THE MATHEMATICS OF LATTICE-BASED CRYPTOGRAPHY

7. Module-SIS and Module-LWE

Alfred Menezes
cryptography101.ca

Outline

1. The module R_q^k
2. Module-SIS (MSIS)
3. Module-LWE (MLWE)

Modules

- **Main idea** in Module-SIS (MSIS)
  Replace polynomials $a_1, a_2, \ldots, a_\ell$ in Ring-SIS by vectors of polynomials in R_q^k.
- **Main idea** in Module-LWE (MLWE)
  Replace polynomials $a_1, a_2, \ldots, a_k$ in Ring-LWE by vectors of polynomials in R_q^ℓ.
- The MSIS and MLWE lattices are less structured than their Ring-SIS and Ring-LWE counterparts.
- Recall: $R = \mathbb{Z}[x]/(x^n + 1)$ and $R_q = \mathbb{Z}_q[x]/(x^n + 1)$, where $n = 2^w$.
- We will work with **modules** R_q^k for MSIS (and R_q^ℓ for MLWE).
  - The module R_q^k is comprised of the length-k vectors of polynomials in R_q.
  - Such vectors can be added and subtracted component-wise, so the result is also a vector in R_q^k.
  - The **inner product** (multiplication) of two vectors in R_q^k results in a polynomial in R_q.
  - The **size** of $a = (a_1, a_2, \ldots, a_k) \in R_q^k$ is $\|a\|_\infty = \max_i \|a_i\|_\infty$.
- See V1b of my "Kyber and Dilithium" course for examples.

Module-SIS (1)

- **MSIS(n, k, ℓ, q, B)**:
  Given $a_1, a_2, \ldots, a_\ell \in_R R_q^k$ (where $\ell > k$), find $z_1, z_2, \ldots, z_\ell \in R_q$ such that $a_1 z_1 + a_2 z_2 + \cdots + a_\ell z_\ell = 0$ where $\|z_i\|_\infty \le B$ and not all z_i are 0.
- **Note**: Each a_i is now a vector of polynomials: $a_i = [a_{i1} \quad a_{i2} \quad \cdots \quad a_{ik}]^T$.
- So, Module-SIS asks for a "small" nonzero solution to the polynomial-matrix equation:

$$\begin{bmatrix} a_{11} & a_{21} & \cdots & a_{\ell 1} \\ a_{12} & a_{22} & \cdots & a_{\ell 2} \\ \vdots & \vdots & & \vdots \\ a_{1k} & a_{2k} & \cdots & a_{\ell k} \end{bmatrix}_{k\times\ell} \begin{bmatrix} z_1 \\ z_2 \\ \vdots \\ z_\ell \end{bmatrix}_{\ell\times 1} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}_{k\times 1}.$$

- **Note**: If $(z_1, z_2, \ldots, z_\ell)$ is a solution then so is $(xz_1, xz_2, \ldots, xz_\ell)$.

Module-SIS (2)

- Equivalent formulation of **MSIS(*n*, *k*, *ℓ*, *q*, *B*)**:
Given $a_1, a_2, \ldots, a_\ell \in_R R_q^k$, find nonzero $z \in [-B, B]^m$ (where $m = \ell n$) such that $Az = 0 \pmod{q}$, where

$$A = \begin{bmatrix} \overline{\text{circ}}(a_{11}) & \overline{\text{circ}}(a_{21}) & \cdots & \overline{\text{circ}}(a_{\ell 1}) \\ \overline{\text{circ}}(a_{12}) & \overline{\text{circ}}(a_{22}) & \cdots & \overline{\text{circ}}(a_{\ell 2}) \\ \vdots & \vdots & & \vdots \\ \overline{\text{circ}}(a_{1k}) & \overline{\text{circ}}(a_{2k}) & \cdots & \overline{\text{circ}}(a_{\ell k}) \end{bmatrix}_{kn \times \ell n}.$$

- So, MSIS is a special case of SIS where the matrix A is *structured*.

