Review of the PhD thesis of Ida Tucker

Ivan Damgård

Department of Computer Science, Aarhus University

1 Overview

The thesis of Ida Tucker (IT) is entitled "Functional encryption and distributed signatures based on projective hash functions, the benefit of class groups" and is organized in 6 chapters. The first one contains an introduction with background and history on the main subjects of the thesis, as well as a summary on the contributions of the thesis. Then follows some preliminaries along with a survey of known concepts and results in chapter 2. In chapters 3, 4 and 5, the research results of the thesis are presented. Finally, in chapter 6, a conclusion and some opens problems are presented.

Overall, the thesis is very carefully worked out. It is not only a collection of papers, but a consistent and modular exhibition of the constructions put forward.

The results in the thesis are mainly based on four papers that IT co-authored, one of which is in submission and the others appeared at AsiaCrypt 2018, Crypto 2019 and PKC 2020, all of them major and highly respected venues in Cryptography.

2 Evaluation

2.1 Chapters 1 and 2.

These chapters give a comprehensive and carefully written introduction to a large number of known concepts that are important in the thesis. Particular attention is given to the CL framework (which I will come back to in a moment) which forms the basis of all the work in the thesis. These chapters clearly prove that the author masters her field and is on top of the latest developments.

2.2 Chapter 3.

This chapter describes the framework of Castagnos and Laguillaumie (the CL framework), that forms the foundation of the work in this thesis. The notable property of this framework is that it allows to build from class groups a setting where we have a group of large unknown order, which nevertheless contains a cyclic group of known prime order q which can be chosen according to one's needs when the group is instantiated. Furthermore, the discrete logarithm problem in the subgroup is easy, but nevertheless certain decision problems in the group as a whole can still reasonably be assumed to be hard.

It was already known that one can build a CPA secure and linearly homomorphic cryptosystem from the CL framework, very similar to Damgård and Jurik's variant of the Pailler's cryptosystem. This thesis takes this number of steps forward by using the CL framework and some new hardness assumption to build projective hash functions with additional homomorphic properties. This leads to a much more powerfull tool than the CL framework might seem to be a first sight: the projective hash functions suggested by IT can be used to build CPA-secure homomorphic encryption but also much more, as detailed in the next chapters.

Finally, Chapter 3 introduces a number of zero-knowledge proofs for use with the cryptosystems. For instance, one has to remember that even the property of being a valid ciphertext is not something anyone can verify (as is the case for Paillier), but it can be proved in ZK by the party who encrypts the data.

2.3 Chapter 4.

In this chapter, a functional encryption scheme is developed that allows computation of the inner product of a plaintext and a vector in the secret decryption key. Notably, the construction is generic, based on projective hash functions. While the constructions are similar to previous work, the underlying projective hash functions can be assumed to have new and stronger properties when based on the CL framework and this allows tighter security reductions and hence more efficient instantiations.

2.4 Chapter 5.

This chapter is concerned with a distributed implementation of the EC-DSA signature scheme. This signature scheme is interesting because it is very widely used in practical applications, and is often used to protect data of great value, for instance in the Bitcoin system. To improve security of a practical instance of the scheme, a distributed implementation where the secret key is shared between several parties, is very useful,

A large number of such distributed schemes were known before, but most of them are quite inefficient, particularly when it somes to schemes for dishonest majority. This is partly due to the use of the Paillier encryption scheme in these constructions. Paillier is attractive because it is linearly homomorphic and decryption is efficient even of the plaintext space is large. But the plaintext space is always $\mathbb{Z}_n$ for a large composite n, whereas when working with EC-DSA one would like to replace this by $\mathbb{Z}_q$ for a prime q. This "incompatibility" can be handled, but at the expense of more work and larger communication complexity. In this chapter, IT observes Paillier can be replaced by an encryption scheme based on CL framework. Such a scheme can be designed to have plaintext space $\mathbb{Z}_q$, then the incompatibility problem disappears and one gets a more efficient scheme.

3 Conclusion

The thesis of Ida Tucker is of high international standard, it contains interesting and useful research results and is clearly sufficient for awarding the PhD degree in Computer Science. Thus I recommend, of course, that the thesis is defended.

August 31, 2020, Ivan Damgård,
Professor, Phd.

Dept. of Computer Science, Aarhus University,
Aabogade 34, 8200 Aarhus N, Denmark.