Security of Lattice-Based Cryptography under "Imperfect" Scenarios*

Huijing Gong
University of Maryland, College Park. huijing.gong@gmail.com

Abstract

We propose a new framework for integrating the leaked secret information of Learning with Errors (LWE), in the form of "hint", into the lattice reduction attack. It can have many applications in cryptanalysis.

Motivation

Cryptanalysis of LWE instances:

A. Algorithmic attack: run primal lattice reduction attack; can predict security of larger LWE instances
B. Side-channel attack: previous works on lattice cryptosystems use ad-hoc methods and most require substantial amounts of information leakage.

Can we use the lattice reduction attack and take the side information into account? Can we estimate how much security dropped from using the side information?

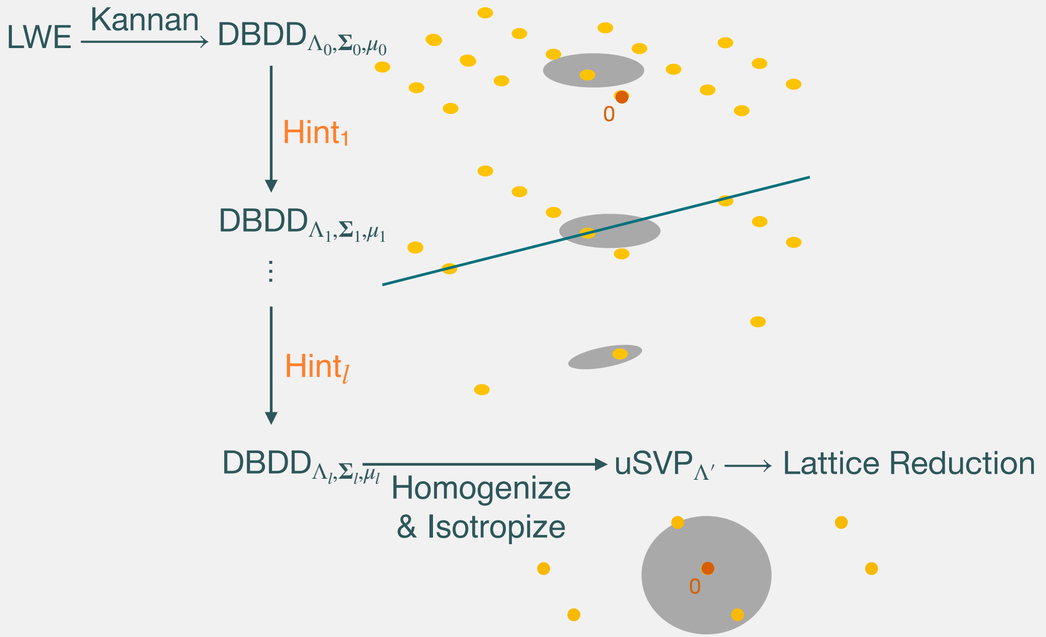
Our Framework

Standard primal lattice reduction attack:

$$\text{LWE} \xrightarrow{\text{Kannan}} \text{uSVP}_{\Lambda'} \longrightarrow \text{Lattice Reduction}$$

when hints are introduced…

Our framework generalizes the primal lattice reduction attack, and allows the progressive integration of hints before running a final lattice reduction step.



Hints

- Perfect Hint. $\langle \mathbf{s}, \mathbf{v} \rangle = \ell$
- Modular Hint. $\langle \mathbf{s}, \mathbf{v} \rangle = \ell \mod k$
- Approximate Hint. $\langle \mathbf{s}, \mathbf{v} \rangle \approx \ell$
- Short Vector Hint. $\mathbf{v} \in \Lambda$

Our techniques for integrating hints include sparsifying the lattice, projecting onto and intersecting with hyperplanes, and/or altering the distribution of the secret vector.

An Application Example

By integrating the side-channel information obtained from the 1st unsuccessful attack of [1] against FrodoKEM, our framework predicts that the bit-security of the scheme is heavily decreased. E.g. The CCS2 parameter set originally has 128-bit security, by exploiting the side information, we predict it can be broken with BKZ-29.

*This is a joint work with Dana Dachman-Soled, Léo Ducas, and Mélissa Rossi. https://ia.cr/2020/292. In Crypto 2020.
**Our framework is implemented on python/sage 9.0. Code is available at github.com/lducas/leaky-LWE-Estimator

1. J. W. Bos, S. Friedberger, M. Martinoli, E. Oswald, and M. Stam. Assessing the feasibility of single trace power analysis of frodo. In SAC, 2018