Efficient k-out-of-n oblivious transfer scheme with the ideal communication cost

Jianchang Lai  
*University of Wollongong, jl967@uowmail.edu.au*

Yi Mu  
*University of Wollongong, ymu@uow.edu.au*

Fuchun Guo  
*University of Wollongong, fuchun@uow.edu.au*

Rongmao Chen  
*National University of Defense Technology Changsha, rc517@uowmail.edu.au*

Sha Ma  
*South China Agricultural University, sma@uow.edu.au*

Publication Details  
Efficient k-out-of-n oblivious transfer scheme with the ideal communication cost

Abstract
In this paper, we propose a two-round k-out-of-n oblivious transfer scheme with the minimum communication cost. In our proposed scheme, the messages sent by the receiver R to the sender S consist of only three elements, which is independent of n and k, while the messages from S to R are (n+1) elements when the sender holds n secrets. Our scheme features a nice property of universal parameter, where the system parameter can be used by all senders and receivers. The proposed k-out-of-n oblivious transfer scheme is the most efficient two-round scheme in terms of the number of messages transferred between two communicating parties in known constructions. The scheme preserves the privacy of receiver’s choice and sender’s security.

Disciplines
Engineering | Science and Technology Studies

Publication Details

This journal article is available at Research Online: https://ro.uow.edu.au/eispapers1/966
Efficient $k$-out-of-$n$ Oblivious Transfer Scheme with the Ideal Communication Cost

Jianchang Lai$^{a,*}$, Yi Mu$^a$, Fuchun Guo$^{a,*}$, Rongmao Chen$^b$, Sha Ma$^c$

$^a$Institute of Cybersecurity and Cryptology, School of Computing and Information Technology, University of Wollongong, Wollongong, Australia
$^b$College of Computer, National University of Defense Technology, Changsha, China
$^c$College of Mathematics and Informatics, South China Agricultural University, Guangzhou, Guangdong, China

Abstract

In this paper, we propose a two-round $k$-out-of-$n$ oblivious transfer scheme with the minimum communication cost. In our proposed scheme, the messages sent by the receiver $R$ to the sender $S$ consist of only three elements, which is independent of $n$ and $k$, while the messages from $S$ to $R$ are $(n + 1)$ elements when the sender holds $n$ secrets. Our scheme features a nice property of universal parameter, where the system parameter can be used by all senders and receivers. The proposed $k$-out-of-$n$ oblivious transfer scheme is the most efficient two-round scheme in terms of the number of messages transferred between two communicating parties in known constructions. The scheme preserves the privacy of receiver’s choice and sender’s security.

Keywords: Oblivious Transfer, Privacy, Minimum Communication Cost, Encryption.

1. Introduction

Oblivious transfer (OT) is one of the most important building blocks to construct secure and privacy-preserving protocols in cryptography, such as contract
signing [11], private information retrieval [6] and secure function evaluation [12].

An oblivious transfer scheme is a two-party protocol between a sender $S$ and a receiver $R$. The sender holds several secrets and the receiver wants to obtain some of them in the way that the receiver gets the secrets of his/her choice only, without revealing anything about his choice to the sender. The sender should not know which secrets are obtained by the receiver. The first OT scheme was proposed by Rabin [32], where the sender sends a secret to the receiver, and the receiver obtains the secret with probability $1/2$. Even, Goldreich and Lempel [11] gave a more general OT scheme called 1-out-of-2 OT ($OT^1_2$) where the sender has two one-bit secrets ($m_0, m_1$). Brassard, Crépeau and Robert [4] extended the $OT^1_2$ to 1-out-of-$n$ OT ($OT^1_n$) where the sender holds $n$ secrets and the receiver wants to obtain one of them of its choice.

In OT schemes, one of the most general types is $k$-out-of-$n$ oblivious transfer ($OT^k_n$), where the sender holds $n$ different secrets and the receiver wants to obtain $k$ ($k < n$) secrets simultaneously\(^1\). As the large bandwidth resource is not always available and usually expensive, it is desired to reduce the total communication cost as much as possible during the communication. Many $OT^k_n$ schemes [28, 8, 7, 15, 14, 27, 34] have been studied. In these schemes, the ideal communication rounds can be two only. Supposing the indices of secrets and system parameters are known by the sender and the receiver, the receiver sends her/his choice as a request to the sender in the first round, then the sender should respond the request in the second round\(^2\).

From the state-of-art two-round $OT^k_n$ schemes in the literature, the most efficient one with the minimum number of messages from $R$ to $S$ was proposed by Guo, Mu and Susilo in [15]. The authors first presented an efficient subset membership encryption scheme (SME) and applied the SME scheme to con-

---

\(^1\)The $OT^k_n$ scheme with such features is called non-adaptive $OT^k_n$.

\(^2\)We refer one communication (a flow of information transmission) between two parties as one round in this paper. Thus the ideal communication rounds OT schemes under this definition is "two-round" OT schemes.
struct an efficient $\text{OT}_n^k$ scheme. In their scheme, the receiver sends only three messages to the sender, which is independent of $k$ and $n$. While the tradeoff is that the messages from $S$ to $R$ are $2n$, which is larger than the other $\text{OT}_n^k$ schemes. Chu and Tzeng [7] proposed an efficient $\text{OT}_n^k$ scheme based on [29]. Their scheme achieves the minimum number of messages from $S$ to $R$, namely $n + k$, in the known constructions. But the messages from $R$ to $S$ in [7] are linear in the receiver’s choice $k$.

1.1. Ideal Communication Cost

In the $\text{OT}_n^k$ schemes with ideal communication rounds, as the sender holds $n$ secrets and does not know the receiver’s choice, $S$ has to send the messages including $n$ encrypted secrets to $R$. To decrypt the ciphertext successfully, the messages from $S$ to $R$ should be $O(n)$. For example, to encrypt a secret using ElGamal encryption, the ciphertext consists of two elements. One of them is used to recover the encryption key. Thus, in a secure $\text{OT}_n^k$ scheme, the ideal communication cost is that the messages from $R$ to $S$ are constant which is independent of $n$ and $k$, and the messages from $S$ to $R$ is $(n + 1)$ in public key cryptosystems. The additional one element is used to recover the decryption keys. From the above, we note that both schemes in [15] and [7] cannot achieve ideal communication cost. The scheme in [15] achieves ideal communication cost from $R$ to $S$, but cannot achieve that from $S$ to $R$. While the scheme in [7] does not possess this property in any round. There are no existing known constructions of secure $\text{OT}_n^k$ in the literature can achieve the ideal communication cost.

