Introductory sharing on Post-Quantum Cryptography (lattices)

Low Yu Xuan

Orcacode Sharing
March 19, 2025

Storytime!

1. The year is 2040, and Quantum computers have broken all traditional cryptographic methods.
2. The evil entities, who have been havesting encrypted data since 2000s, have managed to obtain all your passwords and your browsing history by decrypting using quantum computers.

Storytime!

1. The year is 2040, and Quantum computers have broken all traditional cryptographic methods.
2. The evil entities, who have been havesting encrypted data since 2000s, have managed to obtain all your passwords and your browsing history by decrypting using quantum computers.
3. You have a time machine to go back in time to design new primitives that are quantum-resistant.
4. Your friend tells you that ”lattice problems” are supposedly hard against quantum computer. (This is still open area of research).
5. You now have to design new Hash functions and methods to encrypt and decrypt messages.

Threat of Quantum Computing

Quantum computers are coming.
— Some physics researcher, somewhere, probably looking for more grant funding…

Threat of Quantum Computing

Quantum computers are coming.
— Some physics researcher, somewhere, probably looking for more grant funding…

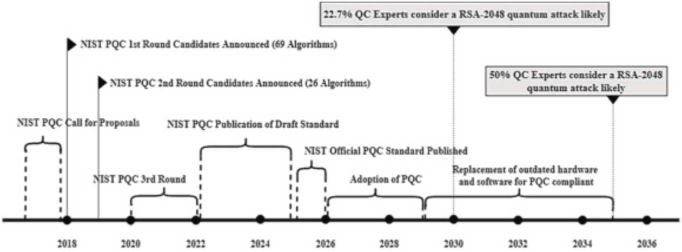


Figure: https://www.sciencedirect.com/science/article/pii/S2590005622000777

What makes something good for cryptography?

Hash function

What makes something good for cryptography?

Hash function

- Compression function
- Collision resistant

What makes something good for cryptography?

Hash function

- Compression function
- Collision resistant

Encryption/Decryption

What makes something good for cryptography?

Hash function

- Compression function
- Collision resistant

Encryption/Decryption

- Asymmetry in hardness of computation
- Existence and uniqueness(of private key)
- Ease of scalability

Shortest Integer Solution

Introduced by Ajtai in 1996.

Definition

SIS(n, m, q, B): Given $A \in_R \mathbb{Z}_q^{n\times m}$, find $z \in \mathbb{Z}^m$ such that $Az = 0 \pmod q$, where $z \neq 0$ and $z \in [-B, B]^m$ (and $B \ll q/2$).

- $Z_q = 0, 1, ..., q - 1$
- $x \in_r S$ means x is uniformly chosen from S
- all vectors are column vectors

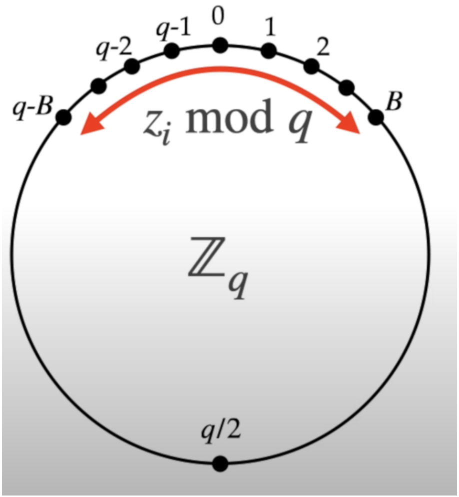


Figure: $B \ll q/2$

SIS Example

Example

- Let $n = 3$, $m = 5$, $q = 13$, and $B = 3$.
- SIS instance: $A = \begin{pmatrix} 1 & 0 & 7 & 12 & 4 \\ 2 & 11 & 3 & 6 & 12 \\ 9 & 8 & 10 & 5 & 1 \end{pmatrix}$
- We need to find nonzero $z = (z_1, z_2, z_3, z_4, z_5) \in [-3, 3]^5$ with $Az \equiv 0 \pmod{13}$.
- Some solutions within our bound $[-3, 3]^5$ are:

$$z_1 = \pm(3, 1, -1, 0, 1) \tag{1}$$
$$z_2 = \pm(-1, 0, 2, 1, -2) \tag{2}$$
$$z_3 = \pm(2, 1, 1, 1, -2) \tag{3}$$

When does a solution exist?

