Bulletproof+ and Range Proving System Security assessment

Technical & Financial proposal

Monero

V1.0 – 12/02/2021

Quarkslab
www.quarkslab.com

Proposal

CONTEXT & OBJECTIVES

- **Context**

  The Monero Research Lab has completed design and coding for an implementation of the Bulletproofs+ range proving system (https://eprint.iacr.org/2020/735.pdf) as a drop in replacement to the existing range proof protocol Bulletproofs.

  An initial audit and review of the code and preprint has already been done and Monero want to make results the start of a new full review of the implementation.

- **Scope & objectives**

  - Analysis of the Bulletproof+ code implementing prove and verify algorithms:
    - To check if the code allows an attacker to generate a false proof that the verify algorithm deems as correct
    - To check if the code leaks any information to an attacker from examining the proof generated by an honest prover
  - Assess the correctness of the C++ code (~1500 lines of code of BP+ including tests and headers) from a logical and an implementation point of view, including the underlying elliptic curve arithmetic used.
  - Focus on identifying vulnerabilities related to security and in particular the cryptographic properties.

SOURCE AND DOCUMENTATION

- **Documentation**
  - Bulletproofs+: Shorter Proofs for Privacy-Enhanced Distributed Ledger
    - By Heewon Chung , Kyoohyung Han , Chanyang Ju , Myungsun Kim , and Jae Hong Seo
    - https://eprint.iacr.org/2020/735.pdf
  - Blog by Dr. Sarang
    - https://gist.github.com/SarangNoether/ee6367fa8b5500120b2a4dbe23b71694

- **Source code**
  - *bp-plus* git branch
    - https://github.com/SarangNoether/monero/tree/bp-plus
    - Focus on
      - ./tests/unit_tests/bulletproofs_plus.cpp
      - ./src/ringct/bulletproofs_plus.h & bulletproofs_plus.cc

    The dependencies of these codes are considered out-of-scope, but may be quickly reviewed, to understand the inputs and outputs of the function. These three files are around 1500 LOC-length.

QUARKSLAB'S APPROACH (1/2)

Quarkslab proposes the following operation flow for the audit :

- **Dive into related papers and code (step 1)**

The Bulletproofs+ protocol is described in https://eprint.iacr.org/2020/735.pdf. The implementation we will reviewed is in a vast majority implemented in the three files to audit. The report of the previous audit on the implementation will be available for this audit. To dive into all this literature, we estimate to around 10 man / days to read, verify the workflow of the implementation compared to the article, understand the underlying functions and check their usage, …

Time estimation: **10 man / days**

- **Resistance against a malicious prover**

One of the major threat of the Bulletproofs+ protocol is the ability for a prover (or a player for the aggregate range proof protocol) to forge or build a proof that will be validated even if it must not be accepted.

Time estimation: **8 man / days**

QUARKSLAB'S APPROACH (2/2)

- **Advanced attacks - more powerful attacker (optional step 3)**

In most MPC protocols, the attacker is modeled as an honest-but-curious user. If the protocol is proved secure in this model, this model does not capture attackers who may send data whose only goal is to gain information about the secret value of the other players. We will give recommendations and advice about this more powerful attacker.

Time estimation: **5 man / days**

- **Important note:** if steps 1 or 2 can be completed faster than expected, Quarkslab can use the remaining days for step 3.

- **Out of scope**
    - Rust code layer
    - Side-channel attacks

QUOTE

ID	Analysis	man/d	Price HT.
1	**Bulletproof+ and Range Proving System Security Assessment** • Review of code and results from the academic paper audit (step 1) • Resistance analysis against a malicious prover (step 2)	18	29,700 USD
2	**(Optional) Advanced attacks considering a more powerful attacker (step 3)**	5	8,250 USD
3	**Deliverables** • Detailed report • Restitution and slidedeck (visio)	2	3,300 USD
TOTAL (without option)		**20**	**$33,000 USD**
TOTAL (with option)		**25**	**$41,250 USD**

- The **daily rate** is fixed to **$1,650 USD VAT excl**.
- This proposal is valid until April 30th 2021 included.

- Firm, non-revisable price for purchase order submitted under 3 months.
- Payment schedule: 50% at the launch of the mission and 50% upon completion of the mission

CONFIDENTIALITY

Quarkslab and its employees are committed to confidentiality of information they will be dealing with. All Quarkslab employees are subjected to professional secrecy by contract.

All information which they have had access as part of the mission will therefore be confidential. Confidentiality does not apply to any information:

- which is or which falls into the public domain at any time other than as a result of a breach by either Party of its obligations under the Contract or any obligation of confidentiality which binds it to third parties;
- which is already in possession of a party before its submission by the other party;
- which was lawfully communicated to a party by a third party who has not obtained, directly or indirectly, of the other party and that this communication does not constitute a breach of a duty of confidentiality which binds a party to a third party;
- That a Party is required to report under a legal obligation or legal proceedings, it being understood that in this case, parties shall agree on the scope of this disclosure.
- Otherwise, all information made known to the stakeholders' provider directly or indirectly will be treated confidentially.

Confidential information will not be transmitted in clear text over the Internet. If such information is transmitted over the Internet (e.g. by email), it will be protected by means of strong encryption allowed by French law. The use of such means will not require from the recipient of the information the use of any additional equipment other than standard desktop systems (i.e. a Windows PC).

RESPONSABILITY

In part because of the specificity of penetration testing, the customer acknowledges that obligations of Quarkslab under the contract are an obligation of means.

Customer acknowledges that delivery has been accomplished on the basis of the technology and state of the art at the time of its completion.

Customer is aware of the relativity of test results with respect to changes in technology.

Customer acknowledges that the proposed measures to improve the security of its information system are complementary and that a partial implementation, or separate parcel of these measures cannot guarantee him the degree of protection expected.

Customer waives any liability for Quarkslab for destruction, alteration or degradation data and / or information contained in its information system and for any damages arising therefrom. The customer acknowledges being aware of the risks for services ordered.

If responsibility for Quarkslab were to be retained, parties agree that responsibility for Quarkslab for any cause whatsoever shall be limited to the total benefit of purchased services. In no event Quarkslab can be held liable for indirect losses, such as financial damages, consequential loss, loss of production, lower income and / or revenue loss or loss of information.


Quarkslab
SECURING EVERY BIT OF YOUR DATA