From: Ward Beullens <ward@beullens.com>
Sent: Saturday, September 7, 2019 3:15 PM
To: pqc-comments; pqc-forum
Subject: ROUND 2 OFFICIAL COMMENT: LUOV

Dear all,

As announced at the second PQC standardization conference the LUOV team proposes new parameter sets. The updated submission package is available at the LUOV website: https://www.esat.kuleuven.be/cosic/pqcrypto/luov/

The updated version of LUOV uses finite fields GF(2^r), where r is prime. This ensures that there are no nontrivial subfields which could be exploited by an attacker. Moreover, our implementation of the field arithmetic in the new fields is faster than in the old fields, which speeds up the signing and verification algorithms. The impact of changing the fields on the key and signature sizes is minimal (keys get a few percents larger and signatures a few percent smaller). However, to allow for a fair comparison with the other signature schemes we have decided to aim for Security levels 1,3, and 5 (instead of 2,4 and 5).
Therefore, the overall performance of the new SL1 and SL3 parameter sets is better than the old SL2 and SL4 parameter sets. We will submit the updated implementation to SUPERCOP in the coming weeks.

All the best,
The LUOV team