

Cryptography: from the Mind to the Chip

Katharina Boudgoust, Loïc Masure

HCERES, 8 October 2025, Montpellier



Content

Intro Cryptography

Lattice Cryptography

Lattice Challenges

Crypto on the Chip

Provable Material Security

Cryptography

The word *cryptography* is composed of the two ancient Greek words *kryptos* (hidden) and *graphein* (to write). Its goal is to provide *secure communication*.

- Encryption
- Digital Signatures



Cryptography

The word *cryptography* is composed of the two ancient Greek words *kryptos* (hidden) and *graphein* (to write). Its goal is to provide *secure communication*.

- Encryption
- Digital Signatures
- Zero-Knowledge Proofs
- Fully-Homomorphic Encryption



5	3		7			
6			1	9	5	
	9	8				6
8			6			3
4			8	3		1
7			2			6
	6				2	8
			4	1	9	5
			8		7	9



Security Paradigm

The security in cryptography relies on presumably hard mathematical problems.

Currently used problems:

- Discrete logarithm
- Factoring

Given N , find p, q such that

$$N = p \cdot q$$

¹Shor, “Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer”

Security Paradigm

The security in cryptography relies on presumably hard mathematical problems.

Currently used problems:

- Discrete logarithm
- Factoring

Given N , find p, q such that
 $N = p \cdot q$

Quantum-resistant candidates:

- Codes
- Lattices
- Isogenies
- Multivariate systems
- ?

⚠ $\exists$ quantum algorithm¹

¹Shor, “Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer”

Security Paradigm

The security in cryptography relies on presumably hard mathematical problems.

Currently used problems:

- Discrete logarithm
- Factoring

Given N , find p, q such that
 $N = p \cdot q$

⚠ $\exists$ quantum algorithm¹

Quantum-resistant candidates:

- Codes
- Lattices $\Rightarrow$ today's focus
- Isogenies
- Multivariate systems
- ?

¹Shor, "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer"

Post-Quantum Standardization Project

- 2016: start of NIST's post-quantum cryptography project²
- 2022+25: selection of 5 schemes, 3 of them relying on lattice problems

Public Key Encryption:

- Kyber
- HQC

Digital Signature:

- Dilithium
- Falcon
- SPHINCS+

Lattice-based cryptography plays a leading role in designing post-quantum cryptography.

²<https://csrc.nist.gov/projects/post-quantum-cryptography>

Lattices Can Do Much More!

Example: Fully-Homomorphic Encryption

- Securely outsource data and do analysis on the encrypted data
- Very powerful
- Only known from lattices so far

Content

Intro Cryptography

Lattice Cryptography

Lattice Challenges

Crypto on the Chip

Provable Material Security

Learning With Errors

- Introduced by Regev³
- Most important hardness assumption in lattice-based cryptography
- Informal: solve random noisy linear equations over finite fields

³Regev, “On lattices, learning with errors, random linear codes, and cryptography”

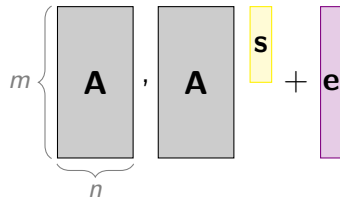
Learning With Errors

Let $\mathbb{Z}_q$ be a finite field.

Sample matrix $\mathbf{A} \in \mathbb{Z}_q^{m \times n}$ uniformly at random.

Set $\mathbf{b} \in \mathbb{Z}_q^m$, where $\mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e} \bmod q$ for

- secret $\mathbf{s} \in \mathbb{Z}_q^n$ sampled from distribution D_s
- noise/error $\mathbf{e} \in \mathbb{Z}^m$ sampled from distribution D_e such that $\|\mathbf{e}\|_2 \leq \delta \ll q$.



Learning With Errors

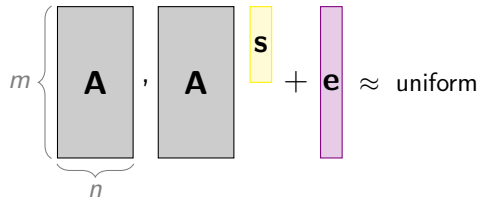
Let $\mathbb{Z}_q$ be a finite field.

Sample matrix $\mathbf{A} \in \mathbb{Z}_q^{m \times n}$ uniformly at random.

Set $\mathbf{b} \in \mathbb{Z}_q^m$, where $\mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e} \bmod q$ for

- secret $\mathbf{s} \in \mathbb{Z}_q^n$ sampled from distribution D_s
- noise/error $\mathbf{e} \in \mathbb{Z}^m$ sampled from distribution D_e such that $\|\mathbf{e}\|_2 \leq \delta \ll q$.

Learning with errors (LWE) asks to distinguish $(\mathbf{A}, \mathbf{b})$ from the uniform distribution over $\mathbb{Z}_q^{m \times n} \times \mathbb{Z}_q^m$.



