4-3 A Survey on Oblivious Transfer Protocols

Le Trieu Phong

In this paper, we survey some constructions of oblivious transfer (OT) protocols from public key encryption schemes. We begin with a simple construction of 1-out-of-2 OT when both the sender and the receiver are assumed to be honest. We then move to a more complex construction assuming either dishonest sender or receiver, enjoying the so-called fully simulatable security. We then highlight some concrete instantiations secure under the decisional Diffie-Hellman (DDH) and the decision linear assumptions.

Keywords
Oblivious transfer, Public key encryption schemes

1 Introduction

1.1 Background

Oblivious transfer protocols[2] have been extensively studied in the literature. In its simple form, we have a sender having two messages and a receiver wants to get one of them without revealing which one was taken to the sender. This is called 1-out-of-2 in the literature, and it is one of the basic tools for building more complicated protocols (see e.g. [3]). An illustration is given in Fig. 1.

Oblivious transfer with adaptive queries, or adaptive OT for short, was first examined by Naor and Pinkas in [12], in which there are a sender and a receiver. The sender holds n messages, and the receiver would like to retrieve k of them, one after the other, so that: (1) the sender does not know what the receiver obtains, and (2) the receiver gets nothing more beside the k messages. The key applications of this type of OT are in patent searches, oblivious search, medical databases etc.

The security notion capturing the above requirements has evolved in the literature. The notion of full simulatability was introduced by Camenisch et al. in [1], following the real-world, ideal-world paradigm. In the ideal world, there exists a trusted third party (TTP), to which the sender gives all of his messages. When a receiver wants to obtain a message, he simply sends the corresponding index to the TTP. On the other hand, in the real world, there is no TTP at all, and the protocol of adaptive OT is run by the sender and the receiver. The intuition of full simulatability is that the

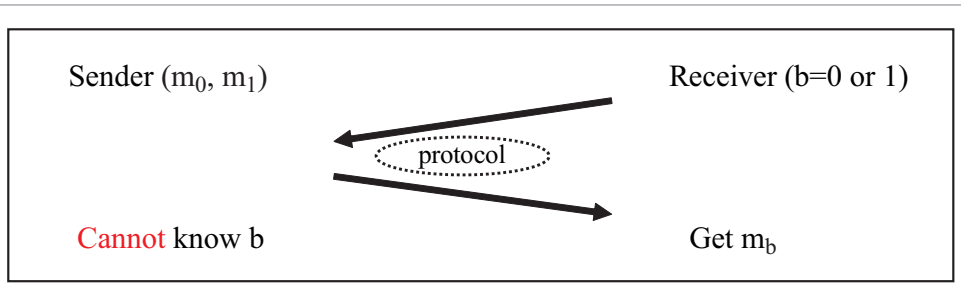

Fig.1 *1-out-of-2 oblivious transfer*

real world is indistinguishable from the ideal world, with respect to any poly-time adversary.

Camenisch et al. additionally provided us with some first constructions of adaptive OT which were fully simulatable, in both the random oracle model (ROM) and the standard model. In particular, they showed with a refinement that the scheme in ROM of Ogata and Kurosawa[15] achieved fully simulatable security. They furthermore gave a construction in the standard model, using q-based assumptions (in which q depends on n) in pairing groups.

After the work of Camenisch et al., much effort has been devoted to further extending the direction. In [5], Green and Hohenberger constructed a universally-composable, so fully-simulatable, scheme under the so-called q-hidden LRSW assumption. Jarecki and Liu[8] joined the research line with a scheme based on the q-DHI (Diffie-Hellman Inversion) assumption yet in RSA groups.

With respect to assumptions which are not q-based, Kurosawa and Nojima[9] showed a simple scheme fully simulatable under the DDH assumption. However, the scheme suffered from a large communication cost of $O(n)$ in each transfer, as pointed out by Green and Hohenberger in [6], who further gave a construction under the decision 3-party DDH (3DDH) assumption in pairing groups. Concurrently, Kurosawa, Nojima, and Phong[10], using a verifiable shuffle protocol, overcome the demerit of [9], reducing the cost to $O(1)$, while still maintaining the DDH assumption for security. Furthermore, in [11], the same authors propose generic constructions of adaptive OT, whose instantiations are secure under standard, well-known assumptions.

