“The Simplest Protocol for Oblivious Transfer” Revisited

Ziya Alper Genç, Vincenzo Iovino, and Alfredo Rial

University of Luxembourg
ziya.genc@uni.lu, vinciovino@gmail.com, alfredo.rial@uni.lu

Abstract. In 2015, Chou and Orlandi presented an oblivious transfer protocol that already drew a lot of attention both from theorists and practitioners due to its extreme simplicity and high efficiency. Chou and Orlandi claimed that their protocol is UC-secure in the random oracle model under dynamic corruptions, which is a very strong security guarantee. Unfortunately, in this work we point out a flaw in their security proof for the case of sender corruption.

We define a decisional problem and we prove that, if a correct proof is provided, then this problem can be solved correctly with overwhelming probability. Therefore, the protocol by Chou and Orlandi cannot be instantiated securely with groups for which our decisional problem cannot be solved correctly with overwhelming probability. Our decisional problem can be solved with overwhelming probability when a DDH oracle is provided. Therefore, it seems likely that the protocol by Chou and Orlandi can be instantiated securely with gap-DH groups.

Keywords: oblivious transfer, universal composability.

1 Introduction

Oblivious Transfer. In an oblivious transfer (OT) protocol, a sender receives as input messages $M_1, \dots M_N$ and a receiver receives as input indices $\sigma_1, \dots, \sigma_k \in [1, N]$. At the end of the protocol, the receiver outputs $M_{\sigma_1}, \dots, M_{\sigma_k}$ and learns nothing about the other messages. The sender does not learn anything about the indices.

OT was introduced by Rabin [Rab81] and generalized by Even, Goldreich and Lempel [EGL82] and Brassard, Crépeau and Robert [BCR87]. (The notion of OT was also developed independently by Wiesner in the 1970’s but published only later [Wie83].) OT has a lot of applications and it is at the core of multiparty computation [Yao86,GMW87,Kil88].

Chou and Orlandi’s OT Protocol. Chou and Orlandi (CO) [CO15] present a novel OT protocol and claim that it is universally composable (UC) [Can01] under dynamic corruptions. Their protocol has the advantages of being extremely simple and efficient. The work of CO has already gained some popularity both from theorists and practitioners and has so far been cited 21 times according to Google Scholar.

CO present a 1-out-of-2 OT protocol and extend it to a 1-out-of-n OT protocol in a straightforward manner. For the purpose of this work, which focuses on negative results about the security of the CO protocol, it suffices to analyze the 1-out-of-2 OT protocol. We note that our negative results also apply to the 1-out-of-n OT protocol.

The 1-out-of-2 OT protocol by CO is depicted in Figure 1. To run the protocol, Alice (the sender) and Bob (the receiver) have first to agree on a group $\mathbb{G}$ and a generator g of prime order p. In the first message, Alice samples a random element a in $\mathbb{Z}_p$ and sends $A = g^a$ to Bob. Bob picks random b in $\mathbb{Z}_p$ and, depending on his index $c \in [0, 1]$, sends either $B = g^b$ or $B = Ag^b$ to Alice. Then, Alice derives two keys k_0 and k_1 from $(B)^a$ and $(B/A)^a$ respectively. Alice encrypts the messages M_0 and M_1 by using the keys k_0 and k_1 respectively. Bob can derive the key k_R from A^b, which allows Bob to obtain M_c. However, it is computationally hard for him to compute the key that allows the obtention of M_{1-c}.

The protocol uses as building block a symmetric-key encryption scheme given by two algorithms Enc and Dec. Security against a corrupt receiver holds in the random oracle model if the scheme (Enc, Dec) is non-committing and if the CDH assumption holds in the group $\mathbb{G}$. In [CO15], it is claimed that security against a corrupt sender holds in the random oracle model if the scheme (Enc, Dec) is robust.

