Hardness of Learning with Physical Rounding and Noise from Learning With Errors

C. Hoffmann[1] **E. Repel**[2] A. Roux-Langlois[2] F-X. Standaert[3]

[1]NTT Social Informatics Laboratories - Japan

[2]CNRS
Université de Caen Normandie - France

[3]UCLouvain
Université Catholique de Louvain - Belgium

October 2026





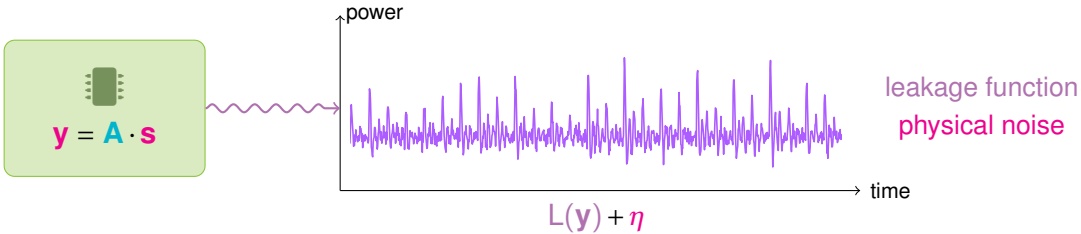






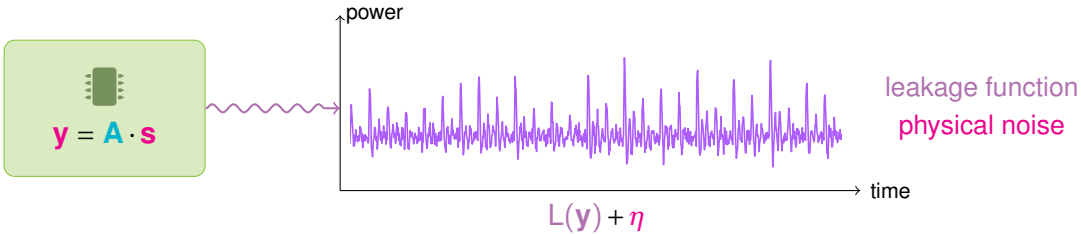
Physical security

Computations leak



Physical security

Classical answer: hide the computation



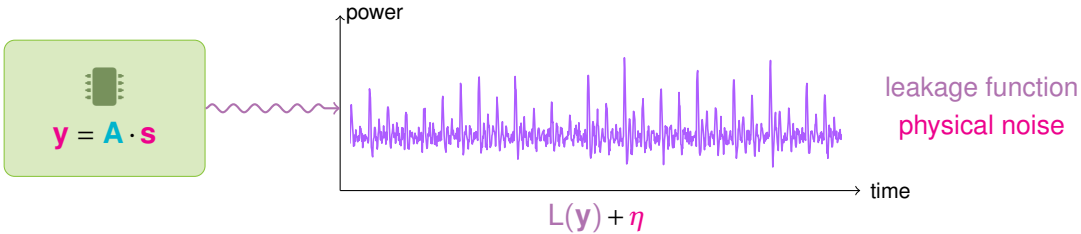
Masking

$\mathbf{y} \longrightarrow \mathbf{y}_1 \quad \mathbf{y}_2 \quad \cdots \quad \mathbf{y}_d$

✔ proofs ✖ cost $\sim d^2$

Physical security

Alternative: prove the leakage is hard to exploit



Masking

$\mathbf{y} \longrightarrow \mathbf{y}_1 \quad \mathbf{y}_2 \quad \cdots \quad \mathbf{y}_d$

✔ proofs ✖ cost $\sim d^2$

Hard physical learning problem

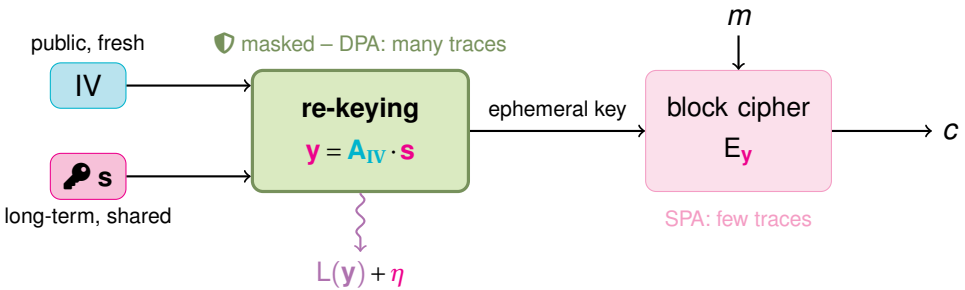
recovering $\mathbf{s}$ from $\mathsf{L}(\mathbf{y}) + \eta$
is **provably hard**

product protected ✔ $\mathbf{y}$ unprotected

Introduced for symmetric re-keying [DFHJMS16,DMMS21] · similar objects in PQ leakage analysis

