From: Loïc Bidoux <loic.bidoux@owndata.org>
Sent: Monday, October 16, 2023 4:26 PM
To: pqc-comments
Cc: pqc-forum
Subject: Round 1 (Additional Signatures) OFFICIAL COMMENT: PERK

Dear all,

We are happy to announce a new release for PERK that can be found in the PERK website: https://pqc-perk.org

This release features the following modifications:
- Reduction of the signature sizes for the short parameters by approximately 5% using a ranking algorithm for permutations encoding ;
- Improvements of the implementation (reduced stack-memory usage and bug fixing).

Best regards,
PERK Team

From: Loïc Bidoux <loic.bidoux@owndata.org>
Sent: Sunday, June 16, 2024 12:46 PM
To: pqc-comments
Cc: pqc-forum
Subject: Round 1 (Additional Signatures) OFFICIAL COMMENT: PERK

Dear all,

The PERK team is working on improvements for PERK based on a new modeling for PKP along with recent improvements in MPCitH related proof systems. A note explaining what can be expected from PERK should it advance to Round 2 can be found on our website: https://pqc-perk.org/assets/downloads/perk-improvement.pdf

In a nutshell, PERK signature size can be halved and can go down as low as 3.0 kB for NIST-1 security level while the security assumption is improved and the performances are expected to be better or similar to the performances of the the initial submission.

Best regards,
PERK Team

From: Loïc Bidoux <loic.bidoux@owndata.org>
Sent: Wednesday, July 10, 2024 5:47 AM
To: pqc-comments
Cc: pqc-forum
Subject: Round 1 (Additional Signatures) OFFICIAL COMMENT: PERK

Dear all,

We would like to thank Thibauld Feneuil for pointing out an error affecting the signature size reported in our recent note regarding future improvements for PERK. The note has been updated accordingly and can be found on our website: https://pqc-perk.org/assets/downloads/perk-improvement.pdf

Best regards,
PERK Team