Learning With Errors

Let $\mathbb{Z}_q$ be a finite field.

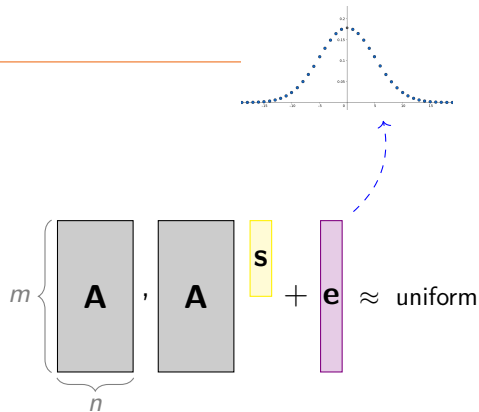
Sample matrix $\mathbf{A} \in \mathbb{Z}_q^{m \times n}$ uniformly at random.

Set $\mathbf{b} \in \mathbb{Z}_q^m$, where $\mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e} \bmod q$ for

- secret $\mathbf{s} \in \mathbb{Z}_q^n$ sampled from distribution D_s
- noise/error $\mathbf{e} \in \mathbb{Z}^m$ sampled from distribution D_e such that $\|\mathbf{e}\|_2 \leq \delta \ll q$.

Learning with errors (LWE) asks to distinguish $(\mathbf{A}, \mathbf{b})$ from the uniform distribution over $\mathbb{Z}_q^{m \times n} \times \mathbb{Z}_q^m$.

⚠ The norm restriction on $\mathbf{e}$ makes LWE a hard problem.



Reminder: Encryption

An encryption scheme $\Pi = (\text{KeyGen}, \text{Enc}, \text{Dec})$ consists of three algorithms:

- $\text{KeyGen} \rightarrow \text{sk}$
- $\text{Enc}(\text{sk}, m) \rightarrow \text{ct}$
- $\text{Dec}(\text{sk}, \text{ct}) = m'$

Correctness: $\text{Dec}(\text{sk}, \text{Enc}(\text{sk}, m)) = m$ during an honest execution

Security: $\text{Enc}(\text{sk}, m_0)$ is indistinguishable from $\text{Enc}(\text{sk}, m_1)$

Encryption from LWE

Let D_s and D_e be secret and error distributions and $\mathbb{Z}_q$ be a finite field.

KeyGen:

Output $\mathbf{s} \leftarrow D_s$

Enc($\mathbf{s}, m \in \{0, 1\}^n$):

$\mathbf{A} \leftarrow \text{Unif}(\mathbb{Z}_q^{n \times n})$

$\mathbf{e} \leftarrow D_e$

$\mathbf{u} = \mathbf{A}\mathbf{s} + \mathbf{e} + \lfloor q/2 \rfloor \cdot m \bmod q$

Output $(\mathbf{A}, \mathbf{u})$

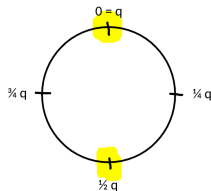
Dec($\mathbf{s}, \mathbf{A}, \mathbf{u}$):

For every coefficient of $\mathbf{u} - \mathbf{A}\mathbf{s}$:

If closer to 0 than to $q/2$,

output 0

Else output 1



Encryption from LWE

Let D_s and D_e be secret and error distributions and $\mathbb{Z}_q$ be a finite field.

KeyGen:

Output $\mathbf{s} \leftarrow D_s$

Enc($\mathbf{s}, m \in \{0, 1\}^n$):

$\mathbf{A} \leftarrow \text{Unif}(\mathbb{Z}_q^{n \times n})$

$\mathbf{e} \leftarrow D_e$

$\mathbf{u} = \mathbf{As} + \mathbf{e} + \lfloor q/2 \rfloor \cdot m \bmod q$

Output $(\mathbf{A}, \mathbf{u})$

Dec($\mathbf{s}, \mathbf{A}, \mathbf{u}$):

For every coefficient of $\mathbf{u} - \mathbf{As}$:

If closer to 0 than to $q/2$,

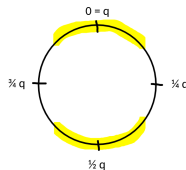
output 0

Else output 1

Correctness:

$$\begin{aligned} \mathbf{u} - \mathbf{As} &= \mathbf{As} + \mathbf{e} + \lfloor q/2 \rfloor \cdot m - \mathbf{As} \\ &= \mathbf{e} + \lfloor q/2 \rfloor m \end{aligned}$$

Decryption succeeds if $\|\mathbf{e}\|_\infty < q/8$



Encryption from LWE 2/2

Let D_s and D_e be secret and error distributions and $\mathbb{Z}_q$ be a finite field.