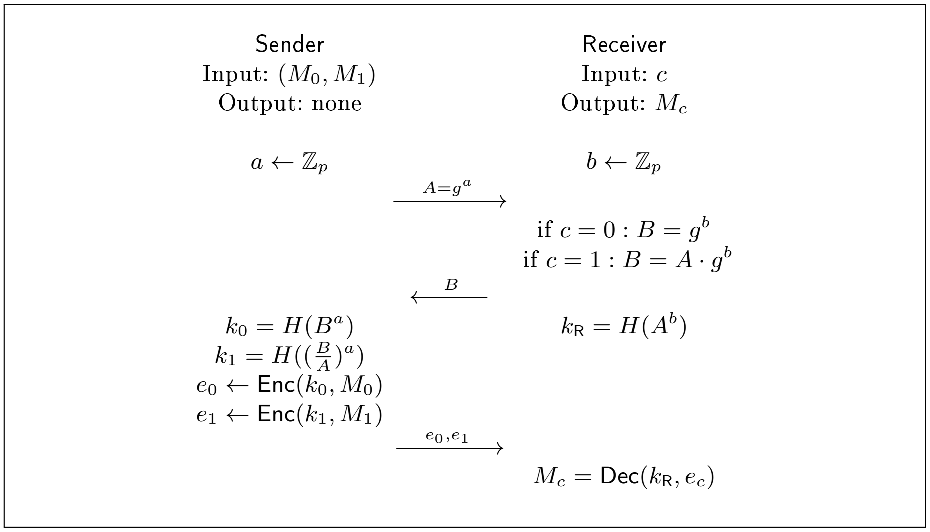
Sender
Input: (M_0, M_1)
Output: none
Receiver
Input: c
Output: M_c
$a \leftarrow \mathbb{Z}_p$
$b \leftarrow \mathbb{Z}_p$
$\xrightarrow{A=g^a}$
if $c = 0 : B = g^b$
if $c = 1 : B = A \cdot g^b$
$\xleftarrow{B}$
$k_0 = H(B^a)$
$k_1 = H((\frac{B}{A})^a)$
$e_0 \leftarrow \mathsf{Enc}(k_0, M_0)$
$e_1 \leftarrow \mathsf{Enc}(k_1, M_1)$
$k_{\mathsf{R}} = H(A^b)$
$\xrightarrow{e_0,e_1}$
$M_c = \mathsf{Dec}(k_{\mathsf{R}}, e_c)$

Fig. 1. Chou and Orlandi's 1-out-of-2 OT Protocol.

1.1 Our Results

We show a mistake in the security proof given by CO for the case of a corrupt sender. Namely, in their security proof, their simulator extracts incorrectly the messages M_0 and M_1 that are sent to the ideal functionality.

We also define a decisional problem in the group $\mathbb{G}$ and we prove that, if a correct simulator is provided for the case of a corrupt sender, then this problem can be solved with overwhelming probability. Therefore, the protocol by CO cannot be instantiated securely with groups $\mathbb{G}$ in which our decisional problem cannot be solved with overwhelming probability.

Consequently, the protocol by CO cannot be instantiated with any group $\mathbb{G}$ in which the CDH problem is intractable, but only with groups where both the CDH problem is intractable and our decisional problem can be solved with overwhelming probability. Our decisional problem can be solved with overwhelming probability when the DDH problem is easy in $\mathbb{G}$. Therefore, it seems likely that the protocol by CO can be instantiated securely with gap-DH groups.

Outline of the Paper. In Section 2, we describe an ideal functionality for OT, which we use in our proof in Section 4. This ideal functionality takes into account an observation made by Li and Micciancio [LM16] on the definition of ideal functionality for OT that the protocol by CO realizes. In Section 3, we describe the flaw in the simulator by CO for the case of sender corruption. In Section 4, we define a decisional problem and we prove that the CO protocol cannot be instantiated securely with groups $\mathbb{G}$ where this problem cannot be solved with overwhelming probability. We conclude in Section 5.

