Adaptive and Composable Oblivious Transfer Protocols
(Short Paper)

Huafei Zhu and Feng Bao

I²R, A*STAR, Singapore

Abstract. An adaptive $k$-out-of-$n$ oblivious transfer protocol ($\mathrm{OT}_{k \times 1}^n$) allows a receiver to obtain $m_{\sigma_{i-1}}$ before deciding on the $i$-th index $\sigma_i$. This paper studies adaptive $k$-out-of-$n$ oblivious transfer protocols in the presence of static adversaries in the universal composition (UC) framework. We show that the proposed $\mathrm{OT}_{k \times 1}^n$ protocol realizes the UC-security in the $\mathcal{F}_{\text{crs}}$-hybrid model under the joint assumptions that the underlying signature scheme is secure, the decisional Diffie-Hellman problem and the decisional composite residuosity problem in $\mathbb{Z}_{N^2}$ are hard as well as all knowledge proof protocols applied in this paper are computational zero-knowledge in the presence of static adversaries.

Keywords: Adaptive security, oblivious transfer, simulator, universal composability.

1 Introduction

An adaptive $k$-out-of-$n$ oblivious transfer protocol ($\mathrm{OT}_{k \times 1}^n$), first introduced by Naor and Pinkas in the context of the half-simulation model, allows a receiver to obtain $m_{\sigma_{i-1}}$ before deciding on the $i$-th index $\sigma_i$. Naor and Pinkas proposed interesting $\mathrm{OT}_{k \times 1}^n$ protocols in the half-simulation model and showed that their schemes analyzed in the half-simulation model might admit practical attacks on the receiver’s privacy [16]. Camenisch, Neven and Shelat [2] and Green and Hohenberger [13] proposed fully-simulatable $\mathrm{OT}_{k \times 1}^n$ protocols under the bilinear assumptions. The proofs of their protocols employ adversarial rewinding, and thus do not support the universally composable security. Green and Hohenberger [14] proposed the first implementation of universally composable adaptive oblivious transfer protocols based on the joint hardness assumptions of symmetric external Diffie-Hellman problem, decision linear problem and $q$-hidden LR$k$RW problem. A well-motivated problem is thus to find new frameworks for adaptive oblivious transfer schemes in the universally composable framework of Canetti under the standard cryptographic assumptions. At Crypto’08, Peikert, Vaikuntanathan and Waters [18] proposed non-adaptive, universally composable 1-out-of-2 oblivious transfer protocols in the presence of static adversaries. Their protocols are based on a new notion called dual-mode cryptosystem. The dual-mode cryptosystem is set up in one of two modes: extraction mode or decryption mode. A crucial of the dual-mode cryptosystem is that no adversary can distinguish
the common reference string between two modes. The recent work of Kurosara and Nojima \cite{15} provides two weaker simulatable adaptive $k$-out-of-$n$ oblivious transfer protocols in the standard cryptographic assumptions. However, their proofs invoke the rewinding technique and thus their protocols are not secure in the standard universally composable framework.

To the best of our knowledge, no universally composable adaptive $k$-out-of-$n$ oblivious transfer protocols constructed from the standard cryptographic assumptions are available in the research community. This paper aims to provide $\text{OT}^n_{k \times 1}$ protocols in the present of malicious adversaries under the standard cryptographic assumptions. We first set up a verifiably committed database in an initial stage of a protocol execution once the committer gets the instruction $(\text{send, sid, ssid, S, R})$ from an environment $\mathcal{Z}$, where $\text{sid}$ is a session id of an $\text{OT}^n_{k \times 1}$ query and $\text{ssid}$ is a sub-session id of any $j\text{th}$ query in the $\text{OT}^n_{k \times 1}$ execution ($1 \leq j \leq k$). Such a verifiably committed database must be equivocable since the simulator does not know the honest receiver’s adaptive index $\sigma_i$. This is not the case in the non-adaptive, 1-out-of-2 oblivious transfer protocols. We then ensure that the verifiably public database is extractable during the course of the OT executions since the simulator must extract the malicious sender’s input and forward the extracted input to the OT functionality when the environment $\mathcal{Z}$ instructs an adversary $\mathcal{A}$ to send messages to the receiver $R$ on behalf of the corrupted sender $S$. In a nutshell, we apply the Damgård-Neilsen’s mixed commitment protocol \cite{10} to realize the equivocable property and the Bresson-Catalano-Pointcheval’s double trapdoor protocol \cite{1} to realize the extractable property.

