HARDNESS OF LEARNING WITH PHYSICAL ROUNDING AND NOISE FROM LEARNING WITH ERRORS

Emeline Repel[1] joint work with C. Hoffman[2], A. Roux-Langlois[1] ad F.X. Standaert[2]

[1]Université Caen Normandie, ENSICAEN, CNRS, France - [2]Université Catholique de Louvain, Belgique

GREYC
Electronics and Computer Science Laboratory

Normandie Université

UNICAEN

ENSI CAEN
ÉCOLE PUBLIQUE D'INGÉNIEURS
CENTRE DE RECHERCHE

cnrs

Table of contents

Outline

Introduction to Cryptography

Cryptography = enable listening or modifying messages

- 🔑: Public key - 🔑: Private key

Introduction to Cryptography

Cryptography = enable listening or modifying messages

- Asymmetric Cryptography: occasional exchanges (Private key exchange)

- : Public key - : Private key

Introduction to Cryptography

Cryptography = enable listening or modifying messages

- Asymmetric Cryptography: occasional exchanges (Private key exchange)

- : Public key - : Private key

Introduction to Cryptography

Cryptography = enable listening or modifying messages

- Asymmetric Cryptography: occasional exchanges (Private key exchange)

- Symmetric Cryptography: frequent interactions (daily communication)

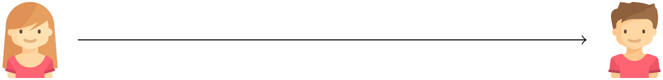
- : Public key - : Private key
- : Shared but Private key

Introduction to Cryptography

Cryptography = enable listening or modifying messages

- Asymmetric Cryptography: occasional exchanges (Private key exchange)

- Symmetric Cryptography: frequent interactions (daily communication)



- : Public key - : Private key
- : Shared but Private key

Introduction to Cryptography

Cryptography = enable listening or modifying messages

- Asymmetric Cryptography: occasional exchanges (Private key exchange)

- Symmetric Cryptography: frequent interactions (daily communication)

- : Public key - : Private key
- : Shared but Private key

Introduction to Cryptography

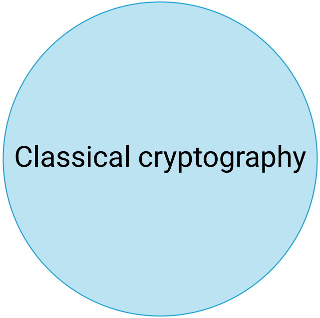
Cryptography = enable listening or modifying messages

- Asymmetric Cryptography: occasional exchanges (Private key exchange)

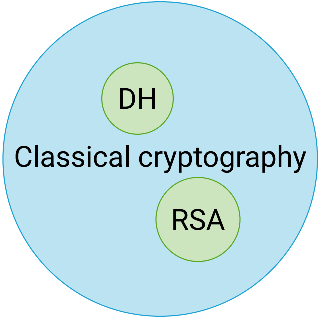
- Symmetric Cryptography: frequent interactions (daily communication)

