ASPDAC 2022

A Voltage Template Attack on the Modular Polynomial Subtraction in Kyber

Jianan Mu, Yixuan zhao, Zongyue Wang, Jing Ye, Junfeng Fan, Shuai Chen, Huawei Li, Xiaowei Li, Yuan Cao

State Key Laboratory of Computer Architecture,
Institute of Computing Technology, Chinese Academy of Sciences,
CASTEST, Open Security Research, Rock-Solid Security Lab, Fiberhome, Hohai University

Introduction

💻 Modern Cryptography

- Symmetric Cryptography: e.g., AES-128
- Hash Functions: e.g., SHA2-256
- Asymmetric Cryptography: RSA, ECC, etc

Introduction

Modern Cryptography vs Quantum Computers

- Symmetric Cryptography: e.g., AES-128
- Hash Functions: e.g., SHA2-256

→ Halved Security

- Asymmetric Cryptography: RSA, ECC, etc

→ Fully Compromised!

Introduction

Modern Cryptography vs Quantum Computers

- Symmetric Cryptography: e.g., AES-128
- Hash Functions: e.g., SHA2-256

→ Doubled Security

- Asymmetric Cryptography: RSA, ECC, etc

→ Post-Quantum Cryptography

National Institute of Standards and Technology (NIST)
Post Quantum Cryptography standardization competition

Introduction

NIST PQC standardization competition

	Key Encapsulation Mechanisms		Digital Signature Algorithms	
Type	Finalists	Alternates	Finalists	Alternates
Code-based	Classic McEliece	BIKE HQC		
Lattice-based	CRYSTALS-KYBER NTRU SABER	FrodoKEM NTRU Prime	CRYSTALS-DILITHIUM FALCON	
Isogeny-based		SIKE		
Multivariate			Rainbow	GeMSS
Zero-Knowledge				Picnic
Hash-based				SPHINCS+

Introduction

Post Quantum Cryptography Evaluation

Evaluation Criteria

NIST

Performance – measured on various classical platforms

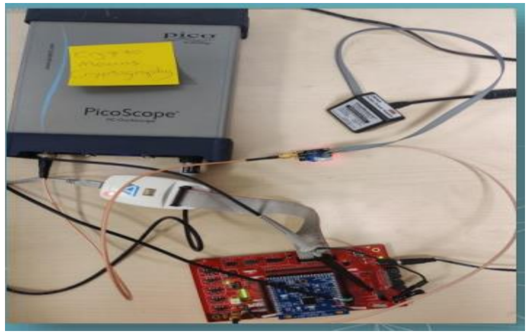
Other properties: Drop-in replacements, Perfect forward secrecy, Resistance to side-channel attacks, Simplicity and flexibility, Misuse resistance, etc.

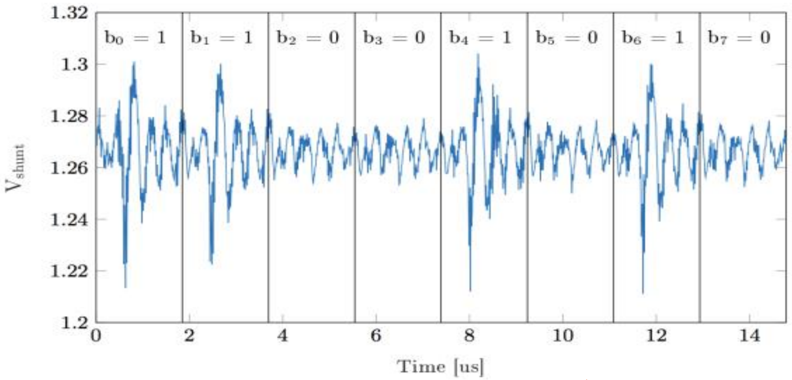
NIST repeatedly states the importance of side channel analysis (SCA) attack and countermeasures

