Simple Adaptive Oblivious Transfer Without Random Oracle

Kaoru Kurosawa and Ryo Nojima

[1] Ibaraki University, Japan
[2] NICT, Japan

Abstract. Adaptive oblivious transfer (adaptive OT) schemes have wide applications such as oblivious database searches, secure multiparty computation and etc. It is a two-party protocol which simulates an ideal world such that the sender sends $M_1, \cdots, M_n$ to the trusted third party (TTP) first, and then the receiver receives M_{σ_i} from TTP adaptively for $i = 1, 2, \cdots k$. In the standard model, however, the fully simulatable schemes known so far had to rely on dynamic assumptions such as q-strong DH assumption, q-PDDH assumption and q-hidden LRSW assumption.
This paper shows two fully simulatable adaptive OT schemes which do not rely on dynamic assumptions in the standard model. Our first scheme holds under the DDH assumption and our second scheme holds under the Paillier's decisional Nth residuosity assumption, respectively.

Keywords: Adaptive OT, Fully Simulatable, DDH, Standard Model

1 Introduction

The basic 1-out-of-2 oblivious transfer [6], OT^2_1, is a two-party protocol which realizes the ideal world such that the sender sends two strings M_0 and M_1 to the trusted third party (TTP), and the receiver receives M_σ from TTP, where $\sigma \in \{0, 1\}$. Note that the sender learns nothing on σ, and the receiver learns nothing on $M_{1-\sigma}$. Non-adaptive k-out-of-n oblivious transfer, OT^n_k, is defined similarly [1, 15]. Efficient OT schemes are important because OT^4_1 is a key building block for secure multi-party computation [21, 9, 12].

Adaptive k-out-of-n oblivious transfer, denoted by $OT^n_{k\times 1}$, was introduced by Naor and Pinkas [16]. In the ideal world of this model, the sender sends $M_1, \cdots, M_n$ to TTP, and the receiver receives M_{σ_i} adaptively from TTP, where the choice index σ_{i+1} can depend on $M_{\sigma_1}, \cdots, M_{\sigma_i}$.

On the definition of security, only half simulatability (for both non-adaptive and adaptive) was considered until recently [16, 17, 11, 19]. This definition requires that for any receiver R in the real world, there exists a receiver $\hat{R}$ in the ideal world such that the outputs of R and $\hat{R}$ are indistinguishable. For the receiver's privacy, it is only required that the view of the sender must be indistinguishable for any input to the receiver. Note that the honest sender outputs nothing in $OT^n_{k\times 1}$. However, Naor and Pinkas noticed that there can be a practical attack on the receiver's privacy in a half simulatable adaptive OT [16].

To solve this problem, Camenisch, Neven and shelat formalized a notion of full simulatability [5]. In this definition, we consider the output of the sender as well. For example, a malicious sender may output its view in the execution of the protocol. Full simulatability now requires that, in addition to half simulatability, for any sender S in the real world, there exists a sender $\hat{S}$ in the ideal world such that $(\hat{S}_{out}, \hat{R}_{out})$ is indistinguishable from (S_{out}, R_{out}), where A_{out} denotes the output of A. Then they showed a fully simulatable adaptive OT in the random oracle model, and one in the standard model, respectively.

We focus on the standard model in this paper. Then all the constructions of fully simulatable adaptive OT known so far rely on dynamic assumptions (which depend on n). The scheme of Camenisch et al. relies on q-strong DH assumption and q-PDDH assumption. The scheme of Green and Hohenberger relies on q-hidden LRSW assumption [8]. The scheme of Jarecki and Liu proposed relies on the decisional q-DHI assumption [10]. [1]

On the other hand, Lindell showed a fully simulatable OT^2_1 under DDH, Paillier's decisional Nth residuosity, and qudratic residuosity assumptions as well as under the assmption that homomorphic encryption exists in the standard model [14].

This paper shows two fully simulatable adaptive OT schemes in the standard model which do not rely on dynamic assumptions. Our first scheme holds under the DDH assumption and our second scheme holds under the Paillier's decisional Nth residuosity assumption (DCNR assumption), respectively. They are very simple and efficient. In each scheme, the initialization phase and each transfer phase are constant round protocols. Hence the total round complexity is proportional to k.

While the previous schemes use signature scheme as a building block, our first scheme uses ElGamal encryption scheme, and our second scheme uses Paillier's encryption scheme, respectively. (Hence we do not need a bilinear map.) As a special case, we obtain more efficient fully simulatable OT^2_1s than Lindell [14].

Finally we show an extension of our schemes to constant round non-adaptive OT^n_ks, where the choice index σ_{i+1} cannot depend on $M_{\sigma_1}, \cdots, M_{\sigma_i}$. Green and Hohenberger showed a fully simulatable non-adaptive OT^n_k under the decisional BDH assumption in the standard model [7]. Note that, on the other hand, our first OT^n_k relies on the DDH assumption, and our second OT^n_k relies on the DCNR assumption.

2 Preliminaries

2.1 Notations

In this paper, we denote a security parameter by $\tau \in \mathbb{N}$. All the algorithms take τ as the first input and run in (expected) polynomial-time in τ. We denote prob-

[1] In the random oracle model, Ogata and Kurosawa showed an adaptive OT based on Chaum's blind signature scheme [19]. Camenisch, Neven and shelat [5] proved that it is fully simulatable as well as they corrected a flaw of [19]. Green and Hohenberger showed such a scheme under the decisional BDH assumption [7].

