NANYANG TECHNOLOGICAL UNIVERSITY SINGAPORE

Practical Fault Injection Analysis of Lattice-based NIST PQC Standards - Kyber and Dilithium

Prasanna Ravi

Temasek Labs, NTU, Singapore

NIST PQC Seminars,
5th May 2023

Notice

- **Main Motive**:
  - Flavor of reported fault attacks on Kyber and Dilithium (and countermeasures)
  - Algorithmic properties and Implementation Choices facilitate efficient FIA
  - Towards fault resistant implementations of Kyber and Dilithium

- Most fault attacks demonstrated on bare-metal PQC software running on ARM Cortex-M4 processor: Clock/Voltage Glitching, EMFI

- Talk includes published works from journals, conferences, and IACR ePrint Archive.

- Talk includes works of other researchers (cited appropriately)

- For easier explanation, we ‘simplify’ concepts, and contains lots of illustrations!!

Outline

- ❑ FIA on Kyber:
  - ❑ FIA on Key Generation and Encapsulation
  - ❑ FIA on Decapsulation
- ❑ FIA on Dilithium
  - ❑ FIA on Signing
  - ❑ FIA on Verification
- ❑ Conclusion

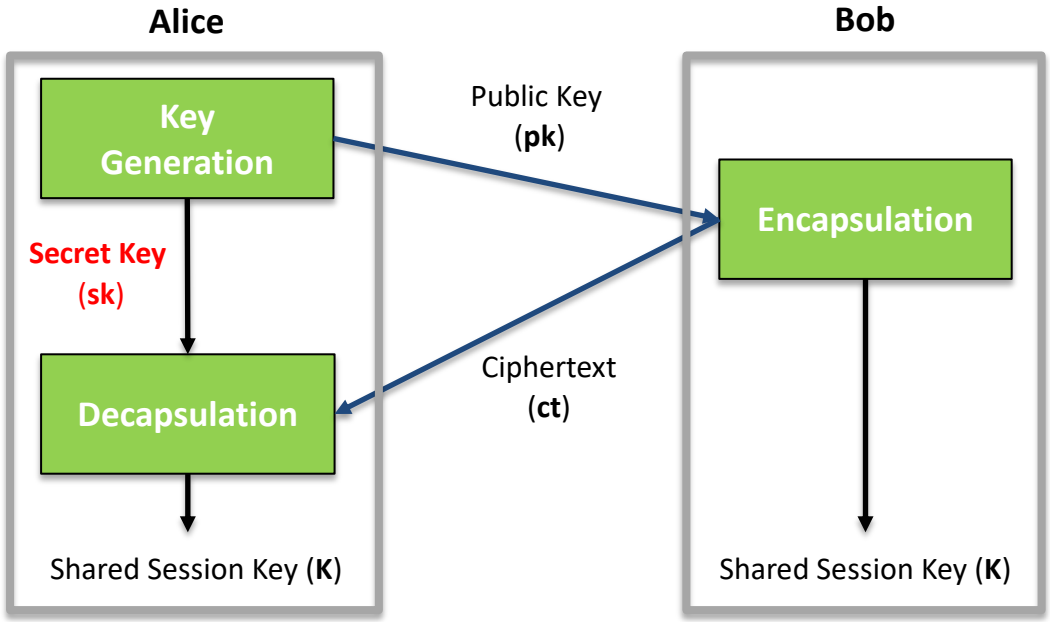
Outline

- ❑ **FIA on Kyber:**
  - ❑ **FIA on Key Generation and Encapsulation**
  - ❑ **FIA on Decapsulation**

- ❑ FIA on Dilithium
  - ❑ FIA on Signing
  - ❑ FIA on Verification

- ❑ Conclusion

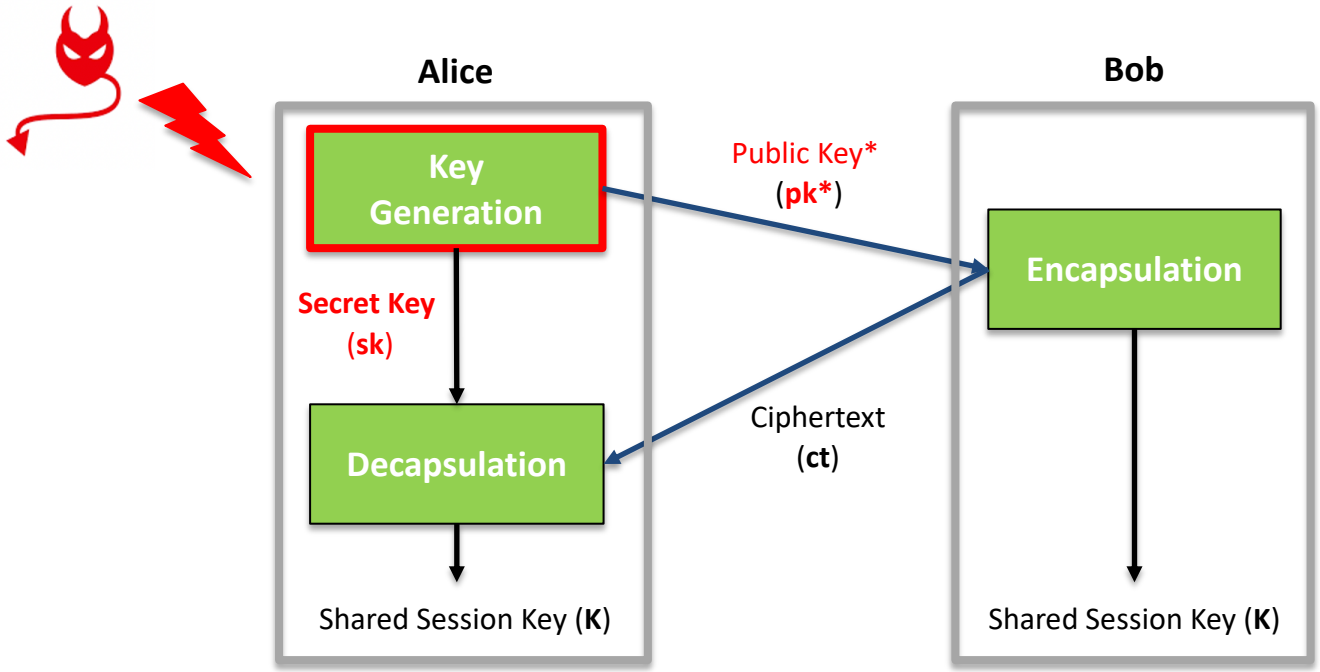
Key Encapsulation Mechanisms (KEMs)



Two Modes Possible:

