SIS and LWE lattice problems

Marcel Šebek

MFF UK

March 23, 2012 / Spring School of Algebra

Table of Contents

Reductions

$$
\begin{tikzcd}
\text{Worst case} & \text{Average case} & \text{Cryptographic primitives} \\
\text{SIVP} & \text{SIS} \arrow[l] & \text{OWF} \arrow[l] \\
\text{GapSVP} & \text{LWE} \arrow[l] \arrow[ul, squiggly, "\text{quantum}"] & \text{PKE} \arrow[l]
\end{tikzcd}
$$

Lattices Used in Cryptography

- $n \in \mathbb{N}$ main security parameter
- $q \geq 2$ integer (not necessarily a prime)
- $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$ matrix

Lattices Used in Cryptography

- $n \in \mathbb{N}$ main security parameter
- $q \geq 2$ integer (not necessarily a prime)
- $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$ matrix
- $\mathbf{A} : \mathbb{Z}^m \to \mathbb{Z}^n$ is a group homomorphism
- similarly $\mathbf{A}^T : \mathbb{Z}^n \to \mathbb{Z}^m$

Lattices Used in Cryptography

- $n \in \mathbb{N}$ main security parameter
- $q \geq 2$ integer (not necessarily a prime)
- $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$ matrix
- $\mathbf{A} : \mathbb{Z}^m \to \mathbb{Z}^n$ is a group homomorphism
- similarly $\mathbf{A}^T : \mathbb{Z}^n \to \mathbb{Z}^m$
- let $\pi_q : \mathbb{Z}^n \to \mathbb{Z}_q^n$ be the natural projection
- the following sets are (full-rank) lattices

$$\mathcal{L}(\mathbf{A}^T) = \operatorname{Im} \mathbf{A}^T + q\mathbb{Z}^m = \\ = \{\mathbf{z} \in \mathbb{Z}^m \mid \exists \mathbf{x} \in \mathbb{Z}^n : \mathbf{z} = \mathbf{A}^T\mathbf{x} \pmod{q}\} \leq \mathbb{Z}^m$$

$$\mathcal{L}^{\perp}(\mathbf{A}) = \operatorname{Ker} \pi_q \mathbf{A} = \{\mathbf{z} \in \mathbb{Z}^m \mid \mathbf{A}\mathbf{z} = 0 \pmod{q}\} \leq \mathbb{Z}^m$$

Lattices Used in Cryptography

- $n \in \mathbb{N}$ main security parameter
- $q \geq 2$ integer (not necessarily a prime)
- $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$ matrix
- $\mathbf{A} : \mathbb{Z}^m \to \mathbb{Z}^n$ is a group homomorphism
- similarly $\mathbf{A}^T : \mathbb{Z}^n \to \mathbb{Z}^m$
- let $\pi_q : \mathbb{Z}^n \to \mathbb{Z}_q^n$ be the natural projection
- the following sets are (full-rank) lattices

$$\begin{aligned}\mathcal{L}(\mathbf{A}^T) &= \operatorname{Im} \mathbf{A}^T + q\mathbb{Z}^m = \\ &= \{\mathbf{z} \in \mathbb{Z}^m \mid \exists \mathbf{x} \in \mathbb{Z}^n : \mathbf{z} = \mathbf{A}^T\mathbf{x} \pmod{q}\} \leq \mathbb{Z}^m\end{aligned}$$

$$\mathcal{L}^\perp(\mathbf{A}) = \operatorname{Ker} \pi_q \mathbf{A} = \{\mathbf{z} \in \mathbb{Z}^m \mid \mathbf{Az} = 0 \pmod{q}\} \leq \mathbb{Z}^m$$

- both are full-rank because they contain $q\mathbb{Z}^m$ as a sub-lattice
- both are q-periodic

Table of Contents

SIS (Small Integer Solution)

- Let $\mathbf{a}_1, \dots, \mathbf{a}_m \in \mathbb{Z}_q^n$ be given, find $z_1, \dots, z_m \in \{-1, 0, 1\}$ such that

$$z_1\mathbf{a}_1 + \cdots + z_m\mathbf{a}_m = 0 \pmod{q}$$

SIS (Small Integer Solution)

- Let $\mathbf{a}_1, \ldots, \mathbf{a}_m \in \mathbb{Z}_q^n$ be given, find $z_1, \ldots, z_m \in \{-1, 0, 1\}$ such that

$$z_1 \mathbf{a}_1 + \cdots + z_m \mathbf{a}_m = 0 \pmod{q}$$

- Matrix version: given $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$, find $\mathbf{z} \in \{-1, 0, 1\}^m$ such that

$$\mathbf{A}\mathbf{z} = 0 \pmod{q}$$

SIS (Small Integer Solution)