KeyGen:

Output $\mathbf{s} \leftarrow D_s$

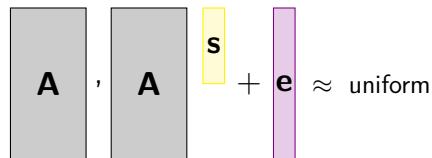
Enc($\mathbf{s}, m \in \{0, 1\}^n$):

$\mathbf{A} \leftarrow \text{Unif}(\mathbb{Z}_q^{n \times n})$

$\mathbf{e} \leftarrow D_e$

$\mathbf{u} = \mathbf{A}\mathbf{s} + \mathbf{e} + \lfloor q/2 \rfloor \cdot m \bmod q$

Output $(\mathbf{A}, \mathbf{u})$



Security:

- Assume hardness of LWE
- m hidden by LWE instance

Content

Intro Cryptography

Lattice Cryptography

Lattice Challenges

Crypto on the Chip

Provable Material Security

Challenges from Encryption

KeyGen:

Output $\mathbf{s} \leftarrow D_s$

Enc($\mathbf{s}, m \in \{0, 1\}^n$):

$\mathbf{A} \leftarrow \text{Unif}(\mathbb{Z}_q^{n \times n})$

$\mathbf{e} \leftarrow D_e$

$\mathbf{u} = \mathbf{A}\mathbf{s} + \mathbf{e} + \lfloor q/2 \rfloor \cdot m \bmod q$

Output $(\mathbf{A}, \mathbf{u})$

Dec($\mathbf{s}, \mathbf{A}, \mathbf{u}$):

For every coefficient of

$\mathbf{u} - \mathbf{A}\mathbf{s} \bmod q$:

If closer to 0 than to $q/2$, output 0

Else output 1

- Difficult to distribute calculation among multiple people⁴
- Difficult to protect against side-channel attacks (ongoing work)

⁴Boudgoust and Scholl, “Simple Threshold (Fully Homomorphic) Encryption from LWE with Polynomial Modulus”, AC’23.

Content

Intro Cryptography

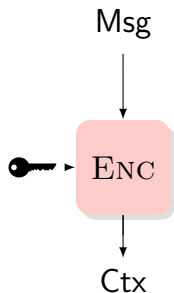
Lattice Cryptography

Lattice Challenges

Crypto on the Chip

Provable Material Security

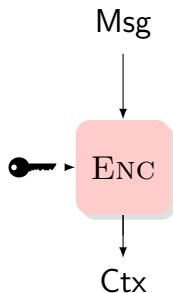
Context : Side-Channel Analysis (SCA)



Black-box security: (Msg, Ctx) indist. from random?

Context : Side-Channel Analysis (SCA)

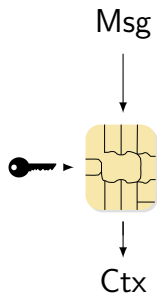
“Cryptographic algorithms don’t run on paper,



Black-box security: (Msg, Ctx) indist. from random?

Context : Side-Channel Analysis (SCA)

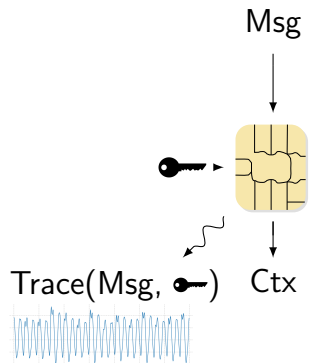
“Cryptographic algorithms don’t run on paper, they run on physical devices”



Black-box security: (Msg, Ctx) indist. from random?

Context : Side-Channel Analysis (SCA)

“Cryptographic algorithms don’t run on paper, they run on physical devices”

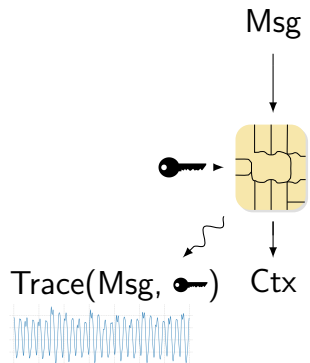


Black-box security: (Msg, Ctx) indist. from random?

Trace : power, EM, acoustics, runtime, ...

Context : Side-Channel Analysis (SCA)

“Cryptographic algorithms don’t run on paper, they run on physical devices”



Black-box security: (Msg, Ctx) indist. from random?

SCA: (Msg, Ctx, Trace) indist. from random?

Trace : power, EM, acoustics, runtime, ...

