(Introduction to) Relaxed Assumptions In Lattice-based Cryptography

CNRS, GREYC, Caen

Séminaire Pampers, IRMAR Rennes

October 15, 2026

GREYC
Laboratoire de recherche en sciences du numérique

cnrs

RÉGION NORMANDIE

[Logos] https://www.flaticon.com

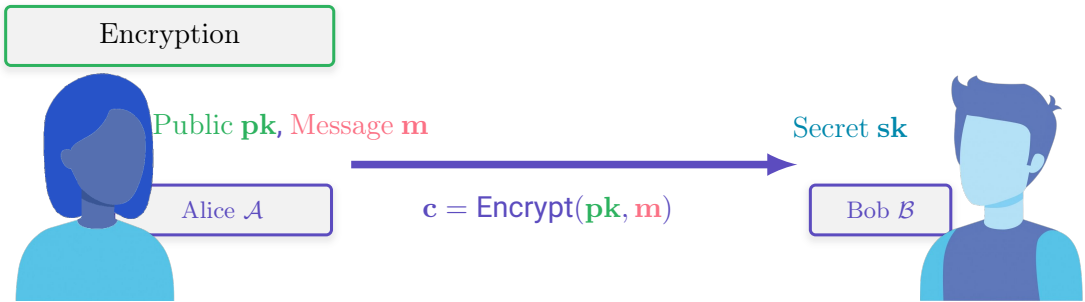
Public key cryptography

Security of cryptographic schemes

Lattices and fundamental problems

So what is the problem?

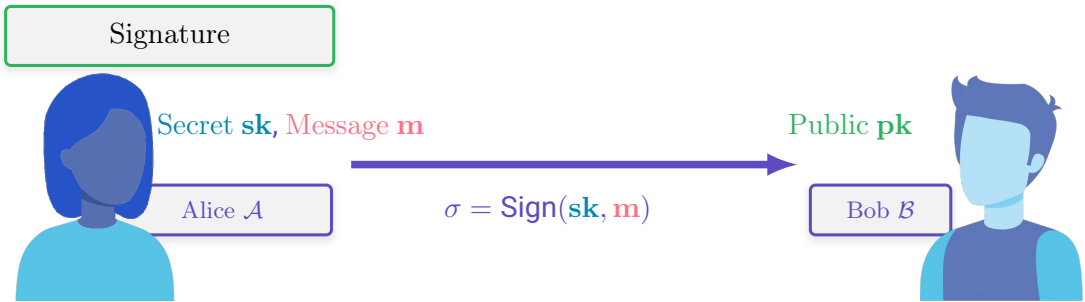
Public key cryptography



Encryption

$\mathcal{A}$ transmits confidential message to $\mathcal{B}$.

Public key cryptography



Encryption

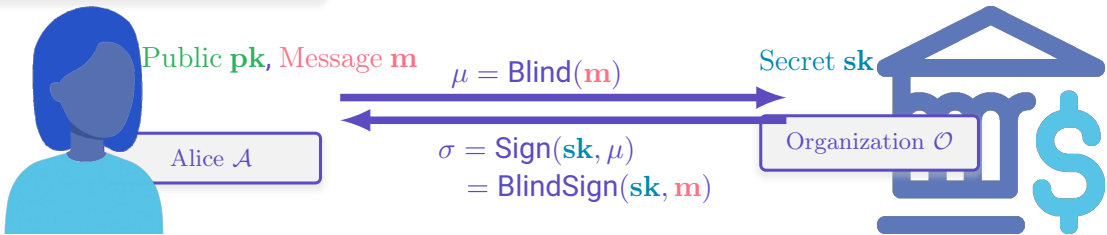
$\mathcal{A}$ transmits confidential message to $\mathcal{B}$.

Signature

Assert that the message is written by $\mathcal{A}$.

An example of advanced construction

Blind Signature



Security

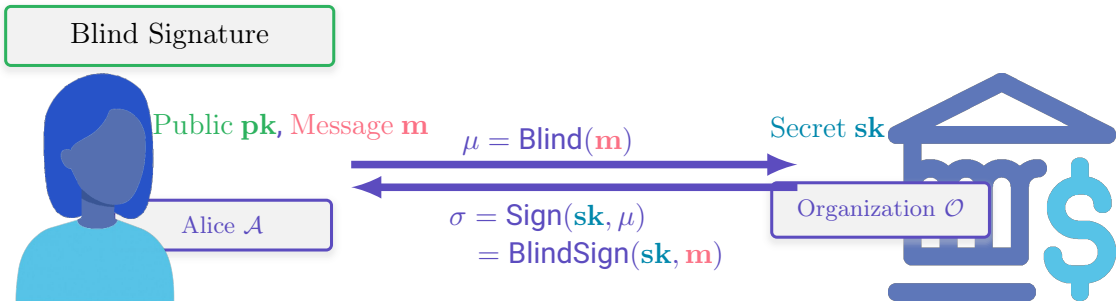
$\mathcal{B}$ does not gain information about $\mathbf{m}$ and $\mathcal{A}$.