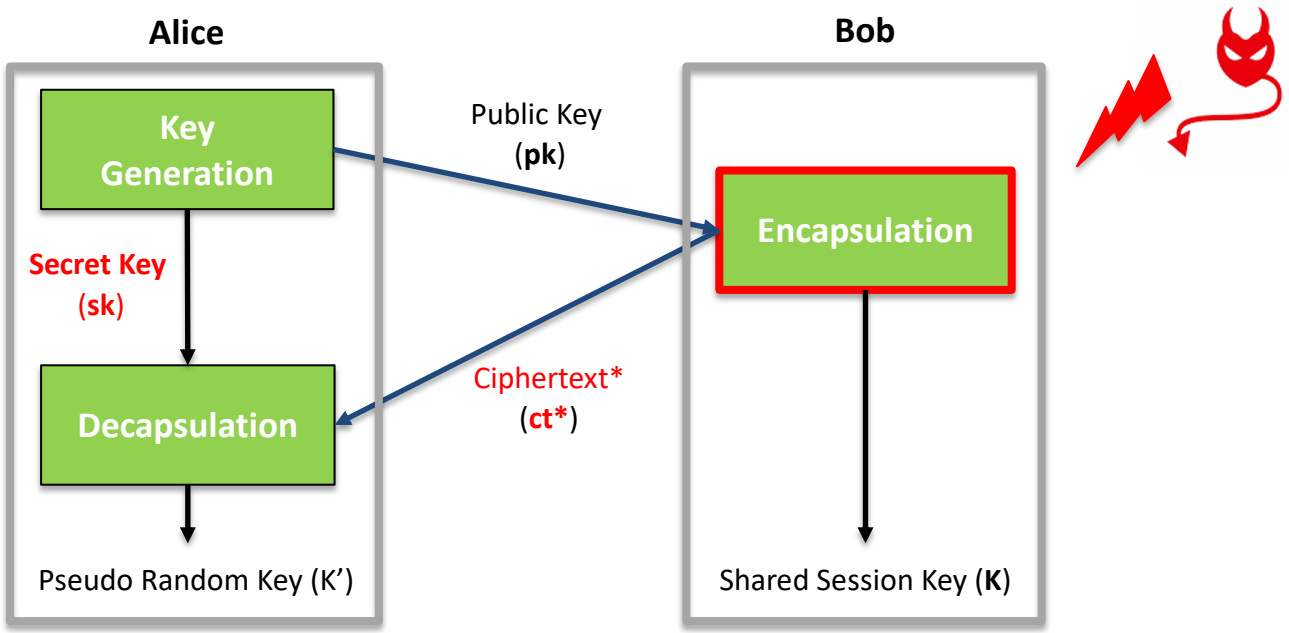
1. Ephemeral Key
2. Static Key

KEM in Ephemeral Mode: Attacking Alice



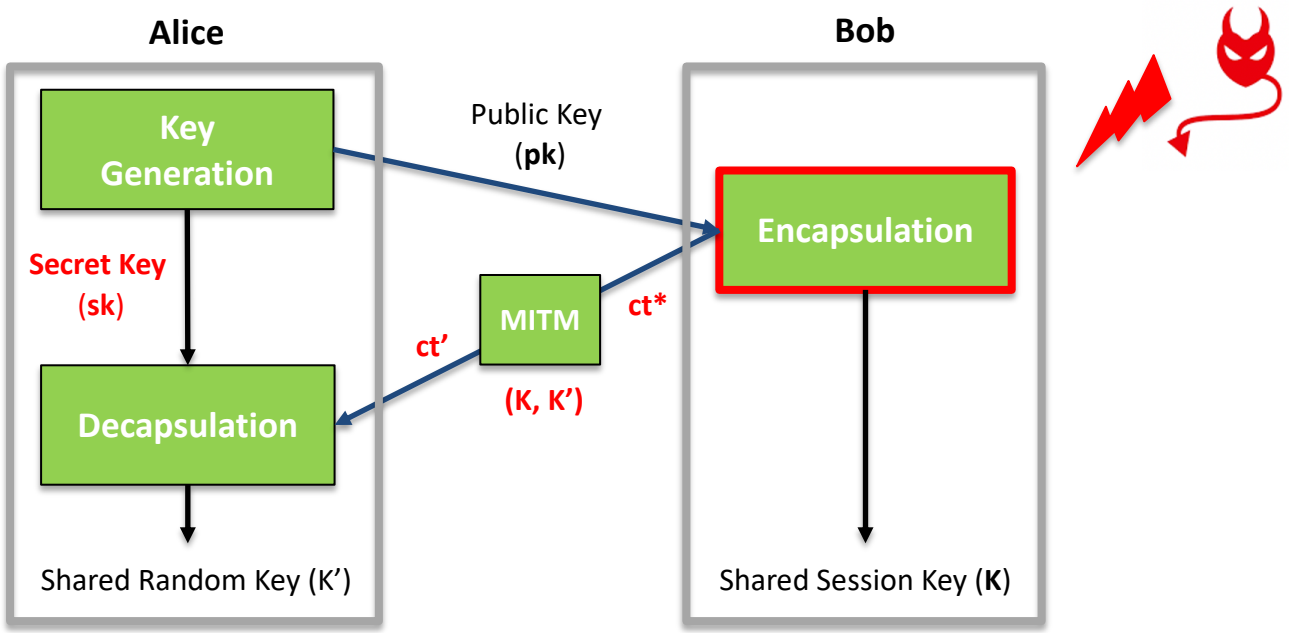
- Single execution to target Key Generation: Key Recovery Attack
  - Recover Secret key from Faulty but valid Public Key
- Decapsulation does not serve as an effective target – Attacker can only observe binary output (1-bit)

