J. Cryptol. (2013) 26: 75–79
DOI: 10.1007/s00145-011-9113-2

Journal of
CRYPTOLOGY

# Analysis of an Unconditionally Secure Distributed Oblivious Transfer

Hossein Ghodosi

Department of Information Technology, School of Business, James Cook University, Townsville, Qld 4811, Australia

Communicated by Nigel Smart

Received 7 September 2010
Online publication 10 November 2011

**Abstract.** In the Journal of Cryptology (20(3):323–373, 2007), Blundo, D'Arco, De Santis and Stinson proposed a general model for unconditionally secure distributed oblivious transfer (DOT), where a sender has $n$ secrets and a receiver is interested to one of them.

We show that their "$t$-private weak one-round $(k, m)$-DOT $\binom{n}{1}$" protocol cannot prevent a receiver who attempts to obtain more than one secret. We present a modification to Blundo et al.'s protocol that fixes this problem.

**Key words.** Oblivious transfer, Secret sharing, Distributed cryptography.

## 1. Introduction

Oblivious transfer (OT) protocols [2,6] allow two interacting parties, Alice as a sender and Bob as a receiver, to exchange a secret message in an oblivious way. Execution of these OT protocols, however, requires the availability of a unique sender. Naor and Pinkas [5] introduced the concept of 1-out-of-2 distributed oblivious transfer (DOT), where Alice is replaced with $m$ servers. In [1], Blundo, D'Arco, De Santis, and Stinson generalize Naor and Pinkas's 1-out-of-2 DOT protocol to a 1-out-of-$n$ DOT protocol.

A fundamental requirement of every OT protocol is to guarantee that the receiver cannot learn anything about the secrets that he is not supposed to learn. We show that Blundo et al.'s $t$-private weak one-round $(k, m)$-DOT $\binom{n}{1}$ protocol cannot prevent a receiver who attempts to obtain more than one secret. We present a modification to their protocol that fixes this problem.

## 2. A Brief Review of Blundo et al.'s DOT Protocol

In a 1-out-of-$n$ DOT protocol, the sender has $n$ secrets, $w_0, \ldots, w_{n-1}$, and the receiver is interested in one of them, say $w_i$, where $i \in \{0, \ldots, n-1\}$. The protocol has two phases: (i) the set-up phase and (ii) the oblivious transfer phase. In the set-up phase of

the protocol, the sender provides some information to each server. Then, in the oblivious transfer phase, the receiver needs to communicate with at least $k$ servers in order to obtain the desired secret, where $k < m$. In [1], such a protocol is called a $(k, m)$-DOT-$\binom{n}{1}$.

Blundo et al. have claimed that a $(k, m)$-DOT-$\binom{n}{1}$ protocol must satisfy the following properties:

1. Correctness. Using the information acquired during the protocol execution (that involves interaction with $k$ out of $m$ servers), the receiver can compute the chosen secret $w_i$.
2. Receiver's privacy. No coalition of fewer than $k$ servers can determine which secret the receiver has recovered.
3. Sender's privacy with respect to $k-1$ servers and the receiver. A coalition of the receiver with $k-1$ dishonest servers does not learn any information about the secrets.
4. Sender's privacy with respect to a "greedy" receiver. Given the transcript of the interaction with $k$ servers, the receiver should gain information about at most a single secret, and no information about the others. This property should be satisfied even if the receiver colludes with $k-1$ dishonest servers once he has computed a secret.

In [1], Blundo et al. proposed a one-round protocol based on polynomial interpolation that satisfies the first three properties. They have stated that in DOT protocols with only one round of interaction it is impossible to achieve the fourth property. However, they have proposed a $t$-private weak one-round $(k, m)$-DOT-$\binom{n}{1}$ for achieving sender's privacy with respect to a coalition among the receiver and a subset of $t$ servers, where $t < k - 1$. This protocol is shown in Fig. 1.

## 3. Analysis of Blundo et al.'s DOT Protocol

In the sub-protocol of a $t$-private weak one-round $(k, m)$-DOT-$\binom{n}{1}$ protocol, the receiver is required to choose $n-1$ random polynomials, $Z_1(x), \ldots, Z_{n-1}(x)$, of degree $d_z$ such that $Z_1(0) = Z_2(0) = \cdots = Z_{n-1}(0) = 0$ if $i = 0$ or $Z_i(0) = 1$ for a single value $i \in \{1, \ldots, n-1\}$ and $Z_j(0) = 0$ for all values $j \neq i$. In their paper, Blundo et al. state that if the receiver contacts $k$ servers, he obtains one and only one secret, $w_i$, of his choice. This is because if the receiver chooses polynomials $Z_1(x), \ldots, Z_{n-1}(x)$ of degree $d_z$, the polynomial $V(x) = Q(x, Z_1(x), \ldots, Z_{n-1}(x))$ interpolated by the receiver will be of degree $k-1$, and therefore can be reconstructed from the information obtained from $k$ servers.