Example: MSIS (1)

- Let $q = 67$, $n = 4$, $f(x) = x^4 + 1$, $R_q = \mathbb{Z}_{67}[x]/(x^4 + 1)$, $k = 2$, $\ell = 3$, $B = 10$.
- Let $a_1 = [a_{11}, a_{12}]^T = [32 + 66x^2 + 33x^3,\ 30 + 64x + 31x^2 + 65x^3]^T \in R_q^2$,
  $a_2 = [a_{21}, a_{22}]^T = [42 + 44x + 20x^2 + 65x^3,\ 63 + 41x + 19x^2 + 64x^3]^T \in R_q^2$,
  $a_3 = [a_{31}, a_{32}]^T = [2 + 60x + 33x^2 + 42x^3,\ 26 + 9x + 57x^2 + 7x^3]^T \in R_q^2$.
- M**SIS instance:** Find $z_1, z_2, z_3 \in R_q$, not all 0, with $a_{11}z_1 + a_{21}z_2 + a_{31}z_3 = 0 \pmod{q}$, $a_{12}z_1 + a_{22}z_2 + a_{32}z_3 = 0 \pmod{q}$, and $\|z_i\|_\infty \le 10$.
- We have

$$A = \left[\begin{array}{cccc|cccc|cccc} 32 & 34 & 1 & 0 & 42 & 2 & 47 & 23 & 2 & 25 & 34 & 7 \\ 0 & 32 & 34 & 1 & 44 & 42 & 2 & 47 & 60 & 2 & 25 & 34 \\ 66 & 0 & 32 & 34 & 20 & 44 & 42 & 2 & 33 & 60 & 2 & 25 \\ 33 & 66 & 0 & 32 & 65 & 20 & 44 & 42 & 42 & 33 & 60 & 2 \\ \hline 30 & 2 & 36 & 3 & 63 & 3 & 48 & 26 & 26 & 60 & 10 & 58 \\ 64 & 30 & 2 & 36 & 41 & 63 & 3 & 48 & 9 & 26 & 60 & 10 \\ 31 & 64 & 30 & 2 & 19 & 41 & 63 & 3 & 57 & 9 & 26 & 60 \\ 65 & 31 & 64 & 30 & 64 & 19 & 41 & 63 & 7 & 57 & 9 & 26 \end{array}\right]_{8\times 12}.$$

Example: MSIS (2)

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

$$A' = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 17 & 27 & 21 & 28 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 39 & 17 & 27 & 21 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 46 & 39 & 17 & 27 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 40 & 46 & 39 & 17 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 46 & 29 & 44 & 53 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 14 & 46 & 29 & 44 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 23 & 14 & 46 & 29 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 38 & 23 & 14 & 46 \end{bmatrix}.$$

- 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:

$$\begin{aligned} r_1 &= 50r_9 + 40r_{10} + 46r_{11} + 39r_{12} & r_2 &= 28r_9 + 50r_{10} + 40r_{11} + 46r_{12} \\ r_3 &= 21r_9 + 28r_{10} + 50r_{11} + 40r_{12} & r_4 &= 27r_9 + 21r_{10} + 28r_{11} + 50r_{12} \\ r_5 &= 21r_9 + 38r_{10} + 23r_{11} + 14r_{12} & r_6 &= 53r_9 + 21r_{10} + 38r_{11} + 23r_{12} \\ r_7 &= 44r_9 + 53r_{10} + 21r_{11} + 38r_{12} & r_8 &= 29r_9 + 44r_{10} + 53r_{11} + 21r_{12}\,. \end{aligned}$$

Example: MSIS (3)

- The total number of solutions to $A'r = 0 \pmod{q}$ is $q^4 = 20{,}151{,}121$.
  - Of these, the number of solutions r that are nonzero and in $[-10, 10]^{12}$ is 8.
- The MSIS solution (up to multiplication by $\pm 1,\ \pm x,\ \pm x^2,\ \pm x^3$) is:
  $$r = (6, -8, 8, 0, 2, 10, -6, 3, -9, 6, 3, 2)$$
- The solution in polynomial form is:
  $z_1(x) = 6 - 8x + 8x^2,\ \ z_2(x) = 2 + 10x - 6x^2 + 3x^3,\ \ z_3(x) = -9 + 6x + 3x^2 + 2x^3.$
- **Check**:

  (i) $Ar = 0 \pmod{q}$,

  (ii) $a_{11}(x)z_1(x) + a_{21}(x)z_2(x) + a_{31}(x)z_3(x) = 0$ in R_q, and

  (iii) $a_{12}(x)z_1(x) + a_{22}(x)z_2(x) + a_{32}(x)z_3(x) = 0$ in R_q.

