POLKA: Towards Leakage-Resistant Post-Quantum CCA-Secure Public Key Encryption

Clément Hoffmann, Benoît Libert, Charles Momin, Thomas Peters, François-Xavier Standaert

Monday 8th May, 2023

UCLouvain

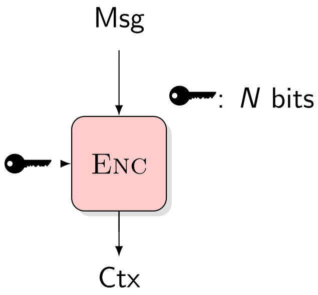
Post-quantum cryptography (PQC) and Side-Channel Attacks (SCA)

Side-channel attacks:

- Generic against lattices: [RRCB19], [NWDP22], [KAPFA21],
- Against the Number Theoretic Transform (NTT): [PPM17], [PP19], [LZHLT22]
- Against the Fujisaki-Okamoto(FO) transform: [UXTITH22]

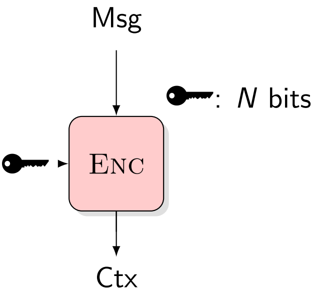
Countermeasures are expensive: [RPBC20], [Pessl16], [NWDP22], [ABHKSS22]

Side-channel attacks



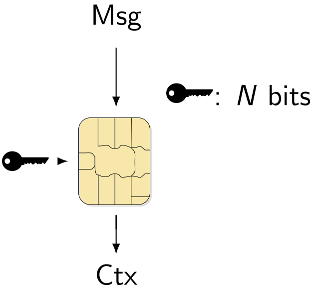
Side-channel attacks

"Cryptographic algorithms don't run on paper,



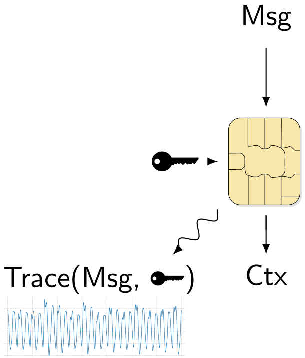
Side-channel attacks

"Cryptographic algorithms don't run on paper, they run on physical devices"



Side-channel attacks

"Cryptographic algorithms don't run on paper, they run on physical devices"



: N bits

For every intermediate value v, an adversary gets a noisy image of the leakage function $L_g(v)$.

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

Side channel attacks - Power Analysis

SPA:

- Require only a few traces
- Can target ephemeral secret
- Typical countermeasure: parallelism, shuffling

Side channel attacks - Power Analysis

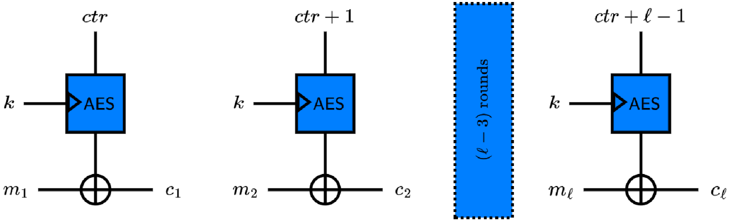
SPA:

- Require only a few traces
- Can target ephemeral secret
- Typical countermeasure: parallelism, shuffling

DPA:

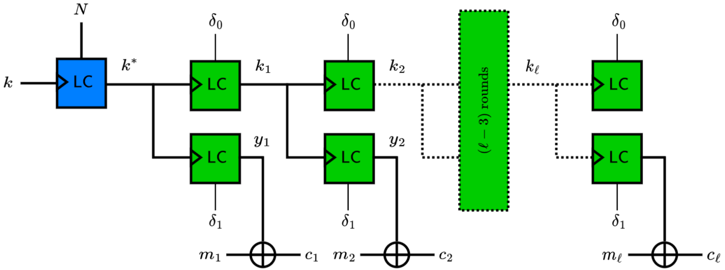
- Require a large amount of trace
- Can only target long-term secret
- Typical countermeasure: masking