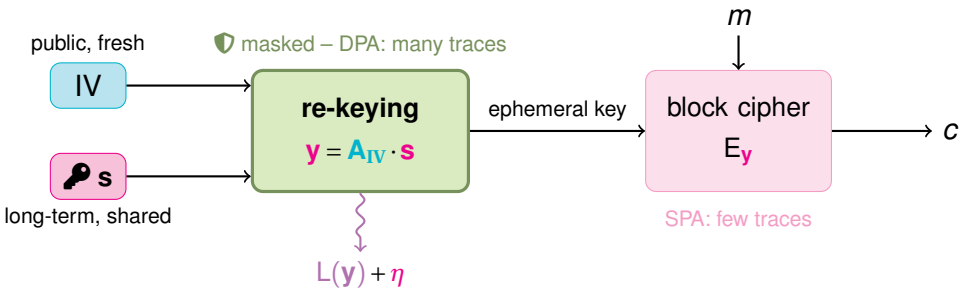
Applications

Symmetric: fresh re-keying



Applications

Post-quantum: public input × secret



POLKA – decryption [HLMPS23]

c_1 $\quad c_2 - \boxed{c_1 \cdot s}$

ciphertext × long-term secret key

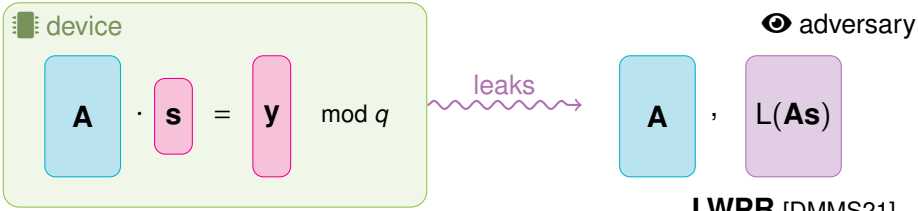
ML-DSA – signing

$\mathbf{A}$ $\quad \mathbf{w} = \boxed{\mathbf{A} \cdot \mathbf{y}}$

public matrix × ephemeral secret

Hard physical learning problems

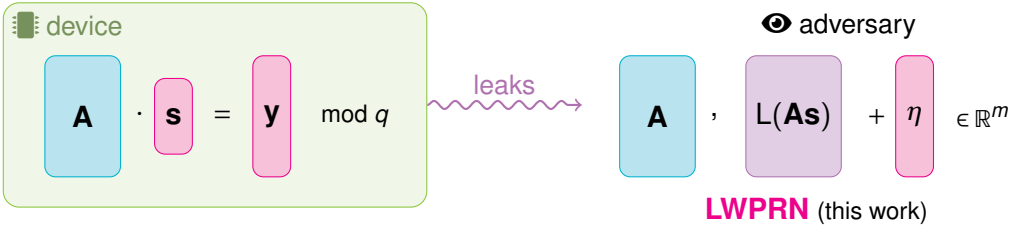
Learning With Physical Rounding



LWPR [DMMS21]

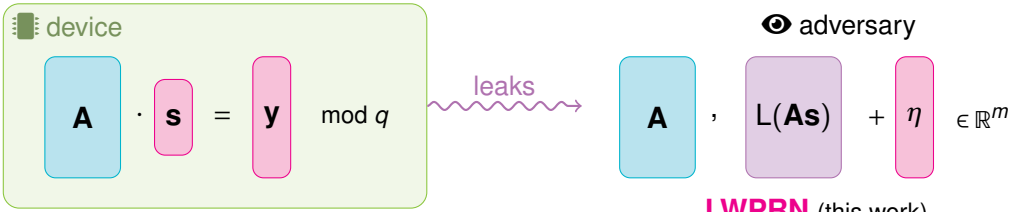
Hard physical learning problems

Learning With Physical Rounding and Noise



Hard physical learning problems

State of the art

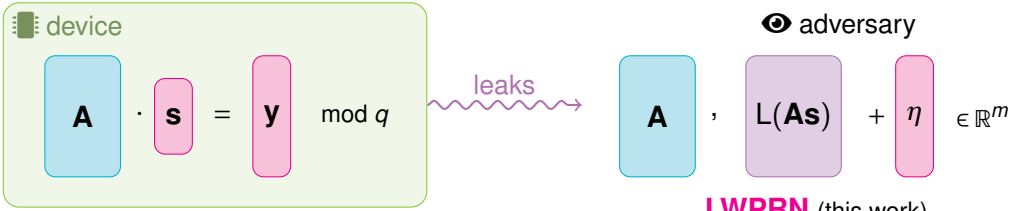


	field	noise	hardness	limitation
LPL [DFHJMS16]	$\mathbb{F}_2$	yes	✔ reduction from LPN	large noise
LWPR [DMMS21]	$\mathbb{Z}_q^*$	no	✘ cryptanalysis only	broken if serial

* q large prime

Hard physical learning problems

State of the art

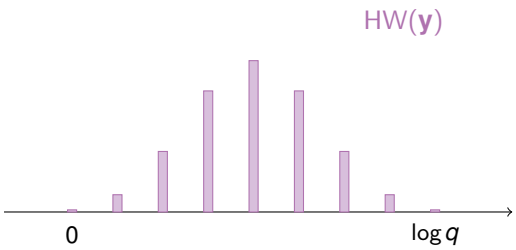


	field	noise	hardness	limitation
LPL [DFHJMS16]	$\mathbb{F}_2$	yes	✔ reduction from LPN	large noise
LWPR [DMMS21]	$\mathbb{Z}_q^*$	no	✘ cryptanalysis only	broken if serial
LWPRN (this work)	$\mathbb{Z}_q$	yes	**?**	**?**

* q large prime

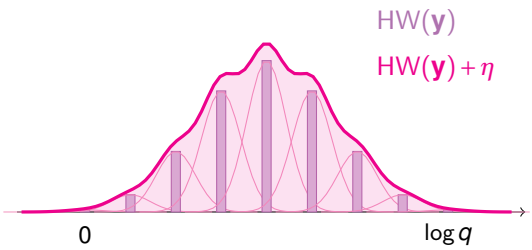
Is LWPRN as hard as LWE, with an affordable level of noise ?

