Journal of Information Hiding and Multimedia Signal Processing ©2014 ISSN 2073-4212
Ubiquitous International Volume **5**, Number **1**, January **2014**

A Provably Secure t-out-of-n Oblivious Transfer Mechanism based on Blind Signature

Chin-Chen Chang

Department of Information Engineering and Computer Science
Feng Chia University
No. 100, Wen-Hwa Rd., Taichung, 40724, Taiwan
Department of Computer Science and Information Engineering
Asia University
No. 500, Lioufeng Rd., Wufeng, Taichung, 41354, Taiwan
alan3c@gmail.com

Ting-Fang Cheng

Department of Computer Science and Information Engineering
Asia University
No. 500, Lioufeng Rd., Wufeng, Taichung, 41354, Taiwan
nthu.tiffany@gmail.com

Received April, 2013; revised May, 2013

Abstract. *Due to the rapid development of the Internet, an increasing number of applications can be implemented using oblivious transfer (OT) as a sub-protocol, such as privacy-preserving auction, secrets exchange, data mining, and e-commerce. Considering the practicability of an OT mechanism, we think that it is also necessary to discuss how to convince a chooser of the integrity and origin of chosen secrets, except for accuracy, privacy of the sender, and privacy of the chooser. In this paper, we redefine the requirements of a well-designed OT scheme and propose a novel t-out-of-n OT mechanism* (OT_t^n) *based on blind signature. The accuracy of our* OT_t^n *mechanism is demonstrated according to the BAN logic. Furthermore, we adopt the problem reduction to prove the security of our* OT_t^n *mechanism. The analyses demonstrate that our proposed mechanism can fulfill all requirements that we redefined and be suitable for further applications.*
Keywords: Oblivious transfer, Verifiability, Non-repudiation, Blind signature, BAN logic, Factorization

1. **Introduction.** Oblivious transfer (OT), first proposed by Rabin in 1981 [22], is a cryptographic primitive used to protect the security of two-party or multiparty computations [16]. In the concept of Rabin's OT, a sender, Alice, has one secret bit x and sends it to a chooser, Bob, who has a 1/2 probability of receiving the correct bit. In other words, Alice does not know whether Bob obtains x or not. On the basis of Rabin's OT, Even proposed an extended scheme, called 1-out-of-2 OT (OT_1^2), in 1985 [13]. For OT_1^2, Alice has two secret bits, x_1 and x_2, and Bob can choose only one of them. Similarly, Alice does not know which secret Bob chooses. Two additional flavors of OT were subsequently presented: 1-out-of-n OT (OT_1^n) and t-out-of-n OT (OT_t^n). OT_1^n, an extension of OT_1^2, was first introduced by Brassard et al. in 1986 [5], in which Alice has n secrets and Bob can choose only one of them without disclosing his choice. According to the concept of OT_1^n, some researchers think that they can perform an OT_1^n protocol t times such that

Bob can choose t secrets from Alice at the same time [3, 21, 24, 29]. However, such a solution is very inefficient due to the need for parallel computing and high computational costs. Therefore, in 2003, Mu et al. proposed a formal t-out-of-n OT (OT_t^n) based on discrete logarithm without parallel computing [20], in which Bob can choose and receive only t secrets out of n secrets sent by Alice.

In this paper, we focus on the t-out-of-n oblivious transfer, OT_t^n. Recently, various OT_t^n schemes have been proposed [2, 10, 14, 19. 26. 27] and most have focused on the requirements of accuracy, privacy of the sender, and privacy of the chooser. However, with the explosive growth of network technologies, an increasing number of applications can be implemented using OT as a sub-protocol, such as privacy-preserving system, secrets exchange, data mining, and e-commerce [17, 28]. For example, in an e-book database system, an e-book provider (Alice) has n e-books and a customer (Bob) can choose and purchase only t e-books from Alice without disclosing his choice. In order to make an OT scheme more suitable and practical for further applications, we think that it is necessary to discuss how to convince a chooser of the integrity and origin of chosen secrets. That is, Bob must have ability to verify the reconstructed messages (e-books) are not modified and really sent by Alice, and Alice cannot deny or repudiate the origin of the messages (e-books) that she provides when a dispute occurs. Hence, in this paper, we expand and redefine the requirements of a well-designed OT scheme as accuracy, privacy of the sender, privacy of the chooser, verifiability, and non-repudiation, in which the last two requirements are not provided by others. Furthermore, we propose a new OT_t^n mechanism based on blind signature [9, 11, 23], which can achieve all these essentials.

The remainder of this paper is organized as follows. We redefine the essentials of a well-designed OT and briefly introduce blind signature in Section 2. In Section 3, we present a new t-out-of-n OT mechanism, followed by the demonstration of the accuracy of our proposed mechanism using BAN logic in Section 4. In Section 5, we employ the problem reduction to prove the security of our t-out-of-n OT mechanism and compare its functionality with recent works. Finally, we make conclusions in Section 6.

2. Preliminaries.

In this section, we briefly define the oblivious transfer and its properties [2, 10, 24, 27, 29], and introduce the technology of blind signature [9, 11, 23] applied in our proposed scheme in Subsections 2.1 and 2.2, respectively.

