Improvement of Camenisch-Neven-Shelat Oblivious Transfer Scheme

Zhengjun Cao and Hanyue Cao
(Corresponding author: Zhengjun Cao)

Department of Mathematics, Shanghai University
No.99, Shangda Road, Shanghai, China.
(Email: caozhj@shu.edu.cn)
(Received Aug. 15, 2013; revised and accepted Nov. 7, 2014)

Abstract

In 2007, Camenisch, Neven and Shelat proposed an adaptive oblivious transfer (OT) scheme in which a sender has n messages, of which a receiver can adaptively choose to receive k one-after-the-other. In this paper, we show that the scheme has a drawback that the sender can serve a single receiver only once. The drawback results from the deterministic encryption used. To fix it, we suggest to replace the deterministic encryption with a probabilistic encryption. The OT scheme adopts the paradigm of "encryption and proof of knowledge" in order to force the sender to keep the consistency of the transferred messages. We remark that the paradigm is unnecessary. In most reasonable applications of OT, the transferred messages must be recognizable for the receiver or the sender is willing to disclose some messages to the receiver. This property has been explicitly specified in the earlier works by Rabin, Even, Goldreich and Lempel.

Keywords: Oblivious transfer, deterministic encryption, probabilistic encryption, recognizable message

1 Introduction

The cryptographic primitive of oblivious transfer (OT) introduced by Rabin [25], is of fundamental importance in multi-party computation [12, 28]. In the model, a particpator (sender S) has only one secret m and would like to have the other participator (receiver R) to obtain m with probability 0.5. On the other hand, R does not want S to know whether it gets m or not.

There are two main OT models: 1-out-of-2 oblivious transfer (OT_1^2 for short) and k-out-of-n oblivious transfer (OT_k^n for short). OT_1^2 was suggested by Even, Goldreich and Lempel [11], as a generalization of Rabin's "oblivious transfer". For OT_1^2, the sender has two secrets m_1 and m_2 and would like to give the receiver one of them at the receiver's choice. Meanwhile, the receiver does not want the sender to know which secret he chooses. OT_k^n is a generalization of OT_1^2 where $k < n$. In the model, the sender has n secrets $m_1, \cdots, m_n$, and would like to give the receiver k of them at the receiver's choice. Again, the receiver does not want the sender to know which secrets he chooses.

In an adaptive oblivious transfer protocol, a sender commits to a database of messages and then repeatedly interacts with a receiver in such a way that the receiver obtains one message per interaction of his choice (and nothing more) while the sender learns nothing about any of the choices. At Eurocrypt'2007, Camenisch, Neven and Shelat [5] presented an adaptive oblivious transfer scheme in which a sender has n messages, of which a receiver can adaptively choose to receive k one-after-the-other. They were the first to propose a method for executing "assisted decryption" efficiently. In the scheme, the sender commits to his database by encrypting each message as $C_i = \mathrm{Enc}(M_i)$, and sends ciphertexts $C_1, \cdots, C_n$ to the receiver. The receiver then checks that each ciphertext is well-formed. To obtain a message, the sender and receiver engage in a blind decryption protocol such that the sender does not view the ciphertext he decrypts and the receiver is convinced that decryption was done correctly. To prevent the receiver from abusing the decryption protocol, the receiver has to provide a proof that his request corresponds to $C_1 \vee \cdots \vee C_n$.

The encryption used in the scheme is deterministic. Concretely, for $pk = (g, g^x, H = e(g,h))$ and $sk = h$, let $C_i = \left(g^{\frac{1}{x+i}}, M_i \cdot e(g,h)^{\frac{1}{x+i}}\right)$, where $g^{\frac{1}{x+i}}$ is a weak Boneh-Boyen signature [3] on i under g^x. The structure results in that a database manager (the sender) can only serve a single user (the receiver). Moreover, the protocol can be run only once even in the presence of a single user. In this paper, we shall improve the Camenisch-Neven-Shelat OT scheme by replacing the deterministic encryption with a probabilistic encryption.

The OT scheme follows the paradigm of "encryption and proof of knowledge" to force the sender to keep the consistency of the transferred messages. We should stress

that the paradigm is unnecessary for OT protocols. That means the sender can simply transfer the encrypted messages without any proofs of knowledge. The property has been explained in the earlier works by Rabin [25], Even, Goldreich and Lempel [11]. Based on the observation, we can further improve the Camenisch-Neven-Shelat OT scheme by removing the computations for some proofs of knowledge.

