proposed protocol satisfies the essential requirements of the general *t*-out-of-*n* OT protocols mentioned in a previous section and presents some comparisons between the protocol and other related work.

Analysis of the Essential Requirements

This subsection demonstrates that the OT protocol presented in this article meets the three essential requirements of the general OT protocols.

Requirement 1: Correctness

At the beginning, it is assumed that both the sender Alice and the chooser Bob are honest. After they both, Alice and Bob, execute the *t*-out-of-*n* OT protocol, Bob will get *t* messages $\{ b_1 ,\ b_2 ,\ \ldots,\ b_t \}$. For $j = 1, 2, \ldots, t$, b_j will be equivalent to one of the n messages $\{ a_1 ,\ a_2 ,\ \ldots,\ a_n \}$ possessed by Alice. It is due to the fact that the T_j s are computed as follows:

$$T_1 = d_1^e \bmod G,$$

$$T_2 = d_2^e \bmod G,$$

$$\vdots$$

$$T_n = d_n^e \bmod G,$$

and chosen by Bob from these n messages sent by Alice. Furthermore, X is generated by the following congruence system:

$$\lfloor X / d_1 \rfloor \equiv a_1 (\bmod k),$$

$$\lfloor X / d_2 \rfloor \equiv a_2 (\bmod k),$$

$$\vdots$$

$$\lfloor X / d_n \rfloor \equiv a_n (\bmod k).$$

That is,

$$X = (D_1) y_1 N_1 + (D_2) y_2 N_2 + \cdots + (D_n) y_n N_n \bmod D \text{ by GCRT,}$$

where $(D_i) y_i \equiv k (\bmod d_i * k)$, $N_i = \lceil a_i * d_i / k \rceil$, for $i = 1, 2, \ldots, n$.

As a result, for each selected item (ID'_j, T'_j), where $j = 1, 2, \ldots, t$, Bob can reveal one corresponding message that he really wants to know by the following derivation,

$$\alpha_j = r_j^e * T'_j \bmod G,$$

$$\rho_j = \alpha_j^d \bmod G,$$

$$d'_j = r_j^{-1} * \rho_j \bmod G, \text{ and}$$

$$b_j = \lfloor X / d'_j \rfloor \bmod k.$$

Consequently, the proposed protocol can satisfy this requirement.

Requirement 2: Privacy of the Chooser

First, it is assumed that these t pairs (ID'_j, T'_j) are the messages that Bob chooses from the n messages sent by Alice, where $j = 1, 2, \ldots, t$. Bob generates a random number r_j for each pair (ID'_j, T'_j), where $j = 1, 2, \ldots, t$. Even if Alice computes $\rho_j = \alpha_j^d \bmod G$ instead of Bob to reveal ρ_j by using her private key d, Alice cannot find d'_j yet. The reason is that d'_j is computed as:

$$d'_j = r_j^{-1} * \rho_j \bmod G.$$

That is, d'_j is protected by r_j^{-1}. However, only Bob knows r_j. Therefore, without knowing r_j Alice cannot reveal which t messages are chosen by Bob. Certainly, Alice may select a set of $\{b'_1, b'_2, \ldots, b'_t\}$ to try guessing which events have happened to Bob. Considering that for each event that Alice guesses the correct choice of Bob is independent, the probability that Alice guesses the correct choices is estimated as follows:

$$\Pr(b_j = b'_j \mid j = 1, 2, \ldots, t) = 1/n^t,$$

where t is the number of the messages that Bob wants to know and n is the total number of the messages kept in Alice's database. Generally speaking, the number of the messages stored in the sender's database is not less than ten thousand. While t is not less than five, the probability that Alice guesses the correct messages chosen by Bob is estimated as follows:

$$\Pr(b_j = b'_j \mid j = 1,2,\ldots,t) \le 1/10^{20}.$$

In other words, the probability that Alice can reveal which t messages are chosen by Bob is quite small. And, therefore, the proposed t-out-of-n OT protocol can conditionally ensure the privacy of Bob's choices. Thus, this requirement is also met by the t-out-of-n OT protocol proposed in this article.

Requirement 3: Privacy of the Sender

First, it is assumed that the sender Alice can be trusted. After the proposed protocol is performed by both Alice and Bob, Bob can get nothing else than the chosen t messages. It is due to the fact that Alice only computes

$$\rho_j = \alpha_j^d \bmod G,$$

for $j = 1, 2, \ldots, t$, by using her private key d. Without knowing Alice's private key d, Bob cannot decrypt the needed ρ_j to retrieve d'_j by computing

$$d'_j = r_j^{-1} * \rho_j \bmod G.$$

As a result, Bob cannot know b_j for $b_j \notin \{b_1, b_2, \ldots, b_t\}$. Consequently, Bob can know nothing else than these t messages that he really wants to know and the presented protocol can meet this requirement.

Comparison between the Proposed t-out-of-n OT and Other Related Work

Protocol

This subsection presents some comparisons between the protocol presented in this article and other related OT protocols described above. The authors begin with description of the notations used in Table 1. As usual, Alice is the sender, while Bob denotes the chooser. n denotes the number of the messages kept in Alice's database. t denotes the number of the messages that Bob wants to know. *Exp* denotes exponential computation operation.

