9-2018

Efficient traceable oblivious transfer and its applications

Weiwei LIU

Yinghui ZHANG

Yi MU

Guomin YANG

Yangguang TIAN
Singapore Management University, ygtian@smu.edu.sg

DOI: https://doi.org/10.1007/978-3-319-99807-7_39

Citation

LIU, Weiwei; ZHANG, Yinghui; MU, Yi; YANG, Guomin; and TIAN, Yangguang. Efficient traceable oblivious transfer and its applications. (2018). *Information security practice and experience: 14th International Conference, ISPEC 2018, Tokyo, Japan, September 25 - 27: Proceedings*. 11125, 610-621. Research Collection School Of Information Systems.
Available at: https://ink.library.smu.edu.sg/sis_research/4157

Efficient Traceable Oblivious Transfer and Its Applications

Weiwei Liu[1,4], Yinghui Zhang[2,3](✉), Yi Mu[4], Guomin Yang[4],
and Yangguang Tian[5]

[1] School of Mathematics and Statistics,
North China University of Water Resources and Electric Power, Zhengzhou, China
liuweiwei@ncwu.edu.cn

[2] National Engineering Laboratory for Wireless Security,
Xi'an University of Posts and Telecommunications, Xi'an 710121, China
yhzhaang@163.com

[3] Westone Cryptologic Research Center, Beijing 100070, China

[4] Institute of Cybersecurity and Cryptology,
School of Computing and Information Technology, University of Wollongong,
Wollongong, NSW 2522, Australia
{ymu,gyang}@uow.edu.au

[5] School of Information Systems, Singapore Management University,
Singapore, Singapore
ygtian@smu.edu.sg

Abstract. Oblivious transfer (OT) has been applied widely in privacy-sensitive systems such as on-line transactions and electronic commerce to protect users' private information. Traceability is an interesting feature of such systems that the privacy of the dishonest users could be traced by the service provider or a trusted third party (TTP). However, previous research on OT mainly focused on designing protocols with unconditional receiver's privacy. Thus, traditional OT schemes cannot fulfill the traceability requirements in the aforementioned applications. In this paper, we address this problem by presenting a novel traceable oblivious transfer (TOT) without involvement of any TTP. In the new system, an honest receiver is able to make a fixed number of choices with perfect receiver privacy. If the receiver misbehaves and tries to request more than a pre-fixed number of choices, then all his previous choices could be traced by the sender. We first give the formal definition and security model of TOT, then propose an efficient TOT scheme, which is proven secure under the proposed security model.

Keywords: Oblivious transfer · Secret sharing · Privacy · Traceability

1 Introduction

Oblivious Transfer is one of the fundamental cryptographic primitives that has been used widely in various security applications such as exchange of secrets

[22,25], contract signing [3,12], secure multiparty computation [24] and Internet of Things (IoT) [2]. Roughly speaking, an oblivious transfer scheme is an interactive protocol running between a sender with a set of messages $\{m_1, m_2, \ldots, m_n\}$ and a receiver with a set of choices $\{\sigma_1, \sigma_2, \ldots, \sigma_k\}$. After running the protocol, the receiver learns the intended messages $m_{\sigma_1}, m_{\sigma_2}, \ldots, m_{\sigma_k}$ but cannot learn anything about m_i for $i \notin \{\sigma_1, \sigma_2, \ldots, \sigma_k\}$. Meanwhile, the receiver's choices $\{\sigma_1, \sigma_2, \ldots, \sigma_k\}$ are completely hidden from the sender. The concept of oblivious transfer was first introduced by Rabin in 1981 [22]. In their original construction, the sender sends a single bit 0 or 1 to the receiver in such a way that with 1/2 probability the receiver will receive the same bit and with 1/2 probability that the receiver will receive nothing. At the same time, the sender has no idea whether the receiver receives the message or not. Since then, oblivious transfer has attracted a lot of attentions, and a number of work [5,8,10,12,20] have been done to improve the original OT scheme in different aspects.

Even et al. [12] proposed a 1-out-of-2 OT (OT_2^1) scheme, in which the sender obliviously sends a message m_i, $i \in \{0, 1\}$, to the receiver. Shortly after that, Brassard et al. [5] extended the OT_2^1 [12] to a more general k-out-of-n (OT_n^k) setting, where the receiver is able to make multiple choices $m_{\sigma_1}, m_{\sigma_2}, \ldots, m_{\sigma_k}$ ($\sigma_i \in \{1, 2, \ldots, n\}$, $1 \le i \le k$) from a set of n messages $\{m_1, m_2, \ldots, m_n\}$ held by the sender, meanwhile the receiver's choices remain oblivious to the sender. Since then, many subsequent work [10,19] aimed to design more efficient OT_n^k schemes. Different from normal OT_n^k, another important research direction on OT is adaptive OT_n^k [20]. In adaptive OT_n^k, the receiver can choose the messages adaptively, namely, the ith value chosen by the receiver depends on the first $i-1$ values.

In the early OT schemes reviewed above, there is no condition on restricting the receiver's ability. Any user in the system can act as a receiver and run the OT protocol to choose messages held by the sender obliviously. To address this problem, Coull et al. [11] proposed an OT scheme supporting access control using state graphs, where for every transaction, the state of the receiver shifts from one to another. The receiver can access the protected services only if some of his states are not used. Camenisch et al. [6] proposed another approach to enforce access control. In their system, the receiver first authenticates himself to a trusted third party to obtain some credentials. Later, the receiver proves to the sender that he possesses a valid credential from the third party using zero-knowledge proof. However, in this construction, the access policy is publicly known.

