Hardness and advantages of Module-SIS and Module-LWE

Adeline Roux-Langlois

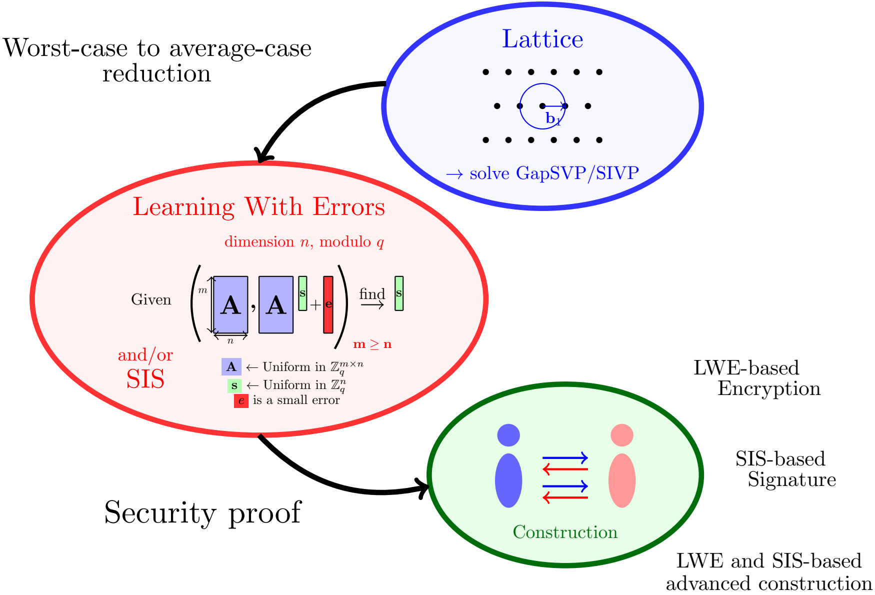
EMSEC: Univ Rennes, CNRS, IRISA

April 24, 2018

Introduction

- **Lattice-based cryptography: why using module lattices?**
- Definition of Module SIS and LWE
- Hardness results on Module SIS and LWE
- Conclusion and open problems

Lattice-based cryptography



Worst-case to average-case reduction

Lattice

$\mathbf{b}_1$

→ solve GapSVP/SIVP

Learning With Errors

dimension n, modulo q

Given $\left(\mathbf{A}, \mathbf{A}\mathbf{s} + \mathbf{e} \right) \xrightarrow{\text{find}} \mathbf{s}$

m n

$\mathbf{m \geq n}$

$\mathbf{A}$ ← Uniform in $\mathbb{Z}_q^{m \times n}$

$\mathbf{s}$ ← Uniform in $\mathbb{Z}_q^{n}$

e is a small error

and/or

SIS

Security proof

Construction

LWE-based Encryption

SIS-based Signature

LWE and SIS-based advanced construction

Lattice-based cryptography

From basic to very advanced primitives

- Public key encryption and Signature scheme (practical), [Regev 05, Gentry, Peikert and Vaikuntanathan 08, Lyubashevsky 12 ...];
- Identity/Attribute-based encryption, [GPV 08 Gorbunov, Vaikuntanathan and Wee 13 ...];
- Fully homomorphic encryption, [Gentry 09, BV 11, ...].

Advantages

- (Asymptotically) efficient;
- Security proofs **from the hardness of lattice problems**;
- Likely to resist attacks from quantum computers.

NIST competition

From 2017 to 2024, NIST competition to find standard on post-quantum cryptography

Total: 69 accepted submissions (round 1)

- Signature (5 lattice-based),
- Public key encryption / Key exchange mechanism (21 lattice-based)

Other candidates: 17 code-based PKE/KEM, 7 multivariate signatures, 3 hash-based signatures, 7 from ”other” assumptions (isogenies, PQ RSA ...) and 4 attacked + 5 withdrawn.

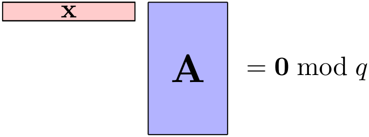
⇒ **lattice-based constructions seem to be serious candidates**

(Assumptions: NTRU, SIS/LWE/LWR, Ring/Module-SIS/LWE/LWR, MP-LWE)

Foundamental problems to build cryptography

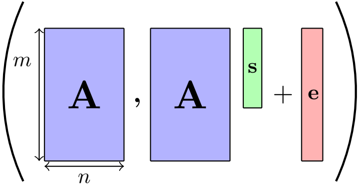
Parameters: dimension n, $m \geq n$, moduli q.
For $\mathbf{A} \leftarrow U(\mathbb{Z}_q^{m \times n})$:

$\mathbf{SIS}_\beta$



Goal: Given $\mathbf{A} \leftarrow U(\mathbb{Z}_q^{m \times n})$,
find $\mathbf{x}$ s.t. $0 < \|\mathbf{x}\| \leq \beta$.