D. Moody et al., “Status report on the second round of the nistpost-quantum cryptography standardization process,” 2020

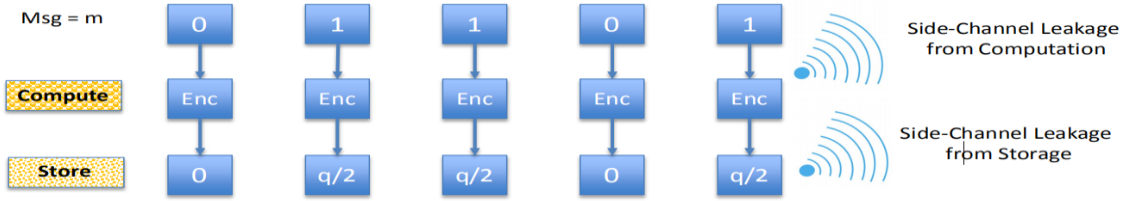
Introduction

SCA on PQC





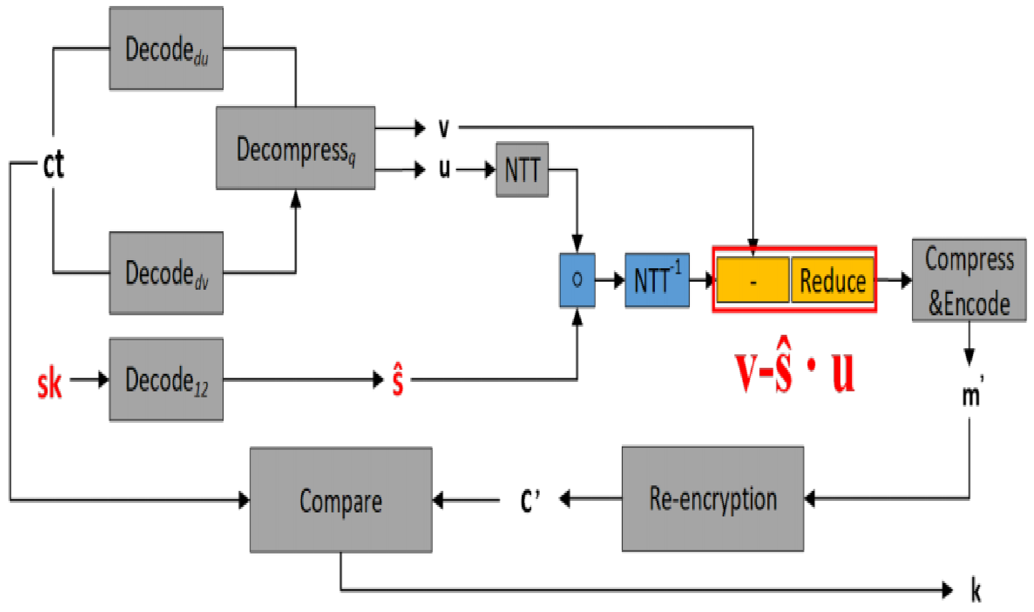
SCA of Message Encoding



Ravi P, Roy S S. Side-Channel Analysis of Lattice-based PQC Candidates[J].
Ravi P et al. Generic Side-channel attacks on CCA-secure lattice-based PKE and KEMs[J]. IACR Trans. Cryptogr. Hardw. Embed. Syst., 2020, 2020(3): 307-335.
Ravi P et al. Drop by Drop you break the rock-Exploiting generic vulnerabilities in Lattice-based PKE/KEMs using EM-based Physical Attacks[J]. Cryptology ePrint Archive, 2020.
Xu Z, Pemberton O M, Roy S S, et al. Magnifying side-channel leakage of lattice-based cryptosystems with chosen ciphertexts: The case study of kyber[J]. IEEE Transactions on Computers, 2021.

Contribution

Post Quantum Cryptography Evaluation



We reveal a new vulnerability under template attack for Kyber, the polynomial modular subtraction.

The recovering accuracy achieves 100% when using 2×11×15 traces, and it still achieves 98% when only using 2×11×2 traces.

