

# LAC

## Lattice-based Cryptosystems

**Principal Submitter:** Xianhui Lu<sup>1,2</sup>, +86-15010131069, luxianhui@iie.ac.cn

**Original Submitters:** Yamin Liu<sup>1,2</sup>, liuyamin@iie.ac.cn

Dingding Jia<sup>1,2</sup>, jiadingding@iie.ac.cn

Haiyang Xue<sup>1,2</sup>, xuehaiyang@iie.ac.cn

Jingnan He<sup>1,2</sup>, hejingnan@iie.ac.cn

Zhenfei Zhang<sup>3</sup>, zhenfei@algorand.com

**Round 2 Contributors:** Zhe Liu<sup>4</sup>, zhe.liu@nuaa.edu.cn

Hao Yang<sup>4</sup>, anonymous@nuaa.edu.cn

Bao Li<sup>1,2</sup>, libao@iie.ac.cn

Kunpeng Wang<sup>1,2</sup>, wangkunpeng@iie.ac.cn

**Organizations:** 1. Data Assurance and Communications Security Center, CAS

2. State Key Laboratory of Information Security, IIE, CAS

3. Algorand

4. Nanjing University of Aeronautics and Astronautics

**Owner:** Xianhui Lu

**Postal Address:** No. 89A, Minzhuang Road, Beijing 100093, China

**Alternative Contact:** hejingnan@iie.ac.cn, +86-18519196307

**Signature:** *Xianhui Lu*