Introduction to Learning Problems in Cryptography

Emeline Repel[3]

[3]CNRS
Université de Caen Normandie

November 17 2026











Joint work with C. Hoffmann[1], A. Roux-Langlois[3] and F.X. Standaert[2]

[1]NTT,Japan
[2]UCL, Louvain la Neuve

Context



Internet



Messageries instantanées



Paiements

Goal

- protect data (encryption),
- authenticate data (signature)

Introduction to Cryptography

- Asymmetric Cryptography: occasional exchanges (Private key exchange)





- 🔑: Public key - 🔑: Private key

Introduction to Cryptography

- Asymmetric Cryptography: occasional exchanges (Private key exchange)



- 🔑: Public key - 🔑: Private key

Introduction to Cryptography

- Asymmetric Cryptography: occasional exchanges (Private key exchange)



- 🔑: Public key - 🔑: Private key

Introduction to Cryptography

- Asymmetric Cryptography: occasional exchanges (Private key exchange)



- Symmetric Cryptography: frequent interactions (daily communication)



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

Introduction to Cryptography

- Asymmetric Cryptography: occasional exchanges (Private key exchange)



- Symmetric Cryptography: frequent interactions (daily communication)

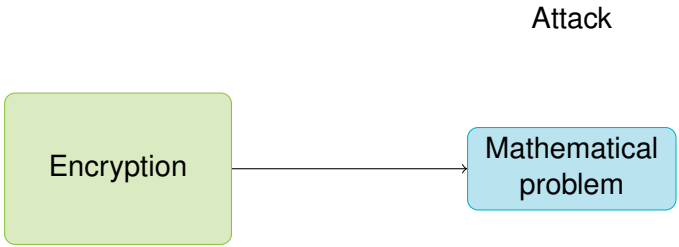


- 🔑: Public key - 🔑: Private key
- 🔑: Shared but Private key

Cryptographic security

Defining the security

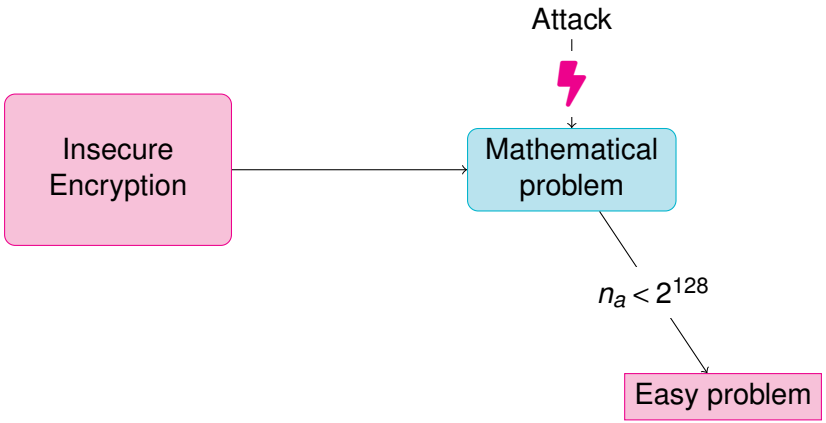
Number of operation n_a needed to retrieve the secret



Cryptographic security

Defining the security

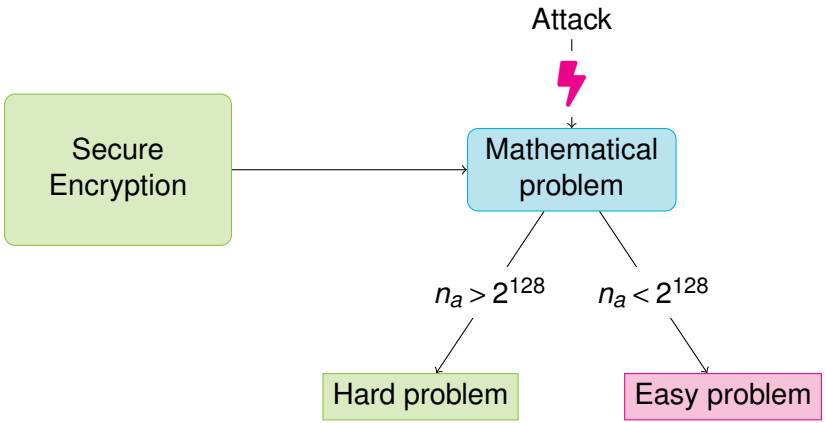
Number of operation n_a needed to retrieve the secret



Cryptographic security

Defining the security

Number of operation n_a needed to retrieve the secret



Two types of Security

Algorithm submission

Achieve Theoretical security

Theoretical security

Going back to a known difficult problem

Known hard problem $\Rightarrow$ Scheme secure

Breaks Known hard problem $\Leftrightarrow$ Insecure scheme

Two types of Security

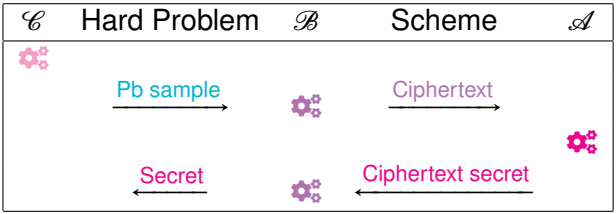
Algorithm submission

Achieve Theoretical security



Theoretical security

Going back to a known difficult problem



Two types of Security

Algorithm submission
Achieve Theoretical security

Testing practical security

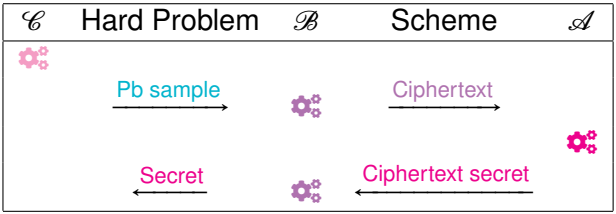
Algorithm standardization
Achieve Practical security

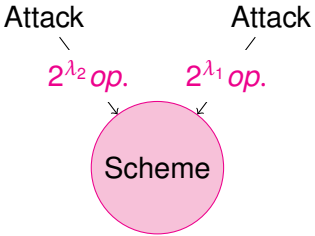
Theoretical security

Going back to a known difficult problem

Practical security

Attack the scheme to approximate the security





Two types of Security

Algorithm submission
Achieve Theoretical security

Testing practical security

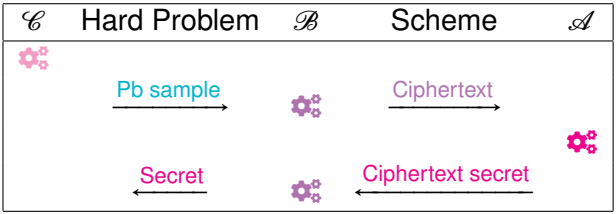
Algorithm standardization
Achieve Practical security