Table 1. Fully simulatable adaptive OT without RO

Camenisch et al. [5]	q-strong DH assumption and q-PDDH assumption
Green and Hohenberger [8]	q-hidden LRSW assumption
Jarecki and Liu [10]	q-DHI assumption
Proposed (1)	DDH assumption
Proposed (2)	Paillier's DCNR assumption

abilistic polynomial-time by PPT for short. We often do not write the security parameter explicitly.

2.2 Proof Systems

To design our scheme, we use several proof systems. We follow the definitions described in [3–5].

Let $R = \{(\alpha, \beta)\} \subseteq \{0,1\}^* \times \{0,1\}^*$ be a binary relation R such that $|\beta| \leq \text{poly}(\alpha)$ for all $(\alpha, \beta) \in R$, where poly is some polynomial. We only consider the relation R such that $(\alpha, \beta) \in R$ can be decided in polynomial in $|\alpha|$ for all (α, β). We define $L_R = \{\alpha \mid \exists \beta \text{ such that } (\alpha, \beta) \in R\}$.

Proof of Membership (PoM): A pair of interacting algorithms (P, V), called a *prover* and a *verifier*, is a *proof of membership* (PoM) for a relation R if the *completeness* and *soundness* are satisfied. Here, we say that (P, V) satisfies the completeness if for all $(\alpha, \beta) \in R$, the probability of $\mathsf{V}(\alpha)$ accepting a conversation with $\mathsf{P}(\alpha, \beta)$ is 1. Also we say that (P, V) satisfies the soundness if for all $\alpha \notin L_R$ and all $\mathsf{P}^*(\alpha)$ (including cheating provers), the probability of $\mathsf{V}(\alpha)$ accepting the conversation with P^* is negligible in $|\alpha|$. We say that this probability as *soundness error* of the proof system.

Proof of Knowledge (PoK): We say a pair of interacting algorithms (P, V) is PoK for a relation R with knowledge error $\kappa \in [0, 1]$ if it satisfies completeness described above and has an expected polynomial-time algorithm, called *knowledge extractor*, E. The algorithm E is a knowledge extractor for a relation R if possibly cheating $\widehat{\mathsf{P}}$ has probability ϵ of convincing V to accept α, then E, when given black-box access to $\widehat{\mathsf{P}}$, outputs a witness β for α with probability $\epsilon - \kappa$.

Witness Indistinguishability (WI): A proof system (P, V) is *perfect* WI if for every $(\alpha, \beta_1), (\alpha, \beta_2) \in R$, and any PPT cheating verifier, the output of $\widehat{\mathsf{V}}(\alpha)$ (including cheating verifier) after interacting with $\mathsf{P}(\beta_1)$ and that of $\widehat{\mathsf{V}}(\alpha)$ after interacting with $\mathsf{P}(\beta_2)$ are identically distributed.

Zero Knowledge (ZK): We say that a proof system (P, V) is *perfect* ZK if there exists an expected polynomial-time algorithm Sim, called a *simulator*, such that for any PPT cheating verifier $\widehat{\mathsf{V}}$ and any $(\alpha, \beta) \in R$, the outputs of $\widehat{\mathsf{V}}(\alpha)$ after interacting with $\mathsf{P}(\beta)$ and that of $\mathsf{Sim}^{\mathsf{V}(\alpha)}(\alpha)$ are identically distributed.

3 k-out-of-n Oblivious Transfer

We consider a weak model of UC framework as follows.

- At the beginning of the game, an adversary A can corrupt either a sender S or a receiver R, but not both.
- A can send a message (which will be denoted by A_{out}) to an environment $\mathcal{Z}$ after the end of the protocol. (A cannot communicate with $\mathcal{Z}$ during the protocol execution.)

The ideal functionalities of OT_k^n and $\mathrm{OT}_{k\times 1}^n$ will be shown below. For a protcol $\pi = (\mathsf{S}, \mathsf{R})$, define $\mathtt{Adv}(\mathcal{Z})$ as

$$\mathtt{Adv}(\mathcal{Z}) = |\Pr(\mathcal{Z} = 1 \text{ in the real world}) - \Pr(\mathcal{Z} = 1 \text{ in the ideal world})|$$

3.1 Non-Adaptive k-out-of-n Oblivious Transfer

In the ideal world of OT_k^n, the ideal functionality $\mathcal{F}_{non}$, an ideal world adversary A' and an environment $\mathcal{Z}$ behave as follows.

The initialization phase:

1. An environment $\mathcal{Z}$ sends $(M_1, \cdots, M_n)$ to the dummy sender S'.
2. S' sends $(M_1^*, \cdots, M_n^*)$ to $\mathcal{F}_{non}$, where $(M_1^*, \cdots, M_n^*) = (M_1, \cdots, M_n)$ if S' is not corrupted.