1.2. Our Contributions

In this paper we propose the first two-round $\text{OT}_n^k$ scheme with ideal communication cost; precisely, the messages from $R$ to $S$ are constant, with only three elements which are independent of $n$ and $k$, and the messages from $S$ to $R$ contain $n + 1$ elements. Compared with the two-round $\text{OT}_n^k$ schemes in the literature, our proposed $\text{OT}_n^k$ scheme is the most efficient one in terms of each
Table 1: Comparison of two-round $\text{OT}_n^k$ schemes in terms of communication cost.

<table>
<thead>
<tr>
<th>System Parameter</th>
<th>Messages $(R \rightarrow S)$</th>
<th>Messages $(S \rightarrow R)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mu et al. [27]</td>
<td>$2n</td>
<td>\mathbb{Z}_p</td>
</tr>
<tr>
<td>Zhang and Wang [34]</td>
<td>$</td>
<td>G</td>
</tr>
<tr>
<td>Chu and Tzeng [8]</td>
<td>$</td>
<td>G</td>
</tr>
<tr>
<td>Chu and Tzeng [7]</td>
<td>$</td>
<td>G</td>
</tr>
<tr>
<td>Guo et al. [14]</td>
<td>$(n^2 + 3n + 3)</td>
<td>G</td>
</tr>
<tr>
<td>Guo et al. [15]</td>
<td>$(n + 1)</td>
<td>G</td>
</tr>
<tr>
<td>Ours</td>
<td>$(2n + 2)</td>
<td>G</td>
</tr>
</tbody>
</table>

round. The system parameter in our scheme is universal, which can be used by any users. We give an overview of the comparing results in Table 1.

In the first round, the receiver sends a token which contains the receiver’s choice, and a proof information which is used to prove that its choice is not larger than $k$ to the sender. In the second round, the sender responds with encrypted secrets after checking the validity of the received token. Finally, the receiver uses its choice set and secret key to decrypt the ciphertext and only retrieves the secrets whose indexes are in its choice set. To analyze the security of our proposed scheme, we propose two new assumptions and prove that our proposed assumptions are hard in the generic group model. Based on these two assumptions, we derive the security of our proposed scheme under three non-adaptive games and show that our scheme is unconditionally secure for receiver’s choice and preserves the sender’s security. Any choice larger than $k$ can be detected easily by the sender. The tradeoff of our scheme is that the system parameter consists of $2n + 2$ elements in the group $G$.

1.3. Other Related Work

The notion of oblivious transfer was put forth by Rabin [32] to achieve secure two-party communication, and the author proposed a bit-OT protocol based on
quadratic roots modulo a composite. Even et al. [11] extended this notion to \( \text{OT}_2^1 \), where the sender holds two one-bit secrets and the receiver would like to receive one of them of his choice. Brassard et al. [4] presented a more general \( \text{OT}_n^1 \) scheme, which is also known as “all-or-nothing disclosure of secrets (ANDOS)” . After that, several oblivious transfer variants have been proposed. They mainly focused on improving the efficiency of secure computation and security.

Oblivious transfer with adaptive queries was proposed by Naor and Pinkas [28] where the receiver can query the \( i \)th value depending on the first \( i - 1 \) values. In this setting, it requires two phases, the commitment phase and the transfer phase. \( S \) first should commit all secrets to \( R \) in the commitment phase, and then \( R \) makes queries of the secret one by one in the transfer phase. Adaptive OT scheme has many applications, such as oblivious search and oblivious database queries. Ogata and Kurosawa [31] proposed an efficient adaptive OT based on the RSA system. Chu and Tzeng [8] proposed an adaptive \( \text{OT}_n^k \) scheme based on basic cryptographic techniques, which is as efficient as the scheme in [31]. Camenisch, Neven and Shelat [5] presented simulatable adaptive oblivious transfer schemes that achieve a stronger security notion. They used the technique of blind signatures and both sender and receiver security can be fully simulated in their scheme. Green and Hohenberger [13] proposed a simulatable oblivious transfer based on blind identity-based encryption. Further research along this line appears in [22, 20, 33].

To solve the problem of that given a small number of oblivious transfers, how to implement a large number of oblivious transfers, Ishai et al. [17] proposed the first two efficient oblivious transfer extension protocols. Their first protocol is only secure against semi-honest (positive) adversaries. The improvements and optimizations to this protocol were given in [1, 18]. To achieve the security for malicious (active) adversaries, the authors used the cut-and-choose technique and proposed the second OT extension protocol. After that, constructing an efficient OT extension protocol that is secure against malicious adversaries has been extensively studied. There are some approaches to achieve security against
malicious adversaries for OT extensions, but most of them were built on the semi-honest protocol of [17] and added the consistency checks.

Nielsen et al. [30] proposed an alternative approach for achieving actively-secure OT extension in the random oracle model. They checked the consistency by hashing the strings that were transferred in the base-OTs and it was very efficient. Larraia [21] introduced a new approach to constructing OT extension schemes, which can be proved secure against malicious adversaries without the random oracle. Asharov et al. [2] presented a more efficient OT extension protocol for the setting of malicious adversaries. Their protocol requires less communication than previous works and can be proved secure with or without random oracles.

The technique of cut-and-choose has been regarded as a useful basic block to construct the two-party protocols against malicious adversaries, and formalized and proven secure by Lindell and Pinkas [24]. A number of cut-and-choose oblivious transfer protocols [25, 26, 23, 16] have focused on reducing the concrete overhead of the cut-and-choose approach. Kolesnikov and Kumaresan [19] proposed an efficient cut-and-choose OT scheme and its variants with small concrete communication overhead in an OT-hybrid model.

Organization. The rest of this paper is organized as follows. In Section 2, we show some preliminaries including notations, the definition of OT\(^k\) scheme and the corresponding security models. In Section 3, we first review the bilinear map and aggregation algorithm. We then present the OT\(^k\) construction and evaluate the scheme. We give two new complexity assumptions in Section 4. The security analysis of the proposed scheme is presented in Section 5 and we conclude the paper in Section 6.