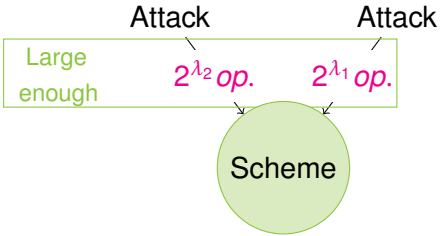
Theoretical security

Going back to a known difficult problem

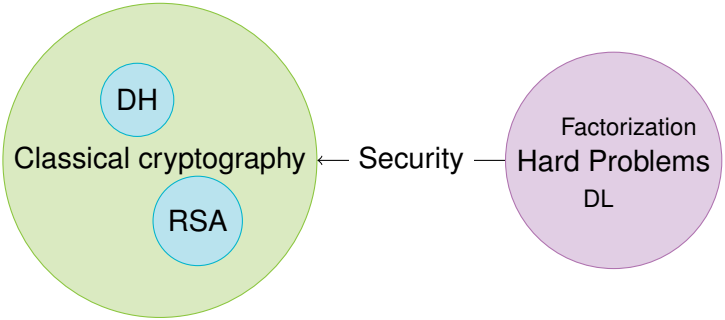
Practical security

Attack the scheme to approximate the security

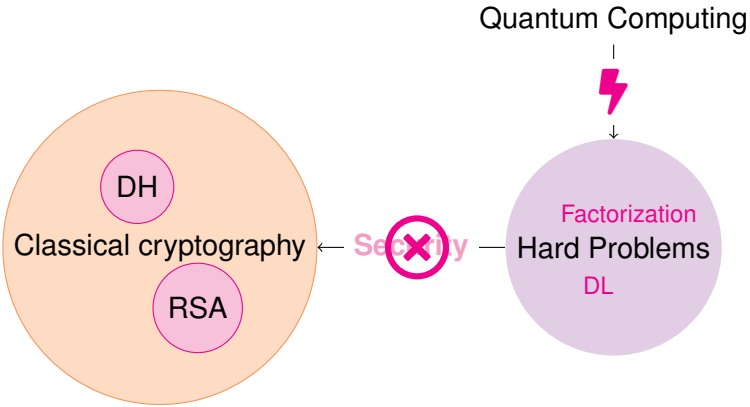




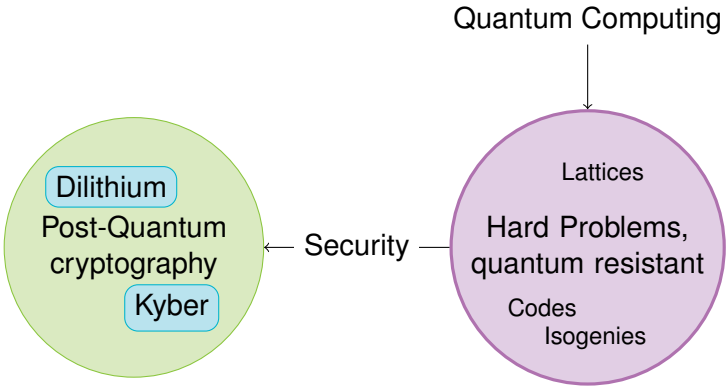
From Classical to Post-quantum cryptography



From Classical to Post-quantum cryptography



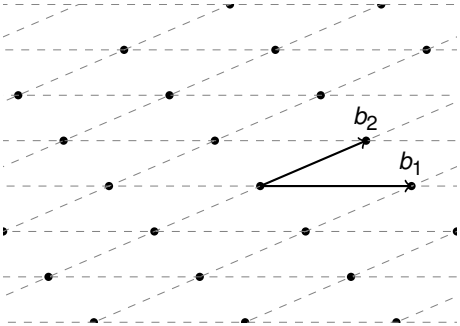
From Classical to Post-quantum cryptography



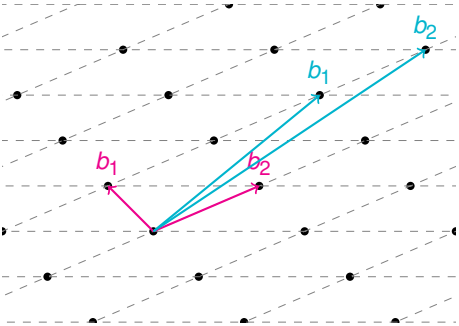
Lattice-based Cryptography

Lattice

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



Bad VS Good basis

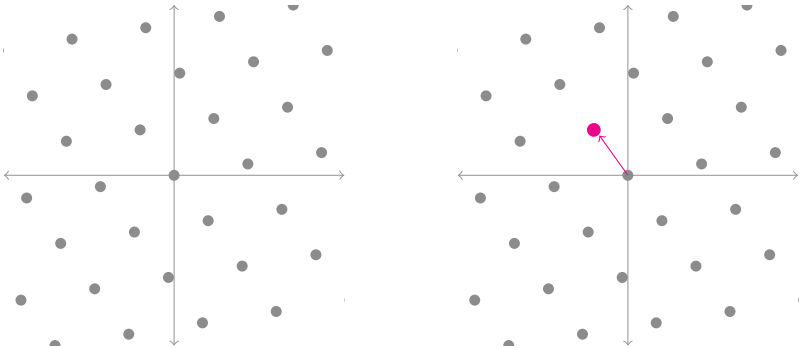


How much hardness ?

- Bad basis = public
- Good basis = secrete

Hard Lattices Problems

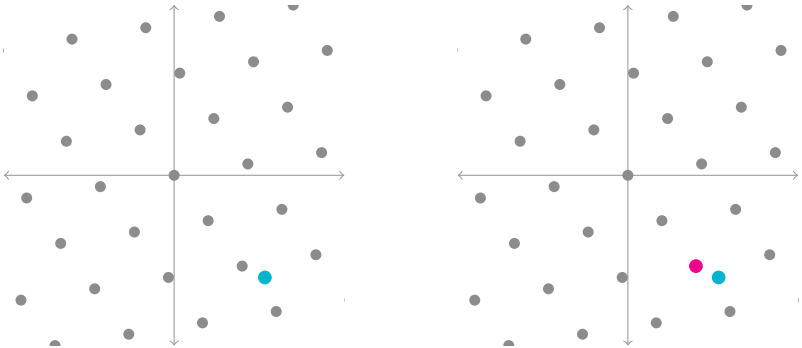
Shortest Vector problem - SVP



Goal: finding the shortest vector of a Lattice

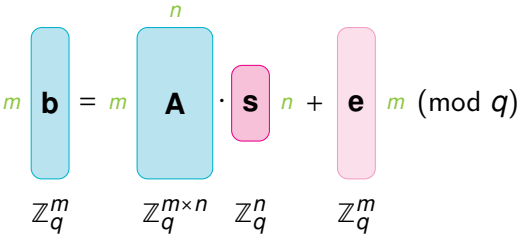
Hard Lattices Problems

Closest Vector problem - CVP



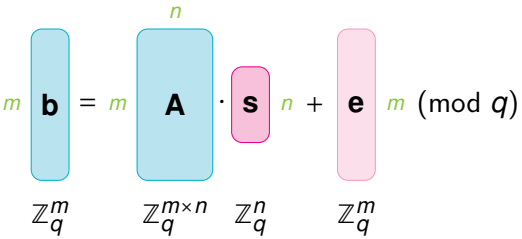
Goal: finding the closest vector of a target in the Lattice

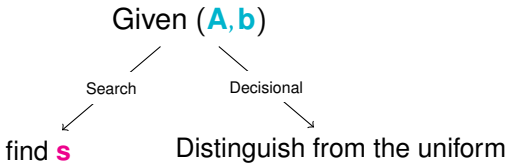
Learning with Error



Learning with Error

Variants





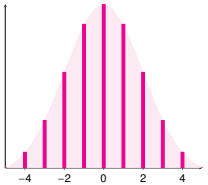
Learning with Error

Hardness

$$\underset{\mathbb{Z}_q^m}{\mathbf{b}} = \underset{\mathbb{Z}_q^{m\times n}}{\mathbf{A}} \cdot \underset{\mathbb{Z}_q^n}{\mathbf{s}} + \underset{\mathbb{Z}_q^m}{\mathbf{e}} \pmod q$$

