


Titel

Bachelor's Thesis Proposal
by Ella Vahle

Arbeitsgruppe 
Codes und Kryptographie

1 Introduction

Secure multiparty-computation (MPC) is a concept for securely computing (potentially probabilistic) functions with multiple parties involved. Each party has private input which must not be disclosed to the other parties. Based on these, the different parties jointly execute a protocol to obtain the functions result. In this context security refers to the privacy of parties' inputs and correctness. To achieve privacy the protocol has to ensure that no information about one party's input is leaked to any other parties. Correctness is attained when the computed result equals the functions output based on the given input.

Secure multiparty-computation has many practical areas of application, one being stable matching algorithms. Matching algorithms are used to match members of two different sets to each other with regards to their respective preferences. A stable matching is achieved when there are no two members (one from each set) that aren't matched to each other, such that they would rather be matched to each other than to their assigned matches.

Such algorithms are used to for example match residents to residency programs or students to public schools [TODO Zitat]. Obviously the best solution would be that every member is assigned to their first preference, but in reality this is rarely possible. Stable matchings are a desirable solution in such cases to still achieve a high level of member satisfaction and in some sense fairness.

One solution for computing a stable matching is the Gale-Shapley algorithm, developed by David Gale and Lloyd Shapley [TODO Zitat], which will also be the one we are interested in.

To provide a solution which is more applicable in reality without sacrificing security, Doerner et al. [TODO Zitat] introduce a new oblivious data structure called "Oblivious Linked Multi-List" and make use of it during the execution of the Gale-Shapley algorithm. The data structure uses data arrays combined with a method by Zahur et al. [TODO Zitat] to obliviously permute them. This provides the means to obliviously access data, thus hiding access patterns and the derivable information. The authors claim that using the Gale-Shapley algorithm combined with the Oblivious Linked Multi-List

ensures security in the honest-but-curious attacker model. Honest-but-curious attackers don't actively interfere with the protocol. They follow instructions correctly and act as expected but try to learn more from the execution than they are supposed to. This could for example be learning about one party's preferences based on the order they are accessed in. Even though the authors give a rough intuition provided in the form of explaining arguments as to why security holds in this setting, it has not been formally proven yet.

2 Current state of research

As mentioned above there are general purpose frameworks for MPC applicable to arbitrary functions. They take an arbitrary function and convert it so that MPC protocols can be applied. The idea of these has been around for many decades already but were not used in real-world applications for a long time because they were not efficient enough [TODO Zitat]. Over the years technical advances allowed for more feasible implementations leading to the development of various products, including tools like EMP-toolkit, Obliv-C or OblivM. Even though there were huge improvements there are still limitations. In addition to efficiency problems Hastings et al. [TODO Zitat] for example point out lack of documentation and correctness errors [TODO Zitat]. One alternative way to securely compute a stable matching without expensive adjustments to classic protocols is to outsource the computation to a trusted third party. This way, both parties' inputs stay hidden to the other party and are only revealed to the commonly trusted party. Relying on a commonly trusted party has many disadvantages. In many cases it is not even possible to find such a party. But even if it is possible it can be hard to find one and entail a lot of efforts.

To avoid this, even prior to Doerner et al. [TODO Zitat] specific-purpose protocols to compute a stable matching that are carried out between the involved parties only were developed. Stable matching in the context of multiparty-computation comprises multiple different aspects, such as data access strategies or the underlying algorithm. Both of these are research topics of their own with several possible approaches and solutions. Naturally this yields various possibilities of combining them to solve the problem of securely computing a stable matching. As opposed to the discussed approach by Doerner et al. [TODO Zitat] which uses the Gale-Shapley algorithm, Blanton et al. [TODO Zitat] for example use Breadth First Search. Some examples of work prior to Doerner et al. [TODO Zitat] are the protocols of Golle [TODO Zitat] with roughly $O(n^5)$ public-key operations [TODO formatieren] or the previously best implementation of the Gale-Shapley algorithm with a runtime of over 33 hours, working on sets of 512 members each [TODO Zitat].

3 Goals of the thesis

As can be seen in the previous section, the problem with most current solutions is feasibility. Even though they guarantee security against different kinds of adversaries,

they are not suited to be used in real world applications because of the operational time the different measures incur.