2. Preliminaries

In this section, we give the definition of OT scheme and its security requirements. Before describing the definitions, we give some notations that will be used in the remaining sections.
2.1. Notations

Now, we present the notations and conventions used in this paper in Table 2. Let $\mathbb{N}$ denote the set of natural numbers. We say a function $\epsilon : \mathbb{N} \to [0, 1]$ is negligible if for every $d \in \mathbb{N}$, there exists a $\lambda_d \in \mathbb{N}$ such that $\epsilon(\lambda) \leq \lambda^{-d}$ for all $\lambda > \lambda_d$.

2.2. Definition of $\text{OT}_n^k$ Scheme

Let $m_1, m_2, \cdots, m_n$ be $n$ secrets held by the sender and receiver’s $k$ chosen indices are $l_1, l_2, \cdots, l_k$, where $k < n$. We assume that the sender is honest-but-curious, that is, it will not send the secrets which are not the same as what he claimed, including the content and the order. We borrow the idea of subset membership encryption in [15] and give the definition of the non-adaptive $\text{OT}_n^k$.
Inputs:

- The system parameter $SP$, generated by a Setup algorithm which takes a security parameter $\lambda$ as input, denoted by $\text{Setup}(1^\lambda)$.
- $S$ holds a secret set $M = \{m_1, m_2, \cdots, m_n\}$.
- $R$ holds his choice set $G = \{l_1, l_2, \cdots, l_k\}$, where $k \in [n]$.

Protocol:

1. $R \rightarrow S : R$ takes the system parameter $SP$ and the choice set $G$ as input, it outputs $(T, sk)$ where $sk$ is a secret key and $T$ includes a token $P(G)$ which contains the receiver’s choice, a proof information $\Sigma$ which is used to check the number of choice set and a number $k$. Then $R$ sends $T$ to $S$.

2. $S \rightarrow R : S$ takes the system parameter $SP$, $T$ and a secret set $M$ as input, it first checks whether $|G| \leq k$ via a verification algorithm and aborts if no. If yes, it performs an encryption algorithm $\text{Encrypt}$ and outputs the ciphertext $CT = \text{Encrypt}(SP, P(G), M)$. Then $S$ sends $CT$ to $R$.

Outputs: $S$ receives no output. $R$ takes the system parameter $SP$, the ciphertext $CT$, his secret key $sk$ and the choice set $G$ as input.

- For every $i \in G$, it outputs $m_i$.
- For every $i \notin G$, it outputs $\bot$.

Figure 1: The definition of $\text{OT}_{n}^{k}$ scheme
scheme in Fig.1.

Correctness. An $\text{OT}_n^k$ scheme is correct if the receiver obtains the secrets of his choice only when the sender and the receiver follow the steps of the scheme.

2.3. Security Models

An $\text{OT}_n^k$ scheme should meet the following security requirements:

- **Receiver’s privacy**

  Given any two distinct sets of choice $G_0 = \{l_1, l_2, \cdots, l_{k_0}\}$ and $G_1 = \{l'_1, l'_2, \cdots, l'_{k_1}\}$, where $k_0, k_1 < k$, the $P(G)$ received by the sender can not be distinguished whether it generated under $G_0$ or $G_1$. That is, it is hard to distinguish whether $G = G_0$ or $G = G_1$.

- **Sender’s security**

  - Indistinguishability: Given any choice set $G = \{l_1, l_2, \cdots, l_k\}$, the unchosen secrets are indistinguishable from the random ones. More precisely, given $(G, P(G))$, a target index $I^* \in [n]$ where $I^* \notin G$, two secrets $m_0, m_1$ (one of them is regarded as $I^*$-th secret) from the same space and a ciphertext $CT^*$ generated under $(I^*, m_{I^*}, P(G))$ where $m_{I^*} = m_c$, $c$ is randomly chosen from $\{0, 1\}$, it is hard to distinguish whether $c = 0$ or $c = 1$.

  - Accountability: Given $(P(G), G, sk)$ satisfying $|G| > k$, it is hard to generate $T$ that passes the verification algorithm.

We define three non-adaptive security models via game playing to meet the above security requirements. The games are defined between a challenger $C$ and an adversary $A$, which are stated as follows.

**Game 1: Receiver’s privacy.**

This model guarantees that the adversary (sender) learns nothing about which indices are chosen by the receiver without a valid secret key.

- **Setup:** $C$ takes as input a security parameter $\lambda$ and runs the Setup algorithm to generate the system parameter $SP$. Then it sends $SP$ to $A$. 

9
• **Challenge:** \(A\) outputs two distinct choice sets \(G_0 = \{l_1, l_2, \cdots, l_{k_0}\}, G_1 = \{l'_1, l'_2, \cdots, l'_{k_1}\}\), where \(k_0, k_1 \leq k\). \(C\) picks a random bit \(c \in \{0, 1\}\), sets \(G = G_c\) and generates \((P(G), G, sk)\). Then it computes \(T = (P(G), \Sigma, k)\) and sends it to \(A\).

• **Output:** \(A\) outputs its guess \(c'\) and wins the game if \(c' = c\).

We define the advantage of \(A\) in winning the game as

\[
\text{Adv}^{\text{RP}}(\lambda) = \left| \Pr[c' = c] - 1/2 \right|.
\]

**Definition 1.** We say that an OT\(_n\) scheme preserves the privacy of receiver’s choice with \((t, \epsilon)\) if for all \(t\)-probability polynomial time (PPT) adversaries, \(\epsilon = \text{Adv}^{\text{RP}}(\lambda)\) is negligible. The choices of the receiver are unconditionally secure if \(\epsilon = 0\) for all PTT adversaries.

**Game 2: Sender’s security (Indistinguishability).**

The model of indistinguishability captures the attack that even the adversary (receiver) can access the secret key, it cannot retrieve the secrets whose indices are not in the choice set.

• **Init:** \(A\) outputs a set \(G^* = \{l^*_1, l^*_2, \cdots, l^*_k\}\) and a target index \(I^* \in [n]\setminus G^*\) which it wants to challenge.