Is LWPRN as hard as LWE, with an affordable level of noise ?



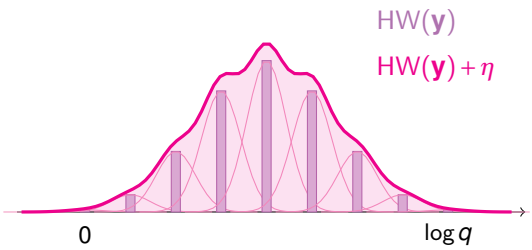
- **Leakage function**: HW

Is LWPRN as hard as LWE, with an affordable level of noise ?



- **Leakage function**: HW
- **Noise**: Gaussian over $\mathbb{R}$

Is LWPRN as hard as LWE, with an affordable level of noise ?

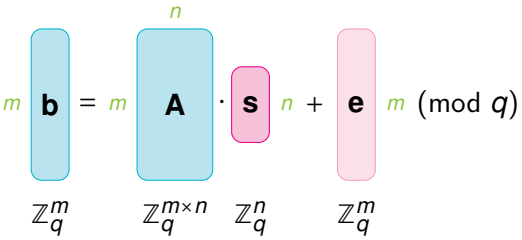


- **Leakage function**: HW
- **Noise**: Gaussian over $\mathbb{R}$
- **Adversary**: m samples

$$\begin{array}{ll} \mathbf{a}_1 & \mathrm{HW}(\langle \mathbf{a}_1, \mathbf{s} \rangle) + \eta_1 \\ \mathbf{a}_2 & \mathrm{HW}(\langle \mathbf{a}_2, \mathbf{s} \rangle) + \eta_2 \\ \vdots & \end{array} \quad \rightarrow \text{find } \mathbf{s}$$

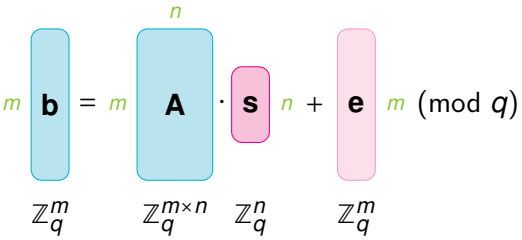
Learning With Error - LWE

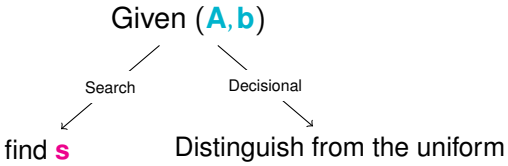
Standardization



Learning With Error - LWE

Variants

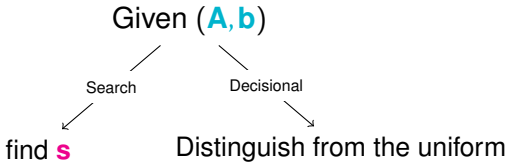


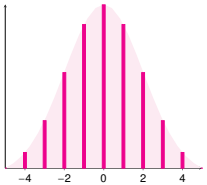


Learning With Error - LWE

Hardness

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

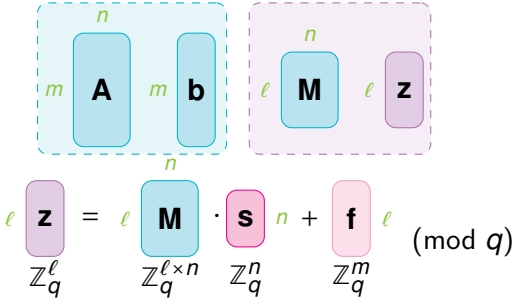




- Security based on worst-case lattices assumption for Gaussian error **e** [Regev05]

LWE variants

LWE with Hints [KLSS23,LSW25]

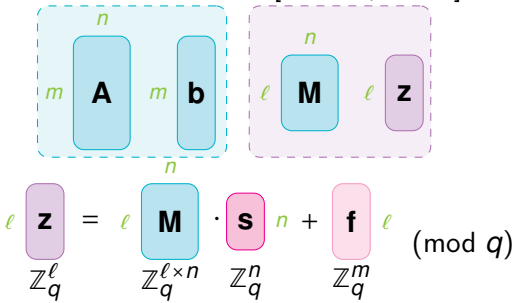


Choice of **M**

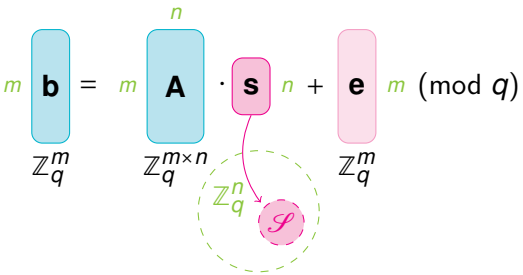
- Adversary
- (possibly) unstructured

LWE variants

LWE with Hints [KLSS23,LSW25]



