LEDGER
ledgerjournal.org

ISSN 2379-5980 (online)
associated article DOI 10.5195/LEDGER.2022.260

Coin Transfer Unlinkability Under the Counterparty Adversary Model: Open Review

Takeshi Miyamae,[*†] Kanta Matsuura[‡]

Reviewers: Reviewer A, Reviewer B

Abstract. The final version of the paper "Coin Transfer Unlinkability Under the Counterparty Adversary Model" can be found in Ledger Vol. 7 (2022) 17-34, DOI 10.5195/LEDGER.2022.260. There were two reviewers involved in the review process, neither of whom has requested to waive their anonymity at present, and are thus listed as Reviewers A and B. After initial review by Reviewer A, the submission was returned to the authors with feedback for revision (1A). The authors resubmitted their work and responded to reviewer comments (1B). After subsequent evaluation by Reviewers A and B (2A), the resubmission was deemed sufficient to address any prior concerns, with all new concerns being deemed too minor for subsequent review, thus ending the peer review process. Author responses have been bulleted for reader clarity.

1A. Review

Reviewer A

Does this paper represent a novel contribution to cryptocurrency or blockchain scholarship?

Not sure

If you answered "yes" to the previous question, in one sentence, describe in your own words the novel contribution made by this paper:Is the research framed within its scholarly context and does the paper cite appropriate prior works?

Important references are missing

Please assess the article's level of academic rigor.

Unsatisfactory (better than poor but a long way from excellent)

[*] 1ERsMcmcaRCri5jYPJ8Tqbr93V9UFXk3eF
[†] T. Miyamae (miyamae.takeshi@fujitsu.com) is a senior researcher at Fujitsu Limited, Japan and a Ph.D. student at The University of Tokyo, Japan.
[‡] K. Matsuura (kanta@iis.u-tokyo.ac.jp) is a professor at The University of Tokyo, Japan.

Please assess the article's quality of presentation.

Unsatisfactory (better than poor but a long way from excellent)

How does the quality of this paper compare to other papers in this field?

Bottom 50%

Please provide your free-form review for the author in this section.

The work reported in this article is concerned with the study of unlinkability of Personal Identifiable Information (PII) in the context of transactions involving cryptocurrencies. The authors focus in systems that use the MimbleWimble (MW) technology. The article begins motivating, with a simple example, the privacy risks posed to users of cryptocurrency transfer systems that create transactions off-chain.

The article puts forward a linkability attack model, called L2LCA, that provides a setting to reason over the requirements that must be satisfied by a cryptocurency system to guarantee the privacy of the users of the system. Then, the authors proceed to define an information sharing model that is intended to generalize the typical behavior and information sharing that takes place in transactions that transfer cryptocurrencies tokens. Associated to this model it is also introduced a (universal) zero-knowledge property concerning cryptocurrency transfer systems whose behavior is captured by the information model. The main result of the work is a theorem that establishes that if a coin transfer system of a cryptocurency is universal zero-knowledge then the cryptocurrency is L2LCA-safe.
The authors then evaluate the L2LCA safety of several MW-based technologies and some well-known cryptocurrency anonymization mechanisms.

In section 1, the authors state that the analyzed problem “has not been thoroughly discussed”. However, there exist several studies related to this issue. For instance, it is an open problem of Grin implementation (https://grin.mw/open-research-problems#7-reducing-linkability-of-outputs-on-chain).

In section 2 it is introduced the definition of the L2LCA model using a probabilistic attack scenario. It is claimed that this model makes it possible to give a precise formulation of the linkability problems that are put forward in the example (presented in Fig.1 – Fujistsuna Co. and Alice). However, no clear explanation is provided that allows to understand how the proposed model captures the discussed linkability problem.