Differences with the previous versions. In a previous version of this work, we claimed that the security proof by CO for the case of receiver corruption was mistaken. As pointed out by Chou and Orlandi, this claim is incorrect. We thank Chou and Orlandi for their comments and we apologize for not contacting them before publishing this paper.

2 Ideal Functionality for 1-out-of-2 OT

In this section, we describe an ideal functionality for OT, which we use in our proof in Section 4. This ideal functionality takes into account an observation made by Li and Micciancio [LM16] on the definition of ideal functionality for OT that the protocol by CO realizes.

The functionality defined by CO does not impose any restriction on the order in which the sender and the receiver send their inputs to the ideal functionality. Li and Micciancio [LM16] observe that this is a problem to prove secure the OT protocol by CO. In the OT protocol by CO, the receiver has to decide his input bit in order to compute the second message of the protocol. The sender decides what messages he inputs in order to compute the third message. In the security proof for the case of sender corruption, the simulator needs to extract the messages from the adversary. The simulator cannot perform such extraction until receiving the third message of the protocol from the adversary. However, to receive this third message, the simulator has to send before the second message to the adversary. The problem here is that the simulator does not know whether the receiver has already input his bit to the functionality, because the functionality does not tell the sender that the receiver has sent her input. Consequently, the simulator does not know whether it can send the second message to the adversary, and so it cannot provide a correct simulation. In the security proof by CO, this problem is overlooked.

In Figure 2, we show a functionality for 1-out-of-2 OT for static corruptions. As suggested by Li and Micciancio, this functionality informs the sender when the receiver sends her input bit. We note that this functionality, like the one by CO, skips many details, such as the communication with the simulator and many other elements that are necessary in the UC framework (session identifiers, . . .).

Ideal $\binom{2}{1}$-OT Functionality

The functionality waits for some input c from the receiver R and before receiving any input from R will ignore any input coming from the sender S. When the input c is received from R, if $c \notin \{0,1\}$, the functionality sends an error message $\perp$ to the receiver, otherwise it notifies the sender by transmitting a special symbol OK. The functionality will ignore further inputs from R.
After receiving $c \in \{0,1\}$ from R, if the functionality did not abort, the functionality waits for either a pair of messages (M_0, M_1) or an error message $\perp$ from the sender S. If the input of S is $\perp$ or a non-valid pair of messages (in the message space) the functionality sends $\perp$ to the receiver, otherwise it sends M_c to the receiver. The functionality ignores further inputs from S.

Fig. 2. Ideal functionality for 1-out-of-2 OT.

We would like to stress that the mistake we found in the simulator of the security proof by CO is independent of the one found by Li and Micciancio. In fact, Li and Micciancio [LM16] provide a simulator for the CO protocol for the case of sender corruption to realize their modified OT functionality and say "we leave the verification that the simulator is indeed correct to the reader." However, the simulator by Li and Micciancio has the same problem as the simulator by CO.

The mistake we found in the simulator by CO is that the simulator does not send the correct messages to the functionality when the sender is corrupt. Therefore, it cannot be patched by using a different ideal functionality because any existing 1-out-of-2 OT functionality requires the sender to send the messages to the functionality.

3 Flaw in CO's Security Proof

In this section, we analyze the security proof provided by CO for the case of sender corruption. We show that the simulator described by CO for this case is incorrect. For simplicity, we analyze the instantiation of the protocol as a 1-out-of-2 OT scheme, but we remark that the mistake we found also holds for the case of m parallel executions of 1-out-of-n OT for other values of m and n.

The simulator needs to extract the messages from the corrupt sender in order to send them to the ideal functionality. To do this, when the corrupt sender makes a random oracle query, the simulator described by CO picks a random key, stores it and replies the query with this random key. After that, when the corrupt sender sends the ciphertexts, the simulator tries to decrypt the ciphertexts (e_0, e_1) by using all the stored keys until the result of one of the decryptions is not $\perp$. If the result of decryption is $\perp$ in all cases, then the message is set to $\perp$.