1.1 Related Works

In 1986, Brassard, et al. [4] extended 1-out-of-2 OT to 1-out-of-n OT for the case of n messages. Bellare and Micali [1], Naor and Pinkas [22, 23, 24], Mu, Zhang, and Varadharajan [21], Chu and Tzeng [9], et al. have studied the modle of k-out-of-n OT. Recently, Chang and Lai [7], Chang and Lee [6], and Liu et al. [8, 15, 19, 26, 27, 29] have presented some efficient OT_k^n schemes.

In 1999, Naor and Pinkas [23] investigated the problem of oblivious transfer with adaptive queries. Their scheme has inspired the latter works [2, 5, 9, 13, 14, 16, 17, 18, 20, 30]. In 2007, Camenisch, Neven and Shelat [5] proposed an adaptive oblivious transfer scheme. The Camenisch-Neven-Shelat scheme uses bilinear groups as the building block and adopts the paradigm of "encryption and proof of knowledge" to force the sender to keep the consistency of the transferred messages. The paradigm has been used in these OT protocols [13, 14, 17, 18, 30].

1.2 Security Requirements for k-out-of-n Oblivious Transfer

We follow the description of security requirements for k-out-of-n oblivious transfer in the work of Chang and Lai [7].

Definition 1. *A k-out-of-n OT is a two-party protocol in which Alice possesses n secrets $m_1, m_2, \cdots, m_n$ and Bob has his secret choices $\sigma = \{i_1, \cdots, i_k\} \subseteq 1, \cdots, n$. It satisfies the following requirements:*

- *Completeness: If both Alice and Bob follow the protocol, Bob gets k secrets m_j for $j \in \sigma$ after executing the protocol with Alice.*
- *Receiver's privacy: After executing the protocol with Bob, Alice shall not learn which k secrets Bob has received.*
- *Sender's privacy: After executing the protocol with Alice, Bob gets no information about the other $n-k$ secrets m_j for $j \notin \sigma$ or their combinations.*

An adaptive k-out-of-n OT scheme is a tuple of four PPT algorithms $(\mathsf{S}_I, \mathsf{R}_I, \mathsf{S}_T, \mathsf{R}_T)$. During the first phase, the sender runs S_I on input messages $m_1, \cdots, m_n$ and the receiver runs R_I without input. At the end of the phase, S_I and R_I produce local outputs S_0 and R_0, respectively. During the i-th transfer, $1 \le i \le k$, the sender and receiver engage in a selection protocol dictated by the S_T and R_T. The sender runs $\mathsf{S}_T(S_{i-1})$ to obtain updated state information S_i, while the receiver runs R_T on input state information R_{i-1} and the index σ_i of the message it wishes to receive, to obtain updated state information R_i and the retrieved message m'_{σ_i}. To capture security of an adaptive k-out-of-n OT scheme, we adopt the real-world/ideal-world paradigm [5].

$\mathrm{Real}_{\hat{S},\hat{R}}(N, k, M_1, \cdots, M_N, \sum)$. Suppose $\hat{S}$ and $\hat{R}$ are arbitrary sender and receiver algorithms. $\hat{S}$ is given messages $(M_1, \cdots, M_N)$ as input and interacts with $\hat{R}(\sum)$, where $\sum$ is an adaptive selection algorithm that, on input messages $M_{\sigma_1}, \cdots, M_{\sigma_{i-1}}$, outputs the index σ_i of the next message to be queried. In the first run, $\hat{S}$ and $\hat{R}$ produce initial states S_0 and R_0 respectively. Next, the sender and receiver engage in k interactions. In the i-th interaction for $1 \le i \le k$, the sender and receiver interact by running $S_i \leftarrow \hat{S}(S_{i-1})$ and $(R_i, M_i^*) \leftarrow \hat{R}(R_{i-1})$, and update their states to S_i and R_i, respectively. At the end of the k-th interaction, sender and receiver output strings S_k and R_k respectively.

$\mathrm{Ideal}_{\hat{S}',\hat{R}'}(N, k, M_1, \cdots, M_N, \sum)$. The (possibly cheating) sender algorithm $\hat{S}'(M_1, \cdots, M_N)$ generates messages $M_1^*, \cdots, M_N^*$ and hands these to the trusted party T. In each of the k transfer phases, T receives a bit b_i from the sender $\hat{S}'$ and an index σ_i^* from the (possibly cheating) receiver $\hat{R}'(\sum)$. If $b_i = 1$ and $\sigma_i^* \in \{1, \cdots, N\}$, then T hands $M_{\sigma_i^*}^*$ to the receiver; otherwise, it hands $\perp$ to the receiver. At the end of the k-th transfer, $\hat{S}'$ and $\hat{R}'$ output a string S_k and R_k.

