Single trace HQC shared key recovery with SASCA

TrustNet

Guillaume Goy[1,2] Julien Maillard [1,2] Philippe Gaborit[1] Antoine Loiseau[2]

[1]XLIM, University of Limoges, France

[2]CEA-LETI, Grenoble Alpes University, France

23 May 2024

Table of Contents

Table of Contents

Modern cryptography

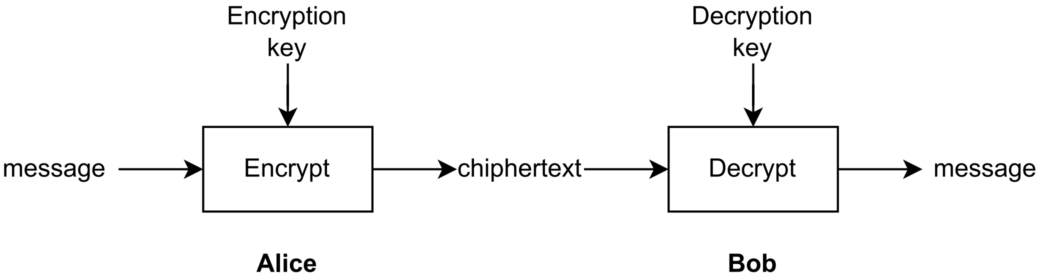


Figure – Overview of a cryptosystem

Modern cryptography

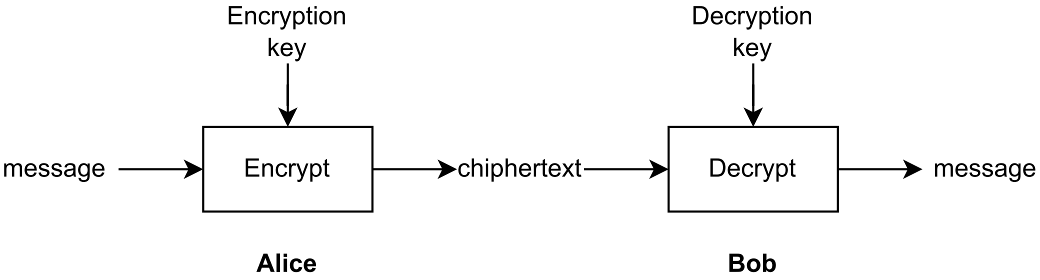


Figure – Overview of a cryptosystem

RSA [RSA78] - Elliptic Curves Cryptography (ECC) [Kob87, Mil85]

Post-Quantum Cryptography [AMAB+17, ABB+17, BCL+, BDK+18, DKL+18]

Cryptographic Security

We have three levels of security : (I) 2^{128}, (II) 2^{192} and (III) 2^{256}
This represents the **minimal number of operation an attacker needs to pay to recover a secret information**.
And often also **The number of different secret keys**.

Cryptographic Security

We have three levels of security : (I) 2^{128}, (II) 2^{192} and (III) 2^{256}

This represents the **minimal number of operation an attacker needs to pay to recover a secret information**.

And often also **The number of different secret keys**.

$$2^{128} = \underbrace{2^{33}}_{\substack{\text{8.6 billion} \\ \text{Number of} \\ \text{human beings} \\ \text{on earth}}} \times \underbrace{2^{33}}_{\substack{\text{8.6 GHz} \\ \text{CPU frequency}}} \times \underbrace{2^{62}}$$

Cryptographic Security

We have three levels of security : (I) 2^{128}, (II) 2^{192} and (III) 2^{256}

This represents the **minimal number of operation an attacker needs to pay to recover a secret information**.

And often also **The number of different secret keys**.

$$2^{128} = \underbrace{2^{33}}_{\substack{\text{8.6 billion}\\ \text{Number of}\\ \text{human beings}\\ \text{on earth}}} \times \underbrace{2^{33}}_{\substack{\text{8.6 GHz}\\ \text{CPU frequency}}} \times \underbrace{2^{62}}_{\substack{> 146 \text{ billion years}\\ > 10\times \text{ Age of the Universe}}}$$

Cryptographic Security

We have three levels of security : (I) 2^{128}, (II) 2^{192} and (III) 2^{256}

This represents the **minimal number of operation an attacker needs to pay to recover a secret information**.

And often also **The number of different secret keys**.

$$2^{128} = \underbrace{2^{33}}_{\substack{\text{8.6 billion} \\ \text{Number of} \\ \text{human beings} \\ \text{on earth}}} \times \underbrace{2^{33}}_{\substack{\text{8.6 GHz} \\ \text{CPU frequency}}} \times \underbrace{2^{62}}_{\substack{> \text{146 billion years} \\ > 10\times \text{ Age of the Universe}}}$$

$2^{256} \approx\approx 10^{80} \leftarrow$ Number of atoms in the observable universe

Side-Channel Attacks

The first side-channel attack was introduced by Paul Kocher in 1996 [Koc96].