2.1. Definition of Oblivious Transfer.

Oblivious transfer (OT) is a cryptographic primitive in which any two communication parties play the roles of a sender and a chooser. In the t-out-of-n oblivious transfer (OT_t^n), the sender has n messages for the chooser and allows the chooser to optionally obtain t messages among n messages. Based on most OT schemes [2, 10, 24, 27, 29], we identified specific requirements that our novel OT_t^n method should achieve.

Accuracy: The chooser can correctly obtain the applied t messages after executing the protocol with the sender if and only if both the sender and the chooser follow the OT protocol [2, 24, 27, 29].

Privacy of the sender: After performing the protocol with the sender, the chooser can only retrieve t messages. In addition, no one can get any information to reconstruct the messages possessed by the sender except the specific chooser [10, 17].

Privacy of the chooser: After a transfer, the sender cannot find out anything related to the chooser's choices. More specifically, any different choices $\{c_1, c_2, \ldots, c_t\}$ and $\{c'_1, c'_2, \ldots, c'_t\} \subset \{m_1, m_2, \ldots, m_n\}$ are computationally indistinguishable to the sender [10, 27], where m_i's are the messages of the sender.

Verifiability: The chooser must be convinced that the reconstructed messages are not modified and really sent by the sender. In other words, the chooser must have the ability to verify the data integrity [18] and origin of all t messages that she/he chooses [29].
Non-repudiation: For the further applications, the sender is unable to deny or repudiate the messages which she/he sends to the chooser. In other words, the sender cannot deny or repudiate the origin of the messages that she/he provides.

Based on these requirements, the OT_t^n can be more suitable for real application scenarios. For example, in an e-book database system, an e-book provider (Alice) has n e-books and a customer (Bob) can choose and purchase only t e-books from Alice without disclosing his choice. Furthermore, Bob has ability to verify the reconstructed e-books are not modified and really sent by Alice, and Alice cannot deny or repudiate the origin of the e-books that she provides when a dispute occurs.

2.2. **Blind Signature.** In order to accomplish the chooser privacy, we apply the concept of blind signature [9, 11, 23] to design our OT mechanism. In other words, the chooser's choices must be blindly processed by the sender before the chooser can extract the original messages. Here, we briefly introduce the blind signature with an example.

Assume that Bob needs Alice's help to sign a message M, but does not want to let her know the content of this message. Based on RSA [23], there is a large composite number N of two large primes, p and q (i.e., $N = pq$), and the public and private key pair of Alice is (e_{Alice}, d_{Alice}). Bob first randomly chooses a seed number v to blind his message M as $M' = M \cdot v^{e_{Alice}} \mathrm{mod} N$ to Alice. After receiving the signing request from Bob, Alice signs M' as $sig' = (M')^{d_{Alice}} \mathrm{mod} N$ and returns it to Bob. Bob can subsequently un-blind it to retrieve the signature of M as $sig = sig' \cdot v^{-1} = (M \cdot v^{e_{Alice}})^{d_{Alice}} \cdot v^{-1} = M^{d_{Alice}} \mathrm{mod} N$. Obviously, Bob can obtain a valid signature of M without revealing it.

3. **Proposed t-out-of-n OT Mechanism.** In this section, we present a new t-out-of-n OT mechanism based on blind signature, which consists of two entities: senders (S) and choosers (C). Note that, in order to avoid the problem of selective failure [8], we assume that the sender in our proposed scheme is a trusted signer, that is, the sender cannot maliciously sign a fake signature to a chooser. Initially, the sender sets her/his public and private key pair (e_S, d_S) such that $GCD(e_S, \phi(N)) = 1$ and $e_S d_S \equiv 1(\mathrm{mod}\phi(N))$, where N is the product of two large primes, p and q (i.e., $N = pq$), and $GCD(\cdot)$ is the function used to compute the greatest common divisor of input numbers. Suppose that the sender S has n messages m_1, m_2, $\ldots$, and m_n. The details of our t-out-of-n OT mechanism are described in the following two phases: commitment phase and transfer phase, with the whole process depicted in FIGURE 1.

Commitment Phase

Step1: If a chooser C wants to access messages possessed by the sender S, she/he needs to send a request message to S.

Step2: Upon receiving the request, S randomly selects n positive integers: r_1, r_2, $\ldots$, and r_n. Then, S computes

$$k_i = r_i^{d_S} \bmod N, \tag{1}$$

$$Sig_i = m_i^{d_S} \bmod N, \text{and} \tag{2}$$

$$m'_i = E_{k_i}(m_i || Si_{g_i}) \tag{3}$$

for $i = 1, 2, \ldots, n$, where Si_{g_i} is the signature of m_i signed by S and $E_{k_i}(\cdot)$ is a symmetric encryption function using key k_i.

Step3: Finally, S sends the pairs of (m'_i, r_i) to C for $i = 1, 2, \ldots, n$.