Content

Intro Cryptography

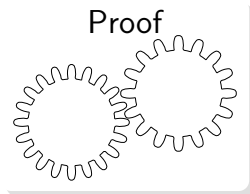
Lattice Cryptography

Lattice Challenges

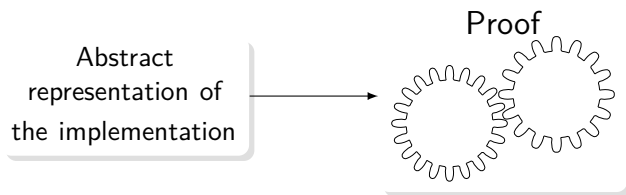
Crypto on the Chip

Provable Material Security

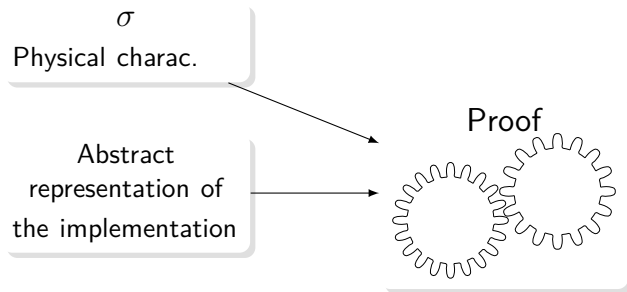
Security Proof



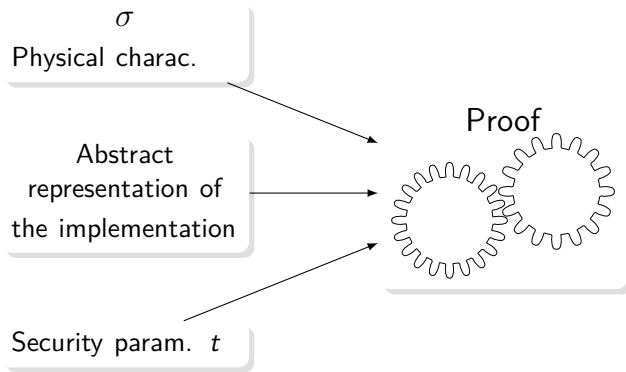
Security Proof



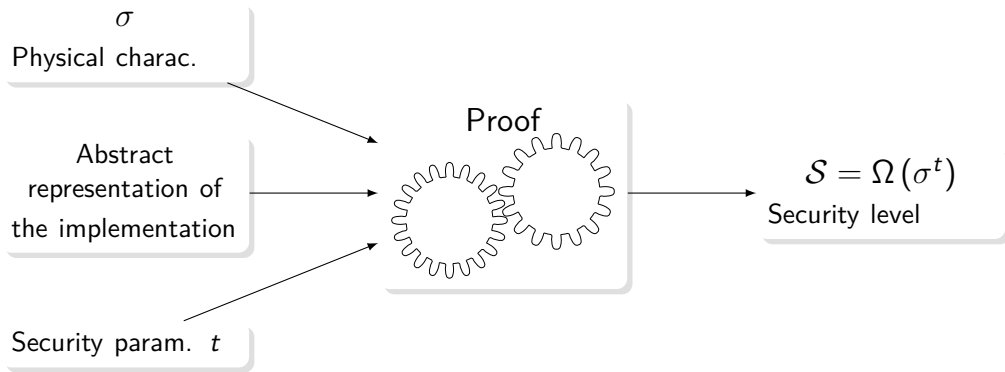
Security Proof



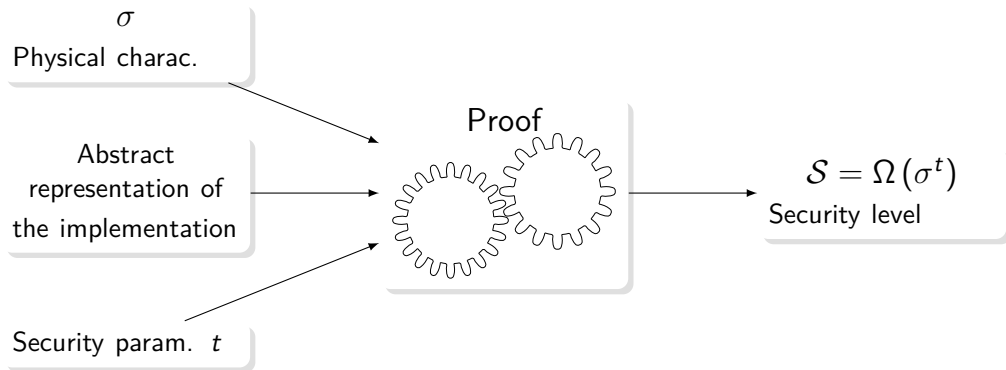
Security Proof



Security Proof



Security Proof



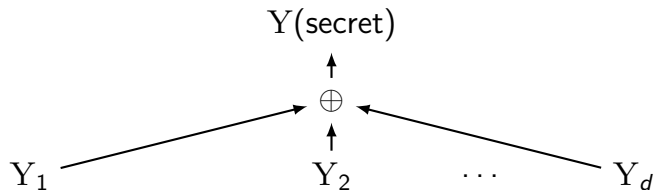
Whatever an adversary can compute with physical access, she can also do it with black-box access, up to some error $\frac{1}{\mathcal{S}}$

Masking: what is that ?