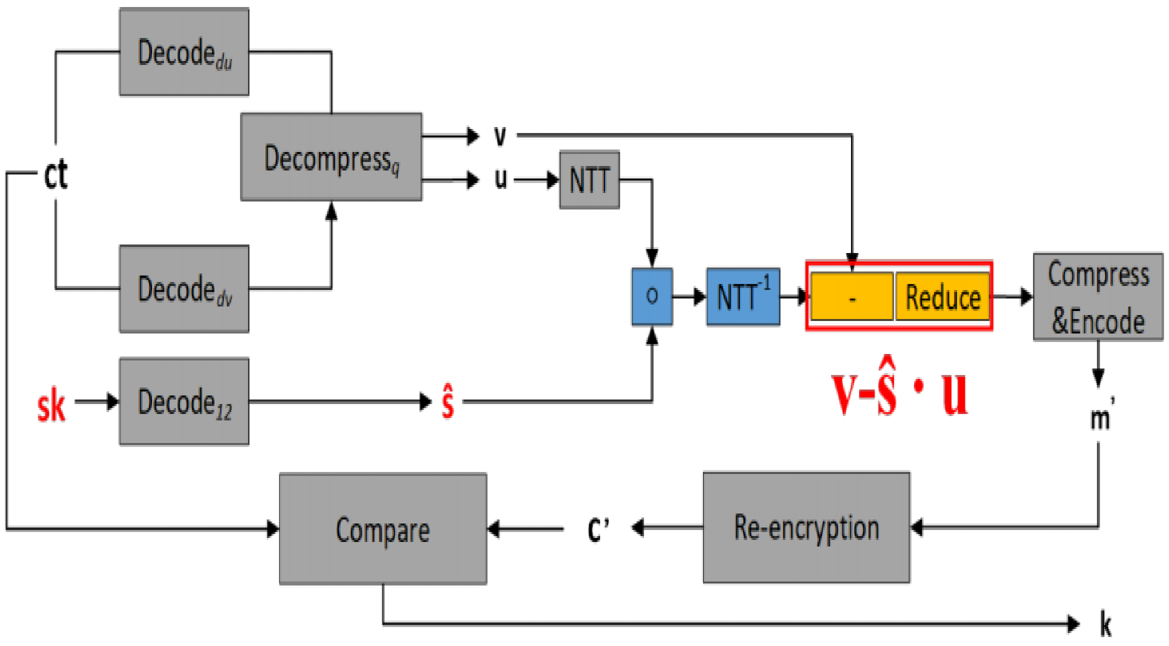
Methodology

Overview

- Attacking model: the attackers can master a profiling device similar to the target device.
  - To the mastered device, the secret key *sk*, and ciphertext *ct* can be controlled by attackers.
  - To the target device, the ciphertext can be chosen and controlled by attackers.
- Analyzing Kyber512 and locating the potential vulnerabilities.
- Learning phase: establish the templates.
- Attacking phase: retrieve the secrets.

Methodology

- Locate the vulnerability in Kyber



Algorithm 1 Kyber.CPAPKE.Dec(c,sk)

Input: Secret Key $sk \in \beta^{2\cdot k\cdot n/8}$
Input: Ciphertext $c \in \beta^{d_u\cdot k\cdot n/8+d_v\cdot n/8}$
Output: Message $m \in \beta^{32}$

1: $u := Decompress_q(Decode_{d_u}(c), d_u)$
2: $v := Decompress_q(Decode_{d_v}(c + d_u \cdot k \cdot n/8), d_v)$
3: $\hat{s} := Decode_{12}(sk)$
4: $m := Encode(Compress(v - NTT^{-1}(\hat{s} \circ NTT(u), 1))$
5: **return** m

Methodology

Secret key in Kyber

$$\begin{cases} sk \rightarrow \hat{s} = NTT(s), s = (sk_1, sk_2) \\ sk_1 = \boxed{a_{1,0}} + a_{1,1}x + a_{1,2}x^2 + \cdots + a_{1,255}x^{255} \\ sk_2 = a_{2,0} + a_{2,1}x + a_{2,2}x^2 + \cdots + a_{2,255}x^{255} \\ a_{i,j} \in [-3, 3],\ \ i \in [1, 2], j \in [0, 255]. \end{cases}$$

