Rank-**O**uroboros, **L**AKE & **LO**CKER : ROLLO

Modifications between first and second round

ROLLO Team

Abstract

ROLLO is a compilation of three candidates to NIST's competition for post-quantum cryptography standardization: LAKE, LOCKER and Ouroboros-R.

In the first section, we present the modifications between the first version of the specifications of these candidates and the current version. In the second section, we indicate the work in progress.

1 Modifications

- The authors of ROLLO are the authors of LAKE, LOCKER and Ouroboros-R, plus Magali BARDET and Ayoub OTMANI.
- The names of the submissions have changed. LAKE becomes ROLLO-I, LOCKER becomes ROLLO-II and Ouroboros-R becomes ROLLO-III.
- ROLLO-III uses ideal codes instead of quasi-cyclic codes for Ouroboros-R.
- We have updated the parameters of the schemes such that the weight of the error, which is the most important parameter for the security, increases at each level of security. In practice it leads to a small increase of parameters. Concerning ROLLO-II, we have only kept the sets of parameters with a Decryption Failure Rate (DFR) inferior to 2^{-128}.

- We have reorganized the specifications for clarifications.
- We have added a description of the quantum speed-up in the section Known Attacks.

2 Work in Progress

- We are working on an optimized implementation that no longer relies on the NTL library nor the MPFQ library and uses AVX2 instructions to speed-up finite field operations. This implementation shall be available before NIST second standardization conference, scheduled on August 22^{nd}.