Entropic LWE [BD20]



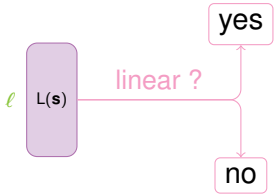
Choice of **M**

- Adversary
- (possibly) unstructured

Choice of $\mathscr{S}$

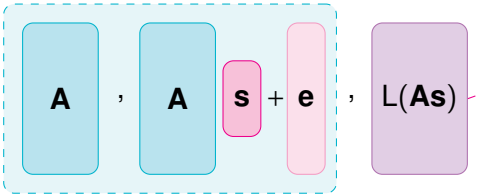
- Large entropy
- Short secret variant

Considering additional leakage

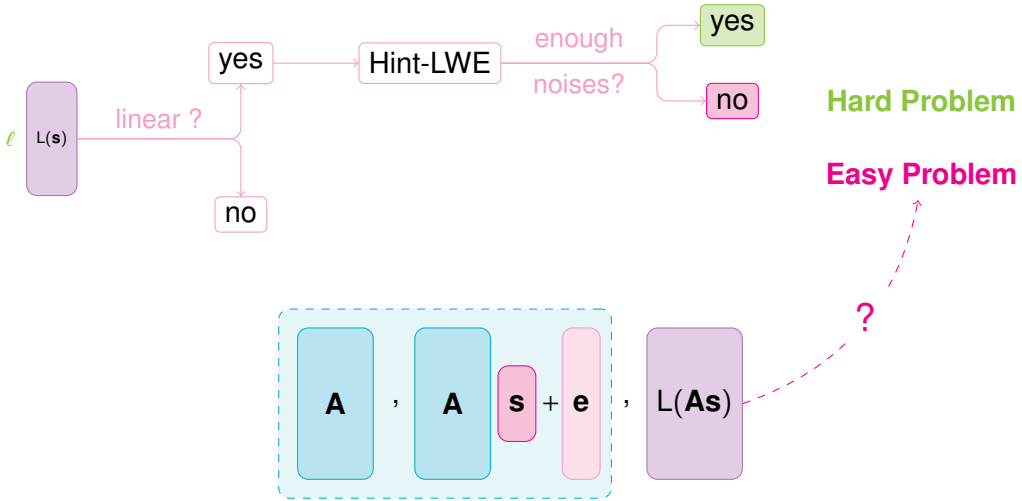


Hard Problem

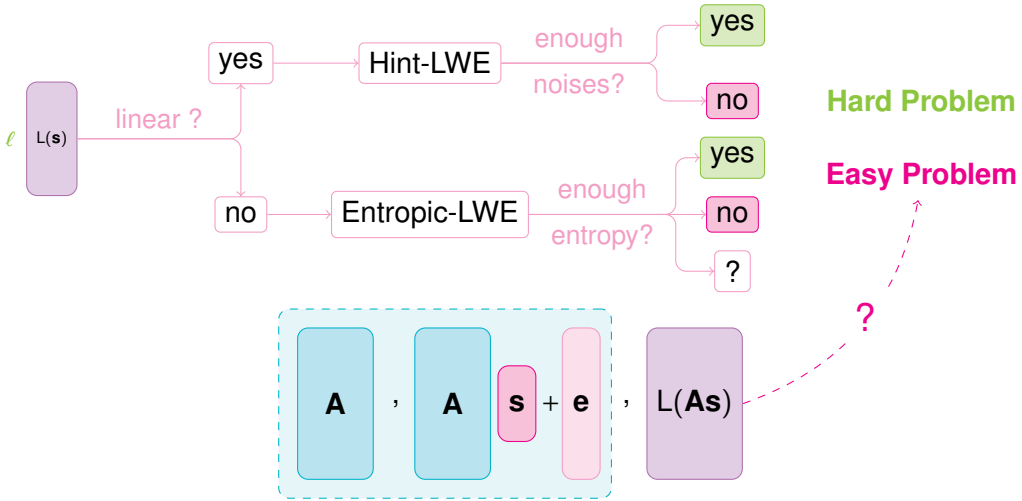
Easy Problem



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



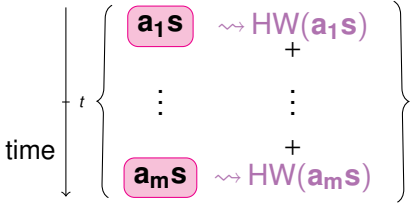
$\sum_{i=1}^{m} \mathrm{HW}(\mathbf{a_i s})$ $\rightarrow \log(m \log(q))$

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

Leakage's entropy

Do variants apply to our case ?

