NANYANG TECHNOLOGICAL UNIVERSITY SINGAPORE

Implementation Attacks on Post-Quantum Lattice-Based Cryptography

Prasanna Ravi (G1802146B)

under supervision of

Dr. Anupam Chattopadhyay

Dr. Shivam Bhasin

School of Computer Science and Engineering, NTU, Singapore

PhD Dissertation Defense

11th May 2023

Outline

- Motivation:
  - Post-Quantum Cryptography
  - Side-Channel Attacks (SCA) and Fault Injection Attacks (FIA)
  - Research Questions

- Research Contributions:
  - Side-Channel Attacks: Side-Channel Assisted Chosen-Ciphertext Attacks
    - Part-I: Binary PC Oracle-based SCA on LWE/LWR-based KEMs (TCHES-2020)
    - Part-II: Full-Decryption Oracle-based SCA on LWE/LWR-based KEMs (IEEE-TIFS-2021)
    - Part-III: SCA Assisted CCA on NTRU-based KEMs (TCHES-2022)

  - Fault-Injection Attacks:
    - Part-IV: Nonce-Reuse based FIA on LWE-based Schemes (COSADE-2019)
    - Part-V: FIA on the Number Theoretic Transform (NTT) (TCHES-2023)

  - Other-Contributions:

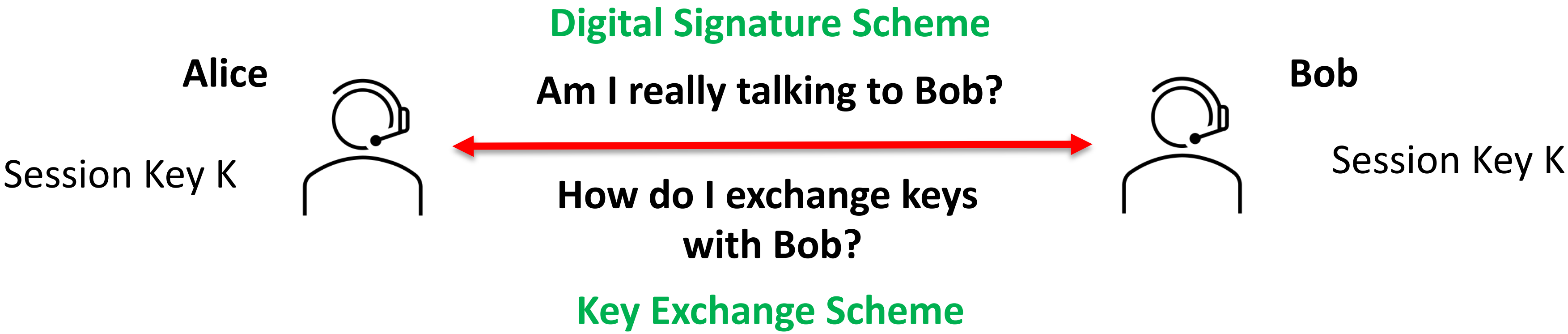
- Conclusion and Future Works:

Outline

- Motivation:
  - Post-Quantum Cryptography
  - Side-Channel Attacks (SCA) and Fault Injection Attacks (FIA)
  - Research Questions
- Research Contributions:
  - Side-Channel Attacks: Side-Channel Assisted Chosen-Ciphertext Attacks
    - Part-I: Binary PC Oracle-based SCA on LWE/LWR-based KEMs (TCHES-2020)
    - Part-II: Full-Decryption Oracle-based SCA on LWE/LWR-based KEMs (IEEE-TIFS-2021)
    - Part-III: SCA Assisted CCA on NTRU-based KEMs (TCHES-2022)
  - Fault-Injection Attacks:
    - Part-IV: Nonce-Reuse based FIA on LWE-based Schemes (COSADE-2019)
    - Part-V: FIA on the Number Theoretic Transform (NTT) (TCHES-2023)
  - Other-Contributions:
- Conclusion and Future Works:

Public-Key Cryptography (PKC)

- Foundation for security and trust when **Untrusted** parties
  - Net Banking, Online Gaming, Internet Commerce, Social Networking and many more…



- PKC we use today is based on:
  - Rivest-Shamir-Adleman (RSA): **Prime Factorization** problem (1977)
  - Elliptic Curve Cryptography (ECC): **Discrete Logarithm** problem (1983)
  - No Polynomial time algorithm to solve these problems on classical computers…

Life for Cryptographers was good!!!

Until...

In 1994….

Algorithms for Quantum Computation: Discrete Logarithms and Factoring

Peter W. Shor
AT&T Bell Labs
Room 2D-149
600 Mountain Ave.
Murray Hill, NJ 07974, USA

Abstract

A computer is generally considered to be a universal computational device; i.e., it is believed able to simulate any physical computational device with a cost in computation time of at most a polynomial factor. It is not clear whether this is still true when quantum mechanics is taken into consideration. Several researchers, starting with David Deutsch, have developed models for quantum mechanical computers and have investigated their computational properties. This paper gives Las Vegas algorithms for finding discrete logarithms and factoring integers on a quantum computer that take a number of steps which is polynomial in the input size, e.g., the number of digits of the integer to be factored. These two problems are generally considered hard on a classical computer and have been used as the basis of several proposed cryptosystems. (We thus give the first examples of quantum cryptanalysis.)

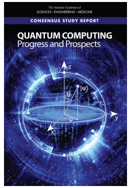
[1, 2]. Although he did not ask whether quantum mechanics conferred extra power to computation, he did show that a Turing machine could be simulated by the reversible unitary evolution of a quantum process, which is a necessary prerequisite for quantum computation. Deutsch [9, 10] was the first to give an explicit model of quantum computation. He defined both quantum Turing machines and quantum circuits and investigated some of their properties.

The next part of this paper discusses how quantum computation relates to classical complexity classes. We will thus first give a brief intuitive discussion of complexity classes for those readers who do not have this background. There are generally two resources which limit the ability of computers to solve large problems: time and space (i.e., memory). The field of analysis of algorithms considers the asymptotic demands that algorithms make for these resources as a function of the problem size. Theoretical computer scientists generally classify algorithms as efficient when the number of steps of the algorithms grows as a polynomial in the size of the input. The class of prob-

Quantum Threat for PKC

- Peter Shor in 1994 developed the **first quantum algorithm** that solves the factoring problem in **polynomial time**.

Cryptosystem	Category	Key Size	Quantum Algorithm	# Logical Qubits Required	# Physical Qubits Required	Time Required to Break System
RSA	Asymmetric-Key Encryption	1024	Shor's Algorithm	2,050	$8.05 \times \mathbf{10^6}$	**3.58 hours**
		2048		4,098	$8.56 \times \mathbf{10^6}$	**28.63 hours**
		4096		8,194	$1.12 \times \mathbf{10^7}$	**229 hours**
ECC Discrete-log problem	Asymmetric-Key encryption	256	Shor's Algorithm	2,330	$8.56 \times \mathbf{10^6}$	**10.5 hours**
		384		3,484	$9.05 \times \mathbf{10^6}$	**37.67 hours**
		521		4,719	$1.13 \times \mathbf{10^6}$	**55 hours**



[QComp19] Quantum Computing: Progress and Prospects (2019). Consensus Study Report. National Academies Press, 2019.

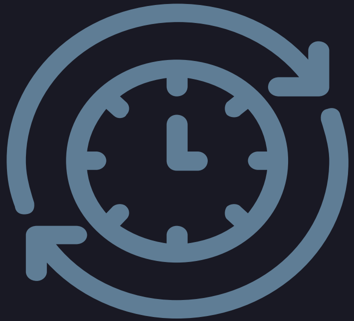
Advances in Quantum Computing

- Huge money is being invested by tech giants like Google, IBM, Intel towards developing the world's first quantum computer [D21, I21, AAB+19, W19].

- Rapid advances are being made in the field of quantum computing [5, 6]
  - Growing in capacity and computational power!!!

A Google Quantum Computer. PC Credits: shorturl.at/mtFIU

[D21] D-Wave demonstrates performance advantage in quantum simulation of exotic magnetism. by D-Wave Systems. https://phys.org/news/2021-02-d-wave-advantage-quantum-simulation-exotic.html
[I21] IBM promises 1000-qubit quantum computer—a milestone—by 2023. Adrian Cho. shorturl.at/loyGT
[AAB+19] Arute, Frank, Kunal Arya, Ryan Babbush, Dave Bacon, Joseph C. Bardin, Rami Barends, Rupak Biswas et al. "Quantum supremacy using a programmable superconducting processor." *Nature* 574, no. 7779 (2019): 505-510.
[W19] Quantum computing takes flight. William D. Oliver. Nature. NEWS AND VIEWS 23 OCTOBER 2019



Countdown to Y2Q

07	31	10	53	35
Years	Days	Hours	Minutes	Seconds

https://globalriskinstitute.org/publication/2022-quantum-threat-timeline-report/
https://cloudsecurityalliance.org/research/working-groups/quantum-safe-security/

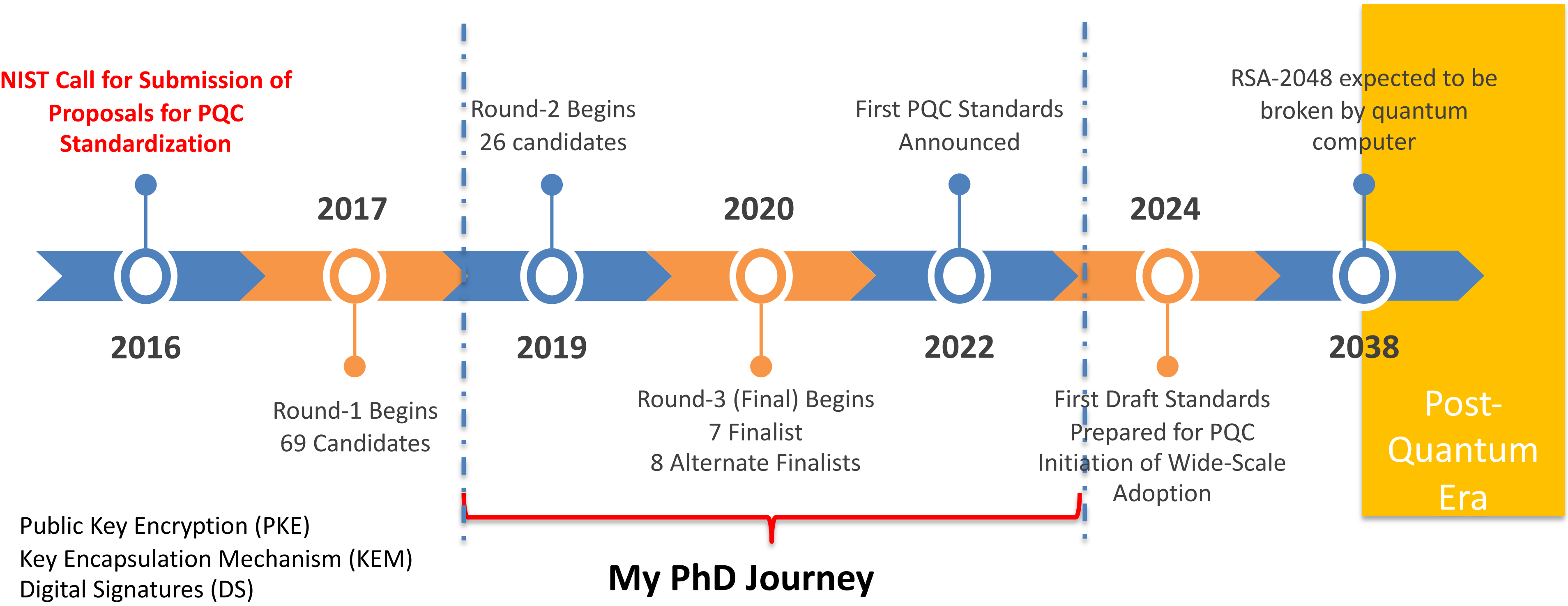
Post-Quantum Cryptography:

Cryptography built upon alternate hard problems

(Conjectured to be hard enough for classical and quantum computers)

PQC can run on classical devices!!!

Post-Quantum Cryptography (PQC)



Public Key Encryption (PKE)
Key Encapsulation Mechanism (KEM)
Digital Signatures (DS)

NIST PQC Standardization: (2017-2022)

First NIST PQC Standards (US):

PKE/KEMs	Digital Signatures
Kyber	Dilithium
	FALCON
	SPHINCS+

BSI Recommendations (Germany):

PKE/KEMs	Digital Signatures
FrodoKEM	XMSS
Classic Mceliece	LMS

Lattice-based

Hash-based

Code-based

[AAC+22] Alagic, Gorjan, Daniel Apon, David Cooper, Quynh Dang, Thinh Dang, John Kelsey, Jacob Lichtinger et al. "Status report on the third round of the NIST post-quantum cryptography standardization process." *US Department of Commerce, NIST* (2022).
[B22] Quantum-safe cryptography – fundamentals, current developments and recommendations, Federal Office for Information Security, Germany, 2022.

Classification of PQC finalists and alternative candidates

- NIST Standard (green)
- BSI Standard (orange)

Lattice-based Cryptography

- **Public Key Encryption (PKE)/ Key Encapsulation Mechanisms (KEM)**
  - **Learning With Errors (LWE)/ Learning With Rounding (LWR) Problem**
    (**Kyber**, SABER, **Frodo**)
  - **Nth Order Truncated Polynomial Ring Unit (NTRU) Problem**
    (NTRU, NTRUPrime)
- **Digital Signature Schemes (DSS)**
  - **LWE/LWR Problem**
    (**Dilithium**)
  - **NTRU-based**
    (**FALCON**)

In a Possible Future with Quantum Computers

Security in Quantum Era: NIST PQC Call

- **Selection Criteria for Standardization Process:**
  - Theoretical PQ Security
  - Performance (Speed, Area, latency, Power) on HW/SW platforms
  - **Resistance against Side-Channel Attacks (SCA) and Fault Injection Attacks (FIA)**

- NIST explicitly states that "*encourages additional research regarding side-channel analysis*" of the finalist candidates and that it "*hopes to collect more information about the costs of implementing these algorithms in a way that provides resistance to such attacks*" [9].

- **We talk about Quantum Attack Resistance, then what is this SCA and FIA???**

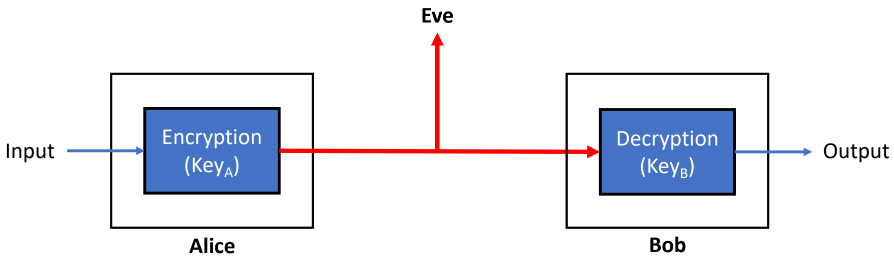
[ASA+20] Alagic, Gorjan, Jacob Alperin-Sheriff, Daniel Apon, David Cooper, Quynh Dang, John Kelsey, Yi-Kai Liu et al. *Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process*. No. NIST Internal or Interagency Report (NISTIR) 8309. National Institute of Standards and Technology, 2020.

