NANYANG
TECHNOLOGICAL
UNIVERSITY
SINGAPORE

Practical Side-Channel and Fault Injection Analysis on Lattice-Based Cryptography

Prasanna Ravi

under supervision of

Dr.Anupam Chattopadhyay

Dr.Shivam Bhasin

Temasek Labs and School of Computer Science and Engineering, NTU, Singapore

1st June 2021, ICHSA 2021

IN THE NOT TOO DISTANT FUTURE…

Security in Quantum Era: NIST PQC Call

- **National Institute of Standards and Technology (NIST)** initiated a standardization process for post-quantum cryptography (**PQC**) in November 2017.
- The first round had **69** candidates, second round had **26** candidates and the process is currently in its **third** and **final** round [AGJS+20].

Type	Signature	PKE/KEM	Finalist (Alternate)
Lattice Based	**2**	**3 (2)**	**5 (2)**
Code-Based	-	1 (2)	1 (2)
Multivariate	1 (1)	-	1 (1)
Hash-Based	- (2)	-	- (2)
Isogeny based	-	- (1)	- (1)
Others	-	-	- (0)
Total	3 (3)	4 (5)	7 (8)

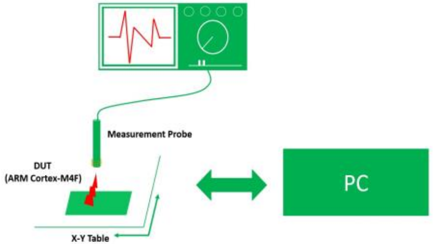
Security in Quantum Era: NIST PQC Call

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

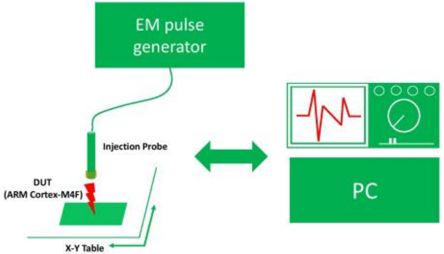
- NIST explicitly states that "*encourages additional research regarding side-channel analysis*" of the finalist candidates and that it "*hopes to collect more information about the costs of implementing these algorithms in a way that provides resistance to such attacks*" [AGJS+20].

Main Focus:

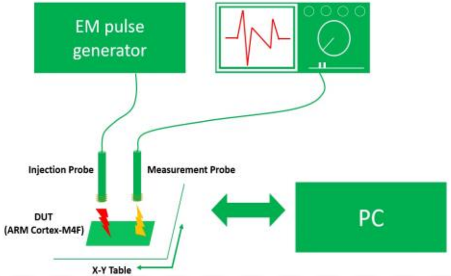
Side-Channel Analysis (SCA)

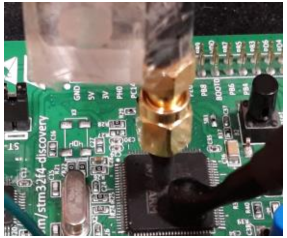


Fault Injection Analysis (FIA)



Combined SCA and FIA





Research Outcomes

Lattice-based Cryptography

Physical Attacks

SCA

[**R**RBC20] (*TCHES 2020*)

[**R**BRC20]** (*IACR ePrint*)

[**R**EBCR21] (*Third NIST PQC Conference*)

FIA

[**R**RBCM19] (*COSADE 2019*)

[**R**JHCB19] (*AsiaCCS 2019*)

Combined SCA and FIA

[**R**BRC20] (*IACR ePrint*)

Survey

[**R**HCB20]
(ACM Computing Surveys)

Implementations

Countermeasures

[**R**PBC20] (*SPACE 2020*)

Optimizations

[**R**GCB19] (*CARDIS 2019*)

[**R**SCBE20] (*ISCAS 2020*)

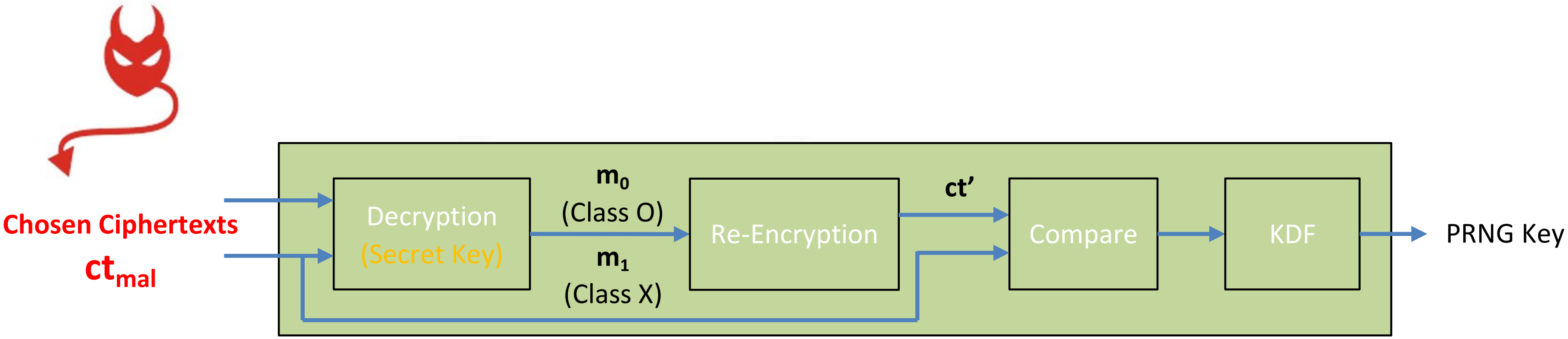
**** Under Submission**

Main Contributions

Side-Channel Analysis (SCA)

