Determine Security Parameters for Dilithium

Attack MSIS with BKZ

Yuncong Zhang

July 3, 2020

Outline

1. Introduction
2. Attack MSIS with BKZ

Introduction

Dilithium bases its security on three hard problems:

- MLWE, against key recovery
- MSIS, for strong unforgeability
- SelfTargetMSIS, against new message forgery

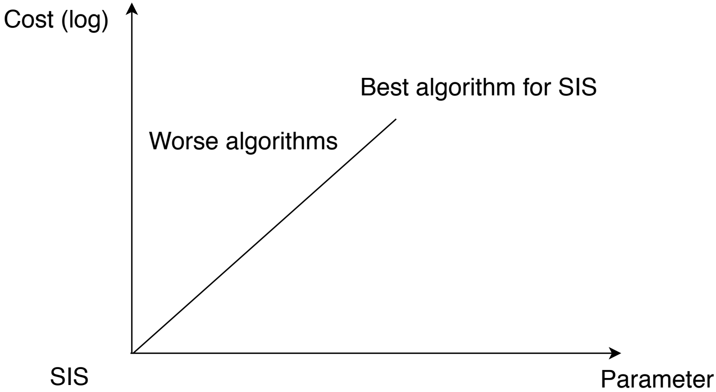
Breaking Dilithium breaks one of them. Breaking any of them breaks Dilithium.

Question

How to determine the security bits of Dilithium under specific parameters?

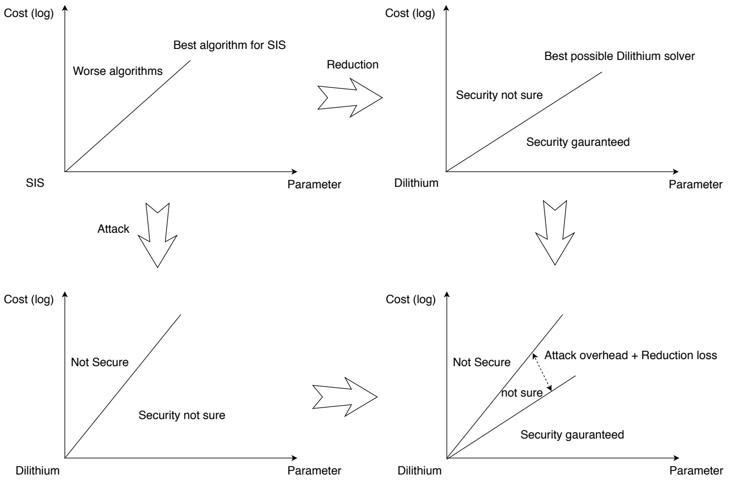
Introduction

The best SIS solver is exponential



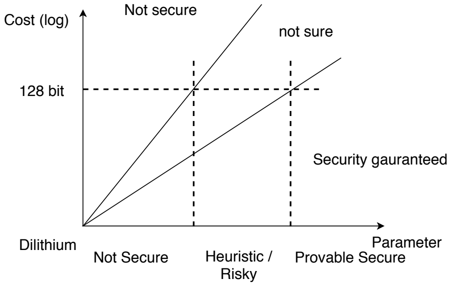
Introduction

- Reduction from SIS to Dilithium: Dilithium solver to SIS solver.
- Attack Dilithium by SIS solver: SIS solver to Dilithium solver.



Introduction

Determine the parameters for target security bits



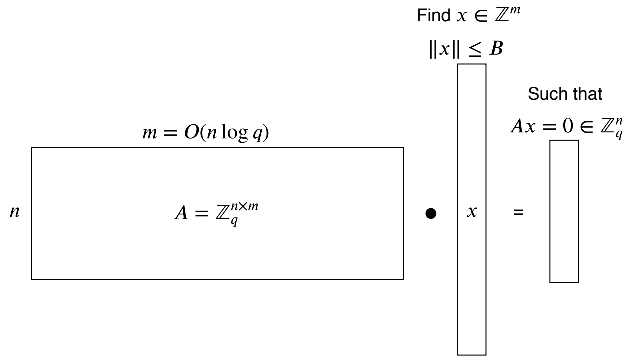
Remark

Starting from this, we can

1. *Find better attacks, move the upper line to right, and prove the tightness of reduction*
2. *If better attacks are hard to find, we may try to find better reduction, and move the lower line to left*