We will make use of the ideas introduced in \cite{19}, \cite{20} and \cite{21} to prove the security. That is, to prove the receiver’s security against a malicious sender, the master secret key $\text{msk}$ is used to extract implicit input of the corrupted sender. Consequently, a simulator for the corrupted sender is well defined; To prove the sender’s security against a malicious receiver, the local keys $s_{k_1}, \ldots, s_{k_n}$ are used to extract implicit input of the corrupted receiver and then the simulator makes use of the extractable keys ($\text{E-keys}$) to interpret a fake commitment to a commitment of any message. Such an interpretation is necessary when we consider the adaptive OT protocols where the simulator does not have any knowledge of an honest sender. This technique is crucial to prove the security without involving the standard rewinding technique even though the zero-knowledge proof systems are involved in our implementation.

We stress that we do not apply the corresponding knowledge extractors of zero-knowledge protocols employed in our OT protocol but the double trapdoor mechanism to prove the security of our implementation that is the most significant difference between our ideas and that of Kurosara and Nojima \cite{15}. The application of the double trapdoor mechanism for extracting implicit inputs of corrupted parties is a key point to realize the universally composable security. The Kurosara and Nojima’s scheme fails to reach the universally composable security since their proof relies on the notion of the corresponding knowledge extractor of a zero-knowledge proof system where the rewinding technique is unavoidable by the definition of any zero-knowledge proof/argument system.
2 Definitions

Throughout the paper, we assume that the reader is familiar with the following building blocks:

- The Canetti’s universally composable framework [4];
- The Bresson, Catalano and Pointcheval’s double trapdoor encryption scheme [1] which is in turn constructed from the Paillier’s encryption scheme [17];
- The Damgård and Neilsen’s mixed commitments [10];
- The standard zero-knowledge proof techniques such as Camenisch and Michels protocol [3] for proving that \( N \) is a product of two safe primes \( p \) and \( q \), Damgård-Fujisaki’s protocol [11] for zero-knowledge proof of knowledge of a commitment and the equality of a commitment and an encryption and the Cramer-Damgård-Schoenmakers’ OR-protocol [8].

Common Reference String Model. Canetti and Fischlin have shown that OT cannot be UC-realized without a trusted setup assumption [5]. We thus assume the existence of an honestly-generated Common Reference String (crs) and work in the so called \( F_{crs}^{D} \)-hybrid model. The functionality of common reference string model assumes that all participants have access to a common string that is drawn from some specified distribution \( D \). The functionality defined below is due to [6].

\[
\text{Functionality } F_{crs}^{D} \\
\text{\( F_{crs}^{D} \) proceeds as follows, when parameterized by a distribution } \mathcal{D}. \\
\text{When receiving a message } (\text{sid}, P_i, P_j) \text{ from } P_i, \text{ let } \text{crs} \leftarrow \mathcal{D}(1^n) \text{ and send } (\text{sid}, \text{crs}) \text{ to } P_i, \text{ and send } (\text{crs}, \text{sid}, P_i, P_j) \text{ to the adversary, where } \text{sid} \text{ is a session identity. Next when receiving } (\text{sid}, P_i, P_j) \text{ from } P_j (\text{and only from } P_j), \text{ send } (\text{sid}, \text{crs}) \text{ to } P_j \text{ and to the adversary, and halt.}
\]

Functionality for adaptive \( k \)-out-of-\( n \) oblivious transfer \( \text{OT}_{k \times 1}^n \). Following [14] and [7], functionality \( \text{OT}_{k \times 1}^n \) is described below.