We observe that, if the chosen polynomials $Z_1(x), \ldots, Z_{n-1}(x)$ are of degree less than $d_z$, then polynomial $V(x)$ will be of degree less than $k-1$, and thus can be interpolated using fewer than $k$ points. For example, if $d_z = 0$, the resulting polynomial $V(x)$ will be of degree $d_x$, and therefore can be interpolated with information obtained from $d_x + 1$ servers. This is because the response of each server provides information about one point associated with the $V(x)$ polynomial. The following example illustrates a possible attack by the receiver on the sender's privacy, in the $t$-private weak one-round $(k, m)$-DOT-$\binom{n}{1}$ protocol.

**A sub-protocol for $t$-private weak one-round $(k, m)$-DOT-$\binom{n}{1}$** (see [1])

Let $w_0, w_1, \ldots, w_{n-1} \in F_P$ be the sender's secrets, and let $i \in \{0, \ldots, n-1\}$ be the receiver's choice.
**Set-up Phase**

- Let $d_x, d_y$ and $d_z$ be integers such that $d_x + d_z d_y (n-1) = k - 1$. The sender generates $r_0, r_1, \ldots, r_{n-1} \in_R F_P$, and sets up an $n$-variate polynomial with values in $F_P$:

$$Q(x, y_1, \ldots, y_{n-1}) = \sum_{j=0}^{d_x} \sum_{\ell_1=0}^{d_y} \cdots \sum_{\ell_{n-1}=0}^{d_y} a_{j,\ell_1,\ldots,\ell_{n-1}} x^j y_1^{\ell_1} \cdots y_{n-1}^{\ell_{n-1}},$$

  where $a_{0,\ldots,0} = r_0 w_0$, for $i = 1, \ldots, n-1$, $\sum_{\ell_i=0}^{d_y} a_{0,\ldots,\ell_i,\ldots,0} = r_i w_i$, and all other coefficients are chosen uniformly at random. It follows that $Q(0, 0, \ldots, 0) = r_0 w_0$, $Q(0, 1, 0, \ldots, 0) = r_1 w_1, \ldots, Q(0, 0, \ldots, 0, 1) = r_{n-1} w_{n-1}$.
- Then the sender constructs Shamir $(k, m)$-threshold scheme [7] for the secret $r_\ell$, where $\ell = 0, \ldots, n-1$. Let $r_\ell^j$, for $j = 1, \ldots, m$, be the corresponding shares. For $j = 1, \ldots, m$, the sender sends the $(n-1)$-variate polynomial $Q(j, y_1, \ldots, y_{n-1})$ and the shares $r_0^j, \ldots, r_{n-1}^j$ to the server $S_j$.

**Oblivious Transfer Phase**

- The receiver chooses $n-1$ random polynomials $Z_1(x), \ldots, Z_{n-1}(x)$ of degree $d_z$ such that $(Z_1(0), \ldots, Z_{n-1}(0))$ is an $(n-1)$-tuple of zeros if $i = 0$ or an $(n-1)$-tuple of zeros and a single one at the position $i$, if $i \in \{1, \ldots, n-1\}$.
- The receiver chooses a subset $X \subseteq \{0, \ldots, n-1\}$ of $k$ indices, and for every $j \in X$, the values $Z_1(j), \ldots, Z_{n-1}(j)$ are sent to the server $S_j$. He then receives the values $V(j) = Q(j, Z_1(j), \ldots, Z_{n-1}(j))$, and all the shares $r_0^j, \ldots, r_{n-1}^j$.
- After receiving the $k$ values $V(j)$, for $j \in X$, the receiver interpolates a univariate polynomial $V(x) = Q(x, Z_1(x), \ldots, Z_{n-1}(x))$ of degree $k-1$, and computes $V(0)/r_i$ where $r_i$ is constructed through the shares $r_i^j$.

**Fig. 1.** A sub-protocol for $t$-private weak one-round $(k, m)$-DOT-$\binom{n}{1}$.

*Example 1.* Assume that the sender has four secret values, $w_0$, $w_1$, $w_2$, and $w_3$, and she chooses the integers $d_x = d_y = d_z = 2$. Therefore, $d_x + d_z d_y (n-1) = k - 1 = 14$, thus the receiver is allowed to contact 15 servers in order to learn one and only one of the secret values $w_0, w_1, w_2, w_3$. However, if the receiver chooses polynomials $Z_1(x)$, $Z_2(x)$, and $Z_3(x)$ of degree 0, the interpolated polynomial $V(x)$ will be of degree $d_x = 2$, which can be reconstructed from the responses of only three servers. As a result, the receiver learns all of the secrets.

*Remark.* Generating polynomials of exact degree $d_z = d_x$, although preventing the receiver from learning more than one secret, breaches the receiver's privacy (see below).