Parallel

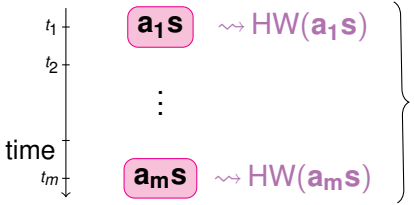


$\sum_{i=1}^{m}$ HW($\mathbf{a_i s}$) $\rightarrow \log(m\log(q))$

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

Leakage's entropy

Serial

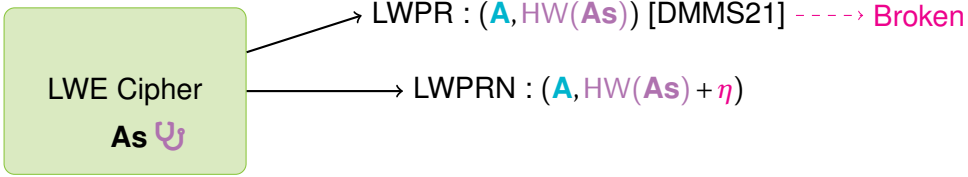


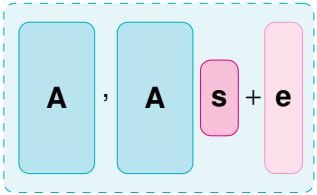
(HW($\mathbf{a_1 s}$),...,HW($\mathbf{a_m s}$)) $\rightarrow m\log(\log(q))$

Already broken [DMMS21,HMM+23]

Hard Learning Problem from Side-channel analysis

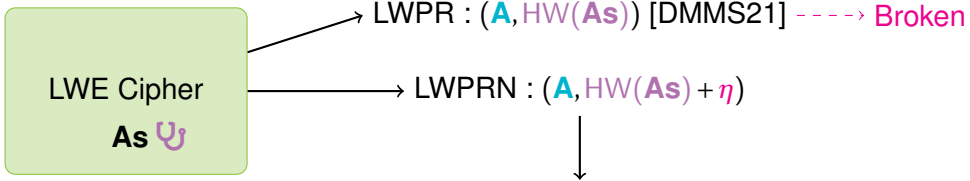
Noisy Hamming Weight LWE





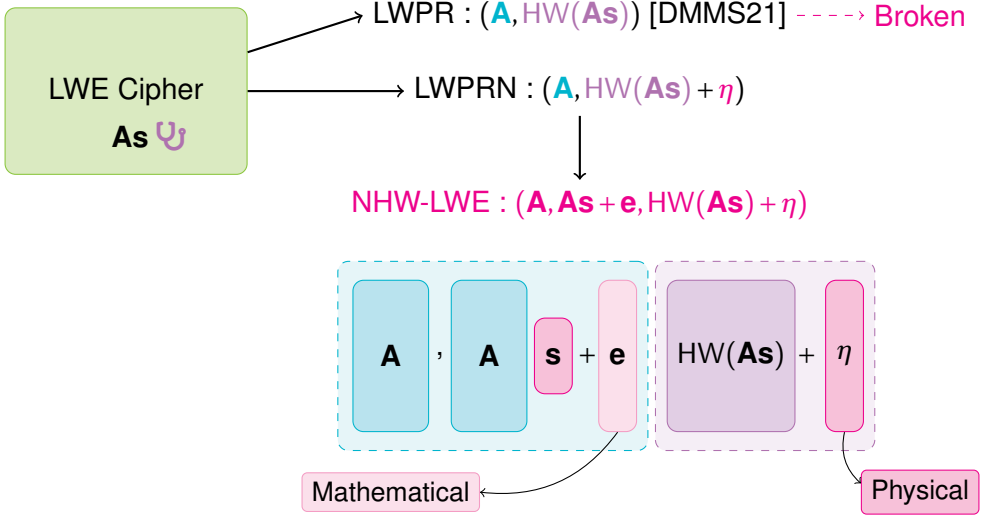
Hard Learning Problem from Side-channel analysis