- Let $\mathbf{a}_1, \ldots, \mathbf{a}_m \in \mathbb{Z}_q^n$ be given, find $z_1, \ldots, z_m \in \{-1, 0, 1\}$ such that

$$z_1\mathbf{a}_1 + \cdots + z_m\mathbf{a}_m = 0 \pmod{q}$$

- Matrix version: given $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$, find $\mathbf{z} \in \{-1, 0, 1\}^m$ such that

$$\mathbf{A}\mathbf{z} = 0 \pmod{q}$$

- $\mathbf{z} \in \mathcal{L}^{\perp}(\mathbf{A})$ is a short vector in the ℓ_∞ norm
- The problem is easy without restriction $z_i \in \{-1, 0, 1\}$
- Hard in average case (reduction to worst-case problems)

SIS Applications

- Hash functions
- One-way functions
- Signature schemes
- Identification schemes

Collision-Resistant Hash Function

- $m > n \log q$ (compression condition)
- $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$ public description
- $f_{\mathbf{A}} : \{0,1\}^m \to \mathbb{Z}_q^n$, $f_{\mathbf{A}}(\mathbf{z}) = \mathbf{Az}$
- $f_{\mathbf{A}}(\mathbf{z}) = f_{\mathbf{A}}(\mathbf{y})$ implies $f_{\mathbf{A}}(\mathbf{y} - \mathbf{z}) = 0$, $\mathbf{y} - \mathbf{z} \in \{-1, 0, 1\}^m$
- Collision-resistance implies one-wayness

Worst-Case to Average-Case Reduction

- Divide $\mathcal{P}(B)$ into q^n parts corresponding to $\mathbf{Z}_q^n$

Worst-Case to Average-Case Reduction

- Divide $\mathcal{P}(B)$ into q^n parts corresponding to $\mathbf{Z}_q^n$
- Sample lattice points $\mathbf{y}_1, \ldots, \mathbf{y}_m$
- For each $\mathbf{y}_i$, sample $\mathbf{c}_i$ close to $\mathbf{y}_i$ using Gaussian distribution with large enough variance
- Therefore, $\mathbf{c}_i$ are uniform modulo $\mathcal{P}(B)$

Worst-Case to Average-Case Reduction

- Divide $\mathcal{P}(B)$ into q^n parts corresponding to $\mathbf{Z}_q^n$
- Sample lattice points $\mathbf{y}_1, \ldots, \mathbf{y}_m$
- For each $\mathbf{y}_i$, sample $\mathbf{c}_i$ close to $\mathbf{y}_i$ using Gaussian distribution with large enough variance
- Therefore, $\mathbf{c}_i$ are uniform modulo $\mathcal{P}(B)$
- let $\tilde{\mathbf{c}}_i$ be lower-left point corresponding to $\mathbf{c}_i$
- let $\mathbf{a}_i \in \mathbf{Z}_q^n$ be the corresponding coordinates

Worst-Case to Average-Case Reduction

- Divide $\mathcal{P}(B)$ into q^n parts corresponding to $\mathbf{Z}_q^n$
- Sample lattice points $\mathbf{y}_1, \dots, \mathbf{y}_m$
- For each $\mathbf{y}_i$, sample $\mathbf{c}_i$ close to $\mathbf{y}_i$ using Gaussian distribution with large enough variance
- Therefore, $\mathbf{c}_i$ are uniform modulo $\mathcal{P}(B)$
- let $\tilde{\mathbf{c}}_i$ be lower-left point corresponding to $\mathbf{c}_i$
- let $\mathbf{a}_i \in \mathbf{Z}_q^n$ be the corresponding coordinates
- $\mathbf{a}_i$ are uniform, give $\mathbf{A}$ to LWE oracle, get $\mathbf{Az} = 0$