Given $(\mathbf{A}, \mathbf{b})$

- Search → find $\mathbf{s}$
- Decisional → Distinguish from the uniform



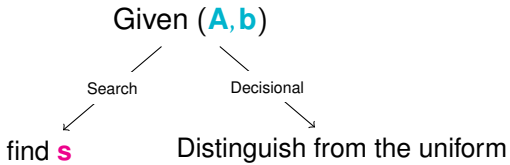
- Security based on worst-case lattices assumption for Gaussian error $\mathbf{e}$ [Regev05]

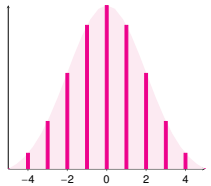
Learning with Error

Standardization

$$\underset{m}{\mathbf{b}} = \underset{m}{\overset{n}{\mathbf{A}}} \cdot \underset{n}{\mathbf{s}} + \underset{m}{\mathbf{e}} \pmod q$$

$$\mathbf{b} \in \mathbb{Z}_q^m \quad \mathbf{A} \in \mathbb{Z}_q^{m \times n} \quad \mathbf{s} \in \mathbb{Z}_q^n \quad \mathbf{e} \in \mathbb{Z}_q^m$$

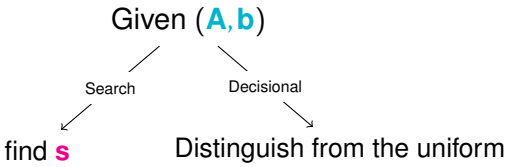


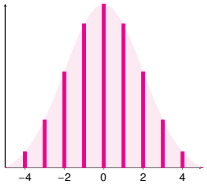


- Security based on worst-case lattices assumption for Gaussian error **e** [Regev05]
- Among 5 standards of the NIST, 3 are based on structured LWE variants

Learning with Error

$$\underset{\mathbb{Z}_q^m}{\mathbf{b}} = \underset{\mathbb{Z}_q^{m\times n}}{\mathbf{A}} \cdot \underset{\mathbb{Z}_q^n}{\mathbf{s}} + \underset{\mathbb{Z}_q^m}{\mathbf{e}} \pmod q$$





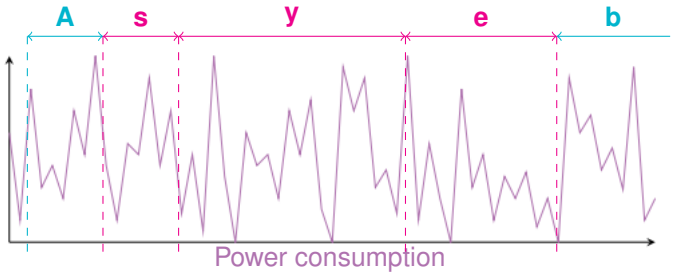
- Security based on worst-case lattices assumption for Gaussian error **e** [Regev05]
- Among 5 standards of the NIST, 3 are based on structured LWE variants

What about Physical Security ?

Physical security

Analysis of computational resources

1: $\mathbf{A} \xleftarrow{\$} \mathbb{Z}_q^{m \times n}$
2: $\mathbf{s} \xleftarrow{\$} \mathbb{Z}_q^n$
3: $\mathbf{y} \leftarrow \mathbf{A} \cdot \mathbf{s}$
4: $\mathbf{e} \xleftarrow{\$} \mathscr{D}_\sigma(\mathbb{Z}_q^m)$
5: $\mathbf{b} \leftarrow \mathbf{y} \oplus \mathbf{e}$



Physical security

Analysis of computational resources

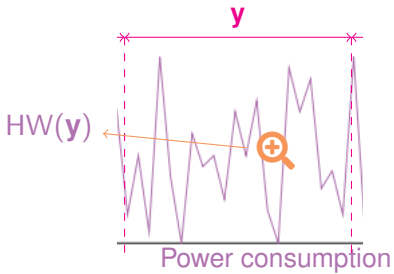
1: $\mathbf{A} \xleftarrow{\$} \mathbb{Z}_q^{m \times n}$

2: $\mathbf{s} \xleftarrow{\$} \mathbb{Z}_q^n$

3: $\mathbf{y} \leftarrow \mathbf{A} \cdot \mathbf{s}$

4: $\mathbf{e} \xleftarrow{\$} \mathcal{D}_\sigma(\mathbb{Z}_q^m)$

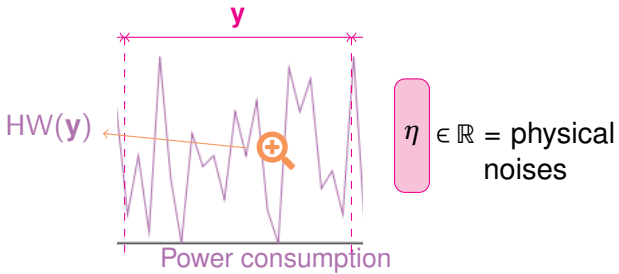
5: $\mathbf{b} \leftarrow \mathbf{y} \oplus \mathbf{e}$



Physical security

Deduction of information on sensitive data

1: $\mathbf{A} \xleftarrow{\$} \mathbb{Z}_q^{m \times n}$
2: $\mathbf{s} \xleftarrow{\$} \mathbb{Z}_q^n$
3: $\mathbf{y} \leftarrow \mathbf{A} \cdot \mathbf{s}$
4: $\mathbf{e} \xleftarrow{\$} \mathcal{D}_\sigma(\mathbb{Z}_q^m)$
5: $\mathbf{b} \leftarrow \mathbf{y} \oplus \mathbf{e}$



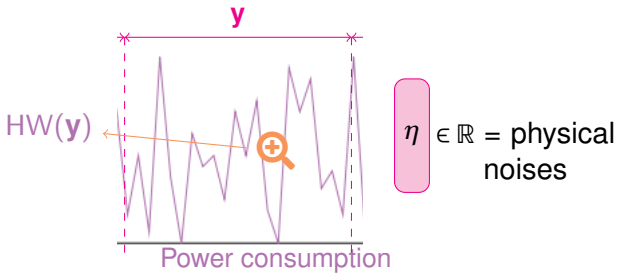
Leveraging problems

- $(\mathbf{A}, \mathbf{y}) \rightarrow$ Not Hard
- $(\mathbf{A}, \mathrm{HW}(\mathbf{y})) \rightarrow$ Hard ?
- $(\mathbf{A}, \mathrm{HW}(\mathbf{y}) + \eta) \rightarrow$ **Hard**

Physical security

How much sensible ?

