# On the Hardness of Learning With Physical Rounding and Noise from Learning With Error

C. Hoffmann[1] E. Repel[2] A. Roux-Langlois[2] F-X. Standaert[1]

[1]UCL
Université Catholique de Louvain

[2]CNRS
Université de Caen Normandie

March 31, 2026

# 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

## Analysis of computational resources

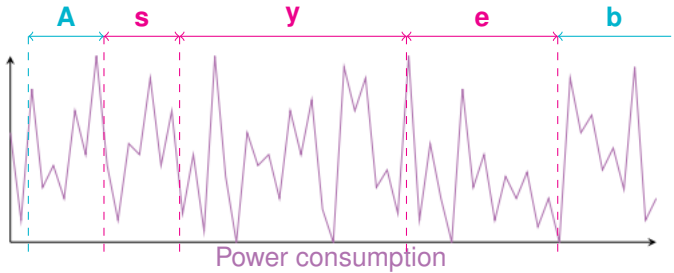
1: $\mathbf{A} \xleftarrow{\$} \mathbb{Z}_q^{m \times n}$

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

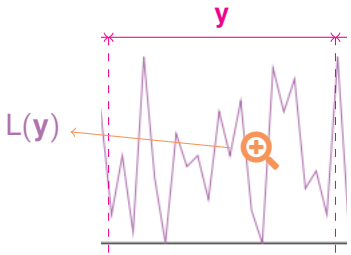
1: $\mathbf{A} \xleftarrow{\$} \mathbb{Z}_q^{m \times n}$

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

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

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

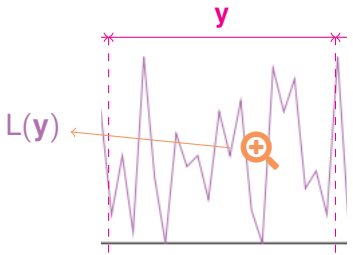
5: $\mathbf{b} \leftarrow \mathbf{y} \oplus \mathbf{e}$



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




$\eta \in \mathbb{R}$ = physical noises

### 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**

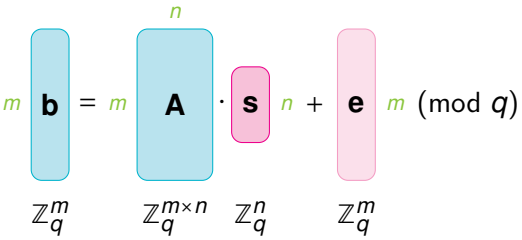
# Learning With Error - LWE

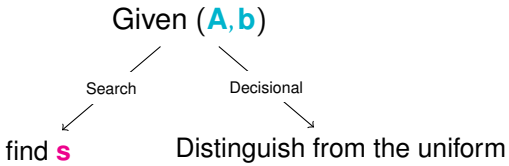
$$\underset{m}{\mathbf{b}} = \underset{m}{\overset{n}{\mathbf{A}}} \cdot \underset{n}{\mathbf{s}} + \underset{m}{\mathbf{e}} \pmod{q}$$

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

# Learning With Error - LWE

## Variants

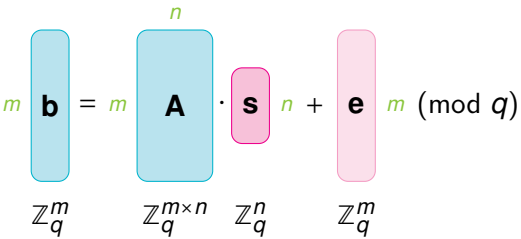


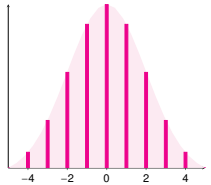



# Learning With Error - LWE

## Hardness

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



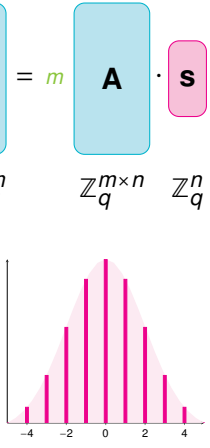




- Security based on worst-case lattices assumption for Gaussian error **e** [Regev05]

