Attaque par canaux auxiliares contre HQC

Guillaume GOY

XLIM, Limoges University

26 avril 2025

Petits déjeuners de la cybersécurité

Table of Contents

1. Introduction
2. Side-Channel Attacks
3. Code-based Cryptography
4. Side-Channel Attacks against HQC
5. Countermeasures
6. Conclusions and Perspectives

Table of Contents

1. Introduction
2. Side-Channel Attacks
3. Code-based Cryptography
4. Side-Channel Attacks against HQC
5. Countermeasures
6. Conclusions and Perspectives

Quantum Computer threat

Quantum Computer is able to perform task that are impossible with a classical computer (Quantum Supremacy [AAB+19]) :

- Shor Algorithm [Sho94]
- Grover Algorithm [Gro96]

Quantum Computer threat

Quantum Computer is able to perform task that are impossible with a classical computer (Quantum Supremacy [AAB+19]) :

- Shor Algorithm [Sho94]
- Grover Algorithm [Gro96]

Solution : Post-quantum cryptography / NIST standardization process.

Post-Quantum Cryptography

- Hash-based cryptography :

  Sphincs+ [BHK+19]

Post-Quantum Cryptography

- Hash-based cryptography :
  Sphincs+ [BHK+19]
- Lattice-based cryptography :
  Kyber [BDK+18]
  Dilithium [DKL+18], $\cdots$

Post-Quantum Cryptography

- Hash-based cryptography :
  - Sphincs+ [BHK+19]
- Lattice-based cryptography :
  - Kyber [BDK+18]
  - Dilithium [DKL+18], $\cdots$
- code-based cryptography :
  - McEliece [McE78][BCL+]
  - HQC [AMAB+17]
  - BIKE [ABB+17], $\cdots$

Post-Quantum Cryptography

- Hash-based cryptography :
  - Sphincs+ [BHK+19]
- Lattice-based cryptography :
  - Kyber [BDK+18]
  - Dilithium [DKL+18], ···
- code-based cryptography :
  - McEliece [McE78][BCL+]
  - HQC [AMAB+17]
  - BIKE [ABB+17], ···
- multivarite-based, isogeny-based [JAC+17], MPC-based, ···

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**.