$\mathcal{A}$ will never be able to sign his message.

Applications

eCash, anonymous token, credentials.

An example of advanced construction



Much more advanced constructions exist:

- Advanced Signatures: Group Signature, Threshold Signature, ...
- Advanced Encryptions: FHE, ABE, (H)IBE, ...
- Independent primitives: Commitment schemes and derivated, ...

Public key cryptography

Security of cryptographic schemes

Lattices and fundamental problems

So what is the problem?

Security of cryptographic schemes

Reductionist security

Successfully **attacking a system** is as hard as **solving a problem**.

Security of cryptographic schemes

Reductionist security

Successfully **attacking a system** is as hard as **solving a problem**.

We need a mathematical structure with:

Security of cryptographic schemes

Reductionist security

Successfully **attacking a system** is as hard as **solving a problem**.

We need a mathematical structure with:

Hard problems	Efficient	Versatile

Security of cryptographic schemes

Reductionist security

Successfully **attacking a system** is as hard as **solving a problem**.

We need a mathematical structure with:

Hard problems	Efficient	Versatile

A solution : Lattices

Public key cryptography

Security of cryptographic schemes

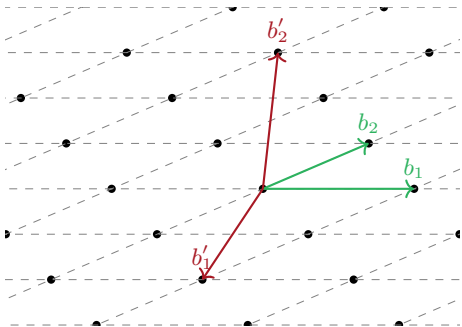
Lattices and fundamental problems

So what is the problem?

Lattices and fundamental problems

Lattice

$\Lambda(\mathbf{B}) = \{\sum_{i=1}^{n} x_i \mathbf{b}_i, x_i \in \mathbb{Z}\}$, where $\mathbf{B} = (\mathbf{b}_i)_{1 \leq i \leq n}$ contains linearly independent vectors, basis of $\Lambda(\mathbf{B})$. The basis is not unique.

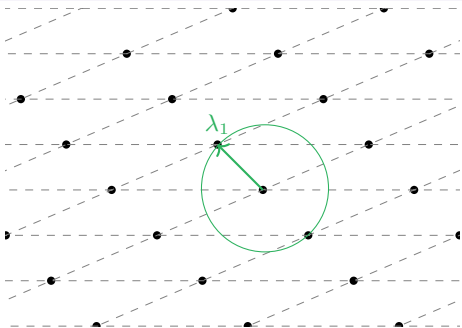


Lattices and fundamental problems

Shortest Vector Problem (SVP)

Input: A lattice $\Lambda(\mathbf{B})$ of dimension n.

Output: Find the shortest (non-zero) vector $\mathbf{x} \in \Lambda(\mathbf{B})$(denote $\lambda_1(\Lambda(\mathbf{B})) := \|\mathbf{x}\|$).

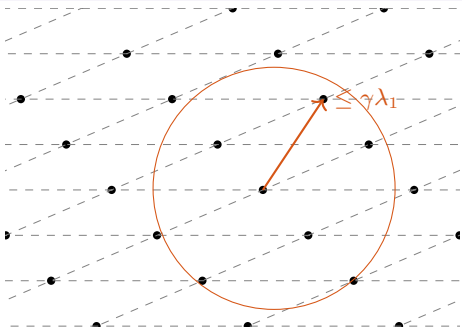


Lattices and fundamental problems

Approximate Shortest Vector Problem (ApproxSVP$_\gamma$)

Input: A lattice $\Lambda(\mathbf{B})$ of dimension n.

Output: Find a non-zero vector $\mathbf{x} \in \Lambda(\mathbf{B})$ such that $\|\mathbf{x}\| \leq \gamma\lambda_1(\Lambda(\mathbf{B}))$.