Worst-Case to Average-Case Reduction

- Divide $\mathcal{P}(B)$ into q^n parts corresponding to $\mathbf{Z}_q^n$
- Sample lattice points $\mathbf{y}_1, \ldots, \mathbf{y}_m$
- For each $\mathbf{y}_i$, sample $\mathbf{c}_i$ close to $\mathbf{y}_i$ using Gaussian distribution with large enough variance
- Therefore, $\mathbf{c}_i$ are uniform modulo $\mathcal{P}(B)$
- let $\tilde{\mathbf{c}}_i$ be lower-left point corresponding to $\mathbf{c}_i$
- let $\mathbf{a}_i \in \mathbf{Z}_q^n$ be the corresponding coordinates
- $\mathbf{a}_i$ are uniform, give $\mathbf{A}$ to LWE oracle, get $\mathbf{Az} = 0$
- $\tilde{\mathbf{C}}\mathbf{z}$ is a lattice vector

Worst-Case to Average-Case Reduction

- Divide $\mathcal{P}(B)$ into q^n parts corresponding to $\mathbf{Z}_q^n$
- Sample lattice points $\mathbf{y}_1, \ldots, \mathbf{y}_m$
- For each $\mathbf{y}_i$, sample $\mathbf{c}_i$ close to $\mathbf{y}_i$ using Gaussian distribution with large enough variance
- Therefore, $\mathbf{c}_i$ are uniform modulo $\mathcal{P}(B)$
- let $\tilde{\mathbf{c}}_i$ be lower-left point corresponding to $\mathbf{c}_i$
- let $\mathbf{a}_i \in \mathbf{Z}_q^n$ be the corresponding coordinates
- $\mathbf{a}_i$ are uniform, give $\mathbf{A}$ to LWE oracle, get $\mathbf{Az} = 0$
- $\tilde{\mathbf{C}}\mathbf{z}$ is a lattice vector
- $(\mathbf{Y} - \tilde{\mathbf{C}})\mathbf{z}$ is a short lattice vector

Table of Contents

LWE (Learning With Errors)

Let

- $n \in \mathbb{N}$ be dimension
- $q \geq 2$ be modulus
- $\mathbf{s} \in \mathbb{Z}_q^n$ be secret
- χ be error distribution over $\mathbb{Z}_q$

$$\begin{array}{lll} \mathbf{a}_1 \leftarrow \mathbb{Z}_q^n & e_1 \leftarrow \chi & b_1 = \langle \mathbf{a}_1, \mathbf{s} \rangle + e_1 \mod q \\ \mathbf{a}_2 \leftarrow \mathbb{Z}_q^n & e_2 \leftarrow \chi & b_2 = \langle \mathbf{a}_2, \mathbf{s} \rangle + e_2 \mod q \\ & \dots & \end{array}$$

- Search-LWE: find $\mathbf{s}$ given enough samples $(\mathbf{a}_i, b_i)_{i=1}^m$.
- Decision-LWE: distinguish $(\mathbf{a}_i, b_i)_{i=1}^m$ from uniform distribution.

LWE (Learning With Errors)

Let

- $n \in \mathbb{N}$ be dimension
- $q \geq 2$ be modulus
- $\mathbf{s} \in \mathbb{Z}_q^n$ be secret
- χ be error distribution over $\mathbb{Z}_q$

$$\mathbf{A} \leftarrow \mathbb{Z}_q^{n \times m} \qquad \mathbf{e} \leftarrow \chi^m \qquad \mathbf{b} = \mathbf{A}^T\mathbf{s} + \mathbf{e} \mod q$$

- Search-LWE: find $\mathbf{s}$ given $(\mathbf{A}, \mathbf{b})$ for a sufficiently large m.
- Decision-LWE: distinguish $(\mathbf{A}, \mathbf{b})$ from uniform distribution.
- $\mathbf{b}$ is a point close to the lattice $\mathcal{L}(\mathbf{A}^T)$

LWE is easier than SIS

- Get $(\mathbf{A}, \mathbf{b})$ on input
- Pass $\mathbf{A}$ to SIS oracle, get $\mathbf{Az} = 0$

LWE is easier than SIS

- Get $(\mathbf{A}, \mathbf{b})$ on input
- Pass $\mathbf{A}$ to SIS oracle, get $\mathbf{Az} = 0$
- If $\mathbf{b}$ is uniform, $\langle \mathbf{b}, \mathbf{z} \rangle$ is "random"
- If $\mathbf{b} = \mathbf{A}^T\mathbf{s} + \mathbf{e} \mod q$, $\langle \mathbf{b}, \mathbf{z} \rangle = \langle \mathbf{A}^T\mathbf{s}, \mathbf{z} \rangle + \langle \mathbf{e}, \mathbf{z} \rangle = \langle \mathbf{e}, \mathbf{z} \rangle$ is small