Parallel with symmetric cryptography - Leveling



AES in CTR mode; uniformly protected against DPA

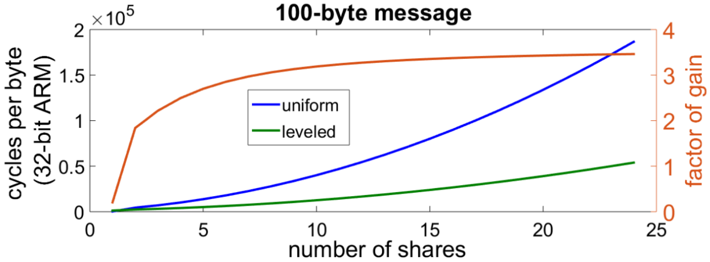
Parallel with symmetric cryptography - Leveling

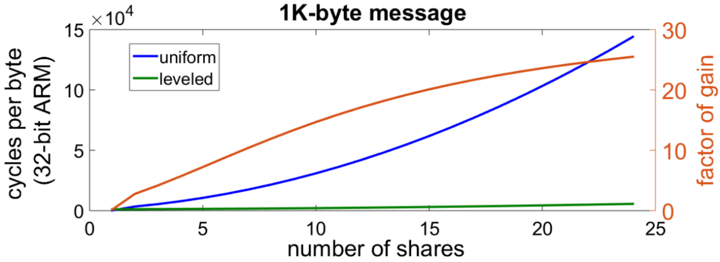


Leakage-resistant mode

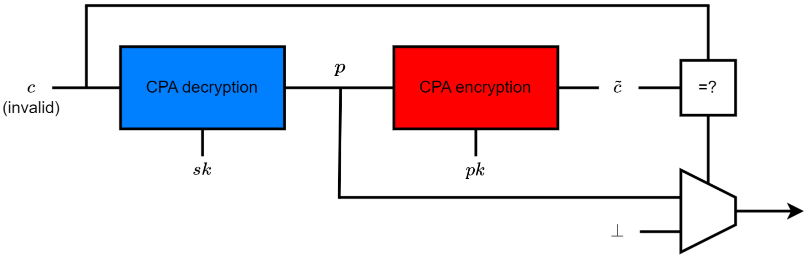
Leveled implementation thanks to rekeying

Leveling impact can be massive

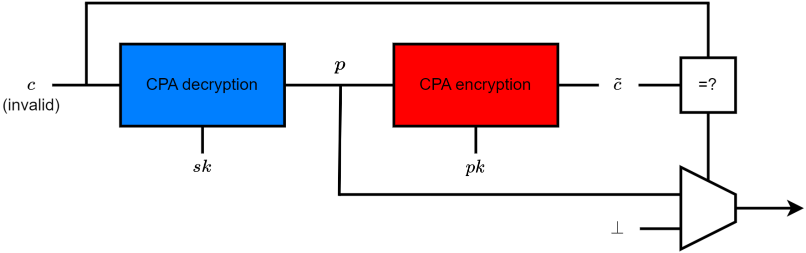




The example of FO



The example of FO



DISTINGUISHING ATTACK:

- Simply distinguish between two values with leakage
- Even more expensive to prevent than DPA

Our contributions

- CCA lattice-based encryption scheme relying on **RLWE**
  - **Relatively efficient**
  - Proven secured in ROM & QROM

Our contributions

- CCA lattice-based encryption scheme relying on **RLWE**
  - **Relatively efficient**
  - Proven secured in ROM & QROM
- Much **cheaper to protect against SCAs** thanks to tweaks:
  - CCA without FO transform
  - Dummy ciphertexts
  - Hard physical learning problems

High-level outline

Classic **[LPR10]**-like encryption scheme

$$\begin{matrix} c_1 = a \cdot r + e_1 \\ c_2 = b \cdot r + e_2 \end{matrix}, \text{ for small } r, e_1, e_2$$