The transfer phase:

1. $\mathcal{Z}$ sends $(\sigma_1, \cdots, \sigma_k)$ to the dummy receiver R', where $1 \le \sigma_i \le n$.
2. R' sends $(\sigma_1^*, \cdots, \sigma_k^*)$ to $\mathcal{F}_{non}$, where $(\sigma_1^*, \cdots, \sigma_k^*) = (\sigma_1, \cdots, \sigma_k)$ if R' is not corrupted.
3. $\mathcal{F}_{non}$ sends `received` to an ideal process adversary A'.
4. A' sends $b = 1$ or 0 to $\mathcal{F}_{non}$, where $b = 1$ if S' is not corrupted.
5. $\mathcal{F}_{non}$ sends Y to R', where
$$Y = \begin{cases} (M_{\sigma_1}^*, \cdots, M_{\sigma_k}^*) & if\ b = 1 \\ \perp & if\ b = 0 \end{cases}$$
6. R' sends Y to $\mathcal{Z}$.

After the end of the protocol, A' sends a message A'_{out} to $\mathcal{Z}$. Finally $\mathcal{Z}$ outputs 1 or 0.

In the real world, a protocol (S, R) is executed without $\mathcal{F}_{non}$, where the environment $\mathcal{Z}$ and a real world adversary A behave in the same way as above.

Definition 1. *We say that (S, R) is secure against the sender (receiver) corruption if for any real world adversary A who corrupts the sender S (the receiver R), there exists an ideal world adversary A' who corrupts the dummy sender S' (the dummy receiver R') such that for any environment $\mathcal{Z}$, $\mathtt{Adv}(\mathcal{Z})$ is negligible.*

Definition 2. *We say that (S, R) is a fully simulatable OT_k^n if it is secure against the sender corruption and the receiver corruption.*

3.2 Adaptive k-out-of-n Oblivious Transfer

In the ideal world of $\mathrm{OT}^n_{k\times 1}$, the ideal functionality $\mathcal{F}_{adapt}$, an ideal world adversary A' and an environment $\mathcal{Z}$ behave as follows.

The initialization phase:

1. An environment $\mathcal{Z}$ sends $(M_1, \cdots, M_n)$ to the dummy sender S'.
2. S' sends $(M_1^*, \cdots, M_n^*)$ to $\mathcal{F}_{adapt}$, where $(M_1^*, \cdots, M_n^*) = (M_1, \cdots, M_n)$ if S' is not corrupted.

The transfer phase: for $i = 1, \cdots, k$,

1. $\mathcal{Z}$ sends σ_i to the dummy receiver R', where $1 \leq \sigma_i \leq n$.
2. R' sends σ_i^* to $\mathcal{F}_{adapt}$, where $\sigma_i^* = \sigma_i$ if R' is not corrupted.
3. $\mathcal{F}_{adapt}$ sends `received` to an ideal process adversary A'.
4. A' sends $b = 1$ or 0 to $\mathcal{F}_{adapt}$, where $b = 1$ if S' is not corrupted.
5. $\mathcal{F}_{adapt}$ sends Y_i to R', where

$$Y_i = \begin{cases} M^*_{\sigma_i} & if\ b = 1 \\ \perp & if\ b = 0 \end{cases}$$

6. R' sends Y_i to $\mathcal{Z}$.

After the end of the protocol, A' sends a message A'_{out} to $\mathcal{Z}$. Finally $\mathcal{Z}$ outputs 1 or 0.

In the real world, a protocol (S, R) is executed without $\mathcal{F}_{adapt}$, where the environment $\mathcal{Z}$ and a real world adversary A behave in the same way as above.

Definition 3. *We say that (S, R) is secure against the sender (receiver) corruption if for any real world adversary A who corrupts the sender S (the receiver R), there exists an ideal world adversary A' who corrupts the dummy sender S' (the dummy receiver R') such that for any environment $\mathcal{Z}$, $\mathtt{Adv}(\mathcal{Z})$ is negligible.*

Definition 4. *We say that (S, R) is a fully simulatable $OT^n_{k\times 1}$ if it is secure against the sender corruption and the receiver corruption.*

3.3 Remarks

The full simulation security of OT^n_k has never been defined (even in [7]).

On the full simulation security of $\mathrm{OT}^n_{k\times 1}$, our definition is weaker than the UC security because our adversaries A cannot communicate with $\mathcal{Z}$ during the protocol execution.

On the other hand, it is stronger than that of [5] because $\mathcal{Z}$ chooses σ_i in our definition. Hence σ_i can depend on $(M_1, \cdots, M_n)$. In the definition of [5], σ_i can depend on $(M_{\sigma_1}, \cdots, M_{\sigma_{i-1}})$ only because the receiver chooses σ_i.

4 Our $\mathrm{OT}^n_{k\times 1}$ Based on ElGamal

In this section, we show an adaptive $\mathrm{OT}^n_{k\times 1}$ based on ElGamal encryption scheme, and prove its full simulatability under the DDH assumption.

Let $\mathbb{G}$ be a multiplicative group of prime order q. Then the DDH assumption states that, for every PPT distinguisher D,

$$\epsilon_{\mathrm{DDH}}(\mathsf{D}) = |\Pr(\mathsf{D}(g, g^\alpha, g^\beta, g^{\alpha\beta}) = 1) - \Pr(\mathsf{D}(g, g^\alpha, g^\beta, g^\gamma) = 1)|$$

is negligible, where the probability is taken over the random bits of D, the random choice of the generator g, and the random choice of $\alpha, \beta, \gamma \in \mathbb{Z}_q$. We denote

$$\epsilon_{\mathrm{DDH}} = \max\{\epsilon_{\mathrm{DDH}}(\mathsf{D})\},$$

where the maximum is taken over all PPT distinguishers D.