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

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

Table of Contents

1 Introduction

2 Side-Channel Attacks

3 Code-based Cryptography

4 Side-Channel Attacks against HQC

5 Countermeasures

6 Conclusions and Perspectives

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
```

Hamming Leakage model

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

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

Hamming Leakage model

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

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

Hamming distance leakage model :

$$L(t) = \alpha \cdot \texttt{HW}\left(\mathbf{v}'(t) \oplus \mathbf{v}(t)\right) + \beta + \texttt{Noise}(t) \tag{2}$$

Hamming Leakage model

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

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

Hamming distance leakage model :

$$L(t) = \alpha \cdot \texttt{HW}\left(\mathbf{v}'(t) \oplus \mathbf{v}(t)\right) + \beta + \texttt{Noise}(t) \tag{2}$$

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

Table of Contents

1. Introduction
2. Side-Channel Attacks
3. Code-based Cryptography
4. Side-Channel Attacks against HQC
5. Countermeasures
6. Conclusions and Perspectives

Error Correcting Codes

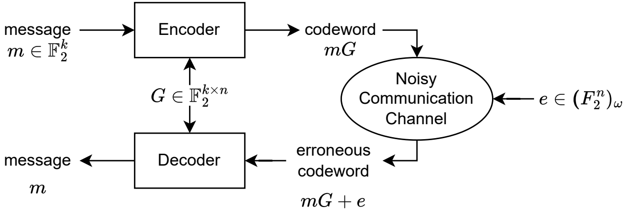

Figure – Overview of an Error Correcting Code.

Building Code-based cryptography

(i) Mask the Code with a random permutation [McE78][ABB+17]

Building Code-based cryptography

(i) Mask the Code with a random permutation [McE78][ABB+17]

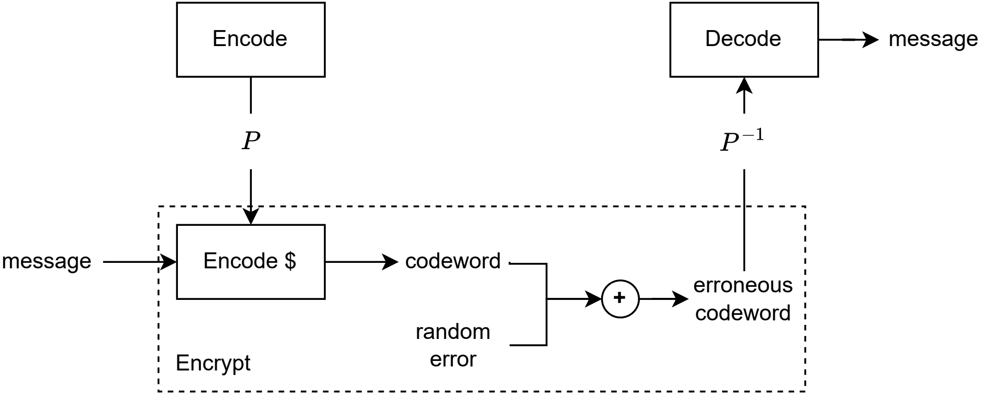

Figure – Masking error correcting code structure to build cryptography

Building Code-based cryptography

(i) Mask the Code with a random permutation [McE78][ABB+17]

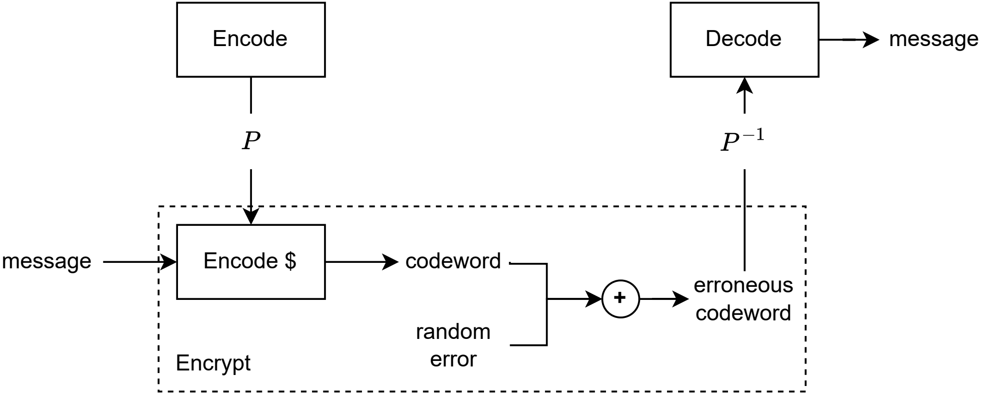

Figure – Masking error correcting code structure to build cryptography

Hamming Quasi-Cyclic

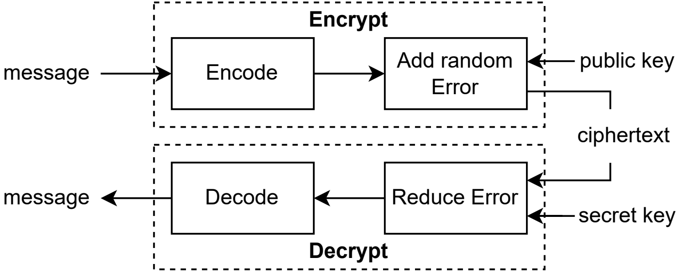

Figure – Hamming Quasi-Cyclic Overview

Table of Contents

1 Introduction

2 Side-Channel Attacks

3 Code-based Cryptography

4 Side-Channel Attacks against HQC