An adaptive k-out-of-n OT scheme is sender-secure if for any PPT real-world cheating receiver $\hat{R}$ there exists a PPT ideal-world receiver $\hat{R}'$ such that the advantage of any PPT distinguisher in distinguishing the distributions $\mathrm{Real}_{S,\hat{R}}(N, k, M_1, \cdots, M_N, \sum)$ and $\mathrm{Ideal}_{S',\hat{R}'}(N, k, M_1, \cdots, M_N, \sum)$ is negligible. It is receiver-secure if for any PPT real-world cheating sender $\hat{S}$ there exists a PPT ideal-world sender $\hat{S}'$ such that the advantage of any PPT distinguisher in distinguishing the distributions $\mathrm{Real}_{\hat{S},R}(N, k, M_1, \cdots, M_N, \sum)$ and $\mathrm{Ideal}_{\hat{S}',R'}(N, k, M_1, \cdots, M_N, \sum)$ is negligible.

2 Preliminaries

Let Pg be a pairing group generator that on input 1^κ outputs descriptions of multiplicative groups $\mathbb{G}_1, \mathbb{G}_T$ of prime order p where $|p| = \kappa$. Let g be a generator of $\mathbb{G}_1$. The bilinear map $e : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_T$ satisfies: (1) for all $a, b \in \mathbb{Z}_p$ it holds that $e(g^a, g^b) = e(g, g)^{ab}$; (2) $e(g, g) \neq 1$; (3) the bilinear map is efficiently computable.

The notation

$$PoM\{(h) : H = e(g,\, h) \wedge W = e(h,\, V)\}$$

denotes a zero-knowledge proof of membership of a group element $h \in \mathbb{G}_1$ such that $H = e(g, h)$ and $W = e(h, V)$ hold. All values not enclosed in ()'s are assumed to be

known to the verifier. Likewise,

$$PoK\{(x,h): y = g^x \wedge H = e(y,h)\}$$

denotes a zero-knowledge proof of knowledge of an integer x and a group element $h \in \mathbb{G}_1$ such that $y = g^x$ and $H = e(y,h)$ hold.

Definition 2. *(ℓ-Strong Diffie-Hellman Assumption). We say that the ℓ-SDH assumption associated to a pairing generator Pg holds if for all PPT adversaries A, the probability that $A(g, g^x, \cdots, g^{x^\ell})$ where $(\mathbb{G}_1, \mathbb{G}_T) \leftarrow \mathsf{Pg}(1^\kappa), g \leftarrow \mathsf{G}_1^*$ and $x \leftarrow \mathbb{Z}_p$, outputs a pair $(c, g^{1/(x+c)})$ where $c \in \mathbb{Z}_p$ is negligible in κ.*

Definition 3. *(ℓ-Power Decisional Diffie-Hellman Assumption). We say that the ℓ–PDDH assumption associated to Pg holds if for all PPT adversaries A, the probability that A on input $(g, g^x, g^{x^2}, \cdots, g^{x^\ell}, H)$ where $(\mathbb{G}_1, \mathbb{G}_T) \leftarrow \mathsf{Pg}(1^\kappa), g \leftarrow \mathbb{G}_1^*, x \leftarrow \mathbb{Z}_p, H \leftarrow \mathbb{G}_T$, distinguishes the vector $T = (H^x, H^{x^2}, \cdots, H^{x^\ell})$ from a random vector $T \leftarrow \mathbb{G}_T^\ell$ is negligible in κ.*

3 Camenisch-Neven-Shelat Oblivious Transfer Scheme

3.1 Review

The protocol is in the standard model. See the following Table 1 for details. Each pair (A_i, B_i) can be seen as an ElGamal encryption [10] in $\mathbb{G}_T$ of M_i under public key H. But instead of using random elements from $\mathbb{G}_T$ as the first component, the protocol uses verifiably random values $A_i = g^{1/(x+i)}$. It allows the sender to check that the receiver is indeed asking for the decryption key for one particular ciphertext, and not for some combination of ciphertexts.

3.2 A Weakness

The encryption used in the scheme is deterministic. Concretely, for

$$pk = (g, g^x, H = e(g,h))$$

and $sk = h$, let

$$C_i = \left(g^{\frac{1}{x+i}}, M_i \cdot e(g,h)^{\frac{1}{x+i}}\right)$$

where $g^{\frac{1}{x+i}}$ is a weak Boneh-Boyen signature [3] on i under g^x. In view of that a database manager usually plays the role of the sender in an OT protocol, the structure results in that a database manager can only serve a single client only once.