1. If $n \geq m$, then one expects that $Az = 0 \pmod{q}$ has no non-trivial solutions. (Why? Since it is likely full rank). Hence, we will assume $n < m$.

When does a solution exist?

1. If $n \geq m$, then one expects that $Az = 0 \pmod q$ has no non-trivial solutions. (Why? Since it is likely full rank). Hence, we will assume $n < m$.
2. If $(B+1)^m > q^n$, then by pigeonhole principle there must exist $z_1, z_2 \in [-B/2, B/2]^m$ such that $z_1 \neq z_2$ and $Az_1 = Az_2 \pmod q$. Then, $z = z_1 - z_2$ is a SIS solution.

When does a solution exist?

1. If $n \geq m$, then one expects that $Az = 0 \pmod{q}$ has no non-trivial solutions. (Why? Since it is likely full rank). Hence, we will assume $n < m$.
2. If $(B+1)^m > q^n$, then by pigeonhole principle there must exist $z_1, z_2 \in [-B/2, B/2]^m$ such that $z_1 \neq z_2$ and $Az_1 = Az_2 \pmod{q}$. Then, $z = z_1 - z_2$ is a SIS solution.
3. Thus, we can always construct a "SIS" problem as long as we have $(B+1)^m > q^n$, or $m > \frac{(n \log q)}{\log B+1}$, as a solution is guaranteed to exist.

When does a solution exist?

1. If $n \geq m$, then one expects that $Az = 0 \pmod{q}$ has no non-trivial solutions. (Why? Since it is likely full rank). Hence, we will assume $n < m$.
2. If $(B+1)^m > q^n$, then by pigeonhole principle there must exist $z_1, z_2 \in [-B/2, B/2]^m$ such that $z_1 \neq z_2$ and $Az_1 = Az_2 \pmod{q}$. Then, $z = z_1 - z_2$ is a SIS solution.
3. Thus, we can always construct a "SIS" problem as long as we have $(B+1)^m > q^n$, or $m > \frac{(n \log q)}{\log B+1}$, as a solution is guaranteed to exist.
4. But this solution is not unique. If z is a SIS solution, $-z$ is a SIS solution too.

Let's create a Hash function using this

- Select $A \in_r Z_q^{n \times m}$, where $m > n \log q$
- Define $H_A : \{0,1\}^m \to Z_n^q$ by $H_a(z) = Az \pmod{q}$

Note:

1. H_a works as a compression function since $m > n \log q \to 2^m > q^n$

Let's create a Hash function using this

- Select $A \in_r Z_q^{n \times m}$, where $m > n \log q$
- Define $H_A : \{0,1\}^m \to Z_n^q$ by $H_a(z) = Az \pmod q$

Note:

1. H_a works as a compression function since $m > n \log q \to 2^m > q^n$
2. **Collision resistance.** Suppose that one can efficiently find $z_1, z_2 \in \{0,1\}^m$ with $z_1 \neq z_2$ and $H_A(z_1) = H_A(z_2)$. Then $Az_1 = Az_2 \pmod q$, whence $Az = 0 \pmod q$ where $z = z_1 - z_2$. Since $z \neq 0$ and $z \in [-1,1]^m$, z is an SIS solution (with $B = 1$) which has been efficiently found. $\square$

Inhomogenous Shortest Integer Solution

also known as ISIS (unfortunately)

Definition

SIS(n, m, q, B): Given $A \in_R \mathbb{Z}_q^{n \times m}$ and $b \in_r Z_q^m$, find $z \in \mathbb{Z}^m$ such that $Az = b \pmod q$, where $z \neq 0$ and $z \in [-B, B]^m$ (and $B \ll q/2$).