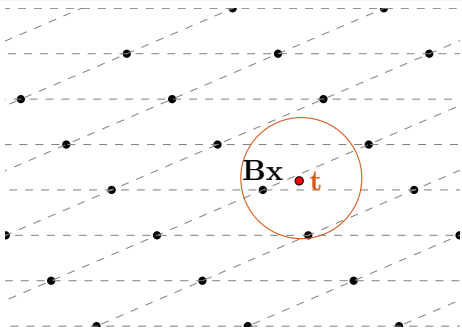


Lattices and fundamental problems

Approximate Closest Vector Problem (ApproxCVP$_\gamma$)

Input: A lattice $\Lambda(\mathbf{B})$ of dimension n, and a target $\mathbf{t} \in \mathbb{R}^m$

Output: Find the (approximate) closest point in $\Lambda(\mathbf{B})$ of $\mathbf{t}$.



Standard lattice assumptions

Learning With Errors (LWE) by [Reg05; Reg09]:

One of the problem that gave rise to lattice-based cryptography

- Solve the linear equation system with some error/noise:

$$
\begin{aligned}
s_1 + 14s_2 + 20s_3 + 15s_4 + 15s_5 &\approx 9 \pmod{29} \\
14s_1 + 5s_2 + 4s_3 + 15s_4 + 15s_5 &\approx 20 \pmod{29} \\
20s_1 + 5s_2 + 1s_3 + 21s_4 + 15s_5 &\approx 19 \pmod{29} \\
19s_1 + 20s_2 + 1s_3 + 21s_4 + 15s_5 &\approx 13 \pmod{29} \\
5s_1 + 21s_2 + 18s_3 + 4s_4 + 15s_5 &\approx 1 \pmod{29} \\
5s_1 + 16s_2 + 5s_3 + 20s_4 + 15s_5 &\approx 12 \pmod{29}
\end{aligned}
$$

Standard lattice assumptions

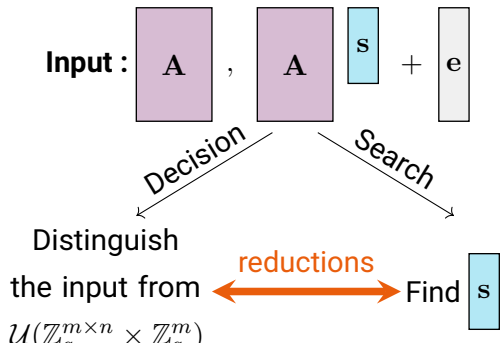
Learning With Errors (LWE) by [Reg05; Reg09]:

Environment: $\mathbb{Z}_q := \mathbb{Z}/q\mathbb{Z}$ for a prime q, $m \geq n$,

Public parameters: $\mathbf{A} \leftarrow \mathcal{U}(\mathbb{Z}_q^{m \times n})$ ($m \times n$)

Private information: $\mathbf{s} \leftarrow \mathcal{U}(\mathbb{Z}_q^n)$ (n)

$\mathbf{e} \leftarrow \mathcal{D}^m_{\mathbb{Z},\alpha q}$ (m)

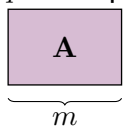


Standard lattice assumptions

Short Integer Solution (SIS) by [Ajt96]:

Environment: $\mathbb{Z}_q := \mathbb{Z}/q\mathbb{Z}$ for a prime q, $m \geq n$,

Public parameters: $\mathbf{A} \xleftarrow{\$} \mathcal{U}(\mathbb{Z}_q^{n \times m})$



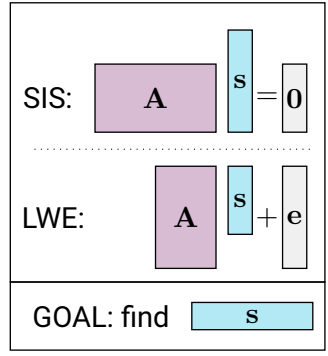
Input : $\mathbf{A}$

Find : $\mathbf{s} \in \mathbb{Z}_q^m$ of small norm $\|\mathbf{s}\| \leq \beta$

such that: $\mathbf{A}\,\mathbf{s} = \mathbf{0}$

Standard lattice assumptions

Reduction wtih fundamental lattice problems:



SIS can be seen as average ApproxSVP over

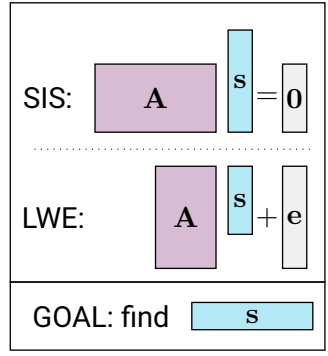
$$\Lambda_q^{\perp}(\mathbf{A}) = \{\mathbf{x} \in \mathbb{Z}^m : \mathbf{A}\mathbf{x} = \mathbf{0} \mod q\}$$

LWE can be seen as average ApproxCVP over

$$\Lambda_q(\mathbf{A}) = \{\mathbf{A}\mathbf{s} \mod q \text{ for } \mathbf{s} \in \mathbb{Z}^n\}$$

Standard lattice assumptions

Reduction wtih fundamental lattice problems:



SIS can be seen as average ApproxSVP over

$$\Lambda_q^{\perp}(\mathbf{A}) = \{\mathbf{x} \in \mathbb{Z}^m : \mathbf{A}\mathbf{x} = \mathbf{0} \mod q\}$$

LWE can be seen as average ApproxCVP over

$$\Lambda_q(\mathbf{A}) = \{\mathbf{A}\mathbf{s} \mod q \text{ for } \mathbf{s} \in \mathbb{Z}^n\}$$

We do have fondamental requirements for cryptography.

Public key cryptography

Security of cryptographic schemes

Lattices and fundamental problems

So what is the problem?

Motivation

It is possible to have lattice-based cryptography.

Reduction to hard lattice problems

Versatility of the constructions

Motivation

It is possible to have lattice-based cryptography.

Reduction to hard lattice problems

Versatility of the constructions

But the **standard assumptions** are **not efficient** enough to handle **practical use**:

Designers conjectures relaxed versions of the standard assumptions.

Motivation

It is possible to have lattice-based cryptography.

Reduction to hard lattice problems

Versatility of the constructions

But the **standard assumptions** are **not efficient** enough to handle **practical use**:

Designers conjectures relaxed versions of the standard assumptions.

Recently, there were **dozens of unproven variants**. We were facing problems:

No classification

No links between variants

More or less cryptanalysis

Lattice Assumption Zoo

Scientific collaboration initiated by **Jan Niklas Siemer** to classify the **lattice-based assumptions** and their **relations**.

Lattice Assumption Zoo



[Siemer26] Lattice Assumption Zoo; https://latticeassumptionzoo.org/

Relaxed lattice-based assumptions

Instance-based relaxations

LWE/SIS over **specific instances**.

Relaxed lattice-based assumptions

Instance-based relaxations

LWE/SIS over **specific instances**.

- (e.g. : structuration),
- **Practical** primitives,
- **Efficient advanced constructions**.

Relaxed lattice-based assumptions

Instance-based relaxations

LWE/SIS over **specific instances**.

- (e.g. : structuration),
- **Practical** primitives,
- **Efficient advanced constructions**.

Hint-based relaxations

LWE/SIS + **additional information**. i.e. we know a **useful information** about the problem.

Relaxed lattice-based assumptions

Instance-based relaxations

LWE/SIS over **specific instances**.

- (e.g. : structuration),
- **Practical** primitives,
- **Efficient advanced constructions**.

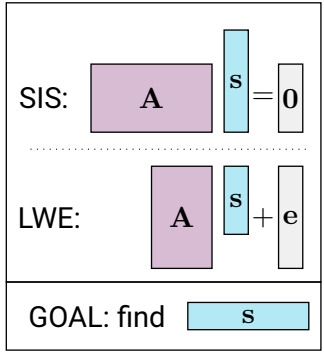
Hint-based relaxations

LWE/SIS + **additional information**. i.e. we know a **useful information** about the problem.

- **Efficient advanced constructions**,
- **Non-black box cryptography** (include side-channel information),
- **Prioritisation** of side-channel protection (efficiency gain).

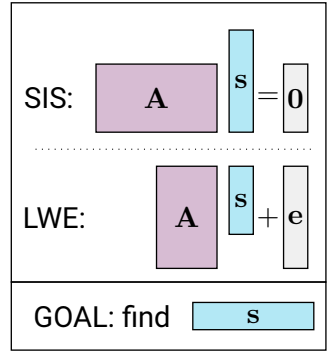
Hint-based lattice relaxations

1. Internal information: Hints are information about the secret



Hint-based lattice relaxations

1. Internal information: Hints are information about the secret



One example: Hint-LWE [Kim+23]