To address this problem, Camenisch et al. [7] proposed another oblivious transfer with access control (AC-OT) in which only the receivers whose attributes satisfy a predicate can access the services. In order to reduce the computation and communication cost, Han et al. [14] proposed two efficient oblivious transfer schemes without using zero-knowledge proof. In addition, different form previous schemes, the receivers could obtain credentials from a trusted third party but do not have to authenticate themselves. Thus, the communication and computation cost is lower than previous schemes supporting access control.

Later on, Han et al. [13] proposed accountable oblivious transfer with access control, such that authorized users are allowed to access sensitive records with accountable times. They claim that it is the first AC-OT scheme where both the timely revocation and the prevention of overusing records are addressed simultaneously. In particular, if a dishonest user misuse the given credential, then his public identity will be revealed due to the k-time anonymous authentication technique [23] is used.

There have been a lot of research works [8,15,21] on defining OT security, which can be classified into honest-but-curious model, half-simulation model [21], full-simulation model [6–8] and Universally Composable (UC) model [13,15], according to whether the OT scheme can provide simulatable security for the sender and/or receiver. In the honest-but-curious model, all participants in the protocol are assumed to be honest, which makes this model too idealistic for practical use. Naor and Pinkas [21] introduced the half-simulation model that allows malicious senders and receivers. However, in this model, the security of the sender and receiver are considered separately. Half-simulation model achieves simulatable security for sender privacy and computationally indistinguishability for receiver privacy.

In order to capture the selective-failure attacks that may be performed by the cheating sender, the full simulatability is introduced. In the full-simulation model [8,15], it achieves simulatable security for both the receiver and sender together. As for the UC-related model, the security of sender and receiver is defined by the indistinguishability between a real world and an ideal world as described in the UC framework [9]. We then compare our proposed TOT with typical works in Table 1 to highlight our distinction: it shows that our proposed TOT enjoys traceability[1] to the receiver's choice if the user misbehaves, and secures in the half simulation model under dynamic assumptions. In Table 1, adaptive means that the receiver chooses the k records one after the other. † denotes the various security models, which includes the honest but curious model, the half/full simulation model and the UC model. Dynamic means that the assumptions are depending on the number of n, such as strong Diffie-Hellman assumptions [4].

1.1 Our Motivation

All the previous research on OT aimed to design OT schemes with perfect receiver and sender privacy. In real-world applications [1,16], it is desirable for the sender to trace the choices of the receiver if they misbehave. Thus, the previous OT schemes are not suitable in these scenarios. To the best of our knowledge, there is only one work [18] aiming to construct OT schemes with traceable receiver's privacy. However, this OT scheme involves a trusted time

[1] Note that the traceability means that the previously *choices* of the cheating receiver are revealed, which is the major distinction between our proposed TOT and the construction in [13]. In the table, we use the symbol traceability* to distinguish our work with that one in [13].

Table 1. A comparative summary for OT protocols.

Function/algorithm	NP [21]	CT [10]	CGS [8]	KN [15]	HSM* [13]	Ours
Adaptive	✓	✓	✓	✓	✓	✓
†-simulation	Half	Half	Full	UC	UC	Half
Standard model	✓	×	✓	✓	✓	×
Dynamic assumptions	×	×	✓	×	✓	✓
Access control	×	×	×	×	✓	✓
Traceability	×	×	×	×	✓	×
Traceability*	×	×	×	×	×	✓

server that publishes trapdoors on a time basis. After releasing the trapdoor, the privacy of all the receivers, including the honest ones, will be lost. The motivation of this work is to propose a new OT with traceable receiver's privacy such that the privacy of an honest receiver is protected unconditionally while all the previous *choices* of a misbehaving receiver can be revealed by the sender if the receiver makes more than the pre-determined number of choices in the OT protocol. It is worth noting that in some real-life applications, the service provider (i.e., database provider) may not only need to detect the identity of dishonest users, but also want to reveal their choices that was made previously in the system. By doing so, the service provider may revoke the operations on the corresponding sensitive data which was anonymously and obliviously made by that cheating user.

Our Contribution. In this paper, we present a novel traceable oblivious transfer that allows a sender to trace the dishonest receivers' choices without the help of any trusted third party. Our contributions can be summarized as follows:

- We present the *first* traceable adaptive OT_n^k scheme and analysed its security under the half-simulation model [21];
- The *traceable* OT_n^k scheme allows the receiver to obtain a fixed number of messages $m_{\sigma_1}, m_{\sigma_2}, \ldots, m_{\sigma_k}$ from the message set $\{m_1, m_2, \ldots, m_n\}$ held by the sender where $\sigma_i \in \{1, 2, \ldots, n\}$ for $1 \leq i \leq k$, while receiver's choice is hidden from the sender;
- The *traceable* OT_n^k scheme allows the receiver cannot learn anything on message m_i such that $i \notin \{\sigma_1, \sigma_2, \ldots, \sigma_k\}$ for $1 \leq i \leq n$. In particular, if the receiver makes more than k requests, then all his previous *choices* $(m_{\sigma_1}, m_{\sigma_2}, \ldots, m_{\sigma_k})$ could be traced by the sender.