# Learning With Error - LWE

## Standardization

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



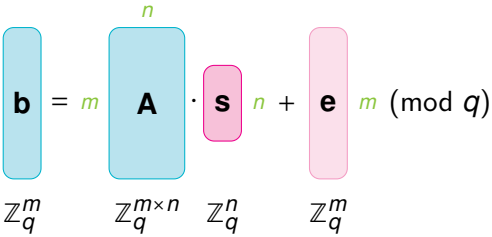


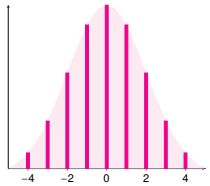


- Security based on worst-case lattices assumption for Gaussian error **e** [Regev05]
- Among 5 standards of the NIST, 3 are based on structured LWE variants

# Learning With Error - LWE

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

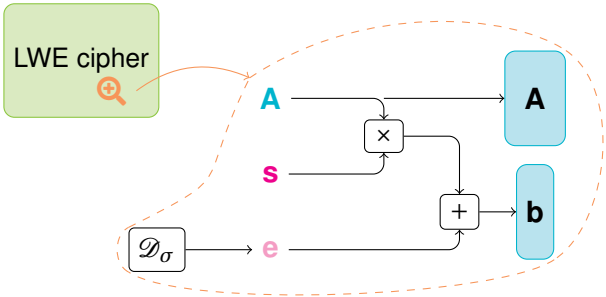



- Security based on worst-case lattices assumption for Gaussian error **e** [Regev05]
- Among 5 standards of the NIST, 3 are based on structured LWE variants