Chosen-ciphertext

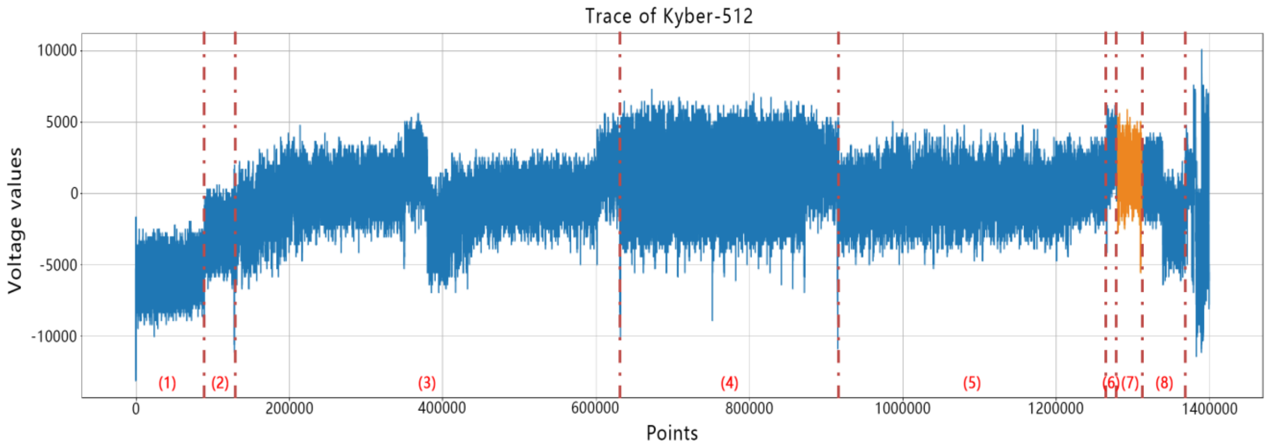
$$\begin{cases} u = (u_1, u_2) \\ u_1 = b_{1,0} + b_{1,1}x + b_{1,2}x^2 + \cdots + b_{1,255}x^{255} \\ u_2 = b_{2,0} + b_{2,1}x + b_{2,2}x^2 + \cdots + b_{2,255}x^{255} \\ v = b_{v,0} + b_{v,1}x + b_{v,2}x^2 + \cdots + b_{v,255}x^{255} \end{cases}$$

$$\begin{aligned} mp =& v - s \cdot u = -sk_1 \cdot u_1 \\ =& -h \cdot \boxed{a_{1,0}} - h \cdot a_{1,1}x \cdots - h \cdot a_{1,255}x^{255} \end{aligned}$$

Methodology

Leaning phase

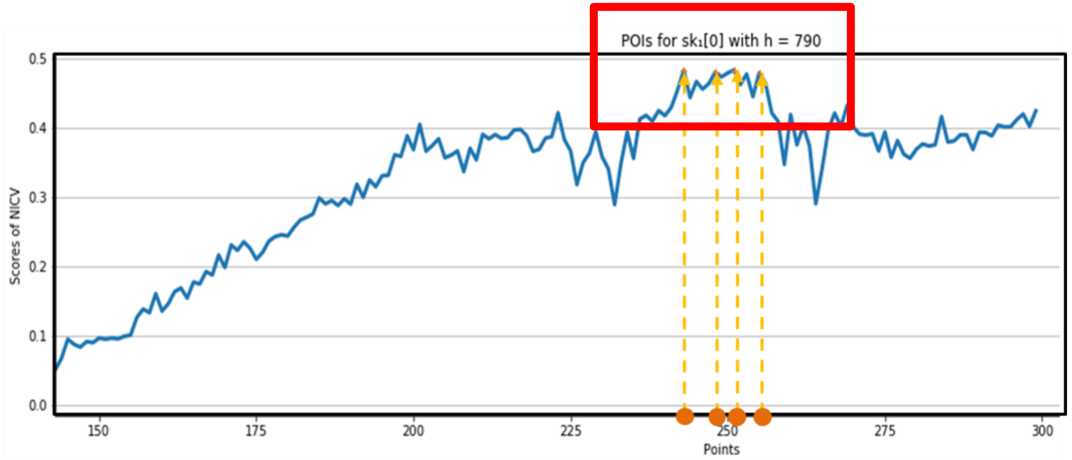
Collect voltage traces



Select points of interest (PoI)

normalized inter-class variance (NICV)