Suppose that $N > 2k$ and there are two users $\mathcal{R}, \hat{\mathcal{R}}$. $\mathcal{R}$ has the ciphertexts $C_1, \cdots, C_N$ and $\hat{\mathcal{R}}$ has the ciphertexts $\hat{C}_1, \cdots, \hat{C}_N$, where

$$C_i = \left(g^{\frac{1}{x+i}}, M_i \cdot e(g,h)^{\frac{1}{x+i}}\right),$$

$$\hat{C}_i = \left(g^{\frac{1}{x+i}}, \hat{M}_i \cdot e(g,h)^{\frac{1}{x+i}}\right)$$

for $1 \le i \le N$. At the end of the two OT protocols executed by the sender, $\mathcal{R}$ and $\hat{\mathcal{R}}$, if $\mathcal{R}$ obtains $M_1, \cdots, M_k$, and $\hat{\mathcal{R}}$ obtains $\hat{M}_{k+1}, \cdots, \hat{M}_{2k}$, then $\mathcal{R}$ and $\hat{\mathcal{R}}$ can collaborate to obtain $M_{k+1}, \cdots, M_{2k}$, $\hat{M}_1, \cdots, \hat{M}_k$. Thus, they obtain $4k$ messages instead of $2k$ messages as usually supposed. In other words, the protocol can be run only once even in the presence of a single user. The drawback results from that the scheme invariably uses N blinders

$$e(g,h)^{\frac{1}{x+1}}, \cdots, e(g,h)^{\frac{1}{x+N}}.$$

We refer to the attack as *session key attack*.

4 A Modification of Camenisch-Neven-Shelat OT Scheme

In the original Camenisch-Neven-Shelat oblivious transfer scheme, the public key is set as (g, H, y), where $y = g^x$. The receiver has to use the public parameter y for the proof of knowledge (σ_i, v), i.e.,

$$PoK\{(\sigma_i, v): e(V, y) = e(V, g)^{-\sigma_i} e(g, g)^v\}.$$

The setting allows the sender to check that the receiver does not ask for some combination of ciphertexts. That is, it makes the sender believe that the queries from the receiver are well-formed. But *it is unnecessary to set y as a public parameter*. It only requires to *set y as a session helper* with respect to the session key x. The authors did not pay more attention to the differences between a public parameter and a session helper. Informally, a public parameter should be used repeatedly except that it has to be authorized by a functionally trusted TTP (trusted third party). Whereas, a session helper can only be used once. The change, removing the public parameter y and introducing a session helper y, successfully transforms the deterministic encryption into a probabilistic encryption. See the following Table 2 for details.

Theorem 1. *If the (N+1)-SDH assumption and the (N+1)-PDDH assumptions associated to Pg hold, then the OT protocol in Table 2 is sender-secure.*

Theorem 2. *The OT protocol in Table 2 is receiver-secure if the transferred messages are recognizable for the receiver.*

We refer to [5] for the proofs of these claims. It suffices to transform the public parameter y into a session helper and transform the associated signatures $A_1, \cdots, A_N$ in the related Games into knowledge proofs (see Pages 15-16 in [5]).

Note that the original proof of receiver-security does not consider that a malicious sender can launch the local-input replacement attack. That is, the sender simply sets $M_1 = M_2 = \cdots = M_N = M^{(i)}$ for some message $M^{(i)}$ during the i-th transfer. At the end of this phase, the receiver always obtains the message $M^{(i)}$. Of course, the

Table 1: Camenisch-Neven-Shelat oblivious transfer scheme

	Initialization	
$\underline{\mathsf{S}_I(1^\ell, M_1, \cdots, M_N):}$		$\underline{\mathsf{R}_I(1^\ell):}$
$(G_1, G_T) \leftarrow \mathsf{Pg}(1^\ell)$		
$g, h \leftarrow \mathbb{G}_1^*; H \leftarrow e(g,h)$		
$x \leftarrow Z_p; y \leftarrow g^x;$		
$pk \leftarrow (g, H, y)$		
For $i = 1, \cdots, N$ do		
$A_i \leftarrow g^{1/(x+i)}$		
$B_i \leftarrow e(h, A_i) \cdot M_i$		
$C_i \leftarrow (A_i, B_i)$	$\overset{pk, C_1, \cdots, C_N}{- - - - - - - \dashrightarrow}$	
$S_0 \leftarrow (h, pk)$	$\overset{PoM\{(h): H = e(g,h)\}}{- - - - - - - \dashrightarrow}$	$R_0 \leftarrow (pk, C_1, \cdots, C_N)$
	Transfer	
$\mathsf{S}_\mathsf{T}(S_{i-1}):$		$\mathsf{R}_\mathsf{T}(R_{i-1}, \sigma_i):$
	$\overset{V}{\dashleftarrow - - - - - - - - - - - - - -}$	$v \leftarrow \mathbb{Z}_p; V \leftarrow (A_{\sigma_i})^v$
	$\overset{PoK\{(\sigma_i, v): e(V,y) = e(V,g)^{-\sigma_i}\, e(g,g)^v\}}{\dashleftarrow - - - - - - - - - - - - - -}$	
$W \leftarrow e(h, V)$	$\overset{W}{- - - - - - - - - - - - \dashrightarrow}$	
	$\overset{PoM\{(h): H = e(g,h) \wedge W = e(h,V)\}}{- - - - - - - - - - - - \dashrightarrow}$	
$S_i = S_{i-1}$		$M \leftarrow B_{\sigma_i}/(W^{1/v})$
		$R_i = R_{i-1}$