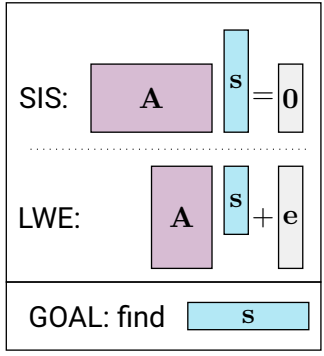
LWE + $\mathbf{H_s}$ $\mathbf{H_e}$ $\mathbf{s}$ $\mathbf{e}$ $+ \mathbf{e}'$ for $\mathbf{e}' \leftarrow \mathcal{D}_{\sigma_{\mathbf{e}'}}$

Hint-LWE $\iff$ LWE when $\mathbf{s}, \mathbf{e}, \mathbf{e}'$ follow Discrete gaussians $\mathcal{D}_{\sigma_i}$.

Allows to transmit linear noisy information [HSS24; ENP24; Ogi25; Dod+25; **D**R25]

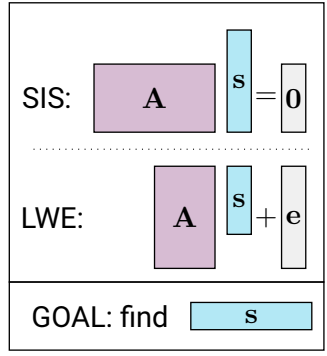
Hint-based lattice relaxations

2. Solutions: Hints are solutions of the problem



Hint-based lattice relaxations

2. Solutions: Hints are solutions of the problem



One example: k-SIS [BF11]

Input: $\mathbf{A}$ and k SIS distincts solutions $\mathbf{s}_i$.

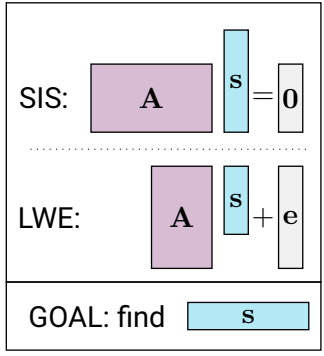
GOAL: Find another solution not in $\mathbb{Q}$-span$(\mathbf{s}_i)$.

k-SIS is reduced to SIS

- Ensure the unforgeability security of advanced signatures such as blind signatures [Bou+20; BF11; Alb+22; Lin+14],
- Analogous to One-More assumptions: [Agr+22; FNR25; ZT25; EKT24].

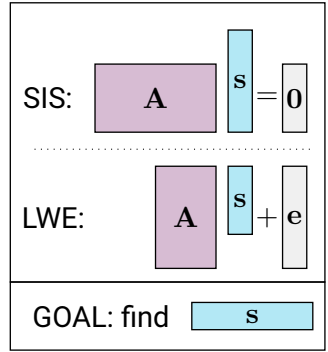
Hint-based lattice relaxations

3. Extra information: Hints are information about the overall problem



Hint-based lattice relaxations

3. Extra information: Hints are information about the overall problem



One example: ℓ-Succinct LWE [Wee24]

Input: $\mathbf{A}$, $\mathbf{W}$, and $\mathbf{T}$ which is a good basis of:

$$\begin{bmatrix} \mathbf{A} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{A} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{A} \end{bmatrix} \mathbf{W}$$

GOAL: Find an LWE solution.

Not reduced from standard problems

- Used when constructing advanced schemes (iO, ...) [Wee25; WW25; FMN24].

Conclusion

Lattice-based advanced primitives do **not have practical security** (yet).

The natural idea is to based the **security** of constructions over **relaxed assumptions**.

Instance-based assumption

Hint-based assumption

Conclusion

Lattice-based advanced primitives do **not have practical security** (yet).

The natural idea is to based the **security** of constructions over **relaxed assumptions**.

Instance-based assumption

Hint-based assumption

There are different class of **hint-based assumptions** with different usecases:

Internal information

Solutions

Extra information

Conclusion

Lattice-based advanced primitives do **not have practical security** (yet).

The natural idea is to based the **security** of constructions over **relaxed assumptions**.

Instance-based assumption

Hint-based assumption

What are the open problems in the area?

Cryptanalysis

Reductions

Exploit existing assumptions rather than create new ones

Conclusion

Lattice-based advanced primitives do **not have practical security** (yet).

The natural idea is to based the **security** of constructions over **relaxed assumptions**.

Instance-based assumption

Hint-based assumption

What are the open problems in the area?

Cryptanalysis

Reductions

Exploit existing assumptions rather than create new ones

Thank you for your attention!