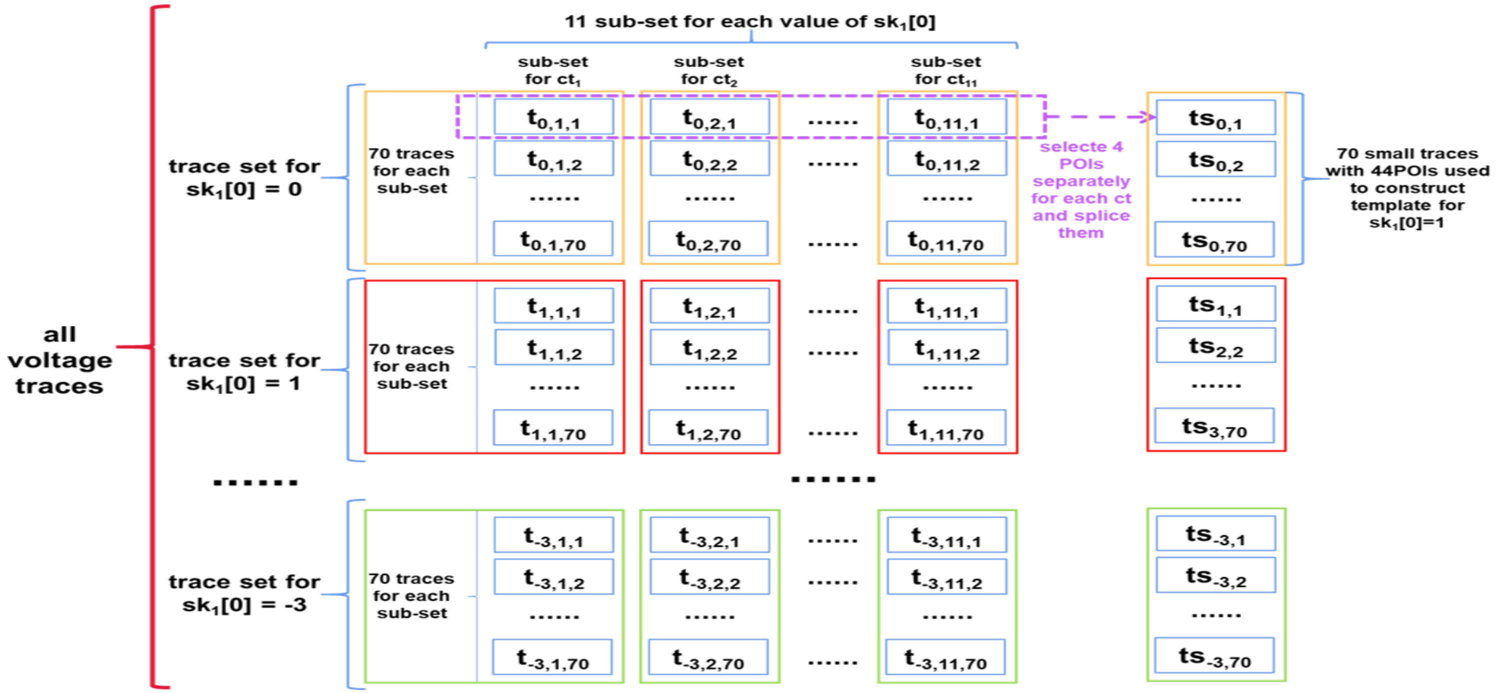
$$\begin{cases} \text{NICV: } \rho^2[\mathbb{E}[Y|X];Y] = \dfrac{Var[\mathbb{E}[Y|X]]}{\mathbb{E}[Y]}. \\ \rho^2(p^*) \rightarrow Var[\mathbb{E}[V(p^*)|sk_1[0]]] \end{cases}$$