KEM in Ephemeral Mode: Attacking Bob



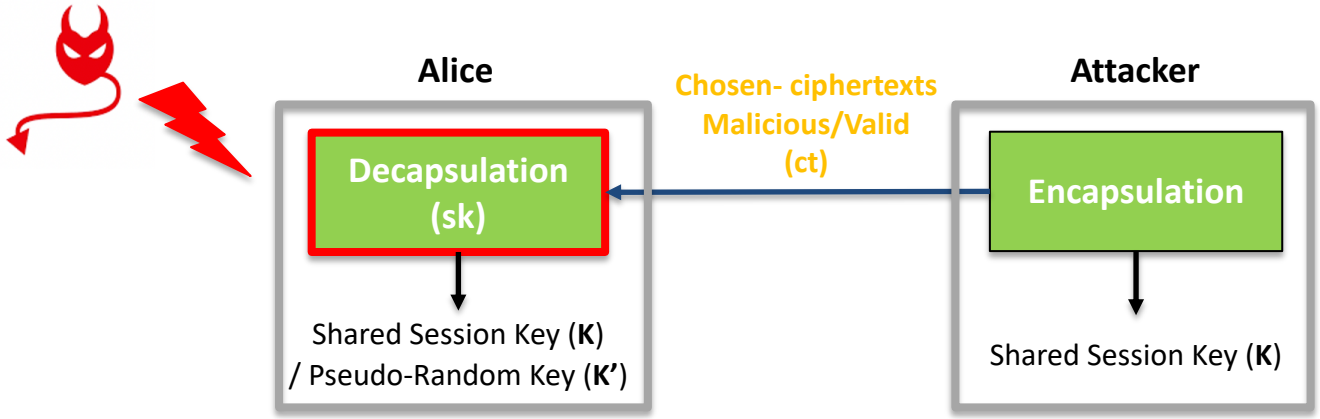
- Single execution to target Encapsulation Procedure: Message Recovery Attack
  - Recover Message from Faulty Ciphertext
  - Results in Decapsulation Failure (CCA Secure)

KEM in Ephemeral Mode: Attacking Bob



- Single execution to target Encapsulation Procedure: Message Recovery Attack
  - Recover Message from Faulty Ciphertext
  - Results in Decapsulation Failure (CCA Secure)
  - Attacker can still perform a MITM Attack!!!

KEM in Static Mode: Attacking Alice



Chosen Ciphertext	Output
CT1	Success
CT2	Failure
CT3	Success
…	…

Decryption Failure (DF) Oracle through Faults

Key Recovery

Fault Assisted Chosen-Ciphertext Attacks

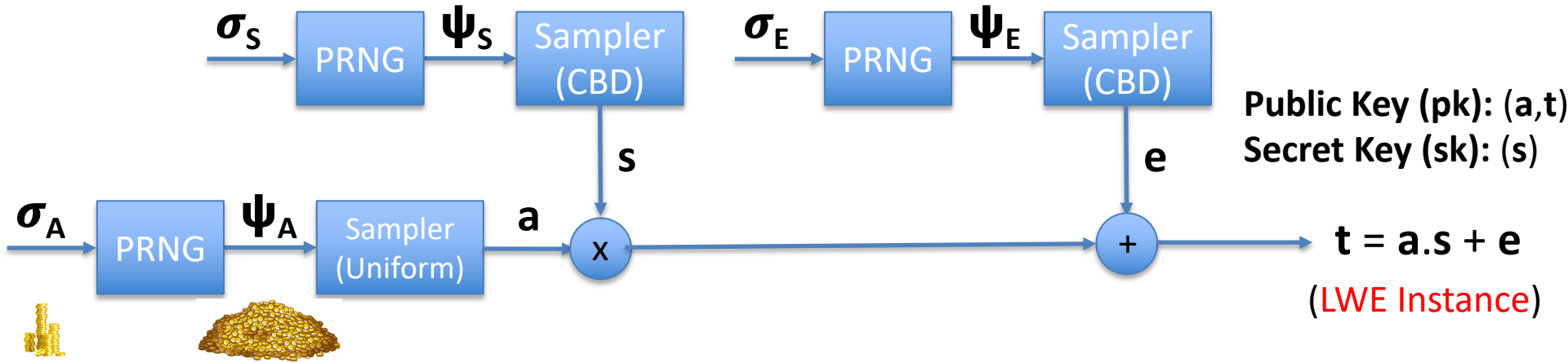
Fault Attack Characteristics

- We describe known fault attacks with the following characteristics:
  - **Attacker's ability to communicate with DUT (DUT_IO_Access):**
    - Observe_DUT_IO: Can only passively observe target's IO
    - Communicate_DUT_IO: Can communicate with target
  - **Targeted or Not (**Profiling, Knowledge of Implementation**):**
    - Targeted_Fault
    - Random_Fault
  - **Type of Fault:** Control Flow, Data
  - **Number of Faults within Single Computation:** Single/Multiple
  - **Total Number of Faulty Computations**

Outline

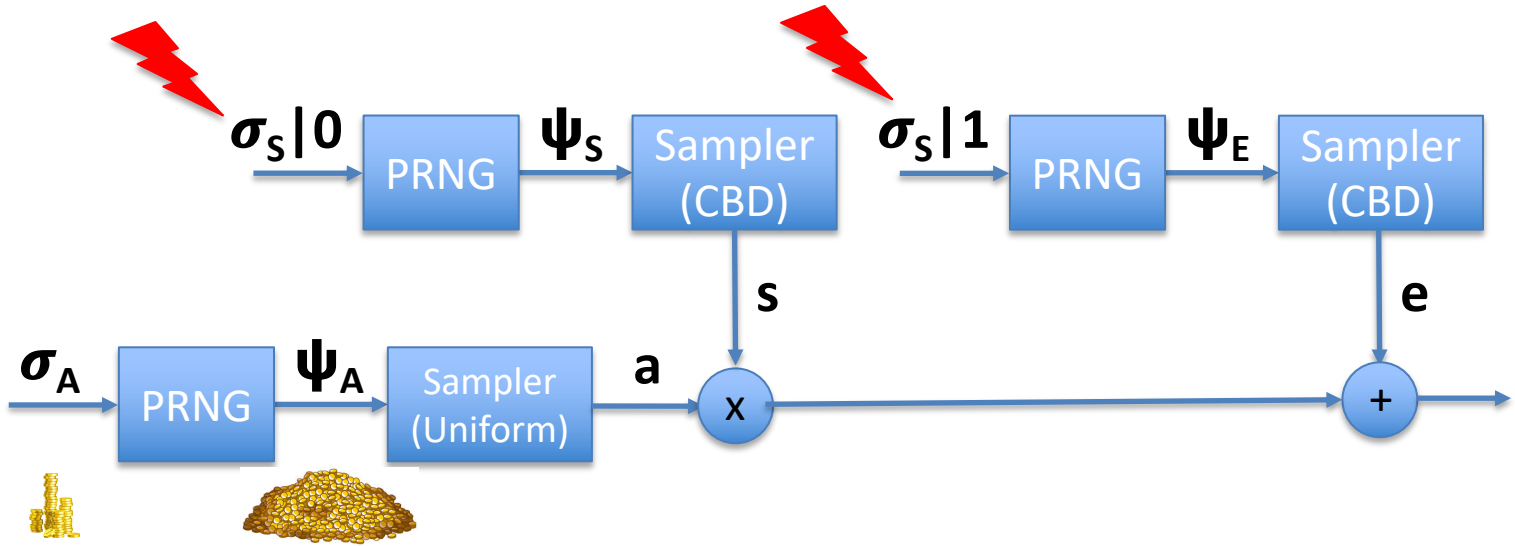
- ❑ **FIA on Kyber:**
  - ❑ **FIA on Key Generation**
  - ❑ FIA on Decapsulation
- ❑ FIA on Dilithium
  - ❑ FIA on Signing
  - ❑ FIA on Verification
- ❑ Conclusion