**What about physical attacks ?**

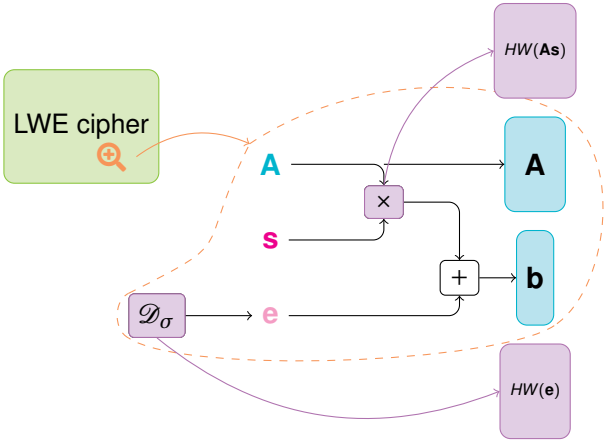
# Side-channel analysis




- power consumption
- timing
- electromagnetic emission
- acoustic emission

# Side-channel analysis

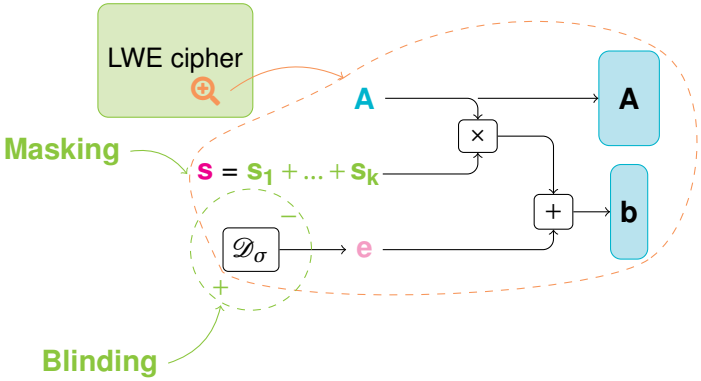
## Possible leakages




- non constant time operation
- sensible operation

# Side-channel analysis

## Countermeasures

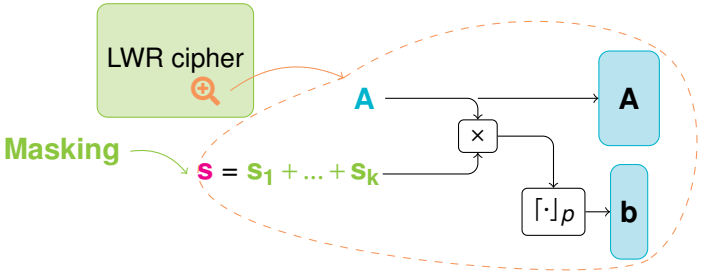



- Masking = share
- Blinding = randomize

**COSTLY**

# Side-channel analysis

## Countermeasures: avoiding blinding

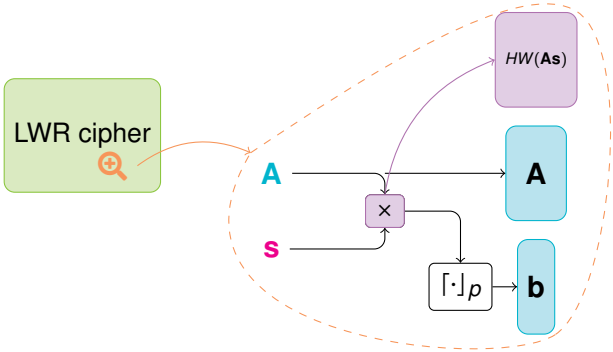



- LWE: $\mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e}$
- LWR: $\mathbf{b} = \lceil \mathbf{A}\mathbf{s} \rfloor_p$ [BPR12]