Module-SIS notes

- Langlois and Stehlé (2015) introduced MSIS and proved that solving MSIS on *average* is at least as hard as solving SIVP_γ for module lattices *in the worst case.*
- Setting $k = 1$ gives an instance of Ring-SIS.
- Setting $n = 1$ (replacing R_q by $\mathbb{Z}_q$) gives an instance of SIS.
- So, MSIS "interpolates" between SIS and Ring-SIS.

$$A = \begin{bmatrix} \overline{\text{circ}}(a_{11}) & \overline{\text{circ}}(a_{21}) & \cdots & \overline{\text{circ}}(a_{\ell 1}) \\ \overline{\text{circ}}(a_{12}) & \overline{\text{circ}}(a_{22}) & \cdots & \overline{\text{circ}}(a_{\ell 2}) \\ \vdots & \vdots & & \vdots \\ \overline{\text{circ}}(a_{1k}) & \overline{\text{circ}}(a_{2k}) & \cdots & \overline{\text{circ}}(a_{\ell k}) \end{bmatrix}_{kn \times \ell n}$$

- A primary advantage of MSIS over Ring-SIS is that parameters q and n can be fixed for MSIS, and then k can be varied for different security levels.
- For example, Dilithium fixes $q = 8380417$, $n = 256$, and $(k, \ell) \in \{(4,4), (6,5), (8,7)\}$, where now the underlying matrix of polynomials is $[A \mid I_k]_{k \times \ell}$ where $A \in_R R_q^{k \times \ell}$.
So, Dilithium is "closer" to Ring-SIS than to SIS.
- Since $2n = 512$ divides $q - 1$, the Number-Theoretic Transform can be used for fast polynomial multiplication in $R_q = \mathbb{Z}_q[x]/(x^{256} + 1)$.

Module-LWE

- **MLWE(n, k, ℓ, q, B)**:
  Let $s \in_R R_q^\ell$ and $e \in_R S_B^k$ where $k > \ell$ and $B \ll q/2$.
  Let $a_1, a_2, \ldots, a_k \in_R R_q^\ell$ and $b_i = a_i^T s + e_i \in R_q$ for $i = 1, \ldots, k$.
  Given the a_i and b_i, determine s.
- Note that each a_i is now a vector of polynomials: $a_i = [a_{i1} \quad a_{i2} \quad \cdots \quad a_{i\ell}]^T$.
- So, Module-LWE asks for a solution $s \in R_q^\ell$, $e \in S_B^k$ to the polynomial-matrix equation:

$$\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1\ell} \\ a_{21} & a_{22} & \cdots & a_{2\ell} \\ \vdots & \vdots & & \vdots \\ a_{k1} & a_{k2} & \cdots & a_{k\ell} \end{bmatrix}_{k \times \ell} \begin{bmatrix} s_1 \\ s_2 \\ \vdots \\ s_\ell \end{bmatrix}_{\ell \times 1} + \begin{bmatrix} e_1 \\ e_2 \\ \vdots \\ e_k \end{bmatrix}_{k \times 1} = \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_k \end{bmatrix}_{k \times 1}.$$

Module-LWE (2)

- Equivalent formulation of **MLWE**(n, k, ℓ, q, B):
  Let $s \in_R R_q^\ell$ and $e \in_R S_B^k$ where $k > \ell$ and $B \ll q/2$.
  Let $a_1, a_2, \ldots, a_k \in_R R_q^\ell$ and $b_i = a_i^T s + e_i \in R_q$ for $i = 1, \ldots, k$.

  Given the a_i and b_i, find $s \in \mathbb{Z}_q^{\ell n}$ and $e \in [-B, B]^{kn}$ such that $As + e = b \pmod{q}$, where

$$A = \begin{bmatrix} \overline{\text{circ}}(a_{11}) & \overline{\text{circ}}(a_{21}) & \cdots & \overline{\text{circ}}(a_{\ell 1}) \\ \overline{\text{circ}}(a_{12}) & \overline{\text{circ}}(a_{22}) & \cdots & \overline{\text{circ}}(a_{\ell 2}) \\ \vdots & \vdots & & \vdots \\ \overline{\text{circ}}(a_{1k}) & \overline{\text{circ}}(a_{2k}) & \cdots & \overline{\text{circ}}(a_{\ell k}) \end{bmatrix}_{kn \times \ell n} \quad \text{and} \quad b = \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_k \end{bmatrix}_{kn \times 1}.$$