Methodology

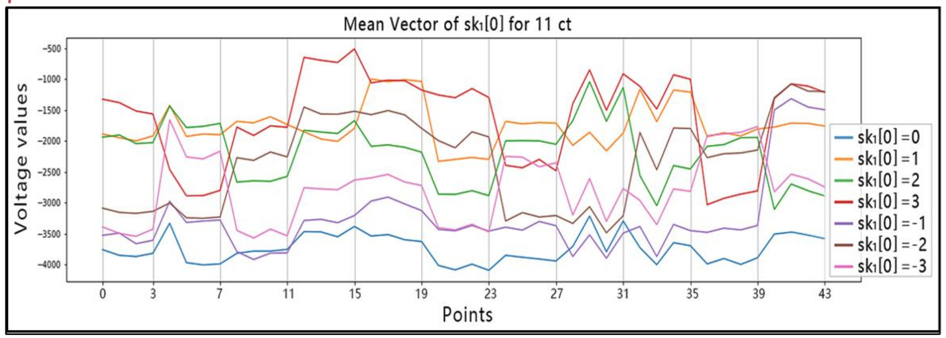
Learning phase

Splice PoI traces



Construct templates

$$
\begin{cases}
\mu_k = \dfrac{1}{|T_k|} \sum\limits_{ts \in T_k} ts_k \\
S_k = \dfrac{1}{|T_k| - 1} \sum\limits_{ts \in T_k} (ts - \mu_k)(ts - \mu_k)^T \\
S_{pooled} = \dfrac{1}{7} \sum\limits_{k} S_k
\end{cases}
$$

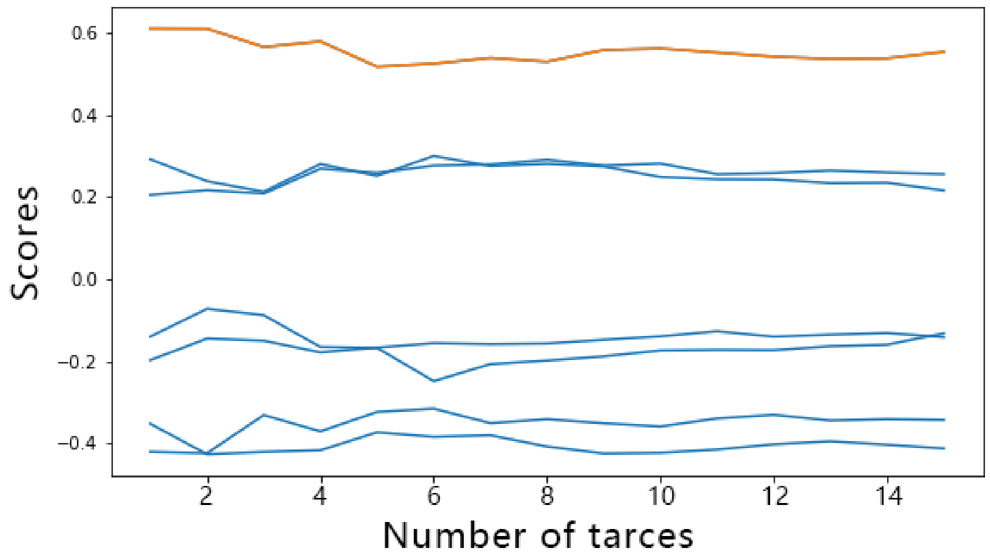


$$
S_{pooled} = \begin{bmatrix} \sigma_{1,1} & \sigma_{1,2} & \cdots & \sigma_{1,44} \\ \sigma_{2,1} & \sigma_{2,2} & \cdots & \sigma_{2,44} \\ \cdots & \cdots & \cdots & \cdots \\ \sigma_{44,1} & \sigma_{44,2} & \cdots & \sigma_{44,44} \end{bmatrix}
$$