References I

Shweta Agrawal et al. “Practical, Round-Optimal Lattice-Based Blind Signatures”. 2022, pp. 39–53. DOI: 10.1145/3548606.3560650.

Miklós Ajtai. “Generating Hard Instances of Lattice Problems (Extended Abstract)”. 1996, pp. 99–108. DOI: 10.1145/237814.237838.

Martin R. Albrecht et al. “Lattice-Based SNARKs: Publicly Verifiable, Preprocessing, and Recursively Composable - (Extended Abstract)”. 2022, pp. 102–132. DOI: 10.1007/978-3-031-15979-4_4.

Dan Boneh and David Mandell Freeman. “Linearly Homomorphic Signatures over Binary Fields and New Tools for Lattice-Based Signatures”. 2011, pp. 1–16. DOI: 10.1007/978-3-642-19379-8_1.

References II

Samuel Bouaziz-Ermann et al. *Lattice-based (Partially) Blind Signature without Restart*. Cryptology ePrint Archive, Report 2020/260. 2020.

Yevgeniy Dodis et al. “Triple Ratchet: A Bandwidth Efficient Hybrid-Secure Signal Protocol”. 2025, pp. 302–331. DOI: 10.1007/978-3-031-91101-9_11.

Antoine Douteau and Adeline Roux-Langlois. “Rejection-Free Framework of Zero-Knowledge Proof Based on Hint-MLWE”. 2025, pp. 119–144. DOI: 10.1007/978-3-032-13301-4_6.

Thomas Espitau, Shuichi Katsumata, and Kaoru Takemure. “Two-Round Threshold Signature from Algebraic One-More Learning with Errors”. 2024, pp. 387–424. DOI: 10.1007/978-3-031-68394-7_13.

References III

Thomas Espitau, Guilhem Niot, and Thomas Prest. “Flood and Submerse: Distributed Key Generation and Robust Threshold Signature from Lattices”. 2024, pp. 425–458. DOI: 10.1007/978-3-031-68394-7_14.

Giacomo Fenzi, Hossein Moghaddas, and Ngoc Khanh Nguyen. “Lattice-Based Polynomial Commitments: Towards Asymptotic and Concrete Efficiency”. 37.3 (July 2024), p. 31. DOI: 10.1007/s00145-024-09511-8.

Sebastian Faller, Guilhem Niot, and Michael Reichle. *Lattice-based Threshold Blind Signatures*. Cryptology ePrint Archive, Paper 2025/1566. 2025.

References IV

Intak Hwang, Jinyeong Seo, and Yongsoo Song. “Concretely Efficient Lattice-Based Polynomial Commitment from Standard Assumptions”. 2024, pp. 414–448. DOI: 10.1007/978-3-031-68403-6_13.

Duhyeong Kim et al. “Toward Practical Lattice-Based Proof of Knowledge from Hint-MLWE”. 2023, pp. 549–580. DOI: 10.1007/978-3-031-38554-4_18.

San Ling et al. “Hardness of k-LWE and Applications in Traitor Tracing”. 2014, pp. 315–334. DOI: 10.1007/978-3-662-44371-2_18.

Adeline Langlois and Damien Stehlé. “Worst-case to average-case reductions for module lattices”. 75.3 (2015), pp. 565–599. DOI: 10.1007/s10623-014-9938-4.

References V

Tabitha Ogilvie. “IND-CPA-D and KR-D Security with Reduced Noise from the HintLWE Problem”. 2025, pp. 263–295. DOI: 10.1007/978-981-95-5122-4_9.

Oded Regev. “On lattices, learning with errors, random linear codes, and cryptography”. 2005, pp. 84–93. DOI: 10.1145/1060590.1060603.

Oded Regev. “On lattices, learning with errors, random linear codes, and cryptography”. *J. ACM* 56.6 (Sept. 2009). ISSN: 0004-5411. DOI: 10.1145/1568318.1568324.

Hoeteck Wee. “Circuit ABE with poly(depth, λ)-Sized Ciphertexts and Keys from Lattices”. 2024, pp. 178–209. DOI: 10.1007/978-3-031-68382-4_6.

References VI

Hoeteck Wee. “Almost Optimal KP and CP-ABE for Circuits from Succinct LWE”. 2025, pp. 34–62. DOI: 10.1007/978-3-031-91131-6_2.