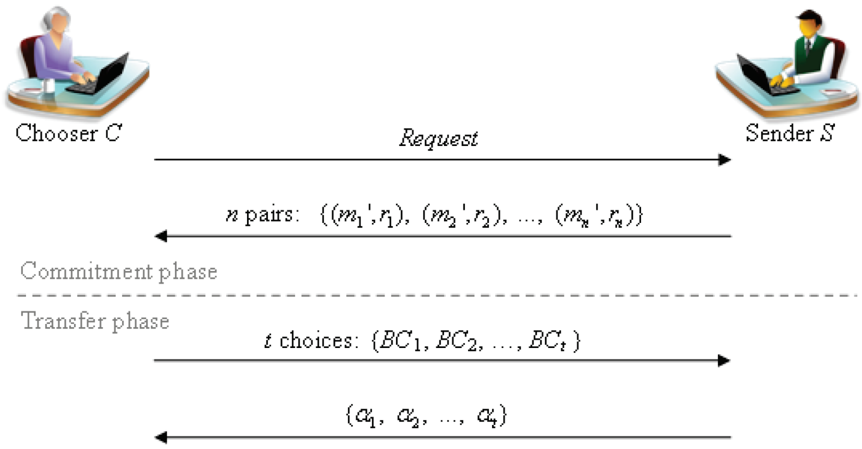

FIGURE 1. The flowchart of our OT_t^n mechanism

Transfer Phase

Step1: When C wants to learn arbitrary t messages among n messages, she/he must select t pairs of (m'_j, r_j), for $j = 1, 2, \ldots, t$, from the messages sent by S. Then, C randomly chooses t positive integers u_1, u_2, …, and u_t, and uses them to blind her/his choices to r_j's as in Equation (4).

$$BC_j = u_j^{es} r_j \bmod N \tag{4}$$

Finally, C sends her/his blind choices BC_1, BC_2, , and BC_t to S.

Step2: After receiving the messages for all $j \in \{1, 2, \ldots, t\}$, S computes

$$\alpha_j = BC_j^{ds} \bmod N \tag{5}$$

and sends them to C.

Step3: Upon receiving the responses from S, C uses the positive integers u_j's to unblind the corresponding α_j's using Equation (6) for $j = 1, 2, \ldots, t$.

$$k'_j = \alpha_j \cdot u_j^{-1} \bmod N \tag{6}$$

Afterward, C employs them to decrypt the original messages and signatures using Equation (7).

$$(m_j || Sig_j) = D_{k'_j}(m'_j) \tag{7}$$

Step4: Finally, C can use S's public key e_S to verify the data integrity and origin of all t messages using the following equation.

$$m_i = Sig_i^{es} \bmod N \tag{8}$$

If the verification fails, C terminates this procedure.

4. **Accuracy of Our t-out-of-n OT Mechanism.** Here, we demonstrate the accuracy of our OT_t^n mechanism using BAN logic [6, 7]. TABLE 1 shows the formulated constructs of the BAN logic.

The logical postulates of the BAN logic that we would apply for our proof are shown as follows.

Message-decryption: $\frac{P|\equiv P \overset{Y}{\rightleftharpoons} Q, P \triangleleft \langle X \rangle_Y}{P \triangleleft X}$, $\frac{P|\equiv \overset{K}{\mapsto} P, P \triangleleft \{X\}_K}{P \triangleleft X}$, and $\frac{P|\equiv Q \overset{K}{\leftrightarrow} P, P \triangleleft \{X\}_K}{P \triangleleft X}$;

Message-meaning: $\frac{P|\equiv \overset{K}{\mapsto} Q, P \triangleleft \{X\}_{K-1}}{P|\equiv Q|\sim X}$;

TABLE 1. The constructs of the BAN logic

$\langle X\rangle_Y$: X combined with the formula Y; it is implied that Y be a secret
$\{X\}_K$: the formula X encrypted under the key K
$P \triangleleft X$: P *receives* X
$P \mid\equiv X$: P *believes* X
$P \mid\sim X$: P once *said* X
$\overset{K}{\mapsto} P$: P has K as a *public key*
$P \overset{K}{\longleftrightarrow} Q$: P and Q may use the *shared key* K to communicate with each other
$P \overset{X}{\rightleftharpoons} Q$: the formula X is a *secret* known only to P and Q
$\#(X)$: the formula X is *fresh*
$P \mid\Rightarrow X$: P has *jurisdiction* over X

P and Q range over principals;
X and Y are statements; and
K refers to the cryptographic key.

Nonce-verification: $\frac{P\mid\equiv\#(X),P\mid\equiv Q\mid\sim X}{P\mid\equiv Q\mid\equiv X}$;
Freshness-propagation: $\frac{P\mid\equiv\#(X)}{P\mid\equiv\#(X,Y)}$;
Session Key: $\frac{P\mid\equiv\#(K),P\mid\equiv Q\mid\equiv X}{P\mid\equiv P\overset{K}{\leftrightarrow}Q}$
Sight-projection: $\frac{P\triangleleft(X,Y)}{P\triangleleft X}$; and
Jurisdiction: $\frac{P\mid\equiv Q\mid\Rightarrow X,P\mid\equiv Q\mid\equiv X}{P\mid\equiv X}$;
Note that the postulate of the $SessionKey$ rule is presented by Yang and Li for the combination key [25], where X is a basic element of the combination key K.