$\mathbf{LWE}_\alpha$

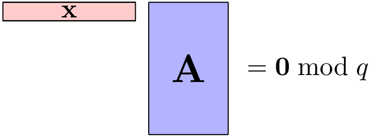
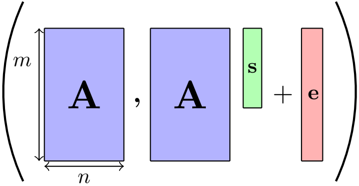


$\mathbf{s} \leftarrow U(\mathbb{Z}_q^n)$,
$\mathbf{e}$ a small error $\approx \alpha q$.

Goal: Given $(\mathbf{A}, \mathbf{A}\mathbf{s} + \mathbf{e})$,
find $\mathbf{s}$.

Foundamental problems to build cryptography

Parameters: dimension n, $m \geq n$, moduli q.
For $\mathbf{A} \leftarrow U(\mathbb{Z}_q^{m \times n})$:

$\mathbf{SIS}_\beta$	$\mathbf{LWE}_\alpha$
	
$= \mathbf{0} \bmod q$	$\mathbf{s} \leftarrow U(\mathbb{Z}_q^n)$, e a small error $\approx \alpha q$.
Find a small vector in $\Lambda_q^\perp(\mathbf{A})$ $= \{\mathbf{x} \in \mathbb{Z}^m \mid \mathbf{x}^T \mathbf{A} = 0 \bmod q\}$	Solve BDD in $\Lambda_q(\mathbf{A})$ $= \{\mathbf{y} \in \mathbb{Z}^m : \mathbf{y} = \mathbf{A}\mathbf{s} \bmod q$ for some $\mathbf{s} \in \mathbb{Z}^n\}$

Hardness results

Worst-case to average-case reductions from lattice problems

- Hardness of the SIS problem [Ajtai 96, MR 04, GPV 08, ...]
- Hardness of the LWE problem [Regev 05, Peikert 09, B**L**PRS 13...]

Also in [B**L**PRS 13]

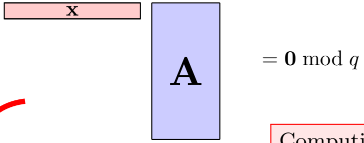
- **Shrinking modulus / Expanding dimension**:
  A reduction from $\mathrm{LWE}_{q^k}^{n}$ to LWE_{q}^{nk}.
- **Expanding modulus / Shrinking dimension**:
  A reduction from LWE_{q}^{n} to $\mathrm{LWE}_{q^k}^{n/k}$.

$\Rightarrow$ The hardness of LWE_q^n is a function of $n \log q$.

Lattice-based signature scheme

Trapdoor for SIS

- TrapGen $\rightsquigarrow$ $(\mathbf{A}, \mathbf{T_A})$ such that $\mathbf{T_A}$ allows to find short $\mathbf{x}$('s)



With $\mathbf{T_A}$, we can solve SIS.

Computing $\mathbf{T_A}$ *given* $\mathbf{A}$ is hard,
Constructing $\mathbf{A}$ *and* $\mathbf{T_A}$ is easy.

- $\mathbf{T_A}$ is a short basis of $\Lambda_q^\perp(\mathbf{A}) = \{\mathbf{x} \in \mathbb{Z}^m | \mathbf{x}^T\mathbf{A} = 0 \bmod q\}$
- In a public key scheme:
  - public key: $\mathbf{A}$
  - secret key: $\mathbf{T_A}$

Lattice-based signature scheme

Signature scheme

- Key generation:
  - $pk = \mathbf{A}, (\mathbf{A}_i)_i$
  - $sk = \mathbf{T_A}$

- To sign a message M:
  - use $\mathbf{T_A}$ to solve SIS: find small $\mathbf{x}$ such that $\mathbf{x}^T \mathbf{A}_M = \mathbf{0} \bmod q$.