Paper Organization. The rest of the paper is organized as follows. We introduce the formal definition and the security model of TOT in Sect. 2. Some preliminaries are presented in Sect. 3 and a concrete scheme TOT scheme is presented in Sect. 4. We prove its security in Sect. 5 and the paper is concluded in Sect. 6.

2 Formal Definition and Security Model

We present the formal definition and security model for TOT in this section. There are two participants in a TOT system, namely, a sender S and a receiver R. S possesses a set of messages $\{m_1, m_2, \ldots, m_n\}$ and R makes a set of choices $\{\sigma_1, \sigma_2, \ldots, \sigma_k\}$ such that $\sigma_i \in \{1, 2, \ldots, n\}$ for $1 \leq i \leq k$.

2.1 Definitions of Traceable Oblivious Transfer

A TOT scheme is essentially an interactive protocol consisting of a tuple of PPT algorithms (*Setup*, *Commitment*, *Request*, *Response*, *Extract*, *Tracing*).

1. *Setup*: Taking as input of a security parameter κ, the setup algorithm outputs the system public parameters.

$$params \leftarrow Setup(1^\kappa)$$

2. *KeyGen*: Taking as input of the public parameter $params$, the key generation algorithm outputs a retrievable key pair[2] (rpk, rsk) for the receiver and a one-time key pair for the sender.

$$(rpk, rsk) \leftarrow KeyGen(params)$$
$$(opk, osk) \leftarrow KeyGen(params)$$

3. *Commitment*: Taking as input of the system parameters $params$, the retrievable public key rpk of the receiver, the messages $m_1, m_2, \ldots, m_n$ and one-time secret key osk of the sender, the commitment algorithm outputs a set of ciphertext $c_1, c_2, \ldots, c_n$.

$$c_1, c_2, \ldots, c_n \leftarrow Commitment(rpk, m_1, m_2, \ldots, m_n, osk, params)$$

4. *Request*: Taking as input of the intended indexes σ, the retrievable private key rsk and $params$, this algorithms outputs the commitment of the user's choice.

$$A_\sigma \leftarrow Request(\sigma; rsk; params)$$

5. *Response*: Taking as input of the commitment A_σ from the receiver, the secret of the sender, the output of the algorithm is response of the sender.

$$D_\sigma \leftarrow Response(A_\sigma, osk, params)$$

6. *Extract*: Taking as input of the response D_σ from the sender, the cipertext c_α and the system parameters $params$, output the message of the receiver's choice.

$$m_\sigma \leftarrow Extract(D_\sigma, c_\sigma, params)$$

[2] We assume there exists a public key infrastructure (PKI) issuing certificates on the users' public keys in our system.

7. *Tracing*: The *Tracing* algorithm is performed by the sender, taking as input of the $k+1$ transcripts $A_{\sigma_1}, A_{\sigma_2}, \ldots, A_{\sigma_{k+1}}$ from a receiver, the retrievable public key rpk and $params$, outputs the receiver's choice $\sigma_1, \sigma_2, \ldots, \sigma_k$.

$$\sigma_1, \sigma_2, \ldots, \sigma_k \leftarrow \mathit{Tracing}(A_{\sigma_1}, A_{\sigma_2}, \ldots, A_{\sigma_{k+1}}; rpk; params)$$

Correctness: We require that for any security parameter $\kappa \in \mathbb{N}$, if $params \leftarrow ParamGen(1^\kappa)$, $(rpk, rsk) \leftarrow KeyGen(params)$, $(opk, osk) \leftarrow KeyGen(params)$, $c_1, c_2, \ldots, c_n \leftarrow Commitment(rpk, m_1, m_2, \ldots, m_n, osk, params)$, $A_\sigma \leftarrow Request$ $(\sigma; rsk, params)$, $D_\sigma \leftarrow Response(A_\sigma, osk; parmas)$, then

- The receiver can extract the correct message.

$$\Pr(m_\sigma \leftarrow \mathit{Extract}(D_\sigma, rsk, params)) = 1.$$

- If the receiver makes less than $k+1$ requests, then the sender cannot obtain any information about the receiver's choice.

$$\Pr(`\perp' \leftarrow \mathit{Tracing}(A_{\sigma_1}, A_{\sigma_2}, \ldots, A_{\sigma_\delta}; rpk; params | \delta \leq k)) = 1.$$

- If the receiver makes more than k requests, then the sender can trace the previous choice of the receiver.

$$\Pr(\sigma_1, \sigma_2, \ldots, \sigma_\delta \leftarrow \mathit{Tracing}(A_{\sigma_1}, A_{\sigma_2}, \ldots, A_{\sigma_\delta}; rpk; params | \delta > k)) = 1.$$

2.2 Security Model for Traceable Oblivious Transfer

In this paper, we review the half-simulation model proposed in [21] to evaluate the security of TOT schemes. Besides the sender and receiver's privacy, we define a new property named traceability to capture the additional feature of TOT. In the half-simulation model, the security of the sender and receiver is considered separately. A secure TOT scheme should meet the following security requirements:

1. *Receiver's Privacy*:
   - If R makes less than $k+1$ requests, then S cannot obtain any information about R's choice.
   - For any two different choice sets $\mathcal{C} = \{\sigma_1, \sigma_2, \ldots, \sigma_k\}$ and $\mathcal{C}' = \{\sigma'_1, \sigma'_2, \ldots, \sigma'_k\}$, the transcripts $\mathcal{A} = \{A_{\sigma_1}, A_{\sigma_2}, \ldots, A_{\sigma_k}\}$ and $\mathcal{A}' = \{A'_{\sigma_1}, A'_{\sigma_2}, \ldots, A'_{\sigma_k}\}$ received by S corresponding to $\mathcal{M} = \{m_{\sigma_1}, m_{\sigma_2}, \ldots, m_{\sigma_k}\}$ and $\mathcal{M}' = \{m'_{\sigma_1}, m'_{\sigma_2}, \ldots, m'_{\sigma_k}\}$ are indistinguishable if the received messages $\mathcal{M} = \{m_{\sigma_1}, m_{\sigma_2}, \ldots, m_{\sigma_k}\}$ and $\mathcal{M}' = \{m'_{\sigma_1}, m'_{\sigma_2}, \ldots, m'_{\sigma_k}\}$ are identically distributed.
2. *Sender's Privacy*:
   - R cannot obtain any information on m_i, $i \notin \{\sigma_1, \sigma_2, \ldots, \sigma_k\}$ for $1 \leq i \leq n$.
   - In the half-simulation model, the security of R is defined by the real-world/ideal-world paradigm. In the real world, R and S execute the

protocol. In the ideal world, the protocol is implemented with the help a trusted third party (TTP). S sends all the messages $m_1, m_2, \ldots, m_n$ to the TTP. While R sends his choices $\{\sigma_1, \sigma_2, \ldots, \sigma_k\}$ adaptively to the TTP. If $\{\sigma_1, \sigma_2, \ldots, \sigma_k\} \in \{1, 2, \ldots, n\}$ the TTP sends messages $\{m_{\sigma_1}, m_{\sigma_2}, \ldots, m_{\sigma_k}\}$ to the receiver. A TOT scheme is said to provide the privacy of the sender if for any receiver R in real world, there exists an probabilistic polynomial-time (PPT) R' in the ideal world such that the output of R and R' are indistinguishable.

3. *Traceability*:
   Traceability is not a necessary requirement for traditional OT schemes, we consider traceability as a special property of our TOT schemes. If a dishonest receiver R makes $k+1$ choices $\{\sigma_1, \sigma_2, \ldots, \sigma_k, \sigma_{k+1}\}$ from S, suppose $\mathcal{A} = \{A_{\sigma_1}, A_{\sigma_2}, \ldots, A_{\sigma_k}, A_{\sigma_{k+1}}\}$ is the transcript set of the $k+1$ choices, then S is able to trace R's choices through an efficient PPT algorithm *Tracing*.

3 Preliminaries

In this section, we introduce some preliminaries that will be used throughout this paper.

Definition 1. ***Decisional Diffie-Hellman (DDH) Assumption:*** *Given a cyclic group G_q of prime order q, the DDH problem states that, given $g, g^a, g^b, Z \in G_q$ for some random $a, b \in \mathbb{Z}_q$ and a random generator g, decide $Z = g^{ab}$. Define the success probability of a polynomial algorithm $\mathcal{A}$ in solving the DDH problem as:*

$$Succ^{DDH}_{\mathcal{A},\mathbb{G}_q}(\kappa) = |\Pr[\mathcal{A}(G_q, g, g^a, g^b, g^{ab}) = 1] - \Pr[\mathcal{A}(G_q, g, g^a, g^b, Z) = 1]|$$

where $\kappa = \mathsf{log}(q)$ is the security parameter. The DDH assumption states that for any probabilistic polynomial algorithm time $\mathcal{A}$, $Succ^{DDH}_{\mathcal{A},\mathbb{G}_q}(\kappa)$ is negligible in κ.

Definition 2. ***One More Diffie-Hellman (OMDH) Assumption*** [21]***:*** *Given a cyclic group G_q of prime order q and g is a generator of G, let $DH(\cdot)$ be the Diffie-Hellman oracle that takes $X = g^x, Y = g^y \in G_q$ for some $x, y \in \mathbb{Z}_q$ and returns the Diffie-Hellman value $Z = g^{xy}$. Let $C(\cdot)$ be a challenge oracle that takes no input and returns a random element in G_q. Let $Y_1, Y_2, \ldots, Y_t$ denote the challenges returned by $C(\cdot)$, we say an OMDH adversary $\mathcal{A}$ wins if $\mathcal{A}$ can output the sequence of Diffie-Hellman values $Z_1, Z_2, \ldots, Z_t$ of all DHP instances with input X, Y_i, $i = 1, 2, \ldots, t$ and the number of queries q_{dh} made by $\mathcal{A}$ to the Diffie-Hellman oracle $DH(\cdot)$ is less than t. Define the success probability of a polynomial algorithm $\mathcal{A}$ in solving the OMDH problem as:*

$$Succ^{OMDH}_{\mathcal{A},G_q}(\kappa) = \Pr[Z_1, Z_2, \ldots, Z_t \leftarrow \mathcal{A}_{DH(\cdot), q_{dh} < t}(X, (Y_1, Y_2, \ldots, Y_t \leftarrow C(\cdot)))]$$

the OMDH assumption states that, for any polynomial algorithm $\mathcal{A}$, $Succ^{OMDH}_{\mathcal{A},G_q}(\kappa)$ is negligible in κ.