Methodology & Evaluation

Attacking phase

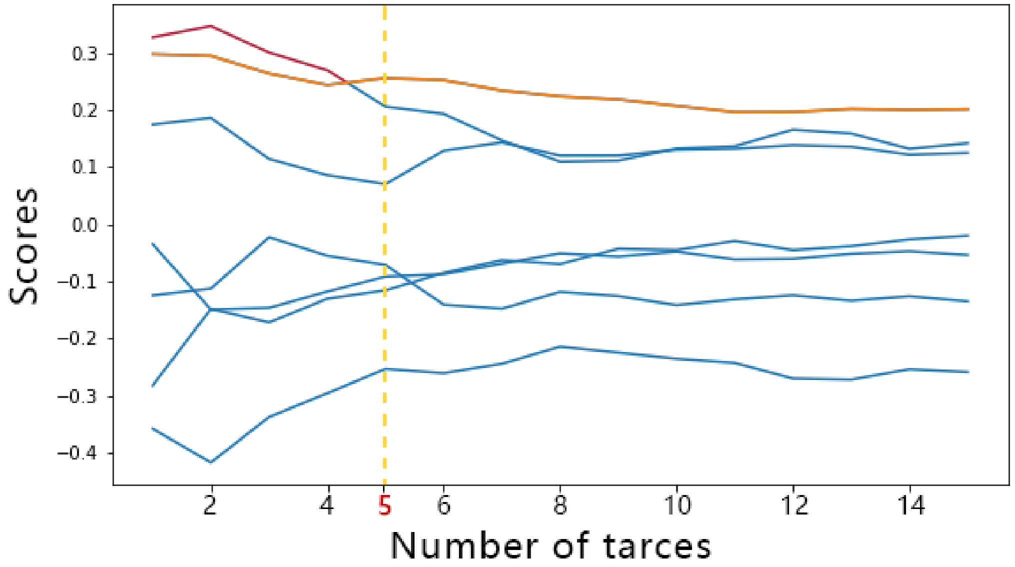
$$\begin{cases} C_{k,i} = \sqrt{(t_i - \mu_k)' S_{pooled}^{-1} (t_i - \mu_k)}; \\ C_k = \dfrac{1}{N_{ct}} \displaystyle\sum_{t_i \in T^*} C_{k,i}^2. \end{cases} \qquad (8)$$



Reference implementation of IND-CCA2 secure Kyber KEM (Kyber512 for particular)

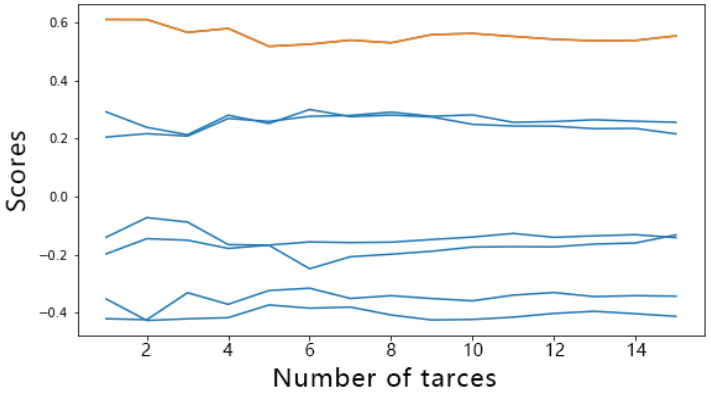
OSR407 boards
(STM32F407IG, ARM Cortex-M4) @53MHz.

Pico 3206D oscilloscope @250MHz.