Outline

- **Motivation:**
  - Post-Quantum Cryptography
  - **Side-Channel Attacks (SCA) and Fault Injection Attacks (FIA)**
  - Research Questions
- Research Contributions:
  - Side-Channel Attacks: Side-Channel Assisted Chosen-Ciphertext Attacks
    - Part-I: Binary PC Oracle-based SCA on LWE/LWR-based KEMs (TCHES-2020)
    - Part-II: Full-Decryption Oracle-based SCA on LWE/LWR-based KEMs (IEEE-TIFS-2021)
    - Part-III: SCA Assisted CCA on NTRU-based KEMs (TCHES-2022)
  - Fault-Injection Attacks:
    - Part-IV: Nonce-Reuse based FIA on LWE-based Schemes (COSADE-2019)
    - Part-V: FIA on the Number Theoretic Transform (NTT) (TCHES-2023)
  - Other-Contributions:
- Conclusion and Future Works:

Side-Channel Analysis (SCA) and Fault Injection Analysis (FIA)

- Security proofs governing cryptographic algorithms make a big assumption:
  - Cryptosystem is a "Non-tamperable Black-Box"



Traditional Model for Cryptanalysis

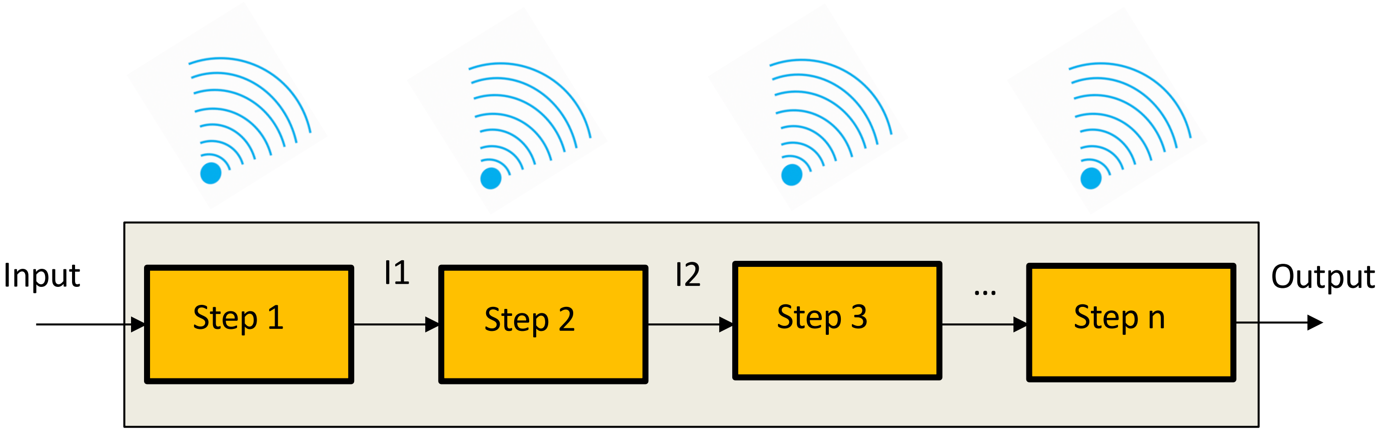
- **Assumption-1**: Attacker cannot know anything apart from the output of the cryptosystem
- **Assumption-2**: Attacker cannot tamper the operation of the cryptosystem

- **Big Question: Are these assumptions true in practice?**

Side-Channel Analysis (SCA) and Fault Injection Analysis (FIA)

- **Reality**: This ideal black-box does not exist!!!

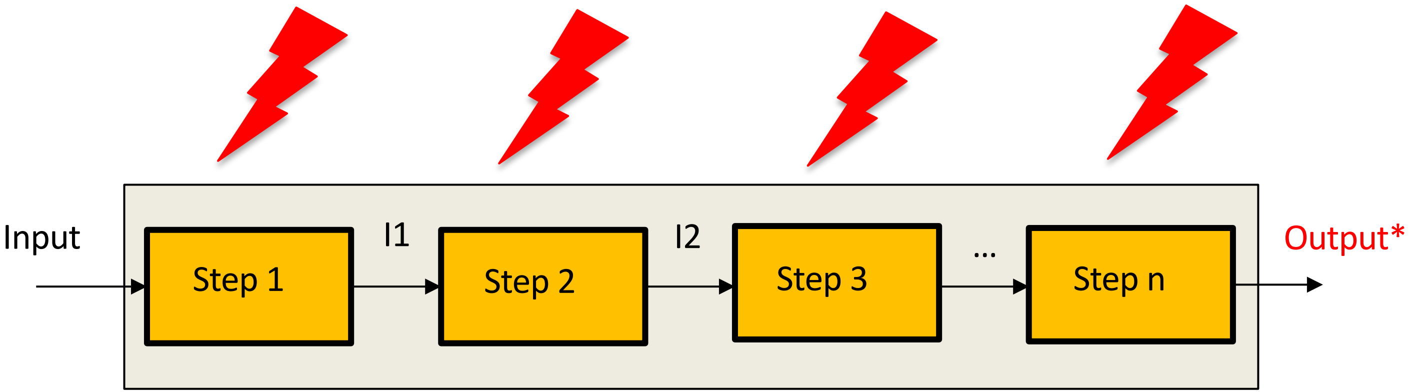
- Cryptosystem is ultimately implemented on our electronic devices:
    - Physical Leakage in the form of Power Consumption, Electromagnetic Emanation (EM), …
        - **Side-Channel Attacks (SCA)**



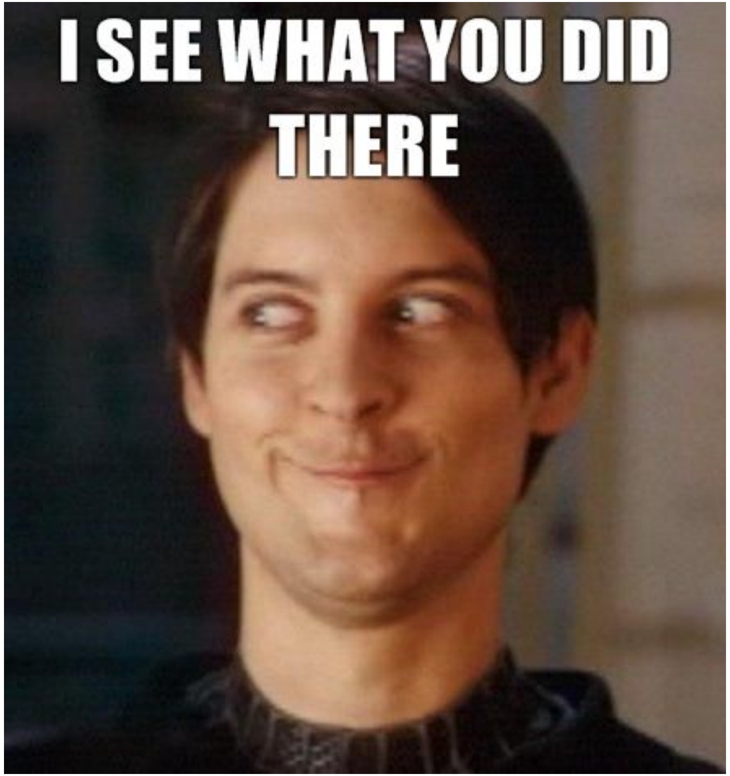
Side-Channel Analysis (SCA) and Fault Injection Analysis (FIA)

- **Reality**: This ideal black-box does not exist!!!

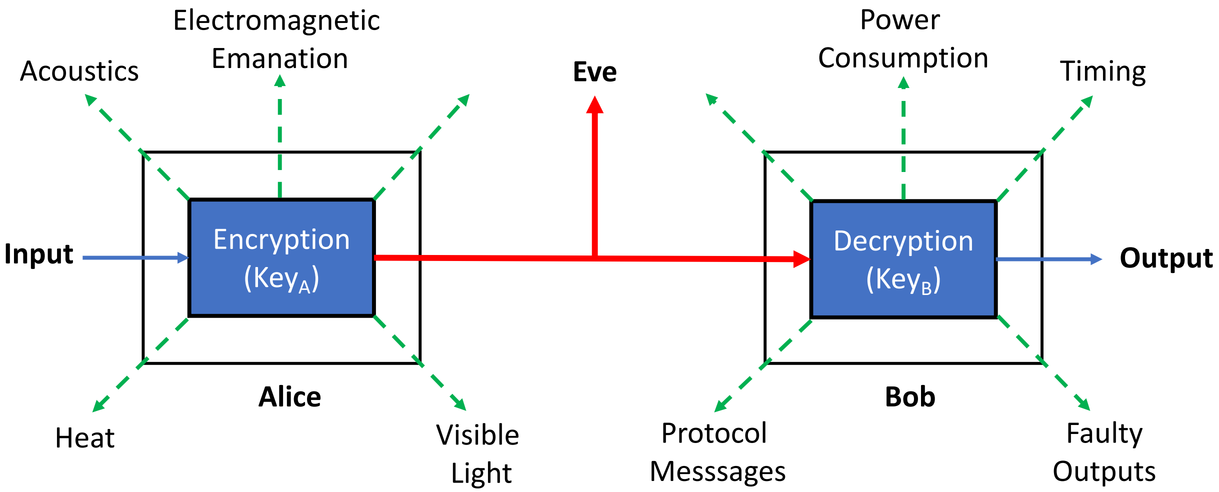
- Cryptosystem is ultimately implemented on our electronic devices:
  - Physical Leakage in the form of Power Consumption, Electromagnetic Emanation (EM), …
    - **Side-Channel Attacks (SCA)**
  - Inject errors in computation through Voltage/Clock Glitch, Laser, EM Pulse
    - **Fault-Injection Attacks (FIA)**



Side-Channel Analysis (SCA) and Fault Injection Analysis (FIA)



Side-Channel Analysis (SCA) and Fault Injection Analysis (FIA)



Revised (Realistic) Model for Cryptanalysis

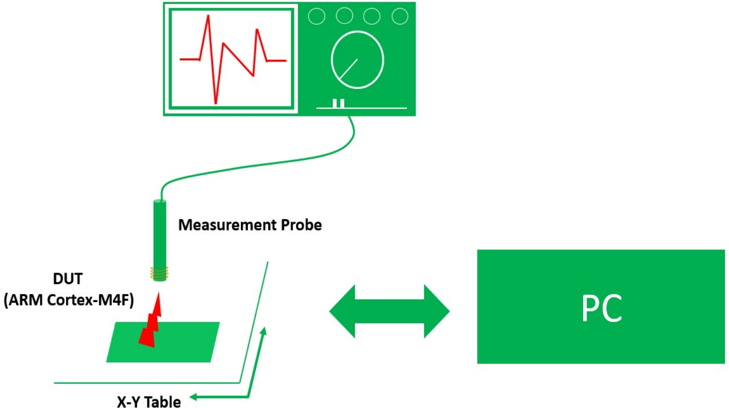
Relevance of SCA and FIA

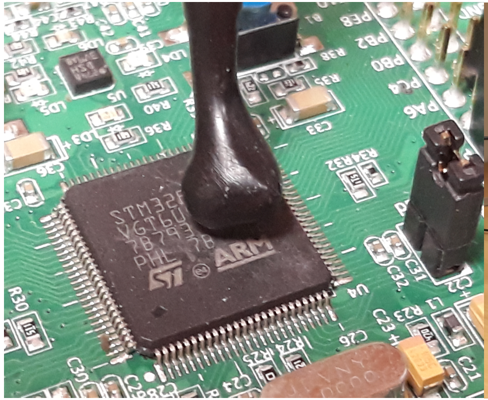
- **Embedded Era**: Wide-scale proliferation of embedded devices.

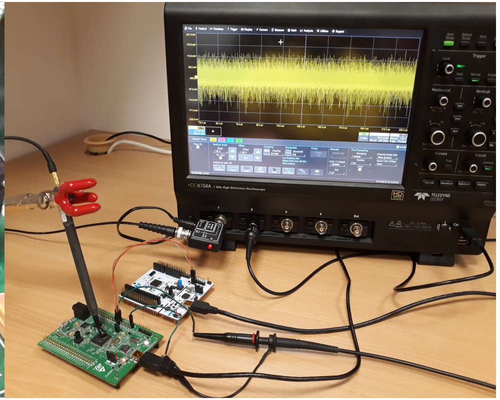
- Embedded devices typically deployed in **remote locations** where an adversary can obtain easy physical access to the device (**adversary might be the user!!**)

- **PQC on embedded devices susceptible to SCA and FIA!!**

SCA Setup: Electromagnetic Emanation

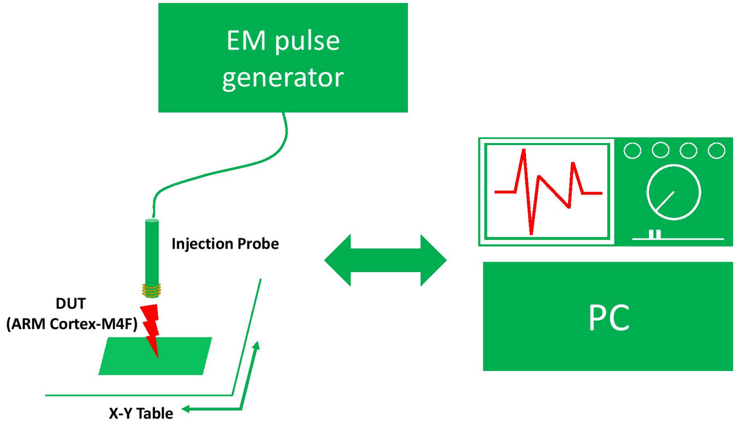






- ❑ Current loops within the device emanate data switching activity as EM waves
- ❑ Electromagnetic Emanation (EM) from target device is captured using a near-field EM probe.

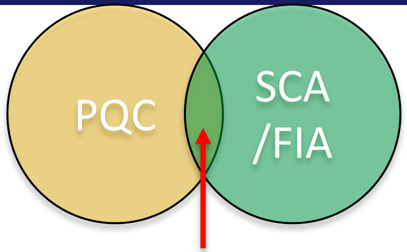
FIA Setup: Electromagnetic Fault Injection



- **High Voltage** (upto 200v) and **short pulses** (2-10 nsec) are injected on top of the chip
- Induces additional currents within device disrupting operation and inducing errors

Outline

- **Motivation:**
  - Post-Quantum Cryptography
  - Side-Channel Attacks (SCA) and Fault Injection Attacks (FIA)
  - **Research Questions**



- Research Contributions:
  - Side-Channel Attacks: Side-Channel Assisted Chosen-Ciphertext Attacks
    - Part-I: Binary PC Oracle-based SCA on LWE/LWR-based KEMs (TCHES-2020)
    - Part-II: Full-Decryption Oracle-based SCA on LWE/LWR-based KEMs (IEEE-TIFS-2021)
    - Part-III: SCA Assisted CCA on NTRU-based KEMs (TCHES-2022)
  - Fault-Injection Attacks:
    - Part-IV: Nonce-Reuse based FIA on LWE-based Schemes (COSADE-2019)
    - Part-V: FIA on the Number Theoretic Transform (NTT) (TCHES-2023)
  - Other-Contributions:
- Conclusion and Future Works:

Research Questions:

- **Question-1:** What types of SCA/FIA are possible on lattice-based schemes?

- **Question-2:** Compared to RSA/ECC, how vulnerable are they to SCA/FIA? Are there any inherent properties that make them susceptible to SCA/FIA ?

- **Question-3:** Can SCA/FIA be used as a criteria to differentiate between different lattice-based schemes?

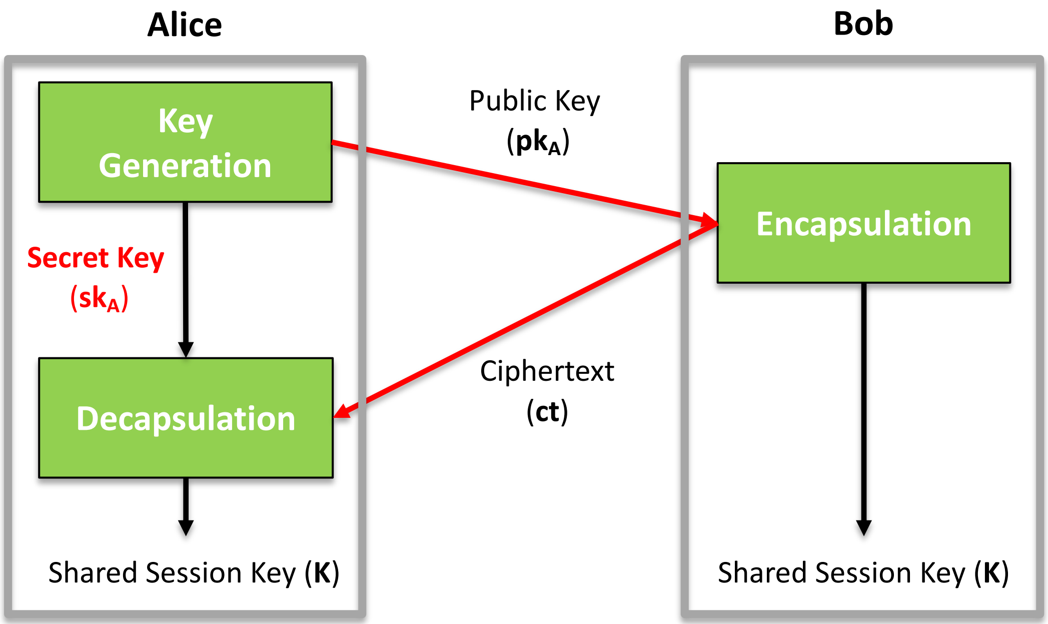
- **Question-4:** What types of countermeasures can be deployed to protect against SCA/FIA? What are the overheads they incur?