- : Public key - : Private key
- : Shared but Private key

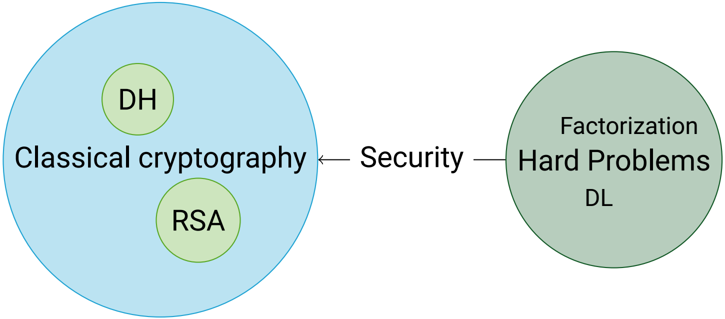
Security and Post-Quantum Cryptography



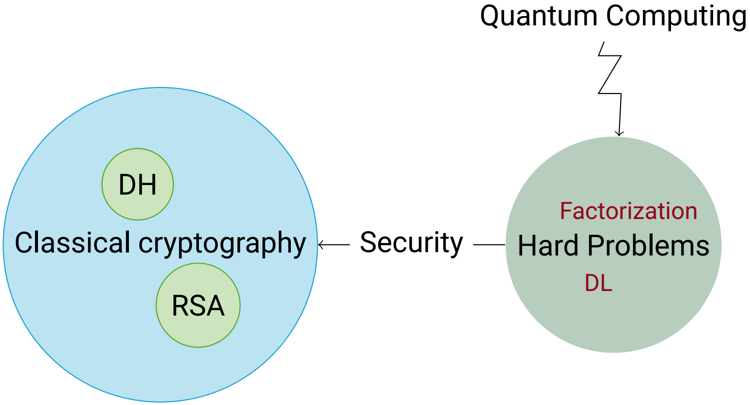
Security and Post-Quantum Cryptography



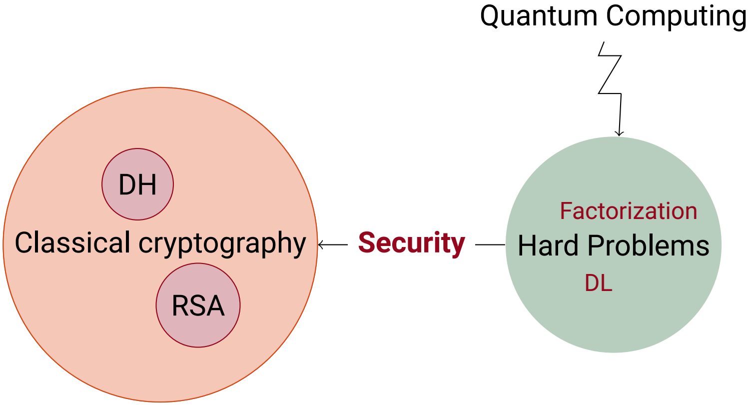
Security and Post-Quantum Cryptography



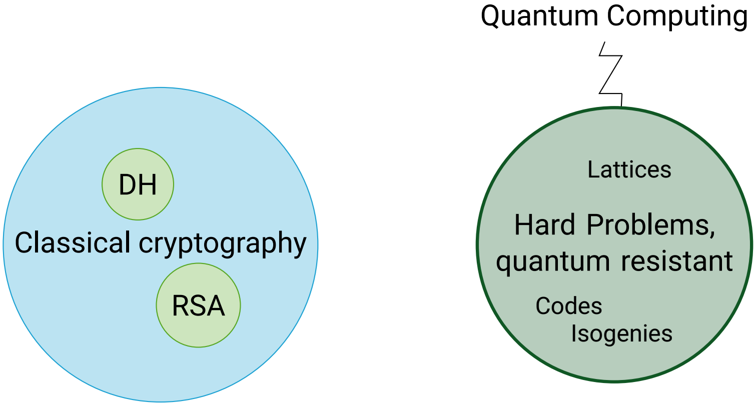
Security and Post-Quantum Cryptography



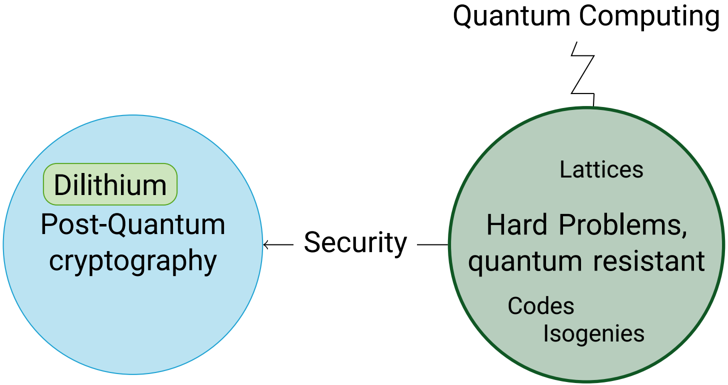
Security and Post-Quantum Cryptography



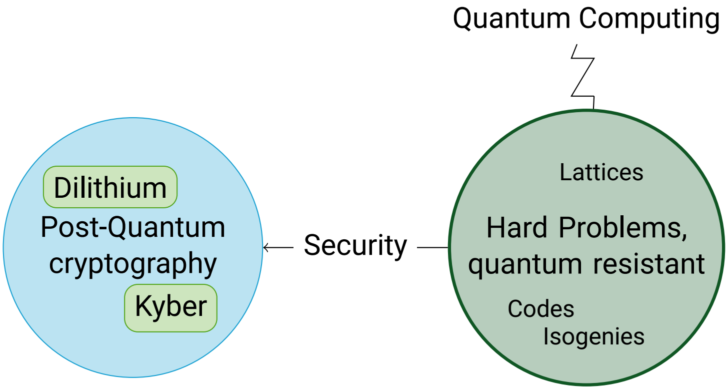
Security and Post-Quantum Cryptography



Security and Post-Quantum Cryptography



Security and Post-Quantum Cryptography

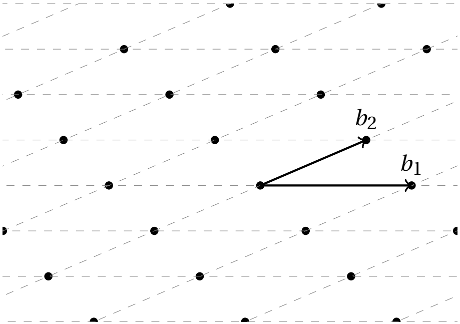


Outline

About Lattices

Lattice

Let $n \in \mathbb{Z}$ and $\mathbf{b_1}, \ldots, \mathbf{b_n} \in \mathbb{R}^n$, a lattice Λ is a discrete subgroup of $\mathbb{R}^n$ given by the set of all integer combinations of linearly independent basis vectors $\mathbf{B} = \mathbf{b_1}, \ldots, \mathbf{b_n}$:
$\Lambda(\mathbf{B}) = \left\{\sum_{i=1}^{n} x_i \mathbf{b}_i : x_i \in \mathbb{Z}\right\}$



Lattice based Cryptography - LWE

- Among 4 finalists of the NIST competition, 3 are based on LWE

$$b = A \cdot s + e \pmod{q}$$

•: public uniform - •: short secret - •: short gaussian error

Lattice based Cryptography - LWE

- Among 4 finalists of the NIST competition, 3 are based on LWE

$$b = A \cdot s + e \pmod{q} \xrightarrow{\mathit{Search}} \text{Given } (\mathbf{A}, \mathbf{b}), \text{ find } \mathbf{s}$$

•: public uniform - •: short secret - •: short gaussian error

Lattice based Cryptography - LWE

- Among 4 finalists of the NIST competition, 3 are based on LWE

$$b = A \cdot s + e \pmod q$$

$\xrightarrow{\textit{Search}}$ Given $(\mathbf{A}, \mathbf{b})$, find $\mathbf{s}$