Side-Channel Attacks

The first side-channel attack was introduced by Paul Kocher in 1996 [Koc96].

Goal : Recover secret information using side-channel leakage :

- Execution time
- **Power consumption**
- **Electromagnetic emanations**
- Sound
- Heat, $\cdots$

Timing attack example

Algorithm Naive PIN verification

Require: $C = (c_1, c_2, c_3, c_4)$ the fair password
Require: $T = (t_1, t_2, t_3, t_4)$ user attempt
Ensure: True si $C = T$, False otherwise.

```
if c1 = t1 then
    if c2 = t2 then
        if c3 = t3 then
            if c4 = t4 then
                return True
return False
```

Leakage models

We consider that the power consumption / electromagnetic emanations leakage follows a Leakage model :
Hamming weight leakage model :

$$L(t) = \alpha \cdot \mathtt{HW}(\mathbf{v}(t)) + \beta + \mathtt{Noise}(t) \quad (1)$$

Leakage models

We consider that the power consumption / electromagnetic emanations leakage follows a Leakage model :

Hamming weight leakage model :

$$L(t) = \alpha \cdot \mathtt{HW}(\mathbf{v}(t)) + \beta + \mathtt{Noise}(t) \tag{1}$$

Binary leakage model :

$$L(t) = \sum_{i=1}^{m} (\alpha_i \cdot v_i(t)) + \beta + \mathtt{Noise}(t) \tag{2}$$

Attack can be perform in Simulation or in a real case scenario.

Soft Analytical Side-Channel Attacks (SASCA)

Idea : combine several weak physical leaks to obtain strong information

- Introduced by Veyrat-Chravrillon et al. [VCGS14] to attack AES in 2014
- Application against Kyber [PPM17, PP19, HHP^{+}21, HSST23, AEVR23]

  $\rightarrow$ Information Propagation through NTT

Soft Analytical Side-Channel Attacks (SASCA)

Idea : combine several weak physical leaks to obtain strong information

- Introduced by Veyrat-Chravrillon et al. [VCGS14] to attack AES in 2014
- Application against Kyber [PPM17, PP19, HHP+21, HSST23, AEVR23]
  - $\rightarrow$ Information Propagation through NTT
- Attack against hash function Keccak [KPP20] in 2020
- First attack against code-based cryptography [GMGL23]

➔ Mainly based on **Belief Propagation** [Mac03, KFL01].

Message passing with Belief Propagation

The goal of Belief Propagation is to compute a **Marginal Distribution** for every **Intermediate values** involved in a given algorithm.

Toy Example : Galois Field Multiplication $v = a \times b$ $(= \alpha^{\log(a)+\log(b)})$:

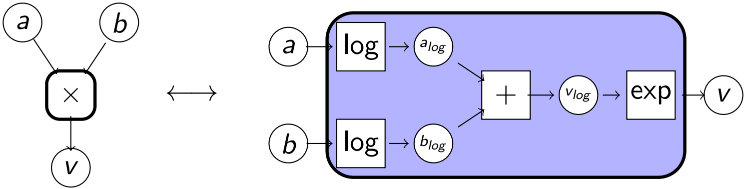


Figure – Graphical representation of a Galois Field Multiplication

Message passing with Belief Propagation

The goal of Belief Propagation is to compute a **Marginal Distribution** for every **Intermediate values** involved in a given algorithm.

Toy Example : Galois Field Multiplication $v = a \times b \; (= \alpha^{\texttt{log}(a)+\texttt{log}(b)})$:

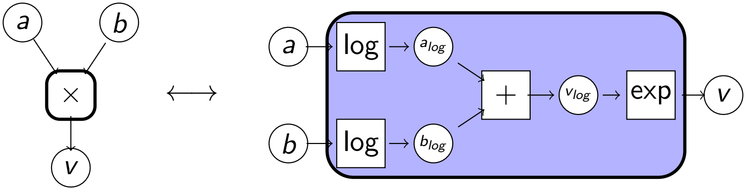


Figure – Graphical representation of a Galois Field Multiplication

The Goal is to compute : $\mathbb{P}(a \mid b, v), \mathbb{P}(b \mid a, v), \mathbb{P}(v \mid a, b)$

Message passing with Belief Propagation

The goal of Belief Propagation is to compute a **Marginal Distribution** for every **Intermediate values** involved in a given algorithm.