Outline

- Motivation:
  - Post-Quantum Cryptography
  - Side-Channel Attacks (SCA) and Fault Injection Attacks (FIA)
  - Research Questions
- **Research Contributions:**
  - **Side-Channel Attacks: Side-Channel Assisted Chosen-Ciphertext Attacks on lattice-based KEMs**
    - Part-I: Binary PC Oracle-based SCA on LWE/LWR-based KEMs (TCHES-2020)
    - Part-II: Full-Decryption Oracle-based SCA on LWE/LWR-based KEMs (IEEE-TIFS-2021)
    - Part-III: SCA Assisted CCA on NTRU-based KEMs (TCHES-2022)
  - Fault-Injection Attacks:
    - Part-IV: Nonce-Reuse based FIA on LWE-based Schemes (COSADE-2019)
    - Part-V: FIA on the Number Theoretic Transform (NTT) (TCHES-2023)
  - Other-Contributions:
- Conclusion and Future Works:

Key Encapsulation Mechanisms (KEMs)

- **Use**: Derive a shared key between two untrusted parties.



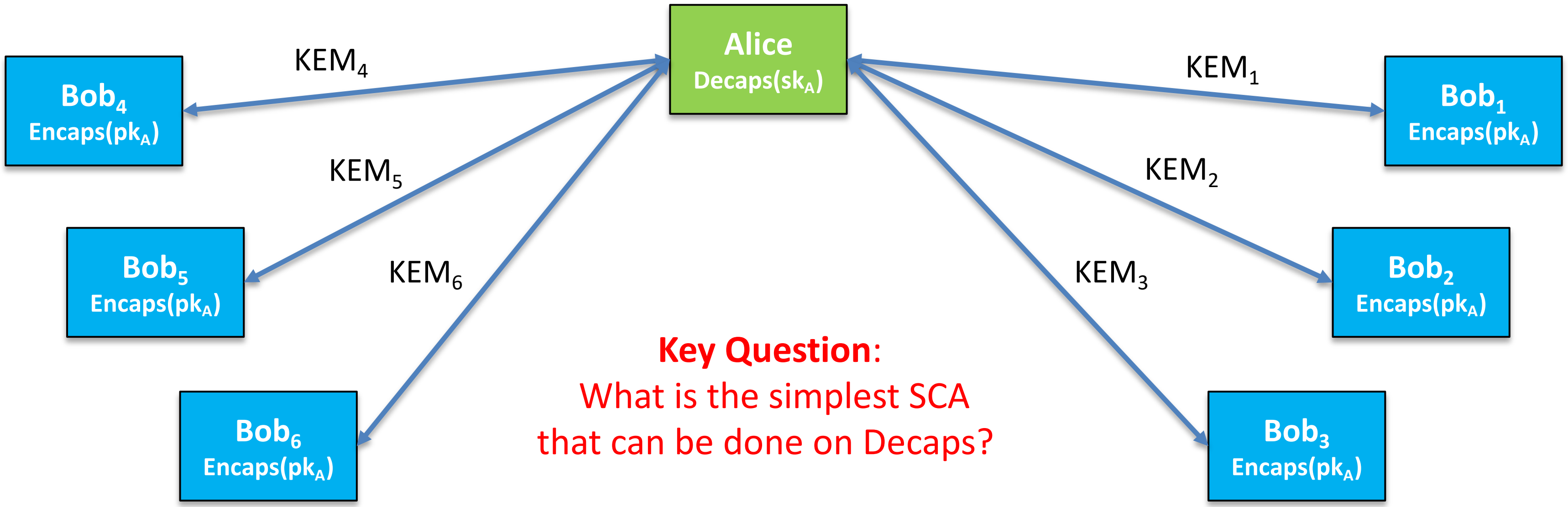
Two Modes:

Ephemeral Mode
New (pk_A,sk_A) to derive new session key

✓ **Static Mode**
Same (pk_A,sk_A) to derive multiple session keys

KEMs in Static Mode

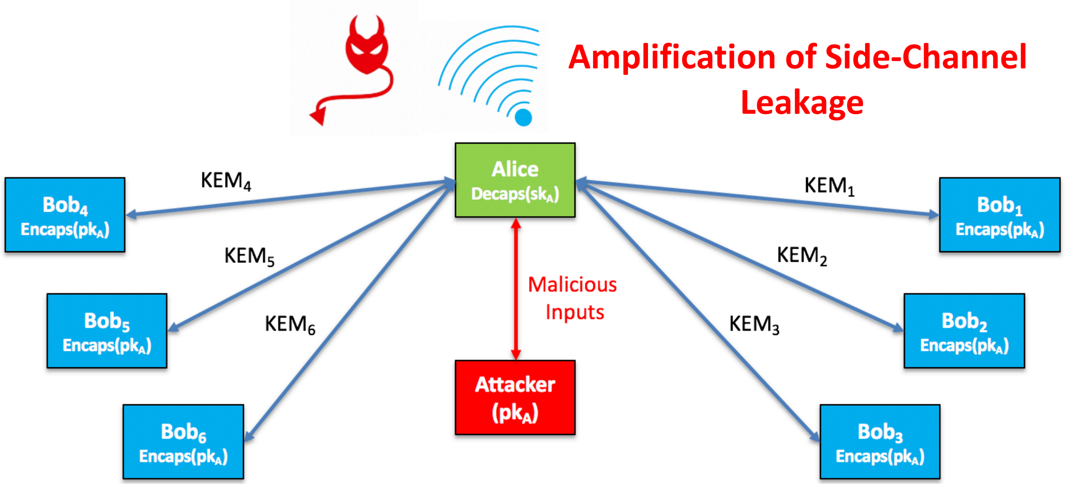
Same Secret manipulated across multiple executions



Key Question:
What is the simplest SCA that can be done on Decaps?

Contribution: SCA Assisted Chosen-Ciphertext Attacks

- We proposed the concept of "SCA Assisted Chosen-Ciphertext Attacks" for lattice-based schemes [TCHES-2020: **R**RCB20, IEEE-TIFS-2021: **R**BRC21, TCHES-2022: **R**EB+22]



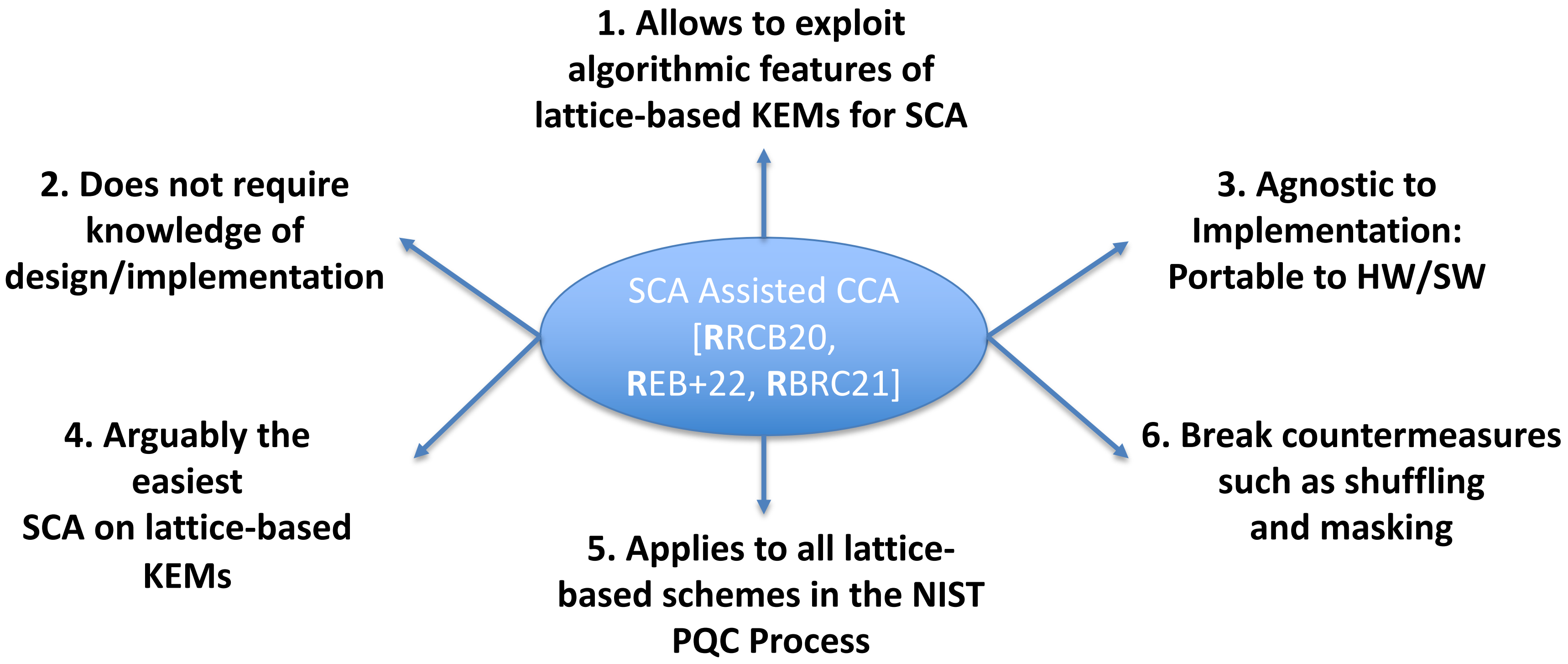
Main Finding:
Query the decapsulation procedure with malicious/handcrafted inputs to amplify side-channel leakage

[RRCB20] **Ravi, Prasanna**, Sujoy Sinha Roy, Anupam Chattopadhyay, and Shivam Bhasin. "Generic Side-channel attacks on CCA-secure lattice-based PKE and KEMs." *IACR Transactions on Cryptographic Hardware and Embedded Systems* (2020): 307-335

[RBRC21] **Ravi, Prasanna**, Shivam Bhasin, Sujoy Sinha Roy, and Anupam Chattopadhyay. "On exploiting message leakage in (few) NIST PQC candidates for practical message recovery attacks." *IEEE Transactions on Information Forensics and Security* 17 (2021): 684-699.

[REB+22] **Ravi, Prasanna**, Martianus Frederic Ezerman, Shivam Bhasin, Anupam Chattopadhyay, and Sujoy Sinha Roy. "Will You Cross the Threshold for Me? Generic Side-Channel Assisted Chosen-Ciphertext Attacks on NTRU-based KEMs." *IACR Transactions on Cryptographic Hardware and Embedded Systems* (2022): 722-761.

Contribution: SCA Assisted Chosen-Ciphertext Attacks



Outline

- Motivation:
  - Post-Quantum Cryptography
  - Side-Channel Attacks (SCA) and Fault Injection Attacks (FIA)
  - Research Questions
- **Research Contributions:**
  - **Side-Channel Attacks: Side-Channel Assisted Chosen-Ciphertext Attacks on lattice-based KEMs**
    - **Part-I: Binary PC Oracle-based SCA on LWE/LWR-based KEMs (TCHES-2020)**
    - Part-II: Full-Decryption Oracle-based SCA on LWE/LWR-based KEMs (IEEE-TIFS-2021)
    - Part-III: SCA Assisted CCA on NTRU-based KEMs (TCHES-2022)
  - Fault-Injection Attacks:
    - Part-IV: Nonce-Reuse based FIA on LWE-based Schemes (COSADE-2019)
    - Part-V: FIA on the Number Theoretic Transform (NTT) (TCHES-2023)
  - Other-Contributions:
- Conclusion and Future Works:

Contribution-I: Binary PC Oracle-based SCA on LWE/LWR-based KEMs

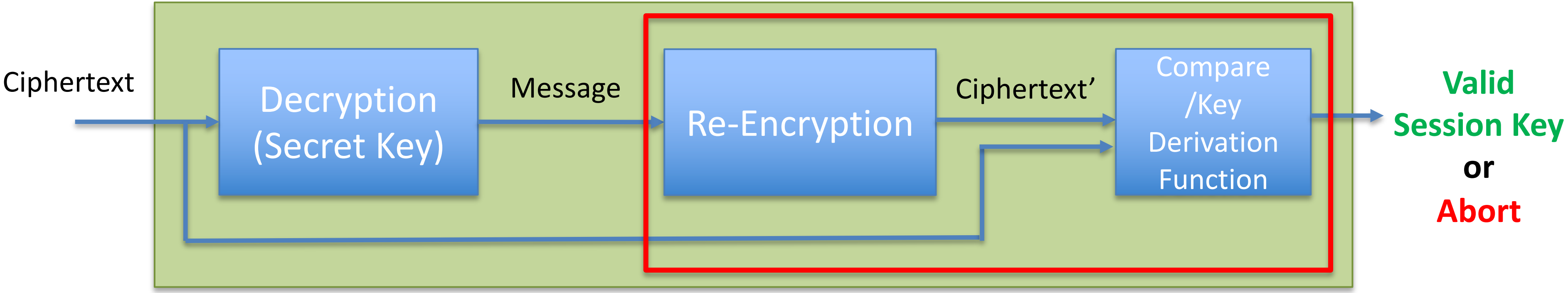
Valid Ciphertext:

- ❑ Generated from Encapsulation Procedure

Invalid Ciphertext:

- ❑ Randomly Sampled
- ❑ Valid Ciphertext with Errors

Theoretically Secure Against Chosen-Ciphertext Attacks



Decapsulation Procedure

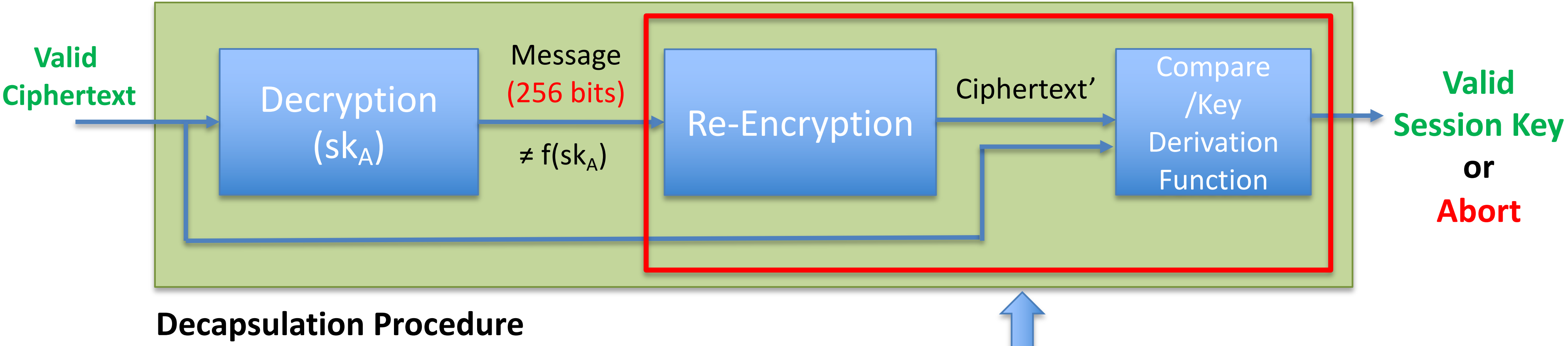
Fujisaki-Okamoto (FO) Transform

Checks Validity of Ciphertext

[RRCB20] **Ravi, Prasanna**, Sujoy Sinha Roy, Anupam Chattopadhyay, and Shivam Bhasin. "Generic Side-channel attacks on CCA-secure lattice-based PKE and KEMs." *IACR Transactions on Cryptographic Hardware and Embedded Systems* (2020): 307-335

Contribution-I: Binary PC Oracle-based SCA on LWE/LWR-based KEMs

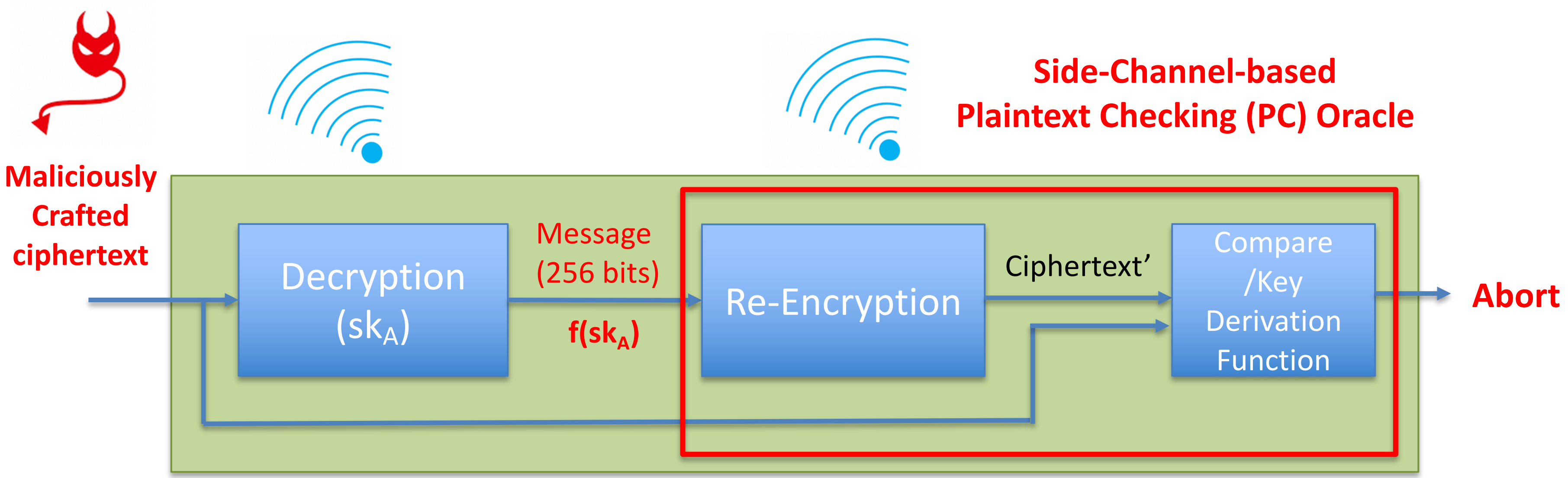
No Leakage of secret key from FO Transform