$\xrightarrow{\textit{Decisional}}$ Distinguish $(\mathbf{A}, \mathbf{b})$ from the uniform

•: public uniform - •: short secret - •: short gaussian error

Lattice based Cryptography - LWE

- Among 4 finalists of the NIST competition, 3 are based on LWE

$$b = A \cdot s + e \pmod{q}$$

$\xrightarrow{\textit{Search}}$ Given $(\mathbf{A}, \mathbf{b})$, find $\mathbf{s}$

$\xrightarrow{\textit{Decisional}}$ Distinguish $(\mathbf{A}, \mathbf{b})$ from the uniform

•: public uniform - •: short secret - •: short gaussian error

- Security based on worst-case lattices assumption for Gaussian error $\mathbf{e}$

Lattice based Cryptography - LWE

- Among 4 finalists of the NIST competition, 3 are based on LWE

$$b = A \cdot s + e \pmod{q}$$

$\xrightarrow{Search}$ Given $(\mathbf{A}, \mathbf{b})$, find $\mathbf{s}$

$\xrightarrow{Decisional}$ Distinguish $(\mathbf{A}, \mathbf{b})$ from the uniform

•: public uniform - •: short secret - •: short gaussian error

- Security based on worst-case lattices assumption for Gaussian error $\mathbf{e}$
- Among 5 finalists of the NIST competition, 3 are based on structured LWE

Lattice based Cryptography - LWE

- Among 4 finalists of the NIST competition, 3 are based on LWE

$$b = A \cdot s + e \pmod{q}$$

$\xrightarrow{\textit{Search}}$ Given $(\mathbf{A}, \mathbf{b})$, find $\mathbf{s}$

$\xrightarrow{\textit{Decisional}}$ Distinguish $(\mathbf{A}, \mathbf{b})$ from the uniform

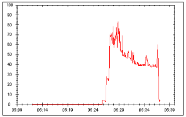
•: public uniform - •: short secret - •: short gaussian error

- Security based on worst-case lattices assumption for Gaussian error $\mathbf{e}$
- Among 5 finalists of the NIST competition, 3 are based on structured LWE

What about physical attacks ?