Section 3 motivates the use of a information sharing model that makes it explicit the information flow that takes place when a transcation is performed by users of a coin transfer system. It is argued that in most systems of that kind, an exception being bitcoin, when a user performs a transaction it always shares information, both public and private, with other users of the system. Then a semi-formal definition of Coin Transfer System is introduced. It is not clear how well the information sharing model generalizes so as to be used to analyze different systems. In addition to that, the definition embodies the use of coin transfer Turing machines, a concept that was not previously introduced nor discussed. No rigorous definition of coin transfer Turing machines is provided (M_prev, M_cur, M_next) in Definition 2. Furthermore,

ISSN 2379-5980 (online)
associated article DOI
10.5195/LEDGER.2022.260

the symbol ‘S’ is used in two different ways. From the definitions it is quite difficult to understand the relation among the described example and the coin transfer Turing machines. The Definition needs to be restructured.
In addition to that, Definition 2 is no longer mentioned in the rest of the manuscript, for instance, in Definition 3.

In section 4 it is defined what is meant by a universal zero-knowledge coin transfer system. This definition heavily relies on the notion of simulators, which are probabilistic polynomial-time algorithms. This later kind of algorithms were not formally introduced and their use is not justified. Then a theorem that establishes that one such system is also L2LCA-safe is stated and informally proved. But no precise definition of what is meant by L2LCA-safe is provided in the paper. In Definition 5, the symbol ‘L’ needs to be defined. No explanation between the concept of zero-knowledge and two identical distributed random variables is provided. One may wonder whether those variables are uniform, for instance.

Section 5 evaluates the L2LCA-safety of different cryptocurrency technologies, namely, the original MW, Sword (Encrypted MW), CoinJoin, CryptoNote and Zerocash. The authors state that for a cryptocurrency to be shown L2CLA-unsafe a counterexample should be presented. However, for each of the discussed technologies only a brief and superficial explanation is provided to sustain the (un)safety characterization. No rigorous definition of privacy and computational complexity is given either. For instance, the authors make the statement “CryptoNote makes it difficult for privacy adversaries … ” and “…. this makes it difficult for most Zcash users …”

What does difficult mean in terms of complexity? Furthermore, in several parts it is said that “the adversaries of L2CLA can always distinguish … ” and Definition 1 is stated in terms of probability. No further explanation regarding the probability of the attacks is provided..
The section ends up with the formulation and proof of a theorem that establishes that Zerocash is a universal zero-knowledge coin transfer system, and therefore L2LCA-safe. The proof proceeds by constructing a universal simulator for the Zerocash protocol. Given that no precise and formal definition of the components and behaviour of that protocol is provided it is quite difficult to assess the correctnes of the proposed construction.
Furthermore, theorem 5.1 is supposed to show a proof based on Definition 5. However, Definition 5 is not mentioned throughout the proof.

The authors classify CoinJoin as a cryptocurrency, however it is a mechanism. It would have been interesting to read the analysis of other techniques like cut-through and Dandelion.

There are several symbols that need to be introduced and explained, like, for instance cm, cm^new, sn, sn^old, PRF. Definition 5 starts with “if and only if … ”, it should be restructured.

The discussion on related work is quite scarce. The authors seem to have a good grasp of the current literature on the topic of the paper, but theu should enrich the related work discussion and precisely describe the contribution of their work.

There are minor errors in English, but this does not affect the general nature of the work.

ISSN 2379-5980 (online)
associated article DOI
10.5195/LEDGER.2022.260

References must be improved, some of them (like reference [3]) must be corrected.

1B. Author Responses

Reviewer A

In section 1, the authors state that the analyzed problem “has not been thoroughly discussed”. However, there exist several studies related to this issue. For instance, it is an open problem of Grin implementation (https://grin.mw/open-research-problems#7-reducing-linkability-of-outputs-on-chain).

- We define 'subjective privacy adversary model' in the revised draft where we assume that the counterparties of a challenger in coin transfer transactions can become privacy adversaries. We meant that the 'subjective privacy adversary model' “has not been thoroughly discussed.” By the way, CoinSwap is proposed based on the assumption that the mixnodes are trusted. Therefore, CoinSwap is not our comparison target in this context.

In section 2 it is introduced the definition of the L2LCA model using a probabilistic attack scenario. It is claimed that this model makes it possible to give a precise formulation of the linkability problems that are put forward in the example (presented in Fig.1 – Fujistsuna Co. and Alice). However, no clear explanation is provided that allows to understand how the proposed model captures the discussed linkability problem.