Checks Validity of Ciphertext

[RRCB20] **Ravi, Prasanna**, Sujoy Sinha Roy, Anupam Chattopadhyay, and Shivam Bhasin. "Generic Side-channel attacks on CCA-secure lattice-based PKE and KEMs." *IACR Transactions on Cryptographic Hardware and Embedded Systems* (2020): 307-335

Contribution-I: Binary PC Oracle-based SCA on LWE/LWR-based KEMs



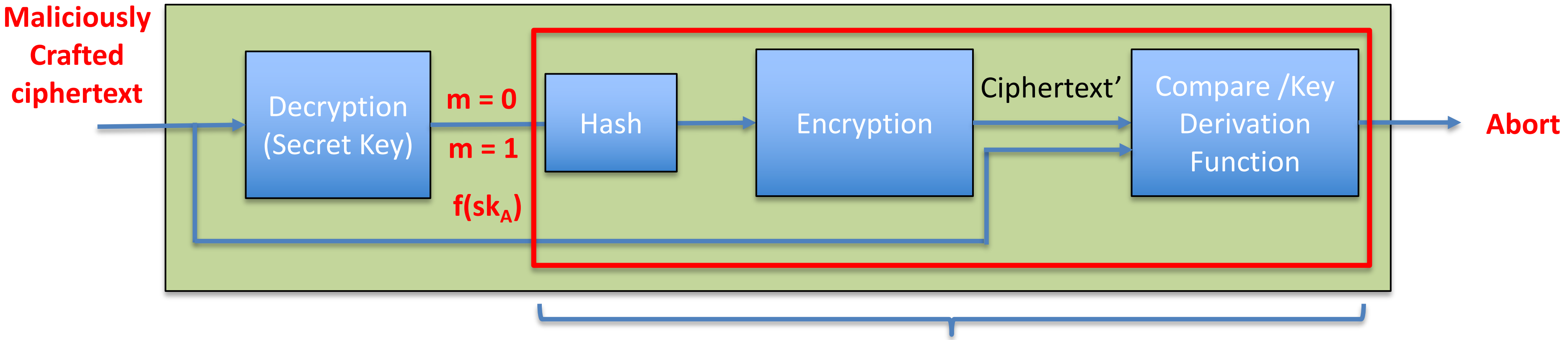
Bad Ciphertext	Message
CT1	M2'
CT2	M3'
CT3	M0'
…	…

→ Full Key Recovery

Contribution-I: Binary PC Oracle-based SCA on LWE/LWR-based KEMs

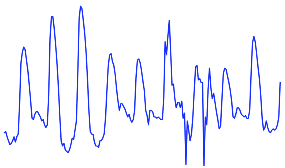
Restrict the Message to **Two** Possible Values

Binary PC Oracle (1-bit)

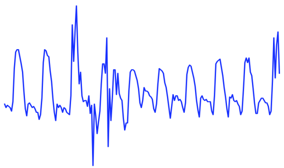


Restrict to **two** Possible Computations

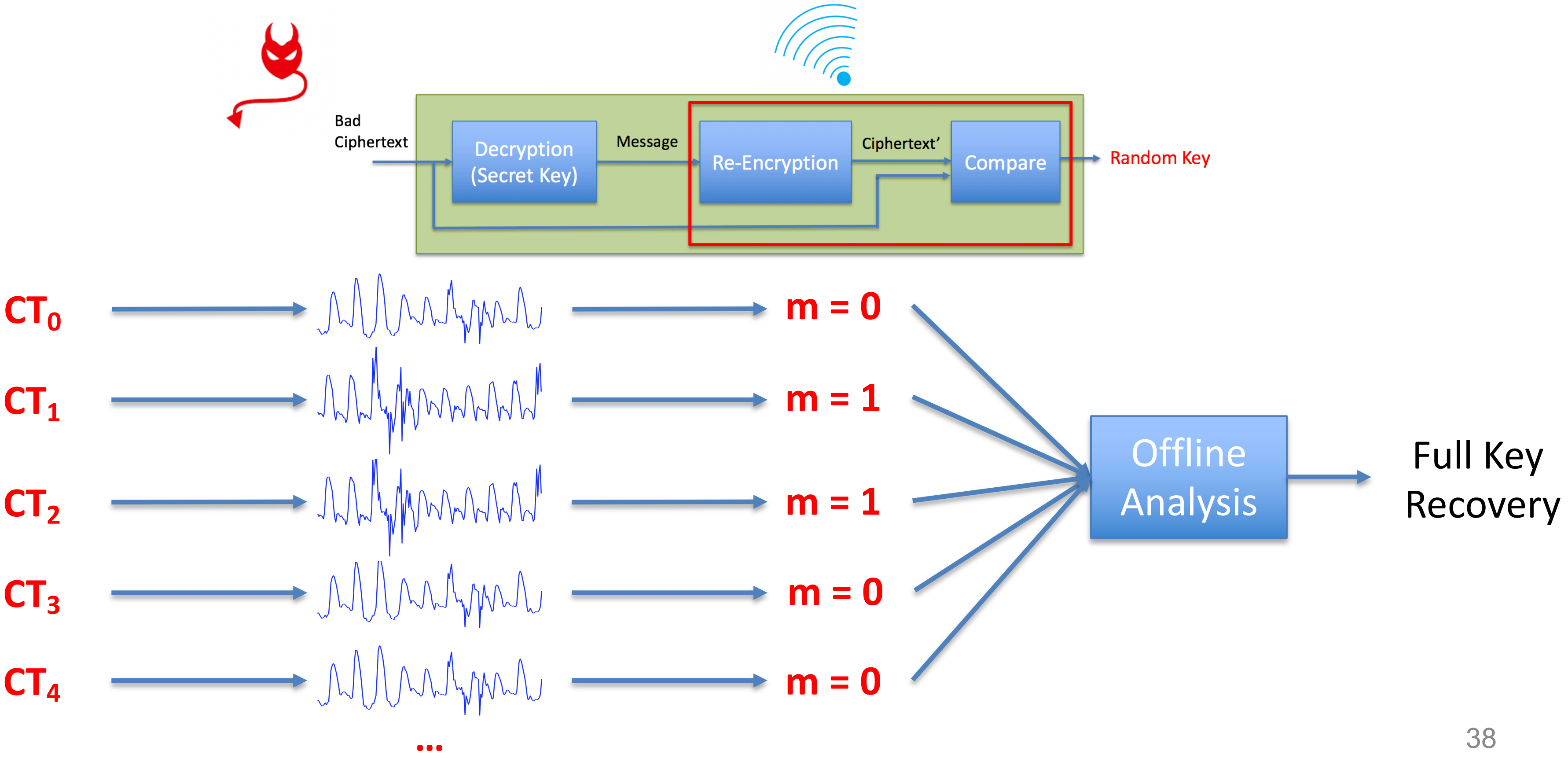
m = 0



m = 1

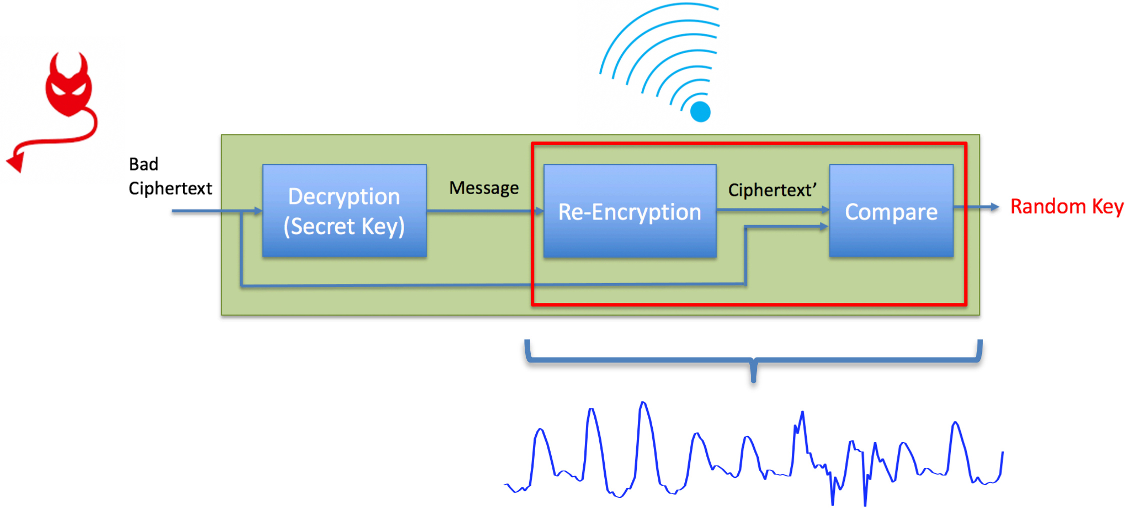


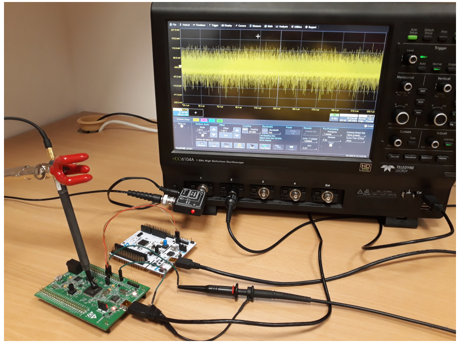
Contribution-I: Binary PC Oracle-based SCA on LWE/LWR-based KEMs

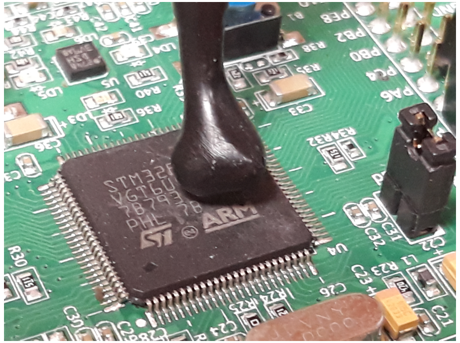


Contribution-I: Binary PC Oracle-based SCA on LWE/LWR-based KEMs

- **Easiest Side-Channel Attack:**
  - Leakage from 60-70 % of operations can be used as oracle
    - **Few Thousand Leakage Points**







  - Does not require sophisticated Setup (Noisy Measurements)

  - No knowledge about implementation design/target platform (HW/SW)

Contribution-I: Binary PC Oracle-based SCA on LWE/LWR-based KEMs

Target: ARM Cortex-M4, EM-side channel
Source: Ravi et al. [RRBC20]

Scheme	# Coeffs	# Attack traces	Time (Minutes)
Kyber (KYBER512)	512 [-3,3]	7.7k	10.8
Round5 (R5ND_1KEM_5d)	490 [-1,1]	2.9k	4.5
LAC (LAC128)	512 [-1,1]	3.0k	25

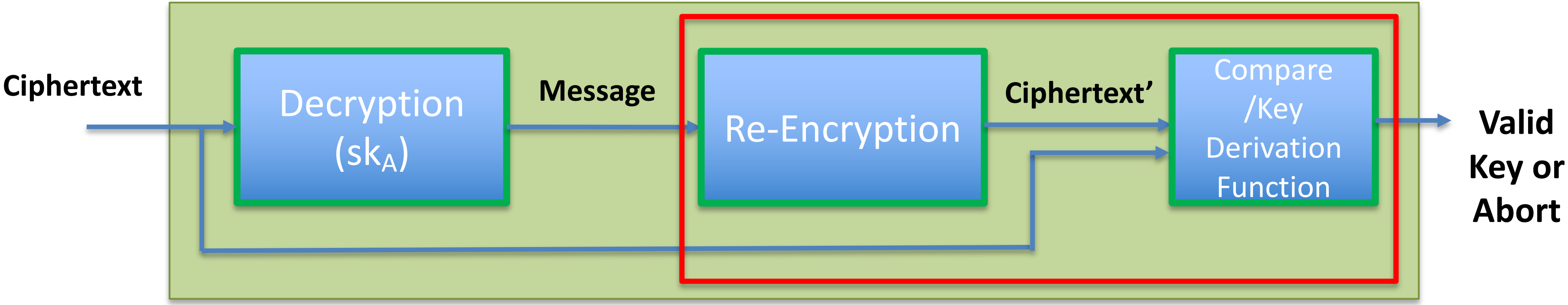
- Attack applicable to 6 lattice-based KEMs based on the LWE/LWR problem.
  - Kyber, Saber, Frodo, NewHope, Round5 and LAC
- Number of queries further reduced by subsequent Works [RRD+22]:
  - **Kyber512 - 1.3k traces**

[RRD+22] Rajendran, Gokulnath, Prasanna Ravi, Jan-Pieter D'Anvers, Shivam Bhasin, and Anupam Chattopadhyay. "Pushing the Limits of Generic Side-Channel Attacks on LWE-based KEMs-Parallel PC Oracle Attacks on Kyber KEM and Beyond." *IACR Transactions on Cryptographic Hardware and Embedded Systems* (2023): 418-446.

[RRCB20] Ravi, Prasanna, Sujoy Sinha Roy, Anupam Chattopadhyay, and Shivam Bhasin. "Generic Side-channel attacks on CCA-secure lattice-based PKE and KEMs." *IACR Transactions on Cryptographic Hardware and Embedded Systems* (2020): 307-335

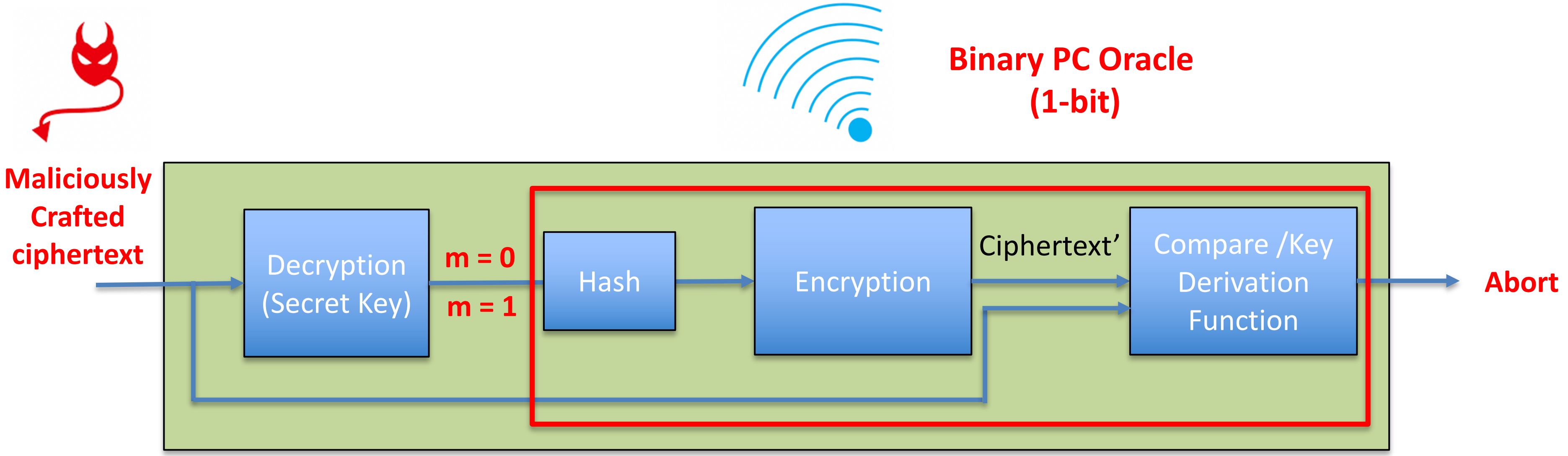
Impact of Binary PC Oracle-based SCA

- Demonstrated need to protect the entire decapsulation procedure against leakage of secret key
  - Efficient masking schemes for lattice-based KEMs [BDK+21,KDB+22, BGR+21]