Recalling once again, in our OT mechanism, all messages possessed by the sender are encrypted with the corresponding signatures. If the chooser wants to learn arbitrary t messages among n messages, she/he must first send her/his blind choices to the sender. Then, the sender further computes t responding messages according to the chooser's choices. Upon receiving t responding messages, the chooser can derive the corresponding decryption keys of t messages which she/he selects using the un-blinding procedure. Afterward, the chooser can use these keys to obtain the messages that she/he wants and verify their integrity and origin through the corresponding signatures. The following shows the expansion of communication procedures of our proposed OT mechanism.
M_0: $C \to S : request$
M_1: $S \to C : E_{k_i}(m_i||(m_i^{ds} \bmod N)), r_i; i \in \{1, 2, \ldots, n\}$
M_2: $C \to S : u_j^{es} r_j \bmod N; j \in \{1, 2, \ldots, t\}$
M_3: $S \to C : u_j \cdot r_j^{ds} \bmod N; j \in \{1, 2, \ldots, t\}$
Before beginning the proof, we translate these procedures into the idealized form as follows.
I_1: $S \to C : \{m_i, \{m_i\}_{e_S^{-1}}\}_{k_i}; i \in \{1, 2, \ldots, n\}$
I_2: $C \to S : r_j\{u_j\}_{eS}; j \in \{1, 2, \ldots, t\}$
I_3: $S \to C : \left\langle \{r_j\}_{e_S^{-1}} \right\rangle_{u_j}; j \in \{1, 2, \ldots, t\}$
We can subsequently proceed with the proof of our proposed OT mechanism.

Theorem 4.1. *The chooser can correctly obtain the applied t messages after executing the protocol with the sender if and only if both the sender and the chooser follow the OT protocol.*

Proof: In our OT mechanism, all messages possessed by the sender are encrypted with corresponding signatures. The chooser must ask the sender to obtain t decryption keys if she/he wants to learn t messages among n messages. To demonstrate that the chooser can correctly retrieve the demanded t messages, we have to prove that our OT mechanism should achieve the following goals. Note that j implies the chooser's choices 1 to t.

G_1:$C| \equiv C \overset{k_j}{\leftrightarrow} S$ G$_2$:$C| \equiv S| \sim m_j$

G_3:$C| \equiv m_j$

We can now carry out the proof using the following assumptions.

A$_1$:$C| \equiv C \overset{u_j}{\rightleftharpoons} C$ A$_2$:$C| \equiv \overset{e_S}{\mapsto} S$

A$_3$:$C| \equiv \#(r_j)$ A$_4$:$C| \equiv S| \Rightarrow m_j$

For the choice j, the reason is drawn by following a series of formulas:

F$_1$: C *receives* $\{r_j\}_{e_S^{-1}}$ using A$_1$ and I$_3$. (*Message-decryption* rule)

F$_2$: C *believes* that S *said* r_j using A$_2$ and F$_1$. (*Message-meaning* rule)

F$_3$: C *believes* that S *believes* r_j using A$_3$ and F$_2$. (*Nonce-verification* rule)

Due to the encryption/decryption key $k_j = r_j^{ds} \bmod N$ (i.e., $k_j = \{r_j\}_{e_S^{-1}}$ in the idealized form), we can deduce following formulas.

F$_4$: C *believes* that k_j is *fresh* using A$_3$. (*Freshness-propagation* rule)

F$_5$: C *believes* $C \overset{k_j}{\leftrightarrow} S$ using F$_4$ and F$_3$. (*Session Key* rule)

F$_6$: C *receives* $(m_j, \{m_j\}_{e_S^{-1}})$ using F$_5$ and I$_1$. (*Message-decryption* rule)

F$_7$: C *receives* $\{m_j\}_{e_S^{-1}}$ using F$_6$. (*Sight-projection* rule)

F$_8$: C *believes* that S *said* m_j using A$_2$ and F$_7$. (*Message-meaning* rule)

As C can verify the data integrity and origin of the retrieved message in Step 4 of the Transfer Phase, we then can infer Formulas F$_9$ and, thus, F$_{10}$.

F$_9$: C *believes* that S *believes* m_j.

F$_{10}$: C *believes* m_j using A$_4$ and F$_9$. (*Jurisdiction* rule)

According to the derivation of Formulas F$_5$, F$_8$, and F$_{10}$, we can infer that-for $j \in \{1, 2, \ldots, t\}$-the chooser can be convinced that she/he and S share an encryption/decryption key k_j for the message m_j and can verify the origin and integrity of the message m_j, respectively. In other words, the chooser can correctly obtain the applied t messages if and only if both the sender and the chooser follow our OT mechanism.

5. **Analyses.** In this section, we further analyze the security of our OT$_t^n$ mechanism and compare its functionality with recent works in Subsections 5.1 and 5.2, respectively.

5.1. **Security Analyses.** Here, we explain that our OT$_t^n$ mechanism can achieve the requirements that we defined in Subsection 2.1. In particular, for the security, we adopt "problem reduction" [15] and the following assumption to demonstrate the privacy preservation of a sender S and a chooser C in our OT$_t^n$ mechanism.

Factorization Assumption:[12, 23]

Let N be a large composite number of two large primes p and q (i.e. $N = pq$) and (e, d) be a pair of two integers such that $GCD(e, \phi(N)) = 1$ and $ed \equiv 1(\bmod \phi(N))$. It is computationally infeasible to solve the following problems:

P1: Given N, find the factor p and q of N.

P2: Given e and N, find d and $\phi(N)$ such that $ed \equiv 1(\bmod \phi(N))$.