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

Example: Module-LWE (1)

- Let $q = 37,\ n = 4,\ f(x) = x^4 + 1,\ R_q = \mathbb{Z}_{37}[x]/(x^4 + 1),\ k = 3,\ \ell = 2,\ B = 1.$
- **Module-LWE instance**: Given

$$a_1 = \begin{bmatrix} a_{11}(x) \\ a_{21}(x) \\ a_{31}(x) \end{bmatrix} = \begin{bmatrix} 21 + 5x^2 + 19x^3 \\ 4 + 14x + 20x^2 + 19x^3 \\ 13 + 7x + 6x^2 + 8x^3 \end{bmatrix}, \quad a_2 = \begin{bmatrix} a_{12}(x) \\ a_{22}(x) \\ a_{32}(x) \end{bmatrix} = \begin{bmatrix} 1 + 23x + 9x^2 + 8x^3 \\ 24 + 23x + 22x^2 + 21x^3 \\ 34 + 33x + 32x^2 + 31x^3 \end{bmatrix},$$

and $b = \begin{bmatrix} b_1(x) \\ b_2(x) \\ b_3(x) \end{bmatrix} = \begin{bmatrix} 19 + 32x + 7x^2 + 20x^3 \\ 32 + 19x^2 + 8x^3 \\ 29 + 15x + 11x^2 + 14x^3 \end{bmatrix},$

find $s = \begin{bmatrix} s_1(x) \\ s_2(x) \end{bmatrix} \in R_q^2$ such that $b_i(x) - a_{i1}(x)s_1(x) - a_{i2}(x)s_2(x) = e_i(x) \in S_1$ for $i = 1,2,3$.

Example: Module-LWE (2)

- Solve $As + e = b \pmod{37}$ for $s \in \mathbb{Z}_{37}^8$ and $e \in [-1,1]^{12}$, where

$$A = \left[\begin{array}{cccc|cccc} 21 & 18 & 32 & 0 & 1 & 29 & 28 & 14 \\ 0 & 21 & 18 & 32 & 23 & 1 & 29 & 28 \\ 5 & 0 & 21 & 18 & 9 & 23 & 1 & 29 \\ 19 & 5 & 0 & 21 & 8 & 9 & 23 & 1 \\ \hline 4 & 18 & 17 & 23 & 24 & 16 & 15 & 14 \\ 14 & 4 & 18 & 17 & 23 & 24 & 16 & 15 \\ 20 & 14 & 4 & 18 & 22 & 23 & 24 & 16 \\ 19 & 20 & 14 & 4 & 21 & 22 & 23 & 24 \\ \hline 13 & 29 & 31 & 30 & 34 & 6 & 5 & 4 \\ 7 & 13 & 29 & 31 & 33 & 34 & 6 & 5 \\ 6 & 7 & 13 & 29 & 32 & 33 & 34 & 6 \\ 8 & 6 & 7 & 13 & 31 & 32 & 33 & 34 \end{array}\right]_{12\times 8} \quad \text{and} \quad b = \left[\begin{array}{c} 19 \\ 32 \\ 7 \\ 20 \\ \hline 32 \\ 0 \\ 19 \\ 8 \\ \hline 29 \\ 15 \\ 11 \\ 14 \end{array}\right]_{12\times 1}.$$

Example: Module-LWE (3)

- Solve $As + e = b \pmod{37}$, where $s \in \mathbb{Z}_{37}^8$ and $e \in [-1,1]^{12}$.
- There are two solutions (s, e):
  - $s = [31, 32, 33, 2, 17, 35, 13, 32]$, $e = [\text{-}1, 0, \text{-}1, 1, 0, \text{-}1, \text{-}1, 0, 1, 0, 0, 1]^T$.
  - $s = [2, 29, 9, 22, 32, 12, 27, 18]$, $e = [\text{-}1, 0, 1, 0, 1, \text{-}1, 0, \text{-}1, 1, \text{-}1, \text{-}1, 0]^T$.
- The first solution in polynomial form is:
  $s_1(x) = 31 + 32x + 33x^2 + 2x^3$, $s_2(x) = 17 + 35x + 13x^2 + 32x^3$,
  $e_1(x) = -1 - x^2 + x^3$, $e_2(x) = -x - x^2$, $e_3(x) = 1 + x^3$.
  - **Check**: $As + e = b \pmod{37}$
    and $a_{i1}(x)s_1(x) + a_{i2}s_2(x) + e_i(x) = b_i(x)$ in R_q for $i = 1,2,3$.