FIA on Key Generation



- **Aim of FIA on KeyGen:**
  - Weak LWE instances (easily solveable)
  - Secrets with Low Entropy

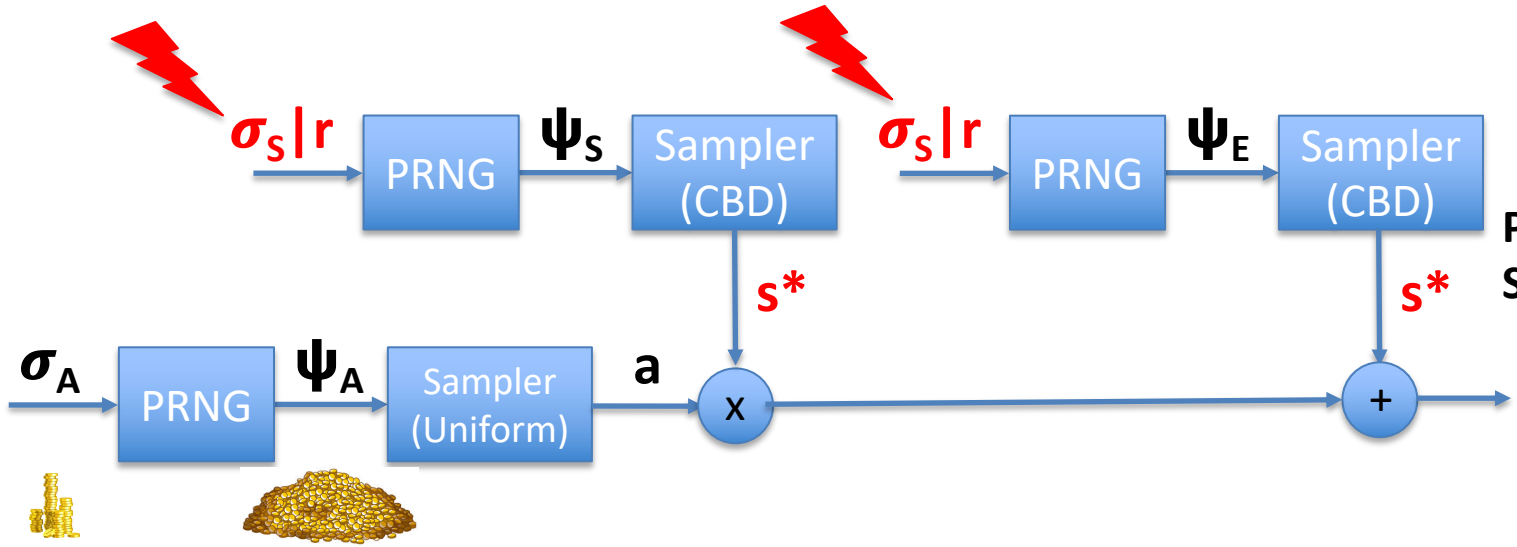
FIA on KeyGen: Weak LWE instances [RRB+19]



- **Fault Vunerability**: Seed used to sample **s** and **e** only differ by a single byte
  - Inject fault to force using same seed for **s** and **e**

[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: 10th International Workshop, COSADE 2019, Darmstadt, Germany, April 3–5, 2019, Proceedings 10*, pp. 232-250. Springer International Publishing, 2019.

FIA on KeyGen: Weak LWE instances [RRB+19]



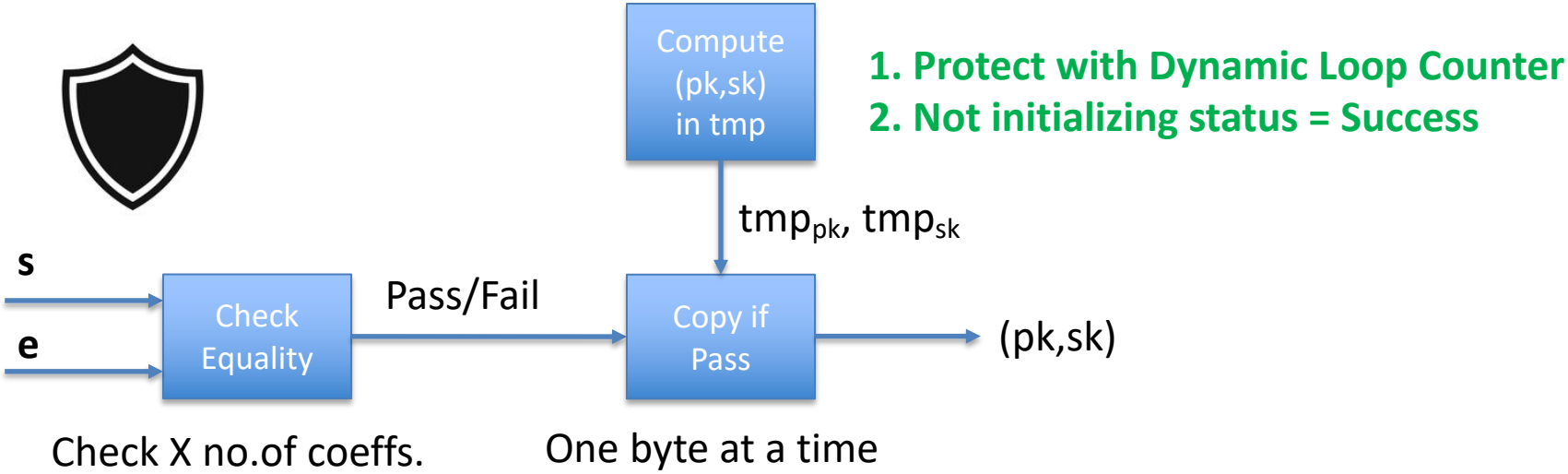
- **Weak LWE Instance**: Solved by Gaussian Elimination
- Applicability to Kyber KEM: Inject **k-2k** targeted faults
- Round-1 Kyber used rounded public keys, but rounding was removed from Round-2

[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: 10th International Workshop, COSADE 2019, Darmstadt, Germany, April 3–5, 2019, Proceedings 10*, pp. 232-250. Springer International Publishing, 2019.