The problem in this simulator is the following. The corrupt sender can submit an oracle query on input $X \neq B^a$ (resp. $Y \neq (\frac{B}{A})^a$) and compute the ciphertexts e_0 (resp. e_1) using key $k'_0 = H(X)$ (resp. $k'_1 = H(Y)$). Then the simulator would decrypt using (k'_0, k'_1) and obtain messages different from $\perp$. However, the honest receiver in the real world would obtain $\perp$ because the oracle query made by the receiver is for the correct value $Z = A^b$, and so the key k_{R} that the honest receiver obtains is different from both k'_0 and k'_1.

CO argue that their simulator is correct thanks to the robustness of the encryption scheme. They claim that, because there is only one key that, for any ciphertext, decrypts the ciphertext to a message different from $\perp$, then the message decrypted by the simulator and the one obtained by the honest receiver have to be equal. However, this is untrue. The problem is that the corrupt sender can compute a ciphertext with a key different from the correct key used by the honest receiver. I.e., the corrupt sender can send a random oracle query for an incorrect value and then compute a ciphertext by using the key obtained for this query. In this case, the honest receiver obtains $\perp$, but the simulator decrypts the ciphertext to a message different from $\perp$ by using the key that was sent to the corrupt sender to answer the random oracle query for an incorrect value.

To fix the simulator, we would need a mechanism that allows the simulator to check whether a random oracle query from the corrupt sender is for a correct value, i.e., $X = B^a$ or $Y = (\frac{B}{A})^a$, or not. In Section 4, we show that the simulator cannot perform this check for both X and Y unless the simulator can solve a decisional problem with overwhelming probability.

4 On the Security Against a Corrupt Sender of CO's OT

In this section, we define a decisional problem in the group $\mathbb{G}$. We prove that, if a correct simulator for CO's OT protocol for the case of a corrupt sender exists, then this simulator can be used to solve this decisional problem with overwhelming probability. Therefore, if we assume that our decisional problem cannot be solved with overwhelming probability in $\mathbb{G}$, then a correct simulator cannot be provided. However, if our problem can be solved with overwhelming probability in $\mathbb{G}$, then a correct simulator can still be provided. Our decisional problem can be solved with overwhelming probability if the DDH problem is easy to solve in $\mathbb{G}$. Therefore, it seems likely that a correct simulator can be provided if the CO's OT protocol is instantiated with gap-DH groups.

As a consequence, security for a corrupt sender does not hold solely in the random oracle model under the assumption that the encryption scheme Enc and Dec is robust, as claimed by CO. An additional requirement is that, in the group $\mathbb{G}$, our decisional problem can be solved with overwhelming probability.

Decisional problem in $\mathbb{G}$. Our decisional problem is parameterized by a group generator $\mathcal{G}$ that on input a security parameter λ outputs a group description $(\mathbb{G}, p, g)$. We define the following game between a challenger and an adversary $\mathcal{A}$. The challenger runs $\mathcal{G}$ on input the security parameter λ to get a group description $(\mathbb{G}, p, g)$ for a group $\mathbb{G}$ of prime order p with generator g. The challenger picks a random value a from $\mathbb{Z}_p$. The adversary $\mathcal{A}$ receives as input the group description $(\mathbb{G}, p, g)$ and g^a. The adversary returns to the challenger a group element B. B draws a bit b at random and proceeds as follows:

- If $b = 0$, set $Z_0 = B^a$ and $Z_1 = B^a/g^{a^2}$.
- If $b = 1$, draw randomly another bit d and proceed as follows.
    - If $d = 0$, set Z_0 as a random element in $\mathbb{G}$ and $Z_1 = B^a/g^{a^2}$.
    - If $d = 1$, set $Z_0 = B^a$ and set Z_1 as a random element in $\mathbb{G}$.