Table 2: A modification of Camenisch-Neven-Shelat OT scheme

	Setup	
$(G_1, G_T) \leftarrow \mathsf{Pg}(1^\ell)$		
$g, h \leftarrow \mathbb{G}_1^*;\ H = e(g,h)$		
$pk \leftarrow (g, H);\ sk \leftarrow h$		
	Transfer	
$\underline{\mathsf{S}_I(1^\ell, M_1, \cdots, M_N):}$		$\underline{\mathsf{R}_I(1^\ell):}$
$x \leftarrow Z_p; y \leftarrow g^x$		
For $i = 1, \cdots, N$ do		
$A_i \leftarrow g^{1/(x+i)}$		
$B_i \leftarrow e(h, A_i) \cdot M_i$		
$C_i \leftarrow (A_i, B_i)$	$\overset{pk, y, C_1, \cdots, C_N}{- - - - - - - \dashrightarrow}$	
$S_0 \leftarrow (h, pk)$	$\overset{PoM\{(h): H = e(g,h)\}}{- - - - - - - \dashrightarrow}$	$R_0 \leftarrow (pk, C_1, \cdots, C_N)$
$\mathsf{S}_\mathsf{T}(S_{i-1}):$		$\mathsf{R}_\mathsf{T}(R_{i-1}, \sigma_i):$
	$\overset{V}{\dashleftarrow - - - - - - - - - - - - - -}$	$v \leftarrow \mathbb{Z}_p; V \leftarrow (A_{\sigma_i})^v$
	$\overset{PoK\{(\sigma_i, v): e(V,y) = e(V,g)^{-\sigma_i}\, e(g,g)^v\}}{\dashleftarrow - - - - - - - - - - - - - -}$	
$W \leftarrow e(h, V)$	$\overset{W}{- - - - - - - - - - - - \dashrightarrow}$	$M_{\sigma_i} \leftarrow B_{\sigma_i}/(W^{1/v})$
	$\overset{PoM\{(h): H = e(g,h) \wedge W = e(h,V)\}}{- - - - - - - - - - - - \dashrightarrow}$	
$S_i = S_{i-1}$		$R_i = R_{i-1}$

malicious sender learns which message that the receiver has received. To resist the local-input replacement attack, the transferred messages in OT schemes must be recognizable for the receiver. See the following section for the further explanations.

5 On the Paradigm of "Encryption and Proof of Knowledge"

The Camenisch-Neven-Shelat oblivious transfer scheme follows the paradigm of "encryption and proof of knowledge" to force the sender to keep the consistency of the committed messages. From the practical point of view, we should remark that the paradigm is unnecessary. In most reasonable applications of OT, *the transferred messages must be recognizable for the receiver*, or *the sender is willing to disclose some messages to the receiver*. The property has been explicitly specified in the earlier works by Rabin, Even, Goldreich and Lempel. We refer to the following descriptions.

In [25], Rabin explained that:

> Bob and Alice each have a secret, SB and SA, respectively, which they wish to exchange. For example, SB may be the password to a file that Alice wants to access (we shall refer to this file as Alice's file), and SA the password to Bob's file. To exclude the possibility of randomizing on the possible digits of the password, we assume that if an incorrect password is used then the file is erased, and that Bob and Alice want to guarantee that this will not happen to their respective files.

In [11], Even, Goldreich and Lempel stressed that:

> The notion of a "recognizable secret message" plays an important role in our definition of OT. A message is said to be a recognizable secret if, although the receiver cannot compute it, he can authenticate it once he receives it. The notion of a recognizable secret message is evidently relevant to the study of cryptographic protocols, in which the sender is reluctant to send the message while the receiver wishes to get it. In such protocols, it makes no sense to consider the transfer of messages that are either not secret (to the receiver) or not recognizable (by the receiver).