- **Attack Scenario:** Chosen-Ciphertext Attacker (CCA)
- **Attack Target:** CCA secure PKE and KEMs for key recovery, message recovery

- *A Chosen Ciphertext Attacker in the presence of side-channels can perform a variety of message recovery and key recovery attacks.*



IND-CCA Secure Decapsulation

Side-Channel Analysis (SCA)

- **PC Oracle-based SCA** in LWE/LWR-based schemes (***TCHES 2020***):
  - Novel EM/power side-channel vulnerabilities to realize a PC Oracle
  - Key Recovery in a few thousand queries
  - No. of target schemes: **six** (**Kyber**, **Saber**, **Frodo**, NewHope, Round5 and LAC)

- **FD Oracle-based SCA** in LWE/LWR-based schemes (***IACR ePrint*****):
  - Novel **single trace** message recovery attacks
  - Exploiting **Ciphertext Malleability** as a powerful tool to aid SCA
  - Break well-known shuffling and masking countermeasures
  - No. of target schemes: **six** (**Kyber**, **Saber**, **Frodo**, NewHope, Round5 and LAC)
  - First practical combined SCA and FIA over lattice-based schemes

- **PC and DF Oracle-based SCA** in NTRU-based schemes (***Third NIST PQC Conference***):
  - Target Scheme: Streamlined NTRU Prime
  - Key Recovery in a few thousand queries

**** Under Submission**

Side-Channel Analysis (SCA)

Side-Channel Assisted Chosen Ciphertext Attacks

- **LWE/LWR-based**
  - **PC Oracle-based**
    - D'Anvers et al. [DTVV19]
    - Ravi et al. [RRBC20]
  - **FD Oracle-based**
    - Xu et al. [XPRO20]
    - Ravi et al. [RBRC20]
    - Ngo et al. [NDGJ21]
  - **DF Oracle-based**
    - Guo et al. [GJN20]
    - Bhasin et al. [BDH+21]
- **NTRU-based**
  - **PC Oracle-based**
    - Ravi et al. [REBCR21]
  - **DF Oracle-based**
    - Ravi et al. [REBCR21]

Fault Injection Analysis (FIA)

- **Fault Injection Analysis:**
  - Forcing **Nonce-Misuse** through Faults (***COSADE 2019***):
    - First practical FIA (EM-based) over lattice-based schemes
    - No. of target schemes: **four** (Kyber, Dilithium, Frodo and NewHope)
    - Countermeasure incorporated into algorithmic specification of Frodo (Alternate Finalist)
  - Exploiting **Determinism** in Lattice-based Signatures (***AsiaCCS 2019***):
    - Fault Attack + Forgery using partial secret key recovery
    - First practical FIA (EM-based) over **two** signature schemes (Dilithium and qTESLA)

Implementations and Countermeasures

- Configurable SCA Countermeasures for Number Theoretic Transform (***SPACE 2020***):
  - Novel **masking** and **shuffling** countermeasures
  - Practical Implementation within Kyber and Dilithium on the ARM Cortex-M4

- Improving Speed of Dilithium's Signing Procedure *(**CARDIS 2019**):*
  - 8-35% improvement in signing speed of Dilithium on ARM Cortex-M4

- PQC Evaluation within Authentication Protocol in Automotive Context (***ISCAS 2020***):
  - Integration of lattice-based schemes within an authentication protocol LASAN.
  - Practical Evaluation on Automotive testbed based on ARM Cortex-R4 MCU (RTOS-based)
  - **Communication Bandwidth** is a main bottleneck in implementing PQC for automotive networks

“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

[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.

[RBRC20] **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.

[RSCBE20] **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).

[RPBC20] **Ravi, Prasanna**, Romain Poussier, Shivam Bhasin, and Anupam Chattopadhyay. "On Configurable SCA Countermeasures Against Single Trace Attacks for the NTT." IACR Cryptol. ePrint Arch. 2020 (2020): 1038 (To appear in SPACE 2020)

References

[RRBCM19] **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.

[RJHCB19] **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.

[RBRC20] **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.

References

[RHCB20] **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.

[REBCR21] **Ravi, Prasanna**, Ezerman, Martianus Frederic, Shivam Bhasin, Anupam Chattopadhyay and Sujoy Sinha Roy. " Generic Side-Channel Assisted Chosen-Ciphertext Attacks on Streamlined NTRU Prime" IACR Cryptol. ePrint Arch. 2021 (2021): 718.

[AGJS+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.