\textbf{Definition 1.} Let \( F \) be a functionality for \( \text{OT}_{k \times 1}^n \). A protocol \( \pi \) is said to universally compositely realize \( F \) if for any adversary \( A \), there exists a simulator \( S \) such that for all environments \( Z \), the ensemble \( \text{IDEAL}_{F,S,Z} \) is computationally indistinguishable with the ensemble \( \text{REAL}_{\pi,A,Z} \).

3 \( \text{OT}_{k \times 1}^n \) Based on Bresson-Catalano-Pointcheval’s Protocol

With the help of the Bresson-Catalano-Pointcheval double trapdoor encryption scheme (BCP) and the Damgård-Nielsen’s mixed commitment scheme, we are now ready to describe our \( \text{OT}_{k \times 1}^n \) protocol, denoted by \( \pi \) which consists of the
following three subprotocols — a common reference string generation protocol, an initialization protocol and an \( i \)th adaptive OT-query protocol.

The common reference string generation protocol. The common reference string generation algorithm is depicted below:

- On input a security parameter \( \lambda \), the common reference generation algorithm \( \text{OTcrsGen}(1^\lambda) \) (for OT) invokes a key generation algorithm \( \mathcal{G} \) of the BCP’s encryption to generate composite modulus of the form \( N = pq \) that is a product of two safe primes \( p \) and \( q \) (i.e., \( p = 2p' + 1, q = 2q' + 1 \)), a cyclic group \( \mathcal{G} \subseteq \mathbb{Z}_{N^2}^* \) of order \( N' \) (\( N' = p'q' \)), and \( n \) random generators \( g_1, \ldots, g_n \) of \( \mathcal{G} \) and \( n \) random elements \( (h_1, \ldots, h_n) \) such that \( h_i = g_i^{x_i} \mod N^2, x_i \in_U \mathbb{Z}_{N'}. \) Let \( \text{crs}_{\text{DE}} = \langle \text{des}(\mathcal{G}), (g_1, h_1), \ldots, (g_n, h_n), N \rangle \).
- \( \text{OTcrsGen}(1^\kappa) \) then invokes a key generation algorithm of Damgård-Nielsen’s mixed commitment scheme to generate the global public key \( \tilde{N} \) and \( n \) random keys \( K_1, \ldots, K_n \in_U \mathbb{Z}_{N^2}^* \), where \( \tilde{N} = \tilde{p} \tilde{q}, \tilde{p} = 2p' + 1, \tilde{q} = 2q' + 1, \) and \( \tilde{p}, \tilde{p}', \tilde{q} \) and \( \tilde{q}' \) are large prime numbers. Let \( \text{crs}_{\text{MC}} = \langle \tilde{N}, K_1, \ldots, K_n \rangle \).
- The common reference string generation algorithm also proves that \( f(x) = x^N \mod N \) and \( \tilde{f}(x) = x^{\tilde{N}} \mod \tilde{N} \) are permutations over \( \mathbb{Z}_{N}^* \) and \( \mathbb{Z}_{\tilde{N}}^* \), respectively. This can be done by invoking Camenisch and Michels protocol that proves in zero-knowledge that the number \( N \) (\( \tilde{N} \), respectively) is the product of two safe primes \( p \) and \( q \) (\( \tilde{p} \) and \( \tilde{q} \) respectively) \( \mathcal{B} \).

Let \( \text{ZK-PRoPrimes} \) be a transcript of zero-knowledge to convince a verifier \( N \) (\( \tilde{N} \), respectively) are product of large safe primes. Given a copy of \( \text{ZK-PRoPrimes} \), one can immediately delivery a proof that \( f(x) = x^N \mod N \) (\( \tilde{f}(x) = x^{\tilde{N}} \mod \tilde{N}, \) respectively) is a permutation over \( \mathbb{Z}_N^* \) (\( \mathbb{Z}_{\tilde{N}}^* \) respectively) since \( \gcd(N, \phi(N)) = 1 \) (\( \gcd(\tilde{N}, \phi(\tilde{N})) = 1 \) respectively) is trivial if \( N \) (\( \tilde{N} \), respectively) is product of two large prime numbers.