FIA on KeyGen: Weak LWE instances [RRB+19]

- Single fault enough for NewHope (Ring-LWE) and FrodoKEM (Standard-LWE)

- **Impact**: The algorithm of FrodoKEM (Finalist NIST PQC candidate) was modified in Round 2 to eliminate the fault vulnerability.
  - Completely different seeds were used to sample **s** and **e**

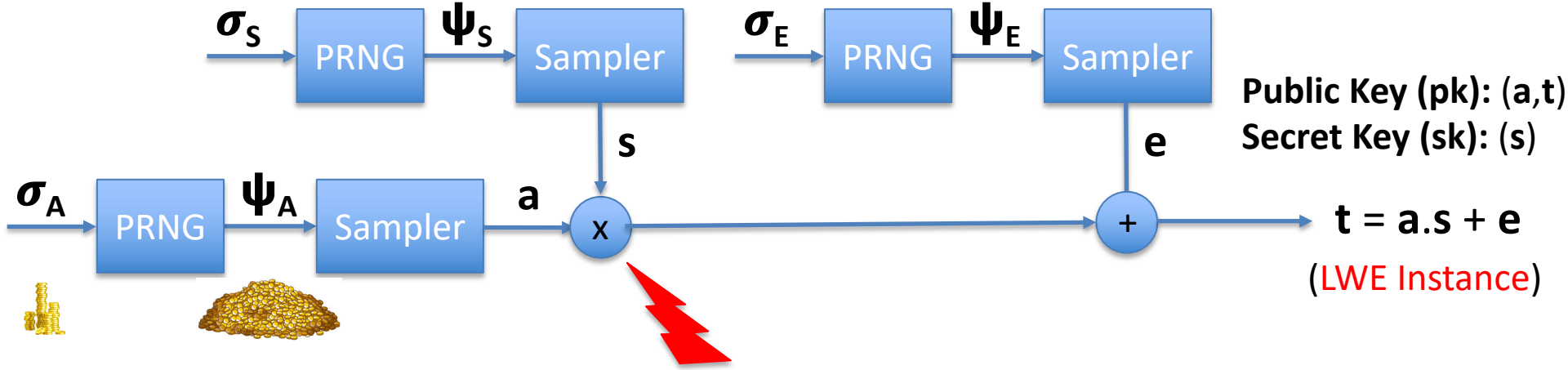


[RRB+19] Ravi, Prasanna, Debapriya Basu Roy, Shivam Bhasin, Anupam Chattopadhyay, and Debdeep Mukhopadhyay. "Number “not used” once-practical fault attack on pqm4 implementations of NIST candidates." In *Constructive Side-Channel Analysis and Secure Design: 10th International Workshop, COSADE 2019, Darmstadt,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

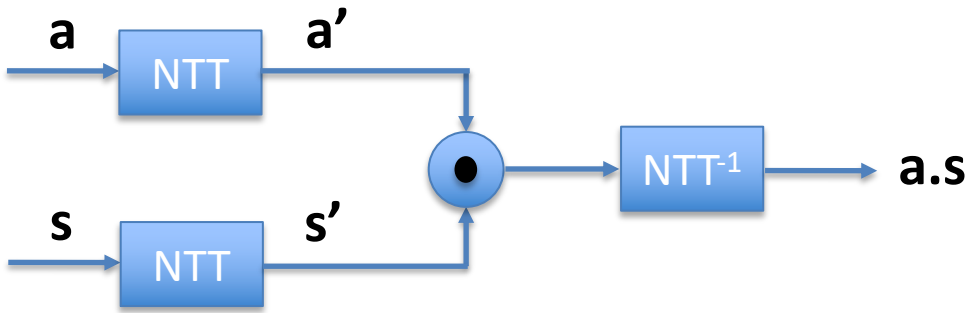
FIA on Kyber KeyGen/Encaps: Summary

Attack Name	DUT_IO_Access	Type of Fault	Targeted_ or_Not	No. of Faults within Single Computation	Total No. of Faulty Computations	Countermeasure
Nonce_Fault _Attack	Observe_DUT_IO	Data /Control	Targeted	k-2k	1	Check equality of s and e Copy Public Key if Pass

FIA on KeyGen: Reduce Entropy of Secret [RYB+23]

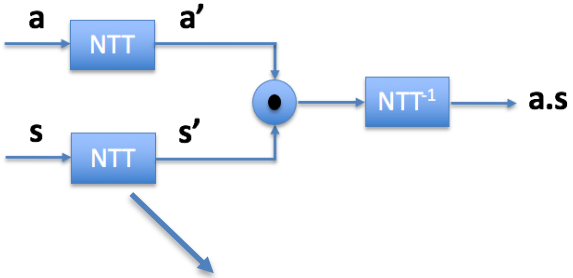


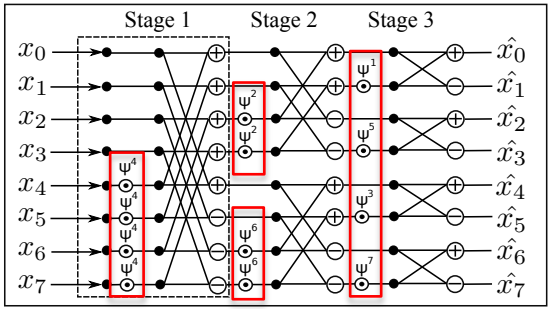
Polynomial multiplication is done using Number Theoretic Transform (NTT)



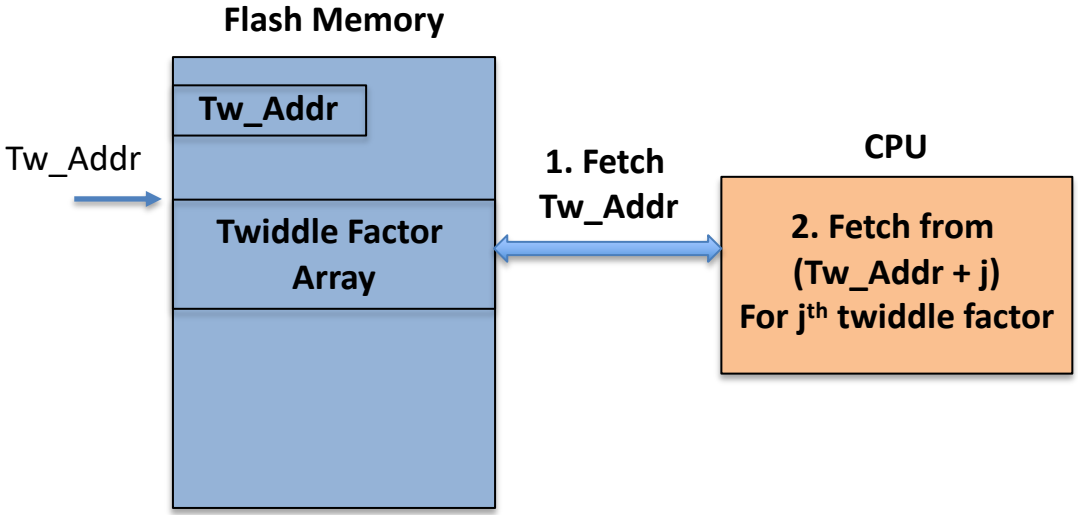
[RYB+23] Ravi, Prasanna, Bolin Yang, Shivam Bhasin, Fan Zhang, and Anupam Chattopadhyay. "Fiddling the Twiddle Constants-Fault Injection Analysis of the Number Theoretic Transform." *IACR Transactions on Cryptographic Hardware and Embedded Systems* (2023): 447-481.