• **Setup:** \(C\) takes as input a security parameter \(\lambda\) and runs the **Setup** algorithm to generate the system parameter \(SP\). Then it sends \(SP\) to \(A\).

• **Challenge:** \(A\) outputs \((G^*, P(G^*), sk^*)\) and two secrets \(m_0, m_1\) from the same secret space for challenge. \(C\) first checks whether \(P(G^*)\) is generated from \(G^*\) by using the secret key \(sk^*\). If yes, it picks a random bit \(c \in \{0, 1\}\) and generates the challenge ciphertext \(CT^* = \text{Encrypt}(SP, P(G^*), m_c)\) for the secret with index \(I^*\). It then sends \(CT^*\) to \(A\). Otherwise, it aborts.

• **Guess:** \(A\) outputs a guess \(c'\) and wins the game if \(c' = c\).

We define the advantage of \(A\) in winning the game as

\[
\text{Adv}^{\text{SS}}(\lambda) = \left| \Pr[c' = c] - 1/2 \right|.
\]
Definition 2. An $OT_k^n$ scheme preserves the indistinguishability security and it is $(t, \epsilon)$-secure if for all $t$-polynomial time adversaries, $\epsilon = \text{Adv}^{SS}(\lambda)$ is negligible.

Game 3: Sender's security (Accountability).

The accountability security guarantees that any forge proofs generated by the choice set with number larger than $k$ will be detected even the adversary (receiver) knows the secret key of computing $P(G)$.

- **Setup**: $C$ takes as input a security parameter $\lambda$ and runs the Setup algorithm to generate the system parameter $SP$. Then it sends $SP$ to $A$.

- **Challenge**: $A$ outputs $(P(G^*), G^*, sk^*)$ and $k$ for challenge. $P(G^*)$ was generated from $(G^*, sk^*)$ and $|G^*| > k$.

- **Output**: $A$ outputs $T^* = (P(G^*), \Sigma^*, k)$ and wins the game if $T^*$ passes the verification algorithm.

We define the advantage of $A$ in winning the game as $\text{Adv}^A(\lambda)$ in computing such $T^*$.

Definition 3. An $OT_k^n$ scheme captures the accountability security and it is $(t, \epsilon)$-secure if for all $t$-polynomial time adversaries, $\epsilon = \text{Adv}^A(\lambda)$ is negligible.

3. Our $OT_k^n$ Scheme

In this section, we present the concrete construction of our scheme. First, we briefly review bilinear groups and the aggregation algorithm used in our proposed scheme.

Let $G, G_T$ be two cyclic multiplicative groups of the same prime order $p$, $g$ be the generator of $G$. A map $e : G \times G \to G_T$ is said to be a bilinear map if

(1) for all $u, v \in G$ and $a, b \in \mathbb{Z}_p$, we have $e(u^a, v^b) = e(u, v)^{ab}$ and $e(g, g) \neq 1$,

and there exists an efficient algorithm to compute $e(g, h)$ for all $g, h \in G$. A bilinear group $BG = (G, G_T, e, p)$ is composed of objects as described above.
3.1. Aggregation Algorithm

Given group elements \( \left( g^{\frac{1}{a+1}}, g^{\frac{1}{a+2}}, \ldots, g^{\frac{1}{a+n}} \right) \) for unknown \( a \in \mathbb{Z}_p^* \), the aim of aggregation algorithm is to compute

\[
g^{\frac{1}{(a+1)(a+2)\cdots(a+n)}}.
\]

From [10], we have that there exists integers \( s_1, s_2, \ldots, s_n \) satisfying

\[
s_1 \prod_{i \in [n], i \neq 1} (a + i) + s_2 \prod_{i \in [n], i \neq 2} (a + i) + \cdots + s_n \prod_{i \in [n], i \neq n} (a + i) = 1
\]

for all \( a \) such that we have

\[
g^{s_1} \cdot g^{s_2} \cdots g^{s_n} = g^{\frac{1}{(a+1)(a+2)\cdots(a+n)}}.
\]

The aggregation is independent of the group element \( g \), which means it is available for all group elements as long as they are identical.

3.2. Overview of technique

In this subsection, we give a highlight of our scheme. Let \( B\mathbb{G} = (G, G_T, e, p) \) be a bilinear group with two generators \( g, h \in G \). \( \alpha \) is known by the system generator only. In our setting, the token \( P(G) = g^{(\alpha+1)(\alpha+2)\cdots(\alpha+n)} \) and each secret \( m_i \) is encrypted using a key \( e \left( g^{\frac{1}{(a+1)(a+2)\cdots(\alpha+n)}}, h \right)^{r} \), that is \( C_i = e \left( g^{\frac{1}{(a+1)(a+2)\cdots(\alpha+n)}}, h \right)^{r} \cdot m_i \).

If \( i \in G \), \( h^{(\alpha+1)(\alpha+2)\cdots(\alpha+n)} \) is computable from the system parameters. Thus, the decryptor can retrieve the encryption (decryption) key \( e \left( g^{\frac{1}{(\alpha+1)(\alpha+2)\cdots(\alpha+n)}}, h \right)^{r} \) together with \( P(G)^r \) and its private key \( s \). If \( i \notin G \), the value of \( h^{(\alpha+1)(\alpha+2)\cdots(\alpha+n)} \) cannot be computed. Therefore, the decryptor is unable to retrieve the encryption key and get the corresponding secret.

3.3. Construction

The concrete OT\(_n^k\) scheme is illustrated in Fig.2. A trusted third party called PKG establishes the system by choosing a security parameter \( \lambda \) and a
Inputs:

- System parameter $SP$. The PKG runs the Setup algorithm as follow. Given a security parameter $\lambda$, this algorithm generates a bilinear group $BG = (G, G_T, e, p)$ with two generators $g, h \in G$. Then it randomly chooses $\alpha \in \mathbb{Z}_p^*$ as the system secret key and computes $g_i = g^{\frac{1}{\alpha + i}}, h_i = h^{\alpha^i}$ for all $i = 1, 2, \cdots, n$. The system parameter $SP$ consists of $(BG, g, h, g_1, g_2, \cdots, g_n, h_1, h_2, \cdots, h_n)$.
- $S$ holds a set of secrets $M = \{m_1, m_2, \cdots, m_n\} \in G_T$.
- $R$ holds his choice set $G = \{l_1, l_2, \cdots, l_k\} \subset [n]$.

