THE MATHEMATICS OF LATTICE-BASED CRYPTOGRAPHY

6. Ring-SIS and Ring-LWE

Alfred Menezes
cryptography101.ca

Outline

1. Polynomials rings
2. Ideal lattices
3. Cyclic lattices
4. Anti-cyclic lattices
5. Ring-SIS
6. Ring-LWE

LWE-based public-key encryption

Key generation: Alice does:

1. Select $s \in_R [-B, B]^n$.
2. Select $A \in_R \mathbb{Z}_q^{n \times n}$ and $e \in_R [-B, B]^n$.
3. Compute $b = As + e$.
4. Alice's **public key** is (A, b); her **private key** is s.

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 $c_2 = b^T r + z' + m\lceil q/2 \rfloor$.
4. Output $c = (c_1, c_2)$.

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

1. Output 0 if $|c_2 - s^T c_1| < q/4$, and 1 otherwise.

Module-LWE: Replace $\mathbb{Z}_q$ elements with polynomials in a certain polynomial ring over $\mathbb{Z}_q$.

Polynomial rings

- $\mathbb{Z}[x]$ is the set of polynomials in x with integer coefficients.
- Let $f \in \mathbb{Z}[x]$ be a *monic* polynomial of degree n.
- The **polynomial ring** $R = \mathbb{Z}[x]/(f)$ is comprised of the set of all polynomials in $\mathbb{Z}[x]$ of degree less than n, with multiplication of polynomials performed modulo the **reduction polynomial** $f(x)$.
- So, to multiply polynomials $a(x), b(x) \in R$:
  1. Multiply $a(x)$ and $b(x)$ in $\mathbb{Z}[x]$, obtaining a polynomial $h(x)$ of degree at most $2n-2$.
  2. Divide $h(x)$ by $f(x)$ to get a remainder polynomial $r(x)$ of degree at most $n-1$.
  3. Then $a(x) \times b(x) = r(x)$ in R.

Representing polynomials as vectors

- A polynomial $a(x) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1}$ in $R = \mathbb{Z}[x]/(f)$ can be represented by its vector of coefficients $a = (a_0, a_1, \ldots, a_{n-1})$. The vector has length exactly n.
- I'll write $a(x) \leftrightarrow a$.
- **Example**: Consider $R = \mathbb{Z}[x]/(x^4 + 2x^2 - 11x + 1)$.
  - The polynomials $a(x) = 23 + 11x^2 + 7x^3 \in R$ and $b(x) = 40 + 5x + 16x^2 \in R$ can be represented by the vectors $a = (23, 0, 11, 7)$ and $b = (40, 5, 16, 0)$
  - In R, we have $a + b = (63, 5, 27, 7)$, $a - b = (-17, -5, -5, 7)$, and $a \times b = (709, 2324, 1618, 111)$.

Ideals

- Let $R = \mathbb{Z}[x]/(f)$.
- An **ideal** of R is a subset $I \subseteq R$ such that:
  - i) $0 \in I$.
  - ii) If $a, b \in I$ then $a + b \in I$ and $a - b \in I$.
  - iii) If $a \in I$ and $r \in R$, then $a \times r \in I$.
- **Example**: Let $a(x) \in R$. Then $\langle a(x) \rangle = \{a(x)r(x) \bmod f(x) \mid r \in R\}$ is an ideal of R, called the **principal ideal** generated by $a(x)$.
- **Example**: Let $a_1(x), a_2(x) \in R$. Then $\langle a_1(x), a_2(x) \rangle = \{a_1(x)r_1(x) + a_2(x)r_2(x) \bmod f(x) \mid r_1, r_2 \in R\}$ is an ideal of R, called the ideal generated by $a_1(x)$ and $a_2(x)$.