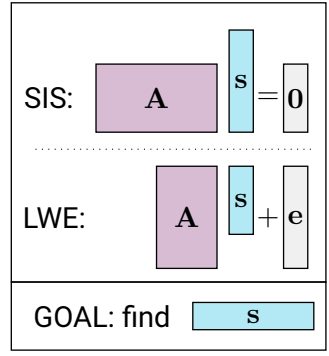
Hoeteck Wee and David J. Wu. “Unbounded Distributed Broadcast Encryption and Registered ABE from Succinct LWE”. 2025, pp. 204–235. DOI: 10.1007/978-3-032-01881-6_7.

Chenzhi Zhu and Stefano Tessaro. “The Algebraic One-More MISIS Problem and Applications to Threshold Signatures”. 2025, pp. 548–581. DOI: 10.1007/978-3-032-01855-7_18.

Structure-based lattice relaxation

We have $\mathbf{A} \leftarrow \mathcal{U}\left(\mathbb{Z}_q^{\text{height} \times \text{width}}\right)$ that lacks of structure.

Consider a structured variant to replace $\mathbb{Z}_q^d$ with $d = 2^k > 0$.

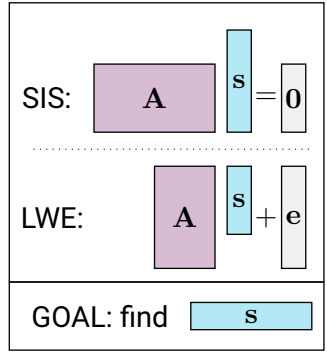


Structure-based lattice relaxation

We have $\mathbf{A} \leftarrow \mathcal{U}\left(\mathbb{Z}_q^{\text{height} \times \text{width}}\right)$ that lacks of structure.

Consider a structured variant to replace $\mathbb{Z}_q^d$ with $d = 2^k > 0$.

How ? Defining $\mathcal{R} := \mathbb{Z}[X]/\langle X^d + 1 \rangle$ such that $\mathbb{Z}^d \cong \mathcal{R}$.



Structure-based lattice relaxation

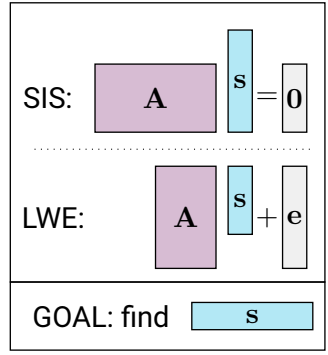
We have $\mathbf{A} \leftarrow \mathcal{U}\left(\mathbb{Z}_q^{\text{height} \times \text{width}}\right)$ that lacks of structure.

Consider a structured variant to replace $\mathbb{Z}_q^d$ with $d = 2^k > 0$.

How ? Defining $\mathcal{R} := \mathbb{Z}[X]/\langle X^d + 1 \rangle$ such that $\mathbb{Z}^d \cong \mathcal{R}$.

Let $a \in \mathcal{R}, a = a_0 + a_1 X + \cdots + a_{d-1} X^{d-1}$,

In $\mathbb{Z}^d$, $\vec{a} = \mathsf{cf}(a) = (a_0, \ldots, a_{d-1})$, $\vec{b} = \mathsf{cf}(b) = (b_0, \ldots, b_{d-1})$.



Structure-based lattice relaxation

We have $\mathbf{A} \leftarrow \mathcal{U}\left(\mathbb{Z}_q^{\mathsf{height}\times\mathsf{width}}\right)$ that lacks of structure.

Consider a structured variant to replace $\mathbb{Z}_q^d$ with $d = 2^k > 0$.

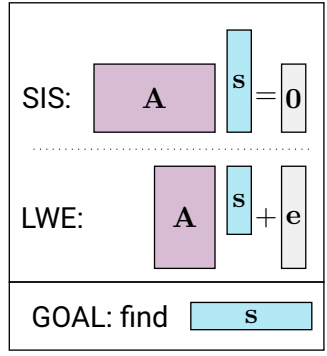
How ? Defining $\mathcal{R} := \mathbb{Z}[X]/\langle X^d + 1\rangle$ such that $\mathbb{Z}^d \cong \mathcal{R}$.

Let $a \in \mathcal{R}, a = a_0 + a_1 X + \cdots + a_{d-1}X^{d-1}$,

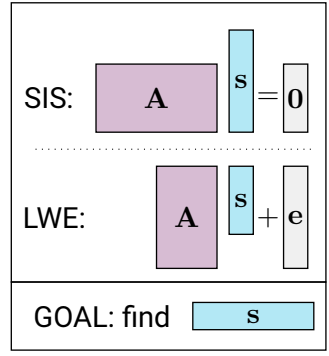
In $\mathbb{Z}^d$, $\vec{a} = \mathsf{cf}(a) = (a_0, \ldots, a_{d-1})$, $\vec{b} = \mathsf{cf}(b) = (b_0, \ldots, b_{d-1})$.