**New Assumption**

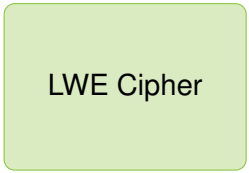
# Side-channel analysis

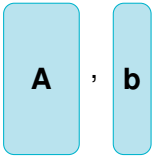
## Countermeasures: avoiding masking




**Relaxed Assumption**

# Hard Learning Problem from Side-channel analysis

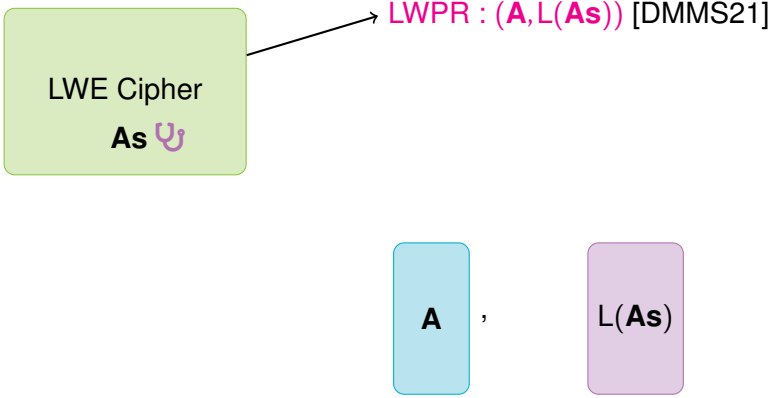


# Hard Learning Problem from Side-channel analysis

## Learning With Physical Rounding

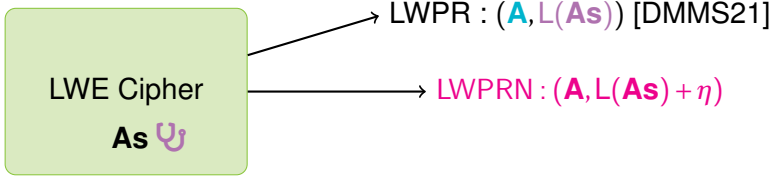
L = Leakage Function

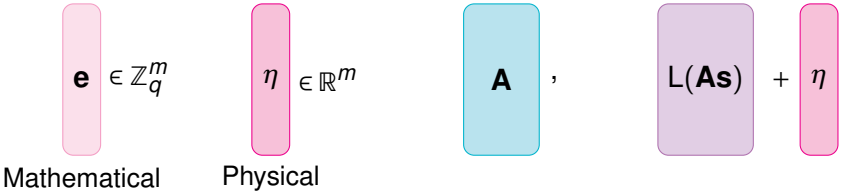


# Hard Learning Problem from Side-channel analysis

## Learning With Physical Rounding and Noises

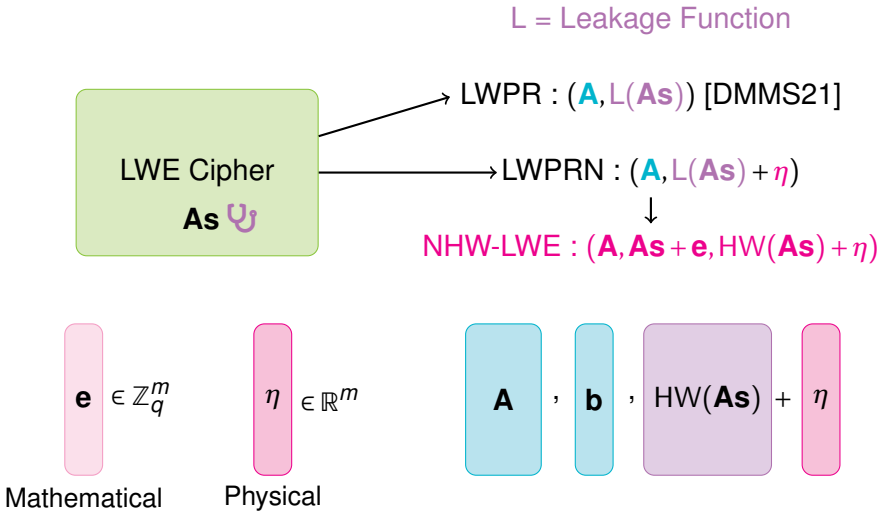
L = Leakage Function



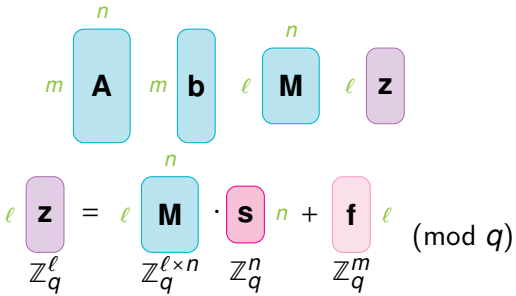
# Hard Learning Problem from Side-channel analysis

## Noisy Hamming Weight LWE



# LWE variants

**LWE with Hints** [KLSS23,LSW25]




## Choice of **M**

- Adversary
- (possibly) unstructured

# LWE variants

**LWE with Hints** [KLSS23,LSW25]

$$\underset{\mathbb{Z}_q^{\ell}}{\mathbf{z}} = \underset{\mathbb{Z}_q^{\ell\times n}}{\mathbf{M}} \cdot \underset{\mathbb{Z}_q^{n}}{\mathbf{s}} + \underset{\mathbb{Z}_q^{m}}{\mathbf{f}} \pmod q$$