Ideal lattices

- Let $R = \mathbb{Z}[x]/(f)$ and let I be a nonzero ideal of R.
- Then $L(I) = \{a \mid a(x) \in I\}$ is an integer lattice in $\mathbb{R}^n$, called an **ideal lattice**.
- **Remark**. $L(I)$ does not necessarily have rank n, i.e., $L(I)$ might be spanned by $n-1$ or fewer linearly independent lattice vectors.
- We'll only be concerned with the cases $f(x) = x^n - 1$ (*cyclic lattices*) and $f(x) = x^n + 1$ (*anti-cyclic lattices*).

Cyclic lattices

- A lattice L is said to be **cyclic** if $v \in L$ implies that the right cyclic shift of v is also in L. (The *right cyclic shift* of $v = (v_0, v_1, \ldots, v_{n-1})$ is $(v_{n-1}, v_0, v_1, \ldots, v_{n-2})$.)
- Cyclic lattices are examples of **structured lattices**.
- Cyclic lattices were first studied by Micciancio in 2002.
- **Claim**. Let $R = \mathbb{Z}[x]/(x^n - 1)$. Then every ideal lattice is cyclic.
- **Proof**. Let $L = L(I)$ be an ideal lattice, and let $v \in L$.

Matrix representation of a cyclic lattice (1)

- Let $R = \mathbb{Z}[x]/(x^n - 1)$, and let $a(x) \in R$.
- Let $I = \langle a(x) \rangle$, and consider $L = L(I)$.
- Now, $I = \{a(x)r(x) \bmod (x^n - 1) \mid r(x) \in R\}$,
- If $r(x) = r_0 + r_1 x + \cdots + r_{n-1}x^{n-1}$, then
  $a(x)r(x) = r_0 a(x) + r_1 x a(x) + \cdots + r_{n-1}x^{n-1}a(x) \bmod (x^n - 1)$.
- Hence, $\{a(x), xa(x), x^2a(x), \ \ldots, x^{n-1}a(x)\}$ is a spanning set for L (all polynomials are modulo $x^n - 1$).
- More precisely, the set of vector representations of
  $a(x), \ xa(x) \bmod (x^n - 1), \ \ \ldots, \ x^{n-1}a(x) \bmod (x^n - 1)$
  is a spanning set for L.

Matrix representation of a cyclic lattice (2)

- Let A be the $n \times n$ matrix whose columns are the vector representations of $a(x), xa(x), \ldots, x^{n-1}a(x) \bmod (x^n - 1)$.

- So, $A = \begin{bmatrix} a_0 & a_{n-1} & a_{n-2} & \cdots & a_1 \\ a_1 & a_0 & a_{n-1} & \cdots & a_2 \\ a_2 & a_1 & a_0 & \cdots & a_3 \\ \vdots & \vdots & \vdots & & \vdots \\ a_{n-1} & a_{n-2} & a_{n-3} & \cdots & a_0 \end{bmatrix}$.

- A is a **circulant matrix**, denoted $A = \text{circ}(a)$.

- **Fact**. A is invertible, i.e., $L(A)$ is a full-rank lattice, if and only if $\gcd(a(x), x^n - 1) = 1$ over $\mathbb{Q}$.

- Let's henceforth assume that $\gcd(a(x), x^n - 1) = 1$.

- Now, if $r = (r_0, r_1, \ldots, r_{n-1})^T \in \mathbb{Z}^n$, then

$$Ar = r_0 \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ \vdots \\ a_{n-1} \end{bmatrix} + r_1 \begin{bmatrix} a_{n-1} \\ a_0 \\ a_1 \\ \vdots \\ a_{n-2} \end{bmatrix} + r_2 \begin{bmatrix} a_{n-2} \\ a_{n-1} \\ a_0 \\ \vdots \\ a_{n-3} \end{bmatrix} + \cdots + r_{n-1} \begin{bmatrix} a_1 \\ a_2 \\ a_3 \\ \vdots \\ a_0 \end{bmatrix}$$

Matrix representation of a cyclic lattice (3)