4 One Construction of Efficient Traceable Oblivious Transfer Schemes

The proposed scheme consists of a tuple of PPT algorithms as follows.

1. **Setup:** Let G_q denote a subgroup of $\mathbb{Z}_p$ with prime order q and $g, h_1, h_2, \ldots,$ h_n be generators of G_q, where $p = 2q + 1$ is also prime. Choose two collision resistant hash functions H, H_1 such that $H : \mathbb{N} \rightarrow Z_q^*$ and $H_1 : G_q \rightarrow G_q$. The system parameters $params = (G_q, p, q, g, h_1, h_2, \ldots, h_n, H, H_1)$.
2. **KeyGen:** The receiver R chooses a random number $s \in \mathbb{Z}_q^*$ and generates a retrievable key pair $(rpk, rsk) = (g^s, s)$. R chooses k random numbers $s_1, s_2, \ldots, s_k \in_R \mathbb{Z}_q$ and computes $S_1 = g^{s_1}, S_2 = g^{s_2}, \ldots, S_k = g^{s_k}$. S chooses a random number $z \in_R \mathbb{Z}_q^*$ and generates a one-time key pair $(opk, osk) = (g^z, z)$. R publishes rpk and $S_1, S_2, \ldots, S_k$ and S publishes opk.
3. **Commitment Phase:** S computes the ciphertext of $m_1, m_2, \ldots, m_n$ as $c_i = H_1((rpk \cdot h_i^{H(i)})^z) \cdot m_i$, $1 \leq i \leq n$, S sends $c_1, c_2, \ldots, c_n$ to R.
4. **Request:** In the i-th round,
   - R chooses $r_i \in_R \mathbb{Z}_q^*$, and computes $B_i = g^{r_i}, B_i' = h_{\alpha_i}^{r_i}$ and $A_i = (g^{r_i})^s (h_{\alpha_i}^{r_i})^{H(\alpha_i)}$, where $\alpha_i \in_R \{1, 2, \ldots, n\}$ is the receiver's choice and $f(B_i) = s + s_1 B_i + \ldots s_k B_i^k$.
   - R sends $(B_i, B_i', f(B_i), A_i)$ to S, and simultaneously does the following proof of knowledge. $PoK\{(H(\alpha_i), s) : A = B_i^s {B_i'}^{H(\alpha_i)} \wedge rpk = g^s\}$.
5. **Response:** S first verifies B_i, the secret share $f(B_i)$ and the PoK by checking:
   - S checks whether B_i appears in previous session.
   - $g^{f(B_i)} \overset{?}{=} rpk \cdot S_1^{B_i} \cdot S_2^{B_i^2} \cdot \ldots \cdot S_k^{B_i^k}$. If this equation holds,
   - S verifies $PoK\{(H(\alpha_i), s) : A_i = B_i^s {B_i'}^{H(\alpha_i)} \wedge rpk = g^s\}$.

   If either of the verification fails, S aborts; Otherwise, S stores $(B_i, B_i', f(B_i),$ $A_i)$ and S generates $D_i = A_i^z$ and sends D_i to R.
6. **Extract:** Upon receiving D_i from S, R computes $K_{\alpha_i} = D_i^{\frac{1}{r_i}}$ and extracts the intended message $m_{\alpha_i} = c_{\alpha_i} / H_1(K_{\alpha_i})$.
7. **Tracing:** Once R and S execute the OT for $k+1$ times, S obtains $k+1$ shares of the secret. S is able to recover s from secret sharing. Once s is calculated, for the previous commitments $A_i = B_i^s {B_i'}^{H(\alpha_i)}$, given B_i, B_i' for $1 \leq i \leq k$. S is able to retrieve α_i for $1 \leq i \leq k$.

The proof of knowledge $PoK\{(H(\alpha_i), s) : A_i = B_i^s {B_i'}^{H(\alpha_i)} \wedge rpk = g^s\}$ can be implemented as follows:

1. R randomly chooses two random numbers $t_1, t_2 \in \mathbb{Z}_p$, computes $T_1 = B_i^{t_1} {B_i'}^{t_2}, T_2 = g^{t_1}$, $c = H(f(B_i), B_i, B_i', T_1, T_2)$, $v_1 = t_1 - cs$ and $v_2 = t_2 - cH(\alpha_i)$. R sends v_1, v_2, T_1, T_2 to S.
2. S accepts if both $A_i^c B_i^{v_1} {B_i'}^{v_2} = T_1$ and $rpk^c g^{v_1} = T_2$ hold.