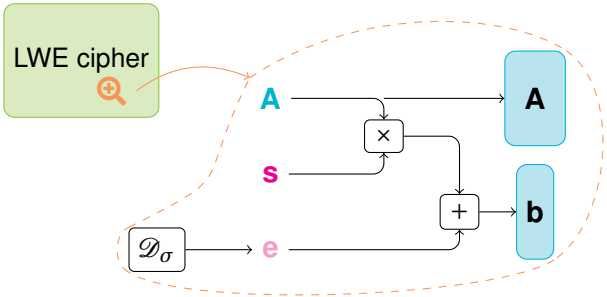
1: $\mathbf{A} \xleftarrow{\$} \mathbb{Z}_q^{m \times n}$
2: $\mathbf{s} \xleftarrow{\$} \mathbb{Z}_q^n$
3: $\mathbf{y} \leftarrow \mathbf{A} \cdot \mathbf{s}$
4: $\mathbf{e} \xleftarrow{\$} \mathcal{D}_\sigma(\mathbb{Z}_q^m)$
5: $\mathbf{b} \leftarrow \mathbf{y} \oplus \mathbf{e}$



Leveraging problems

- $(\mathbf{A}, \mathbf{y})$ → Not Hard
- $(\mathbf{A}, \mathrm{HW}(\mathbf{y}))$ → Hard ?
- $(\mathbf{A}, \mathrm{HW}(\mathbf{y}) + \eta)$ → **Hard**

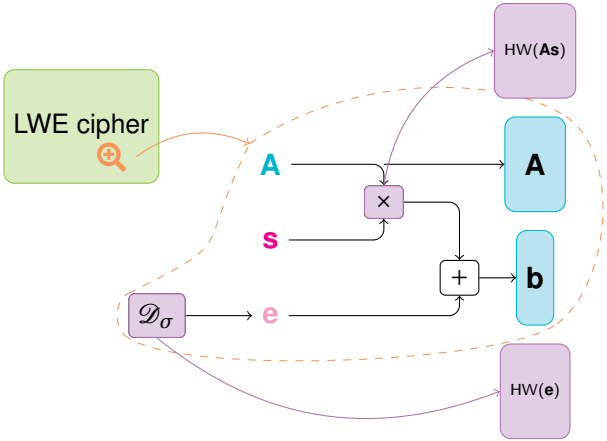
Side Channel Analysis



- power consumption
- timing
- electromagnetic emission
- acoustic emission

Side Channel Analysis

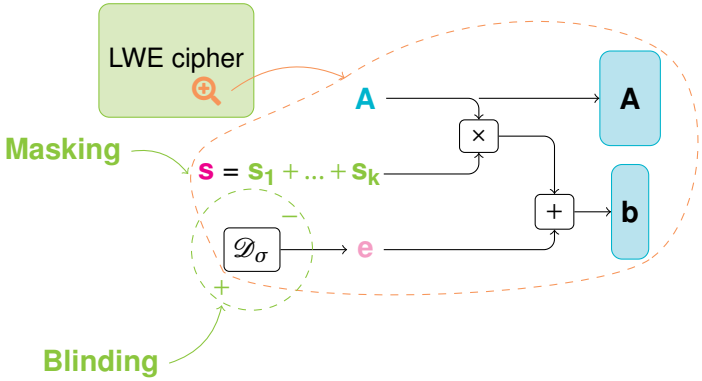
Possible leakages



- non constant time operation
- sensible operation

Side Channel Analysis

Countermeasures

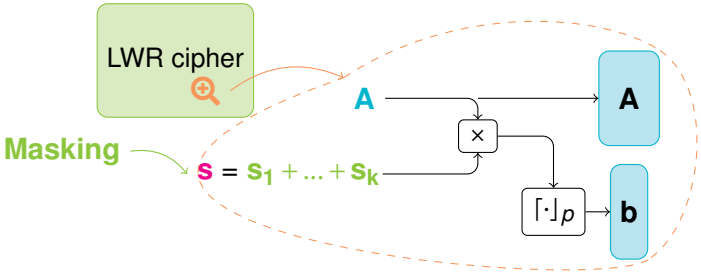


- Masking = share
- Blinding = randomize

COSTLY

Side Channel Analysis

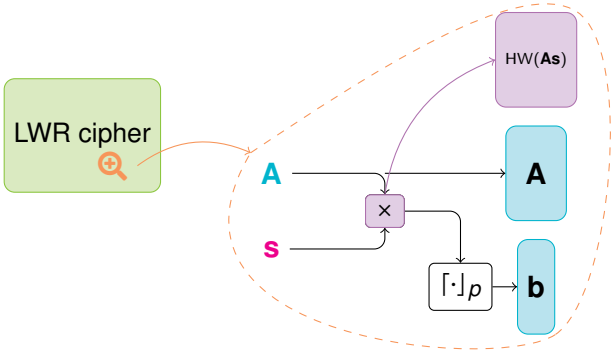
Countermeasures: avoiding blinding



- LWE: $\mathbf{b} = \mathbf{As} + \mathbf{e}$
- LWR: $\mathbf{b} = \lceil \mathbf{As} \rfloor_p$ [BPR12]

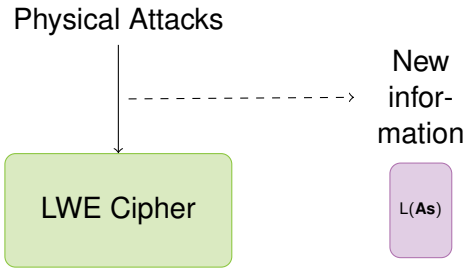
Side Channel Analysis

Countermeasures: avoiding masking

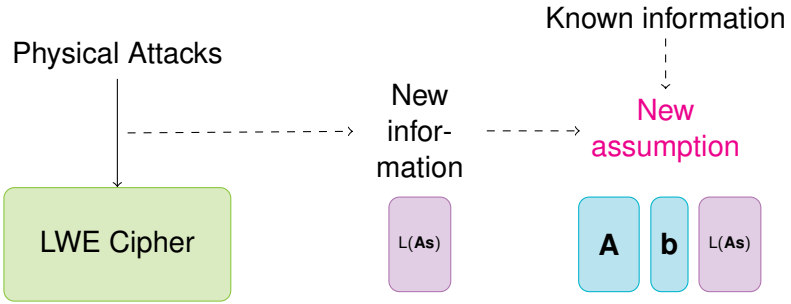


Relaxed Assumption

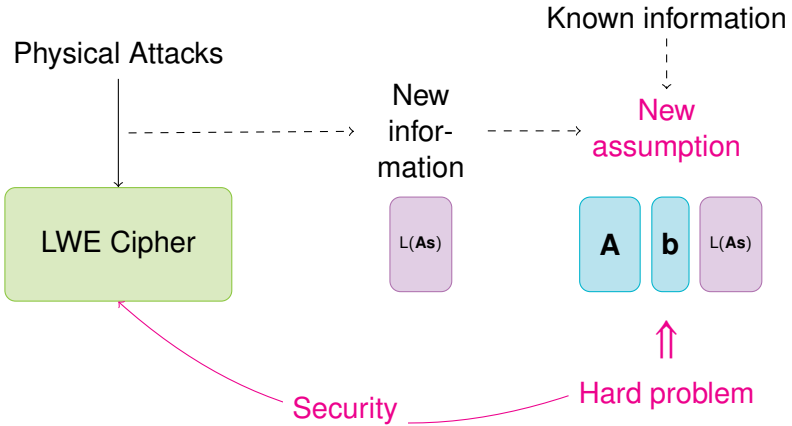
From Physical attacks to Theoretical Security



From Physical attacks to Theoretical Security

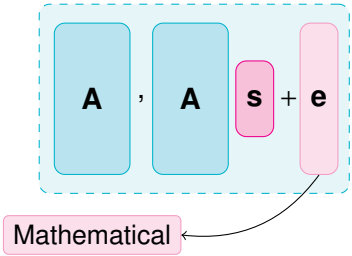


From Physical attacks to Theoretical Security



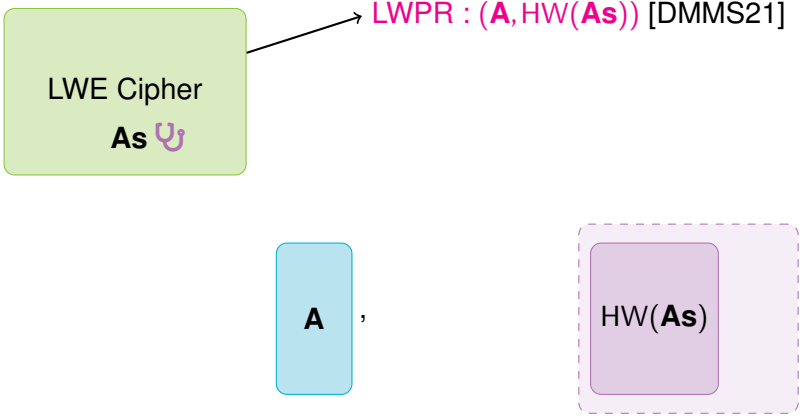
Hard Learning problem from Side channel analysis