To provide a solution which is more applicable in reality without sacrificing security, Doerner et al. [TODO Zitat] introduce a new oblivious data structure called "Oblivious Linked Multi-List". The data structure uses data arrays combined with a method by Zahur et al. [TODO Zitat] to obliviously permute them. This provides the means to obliviously accessing data, thus hiding access patterns and the derivable information. Even though the authors claim that usage of the Oblivious Linked Multi-List ensures security in the honest-but-curious attacker model, it has not been formally proven yet. The goal of this thesis is to formalize the rough intuition given by Doerner et al. [TODO Zitat] and provide a formal proof based on the Simulation Technique introduced by Goldreich [TODO richtig aufschreiben/Zitat]. It was later explained by Lindell in an extensive Tutorial [TODO Zitat] which will also be used as a basis for this thesis.

To do so the whole approach will first be sectioned into its different components such as the Oblivious Linked Multi-List and the Gale Shapley algorithm using it. After proving security for both parts separately we will achieve security for the overall construction.

With regard to optional topics I see (there are) two possible scenarios. The first one is that in the course of working with the presented protocol and its proof of security, it becomes clear that the assumption about the protocols security in context of the presented security model doesn't hold. In this case the first step would be to examine and explain the problems that arise. The insights gained could be used to identify a different, weaker security model that solves the problems the initial protocol implied. With such an altered security model a proof can then again be attempted.

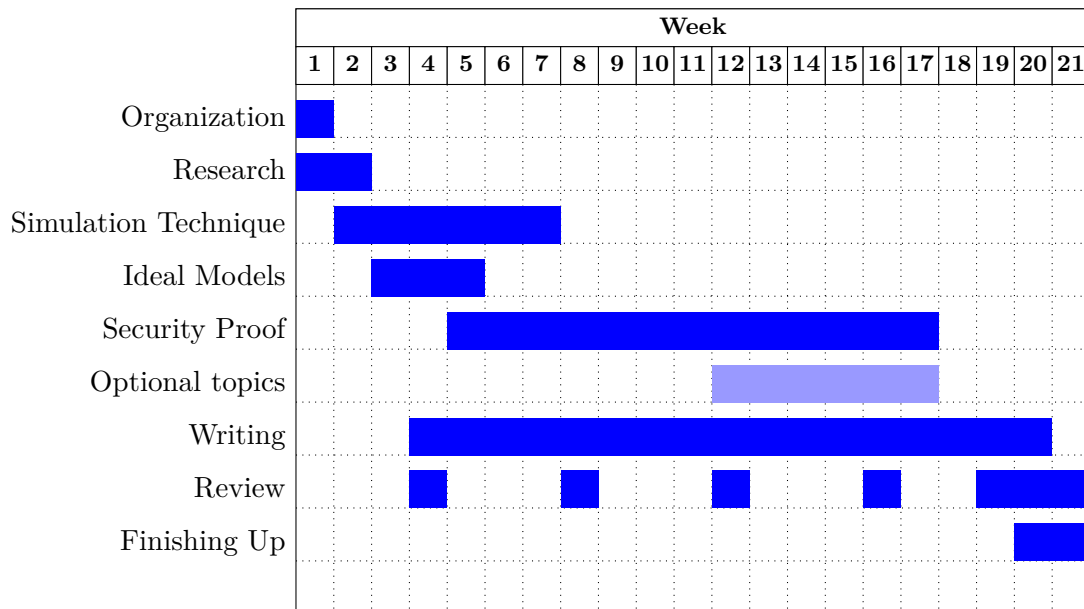
The second one is that the proof turns out to be more straight forward than expected. A reasonable course of action could be to go a step further and investigate how the proven security transfers to other security models, such as an active attacker scenario.

4 Preliminary outline of the thesis

1. Introduction
2. Definitions and notation
 - a) General
 - b) MPC
 - c) Simulation Technique
3. Prior knowledge
 - a) ORAM
 - b) Gale-Shapley
4. Oblivious Linked Multi-lists
 - a) Ideal model

- b) Construction
 - c) Security
 - d) (optional) Security under different security model (i.e. stronger or weaker depending on the prior results)
- 5. Applying Oblivious Linked Multi-lists to Gale-Shapley
 - a) Ideal model
 - b) Construction
 - c) Security
 - d) (optional) Security under different security model (i.e. stronger or weaker)
- 6. Conclusion
- 7. References

5 Work plan



Date:

Prof. Dr. Johannes Blömer

Ella Vahle