5 Security Analysis

Theorem 1. *The proposed TOT scheme is correct.*

Proof. The correctness of the proposed scheme is shown as follows:

1. **Correctness of PoK:** If R is honest, then R has knowledge of $H(\alpha_i)$ and s, R computes $v_1 = t_1 - cs$ and $v_2 = t_2 - cH(\alpha_i)$. S can verify correctly that:

$$\begin{aligned} &A^c B_i^{v_1} B_i'^{v_2} = B_i^{sc} B_i'^{H(\alpha_i)c} B_i^{t_1 - cs} B_i'^{t_2 - cH(\alpha_i)} = B_i^{t_1} B_i'^{t_2} = T_1. \\ &rpk^c g^{v_1} = g^{sc} g^{t_1 - cs} = g^{t_1} = T_2. \end{aligned}$$

2. **Correctness of extracting the message:**

$$m_{\alpha_i} = \frac{c_{\alpha_i}}{H_1(K_{\alpha_i})} = \frac{m_{\alpha_i} H_1(rpk \cdot h_{\alpha_i}^{H(\alpha_i)})^z)}{H_1((g^{r_i sz} h_{\alpha_i}^{r_i H(\alpha_i) z})^{\frac{1}{r_i}})} = \frac{m_{\alpha_i} H_1(g^{sz} h_{\alpha_i}^{H(\alpha_i) z})}{H_1(g^{sz} h_{\alpha_i}^{H(\alpha_i) z})} = m_{\alpha_i}$$

Theorem 2. *The proposed TOT scheme provides receiver's privacy for honest receivers.*

Proof. We followed the methods described in [17] to analyse the security of the proposed TOT scheme. Suppose a honest receiver runs the OT protocol with the sender for k times. The sender could obtain k pairs of transcripts $\{(A_1, B_1, B_1'), (A_2, B_2, B_2'), \ldots, (A_k, B_k, B_k')\}$ such that $A_1 = (g^{r_1})^s (h_{\alpha_1}^{r_1})^{H(\alpha_1)}$, $A_2 = (g^{r_2})^s (h_{\alpha_2}^{r_2})^{H(\alpha_2)}, \ldots, A_k = (g^{r_k})^s (h_{\alpha_k}^{r_k})^{H(\alpha_k)}$, where $\alpha_1, \alpha_2, \ldots, \alpha_k \in \{1, 2, \ldots, n\}$ are the user's choice and $r_1, r_2, \ldots, r_k \in_R \mathbb{Z}_q^*$. Given $B_j = g^{r_j}, rpk = g^s$ for some random $r_j \in \mathbb{Z}_q^*$, it is computation-infeasible to decide the masked value equals $g^{r_j s}$ or a random value Z in G_q, thus for any two transcripts A_j and A_i such that $1 \leq i \neq j \leq k$ from the user, they are computationally indistinguishable to the service provider as long as the DDH problem is hard in G_q.

Theorem 3. *The proposed TOT scheme provides sender's privacy.*

Proof. Suppose a honest receiver runs the OT protocol with the sender k times. For any probabilistic polynomial-time malicious receiver $\hat{R}$ in the real-world model, we are able to construct a probabilistic polynomial-time malicious receiver $\hat{R}^*$ in the ideal model such that the outputs of $\hat{R}$ and $\hat{R}^*$ are indistinguishable.

Briefly, the ideal-world cheating receiver $\hat{R}^*$ can extract α from the proof of knowledge. This enables him to obtain the message m_α form the TTP. $\hat{R}^*$ simulates the honest sender S in the real-world and interacts with $\hat{R}$ as follows:

1. S sends $m_1, m_2, \ldots, m_n$ to the trusted third party TTP.
2. $\hat{R}^*$ sends $c_1^*, c_2^*, \ldots, c_n^*$ to TTP such that $c_i^* \in_R G_q$ for $i = 1, 2, \ldots, n$.
3. $\hat{R}^*$ monitors the outputs $A_{\alpha_1}, A_{\alpha_2}, \ldots, A_{\alpha_k}$ of $\hat{R}$, $\hat{R}^*$ chooses $A_{\alpha_1}^*, A_{\alpha_2}^*, \ldots, A_{\alpha_k}^* \in_R G_q$.

4. After $\hat{R}$ runs *Request* protocol, if the verification of PoK fails, $\hat{R}^*$ sends a value $\alpha_i \notin \{1, 2, \ldots, n\}$ to TTP.
5. If the verification of PoK successes, $\hat{R}^*$ extracts $\hat{R}$'s choice α_i from the PoK and gets back $D^*_{\sigma_1}, D^*_{\sigma_2}, \ldots, D^*_{\sigma_k}$ such that $D^*_{\sigma_i} = A^{z^*}_{\alpha_i}$ for $i = 1, 2, \ldots, k$.
6. If $\hat{R}$ can compute $K_{\alpha_i} = g^{sz} h_{\alpha_i}^{H(\alpha_i)z}$, $\hat{R}^*$ sends α_i to TTP, TTP returns $\frac{c^*_{\alpha_i}}{m_{\alpha_i}}$.
7. $\hat{R}^*$ outputs $(A^*_{\alpha_1}, A^*_{\alpha_2}, \ldots, A^*_{\alpha_k}, D^*_{\sigma_1}, D^*_{\sigma_2}, \ldots, D^*_{\sigma_k}, c^*_1, c^*_2, \ldots, c^*_n)$.

We can see from Theorem 2 and Claim (see proof below) that $\{A_{\alpha_1}, A_{\alpha_2}, \ldots, A_{\alpha_k}\}$ and $\{c_1, c_2, \ldots, c_n\}$ are indistinguishable from random elements in G_q. In addition, the sets of $\{D_{\sigma_1}, D_{\sigma_2}, \ldots, D_{\sigma_k}\}$ and $\{D^*_{\sigma_1}, D^*_{\sigma_2}, \ldots, D^*_{\sigma_k}\}$ are identically distributed. Therefore, no distinguishers can distinguish the outputs of $\hat{R}$ and $\hat{R}'$ with a non-negligible probability.