Protocol:

1. $R \rightarrow S$: Given a choice set $G = \{l_1, l_2, \cdots, l_k\}$ and the system parameters $SP$, $R$ picks a random $s \in \mathbb{Z}_p^*$ as his secret key $sk$ and uses the Aggregation algorithm to compute

$$P(G) = g^{(\alpha + l_1)(\alpha + l_2) \cdots (\alpha + l_k)}, \quad \Sigma = h^{\frac{n(n + 2 \cdots (n + k) \cdot \alpha^k)}{2}}.$$ 

and sets $T = (P(G), \Sigma, k)$.

2. $S \rightarrow R$: $S$ runs the Encrypt algorithm as follow. Given a set $T = (P(G), \Sigma, k)$, a set of secrets $M = \{m_1, m_2, \cdots, m_n\}$ and the system parameter $SP$, it first performs the verification algorithm as:

$$e(P(G), \Sigma) = e\left(g, h^{\alpha^{n-k}}\right).$$

If the equation does not hold, it aborts. Otherwise, it accepts $|G| \leq k$. Then it picks a random $r \in \mathbb{Z}_p^*$ and computes the ciphertext $CT$ for the secrets as

$$C_0 = P(G)^r = g^{\frac{\alpha^r}{(\alpha + l_1)(\alpha + l_2) \cdots (\alpha + l_k)}},$$

and for each $i = 1, 2, \cdots, n$:

$$C_i = e\left(g^{\frac{\alpha^r}{\alpha + i}}, h^r\right) \cdot m_i.$$ 

Outputs: $R$ runs the decryption algorithm as follow. Given a ciphertext $CT = (C_0, C_1, \cdots, C_n)$, a choice set $G = \{l_1, l_2, \cdots, l_k\}$, a secret key $sk$ and the system parameter $SP$, for each $i \in G$, $R$ computes

$$m_i = C_i \cdot e\left(C_0, h^{\frac{(\alpha + l_1)(\alpha + l_2) \cdots (\alpha + l_k)}{(\alpha + i)}}\right)^{-\frac{1}{\alpha^i}}.$$ 

Figure 2: Our $OT^n_k$ scheme
random \( \alpha \) as the system secret key, and generates the system parameter \( SP = (BG, g, h, g_1, g_2, \cdots, g_n, h_1, h_2, \cdots, h_n) \), which is public known.

In the first round, the receiver chooses a random \( s \in \mathbb{Z}_p^* \) as its secret key and a set \( G = \{l_1, l_2, \cdots, l_k\} \). It then uses the Aggregation algorithm to compute a token \( P(G) = g^{(a+1)(a+2)\cdots(a+k)}_{(a+1)}^{r^s} \), and computes a proof information \( \Sigma = h^{(a+1)(a+2)\cdots(a+k)a^{n-k}} \) for its choice set \( G \).

In the second round, upon receiving a request from a receiver, the sender first tests whether \( e(P(G), \Sigma) = e\left(g, h^{a^{n-k}}\right) \) and aborts if no. Otherwise, \( S \) picks a random \( r \in \mathbb{Z}_p^* \) and computes a ciphertext \( CT \) for the secrets as \( C_0 = P(G)^{r} = g^{(a+1)(a+2)\cdots(a+k)}_{(a+1)}^{r^s} \) together with, for each \( i = 1, 2, \cdots, n \): \( C_i = e\left(g^{\frac{1}{a^{n-k}}}, h\right)^r \cdot m_i \).

Once receiving the encrypted secrets \( CT \) from the sender, the receiver, for each \( i \in G \), computes \( m_i = C_i \cdot e\left(C_0, h^{(a+1)(a+2)\cdots(a+k)}_{(a+1)}\right)^{-\frac{1}{a^{n-k}}} \). After the decryption, \( R \) gets only \( k \) secrets with indexes in \( G \) from \( S \).

### 3.4. Correctness

Below we show that our construction meets the correctness requirements.

When everything is computed as above, if \( |G| \leq k \), we have
\[
e(P(G), \Sigma) = e\left(g^{(a+1)(a+2)\cdots(a+k)}, h^{(a+1)(a+2)\cdots(a+k)a^{n-k}}\right) = e\left(g, h^{a^{n-k}}\right).
\]

If \( |G| > k \), it is impossible for receiver to compute the \( \Sigma \) which passes the checking process. In decryption phase, for \( i \in G \), we can compute \( h^{(a+1)(a+2)\cdots(a+k)}_{(a+1)} \) from the system parameter, thus we have
\[
C_i \cdot e\left(C_0, h^{(a+1)(a+2)\cdots(a+k)}_{(a+1)}\right)^{-\frac{1}{a^{n-k}}} = m_i \cdot e\left(g^{\frac{1}{a^{n-k}}}, h\right)^r \cdot e\left(g^{(a+1)(a+2)\cdots(a+k)}, h^{(a+1)(a+2)\cdots(a+k)}_{(a+1)}\right)^{-\frac{1}{a^{n-k}}} = m_i \cdot e\left(g, h\right)^r \left(\frac{r^s}{a^{n-k}}\right) = m_i.
\]
3.5. Evaluation

Our proposed two-round OT\(_k\) scheme is very efficient in terms of communication cost. In our construction, the receiver only sends two group elements and one integer to the sender. The overhead from R to S is the same as the most efficient one [15] in the literature, which is independent of \(n\) and \(k\). While, in the second round, the transfer messages from S to R are \(n + 1\), more precisely, one element in \(G\) and \(n\) elements in \(G_T\). Our scheme achieves the minimum communication overhead in both two rounds comparing with the existing known OT\(_n\) schemes and achieves the ideal communication cost in public key setting. The total communication cost in our scheme is \(n + 4\) elements, namely \(3|G|, n|G_T|\) and \(|\mathbb{Z}_p|\). The size of the system parameter in our scheme is linear in the number of the secrets held by the sender.

Note that in our construction, to avoid sending linear messages to the sender and achieving constant overhead, the receiver requires performing the Aggregation algorithm once which is expensive and \(k\) times exponentiation operations in \(G\). We stress that it is a tradeoff. To reduce the communication overhead, the price to pay is to execute more computation. For the sender, as we described above, without knowing which secrets are required, it has to encrypt and send all secrets, which requires performing one group exponentiation operation in \(G\) and \(n\) exponentiation operations in \(G_T\).