Table 1: Comparison between the Proposed Protocol and Other Related Work.

Protocols \ Members	Alice	Bob
Naor and Pinkas's Protocol	$4(t*n)\ Exp$	$4t\ Exp$
Wakaha and Ryota's Protocol	$4n\ Exp$	$(3t+1)\ Exp$
The Proposed Protocol	$(n+t)\ Exp$	$t\ Exp$

Usually, the computation complexity of an OT protocol depends mainly on the number of the exponential computation operations. Therefore, only the number of the exponentiation computation operations of the proposed OT protocol and the other related protocols is considered in Table 1. Furthermore, repeating a 1-out-of-*n* OT protocol t times still can achieve the functionality of executing a *t*-out-of-*n* OT protocol only once. The computational load of Naor and Pinkas's 1-out-of-*n* OT protocol presented in Table 1 is obtained repeating the 1-out-of-*n* OT protocol t times.

Considering the sender's side, since t is very much less than n, the computational load needed in the proposed protocol is about $4*t$ times lighter than that of Naor and Pinkas's protocol and it is nearly a quarter of the load needed in Wakaha and Ryota's protocol. On the other hand, considering the chooser's side, the computational load required in Naor and Pinkas's and Wakaha and Ryota's protocol are four and three times heavier than that of the protocol presented in this article, respectively. The figures shown in Table 1 clearly demonstrate that the performance of the proposed *t*-out-of-*n* OT protocol is better than that of the related protocols both from sender's and chooser's perspective.

Conclusions

With the rapid development of communication and information technologies, Oblivious Transfer (OT) is widely applied in numerous applications. And, therefore, OT has become an important cryptography tool. The mechanism of the *t*-out-of-*n* OT protocol is a novel and significant version of the OT protocol. In 2004, Wakaha and Ryota proposed a secure *t*-out-of-*n* OT protocol that allows the chooser to get *t* messages from the sender simultaneously in each protocol run. Unfortunately, getting better understanding of Wakaha and Ryota's *t*-out-of-*n* OT protocol, it becomes clear that it still lacks efficiency.

In this article, a secure and more efficient t-out-of-n OT protocol based on the Generalized Chinese Remainder Theorem (GCRT) is proposed. As analyzed in the article, the proposed OT protocol not only satisfies the three essential properties of the general OT protocols, but also has better performance than that of other related protocols. Therefore, the proposed t-out-of-n OT protocol is secure and efficient enough to be applied in real-world applications.

Notes:

1 Michael O. Rabin, "How to Exchange Secrets by Oblivious Transfer," Technical Report TR-81 (Harvard University: Aiken Computation Laboratory, 1981).

2 Narn-Yih Lee and Tzonelih Hwang, "On the Security of Fair Blind Signature Scheme Using Oblivious Transfer," *Computer Communications* 22, no. 3 (1999): 287-290.

3 Wen-Guey Tzeng, "Efficient 1-Out-of-n Oblivious Transfer Schemes with Universally Usable Parameters," *IEEE Transactions on Computers* 53, no. 2 (February 2004): 232-240.

4 Mihir Bellare and Silvio Micali, "Non-Interactive Oblivious Transfer and Applications," in *Proceedings of Advances in Cryptology - CRYPTO'89*, volume 435 of Lecture Notes in Computer Science (Springer-Verlag, 1990), 547-557.

5 Moni Naor and Benny Pinkas, "Efficient Oblivious Transfer Protocols," in *Proceedings of the 12th Annual Symposium on Discrete Algorithms* (Washington, DC, USA, 7-9 January, 2001), 448-457.

6 Bill Aiello, Yuval Ishai, and Omer Reingold, "Priced Oblivious Transfer: How to Sell Digital Goods," in *Proceedings of the International Conference on the Theory and Application of Cryptographic Techniques: Advances in Cryptology* (Aarhus, Denmark, 21-23 May 2001), volume 2045 of Lecture Notes in Computer Science, 119-135.

7 Christian Cachin, "On the Foundations of Oblivious Transfer," in *Advances in Cryptology: EUROCRYPT'98* (Espoo, Finland, May/June 1998), volume 1403 of Lecture Notes in Computer Science, ed. Kaisa Nyberg (Springer-Verlag, 1998), 361-374.

[8] Giovanni Di Crescenzo, Tal Malkin, and Rafail Ostrovsky, "Single Database Private Information Retrieval Implies Oblivious Transfer," in *Advances in Cryptology: EUROCRYPT'00: International Conference on the Theory and Application of Cryptographic Techniques* (Bruges, Belgium, 14-18 May 2000), volume 1807 of Lecture Notes in Computer Science, ed. Bart Preneel (Springer 2000), 122-138.

[9] Yan Zong Ding, "Oblivious Transfer in the Bounded Storage Model," in *Proceedings of Advances in Crypto'01* (Santa Barbara, California, USA, August 2001), volume 2139 of Lecture Notes in Computer Science, 155-170.