- Similarly, we will construct where $n < m$.
- If $(2B + 1)^m > q^n$, ISIS solution likely to exist.
- Hence, with these parameters, we can construct a "ISIS" problem

SIS and ISIS are equivalent

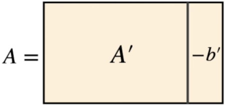
Theorem

SIS and ISIS are equivalent

Proof.

We first show SIS $\leq$ ISIS.
Let A be a SIS instance.
Write $A' = [A| - b']$, where $A' \in Z_q^{n \times m-1}$ and $b' \in Z_q^n$. Determine the solution z' to the ISIS instance (A', b').
We thus have $A'z' = b \pmod q$ and $z' \in [-B, B]^{m-1}$
Then, $z = \begin{bmatrix} z' \\ 1 \end{bmatrix}$ satisfies $Az = 0 \pmod q$, $z \neq 0$, and $z \in [-B, B]^m$.

$\square$



SIS and ISIS are equivalent (cont.)

Proof (continued).

Now, we show ISIS $\leq$ SIS.
Let (A, b) be an ISIS instance.
Select $j \in_R [1, n+1]$ and $c \in_R [-B, B]$ with $c \neq 0$.
Let A' be the $n \times (m+1)$ matrix obtained by inserting $-c^{-1}b \bmod q$ as a new jth column in A.
Determine an SIS solution $z' \in [-B, B]^{m+1}$ to $A'z' = 0 \pmod{q}$.
If indeed the jth entry in z' is c, then $Az = b \pmod{q}$,
where $z \in [-B, B]^m$ is obtained from z' by deleting its jth entry.
Thus, z is an ISIS solution that we have efficiently found. $\square$

Learning with Errors

- LWE was introduced by Regev in 2005.
- **Definition**. *Learning With Errors problem*: LWE(m, n, q, B)
  Let $s \in_R \mathbb{Z}_q^n$ and $e \in_R [-B, B]^m$ where $B \ll q/2$.
  Given $A \in_R \mathbb{Z}_q^{m \times n}$ and $b = As + e \pmod q \in \mathbb{Z}_q^m$, find s.
- **Note**:
  - This is the same as SIS/ISIS, with the extra variable e, but does not require the vector to be short.
  - Recall: ISIS solves for $Az = b \pmod q$

Parameters of LWE - how to set parameters B?

- If $B = 0$, then $As = b \pmod q$ can be solved efficiently.
- If $B > (q-1)/2$, then B is too large and impossible to solve information theoretically
- (Arora-Ge) If B is asymptotically smaller than $\sqrt{n}$, then LWE can be solved in subexponential time for a sufficiently large $m >> n$

Parameters n and m

- We also want $m \gg n$, so that we can expect a unique solution for the LWE problem.
- Uniqueness is guaranteed if no two closed e-balls intersect in Z_q^mspace

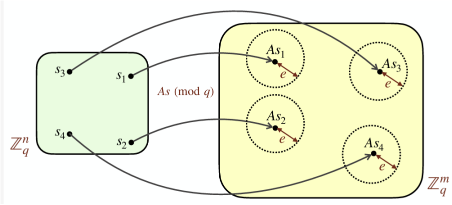


Figure: Visualization

DLWE - Decision LWE

- Given LWE instance, let $c = b$ with probability 0.5 and $c = r$ with probability 0.5, where $r \in_r Z_q^m$.
- Recall that $b = As + e$ and $b \in Z_q^m$
- Given (A, c), decision LWE is to determine whether one can determine whether $c = b$ or $c = r$ better than random guessing.

Theorem

DLWE and LWE are equivalent problems.

