

# Fault Attacks on Post-Quantum Cryptography

Norsk Kryptoseminar 2025

Mohamed Abdelmonem

31.10.2025

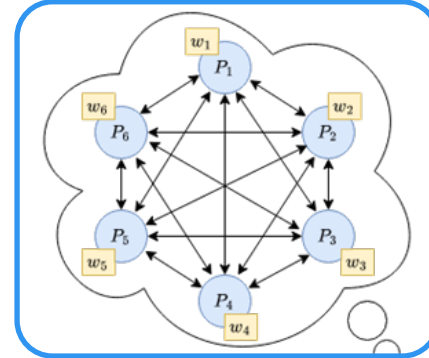
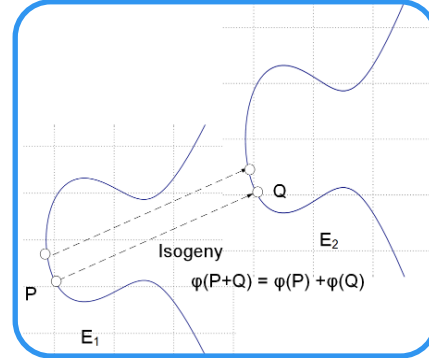
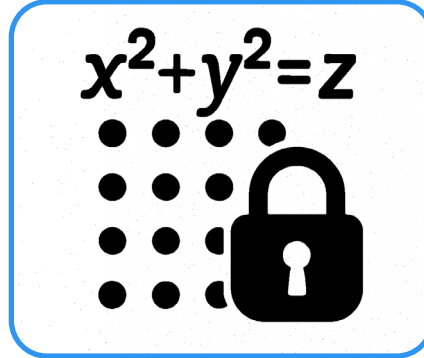
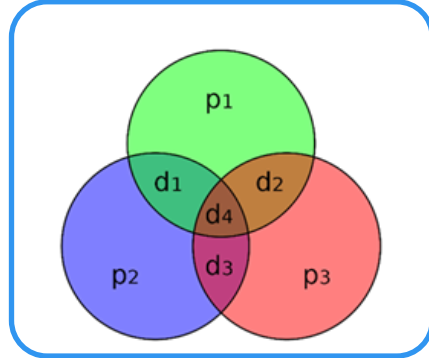
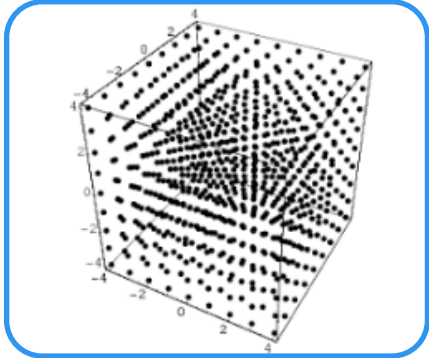


Simula  
UiB

# Flashback

- Norsk Kryptoseminar 2024:
  - “Countermeasure for Fault attacks on Lattice based algorithms”
  - Future work:
    - Find Fault injection attacks and countermeasures on other PQC schemes
    - 40 new NIST **Additional Digital Signature Schemes** in Round 1
    - Update 25. October : 14 Algorithms advanced to Round 2
  
- Norsk Kryptoseminar 2025:
  - What did we do?
  - What else has been done?
  - What else can be done?