In symmetric case, such as exchanging secrets, signing contracts, both two participators can easily verify the correctness of the received messages. In unsymmetric case, such as a database manager plays the role of the sender and a client plays the role of the receiver, it is usual that the sender is willing to disclose some messages to the receiver.

To sum up, *if the transferred messages are not recognizable then the receiver can not decide to retrieve which message*. It is reasonable to assume that the transferred messages in an OT scheme are correct. It is unnecessary for the sender to provide any proofs of knowledge. By the way, the definition of "proof of knowledge" is more strong than that of "recognizable message". The following three common examples of recognizable messages come from [11]: (i) A signature of a user to some known message is a recognizable secret message for everybody else. (ii) The key K, by which the plaintext M is transformed using cryptosystem F into ciphertext $F_K(M)$. (iii) The factorization of a composite number, which has only large prime factors.

Based on the above facts, we now can improve the Camenisch-Neven-Shelat OT scheme by removing the computations for some proofs of knowledge. See Table 3 for the improvement.

Theorem 3. *If the (N+1)-SDH assumption and the (N+1)-PDDH assumptions associated to Pg hold, then the OT protocol in Table 3 is sender-secure.*

Proof (Sketch). The proof of this claim can be easily derived from that of Theorem 1, because the witnesses obtained by the receiver in the model of Table 3 consist of pk, y, $C_1, \cdots, C_N, W,$, which are strictly less than that

$$pk,\, y,\, C_1, \cdots, C_N, W, PoM\{(h) : H = e(g,\, h)\},$$

$$PoM\{(h) : H = e(g,\, h) \wedge W = e(h,\, V)\}$$

obtained by the receiver in the model of Table 2. Loosely speaking, the sender in the model of Table 3 shall leak less information to the receiver.

Theorem 4. *The OT protocol in Table 3 is receiver-secure if the sender is semi-honest and the transferred messages are recognizable for the receiver.*

Proof. Define the following distributions games Game-0, $\cdots$, Game-3 such that Game-0=$\text{Real}_{\hat{S},R}$ and Game-3=$\text{Ideal}_{\hat{S}',R'}$. Let D be a universal distinguisher which can efficiently recognize the output distributions of these games. Let $\Pr[\text{Game-i}] = \Pr[D(X) = 1 : X \leftarrow \text{Game-i}]$.

Game-0: In the game, the semi-honest sender $\hat{S}$ runs against an honest receiver R with selection strategy $\sum$. Obviously, $\Pr[\text{Game-0}] = \Pr[D(X) = 1 : X \leftarrow \text{Real}_{\hat{S},R}]$.

Game-1: In this game, an extractor $\mathcal{E}_1$ is used to extract from $\hat{S}$ the element h such that $e(g, h) = H$. If the extractor fails, then the output of Game-1 is $\perp$; otherwise, the execution of $\hat{S}$ continues as in the previous game, interacting with $R(\sum)$. The difference between the two output distributions is given by randomness of selection of h (because $\hat{S}$ is supposed to be semi-honest), i.e., $\Pr[\text{Game-1}] - \Pr[\text{Game-0}] \leq 1/p$.

Game-2: We refer to [5] for the description of this game. By investigating the games, we have that $\Pr[\text{Game-2}] = \Pr[\text{Game-1}]$.

Game-3: In this game, an ideal-world sender $\hat{S}'$ uses $\mathcal{E}_1$ to extract h from $\hat{S}$, decrypts M_i^* as $B_i/e(h, A_i)$ for $i = 1, \cdots, N$ and submits $M_1^*, \cdots, M_N^*$ to the trusted party

Table 3: An improvement of Camenisch-Neven-Shelat OT scheme

Setup		
$(G_1, G_T) \leftarrow \mathsf{Pg}(1^\ell)$ $g, h \leftarrow \mathbb{G}_1^*$ $pk \leftarrow g$; $sk \leftarrow h$		
Transfer		
$\underline{\mathsf{S}_I(1^\ell, M_1, \cdots, M_N):}$ $x \leftarrow Z_p; y \leftarrow g^x$ For $i = 1, \cdots, N$ do $A_i \leftarrow g^{1/(x+i)}$ $B_i \leftarrow e(h, A_i) \cdot M_i$ $C_i \leftarrow (A_i, B_i)$ $S_0 \leftarrow (h, pk)$	$\xrightarrow{pk, y, C_1, \cdots, C_N}$	$\underline{\mathsf{R}_I(1^\ell):}$ $R_0 \leftarrow (pk, C_1, \cdots, C_N)$
$\mathsf{S}_\mathsf{T}(S_{i-1}):$		$\mathsf{R}_\mathsf{T}(R_{i-1}, \sigma_i):$
	$\xleftarrow{V}$	$v \leftarrow \mathbb{Z}_p; V \leftarrow (A_{\sigma_i})^v$
	$\xleftarrow{PoK\{(\sigma_i, v): e(V,y)=e(V,g)^{-\sigma_i} e(g,g)^v\}}$	
$W \leftarrow e(h, V)$	$\xrightarrow{W}$	$M_{\sigma_i} \leftarrow B_{\sigma_i}/(W^{1/v})$
$S_i = S_{i-1}$		$R_i = R_{i-1}$