Toy Example : Galois Field Multiplication $v = a \times b \; (= \alpha^{\texttt{log}(a)+\texttt{log}(b)})$:

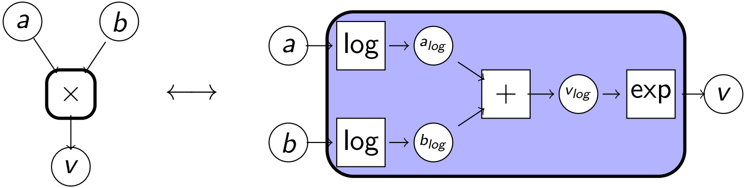


Figure – Graphical representation of a Galois Field Multiplication

The Goal is to compute : $\mathbb{P}(a \mid b, v)\,, \mathbb{P}(b \mid a, v)\,, \mathbb{P}(v \mid a, b)$

Sum Product Algorithm [KFL01] gives a solver for this problem.

Table of Contents

Hamming Quasi-Cyclic

Algorithm Keygen

Input : param
Output : (pk, sk)

$\mathbf{h} \xleftarrow{\$} \mathcal{R}$
$(\mathbf{x}, \mathbf{y}) \xleftarrow{\$} \mathcal{R}_{\omega}^{2}$
$\mathbf{s} = \mathbf{x} + \mathbf{h}\mathbf{y}$
$\mathrm{pk} = (\mathbf{h}, \mathbf{s})$
$\mathrm{sk} = (\mathbf{x}, \mathbf{y})$

Algorithm Encrypt

Input : $(\mathrm{pk}, \mathbf{m} \in \mathbb{F}_2^{\lambda})$
Output : ciphertext $\mathtt{ct}$

$\mathbf{e} \xleftarrow{\$} \mathcal{R}_{\omega_e}$
$(\mathbf{r}_1, \mathbf{r}_2) \xleftarrow{\$} \mathcal{R}_{\omega_r}^{2}$
$\mathbf{u} = \mathbf{r}_1 + \mathbf{h}\mathbf{r}_2$
$\mathbf{c} = \mathtt{Encode}(\mathbf{m})$
$\mathbf{v} = \mathbf{c} + \mathbf{s}\mathbf{r}_2 + \mathbf{e}$
$\mathtt{ct} = (\mathbf{u}, \mathbf{v})$

Algorithm Decrypt

Input : $(\mathrm{sk}, \mathtt{ct})$
Output : $\mathbf{m}'$

$\mathbf{c} + \mathbf{e}' = \mathbf{v} - \mathbf{u}\mathbf{y}$
$\mathbf{m}' = \mathtt{Decode}(\mathbf{c} + \mathbf{e}')$

Hamming Quasi-Cyclic

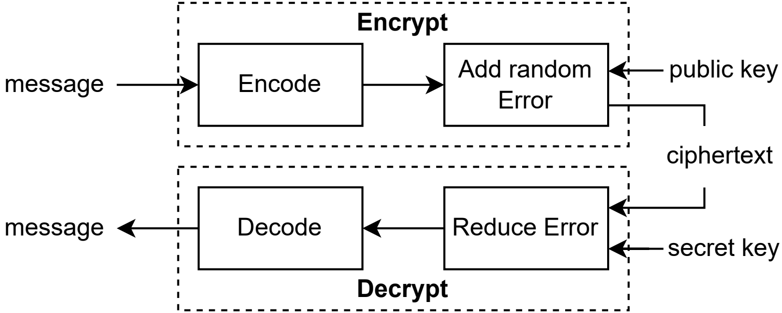


Figure – Hamming Quasi-Cyclic Overview

- Decryption Failure Rate (DFR) is ensured by the error correction capability and analysis of the hamming weight distribution of the error **e**' [AGZ20]
- Most of the Side-Channel Attacks against HQC target the **decoding step**.

Concatenated code structure

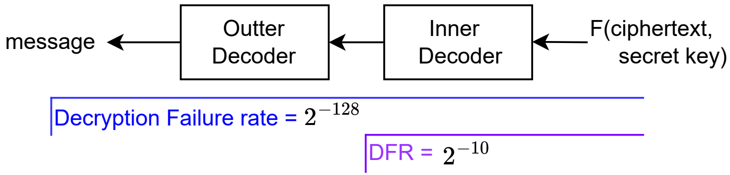


Figure – HQC Concatenated codes structure

Concatenated code structure

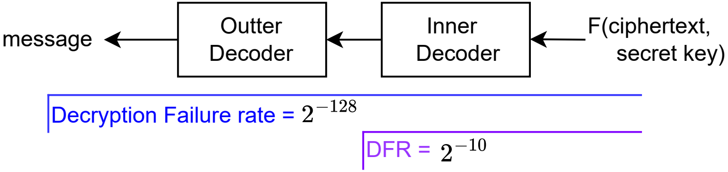


Figure – HQC Concatenated codes structure

(i) **Secret key** recovery attacks : [SHR+22, GLG22a, BMG+24]