**Entropic LWE** [BD20]

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

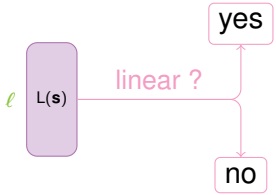
## Choice of **M**

- Adversary
- (possibly) unstructured

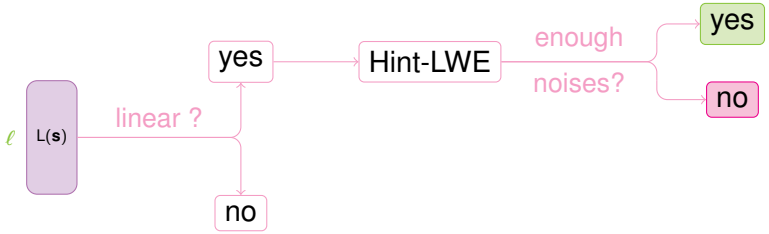
## Choice of $\mathscr{S}$

- Large entropy
- Short secret variant

# Considering additional leakage



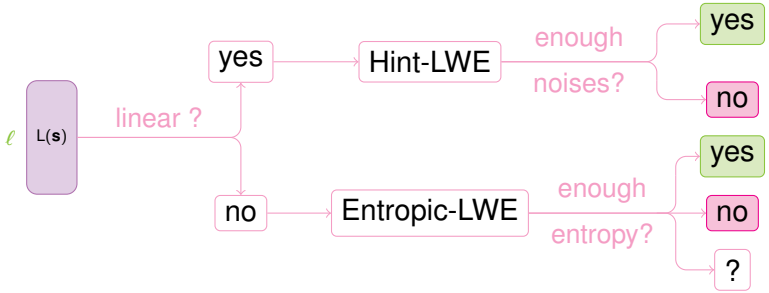
# Considering additional leakage




**Hard Problem**

**Easy Problem**

# Considering additional leakage




**Hard Problem**

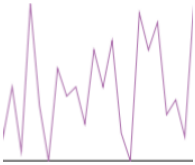
**Easy Problem**

# Summary

- We have

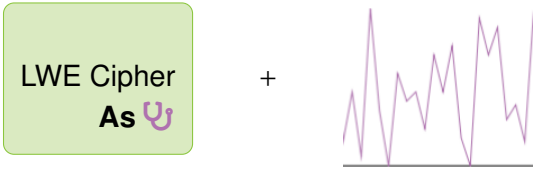
LWE Cipher
**As** 

+



# Summary

- We have




- We want

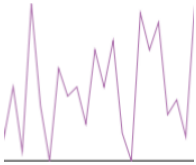

LWPRN hard

# Summary

- We have

LWE Cipher
**As** $\mathcal{U}$

+



- We want

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

LWPRN hard

- We study

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

hardness of NHW-LWE
under LWE assumption

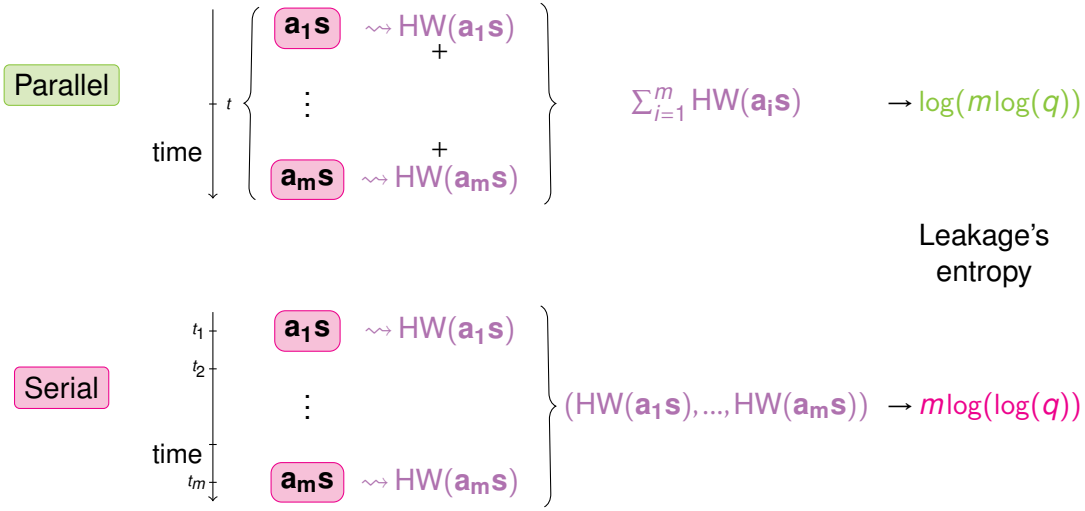
# Do variants apply to our case ?