The initialization phase and each transfer phase are constant round protocols. Hence the total round complexity is proportional to k.

Initialization Phase

1. The sender chooses $\mathbb{G}$, g and $(x_1, \cdots, x_n, r) \in (\mathbb{Z}_q)^{n+1}$ randomly, and computes $h = g^r$.
2. For $i = 1, \cdots, n$, the sender computes
$$C_i = (A_i, B_i) = (g^{x_i}, M_i \cdot h^{x_i}).$$
In loss of generality, we assume that $M_1, \cdots, M_n \in \mathbb{G}$.
3. The sender sends $(\mathbb{G}, h, C_1, \cdots, C_n)$.
4. The sender proves by ZK-PoK that he knows r.
The protocol stops if the receiver rejects.

The jth Transfer Phase

1. The receiver chooses a choice index $1 \le \sigma_j \le n$ based on $M_{\sigma_1}, \cdots, M_{\sigma_{j-1}}$.
2. The receiver chooses $u \in \mathbb{Z}_q$ randomly and computes $U = (A_{\sigma_j})^u$.
He then sends U.
3. The receiver proves in WI-PoK that he knows u such that
$$U = A_1^u \vee \cdots \vee U = A_n^u.$$
The protocol stops if the sender rejects.
4. The sender computes $V = U^r$ and sends V.
5. The sender proves that (g, h, U, V) in ZK-PoM that it is a DDH-tuple.
The protocol stops if the reeiver rejects.
6. The receiver obtains M_{σ_j} by computing $B_{\sigma_j}/V^{1/u}$.

There are three proof systems employed in this scheme. The first proof system can be obtained by transforming the Schnorr's identification scheme [20] into perfect ZK-PoK with [3]. The second proof system is implemented by the or-composition [4] of [20]. The third one comes from the Chaum's ZK-PoM for the DDH-tuple [2]. Note that all of these proof systems run in the constant round. More precisely, these systems are four-round, three-round, and four-round protocols, respectively.

Theorem 1. *The above protocol is a fully-simulatable adaptive* $OT^n_{k\times 1}$ *under the DDH assumption.*

The proof is included in Section 7. We use a simple fact that given $(g, h, g^{x_1}, \cdots, g^{x_n})$, it is hard to distinguish $(h^{x_1}, \cdots, h^{x_n})$ from $(g^{z_1}, \cdots, g^{z_n})$, where $z_1, \cdots, z_n$ are random. Similar observation can be found in [18, 13]. In fact, we use [18] to prove the security.

5 Our $\mathrm{OT}^n_{k\times 1}$ Based on Paillier

In this section, we show an adaptive $\mathrm{OT}^n_{k\times 1}$ based on Paillier encryption scheme, and prove its full simulatability under the Decisional Composite Nth Residuosity (DCNR) assumption. The DCNR assumption is stated as follows. Let $N = pq$ where p and q are large primes. Then given N, it is hard to distinguish between $\mathbb{Z}^*_{N^2}$ and $\{y \mid y = x^N \bmod N^2, \text{ where } x \in \mathbb{Z}^*_N\}$.

The initialization phase and each transfer phase are constant round protocols. Hence the total round complexity is proportional to k.

5.1 Scheme

Initialization Phase

1. The sender chooses two large primes p, q and computes $N = pq$.
2. For $i = 1, \cdots, n$, the sender chooses $r_i \in \mathbb{Z}^*_N$ randomly and computes
$$C_i = r_i^N (1 + M_i N) \bmod N^2$$
where $M_1, \cdots, M_n \in \mathbb{Z}^*_N$.
3. The sender sends $(N, C_1, \cdots, C_n)$.
4. The sender proves by ZK-PoM that $f_N(x) = x^N \bmod N$ is bijective. The protocol stops if the receiver rejects.
5. For each C_i, the sender proves by ZK-PoK that he knows r_i such that
$$C_i = r_i^N \bmod N.$$
The protocol stops if the receiver rejects.

The jth Transfer Phase

1. The receiver chooses a choice index $1 \leq \sigma_j \leq n$ based on $M_{\sigma_1}, \cdots, M_{\sigma_{j-1}}$.
2. The receiver chooses u randomly and computes $U = u^N \cdot C_{\sigma_j} \bmod N$.
3. The receiver sends U.
4. The receiver proves in WI-PoK that he knows u such that
$$(U = u^N C_1 \bmod N) \vee \cdots \vee (U = u^N C_n \bmod N).$$
The protocol stops if the sender rejects.
It is easy to construct a 3-round WI-PoK protocol for this based on [4].
5. The sender computes $V = U^{1/N} \bmod N$ and, then computes T such that
$$V^N = U + TN \bmod N^2 \tag{1}$$
6. The sender sends T, and proves that she knows V satisfying eq.(1) in ZK-PoK. The protocol stops if the receiver rejects.
We can construct a 4-round ZK-PoK protocol for this based on [3]. Note that it holds that
$$\begin{aligned} U + TN &= V^N \bmod N^2 \\ &= (ur_{\sigma_j})^N \bmod N^2 \\ &= u^N r_{\sigma_j}^N \bmod N^2. \end{aligned}$$
7. The receiver computes
$$r_{\sigma_j}^N = (U + TN)/u^N \bmod N^2.$$
He finally computes M_{σ_j} from C_{σ_j} and $r_{\sigma_j}^N \bmod N^2$.