5 Countermeasures

6 Conclusions and Perspectives

Concatenated code structure

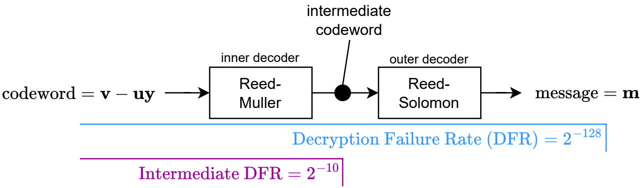

Figure – HQC Concatenanted codes structure

Concatenated code structure

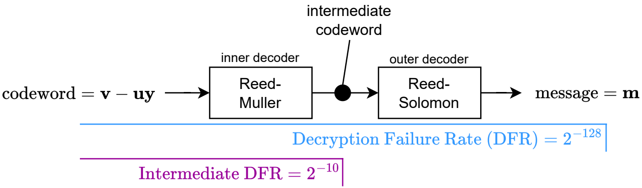

Figure – HQC Concatenanted codes structure

(i) Targeting the Inner code gives information about the **secret key**. [SHR+22, GLG22a]

(ii) Targeting the Outter code gives information about the **message**. [GLG22b, GMGL23]

Message recovery with Belief Propagation

We apply message passing algorithm [Mac03, KFL01] on a **graphical representation** of the target algorithm :

Message recovery with Belief Propagation

We apply message passing algorithm [Mac03, KFL01] on a **graphical representation** of the target algorithm :

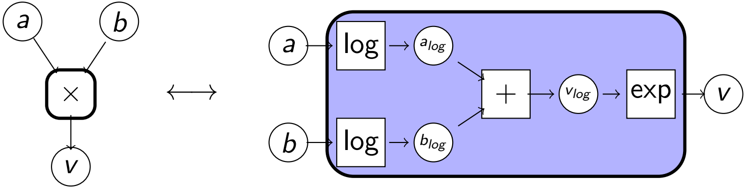

Figure – Graphical representation of a Galois Field Multiplication

Message recovery with Belief Propagation

We apply message passing algorithm [Mac03, KFL01] on a **graphical representation** of the target algorithm :

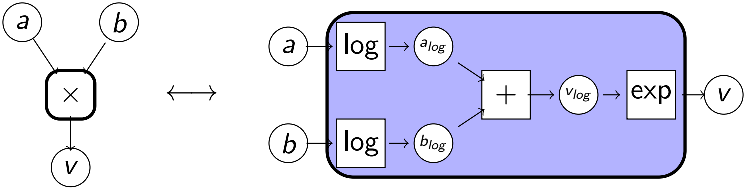

Figure – Graphical representation of a Galois Field Multiplication

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

$$\mu_{x \to f}(x) = \prod_{h \in n(x) \setminus \{f\}} \mu_{h \to x}(x) \tag{3}$$

$$\mu_{f \to x}(x) = \sum_{\sim \{x\}} \left(f(X) \prod_{y \in n(f) \setminus \{x\}} \mu_{y \to f}(y) \right) \tag{4}$$

Inner Decoder graphical representation

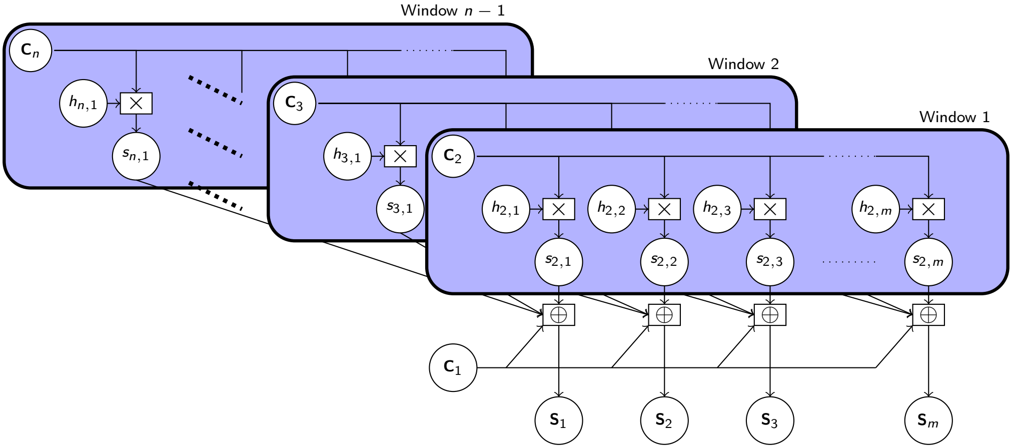

Figure – Graphical representation of the RS syndrome decoding from HQC

Table of Contents

1 Introduction

2 Side-Channel Attacks

3 Code-based Cryptography

4 Side-Channel Attacks against HQC

5 Countermeasures

6 Conclusions and Perspectives

Countermeasures

- **Constant time algorithms**

Countermeasures

- **Constant time algorithms**
- Shuffling :

Countermeasures

- **Constant time algorithms**
- Shuffling :
  For HQC, we obtain a combinatorial complexity of 2^{504}, 2^{614} and 2^{1030}

Countermeasures

- **Constant time algorithms**
- Shuffling :
  For HQC, we obtain a combinatorial complexity of 2^{504}, 2^{614} and 2^{1030}
- Masking :