(ii) **Shared key** (message) recovery attacks : [GLG22b, GMGL23, BMG+24]

Reed-Solomon Syndrome Computation

Algorithm Compute Syndromes from HQC RS Decoder from [AMAB+23]

Require: parameters : k, n the dimension and length of the code
Require: parity check matric $H \in \mathbb{F}_q^{(n-k,n)}$
Require: codeword $c \in \mathbb{F}_q^{n_1}$
Ensure: $s := H^T \times c$ the syndrome of c

1: Initialize s to 0^{n-k}
2: **for** i from 0 to $n-k$ **do**
3:     **for** j from 1 to n **do**
4:         $s[i] = s[i] \oplus c[j] \times H[i, j-1]$ $\triangleright$ $\times$ is the Galois Field multiplication
5:     $s[i] = s[i] \oplus c[0]$

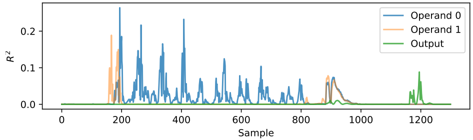
Table of Contents

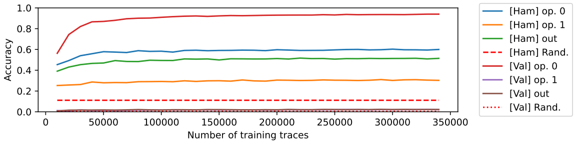
Attacker Model

- Hypothesis
  - Access to a clone device
  - One target function only
  - Isolate and order each occurence
  - No control on the SNR
- In Practice :
  - Both training and attack on the same device
  - Target the Galois field multiplication
  - Pattern matching
  - No trace averaging (true single trace attack)
- Set-Up :
  - STM32F407
  - Langer Near Field Probe
  - Rhode-Schwarz RTO2024

Templates on the Galois field multiplication operands

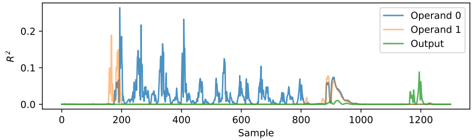
Galois field multiplication based on FFT strategy [BGTZ08]

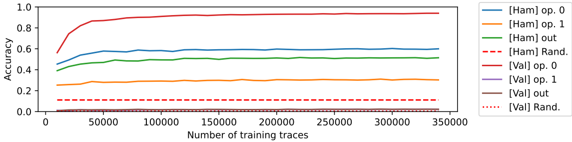




Templates on the Galois field multiplication operands

Galois field multiplication based on FFT strategy [BGTZ08]





	Value template accuracy	Hamming weight template accuracy
Input 1	**0.9389**	0.5929
Input 2	0.0211	**0.3035**
Output	0.0221	**0.5178**

Table – Hamming weight and value templates accuracies on `gf_mul`. Each attack has been performed 400 times. 10%/90% validation/training segmentation.

Outer Decoder syndrome computation graphical representation

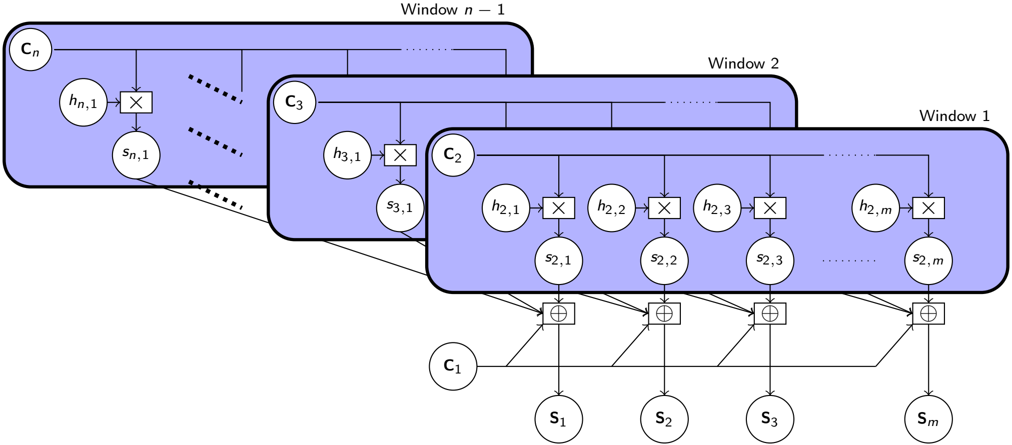
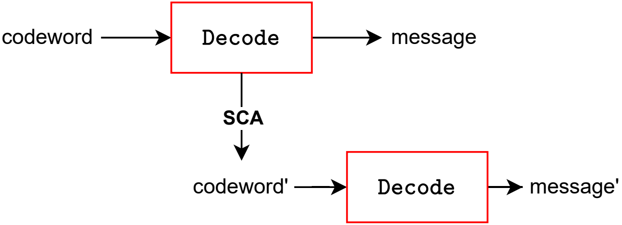