- **Triggered several follow-up works:**
  - Achieve CCA security without FO transform [DOV21, AKS+22]
    - Research on SCA has triggered algorithm modifications for PQC KEMs!!
  - Improving the efficiency of SCA assisted CCA on lattice-based KEMs [NDGJ21, QCZ+21, RRD+22, RBRC21, XPRO20]
  - Porting SCA assisted CCA to other PQC KEMs [REB+22, SRSW20, UTX+21]

A Few Observations on the Binary PC Oracle-based SCA



- ❑ Recovering 1-bit of information per query (Binary Oracle)
  - ❑ Requires thousands of queries for full key recovery

- ❑ **Question: Can we recover more than 1-bit of information from each query?**

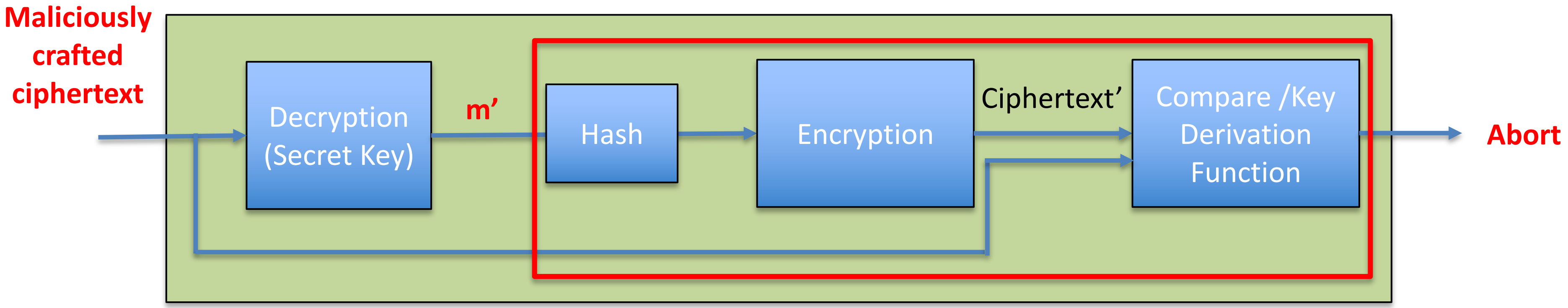
Outline

- Motivation:
  - Post-Quantum Cryptography
  - Side-Channel Attacks (SCA) and Fault Injection Attacks (FIA)
  - Research Questions
- **Research Contributions:**
  - **Side-Channel Attacks: Side-Channel Assisted Chosen-Ciphertext Attacks on lattice-based KEMs**
    - Part-I: Binary PC Oracle-based SCA on LWE/LWR-based KEMs (TCHES-2020)
    - **Part-II: Full-Decryption Oracle-based SCA on LWE/LWR-based KEMs (IEEE-TIFS-2021)**
    - Part-III: SCA Assisted CCA on NTRU-based KEMs (TCHES-2022)
  - Fault-Injection Attacks:
    - Part-IV: Nonce-Reuse based FIA on LWE-based Schemes (COSADE-2019)
    - Part-V: FIA on the Number Theoretic Transform (NTT) (TCHES-2023)
  - Other-Contributions:
- Conclusion and Future Works:

Contribution-II: Full-Decryption Oracle-based SCA on LWE/LWR-based KEMs

Full Decryption Oracle (256-bits)

Reduces the number of queries by a factor of 256!



Simultaneously contains 256 bits of information about the secret key

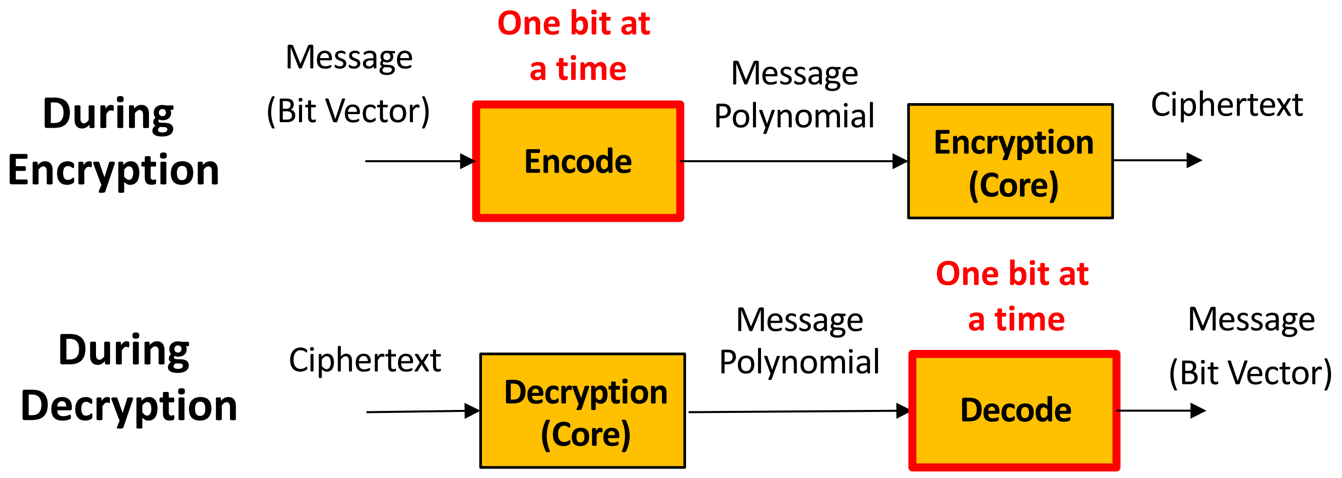
Question:

How to instantiate a Full-Decryption Oracle through Side-Channels?

[RBRC21] **Ravi, Prasanna**, Shivam Bhasin, Sujoy Sinha Roy, and Anupam Chattopadhyay. "On exploiting message leakage in (few) NIST PQC candidates for practical message recovery attacks." *IEEE Transactions on Information Forensics and Security* 17 (2021): 684-699.

Contribution-II: Full-Decryption Oracle-based SCA on LWE/LWR-based KEMs

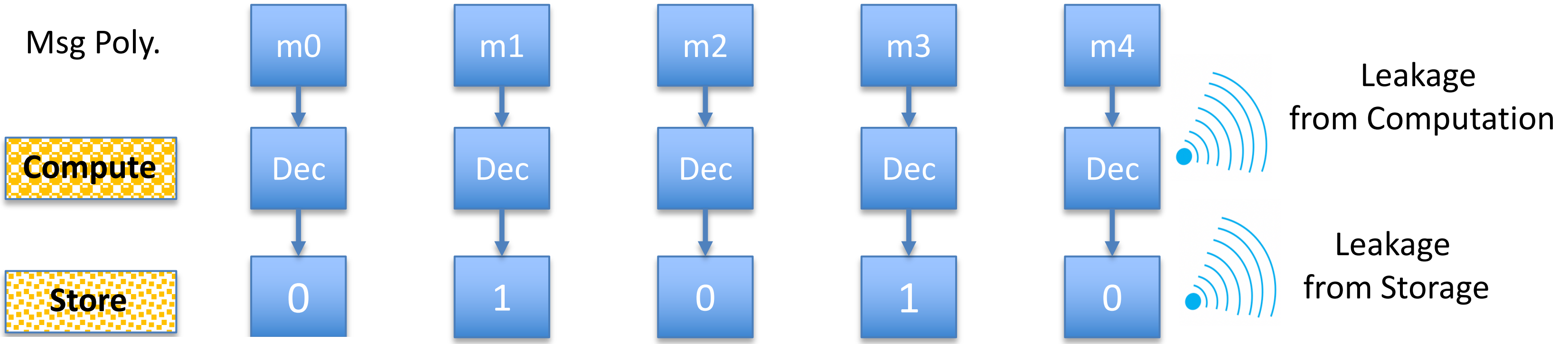
- LWE/LWR-based schemes involve computation over matrices, vectors and polynomials.

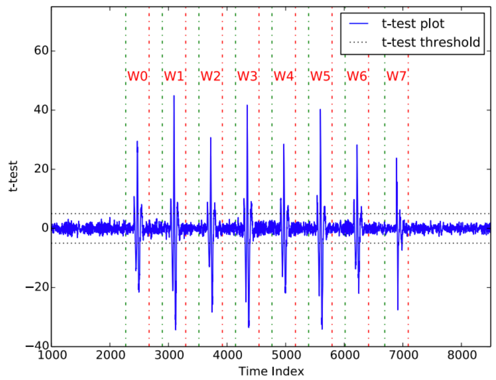


- Bitwise manipulation is an inherent algorithmic property of lattice-based schemes:
  - **Does it lead to side-channel leakage?**

Contribution-II: Full-Decryption Oracle-based SCA on LWE/LWR-based KEMs

Message Decoding Procedure:





Leakage from Individual Bits of the Message

Enables recovery of entire message one bit at a time

Side-Channel based Full-Decryption Oracle

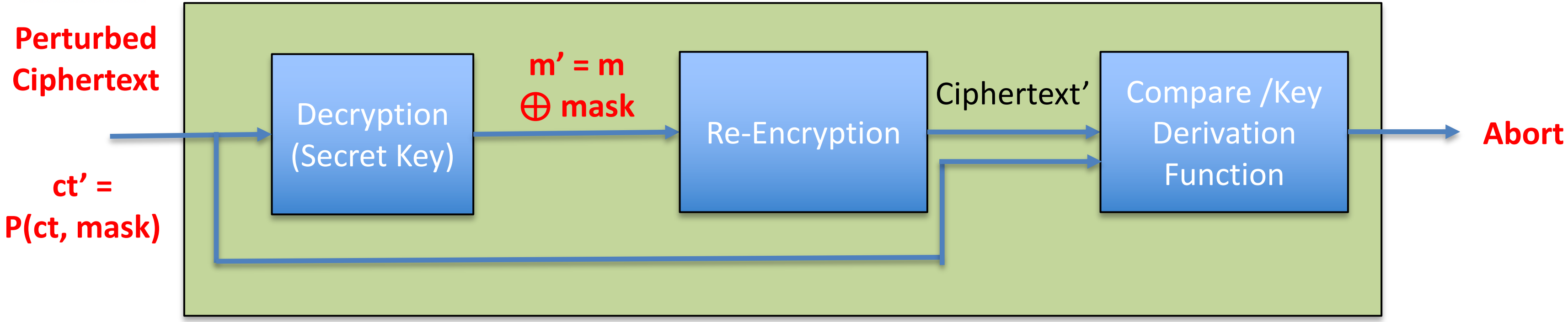
Sensitive to SNR (Fine Leakage Points)

Countermeasure: Why not shuffle the order of decoding?

Contribution-II: Full-Decryption Oracle-based SCA on LWE/LWR-based KEMs

Let Encrypt(m) = ct

Ciphertext Malleability (CM) Property



- ❑ We show that CM property can be used in a side-channel context to break protected implemenations and variants.

[RBRC21] **Ravi, Prasanna**, Shivam Bhasin, Sujoy Sinha Roy, and Anupam Chattopadhyay. "On exploiting message leakage in (few) NIST PQC candidates for practical message recovery attacks." *IEEE Transactions on Information Forensics and Security* 17 (2021): 684-699.ç

Contribution-II: Full-Decryption Oracle-based SCA on LWE/LWR-based KEMs

Implementation Variants	No. of Traces
Message Decoding	
Incremental Storage	1
Bytewise Storage **(CM Assisted)**	9
Wordwise Storage **(CM Assisted)**	33
Shuffled Incremental Storage **(CM Assisted)**	385.5k
Masked Incremental Storage **(CM Assisted)**	1
Masked Bytewise Storage **(CM Assisted)**	1.1k
Message Encoding	
Determiner Leakage	1
Shuffled Determiner Leakage **(CM Assisted)**	257
Masked Determiner Leakage **(CM Assisted)**	1

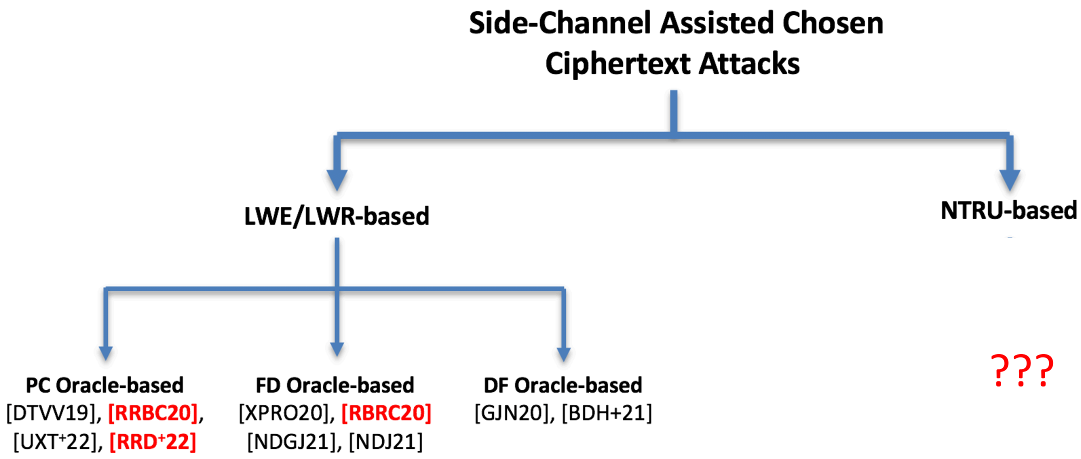
- ❑ Attack applicable to 6 lattice-based KEMs based on the LWE/LWR problem.
  - ❑ Kyber, Saber, Frodo, NewHope, Round5 and LAC
- ❑ Countermeasures and implementation variants increase attacker's effort, but are not foolproof.
- ❑ We show that Ciphertext Malleability like properties can be used as a tool for side-channel attacks

[RBRC21] **Ravi, Prasanna**, Shivam Bhasin, Sujoy Sinha Roy, and Anupam Chattopadhyay. "On exploiting message leakage in (few) NIST PQC candidates for practical message recovery attacks." *IEEE Transactions on Information Forensics and Security* 17 (2021): 684-699.ç

Outline

- Motivation:
  - Post-Quantum Cryptography
  - Side-Channel Attacks (SCA) and Fault Injection Attacks (FIA)
  - Research Questions
- **Research Contributions:**
  - **Side-Channel Attacks: Side-Channel Assisted Chosen-Ciphertext Attacks on lattice-based KEMs**
    - Part-I: Binary PC Oracle-based SCA on LWE/LWR-based KEMs (TCHES-2020)
    - Part-II: Full-Decryption Oracle-based SCA on LWE/LWR-based KEMs (IEEE-TIFS-2021)
    - **Part-III: SCA Assisted CCA on NTRU-based KEMs (TCHES-2022)**
  - Fault-Injection Attacks:
    - Part-IV: Nonce-Reuse based FIA on LWE-based Schemes (COSADE-2019)
    - Part-V: FIA on the Number Theoretic Transform (NTT) (TCHES-2023)
  - Other-Contributions:
- Conclusion and Future Works:

Contribution-III: SCA Assisted CCA on NTRU-based KEMs



- ❑ Upon presenting our research on SCA assisted CCA at NIST Round 3 Seminars [RR21]:
  - ❑ **Main Questions:**
    - ❑ Are similar attacks **possible** on NTRU-based KEMs?
    - ❑ If so, are NTRU-based KEMs more **easy/difficult** to be attacked compared to LWE/LWR-based KEMs?

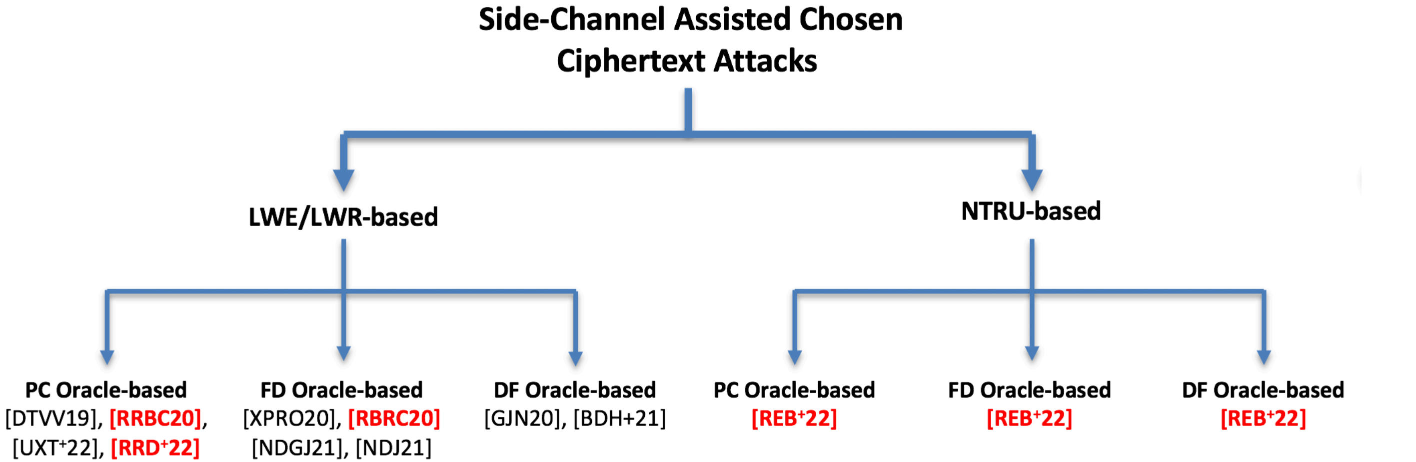
[RR21] Ravi, Prasanna, and Sujoy Sinha Roy. "Side-channel analysis of lattice-based PQC candidates." In *Round 3 Seminars, NIST Post Quantum Cryptography*. 2021.

