More Efficient Zero-Knowledge Range Proofs for Privacy-Preserving Systems

(A Proposal For Monero Fund of Magic Grants)

January 28, 2026

Preface. The work is research-oriented and focuses on strengthening the Monero ecosystem while contributing to the broader privacy-preserving ecosystem, with all outcomes and implementations released publicly as open source.

Introduction. Zero-knowledge range proofs are a powerful privacy-enhancing tool that allows a user to prove that a committed value lies within a specified range without revealing the value itself. Existing privacy-preserving digital finance systems such as Monero rely on range proofs to demonstrate that secret transaction amounts are non-negative, ensuring that users are unable to overdraw their balances. Monero currently adopts Bulletproofs+ [1], an improved version of Bulletproofs (IEEE S&P 18) [2], which uses a bit-decomposition approach that represents a secret value in binary form to prove membership in a range of the form $[0, 2^N - 1]$, where N is the bit-length of the range. A single instance of Bulletproofs+ involves $2\log N + 6$ elements, 3 elements fewer than that of Bulletproofs, making them well suited to blockchain settings where storage costs are a primary constraint.

Research Gap. The communication cost of Bulletproofs-style range proofs has largely reached its limit, leaving little room for further significant reduction. However, computational efficiency is also a critical factor. Prover costs directly affect user experience, while verifier costs determine system scalability, as higher verifier efficiency enables a higher number of transactions to be processed within a given time frame. For instance, network participants need to verify large numbers of range proofs when joining the network and synchronizing to obtain new blocks. For a single instance of Bulletproofs, the computational overhead is dominated by approximately 10N group exponentiations for the prover and 2N group exponentiations for the verifier. According to Monero's official implementation[1], compared to Bulletproofs, Bulletproofs+ achieves only a minor improvement in computational efficiency, offering approximately a 10% speedup for the prover and a 1% speedup for the verifier. These limited gains do little to significantly improve overall user experience or scalability, and the underlying proof systems therefore remain a bottleneck for Monero and many other privacy-preserving systems.

Research Goal. This project aims to substantially improve both prover and verifier efficiency for Bulletproofs-style range proofs, while preserving their compact $\big(2\log N + O(1)\big)$ communication complexity. In particular, it targets practical speedups in the range of 1.5× to 2× over existing Bulletproofs-based constructions, primarily by reducing the number of computationally expensive group exponentiations. The exact efficiency gains will depend on the final construction and implementation details. The proposed constructions will be accompanied by formal security proofs, avoid trusted setups, and be compatible with Monero's use of the Ed25519 elliptic curve, without relying on pairing-based cryptography. The resulting range proofs will follow a Bulletproofs-based structure and preserve the aggregation and batching properties, ensuring compatibility with Monero and providing a clear pathway to peer-reviewed publication.

[1] https://www.getmonero.org/2020/12/24/Bulletproofs+-in-Monero.html

Project Team. There are two members in our team, all affiliated with CSIRO (The Australia's National Research Agency):

- Dr Nan Wang (Principal Investigator & Project Lead). Nan is a research scientist with a strong interest and experience in zero-knowledge proofs and blockchain-based applications. As the lead author, he has published many representative publications at the top-tier security and cryptography venues (USENIX Security, IEEE S&P, AsiaCrypt, PETs). Especially, he has accumulated enriched expertise in zero-knowledge range proofs, Flashproofs (AsiaCrypt 22) [3] and SwiftRange (IEEE S&P 24) [4]. Please see his personal page `https://www.nan-wang.com` for more details.
- Dr Dongxi Liu (Co-Investigator). Dongxi is a principal research scientist. His research topics include applied cryptography, distributed system security, and data security. He has published cryptographic protocol papers and system security papers in top-tier conferences like CCS, IEEE S&P, NDSS, USENIX Security, Crypto, MICRO, and PETs. He has patents covering consensus protocols, fault tolerance, and key distribution. His ordering-preserving indexing scheme has been adopted in industry. Please see his personal page `https://people.csiro.au/L/D/Dongxi-Liu` for more details.