High-level outline

Classic **[LPR10]**-like encryption scheme

$$\begin{array}{l} c_1 = a \cdot r + e_1 \\ c_2 = b \cdot r + e_2 \end{array}, \text{ for small } r, e_1, e_2$$

combined with **Authentificated Encryption** scheme (e.g. ASCON)

$$c_0 = \mathrm{E}_K(m), \text{ where } K = H(r, e_1, e_2)$$

High-level outline

Classic **[LPR10]**-like encryption scheme

$$\begin{array}{l} c_1 = a \cdot r + e_1 \\ c_2 = b \cdot r + e_2 \end{array}, \text{ for small } r, e_1, e_2$$

combined with **Authentificated Encryption** scheme (e.g. ASCON)

$$c_0 = \mathrm{E}_K(m), \text{ where } K = H(r, e_1, e_2)$$

Retrieve $e_2 \Rightarrow$ Retrieve e_1 and $r \Rightarrow$ Decrypt

Rigidity property ([BP18])

p: intermediate modulus

$$
\begin{aligned}
&c_2 - p \cdot c_1 \cdot sk = p \cdot (\dots) + \boldsymbol{e_2} \\
&\boldsymbol{r} = (c_2 - e_2) \cdot b^{-1} \\
&\boldsymbol{e_1} = c_1 - a \cdot r
\end{aligned}
$$

Rigidity property ([BP18])

p: intermediate modulus

$$
\begin{aligned}
&c_2 - p \cdot c_1 \cdot sk = p \cdot (\dots) + \boldsymbol{e_2} \\
&\boldsymbol{r} = (c_2 - e_2) \cdot b^{-1} \\
&\boldsymbol{e_1} = c_1 - a \cdot r
\end{aligned}
$$

Then check $||e_1||, ||e_2||, ||r|| < B$.

Rigidity property ([BP18])

p: intermediate modulus

$$\begin{aligned} &c_2 - p \cdot c_1 \cdot sk = p \cdot (\dots) + \boldsymbol{e_2} \\ &\boldsymbol{r} = (c_2 - e_2) \cdot b^{-1} \\ &\boldsymbol{e_1} = c_1 - a \cdot r \end{aligned}$$

Then check $||e_1||, ||e_2||, ||r|| < B$.

We checked the ciphertext was valid **without re-encryption**.

Rigidity property ([BP18])

p: intermediate modulus

DPA attack path

$$c_2 - p \cdot \boxed{c_1 \cdot sk} = p \cdot (\dots) + \boldsymbol{e_2}$$
$$\boldsymbol{r} = (c_2 - e_2) \cdot b^{-1}$$
$$\boldsymbol{e_1} = c_1 - a \cdot r$$

Then check $||e_1||, ||e_2||, ||r|| < B$.

We checked the ciphertext was valid **without re-encryption**.

Dummy ciphertexts

We use **RLWE homomorphy** to randomize (potentially invalid) ciphertexts:

Dummy ciphertexts

We use **RLWE homomorphy** to randomize (potentially invalid) ciphertexts:

1. Generate $c_1' = a \cdot r' + e_1'$, $c_2' = a \cdot r' + e_2'$

Dummy ciphertexts

We use **RLWE homomorphy** to randomize (potentially invalid) ciphertexts:

1. Generate $c_1' = a \cdot r' + e_1'$, $c_2' = a \cdot r' + e_2'$
2. Compute $\overline{c_1} = c_1 + c_1'$, $\overline{c_2} = c_2 + c_2'$.

Dummy ciphertexts

We use **RLWE homomorphy** to randomize (potentially invalid) ciphertexts:

1. Generate $c_1' = a \cdot r' + e_1'$, $c_2' = a \cdot r' + e_2'$
2. Compute $\overline{c_1} = c_1 + c_1'$, $\overline{c_2} = c_2 + c_2'$.
3. Retrieve $\overline{r}, \overline{e_1}, \overline{e_2}$

Dummy ciphertexts

We use **RLWE homomorphy** to randomize (potentially invalid) ciphertexts:

1. Generate $c'_1 = a \cdot r' + e'_1,\ c'_2 = a \cdot r' + e'_2$
2. Compute $\overline{c_1} = c_1 + c'_1,\ \overline{c_2} = c_2 + c'_2$.
3. Retrieve $\overline{r}, \overline{e_1}, \overline{e_2}$
4. Get $r = \overline{r} - r', e_1 = \overline{e_1} - e'_1, e_2 = \overline{e_2} - e'_2$.

Dummy ciphertexts

We use **RLWE homomorphy** to randomize (potentially invalid) ciphertexts:

1. Generate $c_1' = a \cdot r' + e_1'$, $c_2' = a \cdot r' + e_2'$
2. Compute $\overline{c_1} = c_1 + c_1'$, $\overline{c_2} = c_2 + c_2'$.
3. Retrieve $\overline{r}, \overline{e_1}, \overline{e_2}$
4. Get $r = \overline{r} - r', e_1 = \overline{e_1} - e_1', e_2 = \overline{e_2} - e_2'$.