FIA on KeyGen: Reduce Entropy of Secret [RYB+23]





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



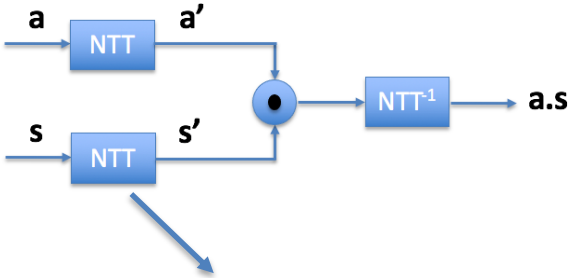
Main Observation: Tw_Addr is used as **base-address** to calculate address for all constants

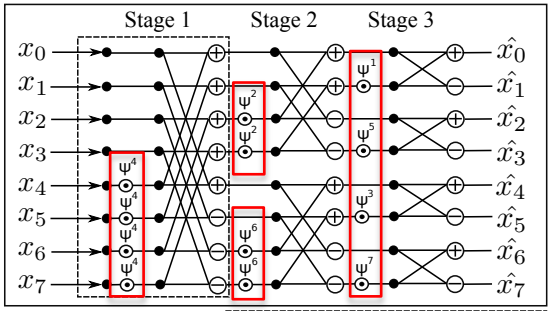
Fault Vulnerability: Can an attacker fault the base address?

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

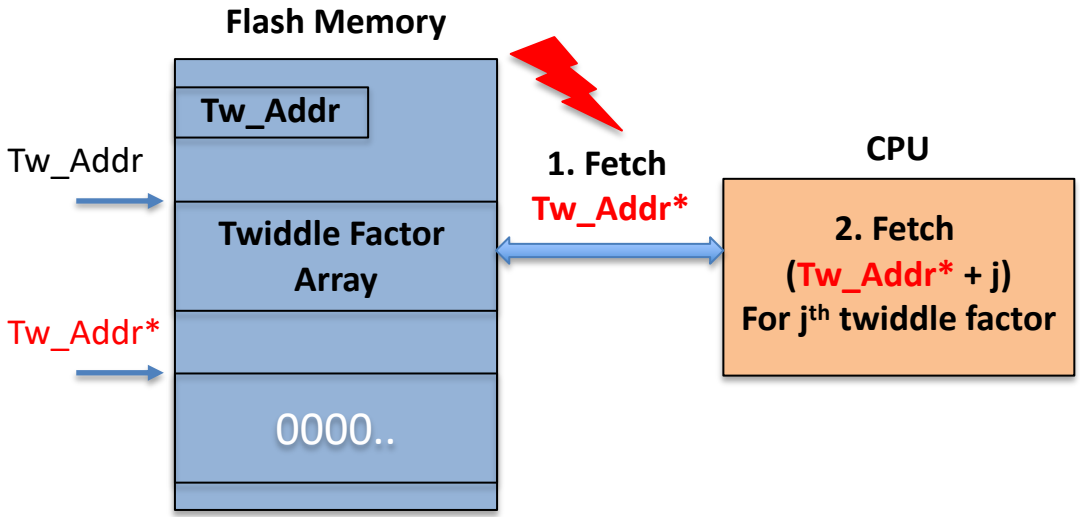
[RYB+22] Ravi, Prasanna, Bolin Yang, Shivam Bhasin, Fan Zhang, and Anupam Chattopadhyay. "Fiddling the Twiddle Constants-Fault Injection Analysis of the Number Theoretic Transform." *IACR Transactions on Cryptographic Hardware and Embedded Systems* (2023): 447-481.

FIA on KeyGen: Reduce Entropy of Secret [RYB+23]





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



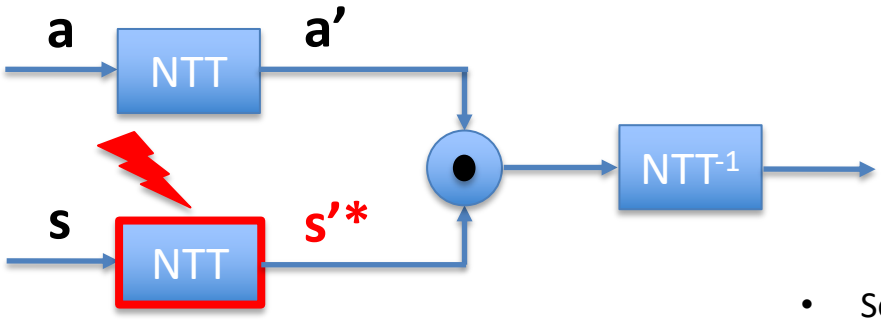
Observation: Can zeroize the entire twiddle factor array in a single fault

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

What happens when twiddle factors are zeroized???

[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.

FIA on KeyGen: Reduce Entropy of Secret [RYB+23]



Valid (pk,sk)

s0	s1	s2	s3	s4	s5	s6	s7

s0	s1	s0	s1	s0	s1	s0	s1

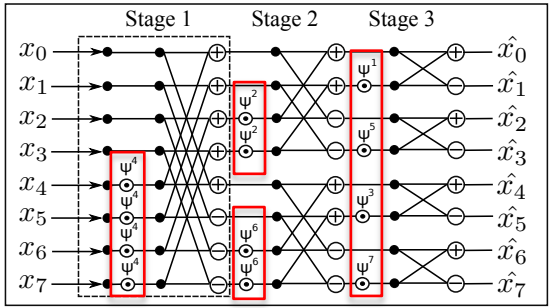
The effective secret s*

s0	s1	0	0	0	0	0	0

- Secret (**s'***) in NTT domain is used for Decaps
  - Kyber saves secret in NTT domain
  - To avoid extra NTT/INTT conversions
- Originally sampled secret **s** is forgotten!!!
  - Memoryless property of Kyber
  - Not applicable to Dilithium
- Attack also applies to masked implementations

[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.