Search and Decision Equivalence

- Works for $q = poly(n)$, q prime
- For bigger q a different construction is needed

Search and Decision Equivalence

- Works for $q = poly(n)$, q prime
- For bigger q a different construction is needed
- Secret shifting:

$$
\begin{aligned}
(\mathbf{a}_i, b_i) = (\mathbf{a}_i, \langle \mathbf{a}_i, \mathbf{s} \rangle + e_i) \rightsquigarrow (\mathbf{a}_i, b_i + \langle \mathbf{a}_i, \mathbf{t} \rangle) = \\
= (\mathbf{a}_i, \langle \mathbf{a}_i, \mathbf{s} + \mathbf{t} \rangle + e_i)
\end{aligned}
$$

Search and Decision Equivalence

- Works for $q = poly(n)$, q prime
- For bigger q a different construction is needed
- Secret shifting:

$$
\begin{aligned}
(\mathbf{a}_i, b_i) = (\mathbf{a}_i, \langle \mathbf{a}_i, \mathbf{s} \rangle + e_i) \rightsquigarrow (\mathbf{a}_i, b_i + \langle \mathbf{a}_i, \mathbf{t} \rangle) = \\
= (\mathbf{a}_i, \langle \mathbf{a}_i, \mathbf{s} + \mathbf{t} \rangle + e_i)
\end{aligned}
$$

- Let $\mathcal{D}$ be the distinguisher for Decision-LWE
- Test for $s_1 = 0$ (use secret shifting for other values):

Search and Decision Equivalence

- Works for $q = poly(n)$, q prime
- For bigger q a different construction is needed
- Secret shifting:

$$(\mathbf{a}_i, b_i) = (\mathbf{a}_i, \langle \mathbf{a}_i, \mathbf{s} \rangle + e_i) \rightsquigarrow (\mathbf{a}_i, b_i + \langle \mathbf{a}_i, \mathbf{t} \rangle) = \\ = (\mathbf{a}_i, \langle \mathbf{a}_i, \mathbf{s} + \mathbf{t} \rangle + e_i)$$

- Let $\mathcal{D}$ be the distinguisher for Decision-LWE
- Test for $s_1 = 0$ (use secret shifting for other values):
  - pick $r \in \mathbb{Z}_q$ uniformly
  - put $\mathbf{a}' = \mathbf{a} - (r, 0, \ldots, 0))$, give $(\mathbf{a}', b)$ to $\mathcal{D}$

Search and Decision Equivalence

- Works for $q = poly(n)$, q prime
- For bigger q a different construction is needed
- Secret shifting:

$$(\mathbf{a}_i, b_i) = (\mathbf{a}_i, \langle \mathbf{a}_i, \mathbf{s} \rangle + e_i) \rightsquigarrow (\mathbf{a}_i, b_i + \langle \mathbf{a}_i, \mathbf{t} \rangle) = \\ = (\mathbf{a}_i, \langle \mathbf{a}_i, \mathbf{s} + \mathbf{t} \rangle + e_i)$$

- Let $\mathcal{D}$ be the distinguisher for Decision-LWE
- Test for $s_1 = 0$ (use secret shifting for other values):
  - pick $r \in \mathbb{Z}_q$ uniformly
  - put $\mathbf{a}' = \mathbf{a} - (r, 0, \ldots, 0))$, give $(\mathbf{a}', b)$ to $\mathcal{D}$
  - $b = \langle \mathbf{a}, \mathbf{s} \rangle + e = \langle \mathbf{a}', \mathbf{s} \rangle + rs_1 + e$
  - $s_1 = 0$ implies $\mathcal{D}$ accepts
  - $s_1 \neq 0$ implies $(\mathbf{a}', b)$ is uniform, $\mathcal{D}$ rejects

Short secrets

- Error term may be sampled from Gaussian distribution with no security loss
- Finding $\mathbf{s}$ is equivalent to finding $\mathbf{e}$ (this limits the amount of "secret information")

Cryptosystem of [Regev05]

- Key generation:
  - Main security parameter: $n \in \mathbb{N}$
  - Public parameters: $q \approx n^2$ prime, $m \approx n \log q$, $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$
  - Secret key: $\mathbf{s} \in \mathbb{Z}_q^n$
  - Public key: $\mathbf{b} = \mathbf{A}^T\mathbf{s} + \mathbf{e}$, $\mathbf{e} \leftarrow \chi^m$
  - LWE implies: $\mathbf{s}$ cannot be obtained from $(\mathbf{A}, \mathbf{b})$

