Post-quantum Secure Oblivious Transfer Extension

Xiaoye Wu
TU Darmstadt
xiaoye.wu@stud.tu-darmstadt.de

Tim Fischer
TU Darmstadt
tim.fischer@stud.tu-darmstadt.de

ABSTRACT

(Tim Fischer) This project aims to realize the adaptation of oblivious transfer (OT) to be secure against post-quantum attackers as part of the preparation for the epoch of quantum computation. While theoretical papers such as that of Büscher et al.[BDK+20] which adapt an efficient OT extension protocol of Asharov et al.[ALSZ17] for a quantum world, theoretically introduces and demonstrates the usability, the main goal of the project is to use their results and based on these implement an improved secure post-quantum OT extension protocol.

1 INTRODUCTION

1.1 Motivation (Xiaoye Wu)

To prepare for the epoch of quantum computation (QC), researchers are exploring post-quantum cryptography as a necessary research direction. Specifically, they strive to adapt oblivious transfer (OT) to be secure against post-quantum adversaries. OT, a pivotal cryptographic primitive in multi-party computation protocols, was first proposed by Michael Rabin[Rab81]. In the 1-out-of-2 OT, a sender sends 2 encrypted messages to a receiver, who can decrypt only one ciphertext out of the two without knowledge of the other message. Meanwhile, the sender learns nothing about which message is chosen. While theoretical studies are important, practical implementation should also consider efficiency optimization in post-quantum secure OT protocols. In practical application of protocols, the need for a large-scale number of OTs efficiently from a few “real” OTs arises. Drawing inspiration from classical OT extensions(public-key based OTs), Ishai et al.[IKNP03] proposed an OT extension protocol against semi-honest adversaries with a cost of only three hash function operations. Furthermore, Asharov et al.[ALSZ17] improved this OT extension protocol by reducing computation and communication complexity, introducing parallelization of the protocol, and using a cache-efficient algorithm for matrix transposition. Fortunately, Büscher et al.[BDK+20] demonstrated the possibility of adapting this more efficient OT extension protocol [ALSZ17]in a quantum world in their paper.

1.2 Problem with QC (Tim Fischer)

Cryptography relies on complex mathematical problems that are difficult to solve. Using these problems, many security and privacy protocols have been developed that are computationally difficult to solve with conventional computers. The problems used in these protocols are, for example, discrete logarithms, prime factorization, or collision resistance of hash functions. However, QC has the potential to solve these problems more efficiently. By using for example algorithms such as Shor’s algorithms[Sho94], discrete logarithms and the prime factorization problem can be solved in more efficient time using QC. Also, the collision resistance of hash functions can be attack by using Grover’s algorithm[Gro96], which was designed for efficient searching in unsorted databases. To maintain security, even considering QC, other stronger mathematical problems can be used. One of these is the learning with errors (LWE) problem, as well as its specialized version, the Ring-LWE (RLWE) problem, which is believed to provide security even for quantum computers. Buescher et al.[BDK+20] uses this RLWE to build a Secure Multiparty Computation protocol.

2 ROADMAP

2.1 Goals (Xiaoye Wu)

Our goals are as follows:

(1) Implement an efficient post-quantum secure OT extension protocol, as proposed by Asharov et al.[ALSZ17] using post-quantum secure OT protocol proposed by Büscher et al.[BDK+20] as the base-OT protocol.
(2) Explore the possibility of proving the post-quantum security of the improved malicious-secure OT extension protocol by Asharov et al.[ALSZ17] based on Nielsen et al.[NNOB12] is post-quantum secure.
(3) Evaluate our efficient post-quantum secure OT extension protocol based on the evaluation settings presented in the papers[ALSZ17] and [BDK+20]. Additionally, we will benchmark other state-of-the-art post-quantum secure OT protocols(e.g., [BNOB18] and [BDGM18]).
(4) Write the final report, including our learning or possible problems which occurred during the processing.

We will write test codes according to the Code for "Secure Two-Party Computation in a Quantum World" by N. Büscher et al.[BDK+20] at https://encrypto.de/code/pq-mpc.