- We separate the definition of PII unlinkability and the definition of CT-unlinkability (previously L2LCA model) in the revised draft. Moreover, we show that CT-unlinkability ensures PII unlinkability in Theorem 4.1.

Section 3 motivates the use of a information sharing model that makes it explicit the information flow that takes place when a transcation is performed by users of a coin transfer system. It is argued that in most systems of that kind, an exception being bitcoin, when a user performs a transaction it always shares information, both public and private, with other users of the system. Then a semi-formal definition of Coin Transfer System is introduced. It is not clear how well the information sharing model generalizes so as to be used to analyze different systems.

- Please note that we found that 'cryptocurrency information sharing model' and 'coin transfer system' were essentially the same, and we only define the 'coin transfer system' (Definition 6) in the revised draft. In Definition 6, we replace the words 'the ledger' with 'a public information channel' to show its generality. Therefore, it can be used to analyze different systems from cryptocurrencies.

In addition to that, the definition embodies the use of coin transfer Turing machines, a concept that was not previously introduced nor discussed. No rigorous definition of coin transfer Turing machines is provided (M_prev, M_cur, M_next) in Definition 2.

ISSN 2379-5980 (online)
associated article DOI
10.5195/LEDGER.2022.260

- Since we did not have to introduce 'coin transfer Turing machines' in the definition of 'coin transfer system,' we revised the definition not to use 'coin transfer Turing machines.'

Furthermore, the symbol ‘S’ is used in two different ways.

- We currently does not use symbol ‘S’ in the definition of 'coin transfer system.'

From the definitions it is quite difficult to understand the relation among the described example and the coin transfer Turing machines. The Definition needs to be restructured. In addition to that, Definition 2 is no longer mentioned in the rest of the manuscript, for instance, in Definition 3.

- We restructed the Definition 2 (current Definition 6) and mentioned in current Definition 7.

In section 4 it is defined what is meant by a universal zero-knowledge coin transfer system. This definition heavily relies on the notion of simulators, which are probabilistic polynomial-time algorithms. This later kind of algorithms were not formally introduced and their use is not justified.

- We add the definition of the probabilistic polynomial-time algorithms and the reason why their use is justified after the definition of coin transfer system (Definition 6).

Then a theorem that establishes that one such system is also L2LCA-safe is stated and informally proved. But no precise definition of what is meant by L2LCA-safe is provided in the paper.

- We introduce CT-unlinkability (previously L2LCA-safety) in Definition 7 and we use CT-unlinkability in the theorem (current Theorem 5.1) instead of using L2LCA-safety in the revised draft.

In Definition 5, the symbol ‘L’ needs to be defined.

- We define the symbol ‘L’ in Definition 8 in the revised draft.

No explanation between the concept of zero-knowledge and two identical distributed random variables is provided. One may wonder whether those variables are uniform, for instance.

- We mention the purpose of the simulation paradigm just before the definition of computational zero-knowledge coin transfer system (Definition 8). Our understanding is that uniformity is not included in the definition of zero-knowledge proof. Therefore, our definition of zero-knowledge coin transfer system also does not include it.

Section 5 evaluates the L2LCA-safety of different cryptocurrency technologies, namely, the original MW, Sword (Encrypted MW), CoinJoin, CryptoNote and Zerocash. The authors state

ISSN 2379-5980 (online)
associated article DOI
10.5195/LEDGER.2022.260

that for a cryptocurrency to be shown L2CLA-unsafe a counterexample should be presented. However, for each of the discussed technologies only a brief and superficial explanation is provided to sustain the (un)safety characterization. No rigorous definition of privacy and computational complexity is given either. For instance, the authors make the statement "CryptoNote makes it difficult for privacy adversaries … " and "…. this makes it difficult for most Zcash users …" What does difficult mean in terms of complexity?

- We explain the difficulty in terms of complexity whenever required in the revised draft.

Furthermore, in several parts it is said that "the adversaries of L2CLA can always distinguish … " and Definition 1 is stated in terms of probability. No further explanation regarding the probability of the attacks is provided..

- CT-unlinkability is formally defined using the formal definition of unlinkability between the two sets of fundamental objects, and we describe the Mimblewimble's CT-linkability in terms of the adversaries' advantage of the CT-unlinkability distinguishability game in the revised draft.

