AARHUS UNIVERSITY

FACULTY OF NATURAL SCIENCES

**RECOMMENDATION**
**PHD DEGREE**

# Nikolaos Melissaris Papanikolaou

## PhD thesis

Title of PhD thesis: Better, Faster, Stronger – Improving Security, Efficiency, and Primitives for MPC
Graduate programme: Computer Science
Submitted on 25 November 2024

## Supervisors

Main supervisor: Associate Professor Peter Scholl, Department of Computer Science, Aarhus University
Co-supervisor: Professor Claudio Orlandi, Department of Computer Science, Aarhus University

## Assessment Committee

Member of assessment committee:
Professor Manoj Prabhakaran, Department of Computer Science and Engineering, IIT Bombay, India
Member of assessment committee:
Associate Research Professor Ignacio Cascudo, IMDEA Software Institute, Madrid, Spain
Chair: Associate Professor Peyman Afshani, Department of Computer Science, Aarhus University

## Introduction

The PhD thesis by Nikolaos Melissaris Papanikolaou is titled "Better, Faster, Stronger – Improving Security, Efficiency, and Primitives for MPC" and it is 206 pages long, including the bibliography. The thesis is written in English with a one-page Resumé written in Danish. The thesis contains two parts and nine chapters. Chapters 6 to 9 are based on two publications, one manuscript under review and one manuscript that is yet to be submitted. The two publications have appeared in high-quality and peer-reviewed venues.

SOLIDUM PETIT IN PROFUNDIS · UNIVERSITAS ARHUSIENSIS ·

# Assessment

## Chapter 1

The chapter is an introductory chapter which mainly serves the purpose of presenting the central concept of the thesis, secure multiparty computation (MPC), and the different definitions of security that are usually considered. The introduction addresses all necessary concepts to understand the goal of MPC and the different security properties it may be required to satisfy depending on the context (adversarial models, and output delivery guarantees) as well as some of the basic tools used in MPC (secret sharing, homomorphic encryption, oblivious transfer). In general, the introduction is well written, but perhaps the part about the basic security definition and the intuition behind the concept of simulator and the real-world/ideal-world paradigm could have been written with some more details for a reader not familiar with the text.

## Chapters 2-4

These chapters introduce the results included in the thesis, and frames them in terms of a common theme of improving various aspects of secure Multi-Party Computation (MPC). Chapters 2-4 serve as brief technical overviews of chapters 6-9, which we assess in detail below.

## Chapter 5

The chapter is a list of articles and manuscripts of Nikolaos Melissaris Papanikolaou.

## Chapter 6 and Section 2.1

This chapter involves the notion of MPC with identifiable abort. This is a class of MPC protocols that enhance the usual security-with-abort model by allowing parties to identify at least one cheater. The chapter details work published in Crypto which presents a new efficient protocol in this setting. The protocol uses lighter techniques than previous works in the same setting and only requires a preprocessing phase that produces similar authenticated information as in secure-with-abort protocols. The work introduces some technical tools: a compiler transforming some types of protocols into others with identifiable cheaters (itself a new notion); and a technical tool called online extractability that captures certain types of UC secure protocols.
The work also includes efficiency comparisons with other protocols with identifiable abort as well as with MPC protocols that are only secure-with-abort, which gives a good idea of what is the overhead incurred in by requiring identifiable abort, at least in this work.

The chapter hence advances the state of the art in a natural class of secure multiparty computation protocols, with practical importance. It is also well written, which is to be expected since it is based on a publication in a strong venue such as Crypto.

## Chapter 7 and Section 2.2

This chapter discusses research regarding multiparty computation with friends and foes, and is based on a work published in INDOCRYPT. This is a relatively new security model in multiparty computation proposed by other authors five years ago. The model strengthens the usual standard security against malicious adversaries by reckoning with the fact that in the usual model, a malicious adversary corrupting some parties can still leak information to some other semi-honest parties which are not corrupted by this adversary, even if the adversary does not get any advantage for itself. The goal of this new security model is to avoid this leakage.

The results presented in this thesis advance the state of the art in two ways: first, by finding separation results with respect to other security notions that a priori might be related, namely "security against a mixed adversary" and "best of both worlds security"; second, by presenting two new constructions of MPC protocols which are secure in this model and improve in different ways the existing protocols: in one case the result constitutes the first constant-round protocol against threshold-optimal adversaries and achieves so-called "weak FaF security", while in the other case, the protocol presented is the first one which achieves "strong FaF security" against adversaries for all thresholds that were not known to be impossible from previous results, therefore characterizing exactly the thresholds for which strong FaF security is possible.