  (i) High level Masking
  (ii) Low level Masking

High Level Masking

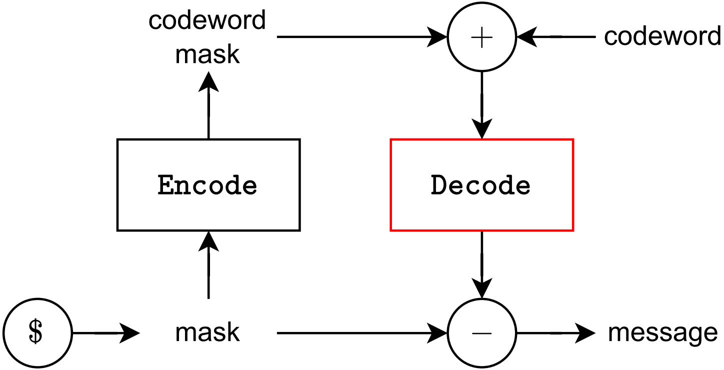

Figure – High level Masking of a decoder (Codeword Masking) [MSS13]

Low level masking

We consider the t-probing attacker model

Low level masking

We consider the t-probing attacker model

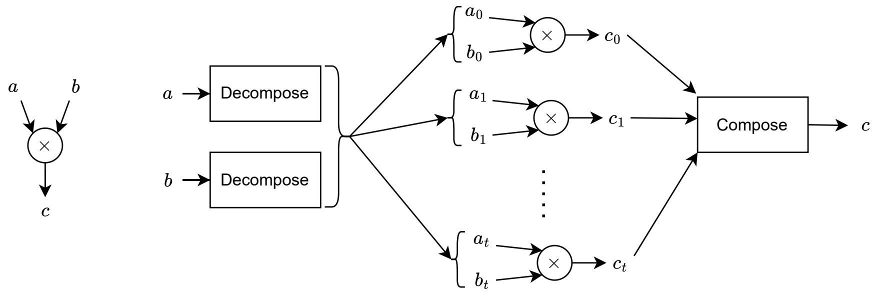

Figure – Low level Masking of an operation $\times$

$$a = f(a_0, \cdots, a_t) \ :$$

Low level masking

We consider the t-probing attacker model

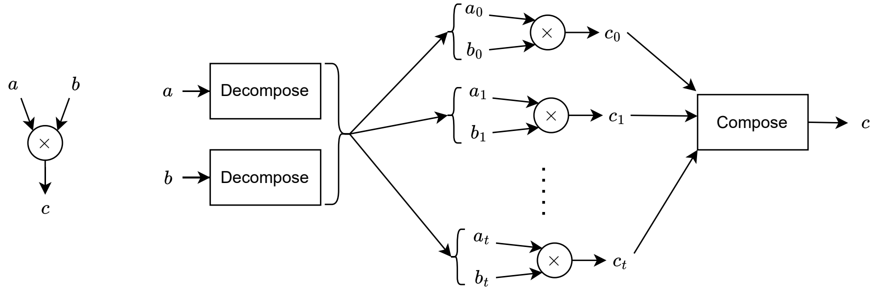

Figure – Low level Masking of an operation $\times$

$$a = f(a_0, \cdots, a_t) \ : [\text{boolean}] \ a = \bigoplus_{i=0}^{t} a_i \ ,$$

Low level masking

We consider the t-probing attacker model

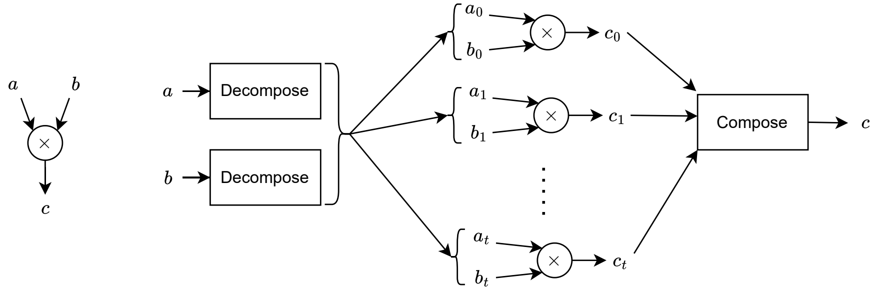

Figure – Low level Masking of an operation $\times$

$$a = f(a_0, \cdots, a_t) \ : \text{[boolean]}\ a = \bigoplus_{i=0}^{t} a_i\ , \text{[arithmetic]}\ a = \sum_{i=0}^{t} a_i \mod q \tag{5}$$

Table of Contents

1. Introduction
2. Side-Channel Attacks
3. Code-based Cryptography
4. Side-Channel Attacks against HQC
5. Countermeasures
6. Conclusions and Perspectives

Conclusions and Persecpectives

- Side-Channel Attacks represents a threat for (PQ) cryptography
- Think about constant time algorithms !

Futur Works

- Target other scheme with Belief Propagation Algorithms
- Secure HQC against side-channel attacks [ABC+22, DR24]

Conclusions and Persecpectives

- Side-Channel Attacks represents a threat for (PQ) cryptography
- Think about constant time algorithms !

Futur Works

- Target other scheme with Belief Propagation Algorithms
- Secure HQC against side-channel attacks [ABC+22, DR24]

Thank you for your attention !
Any questions ?

guillaume.goy@unilim.fr

References I

Frank Arute, Kunal Arya, Ryan Babbush, Dave Bacon, Joseph C Bardin, Rami Barends, Rupak Biswas, Sergio Boixo, Fernando GSL Brandao, David A Buell, et al.
Quantum supremacy using a programmable superconducting processor.
Nature, 574(7779) :505–510, 2019.

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.