Methodology & Evaluation

Evaluation



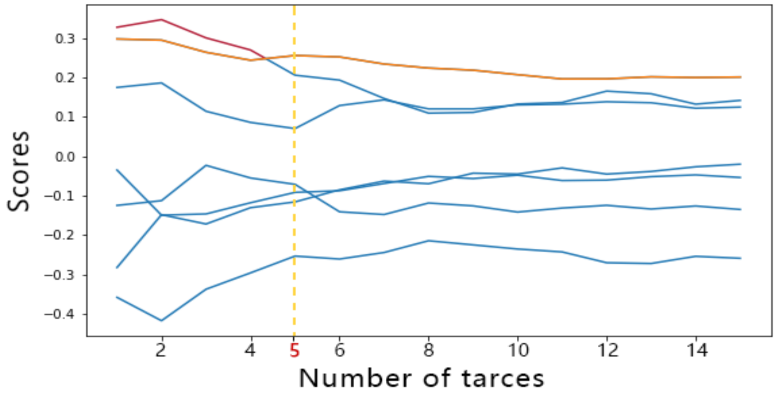


TABLE II

Recovering accuracy of using different N_{ct}

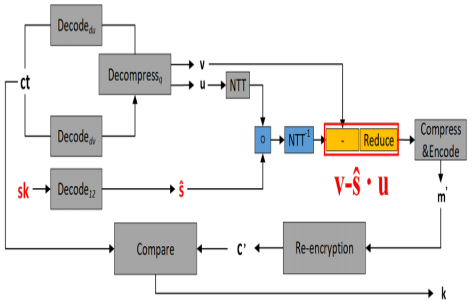
$vl_c \backslash N_{ct}$	1	2	5	15
0	94.4%	97.9%	100.0%	100.0%
1	86.6%	97.6%	97.6%	100.0%
2	97.7%	100.0%	100.0%	100.0%
3	97.7%	100.0%	100.0%	100.0%
-1	92.3%	93.1%	96.6%	100.0%
-2	92.2%	100.0%	100.0%	100.0%
-3	92.2%	100.0%	100.0%	100.0%
Total	93.5%	98.0%	99.0%	100.0%

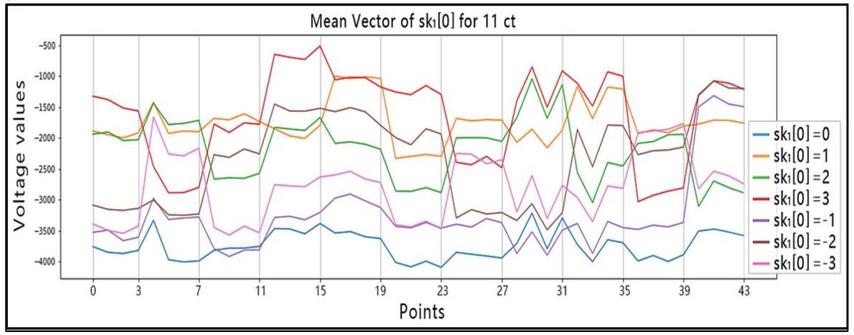
Experiments show that the recovering accuracy achieves 100% when using 2×11×15 = 330 traces, and it still achieves 98% when only using 2×11×2 = 44 traces.

Recap

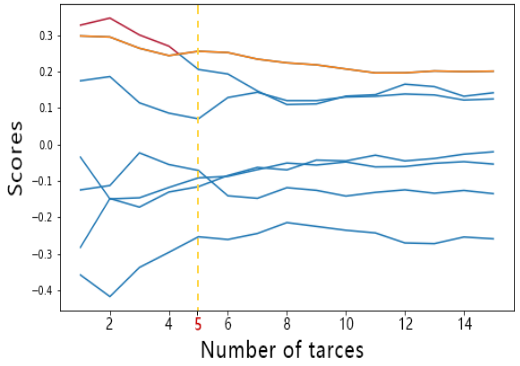
The contribution of this work

- We reveal a new vulnerability under template attack for Kyber, the polynomial modular subtraction.
- The recovering accuracy achieves 100% when using 2×11×15 =330 traces, and it still achieves 98% when only using 2×11×2 =44 traces.





$$S_{pooled} = \begin{bmatrix} \sigma_{1,1} & \sigma_{1,2} & \cdots & \sigma_{1,44} \\ \sigma_{2,1} & \sigma_{2,2} & \cdots & \sigma_{2,44} \\ \cdots & \cdots & \cdots & \cdots \\ \sigma_{44,1} & \sigma_{44,2} & \cdots & \sigma_{44,44} \end{bmatrix}$$



Thank you for listening!

Q&A

Jianan Mu, Yixuan zhao, Zongyue Wang, Jing Ye, Junfeng Fan,
Shuai Chen, Huawei Li, Xiaowei Li, Yuan Cao

State Key Laboratory of Computer Architecture,
Institute of Computing Technology, Chinese Academy of Sciences,
CASTEST, Open Security Research, Rock-Solid Security Lab, Fiberhome, Hohai University