1.2 In this paper

The main purpose of this paper is to survey some constructions of OT from public key encryption schemes. To begin with, we recall a simple, well-known construction of 1-out-of-2 OT from PKE schemes (cf. [3]).

We then present a generic method by Kurosawa, Nojima, and Phong[11] for constructing fully simulatable adaptive OT in the standard model, also using PKE (with some special properties) as the main building block. The method then yield protocols from the DDH and d-linear ($d \geq 2$) assumptions. A brief comparison is given in Table 1.

These techniques for oblivious transfer are very crucial for building more complex yet highly-functional protocols such as two-party computation protocols. Indeed, one may theoretically found cryptography on oblivious transfer. Therefore, oblivious transfer has been fitted well as a research direction in the Security Fundamentals Group.

Table 1 *Fully simulatable adaptive OT schemes without random oracles*

Scheme	Assumption	Comm. Cost (each transfer)	Init. Cost
CNS [1]	q-strong DH and q-PDDH	$O(1)$	$O(n)$
GH [5]	q-hidden LRSW (UC secure)	$O(1)$	$O(n)$
JL [8]	q-DHI (RSA group)	$O(1)$	$O(n)$
KN [9]	DDH	$O(n)$	$O(n)$
GH [6]	decision 3-party DH (3DDH)	$O(1)$	$O(n)$
KNP [10]	DDH	$O(1)$	$O(n)$ (more moves)
KNP [11]	DDH	$O(1)$	$O(n)$ (less moves)
	d-Linear		$O(n)$

2 Notations

Throughout the paper, $\mathrm{OT}^n_{k\times 1}$ denotes the adaptive OT with n messages of the sender and k choices of the receiver. ZKPK stands for zero-knowledge proof of knowledge, while ZKPM for zero-knowledge proof of membership. WIPK means witness-indistinguishable proof of knowledge.

We use $a[i]$ to indicate the i-th component of a. For example, when a is a bit string, $a[i]$ is the i-th bit; when a is a tuple of elements, $a[i]$ becomes the i-th element.

3 A simple construction of 1-out-of-2 OT

Suppose we are given a PKE consisting of algorithms (KGen, Enc, Dec). The algorithm KGen returns a public key pk and a secret key sk. Using pk, Enc on input a message m return a ciphertext c which can be decrypted by Dec with sk.

Now consider a sender with two messages m_0, m_1, and a receiver with a bit b. The receiver wants to obtain m_b without revealing b to the sender. They perform as follows.

1. The receiver sends $(pk_b, sk_b) \leftarrow \mathrm{KGen}$, and truly random pk_{1-b} to the sender.
2. The sender sends $c_0 = \mathrm{Enc}(pk_0, m_0)$ and $c_1 = \mathrm{Enc}(pk_1, m_1)$ to the receiver.
3. The receiver, using sk_b, decrypts c_b to get m_b.

To ensure that the sender knows nothing about the bit b, we require that pk_b is indistinguishable from random. Namely, we require that KGen outputs random-like public keys. This is met by many PKE schemes in practice.

To ensure that the receiver cannot obtain m_{1-b}, we require $\mathrm{Enc}(pk_{1-b}, m_{1-b})$, is indistinguishable from the encryption of zero $\mathrm{Enc}(pk_{1-b}, 0)$, which is exactly the standard semantic security[4] of PKE. This requirement is also fulfilled by many schemes in the literature.

4 Generic adaptive OT from verifiable shuffles

We now describe a generic construction of adaptive OT having fully-simulatable security. We first need some building blocks.

4.1 Building blocks

4.1.1 Threshold PKE

We need an 2-out-of-2 threshold PKE scheme TPKE, which consists of the following algorithms.

- TGen: Two parties S and R run a protocol so that they respectively obtain (pk, sk_S) and (pk, sk_R) where pk is the agreed public key and $sk_\mathrm{S}, sk_\mathrm{R}$ are the shares of secret key. (The public key is needed for all algorithms below, and we omit writing it for clarity.)
- $\mathrm{TEnc}(M; r)$: output a ciphertext C for a plaintext M and a random coin r.
- $\mathrm{TDec}(sk_\mathrm{P}, C)$: for $\mathrm{P} \in \{\mathrm{S}, \mathrm{R}\}$, output μ_P which is the decryption share of the ciphertext C under secret key sk_P.
- $\mathrm{TComb}(C, \mu_\mathrm{S}, \mu_\mathrm{R})$: output a plaintext M by combining the input $C, \mu_\mathrm{S}, \mu_\mathrm{R}$.