In the decryption phase, as the receiver holds its choice set \(G\) and knows the secret key \(sk\), for each index, it can pre-compute \(k - 1\) group exponentiation operations associated with \(h\) without the knowledge of response from the sender. When receiving a ciphertext from the sender, the receiver needs to perform \(k\) pairing computations to retrieve \(k\) message. Therefore, the decryption cost is \(k\) pairing computations in all, which is the same as that in [15].

4. Complex Assumptions

In this section, we define two specific Diffie-Hellman exponent problems introduced by Boneh, Boyen and Goh [3] and denote them as \((f, \hat{g}, F)\)-GDDHE
and \((f, n)\)-DHE. The security of the proposed scheme relies on the corresponding two defined assumptions. The former one is by slightly modifying the \((f, g, F)\)-GDDHE problem in \([9]\). We first give the definition of \((f, \hat{g}, F)\)-GDDHE as follows.

\((f, \hat{g}, F)\)-GDDHE Problem.

**Input:** Let \(BG = (\mathbb{G}, \mathbb{G}_T, e, p)\) be a bilinear group and \(g_0\) be a generator of \(\mathbb{G}\). Let \(f(x) = (x + 1)(x + 2) \cdots (x + n) \in \mathbb{Z}_p[x]\) and \((x + t) \not\mid f(x)\), \(g(x) = \frac{f(x)}{(x + t) \prod_{i=1}^{k} (x + l_i)} \in \mathbb{Z}_p[x]\), where \(t, l_i \in [n]\) for \(i = 1, 2, \ldots, k < n\) and all are distinct. The following group elements are given

\[
g_0, \ g_0^2, \ldots, \ g_0^n, \ g_0^{f(a)}, \ g_0^{g(a)(a+t)b}, \ g_0^{w(a+t)}, \ g_0^{w(a+t)a}, \ g_0^{w(a+t)a^2}, \ g_0^{w(a+t)a^n},
\]

and \(T \in \mathbb{G}_T\), where \(a, b, t\) and \(w\) are unknown random exponents in \(\mathbb{Z}_p\).

**Output:** a bit \(\mu\).

We define that the problem has been solved correctly if the output is

\[
\mu = \begin{cases} 
1 & T = e(g_0, g_0)^{w-bf(a)}, \\
0 & T \neq e(g_0, g_0)^{w-bf(a)}. 
\end{cases}
\]

Let us denote by \(I\) the input of the instance, true the event that \(T\) is indeed equal to \(e(g_0, g_0)^{w-bf(a)}\) and by false the event that \(T\) is a random element of \(\mathbb{G}_T\). The goal of \((f, \hat{g}, F)\)-GDDHE is to decide whether \(T\) is equal to \(e(g_0, g_0)^{w-bf(a)}\) or to some random element of \(\mathbb{G}_T\). We then define the advantage of an algorithm \(B\) in solving the \((f, \hat{g}, F)\)-GDDHE problem in \(BG\) as

\[
\text{Adv}_{\text{gddhe}}(f, \hat{g}, F, B) = \left| \Pr[B(I) = 1 | \text{true}] - \Pr[B(I) = 1 | \text{false}] \right|,
\]

where the probability is over all random choices and over the random coins of \(B\). We say that the \((f, \hat{g}, F)\)-GDDHE assumption holds if for any probability polynomial time algorithm \(B\), we have \(\text{Adv}_{\text{gddhe}}(f, \hat{g}, F, B)\) is negligible.

**Theorem 1.** The defined \((f, \hat{g}, F)\)-GDDHE problem is one of the GDDHE problems fulfilling the hardness conditions defined in [3].
Proof. As the analysis in [9], the \((f, \hat{g}, F)\)-GDDHE problem can be reformulated as

\[
\begin{align*}
\mathbf{P} &= \left( 1, a, a^2, \cdots, a^n, f(a), g(a) \cdot (a + t) \cdot b, w \cdot (a + t) \cdot a, w \cdot (a + t) \cdot a^2, \cdots, w \cdot (a + t) \cdot a^n \right), \\
\mathbf{Q} &= 1, \\
F &= w \cdot b \cdot f(a).
\end{align*}
\]

Now we proof that \(F\) is independent of \(\langle P, Q \rangle\). We show this statement by giving a contradiction as follows.

Assume that \(F\) is dependent of \(\langle P, Q \rangle\) (i.e. \(F \in \langle P, Q \rangle\)), then there exists not-all-zero coefficients \(\{a_{i,j}\}\) and \(b_1\) such that

\[
F = \sum a_{i,j} p_i p_j + b_1 q_1,
\]

where \(p_i, p_j \in P\) and \(q_1 = 1 \in Q\). Noting that \(F = w \cdot b \cdot f(a)\), we have that, all \(a_{i,j} p_i p_j\) should be multiples of \(w \cdot b\). Below we list all the possible products of two polynomials from \(P\) which are multiples of \(w \cdot b\).

\[
\mathbf{R} = \left( w \cdot b \cdot (a + t)^2 \cdot g(a), w \cdot b \cdot a \cdot (a + t)^2 \cdot g(a), w \cdot b \cdot a^2 \cdot (a + t)^2 \cdot g(a), \cdots, w \cdot b \cdot a^n \cdot (a + t)^2 \cdot g(a) \right).
\]

If \(F \in \langle P, Q \rangle\), we have

\[
F = w \cdot b \cdot f(a) = w \cdot b \cdot (a + t)^2 \cdot A(a) \cdot g(a)
\]

where \(A(a)\) is a polynomial with \(\deg(A(a)) \leq n\). We simplify the above equation as follows,

\[
f(a) = (a + t)^2 \cdot A(a) \cdot g(a).
\]

Therefore, we have \((a + t)^2 | f(a)\), which is contradiction with \((a + t)^2 \nmid f(a)\). The assumption that \(F\) is dependent of \(\langle P, Q \rangle\) cannot hold and hence \(F \notin \langle P, Q \rangle\). This completes the proof.
Definition 4 ((\(\hat{f}, n\))-DHE-Problem). Let \(G\) be a cyclic group of prime order \(p\) and \(g, h\) be two generators of \(G\). The \((\hat{f}, n)\)-DHE problem is, given \((g, g^{\frac{1}{\pi}}, \ldots, g^{\frac{1}{\pi}}, h, h^a, h^a, \ldots, h^{a^n})\) for unknown \(a \in \mathbb{Z}_p\), output \((f(x), h^{f(a)})\), where \(f(x) \in \mathbb{Z}_p[x]\) is a polynomial function with degree \(n' > n\).