Masking, a.k.a. *MPC on silicon*:⁵⁶ secret sharing over a finite field $(\mathbb{F}, \oplus, \otimes)$
Y(secret)

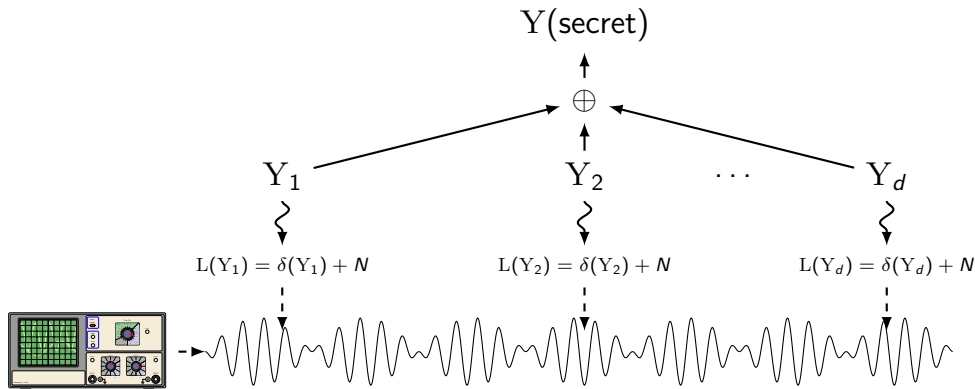
Masking: what is that ?

Masking, a.k.a. *MPC on silicon*:⁵⁶ secret sharing over a finite field $(\mathbb{F}, \oplus, \otimes)$



Masking: what is that ?

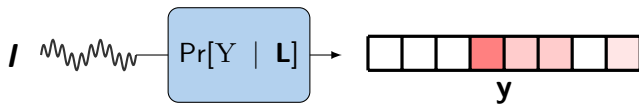
Masking, a.k.a. *MPC on silicon*:⁵⁶ secret sharing over a finite field $(\mathbb{F}, \oplus, \otimes)$



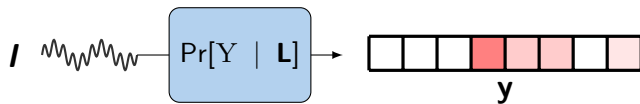
⁵Chari et al., "Towards Sound Approaches to Counteract Power-Analysis Attacks".

⁶Goubin and Patarin, "DES and Differential Power Analysis (The "Duplication" Method)".

The Noisy Leakage Model



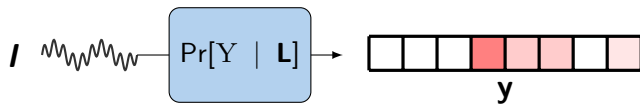
The Noisy Leakage Model



If, the adversary gets:



The Noisy Leakage Model



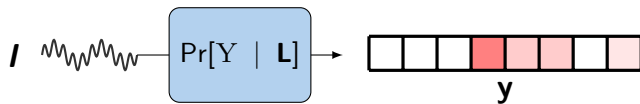
If, the adversary gets:



Very noisy leakage

Y indistinguishable from blind guess

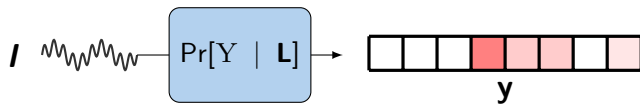
The Noisy Leakage Model



If, the adversary gets:



The Noisy Leakage Model

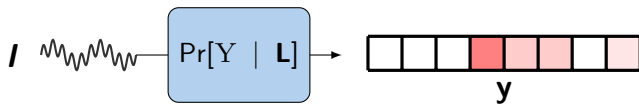


If, the adversary gets:



Low-noise leakage
Exact prediction for Y

The Noisy Leakage Model

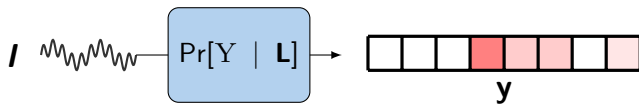


δ -NOISY ADVERSARY

Any intermediate computation Y leaks $L(Y)$ such that:

$$\text{SD}(Y; L) = \mathbb{E}_L \left[\text{TV} \left(\underbrace{\begin{array}{|c|c|c|c|c|c|c|c|} \hline \text{white} & \text{white} & \text{white} & \text{red} & \text{light red} & \text{light red} & \text{white} & \text{light red} \\ \hline \end{array}}_{\Pr[Y | L]}, \underbrace{\begin{array}{|c|c|c|c|c|c|c|c|} \hline \text{light red} & \text{light red} & \text{light red} & \text{light red} & \text{light red} & \text{light red} & \text{light red} & \text{light red} \\ \hline \end{array}}_{\Pr[Y]} \right) \right] \leq \delta$$

The Noisy Leakage Model



δ -NOISY ADVERSARY

Any intermediate computation Y leaks $L(Y)$ such that:

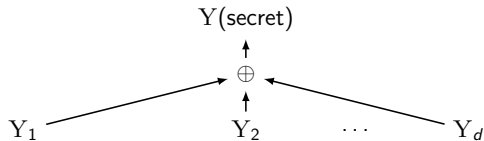
$$\text{SD}(Y; L) = \mathbb{E}_L \left[\text{TV} \left(\underbrace{\begin{array}{|c|c|c|c|c|c|c|c|} \hline \text{white} & \text{white} & \text{white} & \text{red} & \text{light red} & \text{light red} & \text{white} & \text{white} \\ \hline \end{array}}_{\Pr[Y | L]}, \underbrace{\begin{array}{|c|c|c|c|c|c|c|c|} \hline \text{light red} & \text{light red} & \text{light red} & \text{light red} & \text{light red} & \text{light red} & \text{light red} & \text{light red} \\ \hline \end{array}}_{\Pr[Y]} \right) \right] \leq \delta$$

Main assumption: every observed leakage is δ -noisy

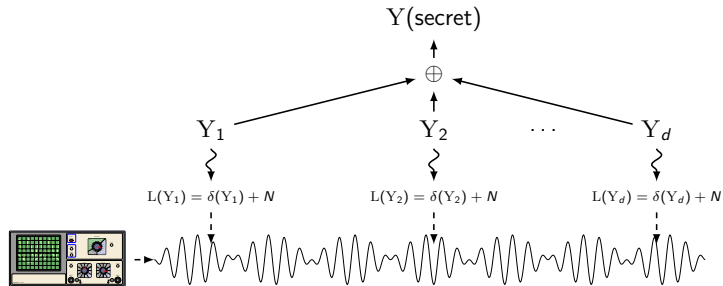
The Effect of Masking

Y(secret)