- **Summary**. Let $R = \mathbb{Z}[x]/(x^n - 1)$, and let $a(x) \in R$ with $\gcd(a(x), x^n - 1) = 1$ over $\mathbb{Q}$. Then $L(\langle a(x) \rangle) = L(A)$ where $A = \mathrm{circ}(a)$.
- More generally, let $a_1, a_2, \ldots, a_\ell \in R$ with $\gcd(a_i, x^n - 1) = 1$ over $\mathbb{Q}$.
- Let $I = \langle a_1(x), a_2(x), \ \ldots, a_\ell(x) \rangle$ be an ideal in R.
- Recall that $I = \{a_1 r_1 + a_2 r_2 + \cdots + a_\ell r_\ell \mid r_i \in R\}$.
- Let $m = \ell n$, and define the $n \times m$ matrix $A = \left[A_1 \,|\, A_2 \,|\, \cdots \,|\, A_\ell\right]$, where $A_i = \mathrm{circ}(a_i)$.
- Then, for $r_1, r_2, \ldots, r_\ell \in \mathbb{Z}^n$,
$$A_1 r_1 + A_2 r_2 + \cdots + A_\ell r_\ell$$
$$\leftrightarrow a_1(x) r_1(x) + a_2(x) r_2(x) + \cdots + a_\ell(x) r_\ell(x) \pmod{(x^n - 1)}.$$
- Hence $L(I) = L(A)$ is a rank-n, cyclic, integer lattice in $\mathbb{R}^n$.

$$A_i = \mathrm{circ}(a_i)$$

$$A = \begin{array}{|c|c|c|c|} \hline A_1 & A_2 & \cdots & A_\ell \\ \hline \end{array}$$

One-way function

- **Setup**. Let $R = \mathbb{Z}[x]/(x^n - 1)$, let $a_1, a_2, \ldots, a_\ell \in_R R$, and let $m = \ell n$.
  Let $A = [A_1 \,|\, A_2 \,|\, \cdots \,|\, A_\ell]$ where $A_i = \mathrm{circ}(a_i)$.
  Let q be a (relatively small) prime number with $2^m > q^n$.

$$A = \begin{array}{|c|c|c|c|} \hline A_1 & A_2 & \cdots & A_\ell \\ \hline \end{array}$$

- Consider the compression function $H_A : \{0,1\}^m \longrightarrow \mathbb{Z}_q^n$
  defined by $H_A(z) = Az \pmod{q}$.
- Micciancio (2002) proved that H_A is a **one-way function** *on average*, provided that a certain lattice problem in cyclic lattices is hard in the *worst-case*.
  (The problem is to approximate the "covering radius" of any cyclic lattice.)
- However, H_A is *not* collision resistant.

Finding collisions for H_A

- **Recall**. $H_A : \{0,1\}^m \longrightarrow \mathbb{Z}_q^n$ is defined by $H_A(z) = Az \pmod q$, where $A = [A_1 \,|\, A_2 \,|\, \cdots \,|\, A_\ell]$ and $A_i = \mathrm{circ}(a_i)$.

$$A = \boxed{A_1} \boxed{A_2} \boxed{\cdots} \boxed{A_\ell}$$

- The problem is that since each A_i is circulant, we have $A_i \begin{bmatrix} 1 \\ \vdots \\ 1 \end{bmatrix} = \begin{bmatrix} c_i \\ \vdots \\ c_i \end{bmatrix}$,
  where c_i is the sum of the entries in the first row (or first column) of A_i.
- This observation can be used to efficiently find a collision for H_A as follows:
  1. Determine $x_1, x_2, \ldots, x_\ell \in \{0, \pm 1\}$, such that $x_1c_1 + x_2c_2 + \cdots + x_\ell c_\ell = 0 \pmod q$. At least one of the x_i's should be 1, and at least one should be -1.
  2. Define z to be the length-m vector $[z_1, z_2, \ldots, z_\ell]^T$, where z_i is the length-n vector all of whose components are x_i. Note that $Az = 0 \pmod q$.
  3. Let r_1 be the length-m vector obtained from z by setting all -1 entries to 0, and let $r_2 = r_1 - z$. Then (r_1, r_2) is a collision for H_A.