**Theorem 1** [3,4]. *Given a Shamir $(k, n)$ threshold scheme, if the degree of the associated polynomial $f(x) = S + a_1 x + \cdots + a_{k-1} x^{k-1}$ is known to be $k-1$ (i.e. $a_{k-1} \neq 0$), then the scheme is not perfect.*

In the light of Theorem 1, if Blundo et al.'s protocol has a mechanism that forces the degree of the polynomials chosen by the receiver to be of degree $d_z$, a coalition of $d_z$ servers may learn the choice of the receiver. The following example demonstrates this threat.

*Example 2.* Let servers $S_1, \ldots, S_{d_z}$ be amongst the set of servers that the receiver has communicated with. If they collaborate in order to possibly learn the receiver's choice, they can construct polynomials $Z'_j(x)$ (for $j = 1, \ldots, n-1$) of degree at most $d_z - 1$. For each polynomial, if $Z'_j(0) = 1$, they learn that $w_j$ is not the chosen secret (because the $d_z$-degree polynomial $Z_j(x)$ chosen by the receiver must satisfy $Z_j(0) = 0$). However, if one of the interpolated polynomials $Z'_\ell(x)$, for $\ell \in \{1, \ldots, n-1\}$, satisfies $Z'_\ell(0) = 0$, the collaborating servers learn that $w_\ell$ is the choice of the receiver. This breaches the privacy of the receiver, since it is claimed (see p. 355 of [1]) that the protocol satisfies the property of receiver's privacy against a coalition of $d_z$ servers.

Note that for all indices $j \in \{1, \ldots, n-1\}$, if $Z'_j(0) \notin \{0, 1\}$, the collaborating servers learn nothing about the choice of the receiver regarding $w_j$.

We acknowledge that Blundo et al.'s protocol states the randomness of $Z_j(x)$ polynomials, and thus privacy of the receiver is guaranteed.

## 4. A Modified $t$-Private Weak One-Round $(m, k)$-DOT-$\binom{n}{1}$ Protocol

Our analysis show that in the $t$-private weak one-round $(k, m)$-DOT-$\binom{n}{1}$ protocol, achieving privacy of the receiver implies the polynomials $Z_j(x)$ chosen by the receiver be of degree at most $d_z$ (not exactly of degree $d_z$). In the meantime, the receiver must not be able to utilize the lower degree polynomials $Z_j(x)$ for learning more secrets. Both requirements can be satisfied if $Z_j(x)$ polynomials are chosen randomly, such that neither the servers nor the receiver know their exact degrees. A possible solution is as follows:

1. In the set-up phase, in addition to existing steps, the sender generates $n-1$ random polynomials $u_j(x)$ of degree at most $d_z$, subject to $u_j(0) = 0$ (for all $j = 1, \ldots, n-1$), and gives each server, $S_i$ (for $i = 1, \ldots, m$), a vector $U_i = (u_1(i), \ldots, u_{n-1}(i))$.
2. In the oblivious transfer phase, each contacted server, $S_j$, instead of responding

$$V(j) = Q\big(j, Z_1(j), \ldots, Z_{n-1}(j)\big),$$

responds

$$V(j) = Q\big[j, \big(Z_1(j) + u_1(j)\big), \ldots, \big(Z_{n-1}(j) + u_{n-1}(j)\big)\big].$$

This minor modification, which adds a zero polynomial to every $Z_j(x)$ polynomial chosen by the receiver, guarantees the randomness required by Blundo et al.'s protocol. It maintains the privacy of the receiver, and prevents the above-mentioned attack by the receiver.

## Acknowledgement

The author gratefully acknowledges the insightful comments of the anonymous referees that led the author to develop the modified protocol in Sect. 4.

## References

[1] C. Blundo, P. D'Arco, A.D. Santis, D. Stinson, On unconditionally secure distributed oblivious transfer. *J. Cryptol.* **20**(3), 323–373 (2007)

[2] S. Even, O. Goldreich, A. Lempel, A randomized protocol for signing contracts. *Commun. ACM* **28**(6), 634–647 (1985)

[3] H. Ghodosi, On insecurity of Naor-Pinkas' distributed oblivious transfer. *Inf. Process. Lett.* **104**(5), 179–182 (2007)

[4] H. Ghodosi, J. Pieprzyk, R. Safavi-Naini, Remarks on the multiple assignment secret sharing scheme, in *Proceedings of ICICS'97—International Conference on Information and Communications Security*, ed. by Y. Han, T. Okamoto, S. Qing, Beijing, P.R. China. Lecture Notes in Computer Science, vol. 1334 (Springer, Berlin, 1997), pp. 72–80

[5] M. Naor, B. Pinkas, Distributed oblivious transfer, in *Advances in Cryptology—Proceedings of ASIACRYPT 2000*, ed. by T. Okamoto. Lecture Notes in Computer Science, vol. 1976 (Springer, Berlin, 2000), pp. 205–219

[6] M. Rabin, How to exchange secrets by oblivious transfer. Technical Report TR-81, Aiken Computation Laboratory, Harvard University, USA (1981)

[7] A. Shamir, How to share a secret. *Commun. ACM* **22**(11), 612–613 (1979)