Changelog

- Inclusion of *canonical forms* for response compression in the underlying Sigma protocol, leading to drastic signature size decreases.

- New choice of protocol parameters to optimize the canonical forms setting. In particular, some of the proposed instances now have a much smaller amount of rounds, leading also to improvements on the overall computational complexity. Note that the coding theory parameters remain the same as in Round 1.

- Various implementation improvements, including

  - multiple speedups for the field arithmetic;
  - improved RREF computation by exploiting pivots reusing. For verification, this has been implemented in a non-constant time fashion to fully exploit pivots reusing. For signature generation, to avoid side-channel information leakage, the number of reused pivots is bounded;
  - canonical forms are implemented in a non-constant-time fashion, for both signature generation and verification. To prevent from side-channel information leakage, signature generation now employs a *blinding* technique;
  - the GGM tree construction has been slightly modified. The worst-case size on the number of released nodes, for the new construction, is tighter than the bound used for the Round 1 submission.

- Added Tung Chou, Patrick Karl and Floyd Zweydinger for substantial contributions to the LESS team.