Anti-cyclic lattices

- A lattice L is said to be **anti-cyclic** if $v = (v_0, v_1, \ldots, v_{n-1}) \in L$ implies that $(-v_{n-1}, v_0, v_1, \ldots, v_{n-2})$ is also in L.
- Anti-cyclic lattices were first studied by Lyubashevsky & Micciancio in 2006.
- Anti-cyclic lattices are **structured lattices.**
- **Claim**. Let $R = \mathbb{Z}[x]/(x^n + 1)$. Then every ideal lattice is anti-cyclic.
- **Proof**. Let $L = L(I)$ be an ideal lattice, and let $v \in L$.
  Recall that $v = (v_0, v_1, \ldots, v_{n-1}) \leftrightarrow v(x) = v_0 + v_1 x + \cdots + v_{n-1}x^{n-1}$.
  Now, $xv(x) = v_0 x + v_1 x^2 + \cdots + v_{n-1}x^n$

$$= -v_{n-1} + v_0 x + v_1 x^2 + \cdots + v_{n-2}x^{n-1} \bmod (x^n + 1)$$

Matrix representation of an anti-cyclic lattice (1)

- Let $n = 2^w$. Then $x^n + 1$ is irreducible over $\mathbb{Q}$.
- Let $R = \mathbb{Z}[x]/(x^n + 1)$, and let $a(x) \in R$ with $a(x) \neq 0$. Then $\gcd(a(x), x^n + 1) = 1$.
- Let $I = \langle a(x) \rangle$, and consider $L = L(I)$.
- Now, $I = \{a(x)r(x) \bmod (x^n + 1) \mid r(x) \in R\}$.
- Hence, the set of vector representations of $a(x), xa(x) \bmod (x^n + 1), \ldots$ $x^{n-1}a(x) \bmod (x^n + 1)$ is a spanning set for L.
- In fact, the vectors are a basis for L.
- Let A be the $n \times n$ matrix whose columns are the vector representations of $a(x), xa(x), \ldots, x^{n-1}a(x) \bmod (x^n + 1)$.
- So, $A = \begin{bmatrix} a_0 & -a_{n-1} & -a_{n-2} & \cdots & -a_1 \\ a_1 & a_0 & -a_{n-1} & \cdots & -a_2 \\ a_2 & a_1 & a_0 & \cdots & -a_3 \\ \vdots & \vdots & \vdots & & \vdots \\ a_{n-1} & a_{n-2} & a_{n-3} & \cdots & a_0 \end{bmatrix}$.
- Then $L(I) = L(A)$.
- A is an **anti-circulant matrix**, denoted $A = \overline{\mathrm{circ}}(a)$.
- Notice that the row sums (and column sums) are no longer equal.

Example: Multiplication in $R = \mathbb{Z}[x]/(x^n + 1)$

- Let $n = 4$, so $R = \mathbb{Z}[x]/(x^4 + 1)$.
- Let $a(x) = 3 - 2x + 5x^2 - 4x^4 \in R$.
- Then $A = \overline{\text{circ}}(a) = \begin{bmatrix} 3 & 4 & -5 & 2 \\ -2 & 3 & 4 & -5 \\ 5 & -2 & 3 & 4 \\ -4 & 5 & -2 & 3 \end{bmatrix}$.
- Let $r(x) = 1 + 2x + 11x^2 - 7x^3 \in R$.
- **Exercise**: Check that $a(x) \times r(x) \pmod{x^4 + 1} = -58 + 83x + 6x^2 - 37x^3$, and $A \cdot r^T = A \cdot [1, 2, 11, -7]^T = [-58, 83, 6, -37]^T$.

Matrix representation of an anti-cyclic lattice (2)

- **Summary**. Let $n = 2^w$, let $R = \mathbb{Z}[x]/(x^n + 1)$, and let $a(x) \in R$ with $a(x) \neq 0$. Then $L(\langle a(x) \rangle) = L(A)$ where $A = \overline{\text{circ}}(a)$.