Module-LWE notes

- Module-LWE was introduced by Brakerski, Gentry and Vaikuntanathan (2011).
- Check: Setting $\ell = 1$ gives an instance of Ring-LWE.
- Setting $n = 1$ (replacing R_q by $\mathbb{Z}_q$) gives an instance of LWE.
- So, MLWE "interpolates" between LWE and Ring-LWE.

$$A = \begin{bmatrix} \overline{\text{circ}}(a_{11}) & \overline{\text{circ}}(a_{21}) & \cdots & \overline{\text{circ}}(a_{\ell 1}) \\ \overline{\text{circ}}(a_{12}) & \overline{\text{circ}}(a_{22}) & \cdots & \overline{\text{circ}}(a_{\ell 2}) \\ \vdots & \vdots & & \vdots \\ \overline{\text{circ}}(a_{1k}) & \overline{\text{circ}}(a_{2k}) & \cdots & \overline{\text{circ}}(a_{\ell k}) \end{bmatrix}_{kn \times \ell n}$$

- Langlois and Stehlé (2015) proved that solving MLWE on *average* is at least as hard as *quantumly* solving SIVP_γ for module lattices *in the worst case.*
- However, as with Regev's worst-case to average-case reduction for LWE, the reduction is *highly non-tight* (and also a quantum reduction).
  - For a concrete analysis of the Langlois-Stehlé reduction for MLWE (and also the Lyubashevsky-Peikert-Regev reduction for Ring-LWE) see: "Concrete analysis of approximate Ideal-SIVP to Decision Ring-LWE reduction" by Koblitz, Samajder, Sarkar and Singha, https://eprint.iacr.org/2022/275.

MLWE versus Ring-LWE

- A primary advantage of MLWE over Ring-LWE is that parameters q and n can be fixed for MLWE, and then ℓ can be changed for different security levels.
- For example, Dilithium fixes $q = 8380417$ and $n = 256$, and $(k, \ell) \in \{(4,4), (6,5), (8,7)\}$.
  - So, one can optimize arithmetic in the polynomial ring $R_q = \mathbb{Z}_{8380417}[x]/(x^{256} + 1)$.
  - Dilithium is "closer" to Ring-LWE than to LWE.

Kyber-PKE: Key generation

Key generation: Alice does:

1. Select $s \in_R S_{\eta_1}^k$.
2. Select $A \in_R R_q^{k \times k}$ and $e \in_R S_{\eta_1}^k$.
3. Compute $b = As + e$.
4. Alice's **public key** is (A, b); her **private key** is s.

- $q = 3329, \quad n = 256.$
- $R_q = \mathbb{Z}_{3329}[x]/(x^{256} + 1).$
- $k \in \{2,3,4\}.$
- $(\eta_1, \eta_2) \in \{(3,2), (2,2), (2,2)\}.$

- Computing s from (A, b) is an instance of **ss-MLWE**.
- Determining any information about s from (A, b) is an instance of **ss-DMLWE**.

Kyber-PKE: Encryption and Decryption

Encryption: To encrypt a message $m \in \{0,1\}^{256}$ for Alice, Bob does:

1. Obtain an authentic copy of Alice's encryption key (A, b).
2. Select $r \in_R S_{\eta_1}^k$, $z \in_R S_{\eta_2}^k$ and $z' \in_R S_{\eta_2}$.
3. Compute $c_1 = A^T r + z$ and $c_2 = b^T r + z' + \lceil q/2 \rfloor m$.
4. Output $c = (c_1, c_2)$.

<u>**Note**</u>: $c \in R_q^k \times R_q$.

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

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

Security:
Kyber-PKE is indistinguishable against chosen-plaintext attack assuming the hardness of short-secret Decisional Module-LWE.

Security

- No attacks (either theoretical or practical) are known on Module-SIS or Module-LWE that are any faster than the fastest attacks known on SIS and LWE.
- In other words, no attacks are known on Module-SIS or Module-LWE that exploit the structure in the matrix A.
- The fastest attacks known on SIS and LWE (see Lecture 5) are used to select MSIS and MLWE parameters in order to attain a desired security level.
  - See the "Bochum challenges": https://bochum-challeng.es