Suppose that \(q(x) = (a + 1)(a + 2) \cdots (a + n) \in \mathbb{Z}_p\) and \(g = h^{q(x)}\), we can compute \((g, g^{\frac{1}{\pi}}, g^{\frac{1}{\pi^2}}, \ldots, g^{\frac{1}{\pi^n}}, h, h^a, h^a, \ldots, h^{a^n})\). That is, the \((\hat{f}, n)\)-DHE problem equals to the hard problem, given \((h, h^a, h^{a^2}, \ldots, h^{a^n})\) for unknown \(a \in \mathbb{Z}_p\), output \((f(x), h^{f(a)})\), where \(f(x) \in \mathbb{Z}_p[x]\) is a polynomial function with degree \(n' > n\), which is defined in [14]. We say that the \((\hat{f}, n)\)-DHE assumption holds if for any probability polynomial time algorithm \(B\), the probability to solve the \((\hat{f}, n)\)-DHE problem is negligible.

5. Security Analysis

We derive the security of our proposed scheme under \((f, \hat{g}, F)\)-GDDHE assumption and \((\hat{f}, n)\)-DHE assumption.

5.1. Receiver Privacy

Theorem 2. For our scheme, receiver’s choices are unconditionally secure.

Proof. The simulator \(B\) establishes the system by choosing a security parameter \(\lambda\) and a random \(\alpha \in \mathbb{Z}_p^*\). Then it generates the system parameter \(SP\) as

\[
\left( B, g, g^{\frac{1}{\pi}}, g^{\frac{1}{\pi^2}}, \ldots, g^{\frac{1}{\pi^n}}, h, h^a, h^a, \ldots, h^{a^n} \right).
\]

Challenge: \(A\) outputs two distinct choice sets \(G_0 = \{l_1, l_2, \ldots, l_k\}\) and \(G_1 = \{l'_1, l'_2, \ldots, l'_k\}\) where \(k_0, k_1 \leq k\). \(B\) picks a random \(sk \in \mathbb{Z}_p^*\) as the secret key. Let \(T = (P(G), \Sigma, k)\) be generated from \(G = G_0\). We have

\[
P(G) = g^{\frac{1}{\prod_{i=1}^{k_1} (\alpha + l_i)}}, \quad \Sigma = h^{\frac{1}{\prod_{i=1}^{k_1} (\alpha + l_i)}}.
\]

For any distinct set \(G_1 = \{l'_1, l'_2, \ldots, l'_k\}\), we define \(sk' \in \mathbb{Z}_p\) as

\[
sk' = sk \cdot \frac{\prod_{i=1}^{k_1} (\alpha + l'_i)}{\prod_{i=1}^{k_1} (\alpha + l_i)}.
\]
We have
\[ P(G) = g^{\prod_{i=1}^{n} (-i)} = g^{\prod_{i=1}^{n} (-i)} = P(G_1), \]
\[ \Sigma = h^{\prod_{i=1}^{n} (-a)} = h^{\prod_{i=1}^{n} (-a)} = \Sigma', \]
such that \((P(G_0), \Sigma, k) = (P(G_1), \Sigma', k)\). As \(sk\) is randomly chosen from \(Z_p^*\), we have \(sk'\) is also universally random in \(Z_p^*\). Thus, the distributions of \((P(G), \Sigma, k)\) for both \(G_0\) and \(G_1\) are identical. Adversary has no advantage in guessing the receiver's choice set in \(P(G)\). Thus, our scheme achieves unconditionally secure for the choice of receiver. This completes the proof of **Theorem 2**.

### 5.2. Sender Security

**Theorem 3 (Indistinguishability).** Our proposed scheme captures the indistinguishability of sender’s security. That is, if the 
\((f, \hat{g}, F)\)-GDDHE assumption holds, the adversary (receiver) gets no information about secrets \(m_i\), where \(i \not\in G\).

**Proof.** Suppose there exists an adversary \(A\) who can distinguish the secret with advantage \(\epsilon\). We can construct an algorithm \(B\) that solves the 
\((f, \hat{g}, F)\)-GDDHE problem with advantage \(\epsilon\). Let \(\mathbb{B}G = (G, G_T, e, p)\) be a bilinear group, \(g_0\) be a generator of \(G\), \(L = \{1, 2, \ldots, n\}\) be all secrets' indices. All these objects are known by \(A\) and \(B\). \(B\) runs \(A\) and programs the reduction as follows.

**Init:** \(A\) outputs a set \(G^* = \{l_1^*, l_2^*, \ldots, l_k^*\} \subset L\) and a target secret index \(I^* \in L \setminus G^*\) for challenge.

**Setup:** To setup the system parameter, \(B\) requires an instant of the 
\((f, \hat{g}, F)\)-GDDHE problem where
\[ t = I^*, \quad f(x) = \prod_{i=1}^{n} (x + i), \quad g(x) = \frac{f(x)}{(x + I^*) \cdot \prod_{i=1}^{k} (x + l_i^*)}. \]
and \(f(x)\) and \(g(x)\) have \(n\) degrees and \((n - k - 1)\) degrees respectively. \(B\) is then given a \((f, \hat{g}, F)\)-GDDHE instance in \(\mathbb{B}G\) as:
\[ g_0, \quad g_0^2, \quad \cdots, \quad g_0^n, \quad g_0^f(a), \quad g_0^{g(a) - (a + I^*)}, \quad g_0^{w(a + I^*)}, \quad g_0^{w(a + I^*)^2}, \quad \cdots, \quad g_0^{w(a + I^*)^n}, \]
and $T \in \mathbb{G}_T$, which is either equal to $e(g_0, g_0)^{w \cdot b \cdot f(a)}$ or to some random element of $\mathbb{G}_T$. It implicitly sets $\alpha = a$ and