Claim. The proposed encryption scheme is semantic secure.

Proof. The security proof is performed using random oracle. Suppose the simulator $\mathcal{B}$ maintains a table T_1 for the hash queries. $\mathcal{B}$ obtains $n + 1$ values $Z, Y_1, Y_2, \ldots, Y_n$ from the challenge oracle $C(\cdot)$. $\mathcal{B}$ sets the one-time public key of the sender $opk = Z$ and sends $Z, Y_1, Y_2, \ldots, Y_n$ to a PPT adversary $\mathcal{A}$. Assume $\mathcal{A}$ queries on a message m_i for $1 \leq i \leq n-1$. $\mathcal{B}$ first obtain the diffie-hellman value of (Z, Y_i) with help of $DH(\cdot)$ oracle. Then $\mathcal{A}$ checks if $DH(Z, Y_i)$ has existed in T_1. If not, $\mathcal{B}$ chooses a new random $Z_i \in G_q$ and stores $(DH(Z, Y_i), Z_i)$ to T_1. Otherwise, assume $H_1(DH(Z, Y_i)) = Z_i$, $\mathcal{B}$ returns $c_i = Z_i \cdot m_i$ as the ciphertext on m_i. After $n - 1$ queries, $\mathcal{A}$ sends two challenge messages m^*_0, m^*_1, $\mathcal{B}$ chooses $b \in \{0, 1\}$ and a random number $Z_n \in G_q$. $\mathcal{A}$ sets the ciphertext c^*_b on m^*_b as $c^*_b = Z_n \cdot m^*_b$. If $\mathcal{A}$ has a non-negligible probability ϵ in distinguishing c^*_b than random guess. Then with an overwhelming probability that $DH(Z, Y_n)$ has been submitted in the hash queries. Thus $\mathcal{B}$ breaks the OMDH assumption, we reach a contradiction. Therefore the proposed encryption scheme is semantic secure.

Theorem 4. *The proposed TOT scheme provides traceability to the receiver.*

Proof. After running the protocol $k + 1$ times with the receiver, the sender obtains $k+1$ shares of the retrievable private key s with respect to the unknown integers $s_1, s_2, \ldots, s_k$ such that

$$f(B_i) = s + s_1 B_i + s_2 B_i^2 \ldots + s_k B_i^k, 1 \leq i \leq k + 1.$$

The corresponding linear equations in a matrix form are as follows:

$$\begin{pmatrix} 1 & B_1 & B_1^2 & \cdots & B_1^k \\ 1 & B_2 & B_2^2 & \cdots & B_2^k \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & B_{k+1} & B_{k+1}^2 & \cdots & B_{k+1}^k \end{pmatrix} * \begin{pmatrix} s \\ s_1 \\ \vdots \\ s_k \end{pmatrix} = \begin{pmatrix} f(B_1) \\ f(B_2) \\ \vdots \\ f(B_{k+1}) \end{pmatrix}$$

As we can see the coefficient matrix is a Vandermonde matrix or a non-singular matrix. The determinant of such a matrix is not equal to zero. Thus the equations have a unique solution to $s, s_1, s_2, \ldots, s_k$.

Once the sender obtains the value of the retrievable private key rsk. For previous commitments on receiver's choice $A_i = B_i^{rsk} {B'_i}^{H(\alpha_i)}$ for $1 \leq i \leq k$. Since S has store the values of B_i and B'_i in the i-th round. Thus, the sender could trace the receiver choice $\alpha_i = j$ in the i-th round by checking that $A_i = B_i^{rsk} {B'_i}^{H(\alpha_i)} = B_i^{rsk} {B'_i}^{H(j)}$ for $1 \leq j \leq n$.

6 Conclusion

In this paper, we proposed a novel oblivious transfer scheme that can achieve retrievable receiver's privacy without the help of a trusted third party. The misbehaving receivers' choices could be traced while the honest receivers' privacy is well protected. We proved the security of the scheme under the proposed security model. We leave the construction of an adaptive traceable OT scheme that is proven secure under non-dynamic assumptions in the full-simulation model or UC model as our future work.

Acknowledgements. This work is supported by the National Key R&D Program of China (2017YFB0802000), the National Natural Science Foundation of China (Nos. 61772418, 61402366). Yinghui Zhang is supported by New Star Team of Xi'an University of Posts & Telecommunications (2016-02).