Dummy ciphertexts

We use **RLWE homomorphy** to randomize (potentially invalid) ciphertexts:

1. Generate $c_1' = a \cdot r' + e_1'$, $c_2' = a \cdot r' + e_2'$
2. Compute $\overline{c_1} = c_1 + c_1'$, $\overline{c_2} = c_2 + c_2'$.
3. Retrieve $\overline{r}, \overline{e_1}, \overline{e_2}$
4. Get $r = \overline{r} - r', e_1 = \overline{e_1} - e_1', e_2 = \overline{e_2} - e_2'$.

Check $||\overline{e_1}||, ||\overline{e_2}||, ||\overline{r}|| < 2B$.

Dummy ciphertexts

We use **RLWE homomorphy** to randomize (potentially invalid) ciphertexts:

1. Generate $c_1' = a \cdot r' + e_1'$, $c_2' = a \cdot r' + e_2'$
2. Compute $\overline{c_1} = c_1 + c_1'$, $\overline{c_2} = c_2 + c_2'$.
3. Retrieve $\overline{r}, \overline{e_1}, \overline{e_2}$
4. Get $r = \overline{r} - r', e_1 = \overline{e_1} - e_1', e_2 = \overline{e_2} - e_2'$.

Check $||\overline{e_1}||, ||\overline{e_2}||, ||\overline{r}|| < 2B$.

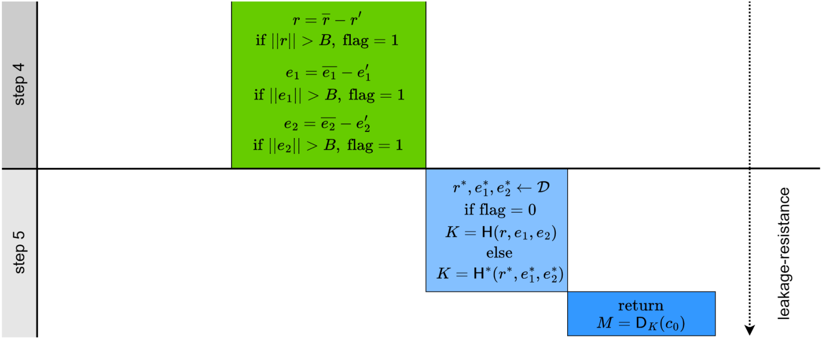
DPA attack paths $\Rightarrow$ SPA attack paths

Leveling Polka.Dec

	SPA	avg-SPA	UP-DPA	DPA
step 1	$r', e_1', e_2' \leftarrow \mathcal{D}$ $c_1' = a \cdot r' + e_1'$ $c_2' = a \cdot r' + e_2'$ $\overline{c_1} = c_1 + c_1'$ $\overline{c_2} = c_2 + c_2'$			
step 2			$t = (p \cdot \overline{c_1}) \cdot s$	
step 3	$\overline{\mu} = \overline{c_2} - t$ $\overline{e_2} = \overline{\mu} \bmod p$ if $\lVert\overline{e_2}\rVert > 2B, \text{ flag} = 1$ $\overline{r} = (\overline{c_2} - \overline{e_2}) \cdot b^{-1}$ if $\lVert\overline{r}\rVert > 2B, \text{ flag} = 1$ $\overline{e_1} = \overline{c_1} - a \cdot \overline{r}$ if $\lVert\overline{e_1}\rVert > 2B, \text{ flag} = 1$			
step 4		$r = \overline{r} - r'$ if $\lVert r\rVert > B, \text{ flag} = 1$ $e_1 = \overline{e_1} - e_1'$ if $\lVert e_1\rVert > B, \text{ flag} = 1$ $e_2 = \overline{e_2} - e_2'$ if $\lVert e_2\rVert > B, \text{ flag} = 1$		

leakage-resilience

Leveling Polka.Dec



Black-box security

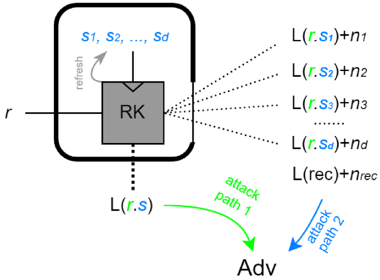
- ROM: rigidity property ([BP18])
- QROM: reduction to implicit reduction