$$g = g_0^{f(a)}, \quad h = g_0^{w(a + l^*)},$$

which are available from the first row and third row of the instance. Then for $g_i, h_i$ in the system parameter, we have

$$g_i = g_0^\frac{1}{\alpha+i} = g_0^{\frac{i}{\alpha+i}}, \quad h_i = h^{\alpha_i} = g_0^{w(a + l^*) \cdot a^i},$$

which can be computed from the group elements in the first row and third row of the instance respectively. Then the system parameter $SP$ is

$$SP = (BG, g, h, g_i, h_i : i = 1, 2, \cdots, n).$$

**Challenge:** $A$ outputs $(P(\mathbb{G}^*), sk^*)$ and two secrets $m_0, m_1$ from the same secret space for challenge. $B$ first verifies that $P(\mathbb{G}^*)$ is indeed generated from $\mathbb{G}^*$ by using the secret key $sk^*$. If the verification fails, it aborts. Otherwise, it picks a random bit $c \in \{0, 1\}$ and computes the challenge ciphertext $CT^* = (C_0^*, C_{l^*})$ as

$$C_0^* = g_0^{sk^* \cdot g(a) \cdot (a + l^*) \cdot b}, \quad C_{l^*} = T \cdot m_c,$$

$C_0^*$ is computable from in the second row of the given instance. Let $r^* = b$, if $T = e(g_0, g_0)^{w \cdot b \cdot f(a)}$, we have

$$P(\mathbb{G}^*) = g^{\frac{sk^* \cdot g(a) \cdot (a + l^*) \cdot b}{\alpha+i+1^*}}, \quad C_0^* = g_0^{sk^* \cdot g(a) \cdot (a + l^*) \cdot b} = g_0^{\frac{sk^* \cdot f(a) \cdot b}{\alpha+i+1^*}}, \quad C_{l^*} = T \cdot m_c = P(\mathbb{G}^*)^b = P(\mathbb{G}^*)^{r^*},$$

Therefore, $CT^*$ is a valid challenge ciphertext.
**Guess:** $A$ outputs its guess $c'$ of $c$.

This completes the description of the reduction. At the end, $B$ outputs 1 as the solution to the $(f, \hat{g}, F)$-GDDHE problem if $c' = c$. Otherwise, it outputs 0.

In the above simulation, there is no abortion caused by that $B$ cannot simulate. If $T = e(g_0, g_0)^{w-b-f(a)}$, we have that the adversary will guess $c$ correctly with probability $\frac{1}{2} + \epsilon$ according to the assumption. Otherwise, we have $C_{T^*}$ is uniformly random and independent of $C_0^*$. The challenge ciphertext is a one-time pad encryption, such that the adversary can only guess a correct $c$ with probability $\frac{1}{2}$. Therefore, the advantage of solving the $(f, \hat{g}, F)$-GDDHE problem is also $\epsilon$, e.g. $\text{Adv}^{\text{gddhe}}(f, \hat{g}, F) = \epsilon$. This yields the **Theorem 3**.

We note that the security of accountability is due to the fact that if $|G| > k$, for example $|G| = k + 1$, the corresponding $\Sigma = h^{a \cdot k - 1} \cdot a^{n-k} \prod_{i \in G} (a + i)$ contains the group element $h^{a \cdot n + 1}$ which is not computable from the system parameter $SP$. The proof is completed in the following theorem.

**Theorem 4 (Accountability).** Our $OT^k_n$ scheme captures the accountability of the sender security if the $(\hat{f}, n)$-DHE assumption holds.

**Proof.** Suppose there exists an adversary $A$ who can break accountability. We can construct an algorithm $B$ that solves the $(\hat{f}, n)$-DHE problem. Let $(g, g^{\frac{1}{\alpha}}, g^{b \cdot \alpha}, \cdots , g^{\frac{1}{\alpha}}, h, h^a, h^a, \cdots , h^n)$ be a random instance of $(\hat{f}, n)$-DHE problem taken as input by $B$ and its goal is to output $(f(x), h^{f(a)})$, where $f(x) \in \mathbb{Z}_p[x]$ is a polynomial function with degree $n' > n$. $B$ interacts with $A$ as the follows.

**Setup:** $B$ implicitly sets $\alpha = a$ for unknown $a$ and generates the system parameter as $SP = \left( \mathbb{B}G, g, g^{\frac{1}{\alpha}}, g^{b \cdot \alpha}, \cdots , g^{\frac{1}{\alpha}}, h, h^a, h^a, \cdots , h^n \right)$.

**Challenge:** $A$ outputs $(P(G^*), G^*, sk^*)$ and $k$ for challenge, where $|G^*| > k$ and $P(G^*) = g^{\prod_{i \in G^*} (a + l_i)}$.

**Output:** $A$ outputs $T^* = (P(G^*), \Sigma^*, k)$ and wins the game if the tuple $(P(G^*), \Sigma^*, k)$ passes the verification algorithm. In this case, we have

$$\Sigma^* = h^{s_{k^*} \cdot a \cdot k - 1} \cdot \prod_{l_i \in G^*} (a + l_i).$$
Let $f(x) = sk^{* - 1} \cdot x^n - k \cdot \prod_{l_i \in G^*} \left(x + l_i\right)$. We have $f(x)$ is a polynomial function in $\mathbb{Z}_p$ with degree larger than $n$. $\mathcal{B}$ outputs $(f(x), \Sigma^*)$ as the solution to the $(\hat{f}, n)$-DHE problem. This completes the description of the simulation and we obtain the **Theorem 4**.

6. **Conclusion**

We proposed an efficient two-round $\text{OT}_n^{k}$ scheme with ideal communication cost. Precisely, the receiver sends only two group elements and one integer to the sender which are independent of the number of secrets held by the sender and the number of receiver’s choice, while the number of messages from $S$ to $R$ is $n + 1$. Compared with the existing $\text{OT}_n^{k}$ schemes in the literature, our scheme achieves the minimum communication cost in both two rounds. We show that our $\text{OT}_n^{k}$ scheme is unconditionally secure for receiver’s choice and preserves the sender security under the specific $(f, \hat{g}, F)$-GDDHE assumption and $(\hat{f}, n)$-DHE assumption.

**References**