The common reference string \( \text{crs} \) is \( \langle \text{crs}_{\text{DE}}, \text{crs}_{\text{CM}}, \text{ZK-PRoPrimes} \rangle \).
The initialization protocol. The initialization protocol enables a sender to set up a verifiably committed database. That is, on input \( n \) messages \((m_1, \ldots, m_n)\) \((m_i \in \mathbb{Z}_N)\) and the common reference string \(\text{crs}\), a sender \(S\) performs the following computations:

- \(S\) invokes the Damgård-Nielsen’s mixed commitment scheme to generate \(n\) commitments \(c_i = \text{COM}_{K_i}(m_i, r_i) \mod \tilde{N}^2 = K_i^{m_i} r_i \tilde{N} \mod \tilde{N}^2\), where \(m_i \in \mathbb{Z}_N\) and \(r_i \in \mathbb{Z}_N^*\).
- \(S\) invokes the Damgård-Fujisaki’s protocol and proves that he knows \(m_i\) and \(r_i\) such that \(c_i = \text{COM}_{K_i}(m_i, r_i) \mod \tilde{N}^2\) \((i = 1, \ldots, n)\). Let \(\text{DB-PRoK}\) be a zero-knowledge proof of the knowledge \(<(m_1, r_1), \ldots, (m_n, r_n)>\) such that \(c_i = \text{COM}_{K_i}(m_i, r_i) \mod \tilde{N}^2\) \((i = 1, \ldots, n)\).
- Let \(C = (c_1, \ldots, c_n)\) and \(D = (C, \text{DB-PRoK})\). \(S\) then signs \(D\) by means of a secure signature scheme which is independent of the described OT protocol (say the Cramer-Shoup’s signature scheme which is secure in the sense of Goldwasser, Micali and Rivest). Let \(\Sigma_D\) be a signature of \(D\) and \(\text{DB} = (D, \Sigma_D)\) (we call \(\text{DB}\) a verifiably committed database). The public database \(\text{DB}\) is then broadcasted to all participants.

The \(i\)th adaptive OT-query protocol. On input common reference strings \(\text{crs}_{\text{DE}} = \langle \text{des}(G), (g_1, h_1), \ldots, (g_n, h_n), N \rangle\), \(\text{crs}_{\text{MC}} = \langle \tilde{N}, K_1, \ldots, K_n \rangle\) and the public database \(\text{DB} = (D, \Sigma_D)\) (we call \(\text{DB}\) a verifiably committed database). The public database \(\text{DB}\) is then broadcasted to all participants.

**Step 1:** \(R\) first verifies the validity of public database \(\text{DB} = (D, \Sigma_D)\) (i.e., verifying the signature of the database). If it is not valid, then outputs \(\bot\); if the database \(\text{DB}\) is valid, \(R\) continues the following procedures:

- On input the retrieved \((i−1)\) messages \(m_{\sigma_1}, \ldots, m_{\sigma_{i−1}}\) and its random string \(r_R\), \(R\) adaptively outputs the \(i\)th index \(\sigma_i \in [1, n]\);
- On input \(\text{crs}\) and \(\sigma_i \in [1, n]\), \(R\) randomly chooses \(z_{\sigma_i} \in [0, N^2/4]\), and computes \(g = g_{\sigma_i}^{z_{\sigma_i}} \mod N^2\) and \(h = h_{\sigma_i}^{z_{\sigma_i}} \mod N^2\). Let \(\text{tpk} = (g, h)\) and \(\text{tsk} = z_{\sigma_i}\). \(R\) then invokes the Cramer-Damgård-Schoenmakers’ OR-protocol and proves to the sender that

\[
(g_1, h_1, g, h) \lor (g_2, h_2, g, h) \lor \cdots \lor (g_n, h_n, g, h)
\]

is a Diffie-Hellman quadruple. Let \(\text{ZK-ProOR}\) be the zero-knowledge proof of the relationship via the Cramer-Damgård-Schoenmakers’ OR-protocol. \(R\) keeps \(\text{tsk}\) as a secret and sends \(\text{tpk}\) together \(\text{ZK-ProOR}\) to \(S\).