  The challenger sends the pair (Z_0, Z_1) to the adversary. The adversary outputs its guess b'. The adversary wins the game if $b' = b$.

The hardness of our decisional problem is based on the difficulty of deciding whether a value given by the challenger equals g^{a^2} or random. We conjecture that our decisional problem cannot be solved with overwhelming probability in groups $\mathbb{G}$ in which the DDH assumption holds. Concretely, we conjecture that, in such groups, the advantage of an adversary in winning the game described above is non-negligibly greater than $3/4 + \nu(\lambda)$. On the other hand, it is easy to see that, if the DDH assumption does not hold in $\mathbb{G}$, then our decisional problem can be solved with overwhelming probability.

Theorem 1 Under the assumption that our decisional problem cannot be solved with overwhelming probability in the group $\mathbb{G}$, the CO's OT protocol cannot be proven UC-secure in the random oracle model when the sender is corrupt.

Proof. We prove Theorem 1 by contradiction. We show that, if a correct simulator for the case of a corrupt sender exists, then we can use that simulator to solve our decisional problem with overwhelming probability.

First, we make the following observation. Consider an environment that sends a random bit c as input to the honest receiver. Given such an environment, any correct simulator must be able to extract correctly the messages M_0 and M_1 from the corrupt sender in order to send them to the ideal functionality. As can be seen, if the message $M_{c'}$ ($c' \in \{0, 1\}$) sent by the simulator is not correct, i.e., if it does not equal the message that the honest receiver outputs in the real world, then the simulation fails whenever the environment sends $c = c'$ to the honest receiver. We omit a formal proof of this observation.

Second, we show that, given a simulator that is able to extract both M_0 and M_1 correctly for the CO protocol, we can build a reduction R to solve our decisional problem with overwhelming probability. R interacts with the challenger and runs a copy of the simulator. R plays the role of the environment, the corrupt sender and the ideal functionality towards the simulator. The reduction R works as follows:

- R receives the instance $(\mathbb{G}, p, g, g^a)$ from the challenger.
- R, acting as the corrupt sender, sends the message $A = g^a$ to the simulator.
- R, acting as the ideal functionality, informs the simulator that the receiver has input his bit c.
- R receives a message B from the simulator. We observe that, after being informed by the ideal functionality that the receiver has input his bit c, a correct simulator must always send a message B indistinguishable from the message B produced by the honest receiver in the real world. Otherwise the simulation fails.
- R sends B to the challenger.
- The challenger sends (Z_0, Z_1) to R.
- R, acting as the corrupt sender, sends (Z_0, Z_1) as a random oracle query to the simulator.
- R receives the reply (k_0, k_1) from the simulator.
- R picks two random messages M_0 and M_1, computes $e_0 \leftarrow \mathsf{Enc}(k_0, M_0)$ and $e_1 \leftarrow \mathsf{Enc}(k_1, M_1)$, and, acting as the corrupt sender, sends e_0 and e_1 to the simulator.
- R receives two messages M'_0 and M'_1 from the simulator. If $M_0 = M'_0$ and $M_1 = M'_1$, R sends $b' = 0$ to the challenger, else R sends $b' = 1$ to the challenger.

