DI/ENS

ENS, CNRS, INRIA, UMR 8548

Ecole Normale Supérieure

DI - Département d'Informatique

Dr. Michel Ferreira Abdalla
École normale supérieure
Département d'Informatique
45 rue d'Ulm
75230 Paris Cedex 05
Tel: +33 1 44 32 21 13

Paris, 18 September 2020

Subject: **Report on Ida Tucker's thesis manuscript "*Functional encryption and distributed signatures based on projective hash functions, the benefit of class groups*"**

The subject of Ida Tucker's thesis is the construction of advanced cryptographic primitives based on projective hash functions. The concept of project hash functions was introduced by Cramer and Shoup in 2002 and used to build encryption schemes secure against active attacks (chosen-ciphertext-secure) under different complexity assumptions. Since its introduction, the concept of project hash functions has been extensively used in the construction of cryptographic primitives, such as password-authenticated key exchange, oblivious transfer, and lossy encryption.

In her thesis, Ida provided further contributions to the concept of project hash functions by identifying novel homomorphic properties and using it to build new functional encryption and threshold signature schemes and new zero-knowledge proof and argument protocols. In addition, Ida provided new instantiations of projective hash functions from class groups of imaginary quadratic fields. The level of these contributions is certainly very high, making this a thesis of exceptional quality. In particular, several of the results already led to publications in top-teer general and area conferences in the field, including CRYPTO, ASIACRYPT, and PKC.

The overall presentation is thematically consistent and of a fairly high quality, demonstrating that Ida put a lot of effort into the writing. For instance, the use of three running examples based on the decision Diffie-Hellman assumption in finite fields and two other assumptions in class groups (HSM-CL and DDH-f) is quite helpful and makes the contents of the thesis more accessible to the reader.

The document itself is organized in 6 chapters, with the core of the contributions appearing in Chapters 3, 4, and 5. The presentation of these chapters is intuitive and differs from that of Ida's published and ongoing articles. In particular, the underlying tools that were developed to build the more advanced cryptographic primitives in Chapters 4 and 5 are detailed in Chapter 3.

Chapter 1 provides a general introduction to the manuscript and highlights the importance of designing practical advanced cryptographic tools that can enable fine-grained access to information and be robust against key compromise. This chapter also provides a general introduction to project hash functions and to class group cryptography. This chapter also summarizes in a clear and detailed manner the main contributions of this thesis.

Chapter 2 introduces necessary notations and basic notions used in thesis. This includes standard complexity assumptions, such as Decision Diffie-Hellman (DDH) and Decisional Composite Residuosity (DCR); primitives such as signatures, linearly homomorphic encryption, and zero-knowledge proofs; and basic technical background on ideal class groups of orders of an imaginary quadratic field. In this chapter, Ida also highlights the difficulties of dealing of groups of unknown order, especially in the context of zero-knowledge arguments, which is quite relevant for threshold signature constructions presented in Chapter 5. The presentation is quite fluid and easy to follow.

Chapter 3 is devoted to enriching the CL framework, originally developed by Castagnos and Laguillaumie in 2015, and contains several new results. In particular, Ida identifies and formalizes new complexity assumptions on class groups and use it to build new families of projective hash functions in these groups. Ida then shows how to use the latter to build new linearly homomorphic encryption schemes with prime-order message space and zero-knowledge proofs and arguments for these schemes. As mentioned in the thesis, some of the complexity assumptions being introduced, such as LO and SR assumptions, are not strictly necessary for security, but they allow to significantly improve the efficiency of some of the protocols in a provable manner.

The results in Chapter 3 are non-trivial and extremely technical but Ida did an excellent job in making them accessible by clearly describing the intuition behind the main constructions. The use of the three running examples, one of which is based on the standard DDH assumption, greatly helps with the understanding, especially for those who are not familiar with class groups. The results in this chapter appeared in several of top-teer publications.

Chapter 4 focuses on the construction of inner-product functional encryption schemes. These are schemes which allow the owner of the master secret to delegate to third parties the computation of different statistics over the encrypted data. This chapter contains several new important contributions to the functional encryption area. In particular, it provides new generic constructions of inner-product functional encryption schemes from projective hash functions which are secure against both passive and active adversaries. This is done by carefully identifying new properties of projective hash functions, such as vector smoothness and vector universality, and using it to build new schemes with tight security proofs. I would like to stress that the result achieving a tight security proof for the scheme secure against active attacks is quite nice and unexpected, since it was not clear how to overcome the looseness of previous security reductions. The fact that this was achieved without sacrificing efficiency and in a generic manner is quite impressive and seems to indicate that projective hash functions appear to be the right abstraction for the construction of inner-product functional encryption schemes. The results in this chapter are part of two papers, one which appeared at ASIACRYPT 2018 and one which is currently under submission.

Chapter 5 is dedicated to the construction of new threshold signature protocols for the standardized elliptic-curve digital signature algorithm (EC-DSA) and contains several significant results. This includes a generic solution for two-party EC-DSA setting together with a C implementation of the latter as well as a new bandwidth-efficient full threshold EC-DSA construction. To achieve these results, Ida exploited the fact that, by using class groups, one can choose the message space of the encryption scheme to be of the same prime order as that used to compute EC-DSA signatures, therefore avoiding the need for range proofs and significantly reducing bandwidth consumption compared to prior schemes. Moreover, in the case of the full threshold EC-DSA, Ida also makes use of several zero-knowledge arguments developed in Chapter 3 to improve the efficiency of these schemes. The results in this chapter appeared at CRYPTO 2019 and PKC 2020. As in previous chapters, the text is clear and easy to follow.

Chapter 6 concludes the manuscript by recapping all the contributions of the thesis and listing a few open problems.

Conclusion. Ida Tucker's thesis manuscript contains several results concerning the construction of advanced cryptographic primitives from class groups. Most of these results are quite significant, such as the new two-party EC-DSA and the construction of efficient inner-product encryption schemes secure against active attacks. Some of these results are also unexpected and highly non-trivial, such as the tight security proof for the inner-product functional encryption schemes. Overall, the thesis is very well written and clearly demonstrates the tremendous effort that Ida put into making it easy to follow and accessible. It also clearly demonstrates a deep understanding of the field, its challenges and open problems.

Recommendation. For the above reasons, I express a very favorable opinion for Ida Tucker to defend her thesis before the committee on the scheduled date.

Please feel free to contact me if I can be of further assistance.

Yours sincerely,

Michel f. Abdalla

Michel Ferreira Abdalla
CNRS Research Director
ENS Adjunct Professor
michel.abdalla@ens.fr