We require the following properties on the TPKE scheme.

Homomorphism: Namely,

$$\mathrm{TEnc}(M; r) \otimes \mathrm{TEnc}(M'; r') = \mathrm{TEnc}(M \oplus M'; r \odot r')$$

where $\otimes$, $\oplus$, $\odot$ are the operators on the corresponding spaces.

Semantic security: We require that for all M, the ciphertext $\mathrm{Enc}(M; r)$ for random r is (almost) uniformly distributed over the ciphertext space.

4.1.2 Verifiable shuffles

Consider a set of ciphertexts $C_i = \mathrm{TEnc}(M_i; r_i)$ for $1 \le i \le n$ of the TPKE scheme forming by S. Let I be the identity element of the message space. It is easy enough for R to choose a permutation π on $\{1, ..., n\}$, and random s_i to form the set of $C_i' = C_{\pi(i)} \otimes \mathrm{TEnc}(I; s_i)$ for $1 \le i \le n$, so that both sets of ciphertexts contain the same plaintexts. The set of C_i' $(1 \le i \le n)$ is called a shuffle of the original one. If the

scheme TPKE is semantically secure, publishing the shuffle $C_i'(1 \le i \le n)$ reveals nothing on the permutation π to S. Correctness of the shuffle is verified via the following protocol

$$\text{ZKPK}\{(\pi, s_i): C_i' = C_{\pi(i)} \otimes \text{TEnc}(I; s_i)\ \forall 1 \le i \le n\},$$

which has efficient implementations for homomorphic encryption schemes such as ElGamal or Paillier as shown in the work of Groth and Lu[7]. More generally, the results of Groth and Lu apply for homomorphic encryption schemes with the following properties:

Proper message space: requiring that the order of the message space does not have any small prime factor (say less than 2^{80}).

Root extraction: from $C^e = \text{TEnc}(M; R)$, it is possible to efficiently extract (m, r) such that $C = \text{TEnc}(m; r)$ for every e co-prime with the order of the message space.

The protocols for verifiable shuffles given in [7] are statistical strong honest verifier zero-knowledge (HVZK) arguments of three rounds, and can be turned into fully zero-knowledge by standard techniques.

4.2 Generic OT protocol

Initialization:

1. The sender S and the receiver R run the protocol TGen so that they obtain a common public key pk; and S gets secret key sk_S, R gets secret key sk_R. The receiver R proves in ZKPK that he knows sk_R corresponding to pk.
2. For $1 \le i \le n$, S computes and sends

   $$C_i = \text{TEnc}(M_i; r_i)$$

   to R where r_i are randomness used by TEnc.
3. The sender S then proves to R by ZKPK that he knows M_i for all i (this is equivalent to proving the knowledge of r_i in our below instantiations).
4. (**Shuffling**) The receiver R chooses a permutation π on $\{1, ..., n\}$ and randomness s_i for $1 \le i \le n$, and computes then sends to S for all i

   $$C_i' = C_{\pi(i)} \otimes \text{TEnc}(I; s_i),$$

   where I is the unit element of the message space.
5. The receiver R proves to S in ZKPK that he knows π and $s_i (1 \le i \le n)$ satisfying the equation at Step 4.

The j-th transfer:

1. The receiver R obtains an index σ as input, and sends $C = C'_{\pi^{-1}(\sigma)}$ to S.
2. The sender S checks

   $$C' \in \{C_1', ..., C_n'\}$$

   then computes and sends

   $$\mu_S = \text{TDec}(sk_S, C)$$

   to R.
3. The sender S then proves in ZKPM that he do the right decryption in the above step.
4. The receiver R himself computes the decryption share

   $$\mu_R = \text{TDec}(sk_R, C)$$

   and then obtaining M_σ by $\text{TComb}(pk, C, \mu_S, \mu_R)$.

The following result was established in [11] by Kurosawa, Nojima, and Phong. See [11] for a proof.

Theorem: The generic $\text{OT}^n_{k\times 1}$ from verifiable shuffles above is fully simulatable, if the TPKE scheme has semantic security.

4.3 Instantiations from DDH and linear assumptions

4.3.1 $\text{OT}^n_{k\times 1}$ from the DDH assumption

We will use the threshold ElGamal encryption scheme. The scheme works on a cyclic group $G = (G, g, q)$ where g is the generator of prime order q, and has semantic security under the DDH assumption on G.

