Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/jisa

One-sided leakage-resilient privacy only two-message oblivious transfer

Partha Sarathi Roy, Avishek Adhikari[*]

Department of Pure Mathematics, University of Calcutta, India

ARTICLE INFO

Article history:
Available online 7 November 2014

MSC:
94A60

Keywords:
Oblivious transfer
Leakage resilient
k-DDH

ABSTRACT

Oblivious transfer protocol (OT) is one of the key components in various cryptographic applications. Construction of OT assumes that local secret state of honest party is perfectly hidden from adversary. However, recently one primary focus of the cryptographic community is to build cryptographic tools resilient to side channel attacks. Such attacks exploit various forms of unintended information leakage which are inherent to almost all physical implementations. In this paper, we initiate a study of oblivious transfer protocol against malicious adversary in the presence of side channel attacks. Specifically, we consider a setting where a cheating sender is allowed to obtain leakage on secret state of the receiver during the protocol execution. We formalize the Definition and propose a construction of a one-sided leakage-resilient privacy only two-message oblivious transfer protocol against malicious adversary. The construction is based on Naor-Pinkas (SODA-2001) two message oblivious transfer protocol. Security of the protocol is based on *k*-DDH assumption. The proposed protocol can tolerate a constant fraction of leakage from the memory of the receiver. To achieve the proposed Definition, we assume *leak free input encoding phase* in the proposed construction.

1. Introduction

Oblivious transfer (OT) is an important primitive in the arsenal of distributed protocols. The concept of “oblivious transfer”, was introduced in the seminal work of Rabin (Rabin, 1981). However, 1-out-2 OT was suggested by Even, Goldreich & Lempel in (Even et al., June 1985). Very briefly, in 1-out-2 OT, Sender sends an ordered pair of strings (x_0, x_1) into the 1-out-2 OT machine. Receiver gives the machine a bit σ, indicating which input he would like to receive. The machine outputs x_σ to the receiver and discards $x_{1-\sigma}$. Sender knows that Receiver has one of the bits but does not know exactly which one. Crepeau (1987) showed that Rabin's OT is equivalent to 1-out-2 OT. There are many variations in OT and these are useful primitives for a variety of applications (Naor and Pinkas, 1999). These include *oblivious sampling* which may be used for comparing securely the sizes of web search engines, protocols for privately solving the *list intersection problem* and for mutually authenticated key exchange based on (possibly weak) passwords, and protocols for anonymity preserving web usage metering.

We note that the standard definition of OT, like most classical security notions, honest party needs to generate and hold local secret values which are assumed to be perfectly hidden from adversary. Unfortunately, over the last two decades, it has become increasingly evident that such an assumption may be unrealistic when arguing security in the real world where the physical implementation (e.g. on a smart card or a hardware token) of an algorithm is under attack.

[*] *Corresponding author.*
E-mail addresses: royparthasarathi0@gmail.com (P.S. Roy), avishek.adh@gmail.com (A. Adhikari).

http://dx.doi.org/10.1016/j.jisa.2014.10.002
2214-2126/© 2014 Elsevier Ltd. All rights reserved.

Motivated by such scenario, we initiate a study of oblivious transfer protocol against malicious adversary in the presence of side channel attacks. Specifically, we consider a setting where a cheating sender is allowed to obtain leakage on secret state of the receiver during the protocol execution. We note that while there has been an extensive amount of research work on leakage-resilient cryptography in the past few years, to the best of our knowledge, almost all prior works have either been on leakage resilient primitives such as encryption and signature schemes (Dziembowski and Pietrzak, 2008; Akavia et al., 2009; Dodis et al., 2009; Naor and Segev, 2009; Katz and Vaikuntanathan, 2009 and more) or leakage resilient (and tamper-resilient) devices (Ishai et al., 2003; Ishai et al., 2006; Ajtai, 2011), while very limited effort has been dedicated towards constructing leakage-resilient interactive protocols (Damgard et al., 2011; Bitansky et al., 2012; Boyle et al., 2011; Boyle et al., 2012; Ganesh et al., 2012; Garg et al., 2011). Leakage resilient zero-knowledge proof system of Garg et al. (2011) tolerates only the leakage of secret state of prover. Leakage resilient secure computation protocols of Ganesh et al. (2012) assume a leak free input encoding phase (which is an offline phase) in which each party encodes its input in a specified format. This phase is assumed to be free of any leakage and may or may not depend upon the function that needs to be jointly computed by the parties. In the interactive phase the adversary gets access to leakage of secret state of honest participants. In Ganesh et al. (2012), two constructions have been provided. One construction makes use of a fully homomorphic encryption scheme and the other construction is based only on the existence of (semi-honest) oblivious transfer. So, construction of leakage resilient OT protocol is required to accelerate the design of leakage resilient secure computation protocol and for other realistic applications.