T. As in Game-2, during the transfer phase, $\hat{S}'$ feeds $V' \leftarrow A_1^{v'}$ to $\hat{S}$ and uses $(v', 1)$ as a witness in the PoK. It is easy to find that $\hat{S}$ can convince $\hat{S}'$ that W is correctly formed (because the transferred messages are recognizable for the receiver). Thus, $\Pr[\text{Game-3}] = \Pr[\text{Game-2}] = \Pr[D(X) = 1 : X \leftarrow \text{Ideal}_{\hat{S}', R'}]$.

Summing up, we have $\Pr[D(X) = 1 : X \leftarrow \text{Ideal}_{\hat{S}', R'}] - \Pr[D(X) = 1 : X \leftarrow \text{Real}_{\hat{S}, R}] \leq 1/p$.

6 Conclusions

We modify the Camenisch-Neven-Shelat adaptive OT protocol by replacing the deterministic encryption with a probabilistic encryption. We further improve it by removing the redundant proofs of knowledge based on the fact that the transferred messages should be recognizable or the sender is willing to disclose some messages to the receiver. We hope the presentation is helpful to clarify some misunderstandings about the primitive of oblivious transfer.

Acknowledgments

This work is supported by the National Natural Science Foundation of China (Project 61303200, 61411146001), the Shanghai Leading Academic Discipline Project (S30104), the Scientific Research Foundation for the Returned Overseas Chinese Scholars, State Education Ministry. The authors gratefully acknowledge the anonymous reviewers for their valuable comments.

References

[1] M. Bellare and S. Micali, "Non-interactive oblivious transfer and applications," in *Proceedings of Advances in Cryptology - CRYPTO'89*, pp. 547–557, Santa Barbara, USA, Aug. 1989.

[2] M. K. Bhatia1, S. K. Muttoo, and M. P.Bhatia, "Secure requirement prioritized grid scheduling model," *International Journal of Network Security*, vol. 15, no. 6, pp. 478–483, 2013.

[3] D. Boneh and X. Boyen, "Short signatures without random oracles," in *Proceedings of Advances in Cryptology - EUROCRYPT 2004*, pp. 56–73, Interlaken, Switzerland, May 2004.

[4] G. Brassard, C. Crepeau, and J. Robert, "All-or-nothing disclosure of secrets," in *Proceedings of Advances in Cryptology - CRYPTO'86*, pp. 234–238, Santa Barbara, USA, Aug. 1986.

[5] J. Camenisch, G. Neven, and A. Shelat, "Simulatable adaptive oblivious transfer," in *Proceedings of Advances in Cryptology - EUROCRYPT 2007*, pp. 573–590, Barcelona, Spain, May 2007.

[6] 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.

[7] C. C. Chang and Y. P. Lai, "Efficient t-out-of-n oblivious transfer schemes," in *Proceedings of the 2008 International Conference on Security Technology*, pp. 3–6, Hainan, China, Dec. 2008.

[8] C. K. Chu and W. G.Tzeng, "Efficient k-out-of-n oblivious transfer schemes," *Journal of Universal Computer Science*, vol. 14, no. 3, pp. 397–415, 2008.

[9] C. K. Chu and W. G. Tzeng, "Efficient k-out-of-n oblivious transfer schemes with adaptive and non-adaptive queries," in *Proceedings of 8th International Workshop on Theory and Practice in Public Key Cryptography (PKC05)*, pp. 172–183, Les Diablerets, Switzerland, Jan. 2005.

[10] T. ElGamal, "A public key cryptosystem and signature scheme based on discrete logarithms," *IEEE Transactions on Information Theory*, vol. 31, pp. 469–472, 1985.

[11] S. Even, O. Goldreich, and A. Lempel, "A randomized protocol for signing contracts," *Commun. ACM*, vol. 28, no. 6, pp. 637–647, 1985.

[12] M. Green and S. Hohenberger, "How to play any mental game or a completeness theorem for protocols with honest majority," in *Proceedings of 19th Annual ACM Conference on Theory of Computing(STOC'87)*, pp. 218–229, New York,USA, May 1987.