P3: Given N, a_1, and a_2, find d such that $a_1^d \equiv a_2(\bmod N)$.

P4: Given N, c, and $a \in Z_N^*$, find b such that $b^c \equiv a(\bmod N)$.

Note that in [23], the authors proved that solving the problem *P2* is not easier than solving *P1*.

5.1.1. ***Accuracy.*** As demonstration in Theorem 4.1, we have proven that the chooser can correctly obtain the applied t messages if and only if both the sender and the chooser follow our OT_t^n mechanism. Hence, we can infer that our OT_t^n mechanism can confirm the requirement of accuracy.

5.1.2. ***Privacy of the sender.*** Here, we consider three different situations to prove the achievement of privacy of the sender in our OT_t^n.

Situatioin 1. If an attacker, Eve, intercepts any pair (m_i', r_i) sent from S to C in Step3 of the commitment phase and tries to obtain the original message m_i from it, where $m'_i = E_{k_i}(m_i||Sig_i)$ and $k_i = r_i^{d_S} \mathrm{mod} N$, she must solve the following problem.

$$P\_S1\text{: Given } N,\ m_i',\ \text{and } r_i,\ \text{find } k_i \text{ such that } k_i = r_i^{d_S} \mathrm{mod} N.$$

Now, we can show that Eve will fail in solving this problem based on Theorem 5.1.

Theorem 5.1. *Given N, m_i', and r_i, it is computationally infeasible to find k_i such that $k_i = r_i^{d_S} modN$ (i.e., P_S1 is computationally infeasible).*

Proof: Assume that there exists an algorithm AM, given that N, m_i', and r_i, that can efficiently solve problem P_S1. Through reduction from problem *P2* of the *Factorization Assumption*, we can use AM to construct another algorithm AM' as follows to efficiently solve *P2*.

Algorithm $AM'(e_S, N)$
1: choose a random integer x lower than N
2: $f \leftarrow GCD(e_S, x)$
3: **if** $f > 1$ **then**
4:     **return to** 1
5: **else**
6:     $d_S \leftarrow e_S^{-1} \bmod x$
7:     $k_i \leftarrow AM(N, m'_i, r_i)$
8:     **if** $k_i = r_i^{d_S} \bmod N$**then**
9:         **return** d_s
10:             $\phi(N) \leftarrow x$
11:     **else**
12:         **return to** 1
13:     **end if**
14: **end if**

However, we have demonstrated that problem *P2* of the Factorization Assumption is computationally infeasible. By contradiction, solving problem P_S1 is also computationally infeasible.

As the proof of Theorem 5.1, we can deduce that any attacker who intercepts the pair (m'_i, r_i) sent from S to C in Step 3 of the commitment phase cannot further obtain the original message m_i by solving the encryption key k_i.

Situatioin 2. Assume that a semi-honest chooser, Clare, has successfully retrieved t encryption keys k_j's in Step 3 of the transfer phase for decrypting t demanded messages. If she attempts to learn other $n - t$ messages, she needs to correctly compute the corresponding encryption keys through the well-known keys k_j's and random numbers r_i's, where $j \in \{1, 2, \ldots, t\}, i \in \{1, 2, \ldots, n\}$, and $t \leq n$. In other words, she must solve the following problem.

P_S2: Given N, r_j, and k_j, find d_S such that $r_j^{ds} \equiv k_j(\text{mod}N)$.

Obviously, this problem is the same as problem *P3* of the Factorization Assumption. Hence, based on the Factorization Assumption, solving problem *P_S2* is also computationally infeasible. Any chooser can only exactly obtain t out of n original messages by performing our OT_t^n mechanism.

Situatioin 3. If an attacker Eve intercepts any α_j sent from S to C in Step 2 of the transfer phase and tries to obtain the original message m_j, she first has to retrieve the corresponding key k_j from α_j. In other words, she must solve the following problem due to $\alpha_j = BC_j^{ds} \bmod N = u_j r_j^{ds} \bmod N = u_j k_j \bmod N$.

P_S3: Given N and α_j, find u_j and k_j such that $\alpha_j = u_j k_j \bmod N$.

This implies that Eve has to intercept the corresponding BC_j sent from C to S in Step 1 of the transfer phase for solving the problem

P_S3-1: Given N, BC_j, and α_j, find d_S such that $BC_j^{ds} \equiv \alpha_j(\text{mod}N)$.

Obviously, this problem is the same as problem *P3* of the *Factorization Assumption*. Hence, based on the *Factorization Assumption*, solving problem *P_S3-1* is also computationally infeasible. Now, we can show that Eve will fail in solving the problem *P_S3* based on Theorem 5.2.

Theorem 5.2. *Given N and α_j , it is computationally infeasible to find u_j and k_j such that $\alpha_j = u_j k_j \bmod N$ (i.e., P_S3 is computationally infeasible).*

Proof: Assume that there exists an algorithm AM, given N and α_j, that can efficiently solve problem *P_S3*. By reduction from problem *P_S3-1*, we can use AM to construct another algorithm AM' as follows to efficiently solve *P_S3-1*. Suppose we have the inputs N, BC_j, and α_j for AM'.