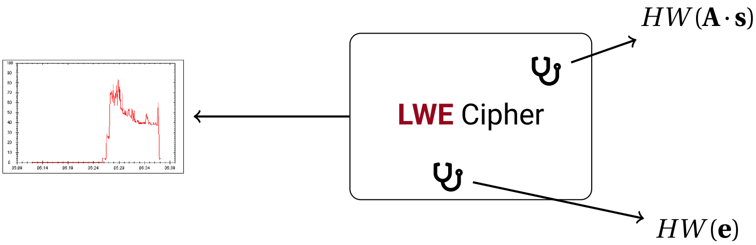
Outline

Side-channel analysis - SC

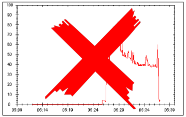


LWE Cipher

Side-channel analysis - SC



Side-channel analysis - SC



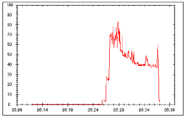
LWE Cipher

Random computation

$HW(\mathbf{A} \cdot \mathbf{s})$

$HW(\mathbf{e})$

Side-channel analysis - SC



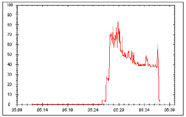
$HW(\mathbf{A} \cdot \mathbf{s})$

LWE Cipher

Random computation

$H\cancel{W}(\mathbf{e})$

Side-channel analysis - SC



$HW(\mathbf{A} \cdot \mathbf{s})$

LWE Cipher

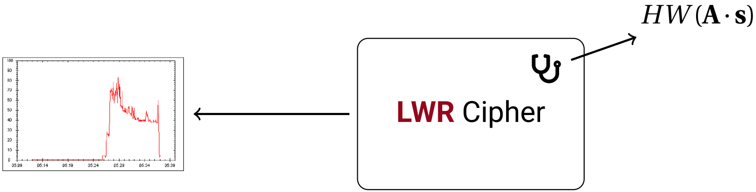
Non efficient error

Probabilistic error $\longrightarrow$ Deterministic error

LWE $\longrightarrow$ LWR

$$(\mathbf{A}, \mathbf{A}\mathbf{s} + \mathbf{e} \pmod q) \longrightarrow (\mathbf{A}, \lceil \mathbf{A}\mathbf{s} \pmod q \rfloor_p)$$

Side-channel analysis - SC



Probabilistic error $\longrightarrow$ Deterministic error

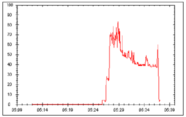
$$\text{LWE} \longrightarrow \text{LWR}$$

$$(\mathbf{A}, \mathbf{A}\mathbf{s} + \mathbf{e} \pmod q) \longrightarrow (\mathbf{A}, \lceil \mathbf{A}\mathbf{s} \pmod q \rfloor_p)$$

Outline

Hard Learning Problem from Side channel analysis

LWE Cipher

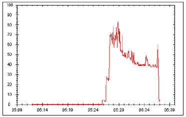


A

Hard Learning Problem from Side channel analysis

LWE Cipher

$\mathbf{As}$ ⚕



$\mathrm{LWPR} : (\mathbf{A}, \mathsf{L}(\mathbf{As}))$

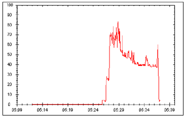
Learning With Physical Rounding

A , $\mathsf{L}(\mathbf{As})$

Hard Learning Problem from Side channel analysis

LWE Cipher

$\mathbf{As}$



$\mathrm{LWPR} : (\mathbf{A}, \lfloor(\mathbf{As})\rceil)$

$\mathrm{LWPRN} : (\mathbf{A}, \lfloor(\mathbf{As})\rceil + \eta)$

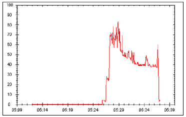
Learning With Physical Rounding and Noise

$$A \; , \; \lfloor(\mathbf{As})\rceil + \eta$$

Hard Learning Problem from Side channel analysis

LWE Cipher

$\mathbf{As}$



$\mathrm{LWPR} : (\mathbf{A}, \mathsf{L}(\mathbf{As}))$

$\mathrm{LWPRN} : (\mathbf{A}, \mathsf{L}(\mathbf{As}) + \eta)$

$\downarrow$

$\Phi - \mathrm{LWE} : (\mathbf{A}, \mathbf{As} + \mathbf{e}, \Phi(\mathbf{As} + \mathbf{e}))$