- TGen: S chooses $sk_S = x_0 \leftarrow Z_q$, computes and sends $h_0 \leftarrow g^{x_0}$ to R. Similarly, R chooses $sk_R = x_1 \leftarrow Z_q$ and sends $h_1 \leftarrow g^{x_1}$ to S. The agreed public key is then $h = h_0 h_1$.
- $\text{TEnc}(M; r)$: Output

  $$C = (C[1], C[2]) = (g^r, M \cdot h^r)$$

  for $r \leftarrow Z_q$ and $M \in G$.
- $\text{TDec}(sk_P, C)$: Output $\mu_P = C[1]^{sk_P}$ for P is either S or R.

– TComb(C, μ_S, μ_R): Output $C[2]/(\mu_S\mu_R)$.

The TPKE scheme satisfies all requirements described in Section **4.1**. Thus we obtain the $OT^n_{k\times1}$ protocol from the threshold ElGamal encryption scheme. Since the threshold ElGamal encryption scheme has semantic security under the DDH assumption, thanks to the above theorem, the $OT^n_{k\times1}$ is fully-simulatable under the same assumption.

4.3.2 $OT^n_{k\times1}$ from the d-linear assumptions

We also works on $G=(G,g,q)$, and let us introduce some more notations. For vectors

$$v=(v[1],...,v[l])\in G^{1\times l}$$
$$u=(u[1],...,u[l])\in Z_q^{1\times l}$$

define

$$v\cdot u^{\intercal}=u\cdot v^{\intercal}=\prod_{i=1}^{l} v[i]^{u[i]}\in G.$$

Matrix-matrix and matrix-vector multiplications are defined in the same manner. Sometimes, the $\cdot$ operators are implicitly understood. Also recall that for $u,u'\in Z_q^{1\times l}$, we have $u+u'=(u[1]+u'[1],...,u[l]+u'[l])$ as normal. It is easy to check that $(u+u')\cdot v^{\intercal}=(u\cdot v^{\intercal})(u'\cdot v^{\intercal})\in G$,
and $v\cdot(u+u')^{\intercal}=(v\cdot u^{\intercal})(v\cdot u'^{\intercal})\in G$.

For $d\geq2$, the following PKE scheme, introduced by Naor and Segev[13], has semantic security under the d-linear assumption.

– Gen: $sk\leftarrow Z_q^{(d+1)\times1}$, $\varphi\leftarrow G^{d\times(d+1)}$. The secret key is sk, and the public key is $pk=(\varphi,\psi)$ for $\psi=\varphi\cdot sk\in G^{d\times1}$.
– Enc$(M;R)$: On message $M\in G$ and random $R\in Z_q^{1\times d}$ as input, output the ciphertext

  $$C=(R\varphi,(R\psi)M)\in G^{1\times(d+1)}\times G.$$

– Dec(sk,C): On input C and sk, output $C[2]/(C[1]\cdot sk)$.

  The correctness of the PKE scheme comes from the equation $(R\cdot\varphi)\cdot sk=R\cdot(\varphi\cdot sk)$. The semantic security of the PKE scheme implies that, given φ,ψ, the pair Enc$(1;R)=(R\varphi,R\psi)$ is indistinguishable from random over $G^{1\times(d+1)}\times G$.

  We now present the 2-out-of-2 threshold variant of the above PKE, which then results in an adaptive OT based on the decision linear assumption.

– TGen: The parties S and R, using G, agree on the matrix $\varphi\in G^{d\times(d+1)}$. They then choose secrets sk_S and sk_R respectively in $Z_q^{(d+1)\times1}$; S publishes $\psi_S=\varphi\cdot sk_S\in G^{d\times1}$ while R does the same with $\psi_R=\varphi\cdot sk_R\in G^{d\times1}$. The agreed common public key is φ,ψ_S,ψ_R in which

  $$\psi=\psi_S\psi_R=(\psi_S[1]\psi_R[1],...,\psi_S[d]\psi_R[d])^{\intercal}\in G^{d\times1}$$

  will be used in encryption. Note that $\psi=\varphi\cdot(sk_S+sk_R)$.
– TEnc$(M;R)$: Output

  $$C=\text{Enc}(M;R)=(R\varphi,(R\psi)M)\in G^{1\times(d+1)}\times G$$

– TDec(sk_P,C): Output

  $$\mu_P=C[1]\cdot sk_P\in G$$

  for $P\in\{S,R\}$.
– TComb(C,μ_S,μ_R): Output $C[2]/(\mu_S\mu_R)$.