**Step 2:** On input \(\text{crs}, \text{tpk}\) and \(\text{ZK-ProOR}\), the sender \(S\) checks the following three conditions: 1) \(g \in \mathbb{Z}_{N^2}^*\) and \(h \in \mathbb{Z}_{N^2}^*\); 2) \(g^{2N} \neq 1\) and \(h^{2N} \neq 1\) and 3) the transcript \(\text{ZK-ProOR}\) is valid. If any of three conditions is violated, then outputs \(\bot\); otherwise, \(S\) performs the following computations:
1. \( S \) randomly chooses \( s_j, t_j \in [0, N^2/4] \);
2. \( S \) computes \( u_j = g_j^{s_j} h_j^{t_j} \mod N^2 \), \( \nu_j = g_j^{s_j} h_j^{t_j} (1 + N)^{m_j} \mod N^2 \); Let \( E_j = (u_j, \nu_j) \). \( S \) then invokes the Damgård-Fujiyaki's protocol \( \Pi \) and proves that \( c_j \) (the ciphertext \( c_j \) is generated in the initial stage) and \( E_j \) are ciphertexts of the same message \( m_j \). Let \( \text{ZK-PKoEQ} \) be a zero-knowledge proof of the equality of two ciphertexts \( E_i \) and \( c_i \) (\( i = 1, \ldots, n \)). \( S \) then sends \( n \) ciphertexts \( (E_1, \ldots, E_n) \) together with \( \text{ZK-PKoEQ} \) to \( R \).

**Step 3:** Upon receiving \( (E_1, \ldots, E_n) \) and \( \text{ZK-PKoEQ} \), \( R \) checks the proof. If the check is valid, \( R \) decrypts \( E_{\sigma_i} \), to obtain \( m_{\sigma_i} \), otherwise, outputs \( \bot \).

This ends the description of the protocol \( \pi \).

**Theorem 1.** The proposed adaptive oblivious transfer protocol \( \text{OT}_{k \times 1}^n \) is universally composable in the \( \mathcal{FD}_{crs} \)-hybrid model in the presence of static adversaries under the joint assumptions that the underlying signature scheme is secure in the sense of Goldwasser, Micali and Rivest \( [12] \), the decisional Diffie-Hellman problem over \( G \) and the decisional composite residuosity problem in \( Z_{N^2} \) are hard as well as all knowledge proof protocols are (either statistical or computational) zero-knowledge against malicious participants.

**Proof.** Let \( A \) be a static adversary that interacts with the parties \( S \) and \( R \) running the protocol \( \pi \). We will construct an ideal world adversary \( S \) interacting with the ideal functionality \( \text{OT}_{k \times 1}^n \) such that no environment \( Z \) can distinguish an interaction with \( A \) in the protocol \( \pi \) from an interaction with the simulator \( S \) in the ideal world.

**Simulating the corrupted sender.** When \( S \) is corrupted and \( R \) is honest, the adversary \( A \) gets \( S \)'s input from the environment \( Z \), and generates all the messages from \( S \). The goal of a simulator \( S \) now is to generate the remaining messages (namely, messages from \( R \)) so that the entire transcript is indistinguishable from the real interaction between \( S \) and \( R \) from the point view of the environment \( Z \). The details of simulator for corrupted party \( S \) is described below:

1. when the environment \( Z \) queries to \( \text{OT}_{crsGen}(1^\kappa) \) for a common reference string \( \text{crs} \), the simulator invokes the key generation algorithm \( G \) of the BCP’s encryption to generate composite modulus of the form \( N = pq \) that is a product of two safe primes \( p \) and \( q \) (i.e., \( p = 2p' + 1, q = 2q' + 1 \)), a cyclic group \( G \subset Z_{N^2}^{*} \) of order \( N' \) (\( N' = p' q' \)), and \( n \) random generators \( g_1, \ldots, g_n \) of \( G \) and \( n \) random elements \( (h_1, \ldots, h_n) \) such that \( h_i = g_i^{x_i} \mod N^2 \), \( x_i \in U \ Z_{N'} \), \( i = 1, \ldots, n \). The simulator keeps the auxiliary strings \( (p, q) \) and \( (x_1, \ldots, x_n) \) secret. Let \( \text{crs}_{DE} = < \text{des}(G), (g_1, h_1), \ldots, (g_n, h_n), N > \).