# NIST Additional Signatures



## Lattice Based

- HAWK

## Code Based

- CROSS
- LESS

## Multivariate Based

- UOV
- QR-UOV
- SNOVA
- MAYO

## Isogeny Based

- SQIsign

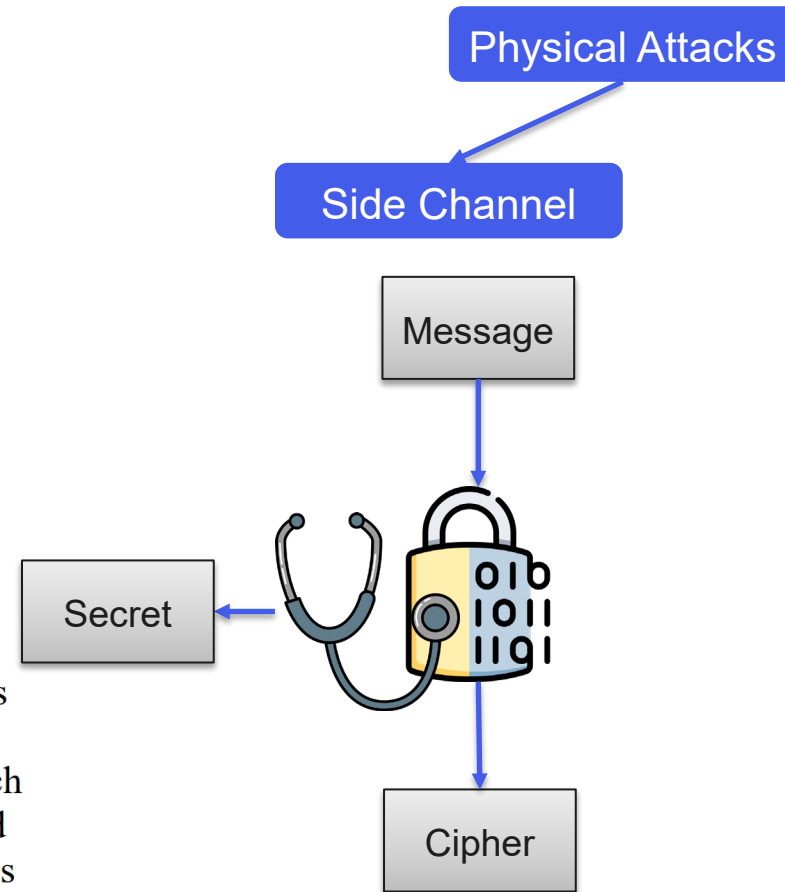
## MPCitH

- Miath
- MQOM
- PERK
- RYDE
- SDitH
- FAEST

# Physical Attacks

**4.B.4 Additional Security Properties** While the previously listed security definitions cover many of the attack scenarios that will be used in the evaluation of the submitted algorithms, there are several other properties that would be desirable:

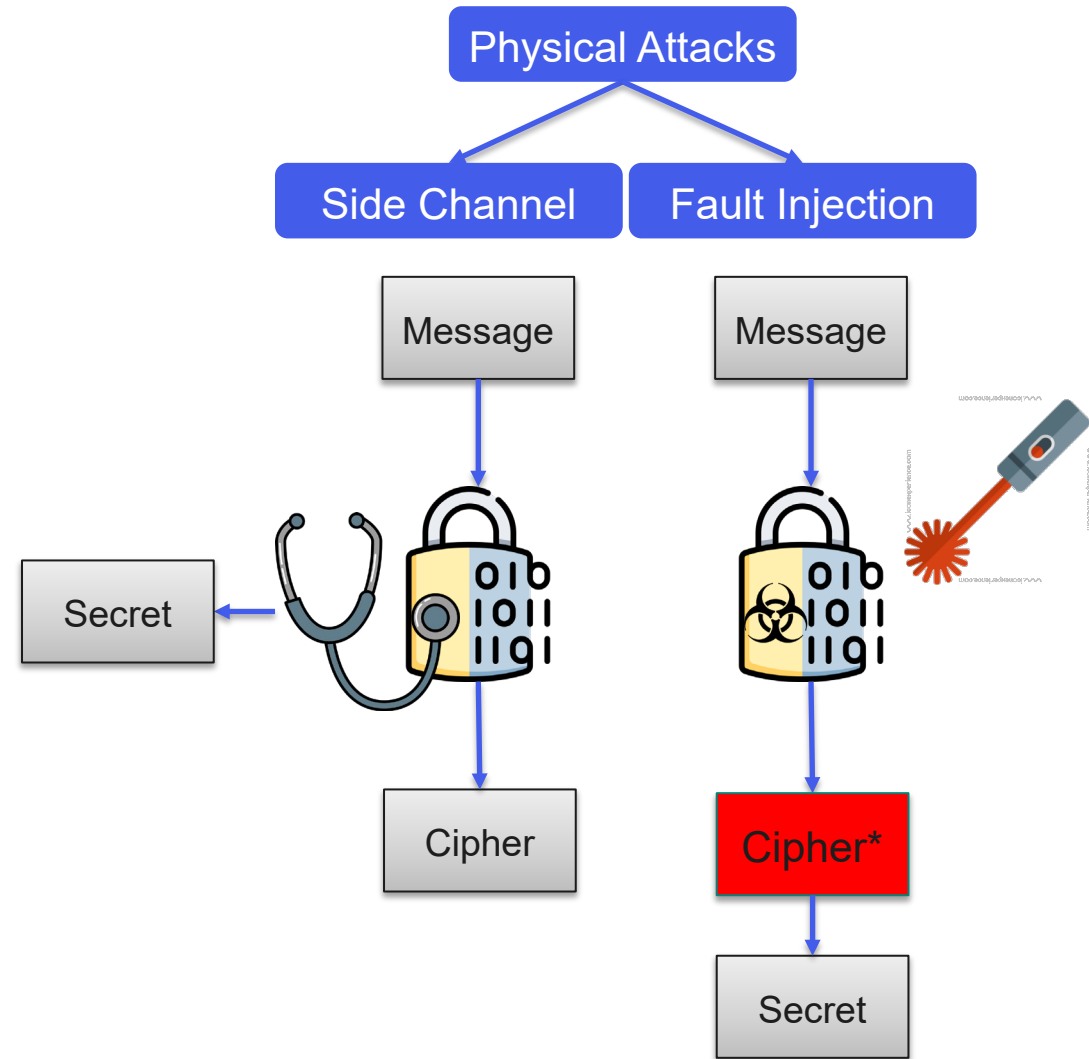
One such property where security and performance interact is resistance to side-channel attacks. **Schemes that can be made resistant to side-channel attack at minimal cost are more desirable than those whose performance is severely hampered by any attempt to resist side-channel attacks.** We further note that optimized implementations that address side-channel attacks (e.g., constant-time implementations) are more meaningful than those which do not. Finally, there are many different kinds of side-channel attacks, which require different kinds of access to the device being attacked. Attacks that can be carried out remotely, using only digital communications over a network, without physical access to the device being attacked, may be of special concern.