Algorithm $AM'(N, BC_j, \alpha_j)$

1: choose a random integer x
2: $(u_j, k_j) \leftarrow AM(N, \alpha_j)$
3: **if** $u_j k_j \equiv BC_j^x(\text{mod}N)$ **then**
4:     **return** $d_S \leftarrow x$
5: **else**
6:     **return to** 1
7: **end if**

However, we have shown that problem P_S3-1 is computationally infeasible based on problem *P3* of the Factorization Assumption. By contradiction, for the attacker, it is also computationally infeasible to solve problem *P_S3*.

As the proof of Theorem 5.2, we can deduce that any attacker who intercepts α_j sent from S to C in Step 2 of the transfer phase cannot further obtain the original message m_i by solving the encryption key k_j.

Based on these demonstrations of different situations, we can summarize that, by performing our OT_t^n mechanism, a chooser can only retrieve t messages and no one can get any information to reconstruct the messages possessed by the sender except the specific chooser.

5.1.3. ***Privacy of the chooser.*** In order to prove the achievement of privacy of the chooser in our OT_t^n, we consider the following two different situations.

Situatioin 1. If a sender Serena wants to determine the chooser's choices after a transfer, she has to retrieve the corresponding integers $r_j's$ from the received blind choices BC_j's. Note that she further computes $\alpha_j = BC_j^{ds} \bmod N = u_j r_j^{ds} \bmod N$ for all BC_j's in Step

2 of the transfer phase, where d_S is her private key. In other words, she must solve the following problem.

P_S4: Given N, α_j, and d_S, find u_j and r_j such that $\alpha_j = u_j r_j^{d_S} \bmod N$.

Now, we can show that Serena will fail in solving this problem based on Theorem 5.3.

Theorem 5.3. *Given N, α_j, and d_S , it is computationally infeasible to find u_j and r_j such that $\alpha_j = u_j r_j^{d_S} \bmod N$ (i.e., P_S4 is computationally infeasible).*

Proof: Assume that there exists an algorithm AM, given N, α_j, and d_S, that can efficiently solve problem *P_S4*. Through reduction from problem *P4* of the *Factorization Assumption*, we can use AM to construct another algorithm AM' as follows to efficiently solve *P4*. Suppose we have the inputs N, d_S, and α'_j for AM', where $\alpha'_j = r_j^{d_S} \bmod N$.

Algorithm $AM'(N, d_S, \alpha'_j)$

1: choose a random integer x
2: $(u_j, r_j) \leftarrow AM(N, \alpha_j, d_S)$
3: **if** $u_j r_j^{d_S} \equiv u_j x^{d_S} (\bmod N)$ **then**
4:     **return** $r_j \leftarrow x$
5: **else**
6:     **return to** 1
7: **end if**

However, we have known that problem *P4* of the *Factorization Assumption* is computationally infeasible. By contradiction, solving problem *P_S4* is also computationally infeasible.

As the proof of Theorem 5.3, we can infer that the sender cannot find out anything related to the chooser's choices.

Situatioin 2. If an attacker Eve intercepts any BC_j sent from C to S in Step 1 of the transfer phase and tries to determine the choices of C, she has to retrieve the involved u_j and r_j from the BC_j, where $BC_j \equiv u_j^{e_S} r_j \bmod N$ and e_S is the public key of S. In other words, she must solve the following problem.

*P_S*5: Given N, BC_j, and e_S, find u_j and r_j such that $BC_j \equiv u_j^{e_S} r_j \bmod N$.

Now, we can show that Eve will fail in solving this problem based on Theorem 5.4.

Theorem 5.4. *Given N, BC_j, and e_S , it is computationally infeasible to find u_j and r_j such that $BC_j \equiv u_j^{e_S} r_j \bmod N$ (i.e., P_S5 is computationally infeasible).*

Proof: Assume that there exists an algorithm AM, given N, BC_j, and e_S, that can efficiently solve problem *P_S5*. Through reduction from problem *P4* of the *Factorization Assumption*, we can use AM to construct another algorithm AM' as follows to efficiently solve *P4*. Suppose we have the inputs N, e_S, and x for AM', where $x = u_j^{e_S} \bmod N$.

Algorithm $AM'(N, e_S, x)$

1: choose a random integer y
2: $(u_j, r_j) \leftarrow AM(N, BC_j, e_S)$
3: **if** $u_j^{e_S} r_j \equiv y^{e_S} r_j (\bmod N)$ **then**
4:     **return** $u_j \leftarrow y$
5: **else**
6:     **return to** 1
7: **end if**

However, we have known that problem *P4* of the *Factorization Assumption* is computationally infeasible. By contradiction, for the attacker, it is also computationally infeasible to solve problem *P_S5*.

As the proof of Theorem 5.4, we can infer that any attacker who intercepts the BC_j sent from C to S in Step 1 of the transfer phase cannot further learn of the relationship between BC_j and r_j.

Overall, based on Theorems 5.3 and 5.4, we can guarantee the privacy of the chooser when both the sender and the chooser follow our OT_t^n mechanism.

5.1.4. ***Verifiability.*** In order to convince the chooser C of the integrity and origin of reconstructed messages, we let the sender S additionally compute a corresponding signature $Sig_i = m_i^{d_S} \bmod N$ for each original message m_i and encrypt them as a cipher message $m'_i = E_{k_i}(m_i||Sig_i)$ before she/he sends to the chooser. Hence, once C derives the encryption key k_j and decrypts the original messages and signatures using Equation (7) in Step 3 of the transfer phase, she/he can further use S's public key to verify that the reconstructed messages are not modified and really sent by the sender S.

