KASTEL – Institut für Informationssicherheit und Verlässlichkeit
Lehrstuhl Prof. Dr. J. Müller-Quade
https://crypto.kastel.kit.edu

Systematization of Protocols for Oblivious Transfer

Bachelor's Thesis

Oblivious Transfer (OT) is a cryptographic protocol that allows a sender to transfer some information to a receiver, without knowing what information the receiver actually obtains. The idea of OT was first introduced by Michael O. Rabin in 1981 [Rab05], who proposed a protocol where the sender sends a bit to the receiver with probability 1/2, and the receiver knows whether it received the bit or not, but the sender does not. Later, a more general form of OT was developed, called "1 out of 2" OT or $\binom{2}{1}$-OT, where the sender has two bits or strings and the receiver has a choice bit, and the receiver gets the bit corresponding to its choice, without revealing its choice to the sender. OT is a fundamental and important problem in cryptography, as it is sufficient to construct secure multiparty computation protocols for any computable function. It can be based on a host of different assumed-to-be-hard problems and achieve varying definitions of security. Additionally, OT extension [Ish+03] is a way to combine a small number of regular oblivious transfers with efficient cryptographic primitives such as hash functions to obtain a large number of oblivious transfers.

This thesis is intended to give an overview of the different security models proposed for OT and OT extensions, and the different hardness assumptions used to fulfill those notions.

Scope of the work

The student is expected to systematize existing literature on oblivious transfer protocols. The goals of the thesis are to

- research the literature for different approaches to obtain oblivious transfer protocols, their assumptions and security definitions. Starting points for the literature search are listed in the references below.
- compare the different approaches regarding their assumptions, security models and guarantees.

Requirements

Following prior knowledge or skills are useful, but can also be acquired while working on the thesis:

- Familiarity with cryptographic security definitions
- Experience in using a literature management software (e.g. Citavi, Zotero)

Interest in the topic is strongly recommended.

Contact

In case of interest or for further information, please contact Markus Raiber, markus.raiber@kit.edu.

References

[Ish+03] Yuval Ishai, Joe Kilian, Kobbi Nissim, and Erez Petrank. "Extending Oblivious Transfers Efficiently". In: *Advances in Cryptology - CRYPTO 2003*. Ed. by Dan Boneh. Lecture Notes in Computer Science. Springer Berlin Heidelberg, 2003, pp. 145–161. URL: https://link.springer.com/chapter/10.1007%2F978-3-540-45146-4_9.

[PVW08] Chris Peikert, Vinod Vaikuntanathan, and Brent Waters. "A Framework for Efficient and Composable Oblivious Transfer". In: *Advances in Cryptology - CRYPTO 2008, 28th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 17-21, 2008. Proceedings*. Ed. by David A. Wagner. Vol. 5157. Lecture Notes in Computer Science. Springer, 2008, pp. 554–571. DOI: 10.1007/978-3-540-85174-5_31. URL: https://doi.org/10.1007/978-3-540-85174-5_31.

[Rab05] Michael O. Rabin. *How To Exchange Secrets with Oblivious Transfer*. Cryptology ePrint Archive, Paper 2005/187. `https://eprint.iacr.org/2005/187`. 2005. URL: `https://eprint.iacr.org/2005/187`.

[RR] Peter Rindal and Lance Roy. *libOTe: an efficient, portable, and easy to use Oblivious Transfer Library.* `https://github.com/osu-crypto/libOTe`.