[REB$^+$22] **Ravi, Prasanna**, Martianus Frederic Ezerman, Shivam Bhasin, Anupam Chattopadhyay, and Sujoy Sinha Roy. "Will You Cross the Threshold for Me? Generic Side-Channel Assisted Chosen-Ciphertext Attacks on NTRU-based KEMs." *IACR Transactions on Cryptographic Hardware and Embedded Systems* (2022): 722-761.

Contribution-III: SCA Assisted CCA on NTRU-based KEMs

- We presented the first SCA assisted CCA on NTRU-based KEMs
    - NTRU (Finalist) and NTRU Prime (Alternate Finalist)

- **No. of Queries/Traces:** Few hundred to Few thousand chosen-ciphertext queries
- **Approximately same effort** to break NTRU-based KEMs compared to LWE/LWR-based KEMs
- Attack works for all parameters for NTRU and NTRU Prime with 100% success rate



[REB+22] **Ravi, Prasanna**, Martianus Frederic Ezerman, Shivam Bhasin, Anupam Chattopadhyay, and Sujoy Sinha Roy. "Will You Cross the Threshold for Me? Generic Side-Channel Assisted Chosen-Ciphertext Attacks on NTRU-based KEMs." *IACR Transactions on Cryptographic Hardware and Embedded Systems* (2022): 722-761.

Outline

- **Motivation:**
  - Post-Quantum Cryptography
  - Side-Channel Attacks (SCA) and Fault Injection Attacks (FIA)
  - Research Questions
- **Research Contributions:**
  - Side-Channel Attacks: Side-Channel Assisted Chosen-Ciphertext Attacks on lattice-based KEMs
    - Part-I: Binary PC Oracle-based SCA on LWE/LWR-based KEMs (TCHES-2020)
    - Part-II: Full-Decryption Oracle-based SCA on LWE/LWR-based KEMs (IEEE-TIFS-2021)
    - Part-III: SCA Assisted CCA on NTRU-based KEMs (TCHES-2022)
  - **Fault-Injection Attacks:**
    - Part-IV: Nonce-Reuse based FIA on LWE-based Schemes (COSADE-2019)
    - Part-V: FIA on the Number Theoretic Transform (NTT) (TCHES-2023)
  - Other-Contributions:
- Conclusion and Future Works:

Contribution: Fault-Injection Attacks

- **Motivation**: Inject faults to
  - Create weak instances of the hard problem (LWE/LWR and NTRU)
  - Reduce Entropy of Secrets/Sensitive Data

- **Questions**:
  - Can we find **Single Point of Failure (SPFs)** for faults in lattice-based schemes?

- We show that algorithmic design choices as well as implementation choices can lead to SPFs, leading to efficient fault attacks [RRB+19, RYB+23].

Achilles Heel

[RRB+19] **Ravi, Prasanna**, Debapriya Basu Roy, Shivam Bhasin, Anupam Chattopadhyay, and Debdeep Mukhopadhyay. "Number “not used” once-practical fault attack on pqm4 implementations of NIST candidates." In *Constructive Side-Channel Analysis and Secure Design: COSADE 2019, Darmstadt, Germany, April 3–5, 2019, Proceedings 10*, pp. 232-250. Springer, 2019.

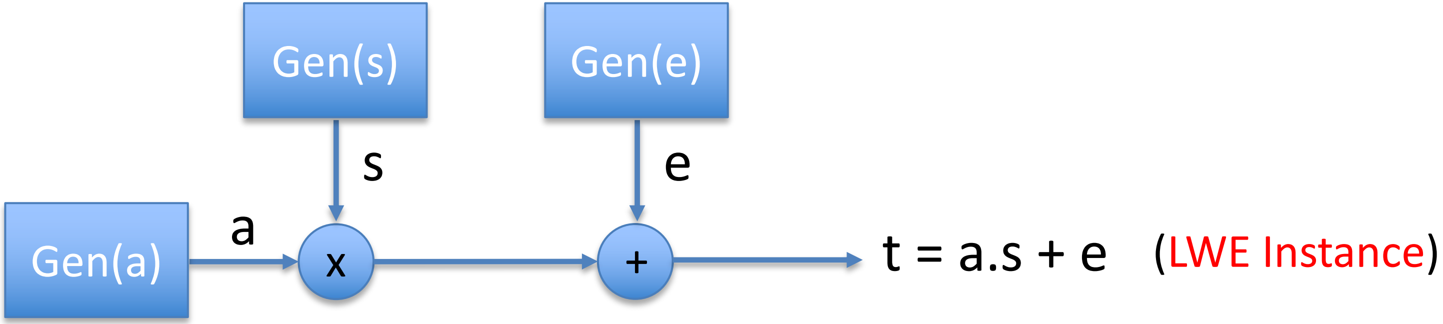
[RYB+23] **Ravi, Prasanna**, Bolin Yang, Shivam Bhasin, Fan Zhang, and Anupam Chattopadhyay. "Fiddling the Twiddle Constants-Fault Injection Analysis of the Number Theoretic Transform." *IACR Transactions on Cryptographic Hardware and Embedded Systems* (2023): 447-481.

Outline

- **Motivation:**
  - Post-Quantum Cryptography
  - Side-Channel Attacks (SCA) and Fault Injection Attacks (FIA)
  - Research Questions
- **Research Contributions:**
  - Side-Channel Attacks: Side-Channel Assisted Chosen-Ciphertext Attacks on lattice-based KEMs
    - Part-I: Binary PC Oracle-based SCA on LWE/LWR-based KEMs (TCHES-2020)
    - Part-II: Full-Decryption Oracle-based SCA on LWE/LWR-based KEMs (IEEE-TIFS-2021)
    - Part-III: SCA Assisted CCA on NTRU-based KEMs (TCHES-2022)
  - **Fault-Injection Attacks:**
    - **Part-IV: Nonce-Reuse based FIA on LWE-based Schemes (COSADE-2019)**
    - Part-V: FIA on the Number Theoretic Transform (NTT) (TCHES-2023)
  - Other-Contributions:
- Conclusion and Future Works:

Contribution-IV: Nonce Reuse based FIA on LWE-based Schemes

- Several LWE instances are created and used in LWE-based schemes.



- The error component **e** is a vital component of the LWE instance.
- Without error or weak error, security is compromised (secret recovered and scheme broken).
- We analyzed the process for generation of secret and error in several LWE-based schemes.

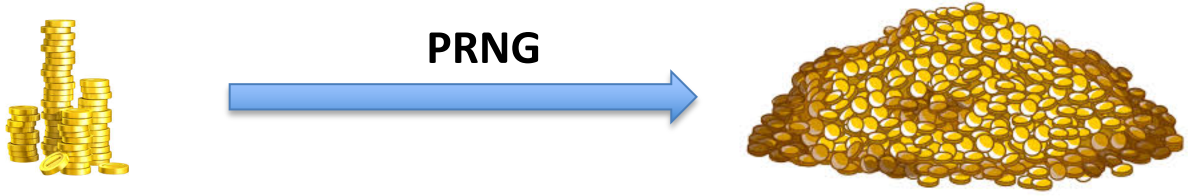
[**R**RB+19] **Ravi, Prasanna**, Debapriya Basu Roy, Shivam Bhasin, Anupam Chattopadhyay, and Debdeep Mukhopadhyay. "Number "not used" once-practical fault attack on pqm4 implementations of NIST candidates." In *Constructive Side-Channel Analysis and Secure Design: COSADE 2019, Darmstadt, Germany, April 3–5, 2019, Proceedings 10*, pp. 232-250. Springer, 2019.

Contribution-IV: Nonce Reuse based FIA on LWE-based Schemes

- ❑ Requires large amount of randomness (random bits) to sample long polynomials/vectors.

- ❑ Randomness is not cheap on embedded devices (consumes a lot of time and energy)

- ❑ To Sample S/E:
  - ❑ A small truly random seed K using TRNG (True Random Number Generator) is generated.
  - ❑ K is fed to a PRNG (Pseudo Random Number Generator) which can output any amount of randomness.

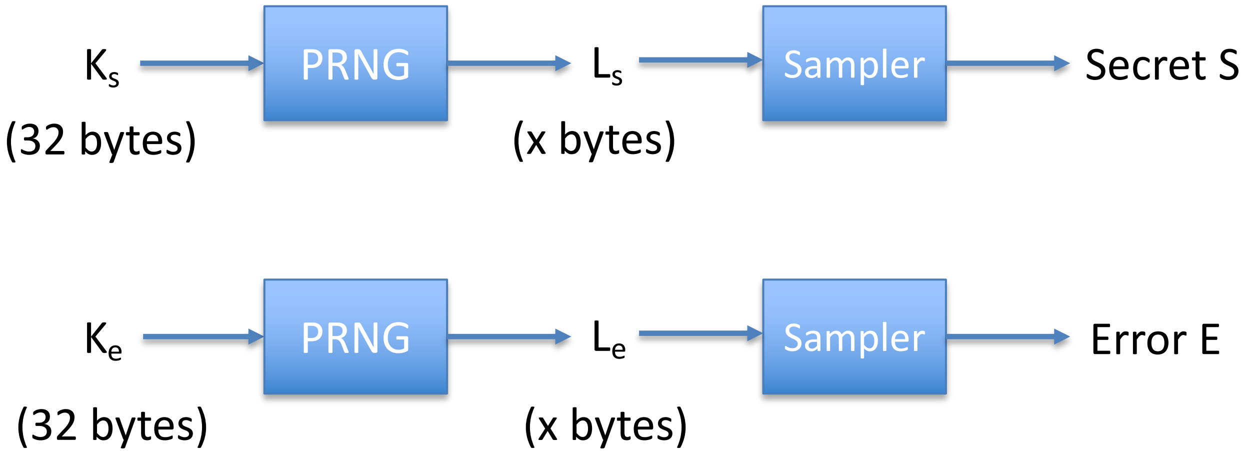


Small Seed K

Large Pseudo-Randomness

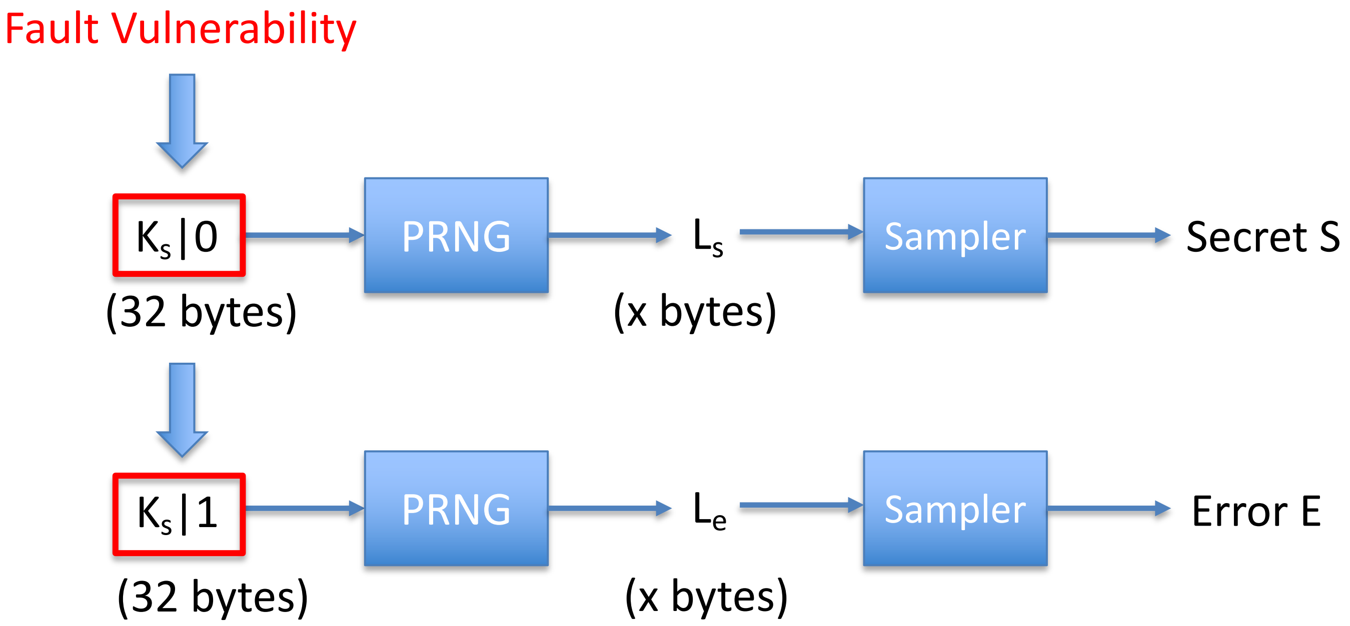
Contribution-IV: Nonce Reuse based FIA on LWE-based Schemes

- Ideally, different short seeds should be used for secret S and E



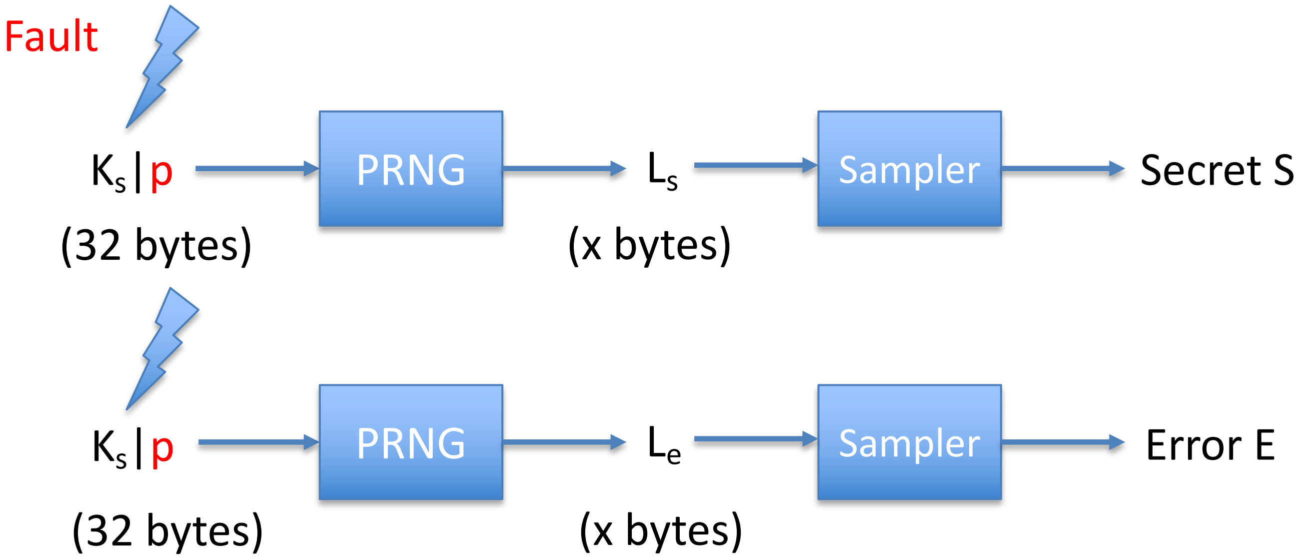
Contribution-IV: Nonce Reuse based FIA on LWE-based Schemes

- Instead, same seed K_s but with a nonce was used to sample S and E (for efficiency)



