Bulletproofs review
Statement of work

Reviewer: Benedikt Bünz

Summary

The Monero Project intends to deploy Bulletproofs as a replacement to its current Borromean bitwise range proofs for confidential transactions, with the goal of decreasing both transaction size and verification time. After coding work by the Monero Research Lab based on the original Bulletproofs paper, the Monero Project wishes to obtain independent third-party review of its implementation to ensure correctness and security.

Code staged for release is written in C++ using existing libraries within the Monero codebase. However, a prototype of Bulletproofs functionality was written in Java by the Monero Research Lab to examine correctness and allow for rapid testing of algorithmic optimizations. This Java code was used by Monero developers for the C++ port. The Java code uses different libraries that make the resulting proofs incompatible with proofs generated by the C++ code.

Scope and deliverables

The reviewer will complete a thorough audit of the Monero Research Lab's Java code as linked below. No review of dependent libraries is expected. The review will determine the following:

- The extent to which the prover and verifier algorithms in the code correctly represent those in the Bulletproofs paper as linked below, and a detailed listing of any discrepancies. The reviewer should note that the Monero Research Lab developed its code against an earlier version of the paper that did not include many optimizations added to the linked version. As a result, the reviewer should take into account any deviations in the code from the paper that are algebraically equivalent.
- Any identified flaws in the code that could allow an attacker to generate a false proof that an honest verifier determines is correct.
- Any identified flaws in the code that could prevent an honest prover from generating a valid proof.
- Any identified flaws in the code that could allow an attacker to gain information (other than the fact that the given input is or is not in the specified range) about proof inputs used by an honest prover to generate a valid proof.

The Monero Research Lab will make its researchers available to the reviewer to provide assistance or clarification during the audit process as requested by the reviewer. Upon completion of the review, the reviewer will produce a detailed report containing the following:

- The methods by which the reviewer conducted the audit and made the determinations as listed above.
- A thorough analysis of any flaws identified in the code, including recommendations for mitigation.
- A thorough analysis of any discrepancies between the code and paper, whether or not the discrepancies are algebraically equivalent.

- An executive summary of the results intended to be understood by non-technical audiences.
- An identification of optimizations that could be made to the code, keeping in mind that the final C++ code may contain optimizations not found in the Java code for performance or library reasons.
- Any associated materials, such as source code files, produced or used in the review.

All materials should be delivered by email to Sarang Noether at sarang.noether@protonmail.com for review. The project is considered to be complete after confirmed receipt of the report and associated materials, and after any reasonable questions by the Monero Research Lab about the results are addressed by the reviewer.

Time and compensation

The reviewer will be compensated 6 XMR per working day, with a maximum compensation of 36.4 XMR allocated. Funds are donated by the Monero community and will be held in escrow by the Monero Project until project completion. Funds will be released to the Monero address of the reviewer's choice no later than one week after project completion.

Disclaimer and release of materials

The reviewer will conduct the audit in good faith and with the intention of identifying flaws and errors present in the design or implementation. However, as with any software, it is possible that flaws may exist that are not discovered in the course of review, or that a suspected flaw found during the audit is not in fact an error. To the extent permitted by law, the reviewer disclaims any warranty, including that the resulting code is free of errors. The final decision on any changes to code remains with the Monero Project and its community developers.

The reviewer grants the Monero Research Lab and Monero Project the right to publicly publish and distribute this statement of work, the final report, and any associated materials without restriction. Additionally, the reviewer consents to be identified by name and institutional affiliation as the author of the report and conductor of the review. However, neither the Monero Research Lab nor Monero Project will assume any particular endorsement of its Bulletproofs implementation by the reviewer as a result of the reviewer's work. The reviewer is entitled to any copyright associated to the final report and associated materials, provided this does not infringe on the release conditions stated above.

Changes made to the Monero codebase as a result of recommendations made by the reviewer may be identified in code, documentation, and commit notes by language similar to the following: "change XYZ made by review recommendation from Benedikt Bünz".

Links

Java prototype code:
https://github.com/b-g-goodell/research-lab/blob/master/source-code/StringCT-java/src/how/monero/hodl/bulletproof/MultiBulletproof.java

Bulletproofs paper:
http://web.stanford.edu/~buenz/pubs/bulletproofs.pdf