In the next subsections, we show a 4-round ZK-PoM and a 4-round ZK-PoK which are used in the initialization phase.

Theorem 2. *The above protocol is a fully-simulatable adaptive* $OT_{k\times 1}^N$ *under the DCNR assumption.*

The proof is similar to that of Theorem 1.

5.2 4-round ZK-PoK for $C_i = r_i^N \bmod N$

We show a Σ-protocol (P, V) for an NP relation R_t such that
$$R_t = \{((y_1, \cdots, y_t), (x_1, \cdots, x_t)) \mid y_i = x_i^N \bmod N \text{ for all } i\}.$$

1. P chooses $r_1, \cdots, r_t \in \mathbb{Z}_N^*$ randomly and computes
$$a_1 = r_1^N \bmod N, \cdots, a_t = r_t^N \bmod N.$$
P sends $a_1, \cdots, a_t$ to V.
2. V sends a random $c \in \mathbb{Z}_N^*$ to P.
3. P computes $d_i = r_i x_i^c \bmod N$ for $i = 1, \cdots, t$, and sends $d_1, \cdots, d_t$ to V.
4. V accepts iff $d_i^N = a_i y_i^c \bmod N$ for $i = 1, \cdots, t$.

It is easy to see that the above protocol satisfies special soundness and special HVZK. Hence we can obtain an efficient 4-round ZK-PoK for R_t from [3].

At step 5 of the initialization phase, we use this 4-round ZK-PoK with $t = n$.

5.3 How to Prove that $f_N(x) = x^N \bmod N$ is Bijective

Let $d = \gcd(N, \phi(N))$, where ϕ is Euler function. Then $f_N = x^N \bmod N$ is bijective over $\mathbb{Z}_N^*$ if and only if $d = 1$. In other words, f_N is not bijective over $\mathbb{Z}_N^*$ if and only if $d \geq 2$. Also, each y such that $y = x^N \bmod N$ for some x has d Nth roots.

Based on this observation, we show a 4-round ZK-PoM which proves that f_N is bijective over $\mathbb{Z}_N^*$. The common input to (P, V) is N.

1. V chooses $x_1, \cdots, x_t \in \mathbb{Z}_N^*$ randomly and computes
$$y_1 = x_1^N \bmod N, \cdots, y_t = x_t^N \bmod N.$$
V sends $y_1, \cdots, y_t$ to P.
2. V proves that he knows each x_i by using the Σ-protocol of Sec.5.2.
3. P sends $x'_1, \cdots, x'_t$ to V.
4. V accepts iff $x'_i = x_i$ for $i = 1, \cdots, t$.

The completeness is clear. If f_N is not bijective, then $\Pr(\mathsf{V} \text{ accepts}) \leq 1/2^t$. Finally it is easy to prove the zero-knowledgeness.

6 Extension to Constant Round Non-Adaptive OT_k^n

It is easy to extend our $\mathrm{OT}_{k\times 1}^n$s to constant round non-adaptive OT_k^ns. In this section, we show a constant round non-adaptive OT_k^n based on ElGamal.

6.1 How to Prove Many DDH-tuples

We show a 4-round ZK-PoM which proves that $(g, h, U_1, V_1), \cdots, (g, h, U_k, V_k)$ are all DDH-tuples.

1. The receiver sends random $(a_1, \cdots, a_k)$.
2. The sender proves that $(g, h, \prod_{i=1}^k U_i^{a_i}, \prod_{i=1}^k V_i^{a_i})$ is a DDH-tuple by using the confirmation protocol of [2].

The confirmation protocol of [2] is a 4-round ZK-PoM on a DDH-tuple. Hence the above protocol runs in 4-round. (Step 1 and the 1st round of the confirmation protocol are merged.)

Lemma 1. *Suppose that some (g, h, U_i, V_i) is not a DDH-tuples. Then $(g, h, \prod_{i=1}^k U_i^{a_i}, \prod_{i=1}^k V_i^{a_i})$ is a DDH-tuples with negligible probability.*

Proof. Assume that $U_i = g^{x_i}$ and $V_i = h^{y_i}$ for $i = 1, \cdots, k$. Then

$$\prod_{i=1}^{k} U_i^{a_i} = g^{\;{}_{i=1}^{k} a_i x_i}$$
$$\prod_{i=1}^{k} V_i^{a_i} = h^{\;{}_{i=1}^{k} a_i y_i}$$

Suppose that (g, h, U_1, V_1) is not a DDH-tuples. That is, $x_1 \neq y_1$. Then for any values of $a_2, \cdots, a_k$, there exists a unique a_1 such that

$$\sum_{i=1}^{k} a_i(x_i - y_i) = 0 \bmod q. \tag{2}$$

Hence the numbers of $(a_1, \cdots, a_k)$ which satisfies eq.(2) is equal to q^{k-1}. Therefore

$$\Pr(\text{eq.(2) holds}) = q^{k-1}/q^k = 1/q.$$

This means that $(g, h, \prod_{i=1}^{k} U_i^{a_i}, \prod_{i=1}^{k} V_i^{a_i})$ is a DDH-tuples with negligible probability. □

Theorem 3. *The above protocol is a ZK-PoM on many DDH-tuples.*

Proof. The completeness is clear. The zero-knowledgeness follows from that of the confirmation protocol of [2]. The soundness follows from Lemma 1 and that of the confirmation protocol of [2]. □

6.2 Constant Round OT_k^n

In this section, we modify our $\mathrm{OT}_{k\times 1}^n$ to obtain a constant round OT_k^n as follows.