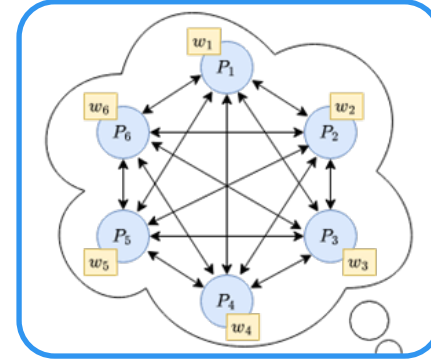
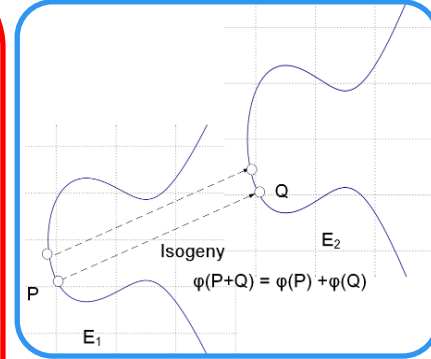
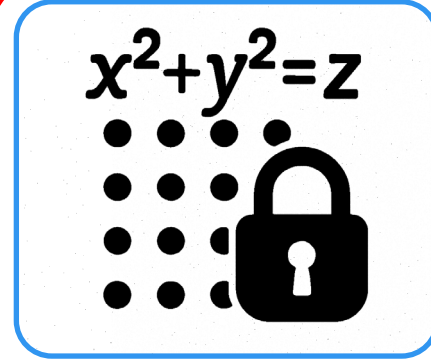
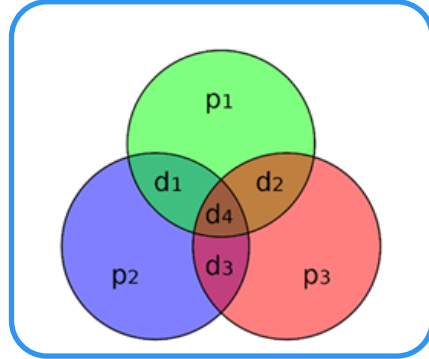
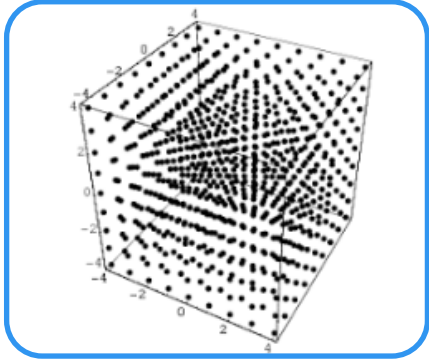
*From NISTs for Additional Digital Signature Schemes for the Post Quantum Cryptography Standardization Process*

# What is a Fault Attack?

- Intentionally cause errors in a system to leak information
  - Clock Glitching
  - Voltage Glitching
  - Laser injection
  - Electromagnetic Fault Injection
- Impact:
  - Skip an instruction
  - Random bit flips
  - Stuck at faults
- Countermeasures:
  - Error detection
  - Hardened Loops
  - Avoid boolean values to access critical functions



# What we did



**Lattice Based**

- HAWK

**Code Based**

- CROSS
- LESS

**Multivariate Based**

- UOV
- QR-UOV
- SNOVA
- MAYO

**Isogeny Based**

- SQISign

**MPCitH**

- Miath
- MQOM
- PERK
- RYDE
- SDitH
- FAEST

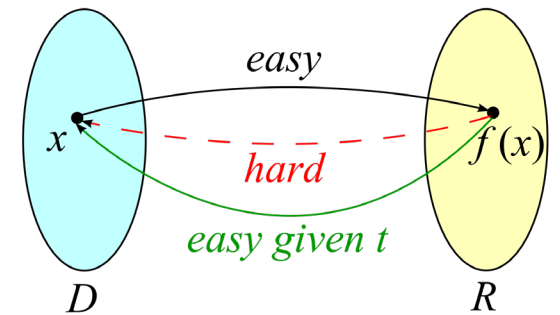
# MAYO

- Relies on the difficulty of solving multivariate quadratic equation systems
- Example: Solve for integers  $x$  and  $y$

$$\begin{aligned}x + 5x^2 + 3xy &= 4 \pmod{7} \\x^2 + 5xy + 5y^2 &= 1 \pmod{7}\end{aligned}$$

- Hard to solve, but easy given a trapdoor

- Public: Quadratic function  $P(x): \mathbb{F}_q^n \rightarrow \mathbb{F}_q^n$
- Secret: Oil space  $\mathcal{O} \subset \mathbb{F}_q^n$  on which  $P$  vanishes
- Signature:  $s$  such that  $P(s) = t$



## Why is $\mathcal{O}$ a trapdoor?

- Differential of  $P$

$$P'(x, y): \mathbb{F}_q^n \times \mathbb{F}_q^n \rightarrow \mathbb{F}_q^n:$$
$$P'(x, y) = P(x + y) - P(x) - P(y)$$