Melissa Azouaoui, Olivier Bronchain, Gaëtan Cassiers, Clément Hoffmann, Yulia Kuzovkova, Joost Renes, Markus Schönauer, Tobias Schneider, François-Xavier Standaert, and Christine van Vredendaal.
Protecting dilithium against leakage : Revisited sensitivity analysis and improved implementations.
Cryptology ePrint Archive, 2022.

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, Maxime Bros, Couvreur Alain, Jean-Christophe Deneuville, Philippe Gaborit, Adrien Hauteville, and Gilles Zémor.
Rank quasi-cyclic (rqc).
2020.

References II

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.

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.

Daniel J Bernstein, Andreas Hülsing, Stefan Kölbl, Ruben Niederhagen, Joost Rijneveld, and Peter Schwabe.
The sphincs+ signature framework.
In *Proceedings of the 2019 ACM SIGSAC conference on computer and communications security*, pages 2129–2146, 2019.

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.

Loïc Demange and Mélissa Rossi.
A provably masked implementation of bike key encapsulation mechanism.
Cryptology ePrint Archive, 2024.

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.

References III

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.

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.

Lov K Grover.
A fast quantum mechanical algorithm for database search.
In *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*, pages 212–219, 1996.

David Jao, Reza Azarderakhsh, Matt Campagna, Craig Costello, Luca De Feo, Basil Hess, Amir Jalili, Brian Koziel, Brian LaMacchia, Patrick Longa, et al.
Sike : Supersingular isogeny key encapsulation.
2017.

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.

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.

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

Robert J McEliece.
A public-key cryptosystem based on algebraic.
Coding Thv, 4244 :114–116, 1978.

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

Peter W Shor.
Algorithms for quantum computation : discrete logarithms and factoring.
In *Proceedings 35th annual symposium on foundations of computer science*, pages 124–134. Ieee, 1994.

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.