- To verify a signature $\mathbf{x}$ given M:
  - check $\mathbf{x}^T \mathbf{A}_M = \mathbf{0} \bmod q$ and $\mathbf{x}$ small

where:

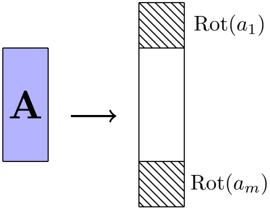
- $\mathbf{A}_M = \left[\dfrac{\mathbf{A}}{\mathbf{A}_0 + \sum_i M_i \mathbf{A}_i} \right]$ in [Boyen 10] for example,
- Knowing a trapdoor for $\mathbf{A} \Rightarrow$ knowing a trapdoor for $\mathbf{A}_M$,
- Several known constructions [Boyen 10, CHKP 10 ..]

From SIS/LWE to structured variants

- **Problem:** constructions based on SIS/LWE enjoy a nice guaranty of security but are too costly in practice.

→ replace $\mathbb{Z}^n$ by a Ring, for example $R = \mathbb{Z}[x]/\langle x^n + 1\rangle$ $(n = 2^k)$.

- Ring variants since 2006:



- Structured $\mathbf{A} \in \mathbb{Z}_q^{m\cdot n\times n}$ represented by $m \cdot n$ elements,
- Product with matrix/vector more efficient,
- Hardness of Ring-SIS, [Lyubashevsky and Micciancio 06] and [Peikert and Rosen 06]
- Hardness of Ring-LWE [Lyubashevsky, Peikert and Regev 10].

Ring-SIS based signature scheme [BFRS 18]

Underlying to [ABB10]

- $\texttt{KeyGen}(\lambda) \to (\text{vk},\text{sk})$
  - choose uniform $\mathbf{a}' \in R_q^{m-2}$
  - sk= $\mathbf{T} \in R^{(m-2)\times 2}$ gaussian
  - pk= $\mathbf{a} = \left(\mathbf{a}'^T | -\mathbf{a}'^T\mathbf{T}\right)^T$

Discrete Gaussian ⇒ short elements in R

For M: $\mathbf{a}_M = \left(\mathbf{a}'^T | H(M)\mathbf{g} - \mathbf{a}'^T\mathbf{T}\right)^T$

MP12 Trapdoors:
– $\mathbf{a}$ looks uniform,
– $\mathbf{T}$ trapdoor (allows to solve Ring-SIS)

$\mathbf{g}$ gadget vector
$H : \{0,1\}^n \to R_q$

- $\texttt{Sign}(\mathbf{a}, \mathbf{T}, M) \to \mathbf{x}$
  - Using $\mathbf{T}$, find small $\mathbf{x} \in R_q^m$ with $\mathbf{x}^T\mathbf{a}_M = 0$,
- $\texttt{Verify}(\mathbf{a}, \mathbf{x}, M) \to \{0,1\}$
  - Accept iff $\mathbf{x}^T\mathbf{a}_M = 0 \bmod qR$ and $\|\mathbf{x}\|$ small.

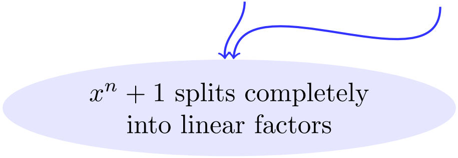
Implementing such a scheme

Lot of conditions on parameters: hardness of Ring-SIS, correctness ...
How to be efficient ?

- Preimage sampling [MP 12, GM 18],
- Fast multiplication of ring elements in $R_q = \mathbb{Z}_q / \langle x^n + 1 \rangle$

For example: use the NFLlib library [Aguilar et al. 16]

- Two important conditions: $n = 2^k$ and $q = 1 \bmod 2n$



$x^n + 1$ splits completely into linear factors

$\Rightarrow$ 3 main constraints on $q = \prod q_i$ described to use the NTT

Example of parameters

Table: Parameters set for the signature scheme

n	$\log q$	σ	R-LWE$_\sigma$	δ	R-SIS	λ
512	30	4.2	2^{64}	1.011380	2^{74}	60
1024	24	5.8	2^{378}	1.008012	2^{156}	140
1024	30	6.3	2^{246}	1.007348	2^{184}	170

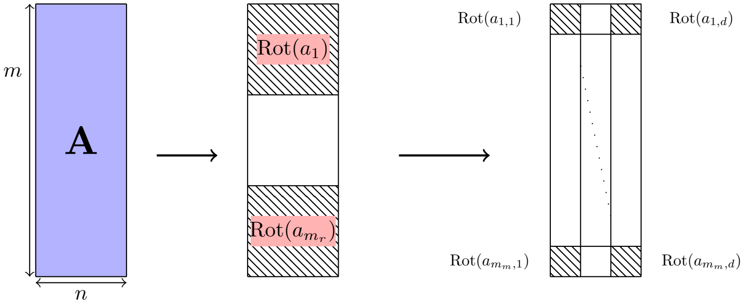
$\rightarrow$ Gap in security because of the constraints on the parameter.