On the other hand, even if an attacker Eve intends to forge a cipher message $m'_i = E_{k_i}(m_i||Sig_i)$ to fool the chooser, she will fail. Based on the *Factorization Assumption*'s *P2* and the proof of Theorem 5.1, it is difficult for Eve to forge a valid message m'_i and fool the chooser without knowing the encryption key k_i and S's private key d_S. As a result, our proposed OTnt mechanism can achieve verifiability.

5.1.5. ***Non-repudiation.*** We apply the RSA-based signature mechanism [23] in our OT_t^n mechanism for a chooser to verify the origin of a message. Based on the *Factorization Assumption*'s *P2*, no one can counterfeit a sender S's (signer's) signature without knowing her/his private key d_S. In other words, only the actual sender can sign the correct and valid signature for the message that she/he possesses. Hence, we can conclude that, in our OT_t^n mechanism, the sender cannot deny or repudiate the origin of the messages that she/he provides.

5.2. **Discussions.** Here, we summarize and compare the functionality of our proposed mechanism with related oblivious transfer schemes. The comparisons of the achievement of requirements and additional properties with recent works are shown in TABLE 2. In this table, "*Y*" implies that the scheme indeed achieves the corresponding property; "*N*" represents that the scheme does not satisfy the property; and "*Half*" denotes that the scheme partially fulfills the appointed property.

TABLE 2. Functionality comparisons with recent t-out-of-n oblivious transfer schemes

Properties	Schemes				
	Ours	[26] (2012)	[14] (2012)	[19] (2011)	[10] (2009)
Assumption	*Factorization*	*DDH*	*CDH*	*CDH*	*Factorization*
Accuracy	*Y*	*Y*	*Y*	*Y*	*Y*
Privacy of the sender	*Y*	*Y*	*Y*	*Y*	*Y*
Privacy of the chooser	*Y*	*Y*	*Y*	*Y*	*Y*
Verifiability	*Y*	*Half*	*N*	*N*	*N*
Non-repudiation	*Y*	*N*	*N*	*N*	*N*

As shown in TABLE 2, our proposed OT_t^n mechanism can achieve all essentials defined in Subsection 2.1. Most operations of the schemes involved in this table are implemented by modular exponentiations. However, in [14, 19], the authors additionally used bilinear pairings [4], which increase their computational overheads. The security of our proposed mechanism and [10] are based on the factorization assumption [12, 23]; of [14] and [19] are based on the Computational Diffie-Hellman (CDH) assumption [1]; and of [26] relies on the Decisional Diffie-Hellman (DDH) assumption [1]. Moreover, it is noteworthy that most OT schemes have focused on the achievement of accuracy, privacy of the sender, and privacy of the chooser. However, in order to make an OT scheme more suitable for further applications, we think that it is necessary to discuss how to convince a chooser of the integrity and origin of reconstructed messages. Therefore, we additionally defined and achieved the requirements of verifiability and non-repudiation in this paper, which have not been provided by others. In particular, in Zeng et al.'s scheme [26], although a chooser (receiver) verifies the chosen instance vectors in the middle of the entire protocol run, she/he does not verify the integrity of the decrypted message when she/he finally receives it. Hence, we think that [26] partially achieves the verifiability requirement.

As a result, our proposed OT_t^n mechanism not only satisfies the basic properties of a general OT scheme (i.e., accuracy, privacy of the sender, and privacy of the chooser), but also achieves the extended properties we have defined herein-namely, verifiability and non-repudiation. Thus, our proposed mechanism could be more suitable for further applications, such as e-commerce applications.

6. **Conclusions.** Considering the practicability of an OT scheme, in this paper, we have added two propertiesXverifiability and non-repudiationXas a part of basic requirements of a well-designed OT scheme and proposed a novel t-out-of-n version using blind signature. In addition to using the BAN logic model to demonstrate that the chooser can correctly obtain the applied t messages after executing the mechanism with the sender, we have proven the security of our OT_t^n mechanism through formal problem reduction. The analyses demonstrated that our proposed OT_t^n mechanism not only satisfies the basic properties of a general OT scheme (i.e., accuracy, privacy of the sender, and privacy of the chooser), but also achieves the extended properties we defined (i.e., verifiability and non-repudiation). As a result, we can conclude that our OT_t^n mechanism could be more suitable for further applications.

REFERENCES

[1] F. Bao, R. H. Deng, and H. Zhu, Variations of diffie-hellman problem, *Proc. of the 5th International Conference on Information and Communications Security*, pp. 301-312, 2003.

[2] A. Beimel, Y. M. Chee, H. X. Wang, and L. F. Zhang, Communication-efficient distributed oblivious transfer, *Journal of Computer and System Sciences*, vol. 78. no. 4, pp. 1142-1157, 2012.

[3] M. Bellare, and S. Micali, *Non-interactive oblivious transfer and applications*, LNCS 435, pp. 547-557, 1990.

