Improvement of Camenisch-Neven-Shelat Oblivious Transfer Scheme

Zhengjun Cao and Hanyue Cao

Department of Mathematics, Shanghai University, Shanghai, China
* caozhj@shu.edu.cn

Abstract. In 2007, Camenisch, Neven and Shelat proposed an adaptive oblivious transfer (OT) 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 only 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 oblivious transfer primitive, introduced by Rabin [12], is of fundamental importance in multi-party computation [9, 13]. 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.

In 2007, Camenisch, Neven and Shelat [2] 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 [1] 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 note, we fix the Camenisch-Neven-Shelat oblivious transfer 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. The paradigm has been used for recent OT protocols [7, 8, 10, 11, 14]. 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 [12], Even, Goldreich and Lempel [5]. Based on the observation, we can further improve the Camenisch-Neven-Shelat OT scheme by removing the computations for some proofs of knowledge.

2 Camenisch-Neven-Shelat oblivious transfer

The scheme requires bilinear groups and associated hardness assumptions. 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 $\mathbb{G}_1^* = \mathbb{G}_1 \setminus \{1\}$ and let $g \in \mathbb{G}_1^*$. The generated groups are such that there exists an admissible bilinear map $e : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_T$, meaning that

(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.

We use the notation of Camenisch and Stadler [3] for the proofs of knowledge. For instance, $PoK\{(x,h) : y = g^x \wedge H = e(y,h) \wedge (1 \leq x \leq n)\}$ denotes a zero-knowledge proof of knowledge of an integer x and a group element $h \in \mathbb{G}$ such that $y = g^x$ and $H = e(y,h)$ hold and $1 \leq x \leq n$. All values not enclosed in ()'s are assumed to be known to the verifier.

2.1 Review

The protocol is in the standard model. See the Table 1 for details.

Each pair (A_i, B_i) can be seen as an ElGamal encryption [6] 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 [4] 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.

Table 1: Camenisch-Neven-Shelat oblivious transfer

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

2.2 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 [1] 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*.

3 A modification

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 $(\sigma_i,\ v)$, 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.

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

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

The change, removing the public parameter y and introducing a session helper y, successfully transforms the deterministic encryption into a probabilistic encryption. See the Table 2 for details.

4 Remarks 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 Ref.[12], 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 Ref.[5], 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 the Ref.[5]:

(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 the following Table 3 for the improvement.

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

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

5 Conclusion

We modify the Camenisch-Neven-Shelat adaptive oblivious transfer 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 keep its consistency.

References

1. 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)
2. 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)
3. Camenisch, J., Stadler, M.: Efficient group signature schemes for large groups. In: CRYPTO'97, LNCS, vol. 1296, pp. 410-424. Springer, Heidelberg (1997)

4. Dodis Y., Yampolskiy A.: A verifiable random function with short proofs and keys. In Vaudenay S.,(Ed.) PKC 2005. LNCS, vol. 3386, pp. 416C431. Springer, Heidelberg (2005)
5. Even S., Goldreich O., Lempel A.: A randomized protocol for signing contracts. Commun. ACM 28(6), 637-647 (1985)
6. ElGamal T.: A public key cryptosystem and signature scheme based on discrete logarithms. IEEE Transactions on Information Theory, 31, 469C472 (1985)
7. Green, M., Hohenberger, S.: Blind identity-based encryption and simulatable oblivious transfer. In: Kurosawa K., (ed.): ASIACRYPT 2007, LNCS, vol. 4833, pp. 265C282. Springer, Heidelberg (2007)
8. Green, M., Hohenberger, S.: Practical adaptive oblivious transfer from simple assumptions. In: Yuval, I., (ed.) TCC 2011. LNCS, vol. 6597, pp. 347-363. Springer, Heidelberg (2011)
9. Goldreich, O., Micali, S., Wigderson, A.: How to play any mental game or a completeness theorem for protocols with honest majority. In: STOC '87, pp. 218-229 (1987)
10. Kurosawa, K., Nojima, R., Le Phong, T.: Efficiency-Improved Fully Simulatable Adaptive OT under the DDH Assumption. In: Garay, J.A., De Prisco, R. (eds.) SCN 2010. LNCS, vol. 6280, pp. 172-181. Springer, Heidelberg (2010)
11. Kurosawa, K., Nojima, R., Le Phong, T.: Generic fully simulatable adaptive oblivious transfer. In: Lopez, J., Tsudik, G. (eds.) ACNS 2011. LNCS, vol. 6715, pp. 274-291. Springer, Heidelberg (2011)
12. Rabin, M.: How to exchange secrets by oblivious transfer. Technical Report TR-81, Aiken Computation Laboratory, Harvard University (1981)
13. Yao, Y.: How to generate and exchange secrets. In: FOCS, pp. 162-167 (1986)
14. Zhang B.S.: Simulatable Adaptive Oblivious Transfer with Statistical Receiver's Privacy. In: Boyen X., Chen X. (eds.) ProvSec 2011, LNCS, vol. 6980, pp. 52C67. Springer, Heidelberg (2011)