Figure – Graphical representation of the RS syndrome computation from HQC

Re-decoding Strategy



Security level	HQC parameters			List decoder
λ	k_1	n_1	t	τ_{GS}
HQC-128	16	46	15	19
HQC-192	24	56	16	19
HQC-256	32	90	29	36

Table – Reed-Solomon error correction capability of the RS decoder for each HQC set of parameters, given for a classical decoder and the Guruswami-Sudan list decoder.

Attack Accuracy in Simulation

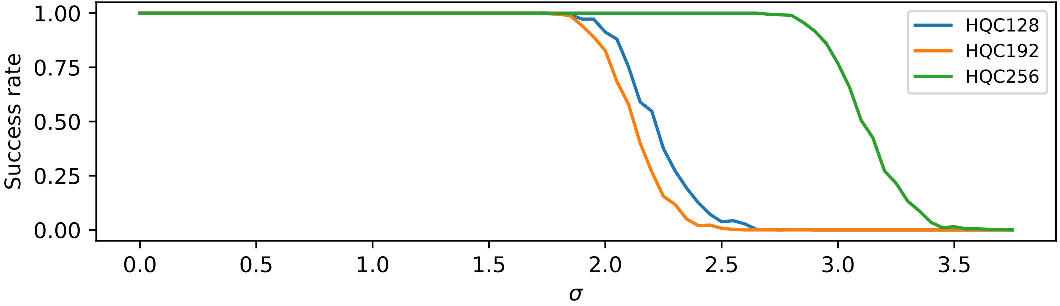


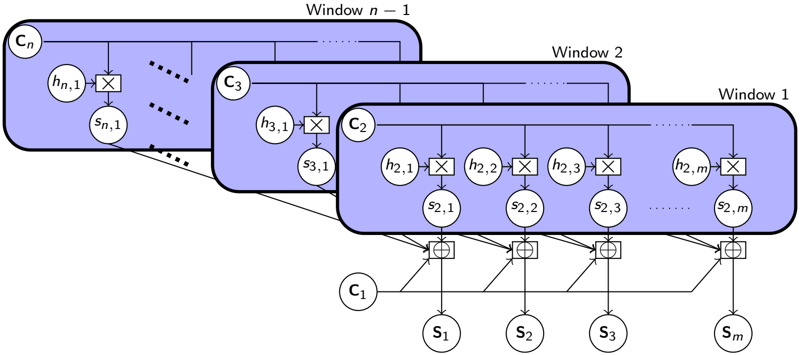
Figure – Simulated success rate of SASCA on the decoder, with re-decoding strategy, depending on the selected security level of HQC

Breaking shuffling countermeasures

- Fine Shuffling (Adapted from a Kyber countermeasure)
  $\rightarrow$ Randomly choose $a \times b$ or $b \times a$.

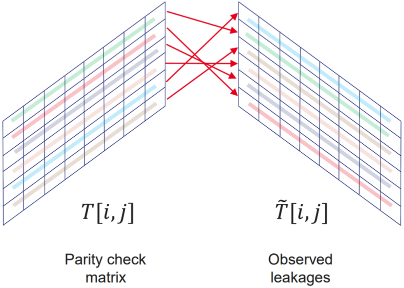
Breaking shuffling countermeasures

- Fine Shuffling (Adapted from a Kyber countermeasure)
  - $\rightarrow$ Randomly choose $a \times b$ or $b \times a$.
- Coarse shuffling (Adapted from a Kyber countermeasure)
  - $\rightarrow$ Randomly shuffle columns of the parity check matrix



Breaking shuffling countermeasures 2

- Window Shuffling (Novelty)
  $\rightarrow$ Randomly shuffle lines of the parity check matrix



$$D[i,i'] = \sum_{j=1}^{256} \mathrm{d}\left(\tilde{T}[i,j], T[i',j]\right)$$

Instance of the assignment Problem.
$\rightarrow$ Solver : Hungarian algorithm.