- More generally, let $a_1, a_2, \ldots, a_\ell \in R$ with $a_i \neq 0$.
- Let $I = \langle a_1(x),\ a_2(x),\ \ldots,\ a_\ell(x) \rangle$ be an ideal in R.
- Let $m = \ell n$, and define the $n \times m$ matrix
$$A = \left[A_1 \,|\, A_2 \,|\, \cdots \,|\, A_\ell \right],$$
where $A_i = \overline{\text{circ}}(a_i)$.

$$A_i = \overline{\text{circ}}(a_i)$$
$$A = \begin{array}{|c|c|c|c|} \hline A_1 & A_2 & \cdots & A_\ell \\ \hline \end{array}$$

- Then, $L(I) = L(A)$ is a rank-n, anti-cyclic, integer lattice in $\mathbb{R}^n$.
- These *structured lattices* can be used to define a special case of SIS, called **Ring-SIS**.

Sizes

- Recall: q prime, $\mathbb{Z}_q = \{0,1,\ldots,q-1\}$, $n = 2^w$.
  - $R = \mathbb{Z}[x]/(x^n + 1)$, $R_q = \mathbb{Z}_q[x]/(x^n + 1)$.
- For $r \in \mathbb{Z}_q$, define $r \bmod\text{s}\ q = \begin{cases} r, & \text{if } 0 \le r \le (q-1)/2, \\ q - r & \text{if } (q-1)/2 < r \le q-1. \end{cases}$
- For $r \in \mathbb{Z}_q$, define $\|r\|_\infty = |\, r \bmod\text{s}\ q \,|$.
  - **Example**: For $q = 23$, $\|3\|_\infty = 3$ and $\|19\|_\infty = 4$.
- For $a(x) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} \in R_q$, define $\|a\|_\infty = \max \|a_i\|_\infty$.
  - **Example**: Let $q = 23$ and $n = 8$. Then $\|3 + 19x^2 + 21x^3 + x^4\|_\infty = 4$.

Ring-SIS

- Introduced by Lyubashevsky-Micciancio and Peikert-Rosen (2006).
- **Ring-SIS(n, ℓ, q, B)**:
  Given $a_1, a_2, \ldots, a_\ell \in_R R_q$, find $z_1, z_2, \ldots, z_\ell \in R_q$ such that $a_1 z_1 + a_2 z_2 + \cdots + a_\ell z_\ell = 0 \pmod{q}$, where $\|z_i\|_\infty \leq B$ and not all z_i are 0.
  - **Note**: If $(z_1, z_2, \ldots, z_\ell)$ is a solution then so is $(xz_1, xz_2, \ldots, xz_\ell)$.
- *Equivalently*, given $a_1, a_2, \ldots, a_\ell \in_R R_q$, find nonzero $z \in [-B, B]^m$ such that $Az = 0 \pmod{q}$, where $A = [\overline{\text{circ}}(a_1) \mid \cdots \mid \overline{\text{circ}}(a_\ell)]_{n \times m}$.
- So, Ring-SIS is a special case of SIS where the matrix A is *structured*.

$$A_i = \overline{\text{circ}}(a_i)$$

$$A = \begin{array}{|c|c|c|c|} \hline A_1 & A_2 & \cdots & A_\ell \\ \hline \end{array}$$

- Lyubashevsky and Micciancio proved that solving Ring-SIS on *average* is at least as hard as solving SVP_γ for anti-cyclic lattices *in the worst case*.