LWE Cipher



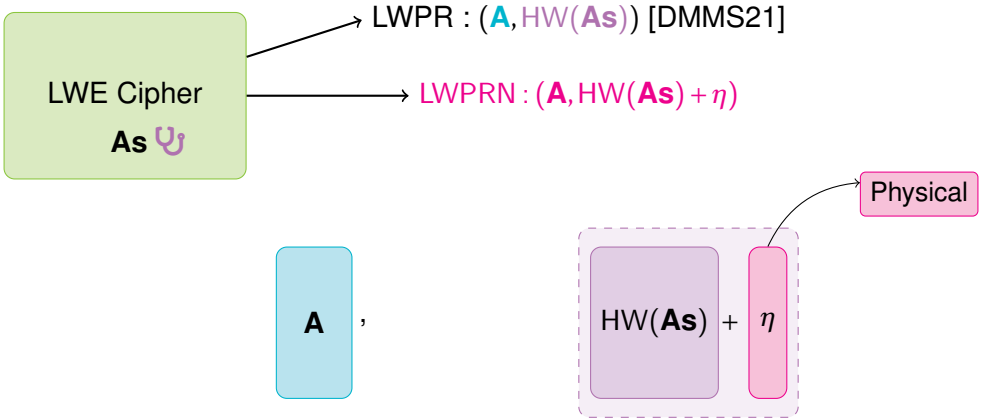
Hard Learning problem from Side channel analysis

Learning With Physical Rounding



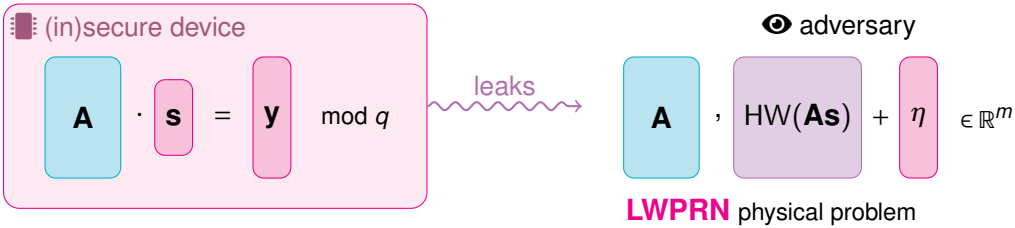
Hard Learning problem from Side channel analysis

Learning With Physical Rounding and Noises



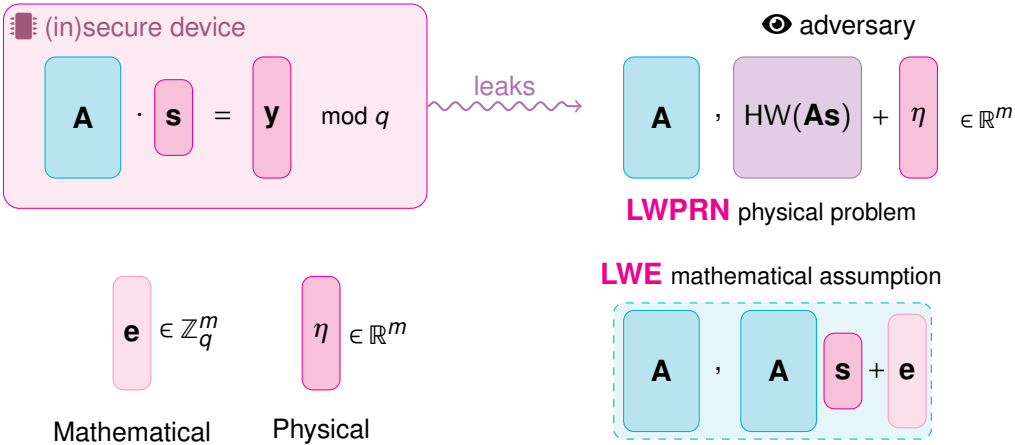
How to obtain a secure device ?

LWRPN hard ⇒ device secure



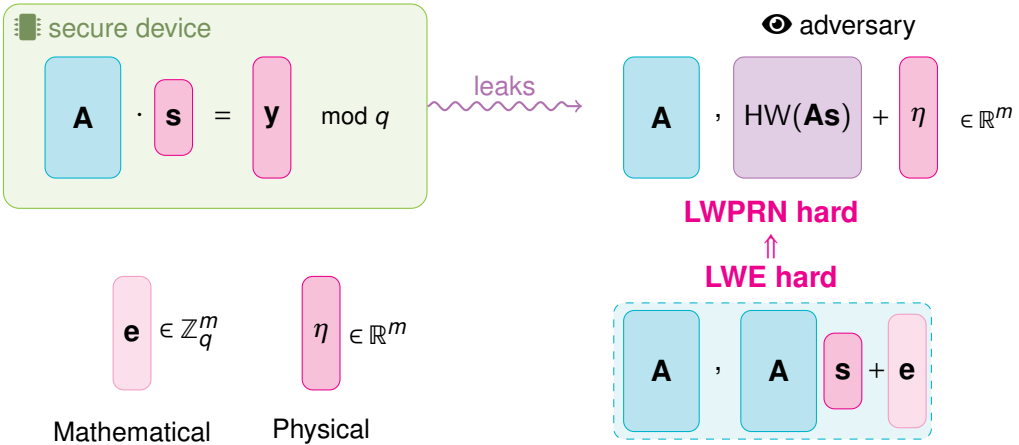
How to obtain a secure device ?

LWRPN hard ⇒ device secure



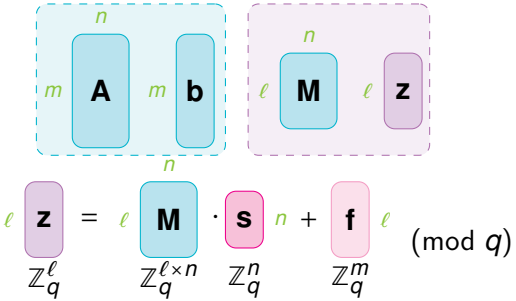
How to obtain a secure device ?