- Goal: find  $s$  s.t.  $P(s) = t$

- Pick random  $v \in \mathbb{F}_q^n$
- Find  $o \in \mathcal{O}$  s.t.  $P(v + o) = t$

$$P(v + o) = P(v) + \cancel{P(o)} + P'(v, o) = t$$

known

Linear in  $o$



- $m$ -dimensional Oil space can be seen as the column space  $\begin{bmatrix} \mathbf{0} \\ I_m \end{bmatrix}$

$$s = \begin{bmatrix} v \\ 0_m \end{bmatrix} + \begin{bmatrix} \mathbf{0} \\ I_m \end{bmatrix} x$$

# Fault Attack on MAYO

- Sign twice:

- $s = \begin{bmatrix} v \\ 0_m \end{bmatrix} + \begin{bmatrix} 0 \\ I_m \end{bmatrix} x$

- $s' = \begin{bmatrix} v \\ 0_m \end{bmatrix}$    $s - s' = \begin{bmatrix} 0 \\ I_m \end{bmatrix} x \in \mathcal{O}$   Recover all of  $\mathcal{O}$

- Two problems with this attack:

- Works only on deterministic MAYO

- Simple Countermeasure: Just check whether  $s$  and  $\begin{bmatrix} v \\ 0_m \end{bmatrix}$  are the same or not

# Fault Attack on MAYO

- Our attack:
  - Only skip the addition of one Index  $j \in \{0, \dots, n - m\}$  at a time

$$s'_i = \begin{cases} v_i, & i = j \\ s_i, & \text{else} \end{cases}$$

- Use Verification as an Oracle to find correction value  $\alpha \in \{0, \dots, 15\}$

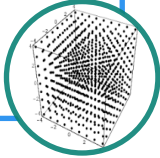
$$s''_j = s'_j + \alpha \quad \longrightarrow \quad o_j = \alpha$$

- Do this multiple times and use linear dependencies to recover whole Oil space

# What else has been done?

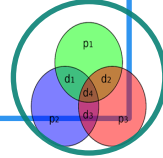
- HAWK

Lattice Based



- CROSS
- LESS

Code Based



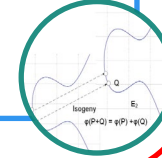
- UOV
- QR-UOV
- SNOVA
- MAYO

Multivariate Based



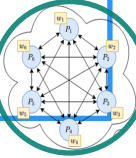
- SQIsign

Isogeny Based



- FAEST
- Miath
- PERK
- RYDE
- SDitH
- MQOM

MPCitH



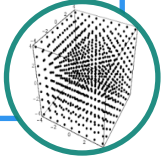
## Fault Attack on SQIsign

J. Lee, D. Heo, H. Kim, G. Kim, S. Kim, H. Kim, S. Hong  
PQCrypto 2024

# What else has been done?

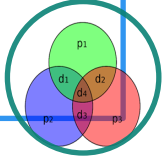
- HAWK

Lattice Based



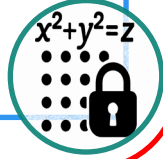
- CROSS
- LESS

Code Based



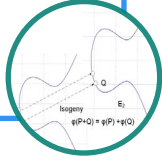
- UOV
- QR-UOV
- SNOVA
- MAYO

Multivariate Based



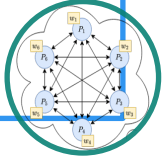
- SQISign

Isogeny Based



- FAEST
- Miath
- PERK
- RYDE
- SDitH
- MQOM

MPCitH



PQCrypto 2024

## SoK: On the Physical Security of UOV-based Signature Schemes

T. Aulbach, F. Campos, J. Krämer  
PQCrypto 2025

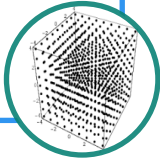
## Variables for Free: Fault Injection Attack on MAYO via Valid Solutions