Parallel


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

Leakage's entropy

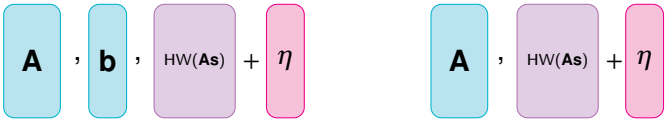
# Do variants apply to our case ?



# Results on Noisy Hamming Weight Learning With Error

## From NHW-LWE to LWPRN

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



# Results on Noisy Hamming Weight Learning With Error

## From LWE to NHW-LWE

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


- 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 $\Rightarrow$ NHW-LWE**

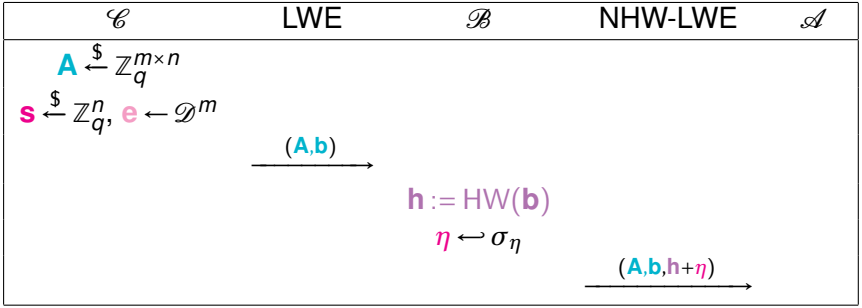
Construct $\mathscr{B}$ an adversary against LWE using $\mathscr{A}$ an adversary against NHW-LWE.

# Intuition of the reduction

## From LWE sample to NHW-LWE sample

**LWE ⇒ NHW-LWE**

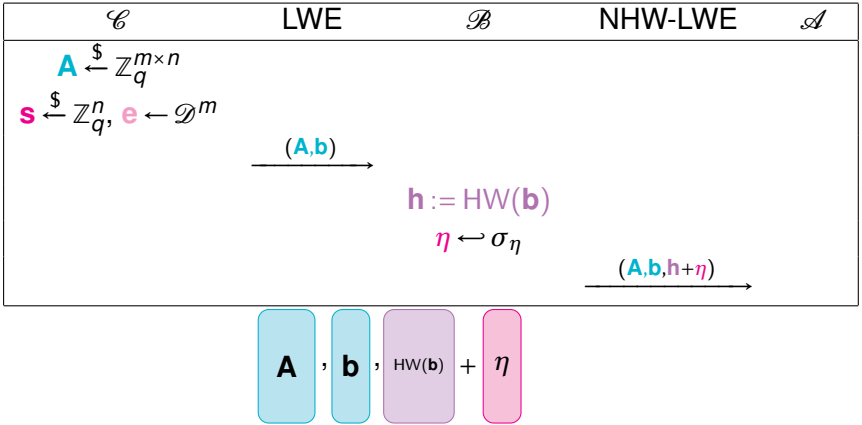
Construct $\mathscr{B}$ an adversary against LWE using $\mathscr{A}$ an adversary against NHW-LWE.



