SCIS 2022 2022 Symposium on
Cryptography and Information Security
Osaka, Japan & Online, Jan. 18 – 21, 2022
The Institute of Electronics,
Information and Communication Engineers

Optimal Lattice Trapdoor for the Klein-GPV and Peikert Sampler

Chao Sun * Thomas Espitau † Mehdi Tibouchi ‡ Masayuki Abe §

Keywords: Lattices, Trapdoor, Discrete Gaussian, Klein-GPV Sampler, Peikert Sampler

Abstract

As a popular candidate for post quantum cryptography, lattice based cryptography is developing at a high speed in the past 10 years. Among all the cryptographic primitives, lattice trapdoor serves as a very important one, especially for constructing lattice based hash-and-sign signatures. A lattice trapdoor is commonly a "good" basis of the lattice. Typically, the better the quality of lattice trapdoor is, the better security gaurantee and the smaller signature/public key size we will have. The quality of lattice trapdoor usually depends on the maximal Euclidean norm of Gram-Schmidt orthogonalization of the secret basis vectors for Klein-GPV sampler, or the largest singular value of the secret basis for Peikert sampler. In this paper, we investigate the trapdoor generation of less structured lattices, whose basis vectors have mostly random entries over discrete Gaussian distribution. For lattice with fixed volume, we generate lattice vectors that have roughly the same Gram-Schmidt length for Klein-GPV sampler (and lattice basis vectors that have small singular value for Peikert sampler). As an application, NIST requires some lattice based signatures that are based on less structured lattices, so the ideas described in this paper might serve as a candidate.

* Kyoto University,
† NTT Corporation
‡ Kyoto University, NTT Corporation
§ Kyoto University, NTT Corporation