Example: Ring-SIS (1)

- Let $q = 59$, $n = 4$, $f(x) = x^4 + 1$, $R_q = \mathbb{Z}_{59}[x]/(x^4 + 1)$, $\ell = 3$, $B = 2$.
- Let $a_1(x) = 10 + 16x^2 + 51x^3$, $a_2(x) = 41 + 10x + 54x^2 + 16x^3$, $a_3(x) = 11 + 17x + 39x^2 + 5x^3 \in R_q$.
- **Ring-SIS instance:**
Find $z_1, z_2, z_3 \in R_q$, not all 0, with $a_1z_1 + a_2z_2 + a_3z_3 = 0 \pmod{q}$ and $\|z_i\|_\infty \le 2$.
- We have $A = \underbrace{\left[\begin{array}{cccc|cccc|cccc} 10 & 8 & 43 & 0 & 41 & 43 & 5 & 49 & 11 & 54 & 20 & 42 \\ 0 & 10 & 8 & 43 & 10 & 41 & 43 & 5 & 17 & 11 & 54 & 20 \\ 16 & 0 & 10 & 8 & 54 & 10 & 41 & 43 & 39 & 17 & 11 & 54 \\ 51 & 16 & 0 & 10 & 16 & 54 & 10 & 41 & 5 & 39 & 17 & 11 \end{array}\right]_{4\times 12}}$.

$$\overline{\text{circ}}(a_1) \qquad \overline{\text{circ}}(a_2) \qquad \overline{\text{circ}}(a_3)$$

Example: Ring-SIS (2)

- Gaussian elimination (mod q) on A yields the following matrix in reduced form:

$$A' = \begin{bmatrix} 1 & 0 & 0 & 0 & 48 & 6 & 43 & 45 & 7 & 3 & 58 & 57 \\ 0 & 1 & 0 & 0 & 14 & 48 & 6 & 43 & 2 & 7 & 3 & 58 \\ 0 & 0 & 1 & 0 & 16 & 14 & 48 & 6 & 1 & 2 & 7 & 3 \\ 0 & 0 & 0 & 1 & 53 & 16 & 14 & 48 & 56 & 1 & 2 & 7 \end{bmatrix}.$$

- The set of all solutions $r = (r_1, r_2, \ldots, r_{12}) \in \mathbb{Z}_{59}^{12}$ to $A'r = 0 \pmod{q}$ is:

$$\begin{aligned} r_1 &= 11r_5 + 53r_6 + 16r_7 + 14r_8 + 52r_9 + 56r_{10} + r_{11} + 2r_{12} \\ r_2 &= 45r_5 + 11r_6 + 53r_7 + 16r_8 + 57r_9 + 52r_{10} + 56r_{11} + r_{12} \\ r_3 &= 43r_5 + 45r_6 + 11r_7 + 53r_8 + 58r_9 + 57r_{10} + 52r_{11} + 56r_{12} \\ r_4 &= 6r_5 + 43r_6 + 45r_7 + 11r_8 + 3r_9 + 58r_{10} + 57r_{11} + 52r_{12}\,. \end{aligned}$$

Example: Ring-SIS (3)

- The total number of solutions to $A'r = 0 \pmod{q}$ is $q^8 = 146{,}830{,}437{,}604{,}321$.
    - Of these, the number of solutions r that are nonzero and in $[-2, 2]^{12}$ is 24.
- The nonzero Ring-SIS solutions (up to multiplication by $\pm 1,\ \pm x,\ \pm x^2,\ \pm x^3$) are:

$$
\begin{aligned}
R_1 &= (1, 2, \text{-}1, 2, \text{-}1, 2, 0, \text{-}2, 1, 0, 0, 0)\\
R_2 &= (1, 1, 0, 0, \text{-}2, \text{-}2, 0, 0, \text{-}2, 2, \text{-}1, 2)\\
R_3 &= (1, 2, \text{-}2, 1, \text{-}1, 2, 2, 0, 0, 2, 2, \text{-}2)\,.
\end{aligned}
$$

- For example, the first solution R_1 in polynomial form is:

$$z_1(x) = 1 + 2x - x^2 + 2x^3, \quad z_2(x) = -1 + 2x - 2x^3, \quad z_3(x) = 1.$$

- **Check**: $AR_1 = 0 \pmod{q}$ and $a_1(x)z_1(x) + a_2(x)z_2(x) + a_3(x)z_3(x) = 0$ in R_q.