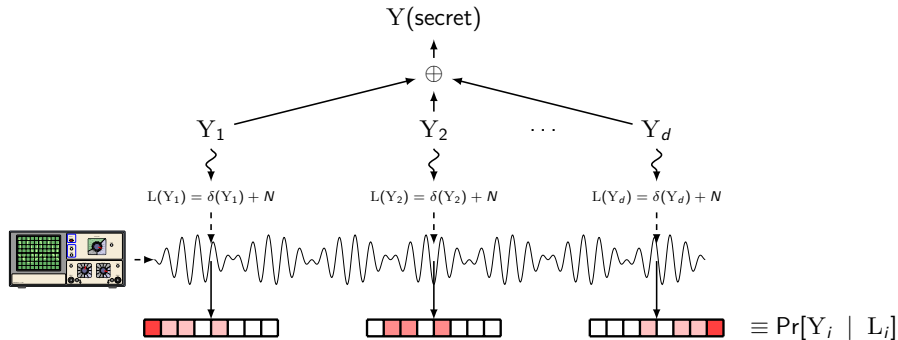
The Effect of Masking



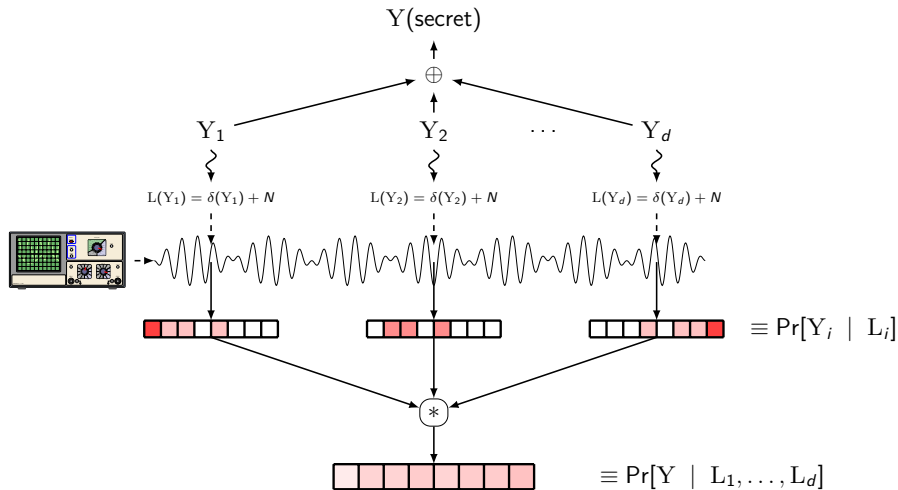
The Effect of Masking



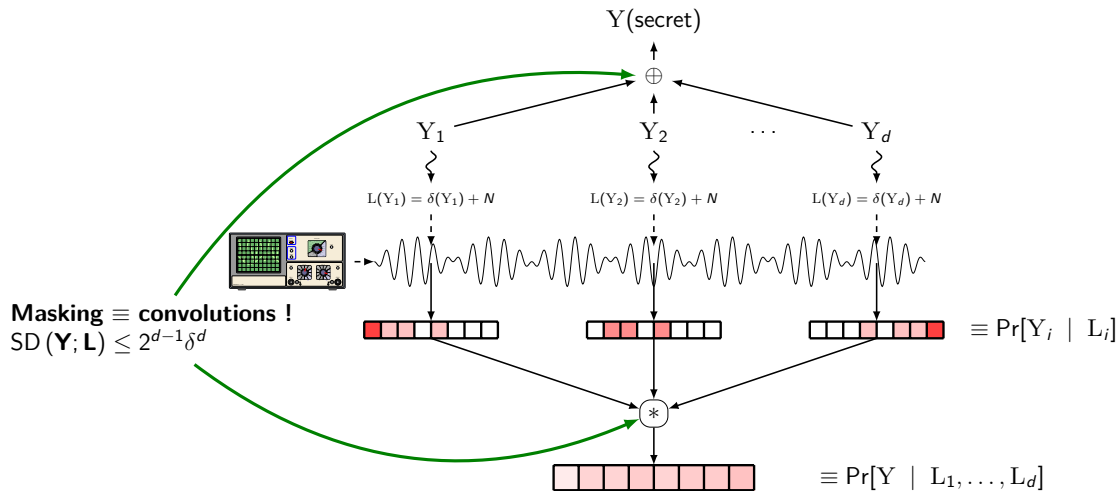
The Effect of Masking



The Effect of Masking



The Effect of Masking



Recent Advances

FANCIER TYPES OF ENCODING (AC'25)

$$\rightarrow Y = \sum_{i=1}^d \omega_i \cdot Y_i \quad (\vec{\omega} \text{ public, but random})$$

Recent Advances

FANCIER TYPES OF ENCODING (AC'25)

- $Y = \sum_{i=1}^d \omega_i \cdot Y_i$ ($\vec{\omega}$ public, but random)
- m bits leaked on the d shares (global leakage)

Recent Advances

FANCIER TYPES OF ENCODING (AC'25)

- $Y = \sum_{i=1}^d \omega_i \cdot Y_i$ ($\vec{\omega}$ public, but random)
- m bits leaked on the d shares (global leakage)
- $\text{SD}(Y; \mathbf{L}) \leq \mathcal{O}\left(\sqrt{2^{-\log|\mathbb{F}| \cdot (d-1) + m}}\right)$ (incentive for large $\mathbb{F}$)

Recent Advances

FANCIER TYPES OF ENCODING (AC'25)

- $Y = \sum_{i=1}^d \omega_i \cdot Y_i$ ($\vec{\omega}$ public, but random)
- m bits leaked on the d shares (global leakage)
- $\text{SD}(Y; \mathbf{L}) \leq \mathcal{O}\left(\sqrt{2^{-\log|\mathbb{F}| \cdot (d-1) + m}}\right)$ (incentive for large $\mathbb{F}$)

LEAKAGE FROM COMPUTATIONS (CURRENT WORK)

For any circuit C protected with d -th order masking, with δ -noisy wires, η -close to uniform:

Recent Advances

FANCIER TYPES OF ENCODING (AC'25)

- $Y = \sum_{i=1}^d \omega_i \cdot Y_i$ ($\vec{\omega}$ public, but random)
- m bits leaked on the d shares (global leakage)
- $SD(Y; \mathbf{L}) \leq \mathcal{O}\left(\sqrt{2^{-\log|\mathbb{F}| \cdot (d-1) + m}}\right)$ (incentive for large $\mathbb{F}$)

LEAKAGE FROM COMPUTATIONS (CURRENT WORK)

For any circuit C protected with d -th order masking, with δ -noisy wires, η -close to uniform:

$$SD(Y; \mathbf{L}) \leq \binom{|C|}{d} \cdot (2\eta\delta)^d$$

Our Holistic Approach

NIST PQC COMPETITION: *THE PRICE OF ANARCHY*

→ Masking Dilithium: 50× slower $\times^7$

⁷Coron et al., “Improved Gadgets for the High-Order Masking of Dilithium”.

⁸Ueno et al., “Curse of Re-encryption: A Generic Power/EM Analysis on Post-Quantum KEMs”.

⁹Pino et al., “Raccoon: A Masking-Friendly Signature Proven in the Probing Model”.

Our Holistic Approach

NIST PQC COMPETITION: *THE PRICE OF ANARCHY*

→ Masking Dilithium: 50× slower X⁷

→ Masking Kyber: “cursed” X⁸

⁷Coron et al., “Improved Gadgets for the High-Order Masking of Dilithium”.

⁸Ueno et al., “Curse of Re-encryption: A Generic Power/EM Analysis on Post-Quantum KEMs”.

⁹Pino et al., “Raccoon: A Masking-Friendly Signature Proven in the Probing Model”.

Our Holistic Approach

NIST PQC COMPETITION: *THE PRICE OF ANARCHY*

→ Masking Dilithium: 50× slower ⁷

→ Masking Kyber: “cursed” ⁸

CHANGE OF PARADIGM

“Whatever an adversary can compute with *physical access* to C, she can also do it with *black-box access* to C with negligible error”

⁷Coron et al., “Improved Gadgets for the High-Order Masking of Dilithium”.