   \( \text{OT}_{crsGen} \) then invokes the key generation algorithm of Damgård-Nielsen’s mixed commitment scheme to generate a public key \( \tilde{N} \) and \( n \) extractable keys \( K_1, \ldots, K_n \in U \ Z_{N^2}^{*} \), where \( \tilde{N} = \tilde{p} \tilde{q}, \tilde{p} = 2\tilde{p}' + 1, \tilde{q} = 2\tilde{q}' + 1 \), and \( \tilde{p}, \tilde{p}', \tilde{q} \) and \( \tilde{q}' \) are large prime numbers.

   Let \( K_i = (1 + \tilde{N})^{k_i} r_{k_i}^{\tilde{N}} \mod \tilde{N} \) (\( i = 1, \ldots, n \)). The simulator keeps \( (\tilde{p}, \tilde{q}) \) and \( < (k_1, r_{k_1}), \ldots, (k_n, r_{k_n}) > \) secret. Let \( \text{crs}_{MC} = < \tilde{N}, K_1, \ldots, K_n > \).
Given \((p, q)\) and \((\tilde{p}, \tilde{q})\) such that \(N = pq\) and \(\tilde{N} = \tilde{p}\tilde{q}\), the simulator further invokes Camenisch and Michels protocol and proves in zero-knowledge that \(N\) (\(\tilde{N}\), respectively) is a product of two safe primes \(p\) and \(q\) (\(\tilde{p}\) and \(\tilde{q}\) respectively). The transcript of zero-knowledge proof is denoted by \(\text{ZK-PRoPrimes}\). Let \(\text{crs} = (\text{crs}_{\text{DE}}, \text{crs}_{\text{MC}}, \text{ZK-PRoPrimes})\). \(F_{\text{crs}}^{D}\) returns \((\text{sid, crs})\) to the environment \(Z\).

2. When the simulator \(S\) receives \((\text{sid, ssid}, (D, \Sigma_D))\) from the real world adversary \(A\) who fully controls the corrupted sender \(S\). The simulator checks the validity of DB. If the signature is invalid, \(S\) outputs \(\perp\).

3. If \(DB\) is valid, then the simulator \(S\) extracts the messages \((m_1, \ldots, m_n)\) from the given ciphertexts \((c_1, \ldots, c_n)\) using the trapdoor strings \((\tilde{p}, \tilde{q})\) and \(<(k_1, r_{k_1}), \ldots, (k_n, r_{k_n})\rangle\) and then forwards the extracted message \(m_1, \ldots, m_n\) to the ideal functionality \(F_{\text{OT}^n_{k\times 1}}\). We stress that the simulator \(S\) must send the messages \((m_1, \ldots, m_n)\) to the functionality \(F_{\text{OT}^n_{k\times 1}}\) at the initial stage.

4. \(S\) randomly selects \((g, h)\) with order \(N'\) and sets \(pk = (g, h)\). We stress that the choice of \((g, h)\) is a trivial task since \(S\) holds the master key \((p, q)\). \(S\) invokes Cramer-Damgård-Schoenmakers’ OR-protocol to prove that there exists an index \(i^* \in [1, n]\) such that \((g_{i^*}, h_{i^*}, g, h)\) is a Diffie-Hellman quadruple. Let \(\text{ZK-PRoOR}\) a transcript of OR-protocol. The simulator then sends \(tpk = (g, h)\) and \(\text{ZK-PRoOR}\) to the adversary \(A\).