# Intuition of the reduction

## LWE ⇒ NHW-LWE

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

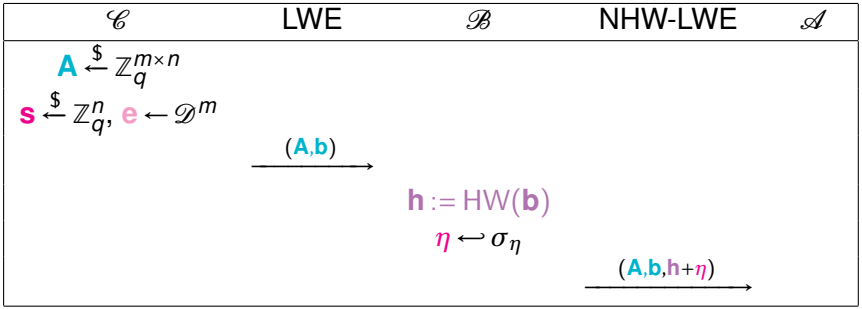


# Intuition of the reduction

## Rewriting HW(**b**)

**LWE ⇒ NHW-LWE**

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

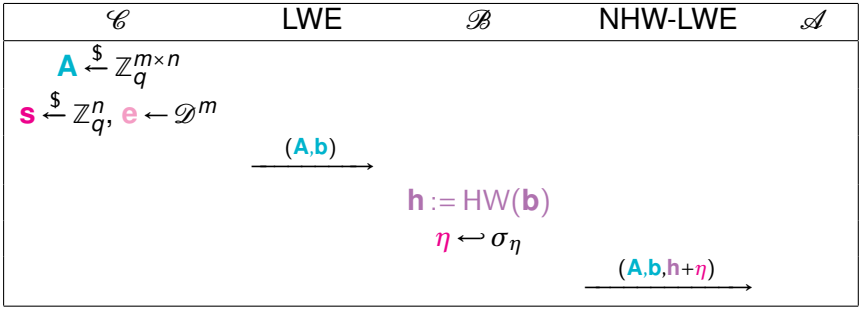


# Intuition of the reduction

## Masking $d$

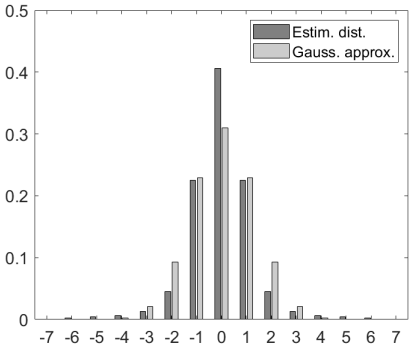
**LWE $\Rightarrow$ NHW-LWE**

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

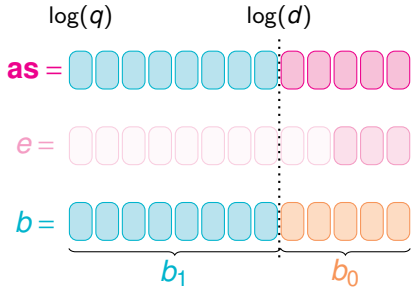


# From LWE sample to NHW-LWE sample

## Influence of the LWE error



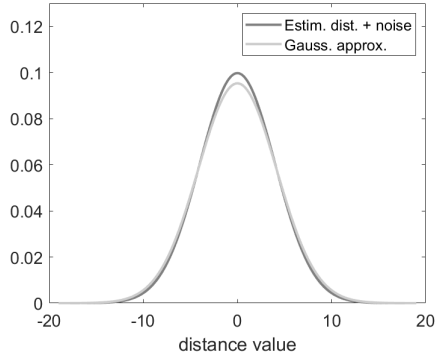

Difference HW(**b**) − HW(**As**) and its Gaussian approximation.



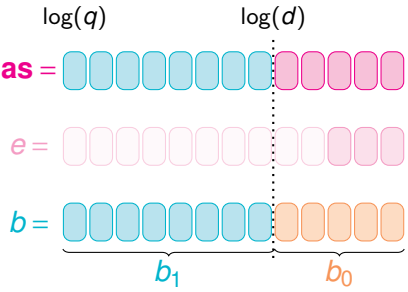

$$\mathrm{HW}(\mathbf{as}) = \mathrm{HW}(b_1) + \mathrm{HW}((\mathbf{as})_0)$$
$$= \mathrm{HW}(b) + d$$

