Aggelos Kiayias
Chair in Cyber Security and Privacy
Informatics Forum
University of Edinburgh
10 Crichton Street
Edinburgh - EH8 9AB
TEL.: +44 (0) 131 6505129
akiayias@ind.ed.ac.uk

To: Professor Damian Niwiński, head of the committee
Re: Grzegorz Fabiański

October 2nd, 2026

Dear Professor Niwnski,

This is an examiner's report for the submitted PhD thesis of Grzegorz Fabianski.

Introduction.

This thesis covers three publications, an ITCS 2021 paper, which gives an impossibility result in the context of off-chain Plasma-type protocols for blockchain systems, a Financial Cryptography 2025 paper giving machine checked proofs for a lightning channel and a CSF 2026 paper giving a Lean formalisation of computationally sound symbolic cryptography using garbled circuits as the case study.

Thesis Overview

The main results of the thesis are laid out as follows. Chapter 1 is an introductory chapter that covers prior art and concepts including blockchain protocols, smart contracts and scalability considerations. Chapter 2 summarises the three research papers that constitute the body of the thesis and outlines the candidate's contribution to each. Chapters 3-5 reproduce the papers, as follows.

Chapter 3 provides the lower bounds for off-chain protocols. In order to produce a lower bound result, a general class of operator-managed synchronous layer-2 blockchain protocols are introduced. Such protocols involve an operator, a smart contract system and the users. The main result is theorem 1, which establishes a lower bound in communication that should be transmitted to the smart contract system of at least $(n - \lceil \gamma n \rceil \cdot \log_2 n - 5)/4$ bits where γ represents the operator collateral fraction. This result is anchored on the requirement that the users need to interact with the contract in the case of exit. The key idea of the proof is based on incompressibility. A compression and decompression algorithm are derived from the protocol, with the message space being all subsets of users excluding user 1. The encoder runs an execution of the protocol with the given

parties V playing the roles of payers to user 1 who then is required to exit with the operator missing the messages from the non-payer parties. The output is the transcripts together with a list of γn identities as auxiliary output that are determined so the decoding is correct. The decoder on the other hand rewinds the users prior to the payment to user 1 and users are told to exit. Let Q be the users who succeed. By the security guarantees this includes all users outside V. By the collateral assumptions, at most γ n of the adversarial users make it. In this way, V can be recovered as the complement of Q with the auxiliary input from the encoder. Information theoretically the transcripts must be close to $n - \lceil \gamma n \rceil \cdot \log_2 n$ bits (with a pigeonhole argument resulting to the ¼ fraction).

Chapter 4, focuses on a two party payment channel from the lightning network and its formal security analysis via a machine checkable proof. It is based on a signature functionality and a ledger functionality and implements the protocol in Why3. The properties in question are funds security and liveness, with the former ensuring that any honest party can recover their funds on layer 1, while the latter ensures that two honest parties can always make progress irrespective of adversarial behavior in the network and the scheduling of payment requests. Only funds security is treated in the thesis.

Chapter 5, furthers the work of Micciancio on symbolic security proofs and provides a formal bridge to proofs in the cryptographic model by formalizing computational soundness in Lean 4. The chapter then builds on the work of Li and Micciancio to improve the security analysis of garbled circuits and removes the need to use a PRG in the garbled circuit construction to create distinct keys per wire intake (which was a "feature" of Li-Micciancio apparently introduced to facilitate the symbolic analysis). The method introduced to address such issues of compositionality and key reuse is the pseudo-fixpoint technique which enables reasoning about key reuse without sacrificing the ability to perform induction on the structure of an arbitrary expression, specifically in the case of garbled circuits, the expression generated by recursing over the circuit.

Technical Assessment

The lower bound result of chapter 3 is technically interesting and useful in practice. It sheds light to the inherent limitations of layer 2 protocols. The chapter 4 result is a good first step on an important real world security objective, the formal verification of the lightning network. The results are narrow but meaningful and pair well with other efforts such as the one on TLA+ as discussed in section 4.2.9.2. It does contribute to the real-world security of payment channels. Chapter 5 solves an open question from prior work in Li and Micciancio regarding a general mechanized proof for garbled circuits as well as handles key reuse so the PRG is not needed from that work to be incorporated along with the garbling of the circuit.

Suggested Corrections

In chapter 3, include a concrete description of the encoder and decoder inclusive of the "reconstruct" algorithm. Typically proofs in a PhD thesis should be complete, avoiding statements like "for completeness we show this fact in the full version."

An implicit assumption appears to be that there are no erasures in the computational model. Random coins are fixed and the encoder and decoder can use these values as hard coded advice. Making this explicit in the statements about the model would be a good idea. Furthermore, commenting whether the results continue to apply in a model where erasures are possible and honest parties can erase part of their private coins would be a good idea since a lot of blockchain protocols and forward secure cryptography in general utilizes erasures.

It is also good to recognise that n/log_2 n is not really "roughly the same order as the total amount of coins stored by the users." For example, for n=10^6 a corresponding collateral of n/log_2(n) =

5% * 10^6 may be reasonable. On the other hand, it appears that 1/log_2 n is just an artifact of the analysis and the result can be tightened.

In chapter 4, the expression channelClosingTime ≥3·deltaNet + 2· deltaWake + channelTimelock + 1 and channelTimelock ≥deltaWake + deltaNet + 1, is put forward – can you compare this with the parameterization of the actually deployed protocol?

For chapter 5, there is theorem symbolicToSemanticIndistinguishability in figure 5.9 and lemma garblingSecureSymbolic in Figure 5.5. The combination of the two is claimed in section 5.2.1 as one of the main results. Can you prove the combined statement in Lean as well, or if not comment on why not, and is the statement resulting from the composition similarly unrestricted in the choice of the circuit as lemma garblingSecureSymbolic is?

Conclusion

Overall, I assess this work as a novel and valuable contribution to the state of the art that is sufficient for conferring a doctoral degree (Ph.D.) to Mr. Fabiański.

Sincerely,



Aggelos Kiayias
Chair in Cyber Security and Privacy
Director, Blockchain Technology Laboratory