5. Upon receiving \((E_1, \ldots, E_n)\) and \(\text{ZK-PKoEQ}\) from the adversary \(A\), the simulator \(S\) checks the given proof. If the check is valid, \(S\) decrypts \(E_{\sigma_i}\) to reveal \(m_{\sigma_i}\); otherwise, outputs \(\perp\).

Let \(\text{IDEAL}_{\pi, S, Z}\) be the view of ideal world adversary \(S\) described above and \(\text{REAL}_{\pi, A, Z}\) be the view of real world adversary \(A\) of protocol \(\pi\). Notice that when \(S\) receives \((\text{sid, ssid}, (D, \Sigma_D))\) from the real world adversary \(A\), it checks the validity of DB. If the signature is invalid, \(S\) outputs \(\perp\). If the signature is valid, \(S\) extracts the messages \((m_1, \ldots, m_n)\) from the given ciphertexts \((c_1, \ldots, c_n)\) using the trapdoor string \((\tilde{p}, \tilde{q})\) to the ideal functionality \(F_{\text{OT}^n_{k\times 1}}\). This means that the rewinding technique for extract implicit messages of the corrupted sender is not applied here. The only difference between \(\text{REAL}_{\pi, A, Z}\) and \(\text{IDEAL}_{\pi, S, Z}\) is the different strategies to generate the public key \((g, h)\) in \(\pi\) and the public key \((g, h)\) generated in the simulation stage. By the Diffie-Hellmann assumption over \(Z_{N^2}^{*}\), we know that \(\text{REAL}_{\pi, A, Z} \approx \text{IDEAL}_{\pi, S, Z}\).

**Simulating the corrupted receiver.** When \(S\) is honest and \(R\) gets corrupted, the adversary \(A\) gets \(R\)’s input from the environment \(Z\), and generates all the messages from \(R\). The goal of the simulator now is to generate the remaining messages (namely, all messages from \(S\)) so that the entire transcript is indistinguishable from the real interaction between \(S\) and \(R\) from the point view of the environment \(Z\).

1. When the environment \(Z\) queries to \(\text{OTcrsGen}(1^n)\) for a common reference string \(\text{crs}\), the simulator \(S\) invokes a key generation algorithm \(G\) of the BCP’s
key generation algorithm to generate \( \text{crs}_{DE} \), where \( \text{crs}_{DE} = < \text{des}(G), (g_1,h_1), \ldots, (g_n,h_n), N > \). The trapdoor string \( \tau \) is \( (x_1, \ldots, x_n) \). The simulator is given the master auxiliary string \( < p, q > \).

The simulator then invokes the key generation \( \text{crs}_{MC} \) to generate \( \text{crs}_{MC} = < \tilde{N}, K_1, \ldots, K_n > \), where \( K_j = \psi(0, k_j) \) (i.e., all \( K_j \) are E-keys). The auxiliary string is \( (k_1, \ldots, k_n) \). The simulator keeps the auxiliary information \( \tilde{p} \) and \( \tilde{q} \) such that \( \tilde{N} = \tilde{p}\tilde{q}, \tilde{p} = 2\tilde{p}^2 + 1, \tilde{q} = 2\tilde{q}^2 + 1 \) secret.

Let \( \text{crs} = (\text{crs}_{DE}, \text{crs}_{MC}) \). \( \mathcal{FE}^D_{\text{crs}} \) returns \( (\text{sid}, \text{crs}) \) to the environment \( \mathcal{Z} \):

2. the simulator \( S \) invokes the Damgård-Nielsen’s mixed commitment scheme to generate \( n \) commitments \( C_i = \text{COM}_{K_i}(m_i, r_i) \mod \tilde{N}^2 = K_i^m_i r_i^N \mod \tilde{N}^2 \), where \( m_i = 0 \) (all are dummy messages) and \( r_i \in Z_N^* \).