[4] D. Boneh, and M. K. Franklin, Identity-based encryption from the Weil pairing, *Proc. of the 21st Annual International Cryptology Conference on Advances in Cryptology*, pp. 213-229, 2001.

[5] G. Brassard, C. Crepeau, and J. M. Robert, Information theoretic reduction among disclosure problems, *Proc. of the 27th Annual Symposium on Foundations of Computer Science*, pp. 168-173, 1986.

[6] M. Burrows, M. Abadi, and R. Needham, Authentication: a practical study in belief and action, *Proc. of the 2nd conference on Theoretical aspects of reasoning about knowledge*, pp. 325-342, 1988.

[7] M. Burrows, M. Abadi, and R. Needham, A logic of authentication, *Journal of ACM Transactions on Computer Systems*, vol. 8, no. 1, pp. 18-36, 1990.

[8] J. Camenisch, G. Neven, and A. Shelat, Simulatable adaptive oblivious transfer, *Proc. of the 26th annual international conference on Advances in Cryptology*, pp. 573-590, 2007.

[9] D. Chaum, Blind signature for untraceable payments, *Proc. of 2nd International Cryptology Conference*, pp. 199-203, 1982.

[10] C. C. Chang, and J. S. Lee, Robust t-out-of-n oblivious transfer mechanism based on CRT, *Journal of Network and Computer Applications*, vol. 32, no. 1, pp. 226-235, 2009.

[11] D. Chaum, Blind signature systems, *Proc. of 3rd International Cryptology Conference*, pp. 153, 1983.
[12] R. Cramer, and V. Shoup, Signature schemes based on the strong RSA assumption, *Journal of ACM Transactions on Information and System Security*, vol. 3, no. 3, pp. 161-185, 2000.
[13] S. Even, O. Goldreich, and A. Lempel, A randomized protocol for signing contracts, *Journal of Communications of the ACM*, vol. 28, no. 6, pp. 637-647, 1985.
[14] J. Han, W. Susilo, Y. Mu, and J. Yan, Efficient oblivious transfers with access control, *Journal of Computers & Mathematics with Applications*, vol. 63, no. 4, pp. 827-837, 2012.
[15] J. E. Hopcroft, R. Motwani, and J. D. Ullman, *Introduction to Automata Theory, Languages, and Computation (2nd Edition)*, Addison-Wesley, Boston, U.S.A., 2001.
[16] J. Kilian, Founding cryptography on oblivious transfer, *Proceedings of the twentieth annual ACM symposium on Theory of computing*, pp. 20-31, 1988.
[17] Y. X. Lai, C. F. Lai, C. C. Hu, H. C. Chao, and Y. M. Huang, A personalized mobile IPTV system with seamless video reconstruction algorithm in cloud networks, *International Journal of Communication Systems*, vol. 24, no. 10, pp. 1375-1387, 2011.
[18] J. S. Li, and K. H. Liu, A hidden mutual authentication protocol for low-cost RFID tags, *International Journal of Communication Systems*, vol. 24, no. 9, pp. 1196-1211, 2011.
[19] X. Ma, L. Xu, and F. Zhang, Oblivious transfer with timed-release receiver's privacy, *Journal of Systems and Software*, vol. 84, no. 3, pp. 460-464, 2011.
[20] Y. Mu, J. Zhang, V. Varadharajan, and Y. X. Lin, Robust non-interactive oblivious transfer, *IEEE Communications Letters*, vol. 7, no. 4, pp. 153-155, 2003.
[21] M. Naor, and B. Pinkas, Efficient oblivious transfer protocols, *Proc. of the 12th annual ACM-SIAM symposium on Discrete algorithms*, pp. 448-457, 2001.
[22] M. O. Rabin, How to exchange secrets by oblivious transfer, *Technical Report TR-81*, Aiken Computation Laboratory, Harvard University, 1981.
[23] R. L. Rivest, A. Shamir, and L. Adleman, A method for obtaining digital signatures and public-key cryptosystems, *Journal of Communications of the ACM*, vol. 21, no. 2, pp. 120-126, 1978.
[24] W. G. Tzeng, Efficient 1-out-of-n oblivious transfer schemes with universally usable parameters, *IEEE Trans. Computers*, vol. 53, no. 2, pp. 232-240, 2004.
[25] S. P. Yang, and X. Li, Defect in protocol analysis with BAN logic on man-in-the-middle attacks, *Journal of Application Research of Computers,*, vol. 24, no. 3, pp. 149-151, 2007.
[26] B. Zeng, C. Tartary, P. Xu, J. Jing, and X. Tang, A practical framework for t-out-of-n oblivious transfer with security against covert adversaries, *IEEE Trans. Information Forensics and Security*, vol. 7, no. 2, pp. 465-479, 2012.
[27] J. Zhang, and Y. Wang, Two provably secure k-out-of-n oblivious transfer schemes, *Journal of Applied Mathematics and Computation*, vol. 169, no. 2, pp. 1211-1220, 2005.
[28] S. Zhong, and T. Chen, An efficient identity-based protocol for private matching, *International Journal of Communication Systems*, vol. 24, no. 4, pp. 543-552, 2011.
[29] S. Zhong, and Y. R. Yang, Verifiable distributed oblivious transfer and mobile agent security, *Journal of Mobile Networks and Applications*, vol. 11, no. 2, pp. 201-210, 2006.