Module variants $\Rightarrow$ tradeoff between security and efficiency

- Hardness of Module SIS and LWE [LS15,AD17]
- Dilithium & Kyber - Crystals NIST submissions [Avanzi et al.]

- Lattice-based cryptography: why using module lattices?
- **Definition of Module SIS and LWE**
- Hardness results on Module variants
- Conclusion and open problems

Module variants



$m_r = m/n$ blocks
of size n

$m_m \times d$ blocks
of size $n_d = n/d$

$\mathbf{a}_i \in \mathbb{Z}_q^n$

$(\mathbf{a}_i, \langle \mathbf{a}_i, \mathbf{s} \rangle + e_i)$

$\mathbf{s} \in \mathbb{Z}_q^n, e_i \in \mathbb{Z}$

$R = \mathbb{Z}[x]/\langle x^n + 1 \rangle$

$a_i \in R_q$

$(a_i, a_i \cdot s + e_i)$

$s \in R_q, e_i \in R$

$R = \mathbb{Z}[x]/\langle x^{n_d} + 1 \rangle$

$\mathbf{a}_i \in (R_q)^d$

$(\mathbf{a}_i, \langle \mathbf{a}_i, \mathbf{s} \rangle + e_i)$

$\mathbf{s} \in (R_q)^d, e_i \in R$

Module SIS and LWE

For example in: $R = \mathbb{Z}[x]/\langle x^n + 1\rangle$ and $R_q = R/qR$.

Module-SIS$_{q,m,\beta}$

Given $\mathbf{a}_1, \ldots, \mathbf{a}_m \in R_q^d$ independent and uniform, find $z_1, \ldots, z_m \in R$ such that $\sum_{i=1}^m \mathbf{a}_i \cdot z_i = 0 \bmod q$ and $0 < \|\mathbf{z}\| \leq \beta$.

Let $\alpha > 0$ and $\mathbf{s} \in (R_q)^d$, the distribution $A_{\mathbf{s},\nu_\alpha}^{(M)}$ is:

- $\mathbf{a} \in (R_q)^d$ uniform,
- e sampled from $\mathcal{D}_\alpha$,

Outputs: $\left(\mathbf{a}, \frac{1}{q}\langle \mathbf{a}, \mathbf{s}\rangle + e\right)$.

Module-LWE$_{q,\nu_\alpha}$

let $\mathbf{s} \in (R_q)^d$ uniform, distinguish between an arbitrary number of samples from $A_{\mathbf{s},D_\alpha}^{(M)}$, or the same number from $U((R_q)^d \times \mathbb{T}_R)$.

$$A_{\mathbf{s},D_\alpha}^{(M)} \approx_c U((R_q)^d \times \mathbb{T}_R).$$

From Ring-SIS/LWE to Module-SIS/LWE

SIS

- Ring-SIS-instance: $a_1, \ldots, a_m \in R_q$,
- For $2 \leq i \leq d$, $1 \leq j \leq m$: sample $a_{i,j}$, $\mathbf{a}_j = (a_j, a_{2,j}, \ldots, a_{d,j})$,
- Module-SIS: gives small $\mathbf{z}$ such that $\sum_j \mathbf{a}_j \cdot z_j = 0$
  $\Rightarrow \sum_j a_j \cdot z_j = 0$

LWE

- Ring-LWE instance: $(a, b = a \cdot s + e)$,
- Sample $a_2, \ldots, a_d$ and $s_2, \ldots, s_d$,
- New sample: $(\mathbf{a} = (a, a_2, \ldots, a_d), b + \sum_{i=2}^{d} a_i \cdot s_i)$.
  - $\mathbf{s} = (s, s_1, \ldots, s_d) \in (R_q)^d$,
  - then $b + \sum_{i=2}^{d} a_i \cdot s_i = \langle \mathbf{a}, \mathbf{s} \rangle + e \Rightarrow$ Module-LWE instance

Module-SIS/LWE$_{n,d,q}$ at least as hard as Ring-SIS/LWE$_{n,q}$
$\Rightarrow$ Module-SIS/LWE$_{n,d,q}$ at least as hard as Ideal-SIVP$_n$

- Lattice-based cryptography: why using module lattices?
- Definition of Module SIS and LWE
- **Hardness results on Module variants**
- Conclusion and open problems

Ideal and Module SIVP

Shortest Independent Vector problem (SIVP_γ)

Input: a basis $\mathbf{B}$ of a lattice,

Output: find $n = \dim(\mathcal{L}(\mathbf{B}))$ linearly independent $\mathbf{s}_i$ such that $\max_i \|\mathbf{s}_i\| \leq \gamma \cdot \lambda_n(\mathcal{L}(\mathbf{B}))$.