Project Feasibility. Our team has a strong background in cryptography and blockchain technologies, with a particular focus on zero-knowledge range proofs. We have demonstrated sustained research leadership in this area through multiple contributions to Top4 security conferences and Top3 cryptography conferences. In particular, we developed *SwiftRange*, published at a Top4 security conference, which is a logarithmic-sized zero-knowledge range proof that achieves a 2× speedup in verifier efficiency and a moderate improvement in prover efficiency over Bulletproofs-style range proofs, while retaining comparable communication costs. For small to moderate range sizes, such as $N < 64$, SwiftRange exhibits a substantial efficiency advantage over Bulletproofs-based constructions in both computational and communication costs. However, SwiftRange exhibits a trade-off: its communication cost becomes approximately 2× that of Bulletproofs-based constructions as the range size increases. This drawback is particularly pronounced when aggregating multiple range proofs. Nevertheless, the result establishes the technical feasibility of verifying with only N group exponentiations for a logarithmic-sized bit-decomposition-based range proof, providing a solid foundation for the proposed research. In addition, we developed *BulletCT*, also published at a Top4 security conference, which represents the most advanced RingCT schemes to date and includes a Bulletproofs-based instantiation. This work reflects the team's deep understanding of Bulletproofs and their role in privacy-preserving blockchain protocols.

Timeline. Overall, the project is expected to run for 13 weeks. We set two primary milestones:

- **Milestone 1 – Protocol Development (9 weeks):** This phase focuses on developing the zero-knowledge protocols, including the design and implementation of the proposed constructions. This phase will develop a Java prototype and benchmark the new construction against original Bulletproofs-based range proofs to evaluate efficiency gains.
- **Milestone 2 – Report Writing (4 weeks):** This phase focuses on delivering a comprehensive technical report to the Monero team, including a full protocol specification, security analysis, and an accompanying Java implementation, to facilitate integration into the Monero ecosystem. The investigators will also provide ongoing technical guidance to support this integration.

Budget. The total budget is approximately AUD 38,076 (≈ USD 25,443) based on a currency exchange rate of 1.5:1, covering total overheads at CSIRO, including labour resources and administration costs. It is a co-invested project between Magic Grants and CSIRO, with a funding split of 70% and 30%, respectively. As shown in Table 1,

- Magic Grants is expected to contribute AUD 26,653 (≈ USD 17,810), covering labour resources for 177 working hours by Nan Wang and 18 working hours by Dongxi Liu.
- CSIRO is expected to contribute AUD 11,423 (≈ USD 7,633).

Note that the currency exchange rate used is based on the rate at the time of proposal submission, and the final amount may vary depending on the exchange rate applied at the time of payment.

Table 1: Contributions.

Contributors	Amount	Ratio
Magic Grants	AUD 26,653 (USD 17,810)	70%
CSIRO	AUD 11,423 (USD 7,633)	30%
Total	AUD 38,076 (USD 25,443)	100%

References

[1] Heewon Chung, Kyoohyung Han, Chanyang Ju, Myungsun Kim, and Jae Hong Seo. Bulletproofs+: Shorter proofs for a privacy-enhanced distributed ledger. *IEEE Access*, 10:42081–42096, 2022.

[2] Benedikt Bünz, Jonathan Bootle, Dan Boneh, Andrew Poelstra, Pieter Wuille, and Greg Maxwell. Bulletproofs: Short proofs for confidential transactions and more. In *2018 IEEE Symposium on Security and Privacy (SP)*, pages 315–334, 2018.

[3] Nan Wang and Sid Chi-Kin Chau. Flashproofs: Efficient zero-knowledge arguments of range and polynomial evaluation with transparent setup. In Shweta Agrawal and Dongdai Lin, editors, *Advances in Cryptology – ASIACRYPT 2022*, pages 219–248, 2022.

[4] Nan Wang, Sid Chi-Kin Chau, and Dongxi Liu. Swiftrange: A short and efficient zero-knowledge range argument for confidential transactions and more. In *2024 IEEE Symposium on Security and Privacy (SP)*, pages 54–54, Los Alamitos, CA, USA, may 2024. IEEE Computer Society.