Breaking Codeword Masking (High Level Masking)

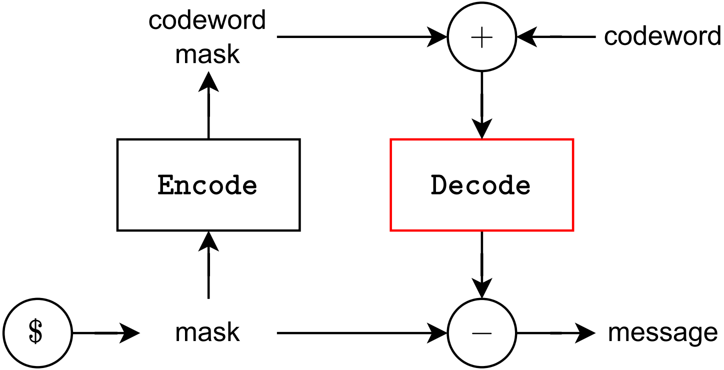


Figure – High level Masking of a decoder (Codeword Masking) [MSS13]

Encoder Attack Accuracy in Simulation

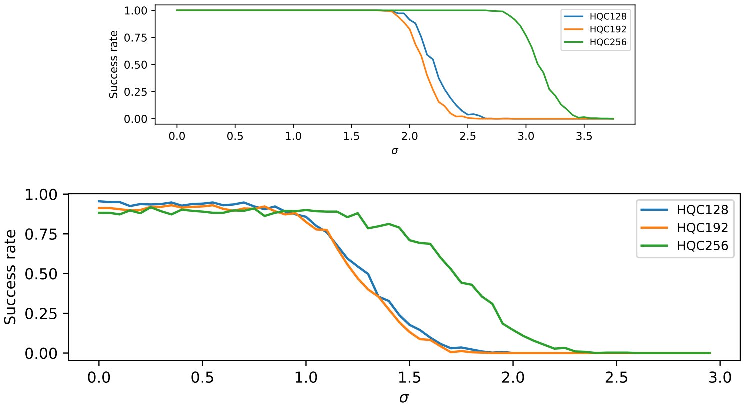


Figure – Simulated success rate of SASCA on the decoder, with re-decoding strategy, depending on the selected security level of HQC

Table of Contents

re-encryption step from HHK transform

- HQC-KEM is based on HHK transform [HHK17]
- This transform introduces a re-encryption step.

re-encryption step from HHK transform

- HQC-KEM is based on HHK transform [HHK17]
- This transform introduces a re-encryption step.

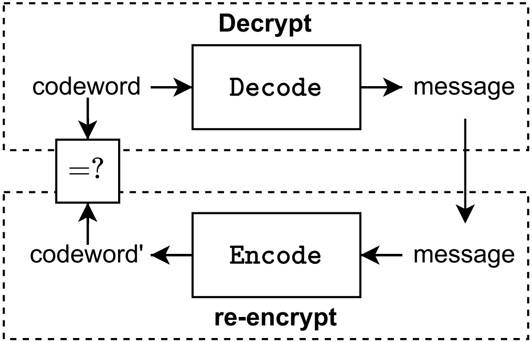
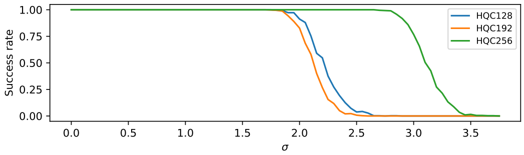
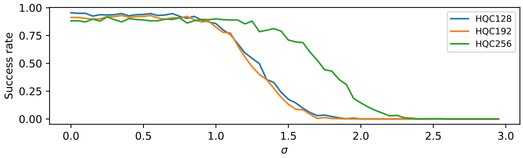


Figure – HQC Structure with HHK transform

FO Attack Accuracy in Simulation



Decoder



Encoder

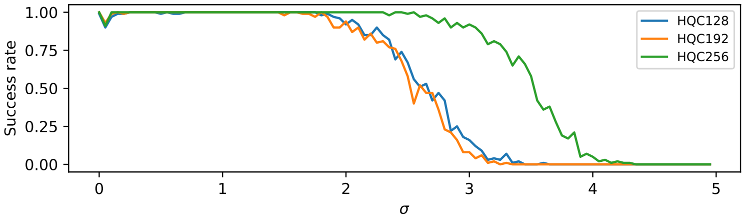


Figure – Simulated success rate of SASCA on the decoder and encoder exploiting re-encryption

Table of Contents

Full Shuffling Countermeasure

- The idea is to shuffle the entire matrix, instead of only rows or columns, during the matrix vector multiplication.
  - $\rightarrow$ Even if an attacker exactly recover the shuffled matrix, there exists 2^{504}, 2^{614} and 2^{1030} different permutations for the three security levels respectively.