Ideal-SIVP problem restricted to ideal lattices.

Module-SIVP problem restricted to module lattices.

Let K be a number field, R its ring of integers,

- Let σ be an embedding from K to $\mathbb{R}^n$, $\sigma(I)$ is an ideal lattice where I is an ideal of R,
- Let $(\sigma, \dots, \sigma)$ be an embedding from K^d to $\mathbb{R}^{n_d \cdot d}$, $\sigma(M)$ is a module lattice where $M \subseteq K^d$ is a module of R.
  → M can be represented by a pseudo basis: $M = \sum_k I_k \cdot b_k$, where (I_k) non zero ideals of R, (b_k) linearly indep. vectors of R^d.

Hardness Results

Langlois Stehlé 2015

- Reduction from Module-SIVP to Module-SIS.
- Quantum reduction from Module-SIVP to Module-LWE.
- Reduction from search to decision Module-LWE.

Parameters:

Module-SIVP → Module-LWE [LS 15]	SIVP → LWE [Regev 05]	Ideal-SIVP → Ring-LWE [LPR 10]
d , n_d	$d = n$ et $n_d = 1$	$d = 1$ et $n_d = n$
$\gamma \gtrsim \sqrt{n_d} \cdot d/\alpha$	$\gamma \gtrsim n/\alpha$	$\gamma \gtrsim \sqrt{n}/\alpha$
arbitrary q	q prime	q prime $q = 1 \bmod 2n$
$q \gtrsim \sqrt{d}/\alpha$	$q \gtrsim \sqrt{n}/\alpha$	$q \gtrsim 1/\alpha$

Hardness Results

Langlois Stehlé 2015

- Reduction from Module-SIVP to Module-SIS.
- Quantum reduction from Module-SIVP to Module-LWE.
- Reduction from search to decision Module-LWE.

Converse reductions

- For $R = \mathbb{Z}[x]/\langle x^n + 1\rangle$ with $n = 2^k$,
- Reduction from Module-SIS to Module-SIVP,
- Reduction from Module-LWE to Module-SIVP.

Hardness Results

Albrecht Deo 2017

- R is a power-of-two cyclotomic ring: the same for both problems,
- Reduction

from Module-LWE | in rank d with modulus q,

to Module-LWE | in rank d/k with modulus q^k.

- If $k = d \Rightarrow$ Reduction from (search) Module-LWE with rank d and modulus q to (search) Ring-LWE with modulus q^d.

→ with error rate expansion: from α to $\alpha \cdot n^2\sqrt{d}$.

Hardness results

Consequences [LS15] + [AD17]

$$\text{Module-SIVP}_\gamma \longleftrightarrow \text{Module-LWE}_{d,q,\alpha} \longrightarrow \text{Ring-LWE}_{q^d,\alpha'}$$

- $\alpha' = \alpha \cdot n^2\sqrt{d}$,
- $\gamma = O(\frac{n^{5/2} \cdot d^{3/2}}{\alpha'})$

Interpretation

- [BLPRS 13]: Ring-LWE in dimension n with exponential modulus is hard under hardness of general lattices problems.
- [LS15] + [AD17]: Ring-LWE in dimension n with exponential modulus is hard under hardness of module lattices problems.
- Cryptanalysis observation: Ring-LWE becomes harder when q increases.

- Lattice-based cryptography: why using module lattices?
- Definition of Module SIS and LWE
- Hardness results on Module variants
- **Conclusion and open problems**

Open problems

Conclusion

- Module problems hard and interesting to build cryptographic constructions, serious NIST submissions:
  - Dilithium (signature - MSIS/MLWE): $n = 256$, $m, d = 3, 4$.
  - Kyber (KEM - MLWE)
  - Saber / 3-bears (KEM - MLWR)

Open problems

- Hardness of Module Learning With Rounding
  - Problem used in several NIST submission,
- A better understanding of Ring-LWE / Module-LWE
- A better understanding of SIVP on module lattices