For the sum:

$$\mathsf{cf}(a+b) = \vec{a} + \vec{b}$$



Structure-based lattice relaxation



We have $\mathbf{A} \leftarrow \mathcal{U}\left(\mathbb{Z}_q^{\text{height}\times\text{width}}\right)$ that lacks of structure.

Consider a structured variant to replace $\mathbb{Z}_q^d$ with $d = 2^k > 0$.

How ? Defining $\mathcal{R} := \mathbb{Z}[X]/\langle X^d + 1\rangle$ such that $\mathbb{Z}^d \cong \mathcal{R}$.

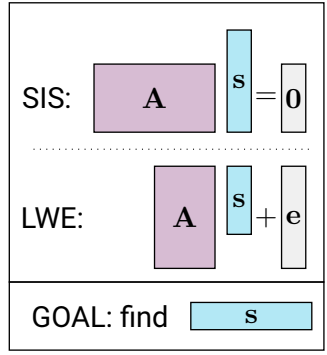
Let $a \in \mathcal{R}, a = a_0 + a_1 X + \cdots + a_{d-1}X^{d-1}$,

In $\mathbb{Z}^d$, $\vec{a} = \mathsf{cf}(a) = (a_0, \ldots, a_{d-1})$, $\vec{b} = \mathsf{cf}(b) = (b_0, \ldots, b_{d-1})$.

For the product:

$$\mathsf{cf}(a \cdot b) = \mathsf{Rot}(a) \cdot \vec{b}^{\top} = \begin{bmatrix} a_0 & -a_{d-1} & \cdots & -a_1 \\ a_1 & a_0 & \cdots & -a_2 \\ \vdots & \vdots & \ddots & \vdots \\ a_{d-1} & a_{d-2} & \cdots & a_0 \end{bmatrix} \cdot \begin{bmatrix} b_0 \\ b_1 \\ \vdots \\ b_{d-1} \end{bmatrix}$$

Structure-based lattice relaxation



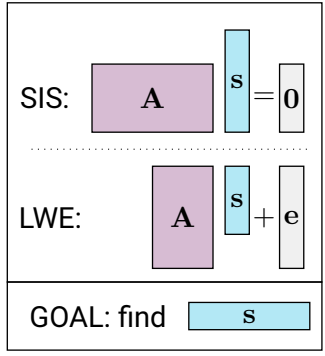
Consider $\mathcal{R} = \mathbb{Z}[X]/\langle X^d + 1\rangle$ and $\mathcal{R}/q\mathcal{R}$ for an integer q.

Module LWE & Module SIS

Consider $\mathbf{A} \leftarrow \mathcal{U}\left(\mathcal{R}_q^{\frac{\text{height}}{d} \times \frac{\text{width}}{d}}\right)$.

- For Module-SIS: $\mathbf{s} \in \mathcal{R}_q^{\frac{\text{height}}{d}}$ with $\mathbf{s} \neq \mathbf{0}$ and $\|\mathbf{s}\| \leq \beta$.
- For Module-LWE: $\mathbf{s} \in \mathcal{R}_q^{\frac{\text{height}}{d}}$ and $\mathbf{e}$ as an element of $\mathcal{R}_q$.

Structure-based lattice relaxation



Consider $\mathcal{R} = \mathbb{Z}[X]/\langle X^d + 1 \rangle$ and $\mathcal{R}/q\mathcal{R}$ for an integer q.

Module LWE & Module SIS

Consider $\mathbf{A} \leftarrow \mathcal{U}\left(\mathcal{R}_q^{\frac{\text{height}}{d} \times \frac{\text{width}}{d}}\right)$.

- For Module-SIS: $\mathbf{s} \in \mathcal{R}_q^{\frac{\text{height}}{d}}$ with $\mathbf{s} \neq \mathbf{0}$ and $\|\mathbf{s}\| \leq \beta$.
- For Module-LWE: $\mathbf{s} \in \mathcal{R}_q^{\frac{\text{height}}{d}}$ and $\mathbf{e}$ as an element of $\mathcal{R}_q$.

- MSIS is reduced to ApproxSVP over Module Lattices.
- MLWE is reduced to ApproxCVP over Module Lattices.

} [LS15]