Noisy Hamming Weight LWE



Hard Learning Problem from Side-channel analysis

Noisy Hamming Weight LWE

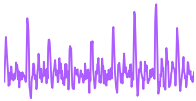


Summary

- We have

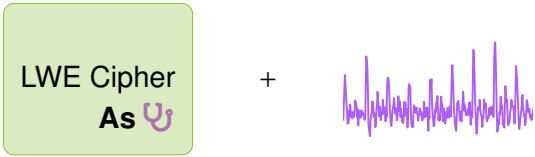
LWE Cipher
As 

+



Summary

- We have



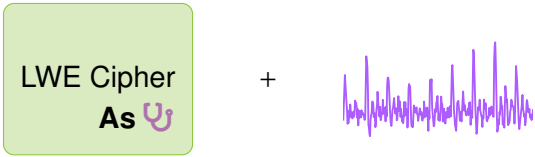
- We want



LWPRN hard

Summary

- We have

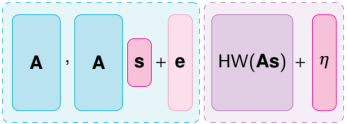


- We want



LWPRN hard

- We study

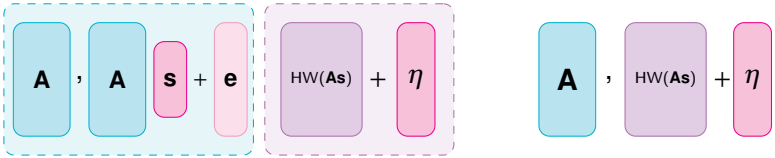


hardness of NHW-LWE under LWE assumption

Results on Noisy Hamming Weight Learning With Error

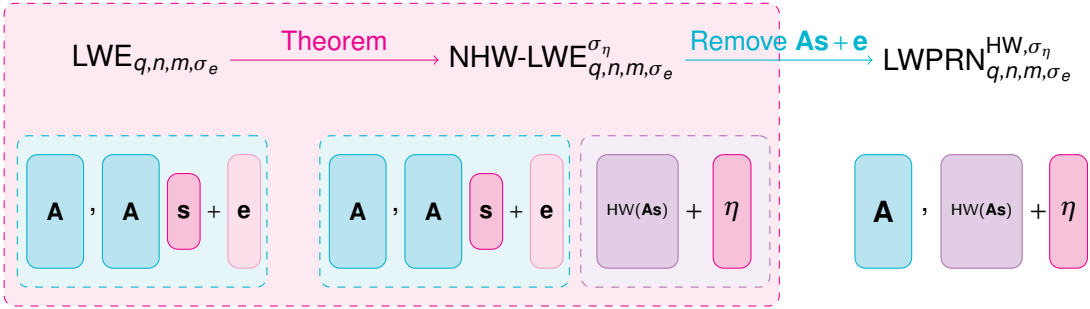
From NHW-LWE to LWPRN

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



Results on Noisy Hamming Weight Learning With Error

From LWE to NHW-LWE

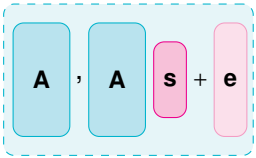


- Statistical distance: $\frac{\lceil \log_2(\sqrt{\lambda}\sigma_e)\rceil}{\sigma_\eta} \leqslant \varepsilon$
- Rényi divergence: $\sigma_\eta \geqslant \sqrt{m}\lceil \log_2(\sqrt{\lambda}\sigma_e)\rceil$

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.



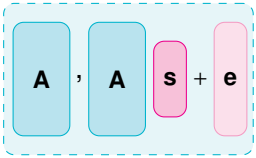
Intuition of the reduction

From LWE sample to NHW-LWE sample

LWE ⇒ NHW-LWE : showing the contraposition

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

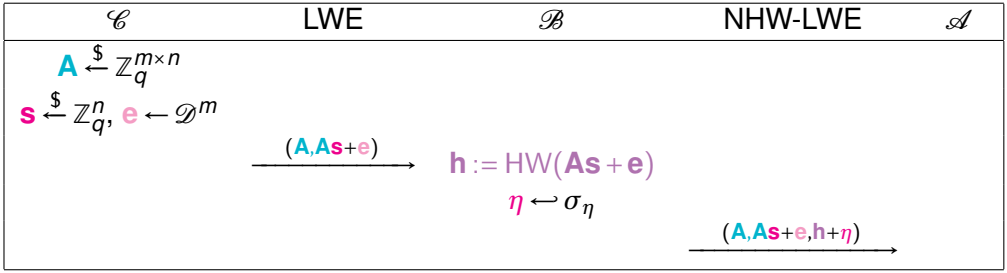
$\mathscr{C}$	LWE	$\mathscr{B}$	NHW-LWE	$\mathscr{A}$
$\mathbf{A} \xleftarrow{\$} \mathbb{Z}_q^{m \times n}$ $\mathbf{s} \xleftarrow{\$} \mathbb{Z}_q^n$, $\mathbf{e} \leftarrow \mathscr{D}^m$	$\xrightarrow{(\mathbf{A}, \mathbf{As}+\mathbf{e})}$	$\mathbf{h} := \mathrm{HW}(\mathbf{As}+\mathbf{e})$ $\eta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

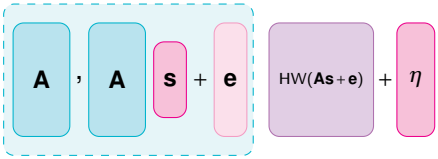


Intuition of the reduction

LWE ⇒ NHW-LWE : showing the contraposition

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





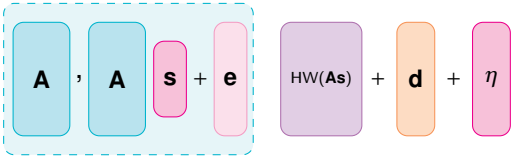
Intuition of the reduction

Rewriting HW(**b**)

LWE ⇒ NHW-LWE : showing the contraposition

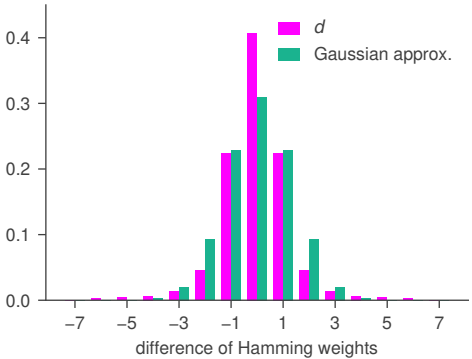
Construct $\mathscr{B}$ an adversary against LWE using $\mathscr{A}$ an adversary against NHW-LWE.