⁸Ueno et al., “Curse of Re-encryption: A Generic Power/EM Analysis on Post-Quantum KEMs”.

⁹Pino et al., “Raccoon: A Masking-Friendly Signature Proven in the Probing Model”.

Our Holistic Approach

NIST PQC COMPETITION: *THE PRICE OF ANARCHY*

→ Masking Dilithium: 50× slower $\times^7$

→ Masking Kyber: “cursed” $\times^8$

CHANGE OF PARADIGM

“Whatever an adversary can compute with *physical access* to C, she can also do it with *black-box access* to $C' \preccurlyeq C$ with negligible error”

⁷Coron et al., “Improved Gadgets for the High-Order Masking of Dilithium”.

⁸Ueno et al., “Curse of Re-encryption: A Generic Power/EM Analysis on Post-Quantum KEMs”.

⁹Pino et al., “Raccoon: A Masking-Friendly Signature Proven in the Probing Model”.

Our Holistic Approach

NIST PQC COMPETITION: *THE PRICE OF ANARCHY*

→ Masking Dilithium: 50× slower $\times^7$

→ Masking Kyber: “cursed” $\times^8$

CHANGE OF PARADIGM

“Whatever an adversary can compute with *physical access* to C, she can also do it with *black-box access* to $C' \preccurlyeq C$ with negligible error”

⇒ Find the best trade-off C' : Masking-Friendly Crypto⁹



⁷Coron et al., “Improved Gadgets for the High-Order Masking of Dilithium”.

⁸Ueno et al., “Curse of Re-encryption: A Generic Power/EM Analysis on Post-Quantum KEMs”.

⁹Pino et al., “Raccoon: A Masking-Friendly Signature Proven in the Probing Model”.

References I

-  Boudgoust, K. and P. Scholl. “Simple Threshold (Fully Homomorphic) Encryption from LWE with Polynomial Modulus”. In: *ASIACRYPT (1)*. Vol. 14438. Lecture Notes in Computer Science. Springer, 2023, pp. 371–404.
-  Chari, S. et al. “Towards Sound Approaches to Counteract Power-Analysis Attacks”. In: *Advances in Cryptology - CRYPTO '99, 19th Annual International Cryptology Conference, Santa Barbara, California, USA, August 15-19, 1999, Proceedings*. Ed. by M. J. Wiener. Vol. 1666. Lecture Notes in Computer Science. Springer, 1999, pp. 398–412. ISBN: 3-540-66347-9. DOI: [10.1007/3-540-48405-1_26](https://doi.org/10.1007/3-540-48405-1_26). URL: https://doi.org/10.1007/3-540-48405-1_26.

References II

-  Coron, J. et al. “Improved Gadgets for the High-Order Masking of Dilithium”. In: *IACR Trans. Cryptogr. Hardw. Embed. Syst.* 2023.4 (2023), pp. 110–145. DOI: [10.46586/TCHES.V2023.I4.110-145](https://doi.org/10.46586/TCHES.V2023.I4.110-145). URL: <https://doi.org/10.46586/tches.v2023.i4.110-145>.
-  Goubin, L. and J. Patarin. “DES and Differential Power Analysis (The "Duplication" Method)”. In: *Cryptographic Hardware and Embedded Systems, First International Workshop, CHES'99, Worcester, MA, USA, August 12-13, 1999, Proceedings*. Ed. by Ç. K. Koç and C. Paar. Vol. 1717. Lecture Notes in Computer Science. Springer, 1999, pp. 158–172. DOI: [10.1007/3-540-48059-5_15](https://doi.org/10.1007/3-540-48059-5_15). URL: https://doi.org/10.1007/3-540-48059-5_15.

References III

-  Pino, R. del et al. “Raccoon: A Masking-Friendly Signature Proven in the Probing Model”. In: *Advances in Cryptology - CRYPTO 2024 - 44th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 18-22, 2024, Proceedings, Part I*. Ed. by L. Reyzin and D. Stebila. Vol. 14920. Lecture Notes in Computer Science. Springer, 2024, pp. 409–444. DOI: [10.1007/978-3-031-68376-3_13](https://doi.org/10.1007/978-3-031-68376-3_13). URL: https://doi.org/10.1007/978-3-031-68376-3_13.
-  Regev, O. “On lattices, learning with errors, random linear codes, and cryptography”. In: *STOC*. ACM, 2005, pp. 84–93.
-  Shor, P. W. “Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer”. In: *SIAM J. Comput.* 26.5 (1997), pp. 1484–1509.

References IV

 Ueno, R. et al. “Curse of Re-encryption: A Generic Power/EM Analysis on Post-Quantum KEMs”. In: *IACR Trans. Cryptogr. Hardw. Embed. Syst.* 2022.1 (2022), pp. 296–322. DOI: 10.46586/TCHES.V2022.I1.296–322. URL: <https://doi.org/10.46586/tches.v2022.i1.296–322>.