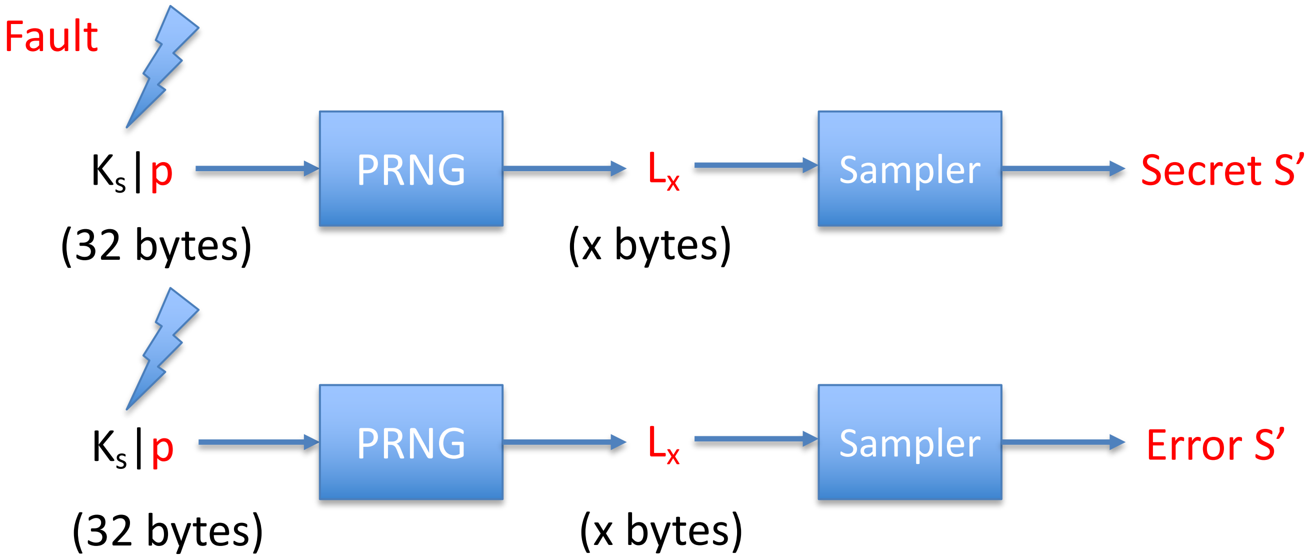
Contribution-IV: Nonce Reuse based FIA on LWE-based Schemes

- Instead, same seed K_s but with a delimiter was used to sample S and E (for efficiency)

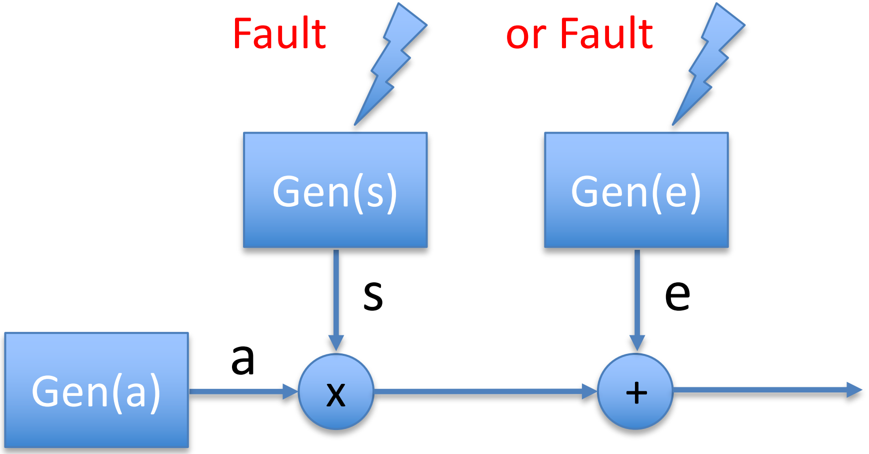


Contribution-IV: Nonce Reuse based FIA on LWE-based Schemes

- Instead, same seed K_s but with a delimiter was used to sample S and E (for efficiency)

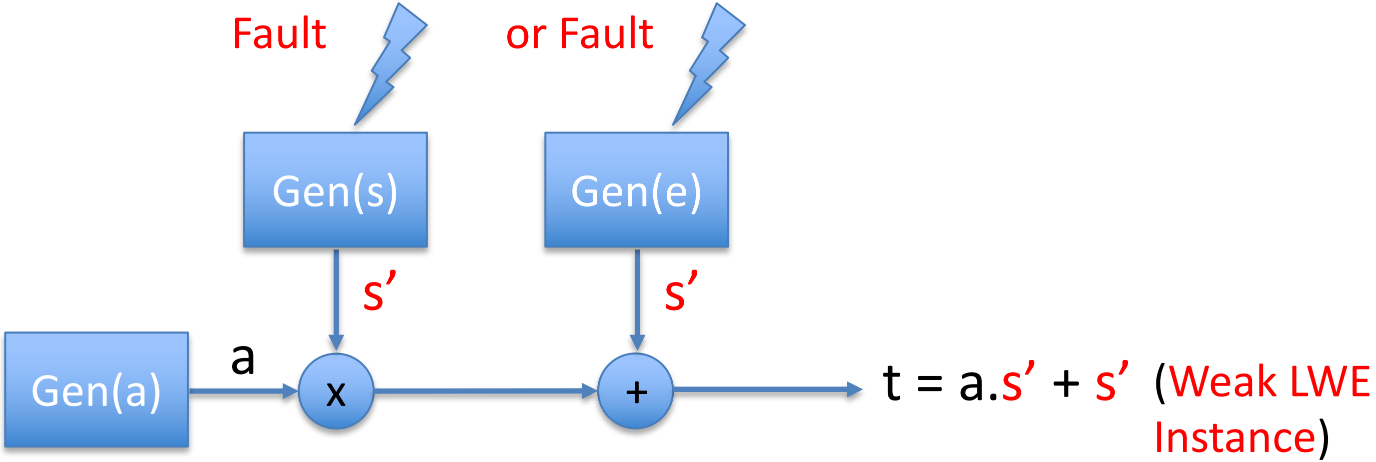


Contribution-IV: Nonce Reuse based FIA on LWE-based Schemes



t = a.s + e (LWE Instance)

Contribution-IV: Nonce Reuse based FIA on LWE-based Schemes



- Weak LWE instance can be easily solved by Gaussian Elimination
- Weak LWE instances:
  - In Key Generation: Key Recovery Attacks
  - In Encapsulation: Message Recovery Attacks
- Four lattice-based schemes (**Kyber**, **Dilithium**, **Frodo**, NewHope) are vulnerable to our proposed attack.

Contribution-IV: Nonce Reuse based FIA on LWE-based Schemes

- Validation on implementations from public ***pqm4 library***
- Fault repeatability using EMFI is 100% at (few) identified locations

Attack Objective	Fault Complexity			
	NEWHOPE		FRODO	
	NEWHOPE512	NEWHOPE1024	Frodo-640	Frodo-976
Key Recovery	1	1	1	1
Message Recovery	1	1	1	1

	KYBER			DILITHIUM			
	KYBER512	KYBER768	KYBER1024	Weak	Med.	Rec.	High
Key Recovery	2	3	4	2	3	4	5
Message Recovery	2	3	4	-	-	-	-

Impact of Nonce Reuse based FIA on LWE-based Schemes

- The designers of FrodoKEM (NIST Finalist and BSI recommended candidate) changed the algorithmic specification to remove the fault vulnerability (From Round 2).

- **Countermeasure**: Use different seeds for secret and error

- While other schemes (Kyber, NewHope) acknowledged the weakness, they did not change the specifications in order to not lose out on efficiency.

Outline

- ❑ Motivation:
  - ❑ Post-Quantum Cryptography
  - ❑ Side-Channel Attacks (SCA) and Fault Injection Attacks (FIA)
  - ❑ Research Questions
- ❑ Research Contributions:
  - ❑ Side-Channel Attacks: Side-Channel Assisted Chosen-Ciphertext Attacks on lattice-based KEMs
    - ❑ Part-I: Binary PC Oracle-based SCA on LWE/LWR-based KEMs (TCHES-2020)
    - ❑ Part-II: Full-Decryption Oracle-based SCA on LWE/LWR-based KEMs (IEEE-TIFS-2021)
    - ❑ Part-III: SCA Assisted CCA on NTRU-based KEMs (TCHES-2022)
  - ❑ **Fault-Injection Attacks:**
    - ❑ Part-IV: Nonce-Reuse based FIA on LWE-based Schemes (COSADE-2019)
    - ❑ **Part-V: FIA on the Number Theoretic Transform (NTT) (TCHES-2023)**
  - ❑ Other-Contributions:
- ❑ Conclusion and Future Works:

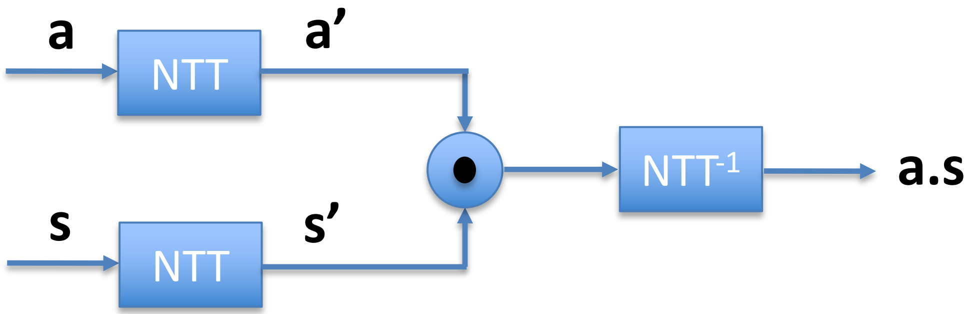
Contribution-V: FIA on the Number Theoretic Transform (NTT)

- **Polynomial multiplication** is one of the most computationally intensive blocks within lattice-based schemes.
- **Number Theoretic Transform** (**NTT**) is a critical sub-block used for polynomial multiplication in several lattice-based schemes (Kyber, Dilithium, SABER, NTRU, NewHope)
- NTT operates over sensitive variables (secret key): attractive target for FIA
- In this work, we proposed the first practical FIA on the NTT:
  - Targeting an implementation-level vulnerability
  - Key Recovery Attacks and Message Recovery Attacks on Kyber KEM
  - Signature Forgery Attacks and Verification Bypass Attacks on Dilithium DS scheme

[RYB+23] **Ravi, Prasanna**, Bolin Yang, Shivam Bhasin, Fan Zhang, and Anupam Chattopadhyay. "Fiddling the Twiddle Constants-Fault Injection Analysis of the Number Theoretic Transform." *IACR Transactions on Cryptographic Hardware and Embedded Systems* (2023): 447-481.

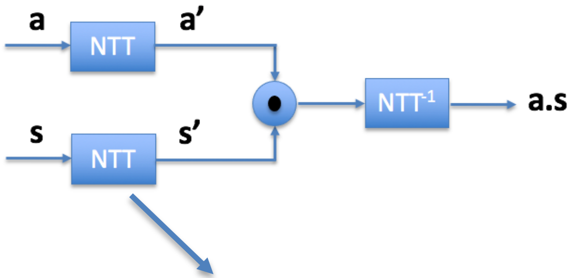
Contribution-V: FIA on the Number Theoretic Transform (NTT)

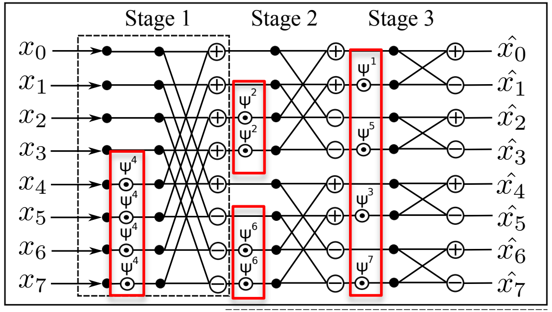
NTT based Polynomial Multiplication:



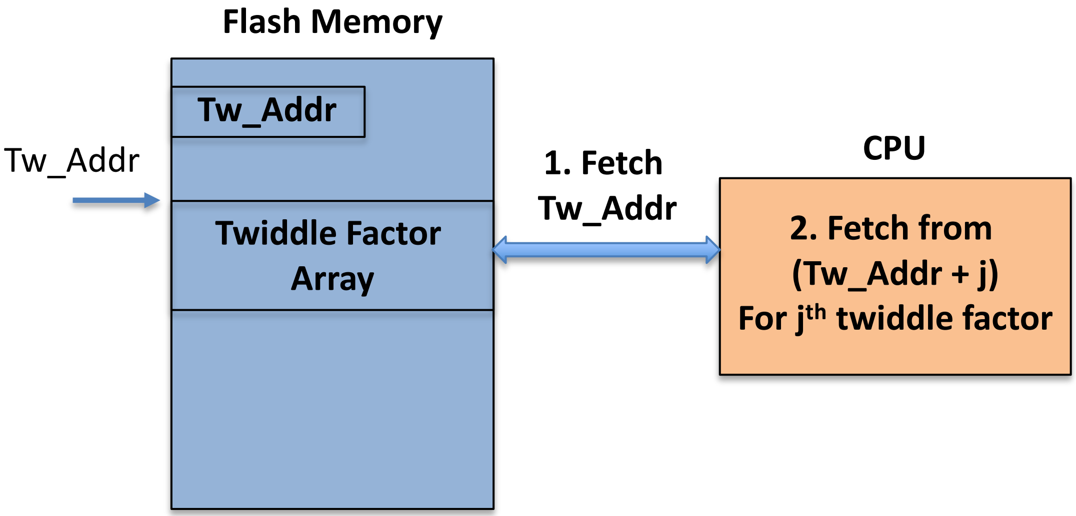
[RYB+23] **Ravi, Prasanna**, Bolin Yang, Shivam Bhasin, Fan Zhang, and Anupam Chattopadhyay. "Fiddling the Twiddle Constants-Fault Injection Analysis of the Number Theoretic Transform." *IACR Transactions on Cryptographic Hardware and Embedded Systems* (2023): 447-481.

Contribution-V: FIA on the Number Theoretic Transform (NTT)





In MCU, Twiddle Constants are stored in Flash Memory as part of Firmware Binary

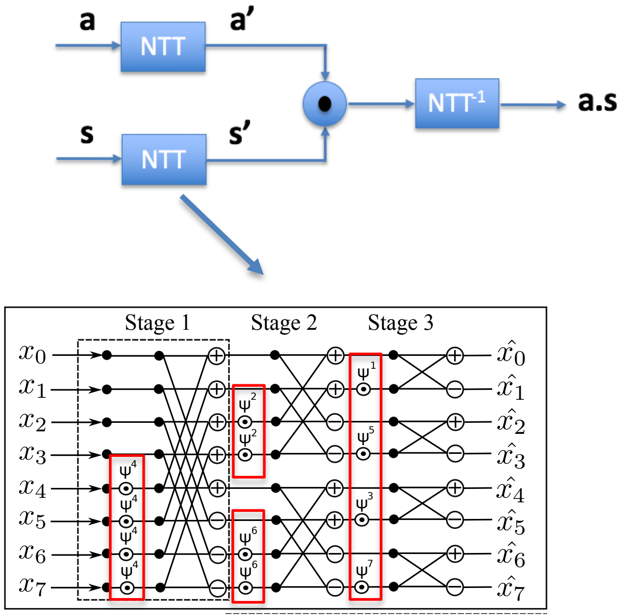


Main Observation: Tw_Addr is used as **base-address** to calculate address for all constants

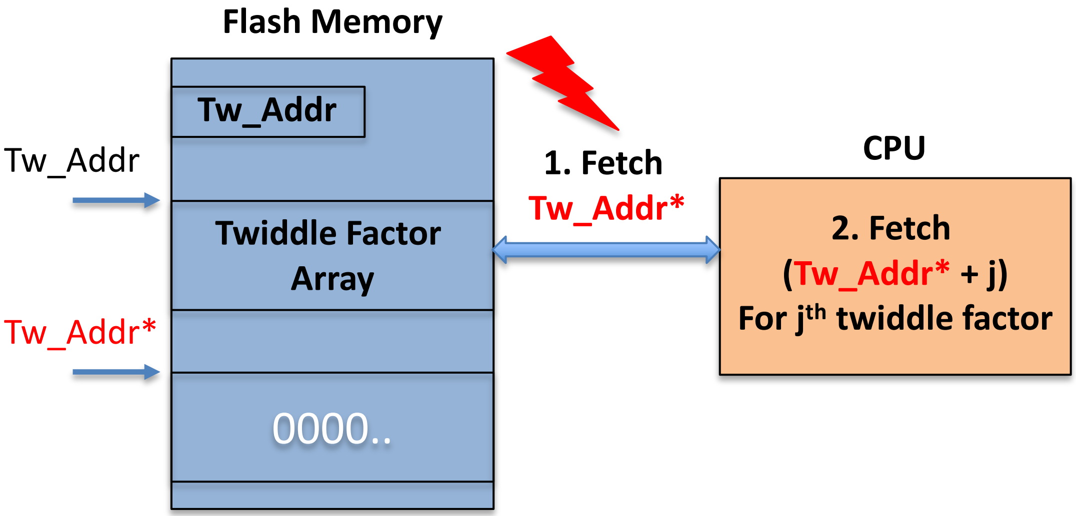
Fault Vulnerability: Can an attacker fault the base address?