References

1. Aiello, B., Ishai, Y., Reingold, O.: Priced oblivious transfer: how to sell digital goods. In: Pfitzmann, B. (ed.) EUROCRYPT 2001. LNCS, vol. 2045, pp. 119–135. Springer, Heidelberg (2001). https://doi.org/10.1007/3-540-44987-6_8
2. Ashton, K.: That internet of things? Thing (1999)
3. Ben-Or, M., Goldreich, O., Micali, S., Rivest, R.L.: A fair protocol for signing contracts. IEEE Trans. Inf. Theory **36**(1), 40–46 (1990)
4. Boneh, D., Boyen, X.: Short signatures without random oracles. In: Cachin, C., Camenisch, J.L. (eds.) EUROCRYPT 2004. LNCS, vol. 3027, pp. 56–73. Springer, Heidelberg (2004). https://doi.org/10.1007/978-3-540-24676-3_4
5. Brassard, G., Crépeau, C., Robert, J.-M.: All-or-nothing disclosure of secrets. In: Odlyzko, A.M. (ed.) CRYPTO 1986. LNCS, vol. 263, pp. 234–238. Springer, Heidelberg (1987). https://doi.org/10.1007/3-540-47721-7_17
6. Camenisch, J., Dubovitskaya, M., Neven, G.: Oblivious transfer with access control. In: Proceedings of the 2009 ACM Conference on Computer and Communications Security, CCS 2009, Chicago, Illinois, USA, 9–13 November 2009, pp. 131–140 (2009)
7. Camenisch, J., Dubovitskaya, M., Neven, G., Zaverucha, G.M.: Oblivious transfer with hidden access control policies. In: Catalano, D., Fazio, N., Gennaro, R., Nicolosi, A. (eds.) PKC 2011. LNCS, vol. 6571, pp. 192–209. Springer, Heidelberg (2011). https://doi.org/10.1007/978-3-642-19379-8_12
8. Camenisch, J., Neven, G., Shelat, A.: Simulatable adaptive oblivious transfer. In: Naor, M. (ed.) EUROCRYPT 2007. LNCS, vol. 4515, pp. 573–590. Springer, Heidelberg (2007). https://doi.org/10.1007/978-3-540-72540-4_33

9. Canetti, R.: Universally composable security: a new paradigm for cryptographic protocols. In: IEEE Symposium on Foundations of Computer Science, p. 136 (2001)
10. Chu, C.-K., Tzeng, W.-G.: Efficient k-out-of-n oblivious transfer schemes with adaptive and non-adaptive queries. In: Vaudenay, S. (ed.) PKC 2005. LNCS, vol. 3386, pp. 172–183. Springer, Heidelberg (2005). https://doi.org/10.1007/978-3-540-30580-4_12
11. Coull, S., Green, M., Hohenberger, S.: Controlling access to an oblivious database using stateful anonymous credentials. In: Jarecki, S., Tsudik, G. (eds.) PKC 2009. LNCS, vol. 5443, pp. 501–520. Springer, Heidelberg (2009). https://doi.org/10.1007/978-3-642-00468-1_28
12. Even, S., Goldreich, O., Lempel, A.: A randomized protocol for signing contracts. Commun. ACM **28**(6), 637–647 (1985)
13. Han, J., Susilo, W., Mu, Y., Au, M.H., Cao, J.: AAC-OT: accountable oblivious transfer with access control. IEEE Trans. Inf. Forensics Secur. **10**(12), 2502–2514 (2015)
14. Han, J., Susilo, W., Mu, Y., Yan, J.: Efficient oblivious transfers with access control. Comput. Math. Appl. **63**(4), 827–837 (2012)
15. Kurosawa, K., Nojima, R.: Simple adaptive oblivious transfer without random oracle. In: Matsui, M. (ed.) ASIACRYPT 2009. LNCS, vol. 5912, pp. 334–346. Springer, Heidelberg (2009). https://doi.org/10.1007/978-3-642-10366-7_20
16. Liu, W., Mu, Y., Yang, G.: An efficient privacy-preserving e-coupon system. In: Lin, D., Yung, M., Zhou, J. (eds.) Inscrypt 2014. LNCS, vol. 8957, pp. 3–15. Springer, Cham (2015). https://doi.org/10.1007/978-3-319-16745-9_1
17. Liu, W., Mu, Y., Yang, G., Yu, Y.: Efficient e-coupon systems with strong user privacy. Telecommun. Syst. **64**(4), 695–708 (2017)
18. Ma, X., Xu, L., Zhang, F.: Oblivious transfer with timed-release receiver's privacy. J. Syst. Softw. **84**(3), 460–464 (2011)
19. Mu, Y., Zhang, J., Varadharajan, V.: m out of n oblivious transfer. In: Batten, L., Seberry, J. (eds.) ACISP 2002. LNCS, vol. 2384, pp. 395–405. Springer, Heidelberg (2002). https://doi.org/10.1007/3-540-45450-0_30
20. Naor, M., Pinkas, B.: Oblivious transfer with adaptive queries. In: Wiener, M. (ed.) CRYPTO 1999. LNCS, vol. 1666, pp. 573–590. Springer, Heidelberg (1999). https://doi.org/10.1007/3-540-48405-1_36
21. Naor, M., Pinkas, B.: Computationally secure oblivious transfer. J. Cryptol. **18**(1), 1–35 (2005)
22. Rabin, M.O.: How to exchange secrets by oblivious transfer (1981)
23. Teranishi, I., Furukawa, J., Sako, K.: k-times anonymous authentication. IEICE Trans. **92-A**(1), 147–165 (2009)
24. Yao, A.C.: Protocols for secure computations (extended abstract). In: 23rd Annual Symposium on Foundations of Computer Science, Chicago, Illinois, USA, 3–5 November 1982, pp. 160–164 (1982)
25. Yao, A.C.: How to generate and exchange secrets (extended abstract). In: 27th Annual Symposium on Foundations of Computer Science, Toronto, Canada, 27–29 October 1986, pp. 162–167 (1986)