- At step 4 of the initialization phase, the sender sends $(\mathbb{G}, h, A_1, \cdots, A_n)$.
- At the end of the transfer phase, the sender sends $(B_1, \cdots, B_n)$.
- In the transfer phase, run step 3 in parallel (still it is a WI protocol).
  At step 5, the sender proves that $(g, h, U_1, V_1), \cdots, (g, h, U_k, V_k)$ are all DDH-tuples by using the ZK-PoM of Sec.6.1.

Theorem 4. *The proposed OT_k^n is a constant round fully-simulatable* OT_k^n *under the DDH assumption.*

The proof is similar to that of Theorem 1.

7 Proof of Theorem 1

We first prove that the proposed scheme is secure against sender corruption. We next prove that it is secure against receiver corruption.

7.1 Security Against Sender Corruption

Lemma 2. *The proposed scheme is secure against sender corruption.*

Proof. For every real-world adversary A who corrupts the sender, we construct an ideal-world adversary A' such that $\mathtt{Adv}(\mathcal{Z})$ is negligible.

We will consider a sequence of games $\mathtt{Game}_0, \mathtt{Game}_1, \cdots, \mathtt{Game}_4$, where $\mathtt{Game}_0$ is the real world experiment of Sec.3, and and $\mathtt{Game}_4$ is the ideal world experiment, respectively. Let

$$\Pr(\textsc{Game}_i) = \Pr(\mathcal{Z} = 1 \text{ in } \texttt{Game}_i).$$

$\texttt{Game}_0$: This is the real world experiment such that the sender is controlled by an adversary A. Hence

$$\Pr(\textsc{Game}_0) = \Pr(\mathcal{Z} = 1 \text{ in the real world}).$$

$\texttt{Game}_1$: This is the same as the previous game except for the following. In the initialization phase, if the receiver accepts the ZK-PoK, then he extracts r from A by running the knowledge extractor E_1 which is allowed to rewind A. This game outputs $\perp$ if the extractor E_1 fails in extracting r. Unless this happens, these two games are identical. Therefore,

$$|\Pr(\textsc{Game}_0) - \Pr(\textsc{Game}_1)| \leq \kappa_1,$$

where κ_1 be the knowledge error of the extractor.

$\texttt{Game}_2$: This is the same as the previous game except for the following. In each transfer phase, if the receiver accepts the ZK-PoM which proves that (g, h, U, V) is a DDH-tuple, then he obtains M_{σ_i} by computing $B_{\sigma_i}/A_{\sigma_i}^r$. These two games are identical unless the above M_{σ_i} is different from $B_{\sigma_j}/V^{1/u}$. This happnes if the receiver accepts the ZK-PoM even though (g, h, U, V) is not a DDH-tuple. Hence

$$|\Pr(\textsc{Game}_1) - \Pr(\textsc{Game}_2)| \leq k\kappa_3,$$

where κ_3 is the soundness error probability of ZK-PoM.

$\texttt{Game}_3$: This is the same as the previous game except for the following. In each transfer phase, the receiver computs U as $U = A_1^u$. (The receiver can still obtain M_{σ_i} as can be seen from $\texttt{Game}_2$.) Since our WI-PoK is perfect,

$$\Pr(\textsc{Game}_2) = \Pr(\textsc{Game}_3).$$

$\texttt{Game}_4$: This game is the ideal world experiment in which an ideal-world adversary A' plays the role of the receiver of $\texttt{Game}_3$ and uses A as a blackbox. A' can do this because the receiver does not use $\sigma_1, \cdots, \sigma_k$ in $\texttt{Game}_3$.

Finally A' outputs what A outputs. It is easy to see that $\texttt{Game}_3$ and $\texttt{Game}_4$ are identical from a view point of $\mathcal{Z}$. Hence

$$\Pr(\textsc{Game}_3) = \Pr(\textsc{Game}_4).$$

Further

$$\Pr(\textsc{Game}_4) = \Pr(\mathcal{Z} = 1 \text{ in the ideal world}).$$

Now, we can summarize this lemma as follows:

$$\begin{aligned}\mathtt{Adv}(\mathcal{Z}) &= |\Pr(\textsc{Game}_4) - \Pr(\textsc{Game}_0)| \\ &\leq \sum_{i=0}^{3} |\Pr(\textsc{Game}_{i+1}) - \Pr(\textsc{Game}_i)| \\ &\leq \kappa_1 + k\kappa_3.\end{aligned}$$

□

7.2 Security Against Receiver Corruption

Lemma 3. *The proposed scheme is secure against receiver corruption under the DDH assumption.*

Proof. For every real-world adversary A who corrupts the receiver, we construct an ideal-world adversary A' such that $\mathtt{Adv}(\mathcal{Z})$ is negligible.