The simulator must extract the messages M'_0 and M'_1 from e_0 and e_1 correctly with overwhelming probability. Therefore, $b = b'$ with overwhelming probability, i.e. R solves our decisional problem with overwhelming probability. As can be seen, if $b = 0$, then both Z_0 and Z_1 are correctly computed by the challenger, and thus the keys (k_0, k_1) used to compute e_0 and e_1 equal the correct key used by the honest receiver in the real world. Because the simulator must send correct messages M'_0 and M'_1 to the functionality, if $M_0 = M'_0$ and $M_1 = M'_1$ we are in the case in which Z_0 and Z_1 are correctly computed by the challenger. If $b = 1$, either Z_0 or Z_1 is computed randomly by the challenger. In this case, either k_0 or k_1 differs from the key used by the honest receiver in the real world. Namely, if $Z_{c'}$ ($c' \in \{0, 1\}$) is random, then $k_{c'}$ differs from the key k_c used by the honest receiver in the real world whenever $c = c'$. Because of the robustness of the encryption scheme, the honest receiver in the real world outputs $\perp$ whenever $c = c'$. Because the simulator must send correct messages to the functionality, in this case the simulator must send $M'_{c'} = \perp$ to the functionality and never $M'_{c'} = M_{c'}$.

5 Conclusion

We have shown that the OT protocol by CO cannot be instantiated securely with every group $\mathbb{G}$ in which the CDH assumption holds, as originally claimed by CO. We have defined a decisional problem and we have shown that, for the protocol to be secure, this decisional problem should be solvable in $\mathbb{G}$ with overwhelming probability for the protocol to be secure. Our decisional problem can be conjectured to be hard in groups $\mathbb{G}$ in which the DDH assumption is hard. If the DDH assumption does not hold in $\mathbb{G}$, our decisional problem can be solved correctly with overwhelming probability. Therefore, it is likely that the CO protocol can be securely instantitated with gap-DH groups.

Acknowledgments. We thank Claudio Orlandi for his insightful comments. Vincenzo Iovino is supported by a CORE Junior grant (no. 11299247) of the Luxembourg National Research Fund.

References

BCR87. Gilles Brassard, Claude Crépeau, and Jean-Marc Robert. All-or-nothing disclosure of secrets. In Andrew M. Odlyzko, editor, *Advances in Cryptology – CRYPTO'86*, volume 263 of *Lecture Notes in Computer Science*, pages 234–238. Springer, August 1987.

Can01. Ran Canetti. Universally composable security: A new paradigm for cryptographic protocols. In *42nd Annual Symposium on Foundations of Computer Science*, pages 136–145. IEEE Computer Society Press, October 2001.

CO15. Tung Chou and Claudio Orlandi. The simplest protocol for oblivious transfer. In *Progress in Cryptology - LATINCRYPT 2015 - 4th International Conference on Cryptology and Information Security in Latin America, Guadalajara, Mexico, August 23-26, 2015, Proceedings*, pages 40–58, 2015.

EGL82. Shimon Even, Oded Goldreich, and Abraham Lempel. A randomized protocol for signing contracts. In David Chaum, Ronald L. Rivest, and Alan T. Sherman, editors, *Advances in Cryptology – CRYPTO'82*, pages 205–210. Plenum Press, New York, USA, 1982.

GMW87. Oded Goldreich, Silvio Micali, and Avi Wigderson. How to play any mental game or A completeness theorem for protocols with honest majority. In Alfred Aho, editor, *19th Annual ACM Symposium on Theory of Computing*, pages 218–229. ACM Press, May 1987.

Kil88. Joe Kilian. Founding cryptography on oblivious transfer. In *20th Annual ACM Symposium on Theory of Computing*, pages 20–31. ACM Press, May 1988.

LM16. Baiyu Li and Daniele Micciancio. Equational security proofs of oblivious transfer protocols. *IACR Cryptology ePrint Archive*, 2016:624, 2016.

Rab81. Michael O. Rabin. How to exchange secrets with oblivious transfer. Technical Report TR-81, Aiken Computation Lab, Harvard University, 1981. Available at `http://eprint.iacr.org/2005/187`.

Wie83. Stephen Wiesner. Conjugate coding. *SIGACT News*, 15(1):78–88, January 1983.

Yao86. Andrew Chi-Chih Yao. How to generate and exchange secrets (extended abstract). In *27th Annual Symposium on Foundations of Computer Science*, pages 162–167. IEEE Computer Society Press, October 1986.