Implementation Style used in all publicly available optimized implementations of Kyber and Dilithium for ARM Cortex-M4 Processor

Contribution-V: FIA on the Number Theoretic Transform (NTT)



In MCU, Twiddle Constants are stored in Flash Memory as part of Firmware Binary



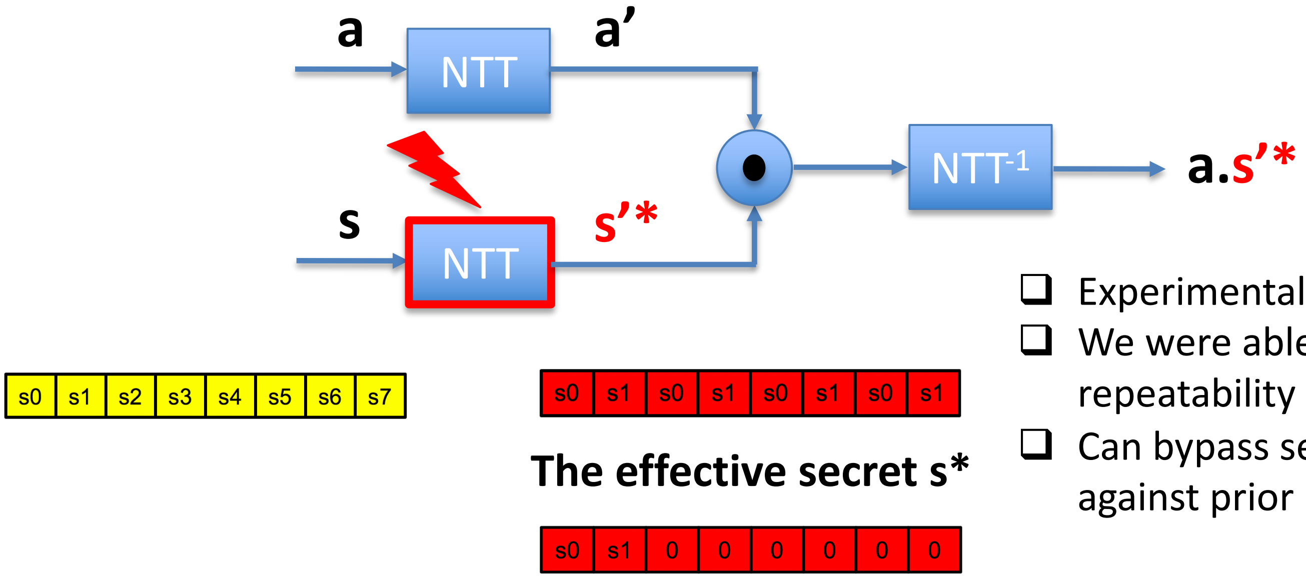
Observation: Can zeroize the entire twiddle factor array in a single fault

25% of random memory locations yield zeros on ARM Cortex-M4 processor

What happens when twiddle factors are zeroized???

Contribution-V: FIA on the Number Theoretic Transform (NTT)

NTT based Polynomial Multiplication in Kyber KEM:



- ❑ Experimental validation was done using EMFI
- ❑ We were able to achieve 100% fault repeatability using several parameters
- ❑ Can bypass several fault countermeasures against prior FIA on Kyber and Dilithium

[RYB+23] **Ravi, Prasanna**, Bolin Yang, Shivam Bhasin, Fan Zhang, and Anupam Chattopadhyay. "Fiddling the Twiddle Constants-Fault Injection Analysis of the Number Theoretic Transform." *IACR Transactions on Cryptographic Hardware and Embedded Systems* (2023): 447-481.

Outline

- Motivation:
  - Post-Quantum Cryptography
  - Side-Channel Attacks (SCA) and Fault Injection Attacks (FIA)
  - Research Questions
- Research Contributions:
  - Side-Channel Attacks: Side-Channel Assisted Chosen-Ciphertext Attacks on lattice-based KEMs
    - Part-I: Binary PC Oracle-based SCA on LWE/LWR-based KEMs (TCHES-2020)
    - Part-II: Full-Decryption Oracle-based SCA on LWE/LWR-based KEMs (IEEE-TIFS-2021)
    - Part-III: SCA Assisted CCA on NTRU-based KEMs (TCHES-2022)
  - Fault-Injection Attacks:
    - Part-IV: Nonce-Reuse based FIA on LWE-based Schemes (COSADE-2019)
    - Part-V: FIA on the Number Theoretic Transform (NTT) (TCHES-2023)
  - **Other-Contributions:**
- Conclusion and Future Works:

Other Contributions

- **SCA/FIA Countermeasures**
    - Configurable Shuffling and Masking SCA Countermeasures for NTT against single-trace attacks (Best Paper Award - SPACE 2019)
    - A Systematic Study of SCA and FIA of Kyber and Dilithium (ACM TECS)
        - Combined SCA+FIA countermeasures
- **Hardware Trojans and Kleptographic Backdoors for Lattice-based Schemes**

[RYB+22] Ravi, Prasanna, Bolin Yang, Shivam Bhasin, Fan Zhang, and Anupam Chattopadhyay. "Fiddling the Twiddle Constants-Fault Injection Analysis of the Number Theoretic Transform." *IACR Transactions on Cryptographic Hardware and Embedded Systems* (2023): 447-481.

Research Outcomes

Lattice-based Cryptography

Physical Attacks

SCA
[**R**RBC20] (*TCHES 2020*)
[**R**BRC21] (*IEEE-TIFS 2021*)
[**R**EB+22] (*TCHES 2022*)
[R**R**D+22] (TCHES 2023)

FIA
[**R**RB+19] (*COSADE 2019*)
[**R**JH+19] (*AsiaCCS 2019*)
[**R**YB+22]** (*TCHES 2023*)

Hardware Trojans and Backdoors
[**R**BC+22] (*IACR ePrint*)
[**R**DB+21] (*SPACE 2021*)

Survey

[**R**HC+20] *(ACM CSUR)*
[**R**CB22]** *(LATS 2022)*

Implementations

Countermeasures
[**R**PB+20] (*SPACE 2020*)
[**R**CDB22] (*ACM TECS*)

Optimizations
[**R**GC+19] (*CARDIS 2019*)
[**R**SC+20] (*ISCAS 2020*)

357 Citations (Google Scholar)

Notable Achievements

- Best (Joint) Student Paper Award at *SPACE-2020* (Security Privacy and Applied Cryptographic Engineering) for paper titled “On Configurable SCA Countermeasures Against Single Trace Attacks for the NTT".

- Best PhD Forum Presentation Award at *IEEE AsianHost-2020*.

- Presented two invited seminars to NIST on Post-Quantum Cryptography [RR21, R23]

- Our nonce-reuse FIA triggered change in the algorithmic specification of FrodoKEM (BSI recommended candidate)

- Several of our research works are cited in NIST’s status report of PQC standardization process [AAC+22]

[AAC+22] Alagic, Gorjan, Daniel Apon, David Cooper, Quynh Dang, Thinh Dang, John Kelsey, Jacob Lichtinger et al. "Status report on the third round of the NIST post-quantum cryptography standardization process." *US Department of Commerce, NIST* (2022).

[RR21] Ravi, Prasanna, and Sujoy Sinha Roy. "Side-channel analysis of lattice-based PQC candidates." In *Round 3 Seminars, NIST Post Quantum Cryptography*. 2021.

[R23] Ravi, Prasanna, and Sujoy Sinha Roy. ”Fault Injection Attacks on NIST PQC Standards – Kyber and Dilithium." In *NIST PQC Seminars, NIST Post Quantum Cryptography*. 2023.

Outline

- Motivation:
  - Post-Quantum Cryptography
  - Side-Channel Attacks (SCA) and Fault Injection Attacks (FIA)
  - Research Questions

- Research Contributions:
  - Side-Channel Attacks: Side-Channel Assisted Chosen-Ciphertext Attacks on lattice-based KEMs
    - Part-I: Binary PC Oracle-based SCA on LWE/LWR-based KEMs (TCHES-2020)
    - Part-II: Full-Decryption Oracle-based SCA on LWE/LWR-based KEMs (IEEE-TIFS-2021)
    - Part-III: SCA Assisted CCA on NTRU-based KEMs (TCHES-2022)
  - Fault-Injection Attacks:
    - Part-IV: Nonce-Reuse based FIA on LWE-based Schemes (COSADE-2019)
    - Part-V: FIA on the Number Theoretic Transform (NTT) (TCHES-2023)
  - Other-Contributions:
- **Conclusion and Future Works:**

Conclusion

- Easy SCA and FIA are possible on unprotected PQC lattice-based schemes!!
- Lattice-based schemes have a lot of underlying algorithmic features that render them susceptible to SCA and FIA!!
- Please refer [RDB+22] for a systematic study of SCA and FIA on Kyber and Dilithium (NIST selected candidates for standardization)
- It is paramount to deploy lattice-based implementations with suitable countermeasures!!
- Existing concrete countermeasures [BGR+22,HKL+22] are very expensive (2-3x overhead in runtime)

[RDB+22] Ravi, Prasanna, Anupam Chattopadhyay, Jan Pieter D'Anvers, and Anubhab Baksi. "Side-channel and fault-injection attacks over lattice-based post-quantum schemes (Kyber, Dilithium): Survey and new results." *Cryptology ePrint Archive* (2022).
[BGR+21] Bos, Joppe W., Marc Gourjon, Joost Renes, Tobias Schneider, and Christine Van Vredendaal. "Masking kyber: First-and higher-order implementations." *IACR Transactions on Cryptographic Hardware and Embedded Systems* (2021): 173-214.
[HKL+22] Heinz, Daniel, Matthias J. Kannwischer, Georg Land, Thomas Pöppelmann, Peter Schwabe, and Daan Sprenkels. "First-order masked Kyber on ARM Cortex-M4." *Cryptology ePrint Archive* (2022).

Open Questions

- Alternatives to FO transform for CCA security [DOV21, AKS+22]
- Dedicated Leakage Detection Framework (SCA + FIA)
- Combined Low-Cost Countermeasures (SCA + FIA)
- Blind Side-Channel Attacks

[AKS+22] Azouaoui, Melissa, Yulia Kuzovkova, Tobias Schneider, and Christine van Vredendaal. "Post-quantum authenticated encryption against chosen-ciphertext side-channel attacks." *Cryptology ePrint Archive* (2022).
[DOV21] D'Anvers, Jan-Pieter, Emmanuela Orsini, and Frederik Vercauteren. "Error term checking: Towards chosen ciphertext security without re-encryption." In *Proceedings of the 8th ACM on ASIA Public-Key Cryptography Workshop*, pp. 3-12. 2021.

Acknowledgements

- **Thesis Advisory Committee**
  - Associate Professor Arvind Easwaran, SCSE, NTU
  - Dr. Khoo Khoong Ming, DSO, Singapore
- All my research collaborators
- Authors of pqm4 library
- Anonymous people who answer queries on Stack Overflow

[KRSS19] Kannwischer, Matthias J., Joost Rijneveld, Peter Schwabe, and Ko Stoffelen. "pqm4: Testing and Benchmarking NIST PQC on ARM Cortex-M4." (2019).

Special Thanks to...

Dr. Anupam Chattopadhyay
SCSE, NTU

Dr. Shivam Bhasin,
Temasek Labs@NTU

Shenbaga and
Nila

Dr. Sujoy Sinha Roy,
TU Graz

GVM

"In a way, these things are like gold nuggets that God left in the forest. If I'm walking along in the forest and I stubbed my toe on it, who's to say I deserve credit for discovering it?"

-- Dr. Martin Hellman on the discovery of Public-Key Cryptography

Thank you!

References

[RRB+19] **Ravi, Prasanna**, Debapriya Basu Roy, Shivam Bhasin, Anupam Chattopadhyay, and Debdeep Mukhopadhyay. "Number “not used” once-practical fault attack on pqm4 implementations of NIST candidates." In International Workshop on Constructive Side-Channel Analysis and Secure Design, pp. 232-250. Springer, Cham, 2019.

[RJH+19] **Ravi, Prasanna**, Mahabir Prasad Jhanwar, James Howe, Anupam Chattopadhyay, and Shivam Bhasin. "Exploiting determinism in lattice-based signatures: practical fault attacks on pqm4 implementations of NIST candidates." In Proceedings of the 2019 ACM Asia Conference on Computer and Communications Security, pp. 427-440. 2019.

[RGCB19] **Ravi, Prasanna**, Sourav Sen Gupta, Anupam Chattopadhyay, and Shivam Bhasin. "Improving speed of Dilithium’s signing procedure." In International Conference on Smart Card Research and Advanced Applications, pp. 57-73. Springer, Cham, 2019.

[RRBC20] **Ravi, Prasanna**, Sujoy Sinha Roy, Anupam Chattopadhyay, and Shivam Bhasin. "Generic Side-channel attacks on CCA-secure lattice-based PKE and KEMs." IACR Transactions on Cryptographic Hardware and Embedded Systems (2020): 307-335.

References

[**R**BRC20] **Ravi, Prasanna**, Shivam Bhasin, Sujoy Sinha Roy, and Anupam Chattopadhyay. "Drop by Drop you break the rock-Exploiting generic vulnerabilities in Lattice-based PKE/KEMs using EM-based Physical Attacks." IACR Cryptol. ePrint Arch. 2020 (2020): 549.

[**R**SC+20] **Ravi, Prasanna**, Vijaya Kumar Sundar, Anupam Chattopadhyay, Shivam Bhasin, and Arvind Easwaran. "Authentication Protocol for Secure Automotive Systems: Benchmarking Post-Quantum Cryptography." In IEEE International Symposium on Circuits and Systems (2020).

[**R**PBC20] **Ravi, Prasanna**, Romain Poussier, Shivam Bhasin, and Anupam Chattopadhyay. "On Configurable SCA Countermeasures Against Single Trace Attacks for the NTT: A Performance Evaluation Study over Kyber and Dilithium on the ARM Cortex-M4." In *Security, Privacy, and Applied Cryptography Engineering: 10th International Conference, SPACE 2020,* pp. 123-146. Springer International Publishing, 2020.

[**R**BRC21] **Ravi, Prasanna**, Shivam Bhasin, Sujoy Sinha Roy, and Anupam Chattopadhyay. "On Exploiting Message Leakage in (few) NIST PQC Candidates for Practical Message Recovery and Key Recovery Attacks." IACR Cryptol. ePrint Arch. 2020 (2020): 1559.

[**R**HCB21] **Ravi, Prasanna**, James Howe, Anupam Chattopadhyay, and Shivam Bhasin. "Lattice-based Key-sharing Schemes: A Survey." ACM Computing Surveys (CSUR) 54, no. 1 (2021): 1-39.

References

[**R**EB+22] **Ravi, Prasanna**, Martianus Frederic Ezerman, Shivam Bhasin, Anupam Chattopadhyay, and Sujoy Sinha Roy. "Will You Cross the Threshold for Me? Generic Side-Channel Assisted Chosen-Ciphertext Attacks on NTRU-based KEMs." *IACR Transactions on Cryptographic Hardware and Embedded Systems* (2022): 722-761.

[**R**YB+22] **Ravi, Prasanna**, Bolin Yang, Shivam Bhasin, Fan Zhang, and Anupam Chattopadhyay. "Fiddling the Twiddle Constants-Fault Injection Analysis of the Number Theoretic Transform." *IACR Transactions on Cryptographic Hardware and Embedded Systems* (2023): 447-481.

[**R**CDB22] **Ravi, Prasanna**, Anupam Chattopadhyay, Jan-Pieter D'Anvers and Anubhab Baksi. "Side-channel and Fault-injection attacks over Lattice-based Post-quantum Schemes (Kyber, Dilithium): Survey and New Results." *Cryptology ePrint Archive* (2022) – Accepted at ACM TECS

[**R**RD+22] Rajendran, Gokulnath, **Prasanna Ravi**, Jan-Pieter D'Anvers, Shivam Bhasin, and Anupam Chattopadhyay. "Pushing the Limits of Generic Side-Channel Attacks on LWE-based KEMs-Parallel PC Oracle Attacks on Kyber KEM and Beyond." *IACR Transactions on Cryptographic Hardware and Embedded Systems* (2023): 418-446.

[**R**BC+22] **Ravi, Prasanna**, Shivam Bhasin, Anupam Chattopadhyay, Aikata Aikata and Sujoy Sinha Roy. "Backdooring Post-Quantum Cryptography: Kleptographic Attacks on Lattice-based KEMs." *Cryptology ePrint Archive* (2022).

References

[**R**DB+22] **Ravi, Prasanna**, Suman Deb, Anubhab Baksi, Anupam Chattopadhyay, Shivam Bhasin, and Avi Mendelson. "On threat of hardware trojan to post-quantum lattice-based schemes: a key recovery attack on saber and beyond." In *Security, Privacy, and Applied Cryptography Engineering: 11th International Conference, SPACE 2021, Kolkata, India, December 10–13, 2021, Proceedings*, pp. 81-103. Cham: Springer International Publishing, 2022.