We will consider a sequence of games $\mathtt{Game}_0$, $\mathtt{Game}_1, \cdots$, $\mathtt{Game}_5$, where $\mathtt{Game}_0$ is the real world experiment of Sec.3, and $\mathtt{Game}_5$ is the ideal world experiment.

$\mathtt{Game}_0$: This is the real world experiment such that the receiver is controlled by an adversary A. Hence

$$\Pr(\textsc{Game}_0) = \Pr(\mathcal{Z} = 1 \text{ in the real world}).$$

$\mathtt{Game}_1$: This is the same as the previous game except for the following. In each transfer phase, instead of running the ZK-PoM which proves that (g, h, U, V) is a DDH-tiple, the sender runs the zero-knowledge simulator of the ZK-PoM which is allowed to rewind A. Since the ZK-PoM is perfect ZK, we have

$$\Pr(\textsc{Game}_1) = \Pr(\textsc{Game}_0).$$

$\mathtt{Game}_2$: This is the same as the previous game except for the following. In each transfer phase, if the sender accepts the WI-PoK, then she extracts u from A by running the knowledge extractor E_2 which is allowed to rewind A. This game outputs $\perp$ if the extractor E_2 fails in extracting u. Unless this happens, these two games are identical. Therefore,

$$|\Pr(\textsc{Game}_2) - \Pr(\textsc{Game}_1)| \leq k\kappa_2,$$

where κ_2 is the knowledge error of the extractor.

$\mathtt{Game}_3$: This is the same as the previous game except for that the sender computes V as $V = (B_\sigma/M_\sigma)^u$ instead of $V = U^r$. It is clear that there is no essential difference between two games. Therefore,

$$\Pr(\textsc{Game}_3) = \Pr(\textsc{Game}_2).$$

$\texttt{Game}_4$: This is the same as the previous game except for that the sender uses a random M_i' to compute each C_i in the initialization phase. The difference $|\Pr(\text{Game}_4) - \Pr(\text{Game}_3)|$ is still negligible by the semantic security of the ElGamal cryptosystem which is implied by the DDH assumption.

Claim. If the DDH problem is hard then $|\Pr(\text{Game}_4) - \Pr(\text{Game}_3)|$ is negligible. More concretely,

$$|\Pr(\text{Game}_4) - \Pr(\text{Game}_3)| \leq \epsilon_{\text{DDH}}. \tag{3}$$

The proof of this claim is given later.

$\texttt{Game}_5$: This game is the ideal world experiment in which an ideal-world adversary A' plays the role of the sender of $\texttt{Game}_4$, and uses A as a blackbox. A' can do this because the sender does not use $M_1, \cdots, M_n$ in $\texttt{Game}_4$.

Finally A' outputs what A outputs. It is easy to see that $\texttt{Game}_4$ and $\texttt{Game}_5$ are identical from a view point of $\mathcal{Z}$. Hence

$$\Pr(\text{Game}_4) = \Pr(\text{Game}_5).$$

Further

$$\Pr(\text{Game}_5) = \Pr(\mathcal{Z} = 1 \text{ in the ideal world}).$$

Now, we can summarize this lemma as follows:

$$\begin{aligned}
\texttt{Adv}(\mathcal{Z}) &= |\Pr(\text{Game}_5) - \Pr(\text{Game}_0)| \\
&\leq \sum_{i=0}^{4} |\Pr(\text{Game}_{i+1}) - \Pr(\text{Game}_i)| \\
&\leq k\kappa_2 + \epsilon_{\text{DDH}}.
\end{aligned}$$

□

To complete the proof, we must provide the proof of the claim. To do so, we need the following lemma [2] which can be thought of as an "extended" version of the DDH assumption.

Lemma 4 (Lemma 4.2 in [18]). *If there exists a probabilistic algorithm* D *with running time* t *such that*

$$\Big| \Pr\left(\mathsf{D}(g, g^r, g^{x_1}, \cdots, g^{x_n}, g^{rx_1}, \cdots, g^{rx_n}) = 1\right) \\ - \Pr(\mathsf{D}(g, g^r, g^{x_1}, \cdots, g^{x_n}, g^{z_1}, \cdots, g^{z_n}) = 1) \Big| \geq \epsilon$$

where the probability is taken over the random bits of D*, the random choice of the generator* g *in* $\mathbb{G}$*, and the random choice of* $x_1, \cdots, x_n, r, z_1, \cdots, z_n \in \mathbb{Z}_q$*, then there exists a probabilistic algorithm with running time* $n \cdot \text{poly}(\tau) + t$ *that breaks the DDH assumption with probability* $\geq \epsilon$ *with some polynomial* poly.

[2] Naor and Reingold proved it by using the random reducibility of the DDH-tuple.

We now show a proof of the claim.