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

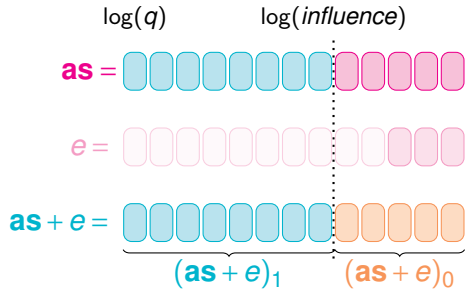


From LWE sample to NHW-LWE sample

Influence of the LWE error



Difference $d = \mathrm{HW}(\mathbf{as} + e) - \mathrm{HW}(\mathbf{As})$
and its Gaussian approximation.



$$\begin{aligned}\mathrm{HW}(\mathbf{as}) &= \mathrm{HW}((\mathbf{as}+e)_1) + \mathrm{HW}((\mathbf{as})_0) \\ &= \mathrm{HW}(\mathbf{as}+e) + d\end{aligned}$$

Link with side-channel security

How much noise do we really need ?

Theorem

$$\sigma_\eta \gg \lceil \log_2(\sqrt{\lambda}\sigma_e) \rceil$$

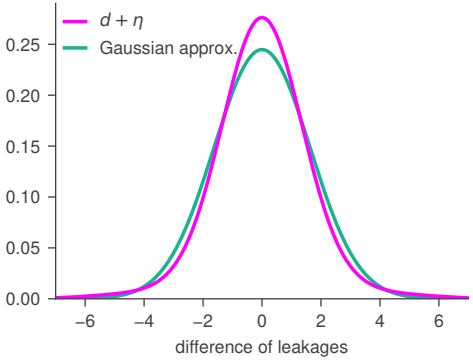
hides the **worst-case** d

→ pessimistic

$d = \mathrm{HW}(\mathbf{As}+\mathbf{e}) - \mathrm{HW}(\mathbf{As})$ change of leakage caused by the LWE error $\mathbf{e}$

Link with side-channel security

What must really be hidden

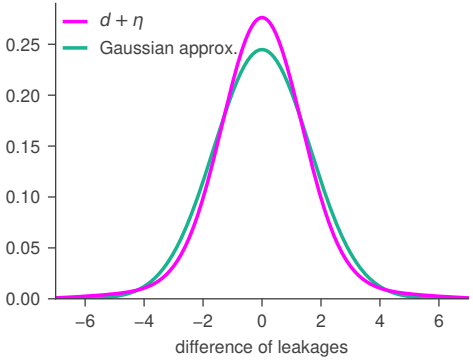


$d + \eta$ vs. Gaussian

$d = \mathrm{HW}(\mathbf{As} + \mathbf{e}) - \mathrm{HW}(\mathbf{As})$ change of leakage caused by the LWE error $\mathbf{e}$

Link with side-channel security

Comparing the moments



$d+\eta$ vs. Gaussian

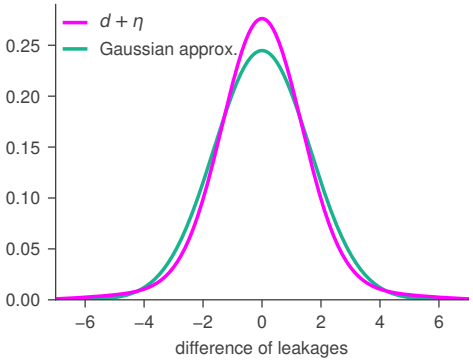
statistical moment

1	mean	= by construction
2	variance	= by construction
3	skewness	= symmetry

Proposition. $\mathrm{f}(U+E)-\mathrm{f}(U)$ is symmetric for **any** f (U uniform, E symmetric)

Link with side-channel security

Comparing the moments



$d+\eta$ vs. Gaussian

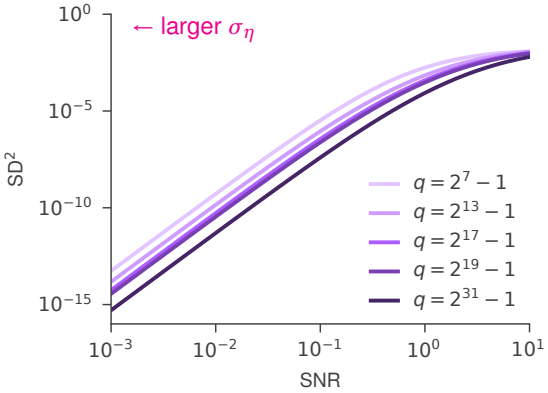
statistical moment

1	mean	$=$ by construction
2	variance	$=$ by construction
3	skewness	$=$ symmetry
4	**kurtosis**	$\neq$ first difference

Proposition. $\mathrm{f}(U+E)-\mathrm{f}(U)$ is symmetric for **any** f (U uniform, E symmetric)

Link with side-channel security

How many samples to tell $d + \eta$ from a Gaussian ?