# From LWE sample to NHW-LWE sample

## Masking this influence



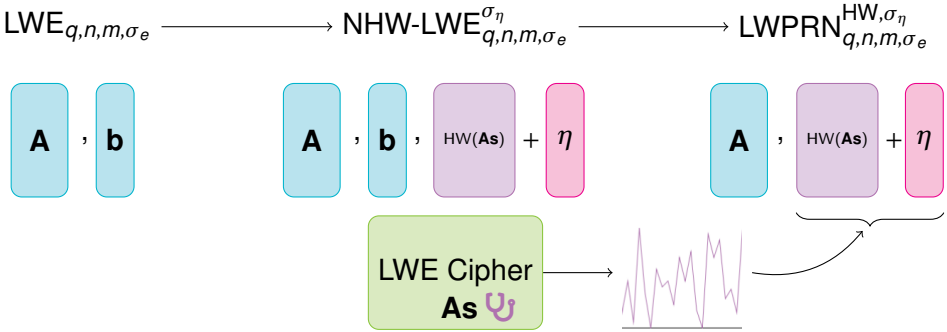

Difference $(\mathrm{HW}(\mathbf{b})+\eta)-(\mathrm{HW}(\mathbf{As})+\eta)$ and its Gaussian approximation.



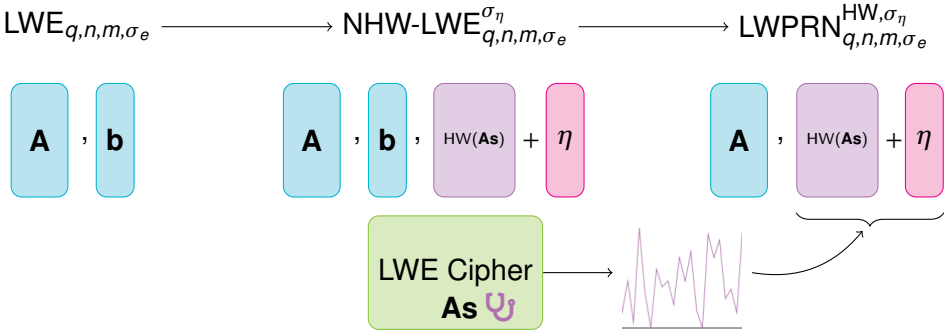

$$\mathrm{HW}(\mathbf{as})+\eta = \mathrm{HW}(b_1)+d+\eta$$
$$\approx \mathrm{HW}(b)+\eta$$

$\eta$ independent of $q$

# Conclusion and Open Problems

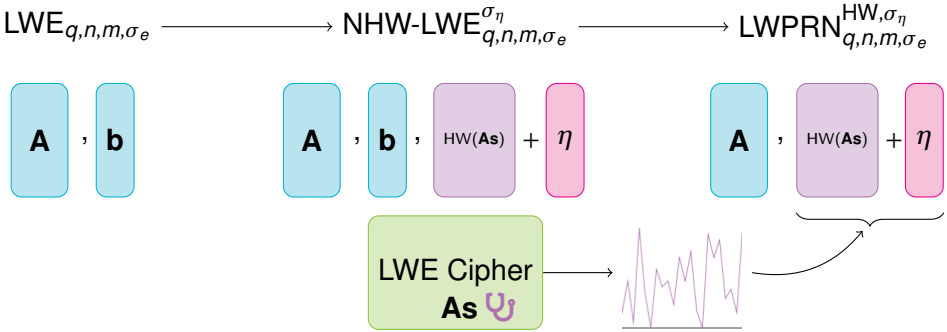


# Conclusion and Open Problems




- How can we better the bound $d$ knowing **A** ?
- Relaxation on masking ?

# Conclusion and Open Problems




- How can we better the bound $d$ knowing **A** ?
- Relaxation on masking ?

**Thank you for your attention !**