The section ends up with the formulation and proof of a theorem that establishes that Zerocash is a universal zero-knowledge coin transfer system, and therefore L2LCA-safe. The proof proceeds by constructing a universal simulator for the Zerocash protocol. Given that no precise and formal definition of the components and behaviour of that protocol is provided it is quite difficult to assess the correctnes of the proposed construction.

- We describe the zero-knowledge proof statement of the Zerocash's POUR transaction in detail, and add a figure that depicts the Zerocash coin transfer system (Fig.13).

Furthermore, theorem 5.1 is supposed to show a proof based on Definition 5. However, Definition 5 is not mentioned throughout the proof.

- In the revised draft, Theorem 6.1 (previously Theorem 5.1) is proved based on Definition 9 (previously Definition 5).

The authors classify CoinJoin as a cryptocurrency, however it is a mechanism. It would have been interesting to read the analysis of other techniques like cut-through and Dandelion.

- I agree that CoinJoin is a mechanism. However, we omit the description of CoinJoin, etc. for want of space.

There are several symbols that need to be introduced and explained, like, for instance cm, cm^new, sn, sn^old, PRF.

- We explain all the introduced symbols in the revised draft.

Definition 5 starts with "if and only if … ", it should be restructured.

- We are sorry that it was our mistake. We revised this description.

ISSN 2379-5980 (online)
associated article DOI
10.5195/LEDGER.2022.260

The discussion on related work is quite scarce. The authors seem to have a good grasp of the current literature on the topic of the paper, but they should enrich the related work discussion and precisely describe the contribution of their work.

- I describe the contribution of each work and enrich the related work discussion in the revised draft.

There are minor errors in English, but this does not affect the general nature of the work.

- We use a grammer checker, but there might remain some errors. If the errors are indicated, we will correct them in the next draft.

References must be improved, some of them (like reference [3]) must be corrected.

- We reviewed the format of the authors in references and corrected [3].

2A. Second Round Review

Reviewer A

Did you review an earlier version of this submission? (If "no," please contact the editor.)

Yes

Has the submission been sufficiently revised to address your previous concerns?

Yes

If you answered "no" to the previous question, please provide more detailed feedback here.

Most of the comments and suggestions included in the first review document were correctly addresses. The formalization of the model was improved, and various figures were added to illustrate the attack scenario.

Math symbols were revised and fixed throughout the definitions.

Do you have any new concerns specific to this revision?

Yes

If you answered "yes" to the previous question, please provide more detailed feedback here.

Please, consider adding a list of abbreviations and acronyms at the end of the manuscript.

ISSN 2379-5980 (online)
associated article DOI
10.5195/LEDGER.2022.260

A thorough grammatical check is required to fix some typos. For instance, “We assume hat at least …” in page 6.

References should be further revised. No access date is identified for URLs.

Notice that Betarte. et al. “Towards a Formally Verified Implementation of the Mimblewimble Cryptocurrency Peotocol” (2020) has a later publication on Sensors: Silveira et al. “A Formal Analysis of the Mimblewimble Cryptocurrency Protocol” (2021). (https://www.mdpi.com/1424-8220/21/17/5951).

Reviewer B

The paper introduces the framework of "subjective" vs "objective" unlinkability between coins, the subjective framework being stronger. The subjective framework considers the possibility that an entity from which Alice received a payment may later collude with an entity to which Alice sent a payment, in order to extract information that allows these entities to identify the web of Alice's transaction history. The paper shows how Mimblewimble coins can be linked under the subjective framework while Zcash coins cannot be linked. I think this is important because it further highlights how "privacy" in a cryptocurrency protocol is not a binary attribute, but rather exists on a spectrum. Some private cryptocurrencies give stronger privacy guarantees than others.

The paper is well-written. The authors use the right mix of formalizations/abstraction vs concrete examples, which makes the paper easy to follow despite its technical nature. I think the paper will be helpful to many readers interested in privacy-preserving cryptocurrencies. The paper also includes a well-written introduction with a nice review of the literature around privacy coins.

I recommend that Ledger accepts this submission.

ISSN 2379-5980 (online)
associated article DOI
10.5195/LEDGER.2022.260