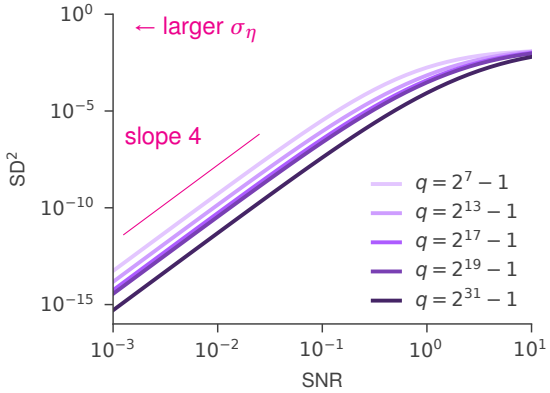
SD = statistical distance · SNR $= \mathrm{Var}(\mathrm{HW}) / \sigma_\eta^2$

#samples to distinguish $\approx 1/\mathrm{SD}^2$

information theory

Link with side-channel security

Noise amplification



SD = statistical distance · SNR = $\mathrm{Var}(\mathrm{HW}) / \sigma_\eta^2$

#samples to distinguish $\approx 1/\mathrm{SD}^2$

information theory

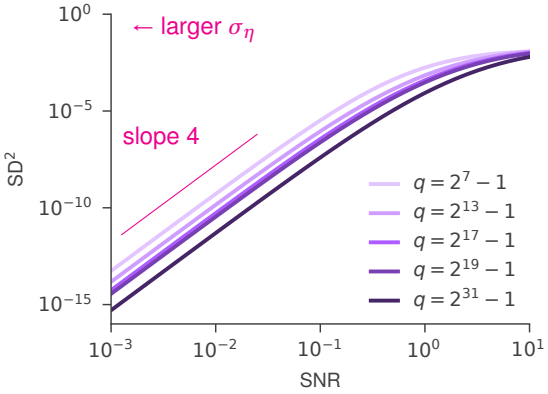
Here (unmasked)

#samples $\propto (\sigma_\eta^2)^{\mathbf{4}}$

numerical, explained by the moments

Link with side-channel security

Same trend as 4th-order masking



SD = statistical distance · SNR $= \mathrm{Var}(\mathrm{HW}) / \sigma_\eta^2$

#samples to distinguish $\approx 1/\mathrm{SD}^2$

information theory

Here (unmasked)

#samples $\propto (\sigma_\eta^2)^{\mathbf{4}}$

numerical, explained by the moments

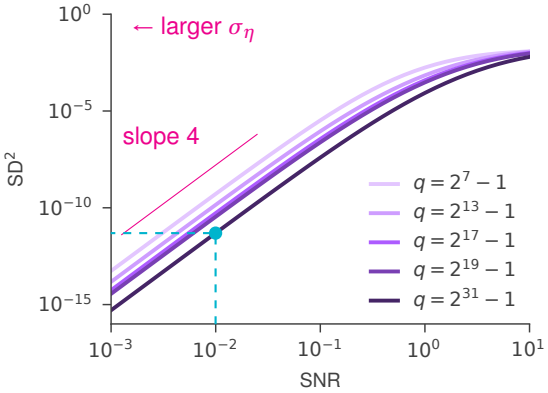
Masking, order d

#traces $\propto (\sigma_\eta^2)^d$

conjectured [DFS19], proven [MRS22]

Link with side-channel security

Concretely



SD = statistical distance · SNR $= \mathrm{Var}(\mathrm{HW}) / \sigma_\eta^2$

SNR $= 10^{-2}$, $q = 2^{31} - 1$ → $\approx 10^{12}$ samples

#samples to distinguish $\approx 1/\mathrm{SD}^2$

information theory

Here (unmasked)

#samples $\propto (\sigma_\eta^2)^{\mathbf{4}}$

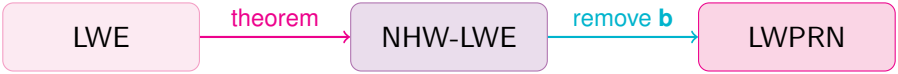
numerical, explained by the moments

Masking, order d

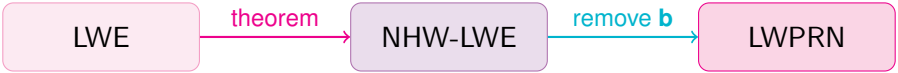
#traces $\propto (\sigma_\eta^2)^d$

conjectured [DFS19], proven [MRS22]

Conclusion



Conclusion

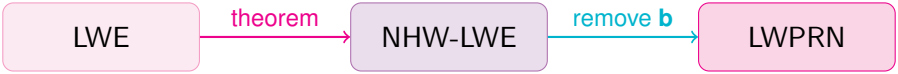


✔ First reduction for physical rounding (serial case included)

✔ Noise level independent of q

✔ Noise amplified as in 4th-order masking

Conclusion



✔ First reduction for physical rounding (serial case included)

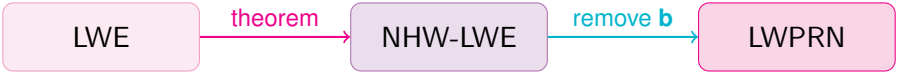
✔ Noise level independent of q

✔ Noise amplified as in 4th-order masking

Follow-up

decisional variant via Entropic-LWE (under submission)

Conclusion



✔ First reduction for physical rounding (serial case included)

✔ Noise level independent of q

✔ Noise amplified as in 4th-order masking

Follow-up

decisional variant via Entropic-LWE (under submission)

Open

algebraic complexity + noise flooding → ?

LWPR, heuristic — LWPRN, this work