Cryptosystem of [Regev05]

- Key generation:
  - Main security parameter: $n \in \mathbb{N}$
  - Public parameters: $q \approx n^2$ prime, $m \approx n \log q$, $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$
  - Secret key: $\mathbf{s} \in \mathbb{Z}_q^n$
  - Public key: $\mathbf{b} = \mathbf{A}^T \mathbf{s} + \mathbf{e}$, $\mathbf{e} \leftarrow \chi^m$
  - LWE implies: $\mathbf{s}$ cannot be obtained from $(\mathbf{A}, \mathbf{b})$
- Encryption of $\alpha \in \{0, 1\}$:
  - $\mathbf{x} \leftarrow \{0, 1\}^m$
  - $\mathbf{u} = \mathbf{A}\mathbf{x}$
  - $u' = \langle \mathbf{b}, \mathbf{x} \rangle + \alpha \left\lfloor \frac{q}{2} \right\rfloor$
  - Security: by Left Hashover Lemma and LWE

Cryptosystem of [Regev05]

- Key generation:
  - Main security parameter: $n \in \mathbb{N}$
  - Public parameters: $q \approx n^2$ prime, $m \approx n \log q$, $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$
  - Secret key: $\mathbf{s} \in \mathbb{Z}_q^n$
  - Public key: $\mathbf{b} = \mathbf{A}^T\mathbf{s} + \mathbf{e}$, $\mathbf{e} \leftarrow \chi^m$
  - LWE implies: $\mathbf{s}$ cannot be obtained from $(\mathbf{A}, \mathbf{b})$
- Encryption of $\alpha \in \{0, 1\}$:
  - $\mathbf{x} \leftarrow \{0, 1\}^m$
  - $\mathbf{u} = \mathbf{A}\mathbf{x}$
  - $u' = \langle \mathbf{b}, \mathbf{x} \rangle + \alpha \left\lfloor \frac{q}{2} \right\rfloor$
  - Security: by Left Hashover Lemma and LWE
- Decryption:

$$u' - \langle \mathbf{s}, \mathbf{u} \rangle = \left(\left\langle \mathbf{A}^\mathbf{T}\mathbf{s} + \mathbf{e}, \mathbf{x} \right\rangle + \alpha \left\lfloor \frac{q}{2} \right\rfloor \right) - \langle \mathbf{s}, \mathbf{A}\mathbf{x} \rangle =$$

$$= \langle \mathbf{e}, \mathbf{x} \rangle + \alpha \left\lfloor \frac{q}{2} \right\rfloor \approx \alpha \left\lfloor \frac{q}{2} \right\rfloor$$

Dual Cryptosystem [GPV08]

- Key generation:
  - Security and public parameters the same as before
  - Secret key: $\mathbf{x} \leftarrow \{0,1\}^m$
  - Public key: $\mathbf{u} = \mathbf{A}\mathbf{x}$

Dual Cryptosystem [GPV08]

- Key generation:
  - Security and public parameters the same as before
  - Secret key: $\mathbf{x} \leftarrow \{0,1\}^m$
  - Public key: $\mathbf{u} = \mathbf{A}\mathbf{x}$
- Encryption of $\alpha \in \{0,1\}$:
  - $\mathbf{s} \leftarrow \mathbb{Z}_q^n$
  - $\mathbf{b} = \mathbf{A}^T\mathbf{s} + \mathbf{e}$, $\mathbf{e} \leftarrow \chi^m$
  - $b' = \langle \mathbf{s}, \mathbf{u} \rangle + e' + \alpha \left\lfloor \frac{q}{2} \right\rfloor$, $e' \leftarrow \chi$
  - Security by LWE

Dual Cryptosystem [GPV08]

- Key generation:
  - Security and public parameters the same as before
  - Secret key: $\mathbf{x} \leftarrow \{0,1\}^m$
  - Public key: $\mathbf{u} = \mathbf{A}\mathbf{x}$
- Encryption of $\alpha \in \{0,1\}$:
  - $\mathbf{s} \leftarrow \mathbb{Z}_q^n$
  - $\mathbf{b} = \mathbf{A}^T\mathbf{s} + \mathbf{e}$, $\mathbf{e} \leftarrow \chi^m$
  - $b' = \langle \mathbf{s}, \mathbf{u} \rangle + e' + \alpha \left\lfloor \frac{q}{2} \right\rfloor$, $e' \leftarrow \chi$
  - Security by LWE
- Decryption:

$$b' - \langle \mathbf{b}, \mathbf{x} \rangle = \langle \mathbf{s}, \mathbf{A}\mathbf{x} \rangle + e' + \alpha \left\lfloor \frac{q}{2} \right\rfloor - \left\langle \mathbf{A}^\mathbf{T}\mathbf{s} + \mathbf{e}, \mathbf{x} \right\rangle =$$

$$= e' + \alpha \left\lfloor \frac{q}{2} \right\rfloor - \langle \mathbf{e}, \mathbf{x} \rangle \approx \alpha \left\lfloor \frac{q}{2} \right\rfloor$$