The results therefore motivate this new security model by establishing that it is not equivalent to other known models, and advance the knowledge of what is possible in this model.

Potential minor improvements to this section, although none of them really essential, would be:

Mentioning what are the known results in terms of feasibility for mixed adversaries and best of both worlds security. This would further help comparing the security notions in this text.

Making explicit whether the separation results apply to strong/weak FaF. It seems that the results should apply in the strongest possible sense (i.e. FaF should not imply any of the other notions, and the other notions do not imply weak FaF) but it would be nice to say it explicitly.

Finally an interesting comment would be that the separation result where FaF does not imply BoBW security in fact seems to extend to the fact that FaF does not even imply security against 1 semihonest party. This is all as long as the number of malicious parties in the FaF definition is assumed to be t>0, which is tacitly assumed. This is reminiscent of the known fact that, depending on how one defines semihonest security, security against malicious parties does not imply security against semihonest parties. All this can however be discussed further in the defense.

## Chapters 3 and 8

These chapters construct a “Pseudorandom Correlation Generator” (PCG) and a “Pseudorandom Correlation Function” (PCF) for a “permutation correlation” (in which party $i$ gets $p(i)$, where $p$ is a random permutation). PCGs and PCFs for certain correlations have been very popular recently, thanks to their implications for practically efficient MPC. This work motivates extending PCGs and PCFs to permutation

correlations, with a couple of interesting applications. Further, for the special case of 3 parties, a PCG and a PCF are constructed, based on a recently proposed hardness assumption.

The construction is clever, and it is non-trivial to get everything working. It certainly merits being part of this thesis, thanks to the technical quality and the novelty. The presentation is also by and large clear. However, the organization of the chapter could potentially be improved:The PCG construction could be a whole section in the chapter (8.3) and the PCF construction, along with the preliminaries on HSS could be a separate section (8.4).

### Chapters 4 and 9

These chapters deal with a construct called "Structured-Seed Local Pseudorandom Generator." It includes the definition, and two constructions that meet this definition. The security of the constructions are based on assumptions of hardness of "Learning Parity with Noise" under different noise distributions. The chapter also outlines four applications of this construct, one of which is to MPC.

The results are technically non-trivial and quite interesting, and worthy of being part of this thesis. The main weakness of this chapter is the editorial quality. Some are mentioned below.

Section 9.3, which gives the formal definition of a Structured-Seed Local PRG, opens with two sections (9.3.1 and 9.3.2) which define "noisy local PRG." This makes it seems as that the main definition in 9.3.3 relates to such a noisy local PRG. However the term "noisy" does not appear anywhere in the thesis outside of the two sections 9.3.1 and 9.3.2. If noisy local PRGs are not relevant to the rest of the thesis, these sections could be removed. If they are needed, it should be clearly mentioned where they are relied upon, along with a clarification as to why the applications are unaffected by the PRG being "noisy."

Another major issue with this chapter is the discussion which promises future results in ongoing work. Indeed, in Section 9.1.2 says "The current version of our *paper* is a work in progress" (emphasis added) and goes on to talk about "posting this working draft on ePrint." This discussion seems out of place and a separate "Conclusion/Future Work" chapter would be a more suitable place for it.

It was not clear to the committee which parts of Section 9.4 are original work and which are directly based on prior work. The proofs/intermediate steps directly borrowed from prior work could be moved to an Appendix, and only the relevant summary included in the main body.

## Summary

The thesis includes several technically non-trivial results in theoretical cryptography, most of which have been published in reputable peer-reviewed conferences. The amount of original research and the technical quality are above the bar for a PhD thesis. The main weakness of the thesis is perhaps its editorial quality.

AARHUS UNIVERSITY

# Recommendation

The thesis is eligible for conferral of the PhD degree and can therefore proceed to defence.

Date: 27th of Jan, 2025

On the authority of the assessment committee consisting of Manoj Prabhakaran, Ignacio Cascudo, and Peyman Afshani

Chair of the assessment committee,
Peyman Afshani

SOLIDUM PETIT IN PROFUNDIS · UNIVERSITAS ARHUSIENSIS ·