LWRPN hard ⇒ device secure



Link with known hint LWE variant [KLSS23,LSW25]

More information from implementation choices

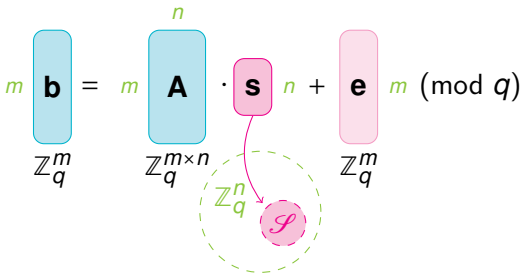


Choice of **M**

- Adversary
- (possibly) unstructured

Link with known Entropic LWE variant [BD20]

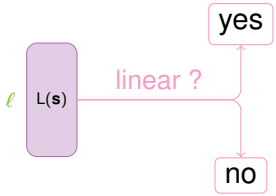
More information from implementation optimization



Choice of $\mathscr{S}$

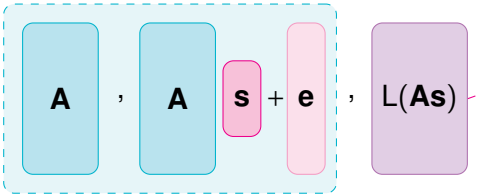
- Large entropy
- Short secret variant

Considering additional leakage

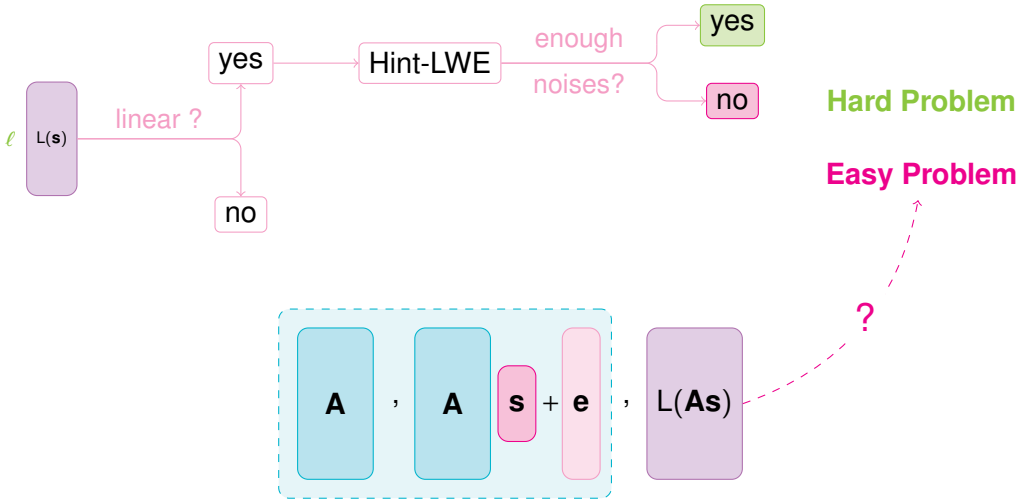


Hard Problem

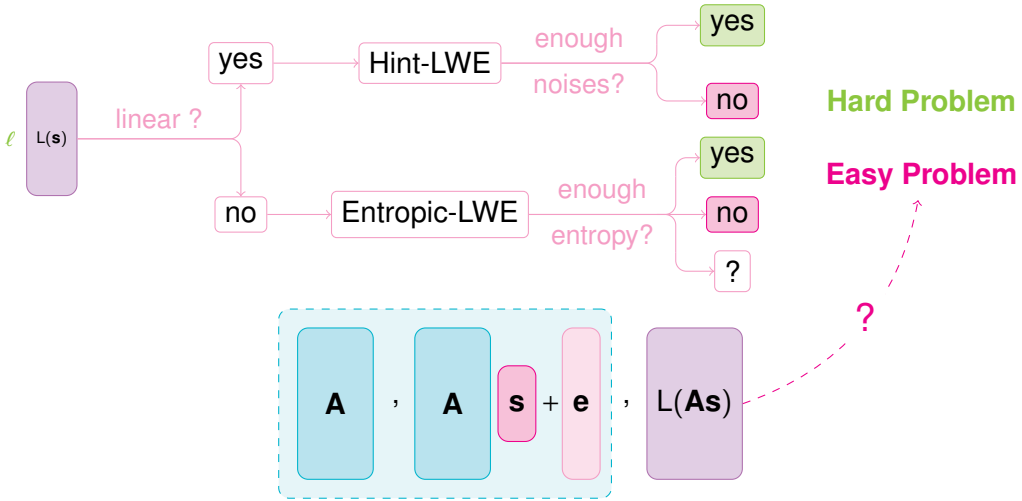
Easy Problem



Considering additional leakage



Considering additional leakage



Do variants apply to our case ?

HW = not linear in the LWE field $\mathbb{Z}_q$

Leakage's entropy

Do variants apply to our case ?

Parallel



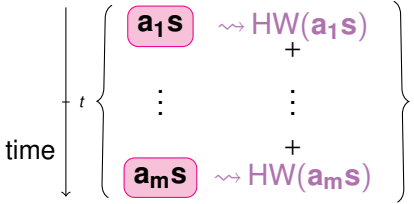
$\sum_{i=1}^{m} \mathrm{HW}(\mathbf{a_i s})$ $\rightarrow \log(m \log(q))$

HW = not linear in the LWE field $\mathbb{Z}_q$

Leakage's entropy

Do variants apply to our case ?

Parallel

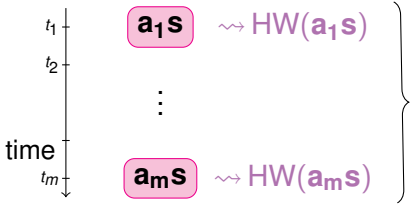


$\sum_{i=1}^{m} \mathrm{HW}(\mathbf{a_i s}) \rightarrow \log(m \log(q))$

HW = not linear in the LWE field $\mathbb{Z}_q$

Leakage's entropy

Serial

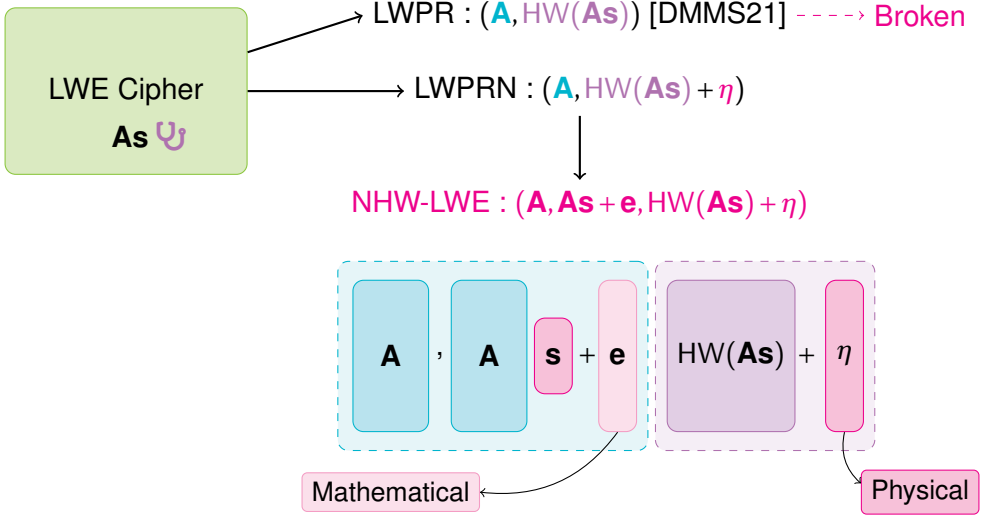


$(\mathrm{HW}(\mathbf{a_1 s}), ..., \mathrm{HW}(\mathbf{a_m s})) \rightarrow m \log(\log(q))$

