Lelantus Spark Audit

Mikerah Quintyne-Collins, Karl Yu, Er-Cheng Tang

HashCloak Inc

December 2021

1 Introduction

Lelantus Spark is the Firo blockchain next generation privacy protocol in order to improve the privacy of its users alongside added features. Several new features of the Lelantus Spark protocol are the multisignature scheme, and selective disclosure functionality. HashCloak has been engaged by the Firo team to conduct an audit of the cryptography of Lelantus Spark. We have not found any issues related to the counterfeiting of coins or direct loss of transaction privacy when using the Lelantus Spark protocol. We did however find several issues within the paper itself. These were live reported to the authors and have been fixed. Further, we provide guidance on the state of implementation details and security proofs for the Lelantus Spark paper.

We started auditing version 363b2597476663c5708b55f985b5130ab54898a8 of the paper. As we found issues, we live reported them to the authors and updated the version we were reviewing accordingly.

2 Findings

2.1 Missing definition of $\{\sigma_i\}$ in Parallel One-Out-Of-Many Proving System

In the audited version of the Lelantus Spark paper, $\{\sigma_i\}$ wasn't defined. As such, it was not possible to independently verify the correctness of the Parallel One-Out-Of-Many Proving System construction and its proof.

Status: The authors updated the notation and clarified where the construction comes from in version 2156a2f152864bd1ffafcad5df36f78acce9e680.

2.2 Condition on $\{a_{i,j}\}$ is missing in Parallel One-Out-Of-Many Proving System

The terms $\{a_{i,j}\}$ which are selected uniformly at random by the prover in the Parallel One-Out-Of-Many Proving System come from *Short Accountable Ring*

Signatures from DDH by Bootle et al. However, in the description provided in Appendix B, it is missing a condition on the terms $\{a_{i,j}\}$.

Status: The authors have added the condition and is now in version a9ec86451b37fd0e620067c4c1435b63feaac13f.

2.3 Verification check in Parallel One-Out-Of-Many Proving System is incorrect

The third and fourth verification steps in the Parallel One-Out-Of-Many Proving System is incorrect as the equality no longer holds. The second summation term within the left hand side of the equality should be a product term as the protocol uses additive notation.

Status: The verification checks have been amended in version 4ef12e8db9a799b1eef8122bda2f5498c927b560 of the paper.

2.4 Type of α_1 in Lemma 1 proof of Appendix C is incorrect

In Lemma 1 in Appendix C used to prove that the Balance property holds for the Lelantus Spark construction, α_1 should be an element of $\mathbb{F}$ instead of F, as F is the generator for $\mathbb{F}$ and not a set.

Status: This was fixed in version df9ee648ee26a2b5073c0946d873d7a9ef988782 of the paper.

2.5 Lemma 1 is stated for both transaction types

In Appendix C, Lemma 1's statement didn't take into account that coins resulting from a mint transaction don't have tags attached to them as these are new coins. The statement should explicitly state that this lemma only holds for spend transactions.

Status: This was fixed in version fc7dd6b10ed563e248a25778f2c02426dee6c94f of the paper

2.6 Π_{rec} should be explicitly parsed in Identify algorithm

The Identify algorithm takes as input a coin and returns the value and memo attached to it to its recipient or designated entity. However, in step 2, upon parsing the coin for the relevant details, Π_rec, the representation proof for the coin, is missing. As such, Step 5 cannot be complete.

Status: This has been fixed as of verion 8217abd24fdf9ab787a74bd5f334c3e4564e7608.

2.7 Typos

There are several typos that we identified in of the paper.

1. On page 35, weather should be whether

2. On page 35, L-IND should be LIND.

Status: This has been fixed as of 4a627cd41ae3fb577ceb3d6bf32f4ed280da1d69

2.8 S is known as the serial number commitment but also called coin public key

Throughout the paper, the term *serial number commitment* and *coin public key* are used interchangeably. This can lead to some confusion as commitments and public keys are different in cryptography.

Status: This has been fixed as of f5fe7bc16d61a6ac2ff94207e2fc292401b2314e

2.9 The parameters of the Identify algorithm's RepVerify step are defined in Appendix D but not within the paper itself

In order to increase clarity when reading the algorithm description for Identify, it would be best to clarify that the inputs to the **RepVerify** check in step 5 is the result of the fact that upon verifying Π_{rec} on K_{div}, we get the identity that $K_{div} = \frac{1}{\mathbb{H}_{\mathbb{Q}_\nu}(s_1,i}K$.

Status: Not fixed.

2.10 Verification of proof of knowledge of mutlisignature key fails

In section 5.1, during the creation of new multisig keys, in step 6, we check that the proof of knowledge from step 3 is valid upon the receipt of $(R_\beta, \mu_\beta, C_\beta, s_{1,\beta}, s_{2,\beta})$. The condition in Step 6.b does not result in the successful completion of the verification, as we get the following

$$\mu_\beta G - \mathbb{H}_{pok}(\beta, C_{\beta,0}, R_\beta) = k_\beta G + \mathbb{H}_{pok}(\beta, a_{\beta,0}G, R_\beta)[a_{\beta,0}G - 1] \neq R_\beta$$

Status: This was fixed in version c1ea7033aafc20c3f4b1def9d2a42f0453dbc3fd of the paper.

3 General Comments

3.1 Citations for bespoke cryptographic constructions

There are several constructions in the paper that are modifications of known cryptographic protocols. It would also be best to cite the original papers that led to these constructions for completeness.

3.2 All protocols should be non-interactive using the Fiat-Shamir Transform

In order to aid with theoretical security proofs, the authors have written all the protocols in the paper interactively. However, these protocols will need to be implemented non-interactively using the Fiat-Shamir Transform. This was not noted in the paper. Since converting interactive protocols to non-interactive variants is a non-trivial matter, it should be noted in the paper.

3.3 Security Proofs for Bespoke Cryptographic Constructions

There are several constructions that are used within the Lelantus Spark protocol that are modified for use with the protocol. As such, it is assumed that since these modifications are minimal that there is no need for security proofs. However, historically, this has been the area in which bugs later appear in. As such, we recommend that proofs for these constructions be carefully written or that if there is a proof in another paper for the construction, that it be cited. Specifically, the Parallel One-Out-Of-Many construction described in Appendix B should have a proof to justify that it is indeed HVZK.

3.4 Details on Communication Channels

In many privacy-preserving protocols, there are assumptions that are made on how information is sent between the various actors in the protocol. However, there is no such discussion in the Lelantus Spark audit. How certain information in the protocol gets communicated can affect the privacy guarantees of the protocol when implemented in practice. Due to this paper's practical application, we recommend that a short discussion about how the choice of communication channels affects Lelantus Spark.