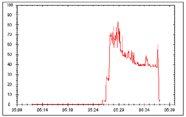
Physical Learning With Error

$$A \;,\; b \;,\; \mathsf{L}(\mathbf{As}) + \eta$$

Hard Learning Problem from Side channel analysis

LWE Cipher

$\mathbf{As}$



$\text{LWPR} : (\mathbf{A}, \mathsf{L}(\mathbf{As}))$

$\text{LWPRN} : (\mathbf{A}, \mathsf{L}(\mathbf{As}) + \eta)$

$\downarrow$

$\Phi - \text{LWE} : (\mathbf{A}, \mathbf{As} + \mathbf{e}, \Phi(\mathbf{As} + \mathbf{e}))$

$\downarrow$

$\text{NHW-LWE} : (\mathbf{A}, \mathbf{As} + \mathbf{e}, \text{HW}(\mathbf{As}) + \eta)$

Noisy Hamming Weight Learning With Error

$$A \; , \; b \; , \; \text{HW}(\mathbf{As}) + \eta$$

Hamming Weight = Number of 1 in the binary decomposition

LWE variants

Hint-LWE gives additional hints:
$(\mathbf{A}, \mathbf{A}\mathbf{s}+\mathbf{e}, (\gamma_i, \gamma_i \mathbf{s} + y_i)_{i \leqslant k})$

LWE variants

Hint-LWE gives additional hints:
$(\mathbf{A}, \mathbf{A}\mathbf{s} + \mathbf{e}, (\gamma_i, \gamma_i \mathbf{s} + y_i)_{i \leqslant k})$

Entropic-LWE considers the entropy of the secret instead of its distribution

LWE variants

Hint-LWE gives additional hints:
$(\mathbf{A}, \mathbf{A}\mathbf{s} + \mathbf{e}, (\gamma_i, \gamma_i \mathbf{s} + y_i)_{i \leqslant k})$

Entropic-LWE considers the entropy of the secret instead of its distribution

- Both security relying on LWE (impact on the dimension of the LWE problem).

LWE variants

Hint-LWE gives additional hints:
$(\mathbf{A}, \mathbf{A}\mathbf{s}+\mathbf{e}, (\gamma_i, \gamma_i \mathbf{s} + y_i)_{i \leqslant k})$

Entropic-LWE considers the entropy of the secret instead of its distribution

- Both security relying on LWE (impact on the dimension of the LWE problem).
- NIST standards are based on short secret distribution

LWE variants

Hint-LWE gives additional hints:
$(\mathbf{A}, \mathbf{A}\mathbf{s}+\mathbf{e}, (\gamma_i, \gamma_i \mathbf{s} + y_i)_{i \leqslant k})$

Entropic-LWE considers the entropy of the secret instead of its distribution

- Both security relying on LWE (impact on the dimension of the LWE problem).
- NIST standards are based on short secret distribution

$$H_\infty(\mathbf{s} \mid \mathbf{A}, \mathrm{HW}(\mathbf{A}\mathbf{s})) \geqslant \underbrace{n \log(q)}_{\texttt{bitLenght}(\mathbf{s})} - \overbrace{m}^{\text{nb of samples}} \cdot \underbrace{\log(\log(q))}_{\texttt{bitLenght}(\mathrm{HW}(\mathbf{a_i}\mathbf{s}))} \tag{1}$$

LWE variants

Hint-LWE gives additional hints:
$(\mathbf{A}, \mathbf{A}\mathbf{s}+\mathbf{e}, (\gamma_i, \gamma_i \mathbf{s} + y_i)_{i \leqslant k})$

Entropic-LWE considers the entropy of the secret instead of its distribution

- Both security relying on LWE (impact on the dimension of the LWE problem).
- NIST standards are based on short secret distribution

$$H_\infty(\mathbf{s} \mid \mathbf{A}, \mathrm{HW}(\mathbf{A}\mathbf{s})) \geqslant \underbrace{n \log(q)}_{\texttt{bitLenght}(\mathbf{s})} - \overbrace{m}^{\text{nb of samples}} \cdot \underbrace{\log(\log(q))}_{\texttt{bitLenght}(\mathrm{HW}(\mathbf{a_i}\mathbf{s}))} \tag{1}$$

- **Entropic-LWE is not conclusive with such a drop of entropy on the secret**

Result on Noisy Hamming Weight Learning With Error

$$\mathrm{LWE}_{q,n,m,\sigma_e} \xrightarrow{\text{Theorem}} \text{NHW-LWE}^{\sigma_\eta}_{q,n,m,\sigma_e} \xrightarrow{\text{remove } \mathbf{b}} \mathrm{LWPRN}^{\mathrm{HW},\sigma_\eta}_{q,n,m}$$