FIA on KeyGen: Reduce Entropy of Secret [RYB+23]



- Sanity Check on Twiddle Constants:
  - Check Arithmetic Properties of Twiddle Constants:
    - n^{th} root of unity
  - Check Entropy of Twiddle Constants
- Not rely on single base address to access Twiddle Constant Array
- Check Entropy of NTT output

[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.

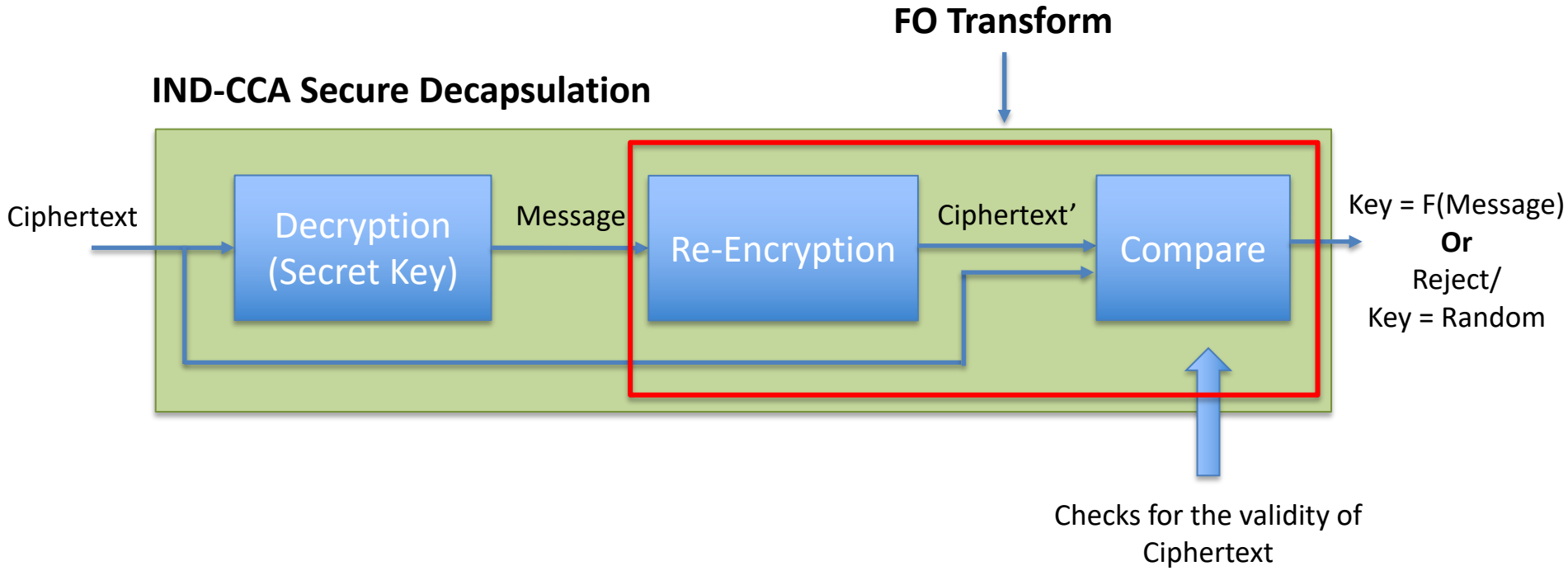
FIA on Kyber KeyGen/Encaps: Summary

Attack Name	DUT_IO_Access	Type of Fault	Targeted_ or_Not	No. of Faults within Single Computation	Total No. of Faulty Computations	Countermeasure
Nonce_Fault_ Attack	Observe_DUT_IO	Data /Control	Targeted	k	1	Check equality of s and e Copy Public Key if Pass
NTT_Fault_ Attack	Observe_DUT_IO	Data	Targeted	1	1	Sanity Check on Twiddle Constants or NTT outputs

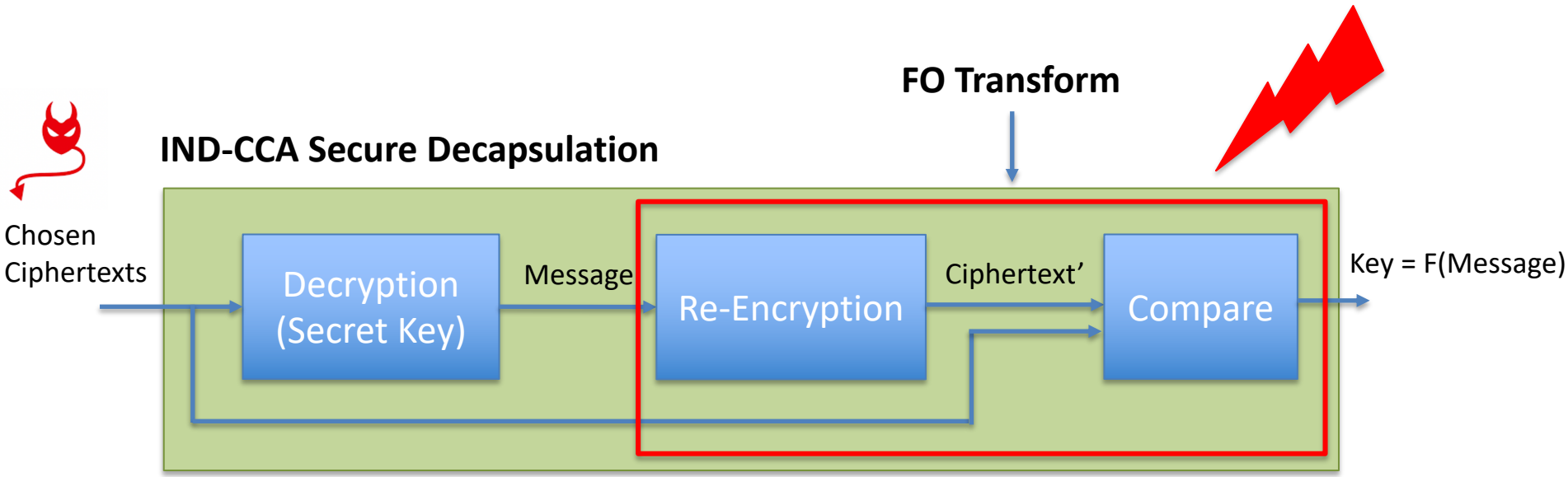
Outline

- ❑ **FIA on Kyber:**
  - ❑ FIA on Key Generation
  - ❑ **FIA on Decapsulation**
- ❑ FIA on Dilithium
  - ❑ FIA on Signing
  - ❑ FIA on Verification
- ❑ Conclusion

FIA on Decapsulation



FIA on Decapsulation: Skip CT Comparison [XIU+21]