In this direction, leakage-resilient secure OT protocols against *semi-honest* adversary have been proposed in Damgard et al. (2011) and Bitansky et al. (2012). Leakage-resilient secure OT against *semi-honest* adversary of Damgard et al. (2011) is based on the OT protocol proposed in Peikert et al. (2008). Leakage-resilient secure OT against *semi-honest* adversary of Bitansky et al. (2012) is based on non-committing encryption with oblivious key sampling (Canetti et al., 1996; Canetti et al., 2002). But to achieve more realistic model, leakage-resilient OT against malicious adversary is essential. There is no doubt that the presence of malicious adversary makes the problem more challenging and interesting. To this end, up to the best of our knowledge, we first propose Definition and construction of a one-sided leakage-resilient privacy only two-message 1-out-2 OT protocol against malicious adversary, based on the two-message oblivious transfer protocol by Naor and Pinkas (2001). To distinguish this notion of leakage of secret state of receiver from leakage of secret state of receiver and sender, we denote it by one-sided.

2. Preliminaries

In this section we are going to state some of the useful definitions, lemmas and the hardness assumption which will be used in the subsequent sections.

Definition 2.1. *The min - entropy of a random variable X is*

$$H_\infty(X) = -\log(\max_x Pr[X = x]).$$

Definition 2.2. *A random variable X is a k-source over Ω if it has min-entropy $H_\infty(X) \geq k$.*

2.1. *Hardness assumption*

2.1.1. k-*DDH assumption* (Canetti, 1997)

We say that the decisional Diffie-Hellman for *k*-sources (*k*-*DDH*) problem is hard relative to a group G if for all PPT algorithms A there exists a negligible function *negl* such that

$$\left|Pr\left[A\left(G,q,g,g_1,g^b,g_2\right)=1\right]-Pr\left[A\left(G,q,g,g_1,g^b,g_1^b\right)=1\right]\right|\leq negl(n),$$

where n is the security parameter, order of G is a prime q, g, g_1 are generators of G and the probabilities are taken over the choices of g, g_1, $g_2 \in G$, $b \in Z_q$ and b is drawn according to B for a k-*source* B over Z_q.

For simplicity we choose $n = \log q$.

2.1.2. k-*DDH game* (Damgard et al., 2011)

G is a cyclic group of order q, g & g_1 are two generators of G and L is a leakage function.

$$\beta \leftarrow Z_q$$

$$L \leftarrow \mathscr{A}_1$$

$$T = \left(g_1, g^\beta, g_1^{\beta^a \gamma^{1-a}}\right), \quad \text{where } a \leftarrow \{0,1\} \ \& \ \gamma \leftarrow Z_q$$

$$a\prime \leftarrow \mathscr{A}_2(L(\beta), T)$$

$$\mathscr{A} \text{ wins if } a\prime = a.$$

Note that in the case when $a = 0$, the view of the adversary is $T = (g_1, g^\beta, g_1^\gamma)$ and $L(\beta)$ while in the case when $a = 1$, the view of the adversary is $T = (g_1, g^\beta, g_1^\beta)$ and $L(\beta)$.

Lemma 2.1. (Damgard et al., 2011) *Let L be a function with leakage rate* $1 - \omega(\log n)/\log q$, *and assume that*

$$\left|Pr\left[A\left(G,q,g,g_1,g^\beta,g_2\right)=1\right]-Pr\left[A\left(G,q,g,g_1,g^\beta,g_1^\beta\right)=1\right]\right| \leq negl(n),$$

where q is the order of G, g, g_1 are generators of G and the probabilities are taken over the choices of g, g_1, $g_2 \in$ G, b $\in Z_q$ and β is drwan according to B for a k-source B over Z_q. Then, A wins the k-DDH game with probability at most 1/2 + negl′(n) for some negligible function negl′().

3. Leakage model

In only computational leakage model, leakage occurs not only from the content of the secret memory, but also from the intermediate computations made by the honest party.