Using the above scheme with the generic construction of OT, we obtain an instantiation fully simulatable under the decision linear assumption.

5 Conclusion

We have surveyed some techniques for building OT, which is theoretically seen as a fundamental ingredient for cryptography.

On the practical side, we expect that the techniques will be useful, in some ways, in developing privacy-friendly systems in cloud storage and computing.

There are still rooms for improvements and we hope to see better OT schemes in the future.

References

1 J. Camenisch, G. Neven, and A. Shelat, "Simulatable adaptive oblivious transfer," In M. Naor, editor, EUROCRYPT, Vol. 4515 of Lecture Notes in Computer Science, pp. 573–590, Springer, 2007.

2 S. Even, O. Goldreich, and A. Lempel, “A randomized protocol for signing contracts,” In CRYPTO, pp. 205–210, 1982.
3 Y. Gertner, S. Kannan, T. Malkin, O. Reingold, and M. Viswanathan, “The relationship between public key encryption and oblivious transfer,” In FOCS, pp. 325–335, 2000.
4 S. Goldwasser and S. Micali, “Probabilistic encryption,” J. Comput. Syst. Sci., 28(2): 270–299, 1984.
5 M. Green and S. Hohenberger, “Universally composable adaptive oblivious transfer,” In J. Pieprzyk, editor, ASIACRYPT, volume 5350 of Lecture Notes in Computer Science, pp. 179–197, Springer, 2008.
6 M. Green and S. Hohenberger, “Practical adaptive oblivious transfer from a simple assumption,” Cryptology ePrint Archive, Report 2010/109, 2010.
http://eprint.iacr.org/
7 J. Groth and S. Lu, “Verifiable shuffle of large size ciphertexts,” In T. Okamoto and X. Wang, editors, Public Key Cryptography, Vol. 4450 of Lecture Notes in Computer Science, pp. 377–392, Springer, 2007.
8 S. Jarecki and X. Liu, “Efficient oblivious pseudorandom function with applications to adaptive OT and secure computation of set intersection,” In O. Reingold, editor, TCC, Vol. 5444 of Lecture Notes in Computer Science, pp. 577–594, Springer, 2009.
9 K. Kurosawa and R. Nojima, “Simple adaptive oblivious transfer without random oracle,” In M. Matsui, editor, ASIACRYPT, Vol. 5912 of Lecture Notes in Computer Science, pp. 334–346, Springer, 2009.
10 K. Kurosawa, R. Nojima, and L. T. Phong “Efficiency-improved fully simulatable adaptive ot under the DDH assumption,” In J. A. Garay and R. D. Prisco, editors, SCN, Vol. 6280 of Lecture Notes in Computer Science, pp. 172–181, Springer, 2010.
11 K. Kurosawa, R. Nojima, and L. T. Phong, “Generic fully simulatable adaptive oblivious transfer,” In 9th International Conference on Applied Cryptography and Network Security (ACNS ’11), 2011. To appear.
12 M. Naor and B. Pinkas, “Oblivious transfer with adaptive queries,” In M. J. Wiener, editor, CRYPTO, Vol. 1666 of Lecture Notes in Computer Science, pp. 573–590, Springer, 1999.
13 M. Naor and G. Segev, “Public-key cryptosystems resilient to key leakage,” In S. Halevi, editor, CRYPTO, Vol. 5677 of Lecture Notes in Computer Science, pp. 18–35, Springer, 2009. Full version available at http://eprint.iacr.org/2009/105.pdf
14 C. A. Neff, “A verifiable secret shuffle and its application to e-voting,” In ACM Conference on Computer and Communications Security, pp. 116–125, 2001.
15 W. Ogata and K. Kurosawa, “Oblivious keyword search,” J. Complexity, 20(2-3): 356–371, 2004. Also available at http://eprint.iacr.org/2002/182

(Accepted June 15, 2011)

Le Trieu Phong, *Ph.D.*
Expert Researcher, Security Fundamentals Laboratory, Network Security Research Institute
Cryptographic Protocol
phong@nict.go.jp