Collision-resistant hash function

- **Setup**. Select q and ℓ with $\ell > \log q$.
  Let $R_q = \mathbb{Z}_q[x]/(x^n + 1)$, let $a_1, a_2, \ldots, a_\ell \in_R R_q$, and let $m = \ell n$.
  Let $A = [A_1 \,|\, A_2 \,|\, \cdots \,|\, A_\ell]$ where $A_i = \overline{\mathrm{circ}}(a_i)$.

$$A_i = \overline{\mathrm{circ}}(a_i)$$

$$A = \begin{array}{|c|c|c|c|} \hline A_1 & A_2 & \cdots & A_\ell \\ \hline \end{array}$$

- Consider the compression function $H_A : \{0,1\}^m \longrightarrow \mathbb{Z}_q^n$ defined by $H_A(z) = Az \pmod{q}$.

- **Exercise**: Prove that H_A is collision resistant provided that Ring-SIS is hard.

- Then H_A is a **collision-resistant function** *on average*, provided that SVP_γ for anti-cyclic lattices is hard to solve i*n the worst case*.

Ring-SIS versus SIS

SIS

1. The $n \times m$ matrix A requires storage for mn $\mathbb{Z}_q$ elements.

2. Computing $Ar \pmod{q}$ takes time $O(mn)$.

Ring-SIS

1. The $n \times m$ matrix $A = [\overline{\text{circ}}(a_1) \mid \cdots \mid \overline{\text{circ}}(a_\ell)]$ can be derived from $\ell n = m$ $\mathbb{Z}_q$ elements.

2. $Ar \pmod{q}$ can be computed in time $O(m \log n)$ using the Number-Theoretic Transform (when n divides $q-1$).

Security

- No attacks (either theoretical or practical) are known on Ring-SIS that are faster than the fastest attacks known on SIS.
- In other words, no attacks are known on Ring-SIS that exploit the structure in the matrix A.

Ring-LWE

- Lyubashevsky-Peikert-Rosen (2010)
- Let S_B denote the polynomials in $R_q = \mathbb{Z}_q[x]/(x^n + 1)$ whose coefficients (when reduced mods q) are in $[-B, B]$.
- **Ring-LWE(n, k, q, B):** Let $s \in_R R_q$ and $e_1, \ldots, e_k \in_R S_B$ where $B \ll q/2$.
  Let $a_1, \ldots, a_k \in_R R_q$ and $b_i = a_i s + e_i \in R_q$ for $i = 1, \ldots, k$.
  Given the a_i and b_i, determine s.
- Equivalently, solve the following noisy linear systems of equations for $s \in \mathbb{Z}_q^n$ (and $e \in [-B, B]^{kn}$):

$$As + e = b \qquad \underbrace{\begin{bmatrix} \overline{\mathrm{circ}}(a_1) \\ \vdots \\ \overline{\mathrm{circ}}(a_k) \end{bmatrix}}_{kn \times n} \underbrace{\begin{bmatrix} s \end{bmatrix}}_{n \times 1} + \underbrace{\begin{bmatrix} e_1 \\ \vdots \\ e_k \end{bmatrix}}_{kn \times 1} = \underbrace{\begin{bmatrix} b_1 \\ \vdots \\ b_k \end{bmatrix}}_{kn \times 1} \pmod{q}$$

- So, Ring-LWE is a special case of LWE where the matrix A is *structured*.

Example: Ring-LWE (1)