Full Shuffling Countermeasure

- The idea is to shuffle the entire matrix, instead of only rows or columns, during the matrix vector multiplication.
  - $\rightarrow$ Even if an attacker exactly recover the shuffled matrix, there exists 2^{504}, 2^{614} and 2^{1030} different permutations for the three security levels respectively.
- The encoder could be change to a classical multiplication with a generator matrix to benefit from the same countermeasure.

Table of Contents

Conclusion and Perspectives

Conclusions

- Soft analytical side-channel attacks are a threat for (code-based) cryptography.
- Efficient countermeasure against these attacks are required.

Conclusion and Perspectives

Conclusions

- Soft analytical side-channel attacks are a threat for (code-based) cryptography.
- Efficient countermeasure against these attacks are required.

Future Works

- Target other code-based schemes with Belief Propagation Algorithms.
- Secure HQC against side-channel attacks in the t-probing model.

Conclusion and Perspectives

Conclusions

- Soft analytical side-channel attacks are a threat for (code-based) cryptography.
- Efficient countermeasure against these attacks are required.

Future Works

- Target other code-based schemes with Belief Propagation Algorithms.
- Secure HQC against side-channel attacks in the t-probing model.

Thank you for your attention !

Any questions ?

guillaume.goy@unilim.fr

DGA cea leti xlim INSTITUT DE RECHERCHE Université de Limoges NANOELEC.

References I

Nicolas Aragon, Paulo Barreto, Slim Bettaieb, Loïc Bidoux, Olivier Blazy, Jean-Christophe Deneuville, Philippe Gaborit, Shay Gueron, Tim Guneysu, Carlos Aguilar Melchor, et al.
BIKE : Bit Flipping Key Encapsulation.
2017.

Guilhèm Assael, Philippe Elbaz-Vincent, and Guillaume Reymond.
Improving single-trace attacks on the number-theoretic transform for cortex-m4.
In *2023 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, pages 111–121. IEEE, 2023.

Nicolas Aragon, Philippe Gaborit, and Gilles Zémor.
HQC-RMRS, an instantiation of the HQC encryption framework with a more efficient auxiliary error-correcting code.
arXiv preprint arXiv :2005.10741, 2020.

Carlos Aguilar-Melchor, Nicolas Aragon, Slim Bettaieb, Loïc Bidoux, Olivier Blazy, Jean-Christophe Deneuville, Philippe Gaborit, Edoardo Persichetti, and Gilles Zémor.
Hamming Quasi-Cyclic (HQC).
2017.

Carlos Aguilar-Melchor, Nicolas Aragon, Slim Bettaieb, Loïc Bidoux, Olivier Blazy, Jean-Christophe Deneuville, Philippe Gaborit, Edoardo Persichetti, and Gilles Zémor.
HQC reference implementation, April, 2023.
`https://pqc-hqc.org/implementation.html`.

Daniel J Bernstein, Tung Chou, Tanja Lange, Ingo von Maurich, Rafael Misoczki, Ruben Niederhagen, Edoardo Persichetti, Christiane Peters, Peter Schwabe, Nicolas Sendrier, et al.
Classic McEliece : conservative code-based cryptography.

References II

Joppe Bos, Léo Ducas, Eike Kiltz, Tancrède Lepoint, Vadim Lyubashevsky, John M Schanck, Peter Schwabe, Gregor Seiler, and Damien Stehlé.
CRYSTALS-Kyber : a CCA-secure module-lattice-based KEM.
In *2018 IEEE European Symposium on Security and Privacy (EuroS&P)*, pages 353–367. IEEE, 2018.

Richard P Brent, Pierrick Gaudry, Emmanuel Thomé, and Paul Zimmermann.
Faster multiplication in GF(2)[x].
In *Algorithmic Number Theory : 8th International Symposium, ANTS-VIII Banff, Canada, May 17-22, 2008 Proceedings 8*, pages 153–166. Springer, 2008.

Chloé Baïsse, Antoine Moran, Guillaume Goy, Julien Maillard, Nicolas Aragon, Philippe Gaborit, Maxime Lecomte, and Antoine Loiseau.
Secret and shared keys recovery on hamming quasi-cyclic with sasca.
Cryptology ePrint Archive, 2024.

Léo Ducas, Eike Kiltz, Tancrede Lepoint, Vadim Lyubashevsky, Peter Schwabe, Gregor Seiler, and Damien Stehlé.
Crystals-dilithium : A lattice-based digital signature scheme.
IACR Transactions on Cryptographic Hardware and Embedded Systems, pages 238–268, 2018.

