Jean-Philippe Aumasson

To OSTIF

# Statement of Work: Monero security audit

The following work will be performed by Jean-Philippe Aumasson (@veorq) and Antony Vennard (@diagprov):

1. Review of the results and security proofs of new concise linkable ring signatures in https://eprint.iacr.org/2019/654. This work includes detailed review of the correctness of the main results in Theorems 1-5, as well as of the validity of the proofs thereof.
2. Review of the implementations of the new signatures in https://github.com/SarangNoether/monero/blob/clsag-device/src/ringct/rctSigs.cpp (and any other relevant file). This work includes in-depth assessment that the code matches the functionality specified in the paper, and search for logical or software flaws that could compromise Monero's security.

The work load was estimated to roughly 3 person-day equivalent for each of the two above work packages, including the creation of a report documenting our findings and assessment. Based on our standard daily rate (USD 2400), we will therefore charge USD 14400 for this security audit project.

As agreed with Monero Project representatives, the work will be performed in June, starting with the first work package (proofs), such that the second work package (code) starts approximately a week after the communication of the results of the first work package (in order to leave Monero time to address any findings).

Signed:

Jean-Philippe Aumasson

OSTIF

Derek Zimmer