$(\mathbf{A}, \mathbf{b})$ — $(\mathbf{A}, \mathbf{b}, \mathrm{HW}(\mathbf{As}) + \eta)$ — $(\mathbf{A}, \mathrm{HW}(\mathbf{As}) + \eta)$

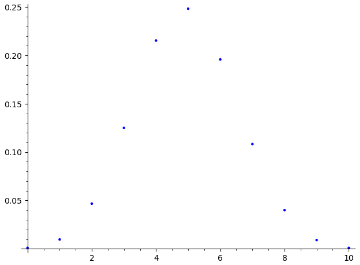


Figure: Distribution of $\mathrm{HW}(\mathbf{As})$ for $q = 1117$ and $n = 20$ for a fixed vector $\mathbf{a}$

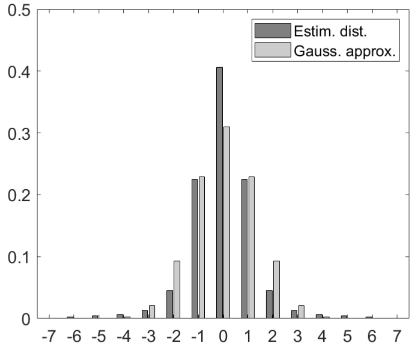
Intuition of reduction

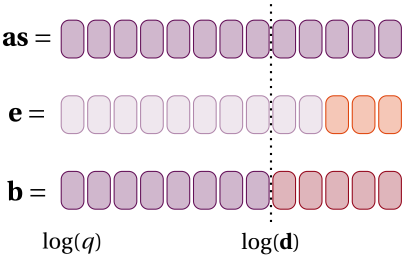
Showing that sNHW-LWE is hard under sLWE = construct an adversary against sLWE using an adversary against sNHW-LWE.

$\mathscr{C}$	LWE	$\mathscr{B}$	Φ-LWE	$\mathscr{A}$
$\mathbf{A} \xleftarrow{\$} \mathbb{Z}_q^{m\times n}$				
$\mathbf{s} \xleftarrow{\$} \mathbb{Z}_q^n,\ \mathbf{e} \leftarrow \chi^m$				
	$\xrightarrow{(\mathbf{A},\mathbf{b}=\mathbf{A}\mathbf{s}+\mathbf{e})}$			
		$\mathbf{h} := \mathrm{HW}(\mathbf{b})$		
		$\approx \mathrm{HW}(\mathbf{A}\mathbf{s}) + \mathbf{d}$		
		$\eta \hookleftarrow \sigma_\eta$		
			$\xrightarrow{(\mathbf{A},\mathbf{b},\mathbf{h}+\eta)}$	

$$(\mathbf{A}, \mathbf{b}, \mathrm{HW}(\mathbf{b}) + \eta) \xrightarrow{\text{Lemma}} (\mathbf{A}, \mathbf{A}\mathbf{s} + \mathbf{e}, \mathrm{HW}(\mathbf{A}\mathbf{s}) + \mathbf{d} + \eta) \xrightarrow{\text{SD/RD}} (\mathbf{A}, \mathbf{A}\mathbf{s} + \mathbf{e}, \mathrm{HW}(\mathbf{A}\mathbf{s}) + \eta')$$

From LWE sample to NHW-LWE sample





Difference $\mathrm{HW}(\mathbf{b}) - \mathrm{HW}(\mathbf{As})$ and its distance to a Gaussian distribution.

Outline

Conclusion

- Known hardness of LWE under physical leakage in a more realistic model (noisy Hamming Weight)
- Possibility of relaxation in masking LWE-based cryptosystems

Conclusion

- Known hardness of LWE under physical leakage in a more realistic model (noisy Hamming Weight)
- Possibility of relaxation in masking LWE-based cryptosystems
- Is the decisionnal variant as hard as the search one ?
- Is there exist a better bound on $\mathbf{d}$ knowing $\mathbf{A}$?
- Can it be possible to lead to a known hint variant with special case modulus such as Mersenne prime or power of two ?

Conclusion

- Known hardness of LWE under physical leakage in a more realistic model (noisy Hamming Weight)
- Possibility of relaxation in masking LWE-based cryptosystems
- Is the decisionnal variant as hard as the search one ?
- Is there exist a better bound on $\mathbf{d}$ knowing $\mathbf{A}$?
- Can it be possible to lead to a known hint variant with special case modulus such as Mersenne prime or power of two ?

Thank you for your attention