

INFO-F-541 - Course Report

Secure computation

Université Libre de Bruxelles

Hakim Boulahya

June 6, 2018

1 Introduction

In this paper we will propose formal definitions of secure computation, also referred as secure multiparty computation. We will also give known examples in the literature that are defined following the logic of secure computation. We will then recall state of the art techniques and protocols that allow to resolve secure computations.

2 Secure computation

A secure multi-part computation problem, is a problem where a computation, or a result, must be computed but the input that each party must use is confidential and not shared between all parties. Such a problem can be defined as a function $f(\cdot)$, that takes n parameters. The idea is to be able to compute the function $f(x_0, \dots, x_n)$ where the input x_i can only be accessed by the party i . The final result is accessible to everyone.

cite $f(\cdot)$

3 Problems

There exist multiple problems that use the secure computation definition. For example the millionaires problem [Yao82], is the problem that for two millionaires they both want to know which one of them is the richer, but they don't want to know the difference. In this problem, the computation function is the usual comparison $<$, and the inputs are the incomes of the individuals.

Oblivious Transfer Another problem is the Oblivious Transfer introduced by Rabin during in 1982 [Rab]. The Oblivious Transfer has many applications and has been first introduced has a protocol to resolve the Exchange Of Secret problem. In the context of secure computation, The 1-out-of-2 Oblivious Transfer (OT_2^1), another approach to the original Oblivious Transfer, is the problem that for a sender and a receiver, one of two messages must be sent from the receiver to the sender. The message received can be chosen by the receiver.

Two constraints are that the sender must never know which message has been chosen, and the receiver must not know the content of the other message.

1-out-of- n Oblivious Transfer (OT_n^1) is an extension of OT_2^1 , where the sender has n messages to send and the receiver must choose one of them. Those two protocols are theoretically equivalent as proven in [Cr8, Cac98].

4 Original Oblivious Transfer

5 1-out-of-2 Oblivious Transfer protocol

One possible protocol for the OT_2^1 problem is by using a pair of keys using the RSA protocol, first proposed in [EGL85].

Let Alice be the sender and Bob the receiver. Alice has two messages m_0, m_1 , and in addition to that a public RSA key (e, d, n) . The protocol is a multi-step communication between the two parties using the RSA public key of Alice.

The first step is for Alice to send the public key and two random values, that is the public key (e, n) and two random values x_0, x_1 contained in the domain $[1, n - 1]$. Now that Bob has those inputs, he will generate on his side two other random values. The first one is the bit b which value is either 0 or 1, and is used to choose which random inputs received from Alice, that is x_b would be either x_0 or x_1 . The second generated random value of Bob is a value k in the domain $[1, n - 1]$.

The second step is for Bob to return his response. Since we don't want Alice to know which value has been chosen, Bob will encrypt the value x_b by blinding it using the random value k that he generated. That is Bob will send to Alice the value $v = (x_b + k^e) \bmod n$. Upon receipt of v , Alice

References

- [Cac98] Christian Cachin. On the foundations of oblivious transfer. In Gerhard Goos, Juris Hartmanis, Jan van Leeuwen, and Kaisa Nyberg, editors, *Advances in Cryptology — EUROCRYPT'98*, volume 1403, pages 361–374. Springer Berlin Heidelberg, Berlin, Heidelberg, 1998.
- [Cr8] Claude Crépeau. Equivalence Between Two Flavours of Oblivious Transfers. In G. Goos, J. Hartmanis, D. Barstow, W. Brauer, P. Brinch Hansen, D. Gries, D. Luckham, C. Moler, A. Pnueli, G. Seegmüller, J. Stoer, N. Wirth, and Carl Pomerance, editors, *Advances in Cryptology — CRYPTO '87*, volume 293, pages 350–354. Springer Berlin Heidelberg, Berlin, Heidelberg, 1988.
- [EGL85] Shimon Even, Oded Goldreich, and Abraham Lempel. A randomized protocol for signing contracts. *Communications of the ACM*, 28(6):637–647, June 1985.
- [Rab] Michael O. Rabin. How to Exchange Secrets with Oblivious Transfer.

Give proper def of RSA public key

explain rsa key pair (add a reminder section)

OT12 vs OT equivalence (check article that OT12 \nRightarrow OT but not OT12)

[Yao82] Andrew C. Yao. Protocols for secure computations. pages 160–164. IEEE, November 1982.