[13] M. Green and S. Hohenberger, "Blind identity-based encryption and simulatable oblivious transfer," in *Proceedings of Advances in Cryptology - ASIACRYPT 2007*, pp. 265–282, Kuching, Malaysia, Dec. 2007.

[14] M. Green and S. Hohenberger, "Practical adaptive oblivious transfer from simple assumptions," in *Proceedings of the Eighth Theory of Cryptography Conference (TCC 2011)*, pp. 347–363, Brown University,USA, Mar. 2011.

[15] A. Jain and C. Har, "A new efficient protocol for k-out-of-n oblivious transfer," *Cryptologia*, vol. 34, no. 4, pp. 282–290, 2010.

[16] M. Kumar, M. K. Gupta, and S. Kumari, "An improved efficient remote password authentication scheme with smart card over insecure networks," *International Journal of Network Security*, vol. 13, no. 3, pp. 167–177, 2011.

[17] K. Kurosawa, R. Nojima, and T. P. Le, "Efficiency-improved fully simulatable adaptive ot under the ddh assumption," in *Proceedings of 7th Conference on Security and Cryptography for Networks (SCN'10)*, pp. 172–181, Amalfi, Italy, Sep. 2010.

[18] K. Kurosawa, R. Nojima, and T. P. Le, "Generic fully simulatable adaptive oblivious transfer," in *Proceedings of 9th International Conference on Applied Cryptography and Network Security (ACNS'11)*, pp. 274–291, Nerja, Spain, June 2011.

[19] Y. J. Liu, C. C. Chang, and S. C. Chang, "An efficient oblivious transfer protocol using residue number system," *International Journal of Network Security*, vol. 15, no. 3, pp. 212–218, 2013.

[20] G. Manikandan, M. Kamarasan, and N. Sairam, "A new approach for secure data transfer based on wavelet transform," *International Journal of Network Security*, vol. 15, no. 2, pp. 106–112, 2013.

[21] Y. Mu, J.Q. Zhang, and V. Varadharajan, "m out of n oblivious transfer," in *Proceedings of Information Security and Privacy, 7th Australian Conference (ACISP2002)*, pp. 395–405, Melbourne, Australia, July 2002.

[22] M. Naor and B. Pinkas, "Oblivious transfer and polynomial evaluation," in *Proceedings of 31th Annual ACM Conference on Theory of Computing(STOC'99)*, pp. 245–254, Atlanta, Georgia, USA, May 1999.

[23] M. Naor and B. Pinkas, "Oblivious transfer with adaptive queries," in *Proceedings of Advances in Cryptology - CRYPTO'89*, pp. 573–590, Santa Barbara,USA, Aug. 1999.

[24] M. Naor and B. Pinkas, "Efficient oblivious transfer protocols," in *Proceedings of 12th Annual ACM-SIAM Symposium on Discrete Algorithms (SODA'01)*, pp. 448–457, Washington, D.C., USA, Jan. 2001.

[25] M. Rabin. "How to exchange secrets by oblivious transfer. technical report,". Tech. Rep. TR-81, May 1981.

[26] W. G. Tzeng, "Efficient 1-out-of-n oblivious transfer protocols with universally usable parameter," *IEEE Transactions on Computers*, vol. 53, no. 2, pp. 232–240, 2004.

[27] Q. H. Wu, J. H. Zhang, and Y. M. Wang, "Practical t-out-n oblivious transfer and its applications," *Information and Communications Security*, vol. 2836, pp. 226–237, 2003.

[28] Y. Yao, "How to generate and exchange secrets," in *Proceedings of 27th Annual Symposium on Foundations of Computer Science (FOCS'86)*, pp. 162–167, Toronto, Canada, Oct. 1986.

[29] B. Zeng and et al., "A practical framework for t-out-of-n oblivious transfer with security against covert adversaries," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 2, pp. 465–479, 2012.

[30] B.S. Zhang, "Simulatable adaptive oblivious transfer with statistical receiver's privacy," in *Proceedings of the 5th International Conference on Provable Security (ProvSec 2011)*, pp. 52–67, Xi'an, China, Oct. 2011.

Zhengjun Cao is an associate professor of department of Mathematics at Shanghai University. He received his Ph.D. degree in applied mathematics from Academy of Mathematics and Systems Science, Chinese Academy of Sciences. He served as a post-doctor in Department of Computer Science, Universit Libre de Bruxelles, from 2008 to 2010. His current research interests include cryptography, random algorithms and quantum computation.

Hanyue Cao received the B.S. degree from Shanghai University, Shanghai, China, in 2012. She is currently pursuing her M.S. degree from Department of Mathematics, Shanghai university. Her research interests include information security and cryptography.