2.2 Timeline (Tim Fischer)

In this section, we explain what steps we are planning. The project is planned for the period from 01.05.2013 to 31.07.2013. The rough schedule for our project is described in the timeline table 1. These milestones or dates may change as the project progresses. Before we can start working directly on our first goal, implementing a secure post-quantum OT extension protocol, we will spend the first three weeks reviewing related work, including that of Asharov et al.[ALSZ17] and Büscher et al.[BDK+20]. In the following half week, we will set up the basic project environment. The next two weeks will be devoted to the technical design of the protocol. In the sixth and seventh week, we want to fulfill our first goal by implementing this protocol, as well as work on our second goal to explore if we can prove post-quantum security. After that, we plan to spend half a week for our third goal, evaluating whether our application works as expected. In the last three weeks of this project, we will end the fourth goal by write the final report.

Milestone	Description	Timing
Literature review	Read related papers	05/28/2023
Project setup	Setting up basic project environment and repository	05/31/2023
Design protocol	Technically design how the adjusted protocol should work	06/14/2023
Implementing Protocol	Implementation of the protocol design	06/30/2023
Evaluating	Check if our goals are reached and Implementation is working as expected	07/04/2023
Final report	Writing and submitting the final report	07/31/2023

Table 1: Roadmap

REFERENCES

[ALSZ17] Gilad Asharov, Yehuda Lindell, Thomas Schneider, and Michael Zohner. More efficient oblivious transfer extensions, 2017.

[BDGM18] Pedro Branco, Jintai Ding, Manuel Goulao, and Paulo Mateus. Universally composable oblivious transfer protocol based on the rlwe assumption. *IACR Cryptol. ePrint Arch.*, 2018:1155, 2018.

[BDK+20] Niklas Büscher, Daniel Demmler, Nikolaos P. Karvelas, Stefan Katzenbeisser, Juliane Krämer, Deevashwer Rathee, T. Schneider, and Patrick Struck. Secure two-party computation in a quantum world, 2020.

[BNOB18] Paulo Barreto, Anderson Nascimento, Glaucio Oliveira, and Waldyr Benits. Supersingular isogeny oblivious transfer (siot). *arXiv preprint arXiv:1805.06589*, 2018.

[Gro96] Lov K. Grover. A fast quantum mechanical algorithm for database search. In *Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing*, STOC '96, page 212–219, New York, NY, USA, 1996. Association for Computing Machinery.

[IKNP03] Yuval Ishai, Joe Kilian, Kobbi Nissim, and Erez Petrank. Extending oblivious transfers efficiently. In Dan Boneh, editor, *Advances in Cryptology - CRYPTO 2003*, pages 145–161, Berlin, Heidelberg, 2003. Springer Berlin Heidelberg.

[NNOB12] Jesper Buus Nielsen, Peter Sebastian Nordholt, Claudio Orlandi, and Sai Sheshank Burra. A new approach to practical active-secure two-party computation. volume 7417, pages 681–700. Springer, 2012.

[Rab81] Michael O Rabin. How to exchange secrets by oblivious transfer. *Tech. Memo TR-81, Aiken Computation Laboratory, Harvard University*, 1981.

[Sho94] Peter W. Shor. Algorithms for quantum computation: discrete logarithms and factoring. *Proceedings 35th Annual Symposium on Foundations of Computer Science*, pages 124–134, 1994.

Erklärung

Hiermit versichern wir, die vorliegende Praktikumsarbeit ohne Hilfe Dritter und nur mit den angegebenen Quellen und Hilfsmitteln angefertigt zu haben. Alle Stellen, die Quellen entnommen wurden, sind als solche kenntlich gemacht worden. Diese Arbeit hat in gleicher oder ähnlicher Form noch keiner Prüfungsbehörde vorgelegen. Uns ist bekannt, dass im Falle eines Plagiats (§38 Abs. 2 APB) ein Täuschungsversuch vorliegt, der dazu führt, dass die Arbeit mit 5,0 bewertet und damit ein Prüfungsversuch verbraucht wird.

Approved: Xiaoye Wu
Xiaoye Wu

Approved: _____
Tim Fischer

(English translation)
Statement

We herewith formally declare that we have written the report independently of any outside support except for the quoted literature and other sources mentioned in the paper. We clearly marked and separately listed all of the literature and all of the other sources which we employed when producing this academic work, either literally or in content. This report has not been handed in or published before in the same or similar form. We are aware, that in case of an attempt at deception based on plagiarism (§38 Abs. 2 APB), the report would be graded with 5,0 and counted as one failed examination attempt.