- Let $q = 17,\ n = 4,\ f(x) = x^4 + 1$,
  $R_q = \mathbb{Z}_{17}[x]/(x^4 + 1),\ k = 3,\ \ B = 3.$
- **Ring-LWE instance**:
  Given $a_1(x) = 10 + 16x^2$,
  $a_2(x) = 7 + 10x + 3x^2 + 16x^3$,
  $a_3(x) = 9 + 12x + 16x^2 + 14x^3$,
  $b_1(x) = 16 + 9x + 6x^2 + 4x^3$,
  $b_2(x) = 2 + 16x + 12x^2$,
  $b_3(x) = 10 + 15x + 7x^2$,
  find $s \in R_q$ such that
  $b_i - a_i s = e_i \in S_3$ for $i = 1,2,3$.
- $$A = \begin{bmatrix} 10 & 0 & 1 & 0 \\ 0 & 10 & 0 & 1 \\ 16 & 0 & 10 & 0 \\ 0 & 16 & 0 & 10 \\ \hline 7 & 1 & 14 & 7 \\ 10 & 7 & 1 & 14 \\ 3 & 10 & 7 & 1 \\ 16 & 3 & 10 & 7 \\ \hline 9 & 3 & 1 & 5 \\ 12 & 9 & 3 & 1 \\ 16 & 12 & 9 & 3 \\ 14 & 16 & 12 & 9 \end{bmatrix} \qquad b = \begin{bmatrix} 16 \\ 9 \\ 6 \\ 4 \\ \hline 2 \\ 16 \\ 12 \\ 0 \\ \hline 10 \\ 15 \\ 7 \\ 0 \end{bmatrix}.$$

Example: Ring-LWE (2)

- Solve $As + e = b \pmod{17}$, where $s \in \mathbb{Z}_{17}^4$ and $e \in [-3,3]^{12}$.
- Two solutions:
  - $s = [5, 15, 15, 12]^T$, $e = [2, 0, \text{-}3, 1, \text{-}2, 1, 2, \text{-}2, \text{-}2, 1, 1, \text{-}3]^T$.
  - $s = [14, 15, 14, 12]^T$, $e = [-2, 0, \text{-}1, 1, 0, \text{-}3, \text{-}1, 0, 3, \text{-}2, 2, 2]^T$.
- The first solution in polynomial form is:
  - $s(x) = 5 + 15x + 15x^2 + 12x^3$, $e_1(x) = 2 - 3x^2 + x^3$, $e_2(x) = -2 + x + 2x^2 - 2x^3$, $e_3(x) = -2 + x + x^2 - 3x^3$.
  - **Check**: $As + e = b \pmod{q}$ and $a_i(x)s(x) + e_i(x) = b_i(x)$ in R_q for $i = 1,2,3$.

Ring-LWE security

- Lyubashevsky-Peikert-Rosen proved that solving Ring-LWE on *average* is at least as hard as *quantumly* solving SIVP_γ for anti-cyclic lattices *in the worst case*.
- No attacks (either theoretical or practical) are known on Ring-LWE that are faster than the fastest attacks known on LWE.
- Ring-LWE has the same advantages over LWE as Ring-SIS has over SIS.

$$As + e = b \qquad \underbrace{\begin{bmatrix} \overline{\mathrm{circ}}(a_1) \\ \vdots \\ \overline{\mathrm{circ}}(a_k) \end{bmatrix}}_{kn \times n} \underbrace{\begin{bmatrix} s \end{bmatrix}}_{n \times 1} + \underbrace{\begin{bmatrix} e_1 \\ \vdots \\ e_k \end{bmatrix}}_{kn \times 1} = \underbrace{\begin{bmatrix} b_1 \\ \vdots \\ b_k \end{bmatrix}}_{kn \times 1} \pmod{q}$$

Ring-LWE-based public-key encryption

Key generation: Alice does:

1. Select $s \in_R S_B$. [Note: short-secret Ring-LWE]
2. Select $a \in_R R_q$ and $e \in_R S_B$.
3. Compute $b = as + e \in R_q$.
4. Alice's **public key** is (a, b);
   her **private key** is s.

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

1. Obtain an authentic copy of Alice's encryption key (a, b).
2. Select $r, z, z' \in_R S_B$.
3. Compute $c_1 = ar + z$ and $c_2 = br + z' + \lceil q/2 \rfloor m$.
4. Output $c = (c_1, c_2) \in R_q \times R_q$.

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

1. Output $\text{Round}_q(c_2 - sc_1)$.

Security: Indistinguishable against chosen-plaintext attacks assuming that Decisional short-secret Ring-LWE is hard.