Proof (of the claim). Let $\mathtt{Game}_3'$ ($\mathtt{Game}_4'$) be the same as $\mathtt{Game}_3$ ($\mathtt{Game}_4$) except for the following. In the initialization phase, instead of running the ZK-PoK in which the sender proves that he knows r, the sender runs the zero-knowledge simulator of the ZK-PoK which is allowed to rewind A. Since the ZK-PoK is perfect ZK, it holds that

$$\Pr(\text{GAME}_3') = \Pr(\text{GAME}_3),$$
$$\Pr(\text{GAME}_4') = \Pr(\text{GAME}_4)$$

We now construct a DDH distinguisher D in the sense of Lemma 4. The input to D is $(g, h, g^{x_1}, \cdots, g^{x_n}, y_1, \cdots, y_n)$, where $y_i = g^{rx_i}$ or g^{z_i}, Our D simulates $\mathcal{Z}$, A and the sender of $\mathtt{Game}_3'$ or $\mathtt{Game}_4'$ faithfully except for that in the initialization phase, D simulates the sender by using $(g, h, g^{x_1}, \cdots, g^{x_n})$, and $h_i = y_i$ for each i. Finally D outputs 1 iff $\mathcal{Z}$ outputs 1.

It is easy to see that D simulates $\mathtt{Game}_3'$ if $y_i = g^{rx_i}$ for each i, and $\mathtt{Game}_4'$ otherwise. Therefore

$$\left|\Pr(\text{GAME}_4') - \Pr(\text{GAME}_3')\right| \leq \epsilon_{\text{DDH}}. \tag{4}$$

Hence eq.(3) holds.

□

8 Fully Simulatable OT_1^2

We have shown two fully-simulatable adaptive OT schemes in the standard model. The first scheme holds under the DDH assumption and the second scheme holds under the decisional Nth residuosity (DCNR) assumption. It is clear that we can obtain fully-simulatable 1-out-of-2 OTs (OT_1^2s) as a special case.

On the other hand, Lindell showed a fully simulatable OT_1^2 under DDH, DCNR, and qudratic residuosity assumptions as well as under the assmption that homomorphic encryption exists in the standard model [14].

Let's compare our first scheme with Lindell's OT_1^2 which is based on the DDH assumption. His scheme builds on the OT_1^2 of [17] and use cut-and-choose techniques. The comutational cost and the communication cost are $O(\ell)$ times larger than those of our first scheme to achieve

$$\mathtt{Adv}(\mathcal{Z}) \leq 2^{-\ell+2}.$$

Hence our scheme is more efficient.

References

1. G. Brassard, C. Crépeau, J.-M. Robert, *All-or-Nothing Disclosure of Secrets*, CRYPTO 1986: pp.234–238

2. D. Chaum, *Zero-Knowledge Undeniable Signatures*, EUROCRYPT 1990, pp.458–464.
3. R. Cramer, I. Damgård, P.D. MacKenzie, *Efficient Zero-Knowledge Proofs of Knowledge Without Intractability Assumptions*, Public Key Cryptography 2000, pp.354–373.
4. R. Cramer, I. Damgård, B. Schoenmakers, *Proofs of Partial Knowledge and Simplified Design of Witness Hiding Protocols*, CRYPTO 1994, pp.174–187.
5. J. Camenisch, G. Neven, a. shelat, *Simulatable Adaptive Oblivious Transfer*, EUROCRYPT 2007, pp.573–590.
6. S. Even, O. Goldreich, A. Lempel, *A Randomized Protocol for Signing Contracts*, Commun. ACM 28(6), pp.637–647, 1985.
7. M. Green, S. Hohenberger, *Blind Identity-Based Encryption and Simulatable Oblivious Transfer*, ASIACRYPT 2007, pp.265–282.
8. M. Green, S. Hohenberger, *Universally Composable Adaptive Oblivious Transfer*, ASIACRYPT 2008, pp.179–197.
9. O. Goldreich, S. Micali, A. Wigderson, *How to Play any Mental Game or A Completeness Theorem for Protocols with Honest Majority*, STOC 1987, pp.218-229.
10. S. Jarecki, X. Liu, *Efficient Oblivious Pseudorandom Function with Applications to Adaptive OT and Secure Computation of Set Intersection*, TCC 2009, pp.577–594.
11. Y.T. Kalai, *Smooth Projective Hashing and Two-Message Oblivious Transfer*, EUROCRYPT 2005, pp.78–95.
12. J. Kilian, *Founding Cryptography on Oblivious Transfer*, STOC 1988, pp.20–31.
13. K. Kurosawa, *Multi-recipient Public-Key Encryption with Shortened Ciphertext*, Public Key Cryptography 2002, pp.48–63.
14. A.Y. Lindell, *Efficient Fully-Simulatable Oblivious Transfer*, CT-RSA 2008, pp.52–70.
15. M. Naor, B. Pinkas, *Oblivious Transfer and Polynomial Evaluation*, STOC 1999, pp.245–254
16. M. Naor, B. Pinkas, *Oblivious Transfer with Adaptive Queries*, CRYPTO 1999, pp.573–590.
17. M. Naor, B. Pinkas, *Efficient oblivious transfer protocols*, SODA 2001, pp.448–457.
18. M. Naor, O. Reingold, *Number-theoretic Constructions of Efficient Pseudo-random Functions*, J. ACM 51(2), pp.231–262, 2004.
19. W. Ogata, K. Kurosawa, *Oblivious keyword search*, J. Complexity 20(2-3), pp.356–371, 2004. (Cryptology ePrint Archive: Report 2002/182)
20. C.-P. Schnorr, *Efficient Signature Generation by Smart Cards*, J. Cryptology 4(3), pp.161–174, 1991.
21. A.C.-C. Yao, *How to Generate and Exchange Secrets*, FOCS 1986, pp.162–167.