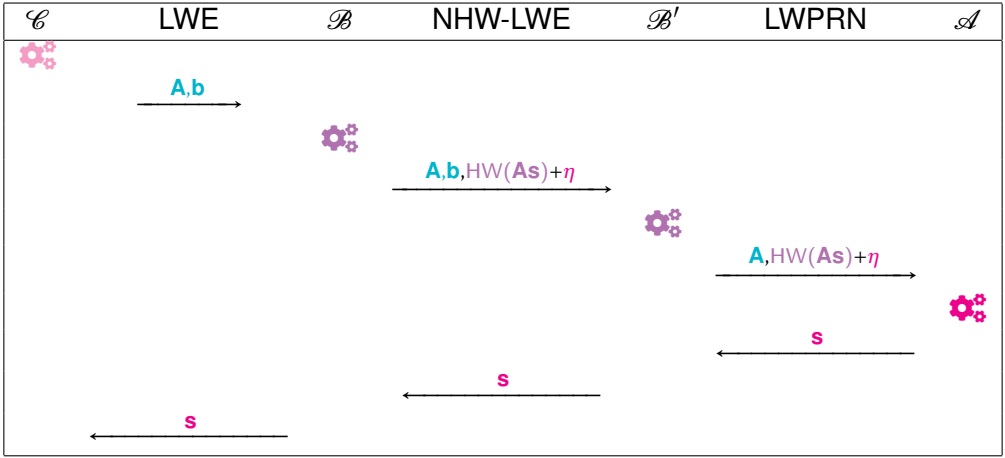
Already broken [DMMS21,HMM+23]

Hard Learning Problem from Side-channel analysis

Noisy Hamming Weight LWE



Targeting LWPRN hardness from LWE assumption



From Learning problem to new Mathematical Assumption

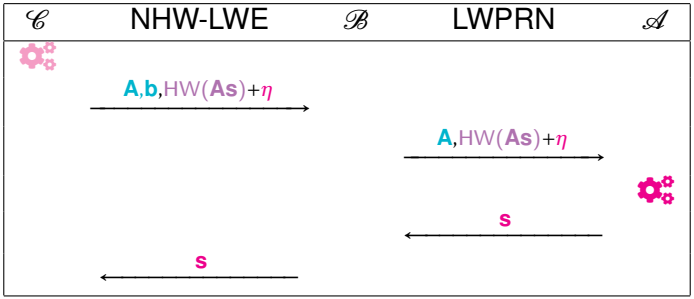
NHW-LWE ⇒ LWPRN - [HRRS26]

Breaking with few information is more difficult than breaking with more information

From Learning problem to new Mathematical Assumption

NHW-LWE ⇒ LWPRN - [HRRS26]

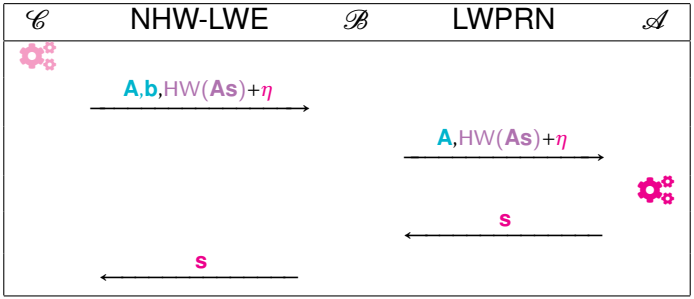
Breaking with few information is more difficult than breaking with more information



From Learning problem to new Mathematical Assumption

NHW-LWE ⇒ LWPRN - [HRRS26]

Breaking with few information is more difficult than breaking with more information



Hardness of LWPRN from LWE ?

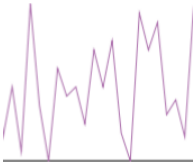
NHW-LWE acts as an intermediate to reach LWPRN from LWE

Summary

- We have

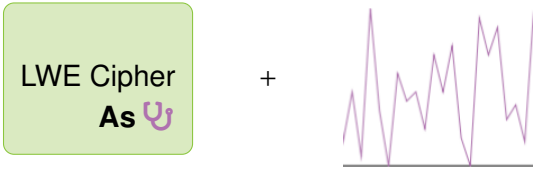
LWE Cipher
As 

+



Summary

- We have

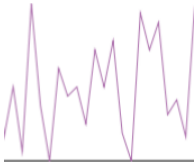


- We want

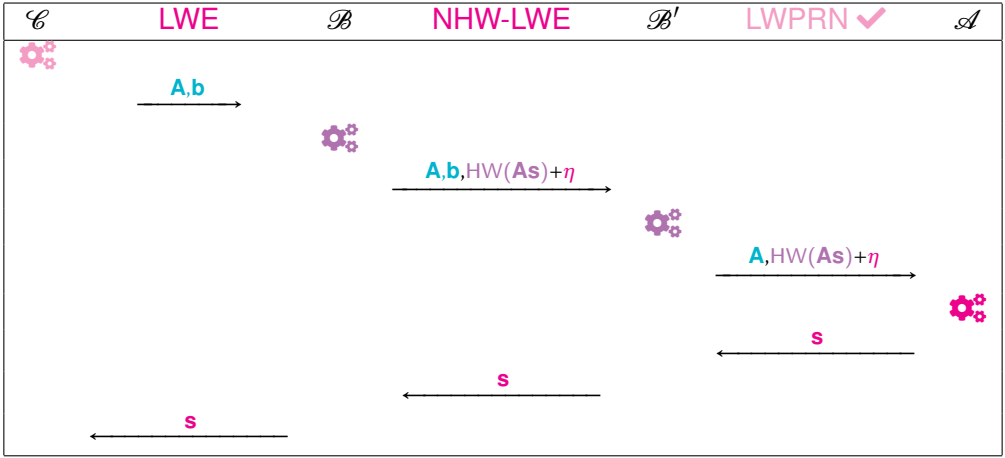


LWPRN hard

Summary

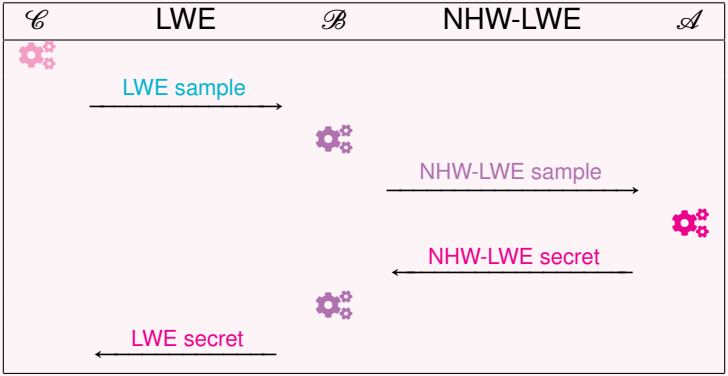
- We have LWE Cipher **As** + 
- We want $\mathbf{A}$, $\mathrm{L}(\mathbf{As})$ + η LWPRN hard
- We study $\mathbf{A}$, $\mathbf{b}$, $\mathrm{HW}(\mathbf{As})$ + η hardness of NHW-LWE under LWE assumption

Targeting LWPRN hardness from LWE assumption check-up



What we need ?