Guillaume Goy, Antoine Loiseau, and Philippe Gaborit.
A new key recovery side-channel attack on HQC with chosen ciphertext.
In *International Conference on Post-Quantum Cryptography*, pages 353–371. Springer, 2022.

Guillaume Goy, Antoine Loiseau, and Phlippe Gaborit.
Estimating the strength of horizontal correlation attacks in the hamming weight leakage model : A side-channel analysis on HQC KEM.
In *WCC 2022 : The Twelfth International Workshop on Coding and Cryptography*, page WCC_2022_paper_48, 2022.

References III

Guillaume Goy, Julien Maillard, Philippe Gaborit, and Antoine Loiseau.
Single trace HQC shared key recovery with SASCA.
Cryptology ePrint Archive, 2023.
https://ia.cr/2023/1590.

Dennis Hofheinz, Kathrin Hövelmanns, and Eike Kiltz.
A modular analysis of the fujisaki-okamoto transformation.
In *Theory of Cryptography Conference*, pages 341–371. Springer, 2017.

Mike Hamburg, Julius Hermelink, Robert Primas, Simona Samardjiska, Thomas Schamberger, Silvan Streit, Emanuele Strieder, and Christine van Vredendaal.
Chosen ciphertext k-trace attacks on masked CCA2 secure kyber.
IACR Transactions on Cryptographic Hardware and Embedded Systems, pages 88–113, 2021.

Julius Hermelink, Silvan Streit, Emanuele Strieder, and Katharina Thieme.
Adapting belief propagation to counter shuffling of NTTs.
IACR Transactions on Cryptographic Hardware and Embedded Systems, pages 60–88, 2023.

Frank R Kschischang, Brendan J Frey, and H-A Loeliger.
Factor graphs and the sum-product algorithm.
IEEE Transactions on information theory, 47(2) :498–519, 2001.

Neal Koblitz.
Elliptic curve cryptosystems.
Mathematics of computation, 48(177) :203–209, 1987.

References IV

Paul C Kocher.
Timing attacks on implementations of diffie-hellman, RSA, DSS, and other systems.
In *Advances in Cryptology—CRYPTO'96 : 16th Annual International Cryptology Conference Santa Barbara, California, USA August 18–22, 1996 Proceedings 16*, pages 104–113. Springer, 1996.

Matthias J Kannwischer, Peter Pessl, and Robert Primas.
Single-trace attacks on keccak.
Cryptology ePrint Archive, 2020.

David JC MacKay.
Information theory, inference and learning algorithms.
Cambridge university press, 2003.

Victor S Miller.
Use of elliptic curves in cryptography.
In *Conference on the theory and application of cryptographic techniques*, pages 417–426. Springer, 1985.

Dominik Merli, Frederic Stumpf, and Georg Sigl.
Protecting PUF error correction by codeword masking.
Cryptology ePrint Archive, 2013.

Peter Pessl and Robert Primas.
More practical single-trace attacks on the number theoretic transform.
In *Progress in Cryptology–LATINCRYPT 2019 : 6th International Conference on Cryptology and Information Security in Latin America, Santiago de Chile, Chile, October 2–4, 2019, Proceedings 6*, pages 130–149. Springer, 2019.

References V

Robert Primas, Peter Pessl, and Stefan Mangard.
Single-trace side-channel attacks on masked lattice-based encryption.
In *Cryptographic Hardware and Embedded Systems–CHES 2017 : 19th International Conference, Taipei, Taiwan, September 25-28, 2017, Proceedings*, pages 513–533. Springer, 2017.

Ronald L Rivest, Adi Shamir, and Leonard Adleman.
A method for obtaining digital signatures and public-key cryptosystems.
Communications of the ACM, 21(2) :120–126, 1978.

Thomas Schamberger, Lukas Holzbaur, Julian Renner, Antonia Wachter-Zeh, and Georg Sigl.
A power side-channel attack on the reed-muller reed-solomon version of the HQC cryptosystem.
In *International Conference on Post-Quantum Cryptography*, pages 327–352. Springer, 2022.

Nicolas Veyrat-Charvillon, Benoît Gérard, and François-Xavier Standaert.
Soft analytical side-channel attacks.
In *Advances in Cryptology–ASIACRYPT 2014 : 20th International Conference on the Theory and Application of Cryptology and Information Security, Kaoshiung, Taiwan, ROC, December 7-11, 2014. Proceedings, Part I 20*, pages 282–296. Springer, 2014.