Y. Zhong  
ePrint 2025/1808

# What else has been done?

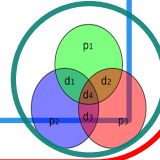
- HAWK

Lattice Based



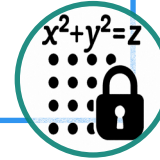
- CROSS
- LESS

Code Based



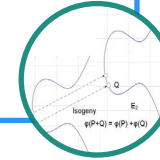
- UOV
- QR-UOV
- SNOVA
- MAYO

Multivariate Based



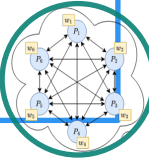
- SQISign

Isogeny Based



- FAEST
- Miath
- PERK
- RYDE
- SDitH
- MQOM

MPCitH



**ZKFault: Fault attack analysis on zero-knowledge based post-quantum digital signature schemes**

P. Mondal, S. Adhikary, S. Kundu, A. Karmakar, AsiaCrypt 2024

 PQCrypto 2025

 ePrint 2025/1808

 PQCrypto 2024

**Fault to Forge: Fault Assisted Forging Attacks on LESS Signature Scheme**

P. Mondal, S. Kundu, H. Nishiyama, S. Adhikary, D. Fujimoto, Y. Hayashi, A. Karmakar  
ePrint 2025/1838

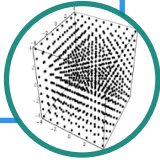
**Correction Fault Attack on CROSS under Unknown Bit Flips**

S. Jendral, E. Dubrova, Q. Guo, T. Johansson  
ePrint 2025/1885

# What else has been done?

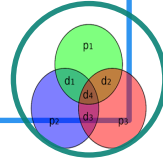
- HAWK

Lattice Based



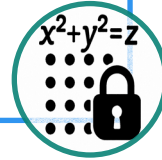
- CROSS
- LESS

Code Based



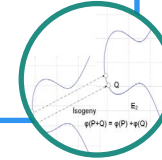
- UOV
- QR-UOV
- SNOVA
- MAYO

Multivariate Based



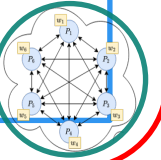
- SQISign

Isogeny Based




- FAEST\*
- Miath
- PERK
- RYDE
- SDitH
- MQOM\*\*

MPCitH



 AsiaCrypt 2024

 ePrint 2025/1838

 ePrint 2025/1885

 PQCrypto 2025

 ePrint 2025/1808

 PQCrypto 2024

**Side-Channel and Fault Injection Attacks on VOLEitH Signature Schemes: A Case Study of Masked FAEST**

S. Jendral, E. Dubrova  
ePrint 2025/378\*

**Fault Attacks on MPCitH Signature Schemes**

H. Banda, J. Brinkmann, J. Krämer  
ePrint 2025/1745

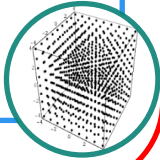
**Differential Fault Attacks on MQOM Breaking the Heart of Multivariate Evaluation**

V. Sarde, N. Debande  
ePrint 2025/1895\*\*

# Future directions

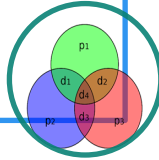
- HAWK

Lattice Based



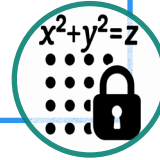
- CROSS
- LESS

Code Based



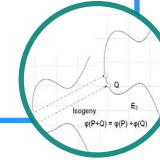
- UOV
- QR-UOV
- SNOVA
- MAYO

Multivariate Based



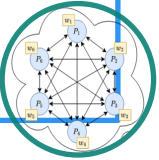
- SQISign

Isogeny Based




- FAEST
- Miath
- PERK
- RYDE
- SDitH
- MQOM

MPCitH



 AsiaCrypt 2024


 ePrint 2025/1838


 ePrint 2025/1885

 PQCrypto 2025

 ePrint 2025/1808

 PQCrypto 2024

 ePrint 2025/378

 ePrint 2025/1745

 ePrint 2025/1895

Beyond that:

- Come up with a countermeasure for FA on SpHincs+
- Study FA attacks on HQC
- FA on Aimer or underlying MPC-Friendly Cipher Aim