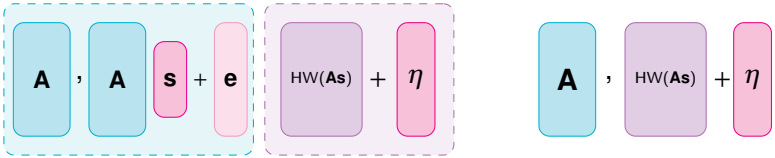
Breaking NHW-LWE ⇒ breaks LWE (supposed hard)



Results on Noisy Hamming Weight Learning With Error

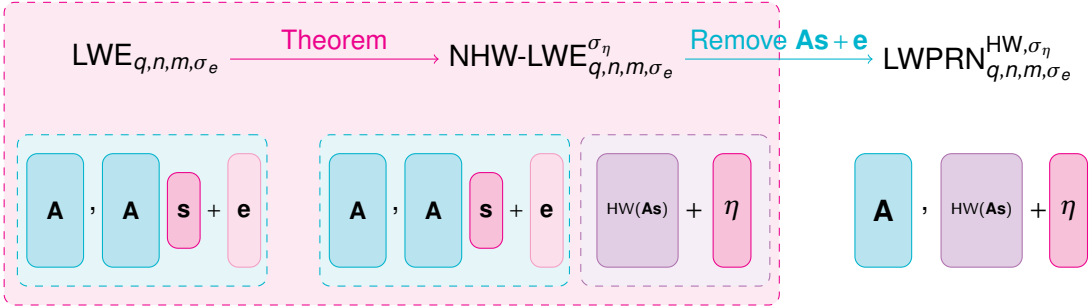
From NHW-LWE to LWPRN

$$\text{NHW-LWE}^{\sigma_\eta}_{q,n,m,\sigma_e} \xrightarrow{\text{Remove } \mathbf{As}+\mathbf{e}} \text{LWPRN}^{\text{HW},\sigma_\eta}_{q,n,m,\sigma_e}$$



Results on Noisy Hamming Weight Learning With Error

From LWE to NHW-LWE

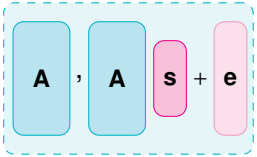


- Statistical distance: $\frac{\lceil \log_2(\sqrt{\lambda}\sigma_e)\rceil}{\sigma_\eta} \leqslant \varepsilon$
- Rényi divergence: $\sigma_\eta \geqslant \sqrt{m}\lceil \log_2(\sqrt{\lambda}\sigma_e)\rceil$

Intuition of the reduction

LWE ⇒ NHW-LWE : showing the contraposition

Construct $\mathscr{B}$ an adversary against LWE using $\mathscr{A}$ an adversary against NHW-LWE.

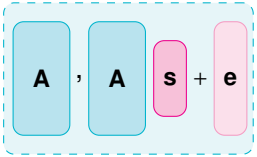


Intuition of the reduction

LWE ⇒ NHW-LWE : showing the contraposition

Construct $\mathscr{B}$ an adversary against LWE using $\mathscr{A}$ an adversary against NHW-LWE.

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

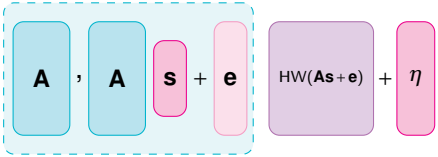


Intuition of the reduction

LWE ⇒ NHW-LWE : showing the contraposition

Construct $\mathscr{B}$ an adversary against LWE using $\mathscr{A}$ an adversary against NHW-LWE.

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

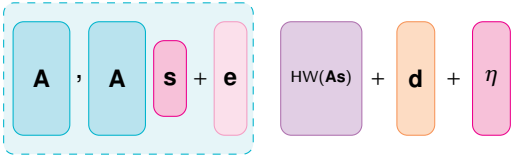


Intuition of the reduction

LWE ⇒ NHW-LWE : showing the contraposition

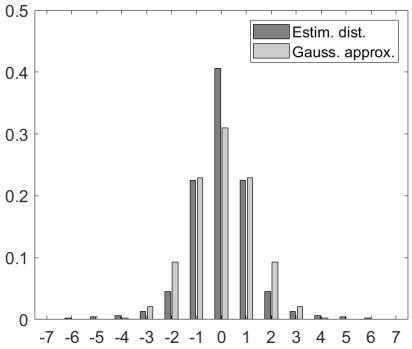
Construct $\mathscr{B}$ an adversary against LWE using $\mathscr{A}$ an adversary against NHW-LWE.

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

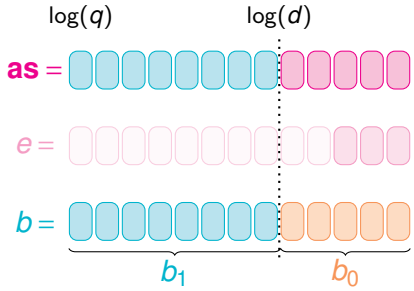


From LWE sample to NHW-LWE sample

Influence of the LWE error



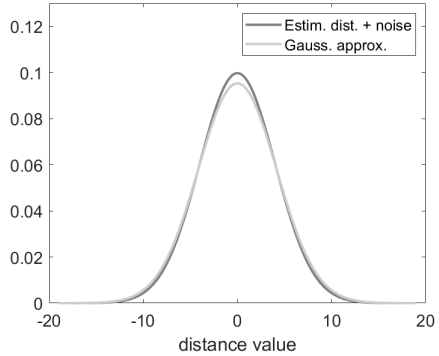
Difference HW(**b**) − HW(**As**) and its Gaussian approximation.



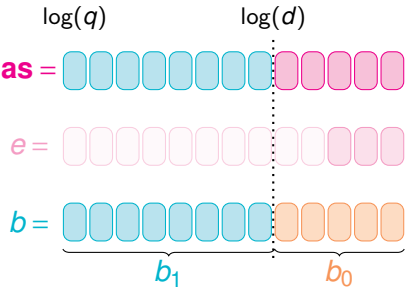
$$\mathrm{HW}(\mathbf{as}) = \mathrm{HW}(b_1) + \mathrm{HW}((\mathbf{as})_0)$$
$$= \mathrm{HW}(b) + d$$

From LWE sample to NHW-LWE sample

Masking this influence



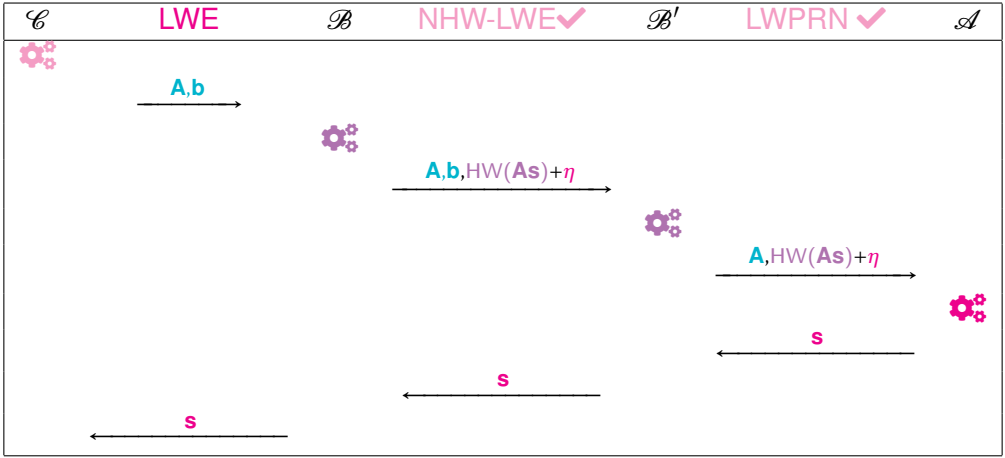
Difference $(\mathrm{HW}(\mathbf{b})+\eta)-(\mathrm{HW}(\mathbf{As})+\eta)$ and its Gaussian approximation.



$$\mathrm{HW}(\mathbf{as})+\eta = \mathrm{HW}(b_1)+d+\eta$$
$$\approx \mathrm{HW}(b)+\eta$$

η independent of q

Targeting LWPRN hardness from LWE assumption - check-up



Conclusion

LWE hard ⇒ LWRPN hard ⇒ device secure