Black-box security

- ROM: rigidity property ([BP18])
- QROM: reduction to implicit reduction

Design tweaks are part of the black-box analysis

Hard physical learning problem (or free rekeying)



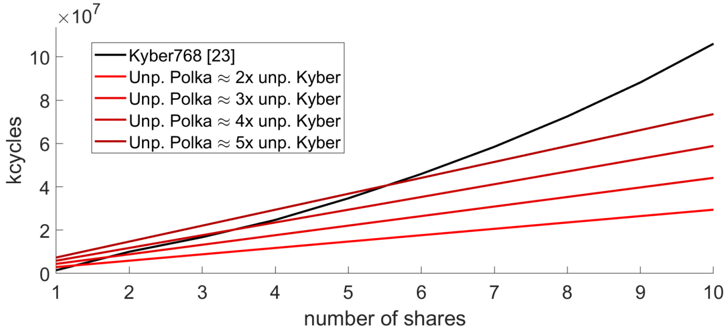
Rekeying with Learning With Physical Rounding (LWPR, [DMMS21])

- Attack path 1 targets the ephemeral values output by the rekeying
- Attack path 2 targets the rekeying operations

Open problems

- Concrete implementation and comparison (e.g. with Kyber)
- Adapt the scheme to protect the message as well
- Proof of LWPR-like problems (reduction to LWR/LWE ?), formal analysis of security with leakage under weak physical assumptions

Conclusion



Expected time complexity of KYBER and POLKA according to orders of masking

Supplementary material - references

[RRCB19] - Generic Side-channel attacks on CCA-secure lattice-based PKE and KEMs; Prasanna Ravi, Sujoy Sinha Roy, Anupam Chattopadhyay & Shivam Bhasin

[KAPFA21] - 2Deep: Enhancing Side-Channel Attacks on Lattice-Based Key-Exchange via 2-D Deep Learning; Priyank Kashyap, Furkan Aydin, Seetal Potluri, Paul D. Franzon & Aydin Aysu

[PPM17] - Single-Trace Side-Channel Attacks on Masked Lattice-Based Encryption; Robert Primas, Peter Pessl & Stefan Mangard

[PP19] - More Practical Single-Trace Attacks on the Number Theoretic Transform; Robert Primas & Peter Pessl

[LZHLT22] - Single-Trace Side-Channel Attacks on the Toom-Cook: The Case Study of Saber; Yanbin Li, Jiajie Zhu, Yuxin Huang, Zhe Liu & Ming Tang

[RPBC20] - On Configurable SCA Countermeasures Against Single Trace Attacks for the NTT; Prasanna Ravi, Romain Poussier, Shivam Bhasin, and Anupam Chattopadhyay

Supplementary material - references

[UXTITH22] - Curse of Re-encryption: A Generic Power/EM Analysis on Post-Quantum KEMs; Rei Ueno, Keita Xagawa, Yutaro Tanaka, Akira Ito, Junko Takahashi & Naofumi Homma

[Pessl16] - Analyzing the Shuffling Side-Channel Countermeasure for Lattice-Based Signatures; Peter Pessl

[NWDP22] - Side-Channel Attacks on Lattice-Based KEMs Are Not Prevented by Higher-Order Masking; Kalle Ngo, Ruize Wang, Elena Dubrova & Nils Paulsrud

[ABHKSS22] - Systematic study of decryption and re-encryption leakage: the case of kyber; Melissa Azouaoui, Olivier Bronchain, Clément Hoffmann, Yulia Kuzovkova, Tobias Schneider & François-Xavier Standaert

[BP18] - Towards KEM Unification; Daniel J. Bernstein & Edoardo Persichetti

[DMMS21] Exploring Crypto-Physical Dark Matter and Learning with Physical Rounding; Sébastien Duval, Pierrick Méaux, Charles Momin & François-Xavier Standaert

[LPR10] On ideal lattices and learning with errors over rings; Vadim Lyubashevsky, Chris Peikert & Oded Regev

Thanks to L. Masure, FX. Standaert, O. Bronchain and C. Momin for letting me use their figures.

Supplementary material - FO transform