[10] Juan A. Garay and Philip D. MacKenzie, "Concurrent Oblivious Transfer," in *Proceedings of the 41st Annual IEEE Symposium on Foundations of Computer Science FOCS 2000* (Redondo Beach, California, USA, 12-14 November) (IEEE Computer Society Press, 2000), 314-324.

[11] Yevgeniy Dodis and Silvio Micali, "Lower Bounds for Oblivious Transfer Reductions," in *Advances in Cryptology: Proceedings of Eurocrypt'99: International Conference on the Theory and Application of Cryptographic Techniques* (Prague, Czech Republic, 2-6 May 1999), volume 1592 of Lecture Notes in Computer Science, ed. Jacques Stern (Springer Verlag, 1999), 42-55.

[12] Moni Naor and Benny Pinkas, "Distributed Oblivious Transfer," in *Advances in Cryptology: ASIACRYPT 2000, 6th International Conference on the Theory and Application of Cryptology and Information Security* (Kyoto, Japan, 3-7 December 2000), volume 1976 of Lecture Notes in Computer Science, ed. Tatsuaki Okamoto (Springer 2000), 205-219.

[13] Moni Naor and Benny Pinkas, "Oblivious Transfer and Polynomial Evaluation," in *Proceedings of the 31st Annual ACM Symposium on Theory of Computing* (Atlanta, Georgia, USA, 1-4 May 1999) (ACM, 1999), 245-254.

[14] Shimon Even, Oded Goldreich, and Abraham Lempel, "A Randomized Protocol for Signing Contracts," *Communications of the ACM* 28, no. 6 (June 1985): 637-647.

[15] Wakaha Ogata and Ryota Sasahara, "k-out-of-n Oblivious Transfer without Random Oracles," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences* 87-A, no. 1 (January 2004): 147-151.

[16] Naor and Pinkas, "Efficient Oblivious Transfer Protocols."

[17] Yeu-Pong Lai and Chin-Chen Chang, "Parallel Computational Algorithms for Generalized Chinese Remainder Theorem," *Computers and Electrical Engineering* 29, no. 8 (November 2003): 801-811.

[18] Moni Naor and Benny Pinkas, "Oblivious Transfer with Adaptive Queries," in *Advances in Cryptology – CRYPTO'99: 19th Annual International Cryptology Conference* (Santa Barbara, California, USA, 15-19 August 1999), volume 1666 of Lecture Notes in Computer Science, ed. Michael J. Wiener (Springer-Verlag, 1999), 573-590.

[19] Naor and Pinkas, "Oblivious Transfer and Polynomial Evaluation."

[20] Even, Goldreich, and Lempel, "A Randomized Protocol for Signing Contracts."

[21] Lai and Chang, "Parallel Computational Algorithms for Generalized Chinese Remainder Theorem."

[22] George I. Davida, David L. Wells, and John B. Kam, "A Database Encryption System with Subkeys," *ACM Transactions on Database Systems* 6, no. 2 (June 1981): 312-328.

[23] Taher ElGamal, "A Public-Key Cryptosystem and a Signature Scheme based on Discrete Logarithms," *IEEE Transactions on Information Theory* IT-31, no. 4 (1985) 469-472.

JUNG-SAN LEE received a BS degree in Computer Science and Information Engineering from the National Chung Cheng University, Chiayi, Taiwan, in 2002. He is currently pursuing his Ph.D. degree in Computer Science and Information Engineering from the National Chung Cheng University, Chiayi, Taiwan. His current research interests include electronic commerce, information security, cryptography, and mobile communications. *Address for correspondence*: Department of Computer Science and Information Engineering, National Chung Cheng University, Chiayi, Taiwan, 621, R.O.C.; *Fax*: 886-5-2720859; *E-mail*: ljs@cs.ccu.edu.tw.

CHIN-CHEN CHANG received a BS degree in Applied Mathematics in 1977 and a MS degree in Computer and Decision Sciences in 1979, both from the National Tsing Hua University, Hsinchu, Taiwan. He received his Ph.D. in Computer Engineering from the National Chiao Tung University, Hsinchu, Taiwan, in 1982. Since February 2005, he has worked as a chair professor at the Department of Information Engineering and Computer Science at Feng Chia University, Taichung, Taiwan. His current research interests include database design, computer cryptography, image compression and data structures. Dr. Chang is a fellow of the IEEE, a fellow of the IEE, a research fellow of the National Science Council of R.O.C., and a member of the Chinese Language Computer Society, the Chinese Institute of Engineers of the Republic of China, the International Association for Crypto-logic Research, the Computer Society of the Republic of China, and the Phi Tau Phi Honorary Society of the Republic of China. Dr. Chang was the chair and is the honorary chair of the executive committee of the Chinese Cryptography and Information Security Association. *Address for correspondence*: Department of Information Engineering and Computer Science, Feng Chia University, Taichung, Taiwan, 40724, R.O.C.; *E-mail*: ccc@cs.ccu.edu.tw.