Attack MSIS with BKZ

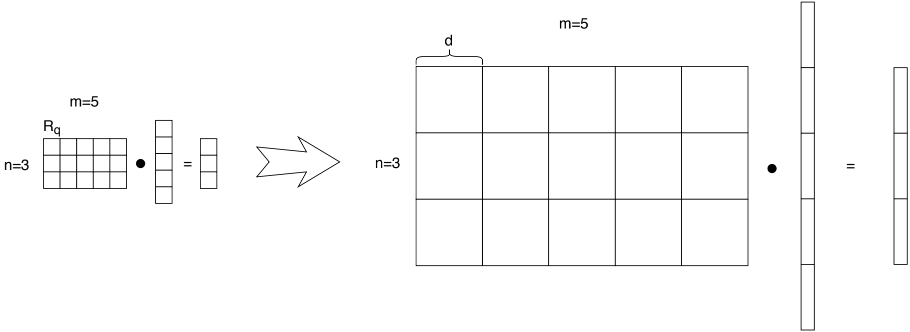
Brief review of SIS



Attack MSIS with BKZ

MSIS is generalization of SIS by replacing $\mathbb{Z}_q$ with ring R_q.

- Currently no attack exploits the algebraic structure.
- MSIS with parameters m, n, q, d, B is considered as secure as SIS with parameters $m \cdot d, n \cdot d, q, B$



Attack MSIS with BKZ

Euclidean-norm (ℓ_2-SIS) v.s. Maximal-norm (ℓ_∞-SIS)

- Since $(q, 0, \cdots, 0)$ is a solution, $B < q$ is required in both cases
- For both of them, the best attack is to view the problem as SVP and solve it with BKZ
- ℓ_2-norm is always greater than ℓ_∞-norm, by scale of $\sqrt{m}$
- For same security level, B for ℓ_∞-SIS should be smaller than for ℓ_2-SIS
- BKZ focuses on the Euclidean norm, the security analysis of ℓ_∞-SIS under BKZ attack has not been studied in detail

Remark

Dilithium relies on the ℓ_∞-MSIS

Remark

There may be techniques specific for ℓ_∞-SIS, e.g. BKZ produces $(5, 1)$, $(1, 5)$. For ℓ_2-SIS, this is done. For ℓ_∞-SIS, if $B = 4$, you can somehow combine them to get $(4, -4)$.

Attack MSIS with BKZ

SIS as SVP

- For $A \in \mathbb{Z}_q^{n \times m}$, the SIS problem is equivalent to finding a "short" vector in lattice

$$\mathcal{L}^{\perp}(A) = \{x \in \mathbb{Z}^m | Ax = 0 \bmod q\}$$

- $\mathcal{L}^{\perp}(A)$ is a q-ary lattice, i.e. contains the lattice $q\mathbb{Z}^m$

Optimization

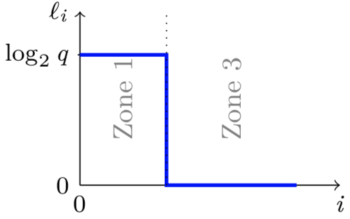
- We do not have to use all m columns. We can randomly select w columns from it. For other columns, set the corresponding x_i to 0
- Let A_w denote the matrix formed by the selected w columns, i.e. $A_w \in \mathbb{Z}_q^{n \times w}$

Attack MSIS with BKZ

Generate original set of vectors $\{\vec{b}_i \in \mathcal{L}^{\perp}(A_w)\}_i^N$:

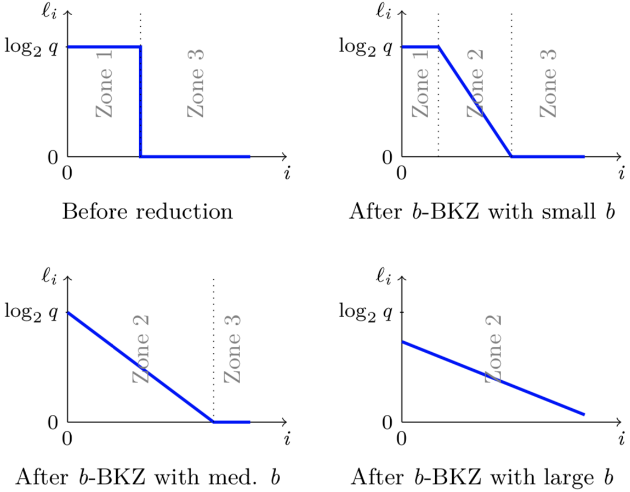
- For $1 \leq i \leq w$, let $\vec{b}_i = q\vec{e}_i = (0, \cdots, 0, q, 0, \cdots, 0)$
- For $w < i \leq N$, generate solutions to $A_w\vec{x} = \vec{0} \bmod q$ uniformly randomly
  - Uniformly randomly select first $w - n$ coordinates in $\mathbb{Z}_q$
  - Solve for the rest n coordinates by linear algebra

The lengths $\{\ell_i\}$ after Gram-Schmidt orthogonalization has the following shape



Attack MSIS with BKZ

The BKZ rounds smoothify the GS length shape



Attack MSIS with BKZ

The cost of BKZ in solving SIS is

$$t_{BKZ} / \epsilon_{BKZ}$$

- t_{BKZ} is the time of BKZ
- ϵ_{BKZ} is the probability that after BKZ reduction, at least one basis vector is bounded by B

Attack MSIS with BKZ

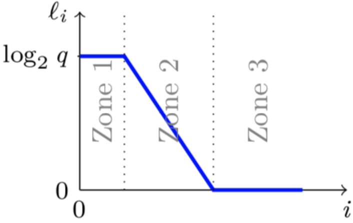
For simplicity, the Dilithium team estimates t_{BKZ} by a single call to SVP solver on local block of size β

- The best asymptotic complexity is achieved by sieving: $\sqrt{4/3}^{\beta}$
- The Dilithium team believes that this estimate is at least 10 bits lower than actual security

Attack MSIS with BKZ

To estimate the probability ϵ_{BKZ}, examine the shape of the basis vectors after BKZ reduction:

- Only consider the vectors in Zone 2, as they are the only vectors modified by BKZ
- These vectors, after projected orthogonally to vectors in Zone 1:
  - Have ℓ_2 norm $\approx 2^{\ell_i}$, where i is the start of Zone 2
  - Have the first $i - 1$ coordinates being 0



Attack MSIS with BKZ

Statements claimed by Dilithium that are hard to understand:

- We can obtain $\sqrt{4/3}^{\beta}$ vectors
- Let j be the end of Zone 2, i.e. the maximal such that $\ell_j > 0$, then the last $w - j$ coordinates (from $j+1$ to w) are 0

From all above

- The middle $j - i + 1$ coordinates have ℓ_2 norm $\approx 2^{\ell_i}$
- Each coordinate is approximately of size $2^{\ell_i}/\sqrt{j-i+1} \approx q/\sqrt{j-i+1}$

Finally, each vector can be modeled as follows

- The first $i - 1$ coordinates modeled by uniform random distribution over $[-q/2, q/2]$
- The middle $j - i + 1$ coordinates modeled by discrete normal distribution with $\sigma = q/\sqrt{j-i+1}$

Attack MSIS with BKZ

The probability that at least one vector is within bound B is approximately

$$\epsilon_{BKZ} := 1 - \left(1 - \left(\frac{2B+1}{q}\right)^{i-1} \left(2\Phi\left(\frac{B\sqrt{j-i+1}}{q}\right) - 1\right)^{j-i+1}\right)^{\sqrt{4/3}^{\beta}}$$

where $\Phi(\cdot)$ is the CDF of standard normal distribution.

Q & A