Most Efficient Cryptosystem

- Key generation:
  - Security parameter: $n \in \mathbb{N}$
  - Public parameters: q prime, $\mathbf{A} \in \mathbb{Z}_q^{n \times n}$ invertible
  - Secret key: $\mathbf{s} \leftarrow \chi^n$
  - Public key: $\mathbf{u} = \mathbf{A}^T\mathbf{s} + \mathbf{e}$, $\mathbf{e} \leftarrow \chi^n$

Most Efficient Cryptosystem

- Key generation:
  - Security parameter: $n \in \mathbb{N}$
  - Public parameters: q prime, $\mathbf{A} \in \mathbb{Z}_q^{n \times n}$ invertible
  - Secret key: $\mathbf{s} \leftarrow \chi^n$
  - Public key: $\mathbf{u} = \mathbf{A}^T\mathbf{s} + \mathbf{e}$, $\mathbf{e} \leftarrow \chi^n$
- Encryption of $\alpha \in \{0, 1\}$:
  - $\mathbf{r} \leftarrow \chi^n$, $\mathbf{x} \leftarrow \chi^n$
  - $\mathbf{b} = \mathbf{A}\mathbf{r} + \mathbf{x}$
  - $b' = \langle \mathbf{u}, \mathbf{r} \rangle + x' + \alpha \left\lfloor \frac{q}{2} \right\rfloor$, $x' \leftarrow \chi$
  - Security by LWE with short secrets

Most Efficient Cryptosystem

- Key generation:
  - Security parameter: $n \in \mathbb{N}$
  - Public parameters: q prime, $\mathbf{A} \in \mathbb{Z}_q^{n \times n}$ invertible
  - Secret key: $\mathbf{s} \leftarrow \chi^n$
  - Public key: $\mathbf{u} = \mathbf{A}^T\mathbf{s} + \mathbf{e}$, $\mathbf{e} \leftarrow \chi^n$
- Encryption of $\alpha \in \{0, 1\}$:
  - $\mathbf{r} \leftarrow \chi^n$, $\mathbf{x} \leftarrow \chi^n$
  - $\mathbf{b} = \mathbf{A}\mathbf{r} + \mathbf{x}$
  - $b' = \langle \mathbf{u}, \mathbf{r} \rangle + x' + \alpha \left\lfloor \frac{q}{2} \right\rfloor$, $x' \leftarrow \chi$
  - Security by LWE with short secrets
- Decryption:

$$b' - \langle \mathbf{s}, \mathbf{b} \rangle = \left\langle \mathbf{A}^T\mathbf{s} + \mathbf{e}, \mathbf{r} \right\rangle + x' + \alpha \left\lfloor \frac{q}{2} \right\rfloor - \langle \mathbf{s}, \mathbf{A}\mathbf{r} + \mathbf{x} \rangle =$$

$$= \langle \mathbf{e}, \mathbf{r} \rangle - \langle \mathbf{s}, \mathbf{x} \rangle + x' + \alpha \left\lfloor \frac{q}{2} \right\rfloor \approx \alpha \left\lfloor \frac{q}{2} \right\rfloor$$

Table of Contents

Trapdoors for Lattices

- SIS based one-way function $f_{\mathbf{A}}(\mathbf{x}) = \mathbf{A}\mathbf{x}$ may be inverted using trapdoor
- $\mathbf{A}$ is (long) lattice basis generated together with a short basis $\mathbf{T}$
- Many useful applications: Identity Based Encryption, Oblivious Transfer, Deniable Encryption, etc.

Identity Based Encryption

- Extension of the Dual Cryptosystem
- Public parameter $\mathbf{A}$ sampled together with trapdoor $\mathbf{T}$
- Public key: $\mathbf{u} = \mathbf{A}\mathbf{x} = hash(id)$, secret key: $f_{\mathbf{A}}^{-1}(\mathbf{x})$

Questions?