3. Given \( \text{crs} \), \( \text{tpk} \) and \( \text{ZK-PRoOR} \), the simulator \( S \) checks the following three conditions: 1) checking \( g \in Z_{N^2}^* \) and \( h \in Z_{N^2}^* \); 2) checking \( g^{2N} \neq 1 \) and \( h^{2N} \neq 1 \) and 3) checking the validity of the transcript \( \text{ZK-PRoOR} \). If any of three conditions is violated, then outputs \( \perp \); otherwise, \( S \) extracts an index \( \sigma_i \) by testing the equation \( h_i \equiv g^{x_{\sigma_i}} \) \( (i = 1, \ldots, n) \). \( S \) sends \( \sigma_i \) to the ideal functionality \( \mathcal{F}_{\text{OT}}^{k \times 1} \) and obtains \( m_{\sigma_i} \).

4. \( S \) modifies the internal states to generate a transcript that is consistent with the given database \( \mathcal{DB} \) according to the following strategy: given \( c_{\sigma_i} \) (the encryption of dummy message with randomness \( r_{\sigma_i} \)), the simulator extracts a new randomness \( r'_{\sigma_i} \) from the equation \( K_{\sigma_i}^0 r_{\sigma_i}^N = K_{\sigma_i}^m x_{\sigma_i} r'_{\sigma_i}^N \), where \( K_{\sigma_i} = \psi(0, k_{\sigma_i}) \).

The simulator then invokes the Damgård-Fujiwaki’s protocol to output a transcript that \( c_j \) (the ciphertext \( c_j \) is generated in the initial stage) and \( E_j \) are ciphertexts of the same message \( m_j \). Let \( \text{ZK-PKoEQ} \) be a transcript of the proof. \( S \) then sends \( n \) ciphertexts \( (E_1, \ldots, E_n) \) together with \( \text{ZK-PKoEQ} \) to the adversary \( \mathcal{A} \).

Let \( \text{IDEAL}_{\mathcal{F}, S, \mathcal{Z}} \) be the view of ideal world adversary \( S \) described above and \( \text{REAL}_{\pi, \mathcal{A}, \mathcal{Z}} \) be the view of real world adversary \( \mathcal{A} \) of protocol \( \pi \). Notice that \( S \) extracts an index \( \sigma_i \) by testing the equation \( h_i \equiv g^{x_{\sigma_i}} \) \( (i = 1, \ldots, n) \) and then sends \( \sigma_i \) to the ideal functionality \( \mathcal{F}_{\text{OT}}^{k \times 1} \) to learn \( m_{\sigma_i} \). This means that the implicit input of the corrupted receiver is extracted by the auxiliary string \( (x_1, \ldots, x_n) \). The only difference between \( \text{REAL}_{\pi, \mathcal{A}, \mathcal{Z}} \) and \( \text{IDEAL}_{\mathcal{F}, S, \mathcal{Z}} \) is the generation of \( n \) keys \( (K_1, \ldots, K_n) \) of the Damgård-Nielsen’s mixed commitment. By the key indistinguishability assumption, we know that \( \text{REAL}_{\pi, \mathcal{A}, \mathcal{Z}} \approx \text{IDEAL}_{\mathcal{F}, S, \mathcal{Z}} \).

A close look at the proof shows that both statistical zero-knowledge proof protocols and computational zero-knowledge proof protocols work in our scheme.

Combining the above statements, we know that the proposed adaptive oblivious transfer protocol \( \text{OT}^n_{k \times 1} \) is universally composable in the \( \mathcal{F}^D_{\text{crs}} \)-hybrid model assuming that the decisional Diffie-Hellman problem over \( G \) is hard as well as all knowledge proof protocols are zero-knowledge. \( \square \)
In this paper, a new implementation of adaptive oblivious transfer protocol $\text{OT}^n_{k \times 1}$ has been proposed. We have shown that the proposed scheme has achieved the UC-security in the $\mathcal{F}^D_{\text{crs}}$-hybrid model under the joint assumptions that the underlying signature scheme is secure, the decisional Diffie-Hellman problem and the decisional composite residuosity problem in $\mathbb{Z}_{N^2}$ are hard as well as all knowledge proof protocols applied in this paper are computational zero-knowledge in the presence of static adversaries.

References