Proof.

We will only prove one side. i.e. DLWE $\leq$ LWE. Let (A, c) be a DLWE-instance. If $c = b$, then our LWE solver can efficiently find a solution (s, e) to $As + e = b$. Else, if $c = r$, then our LWE solver will find no solution / not terminate. And we can conclude that $c = r$. $\square$

ss-LWE Short Secret LWE

- Let $s \in_R \mathbb{Z}_q^n$ and $e \in_R [-B, B]^m$ where $B \ll q/2$.
  Given $A \in_R \mathbb{Z}_q^{m \times n}$ and $b = As + e \pmod q \in \mathbb{Z}_q^m$, find s.
- ss-LWE is the same as LWE. Except $s \in_r [-B, B]^n$ instead of Z_q^n

Theorem

LWE and ss-LWE are equivalent problems.

Proof.

Omitted. □

1. Exercise: Show that ss-LWE and ss-DLWE are equivalent problems.
2. This shows that instead of giving a LWE challenge, I can also give a ss-DLWE challenge which is less resource intensive to create, but equivalently hard.

Key generation

- Alice selects $s, e \in [-B, B]^n$, and $A \in Z_q^{n \times n}$
- Compute $b = As + e \pmod{q}$
- The public key would be (A, b), while private key is s

1. Notice that this now becomes a ss-LWE challenge.
2. The actual PQC(Kyber) implementation uses polynomials instead of integers for optimization purposes, but the steps remain largely the same.

PKE: Encryption and decryption

Encryption

To encrypt a message $m \in \{0, 1\}$ for Alice, Bob does:

1. Obtain an authentic copy of Alice's encryption key (A, b).
2. Select $r, z \in_R [-B, B]^n$ and $z' \in_R [-B, B]$.
3. Compute $c_1 = A^T r + z$ and $c_2 = b^T r + z' + m\lfloor q/2 \rfloor$.
4. Output $c = (c_1, c_2)$.

Note: $c \in \mathbb{Z}_q^n \times \mathbb{Z}_q$.

Decryption

To decrypt $c = (c_1, c_2)$, Alice does:

1. Output $m = \text{Round}_q(c_2 - s^T c_1)$.

Note: Alice uses her private key s.

Round_q

For $x \in [0, q-1]$, define

$$x \pmod q = \begin{cases} x & \text{if } x \leq (q-1)/2, \\ x - q & \text{if } x > (q-1)/2. \end{cases}$$

Then

$$\mathrm{Round}_q(x) = \begin{cases} 0, & \text{if } -q/4 < x \pmod q < q/4, \\ 1, & \text{otherwise.} \end{cases}$$

Time for a demo

Appendix: Why does decryption work?

- **Question:** Does decryption work?
  i.e., does $m = \text{Round}_q(c_2 - s^T c_1)$?
- We have $c_2 - s^T c_1 = (b^T r + z' + m\lfloor q/2 \rfloor) - s^T(A^T r + z)$
  $= (s^T A^T + e^T)r + z' + m\lfloor q/2 \rfloor - s^T(A^T r + z)$
  $= e^T r - s^T z + z' + m\lfloor q/2 \rfloor$.
- So, the decryption works iff $|e^T r - s^T z + z' q| < q/4$.
- Now, suppose that $B \leq \sqrt{q/(4(2n+1))}$.
- Then $|e^T r - s^T z + z' q| \leq nB^2 + nB^2 + B \leq \frac{2nq}{4(2n+1)} + \sqrt{\frac{q}{4(2n+1)}}$
  $= \frac{nq}{2(2n+1)} + \sqrt{\frac{q}{4(2n+1)}} < \frac{q}{4}$,
  so decryption works. $\square$

The End

SCAN ME

Figure: Survey for me to improve

Questions? Comments?

1. Acknowledgments: Slides and some diagrams are adapted based off Prof Alfred Menezes's course on lattice-based cryptography.