PhD Thesis Evaluation Form

Name of the PhD Candidate: Tomasz Lizurej

Title of the PhD Thesis: On Security of Systems Built on Blockchains

Reviewer's name: Ivan Visconti

Reviewer's affiliation: University of Salerno, Italy

Reviewer's e-mail address: visconti@unisa.it

SCIENTIFIC QUALITY OF THE PHD THESIS

The Ph.D. thesis of the candidate Tomasz Lizurej presents very valuable results in the domain of blockchain systems. More specifically, the contributions of the thesis impact on rating systems (used in blockchain trading platforms), on malicious use of shared secrets (of great benefit in blockchain applications like DAOs) and on protection from wire-tampering attacks (providing better security when considering devices enabling the safe use of cryptocurrencies).

All the above topics are both extremely relevant and of great interest because of the huge capitalization markets of cryptocurrencies and the increasing impact of other applications of blockchain systems (e.g., DeFi, DAOs).

The first contribution (Chapter 2) focuses on analysing manipulations of the well-known Fairness-Goodness-Algorithm (FGA). The goal of FGA is to fairly evaluates nodes of a transaction networks and the thesis shows 1) a full axiomatization characterizing FGA; 2) a definition of manipulability of FGA; 3) concrete manipulations of FGA. The proposed results are strong both in original innovations and technical contribution. Moreover, they include an experimental evaluation showing the different impacts of direct and indirect attacks. This excellent work has been published in a top-notch conference (AAAI) and the author of the thesis affirms that the technical contributions are due directly to his work.

The second contribution (Chapter 3) focuses on proposing a completely new adversarial model aiming at avoiding that multiple players could collude to emulate the computation of a single honest player. Notice that past research in cryptography has proposed techniques (i.e., secure multi-party computation) to allow (even) distrusting players to join forces to realize the execution of a functionality based on their private inputs. Here the authors look at a formulation where adversaries in the end play on behalf of a honest player but running the protocol honestly (therefore emulating what the honest player would have done on her own).

In the proposed setting, the known cryptographic techniques to enforce security (e.g., multi-party computation) turn out to be potentially used by those adversaries. Intuitively, players that intend to run the above task to emulate a single player can get shares of the input and make computations over

them. A typical scenario consists of a player having a secret (e.g., a credential to vote or to use a cryptocurrency) and distributing it to others with the goal that none of them individually has the secret but jointly they can emulate the single player with the secret.

The thesis proposes the new concept of Proof of Individual Knowledge and shows formal definitions, constructions, and security analyses. The core idea is that there are tasks like the evaluation of hash function on a secret input that can be run very quickly locally, when the secret is known, but those tasks are quite slow to compute when instead multi-party computations over the shared secret are performed (this is due both to the larger amount of computations and to the required multiple slow interactions in a WAN). Results appeared in CRYPTO 2023, a top-notch conference in Cryptography and the author of the thesis affirms that his contribution was about finalizing/completing notions and proofs.

The third contribution (Chapter 4) consists of a compiler relying on [9] that in concrete and reasonable cases improves the probability of error detection compared to [9]. The setting is that of efficiently testable circuits where the transformed circuit is paired with a test set that can be used to catch non-trivial tampering. Prior works (except [9]) leverage an unrealistic conductivity assumption that is avoided in [9]. The result is obtained by boosting a compression gadget and appeared in TCC 2023 (the same publication [9] mentioned above) which is a major conference for theoretical cryptography. The author of the thesis affirms that his contribution reported in the thesis corresponds to Chapter 5 of the TCC publication.

QUALITY OF WRITING/PRESENTATION

The thesis is very well written is fully satisfying in terms of formal concreteness and in terms of allowing also non-experts to be knowledgeable enough to appreciate the results.

I point out below some minor editorial comments.

Page 7: "section 5" <--> "Section 5"

Page 8: "difficult manipulate", missing "to"

Page 8: "who-trusts-whom" "who-trust-whom"

Page 10, line 1: replace ";" by "."

Page 18: including Jensen's equation would improve readability

Page 19: when specifying that attackers can make no more than k moves, it makes sense to specify the range of possible values of k (e.g., is k polynomial in the running time of the attackers?).

The acronym ISS is used in pages 35 and 36 but it should be defined first.

Page 35: when claiming that it is unrealistic to assume that lambda is large, it would be useful to provide some concrete explanations.

Page 36: "two sub-adversaries:" <--> "two sub-adversaries"

Page 36: "the A_1" <--> "A_1"

Page 37: in "Since P measures the response time" I guess you mean "V"

Page 57, "in Private Circuits II [75]" should be just "in [75] "

In References:

- [8], [9], [19], [51], [62] and several others miss details about the publications

- [21] and several others should have the full list of authors (or at least the same rule for "et al." should be applied to all references

- [59] and others should be cited by referencing the actual proceedings/journal in which the results appeared after peer review

-[60] 2_21 (same about [75] and others)

- [71] has several problems

- [94] appeared in TCS

- perhaps among [112] and [113] it is better to keep [113] only

OVERALL ASSESSMENT

Overall, the thesis contains several interesting results whose originality I judge very good, as demonstrated by the fact that they are included in publications that appeared some of the most important and selective publication venues.

Summing up, the contributions illustrated in this thesis are very good, certainly more than sufficient to grant a PhD.

Date : June 27 2024

Signature : .....