UNIVERSITÄT PADERBORN
Die Universität der Informationsgesellschaft

Titel

Bachelor's Thesis Proposal
by Ella Vahle

Arbeitsgruppe
Codes und Kryptographie

1 Introduction

Secure multiparty-computation (MPC) is a concept for securely computing functions with multiple parties involved. In this context security refers to the different parties' private inputs' confidentiality. The goal is to collectively execute a protocol and as a result obtain the wanted output without the necessity to reveal said private data.
Secure multiparty-computation yields 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. Such algorithms are used to for example match residents to residency programs or students to public schools [TODO Zitat]. 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. 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 achive 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. More precisely we will examine a newly constructed data structure for obliviously managing data in combination with the classic Gale-Shapley algorithm, which yields a supposedly secure version.

2 Current state of research

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. The approach presented by Doerner et al. [TODO Zitat] for example is based on the Gale-Shapley algorithm, whereas Blanton et al. [TODO Zitat] based their construction on Breadth First Search.

One 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 is only revealed to the commonly trusted party.
To avoid the efforts a trusted third party entails protocols that are carried out between the two parties only were developed. Some examples are the ones 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 strucure called "Oblivious Linked Multi-List". The data structure uses data arrays combined with a method by Zahur et al. [TODO Zitat] to obliviously permutate them. This provides the means to obliviousy 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 for example introduced by Lindell [TODO Zitat].
To do so the whole approach will first be sectioned into it's different components such as the Oblivious Linked Multi-List and the Gale Shapley algorithm using it. After proving security for both parts seperately 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 it's 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.
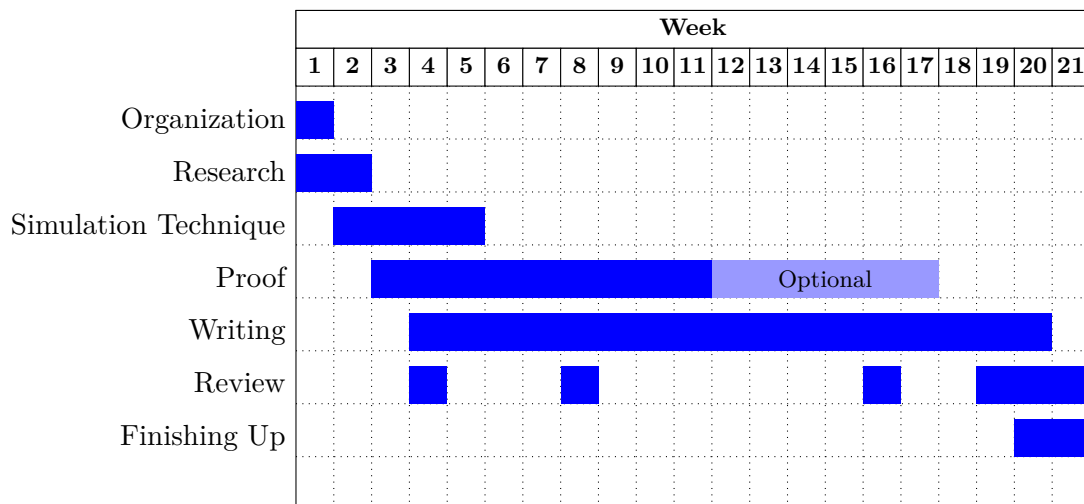The second one is that the proof turns out to be more straight forward than expected. A reasonable course of action could be to go a step further and investigate how the proven security transfers to other security models, such as an active attacker scenario.

4 Preliminary outline of the thesis

1. Introduction

2. Definitions and notation

3. Prior knowledge
   a) ORAM
   b) Gale-Shapley

4. Oblivious Linked Multi-lists
   a) Construction
   b) Security
   c) (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) Construction
   b) Security
   c) (optional) Security under different security model (i.e. stronger or weaker)

6. Conclusion

7. References

5 Work plan

	Week																				
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21

Organization
Research
Simulation Technique
Proof — Optional
Writing
Review
Finishing Up

Date:

_____   _____
Prof. Dr. Johannes Blömer   Ella Vahle