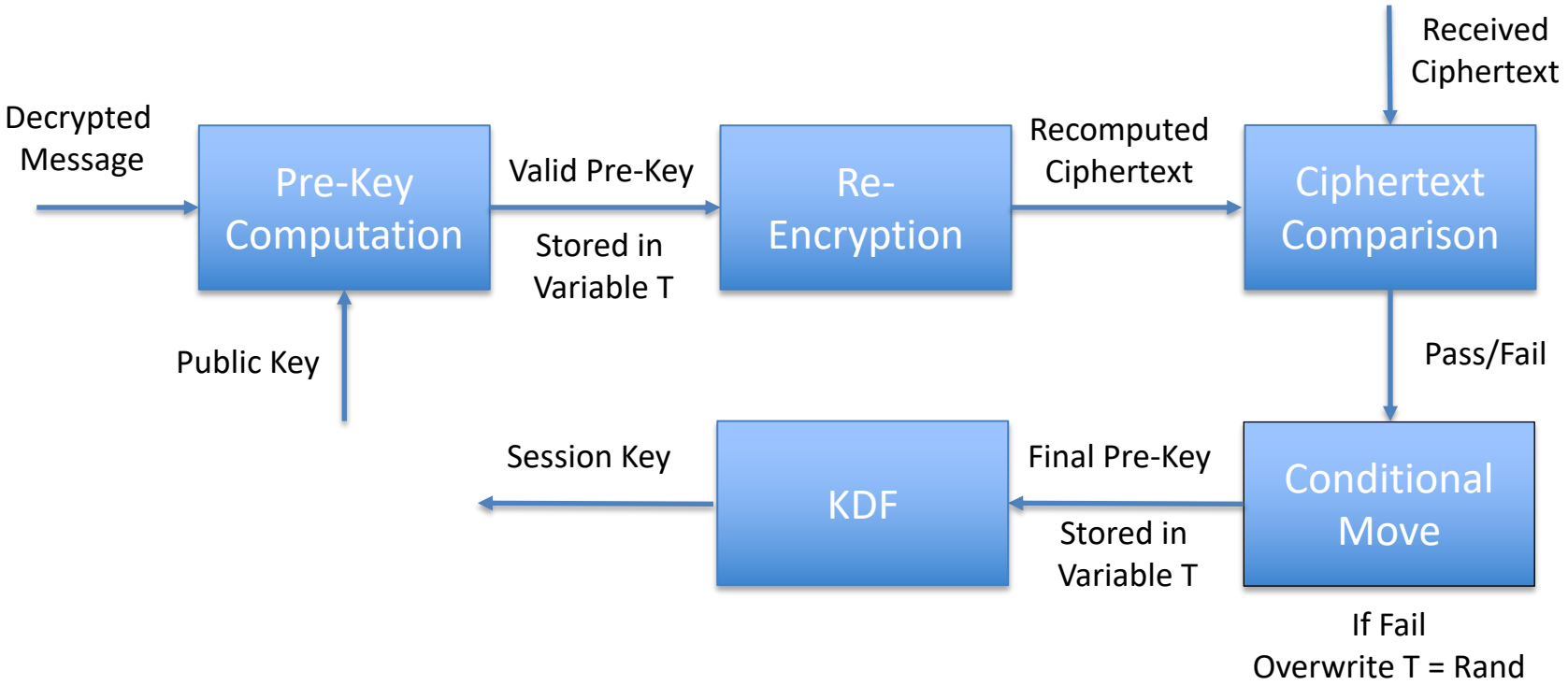


Bypass Comparison ⇒ **Downgrade from CCA to CPA Security**

This attack could have been easily avoided with a more careful implementation

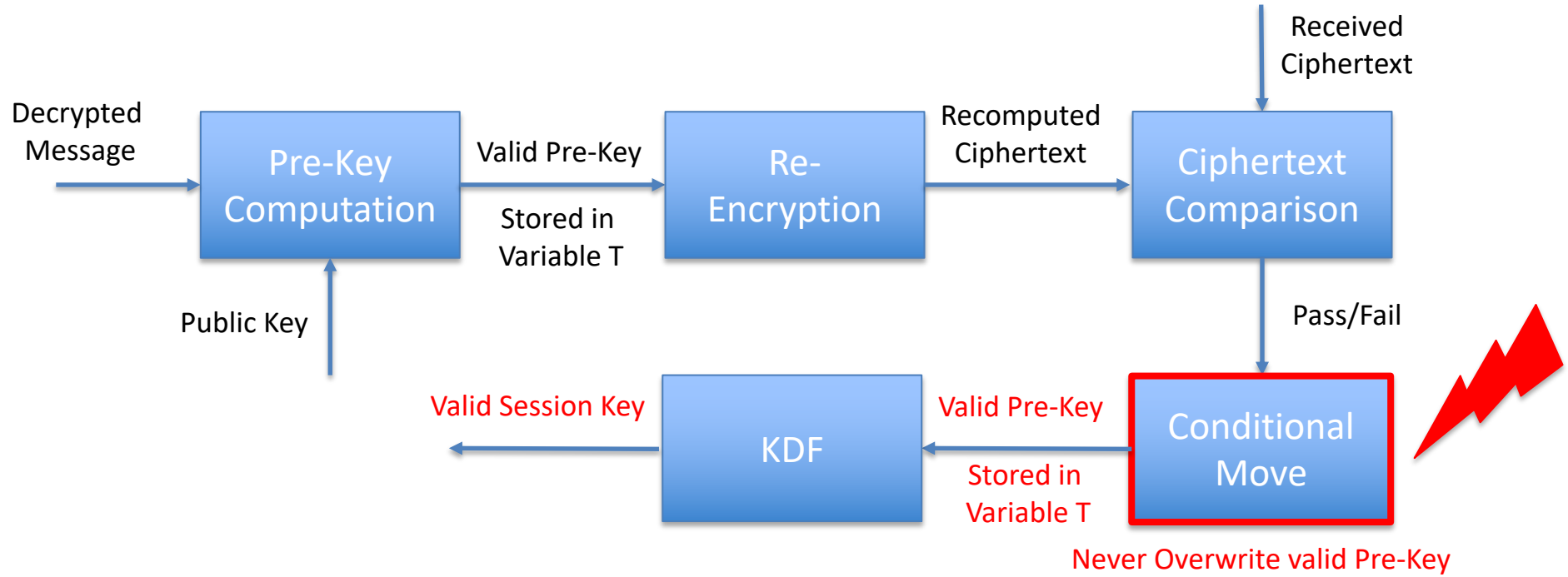
[XIU+21] Xagawa, Keita, Akira Ito, Rei Ueno, Junko Takahashi, and Naofumi Homma. "Fault-injection attacks against NIST's post-quantum cryptography round 3 KEM candidates." In *Advances in Cryptology–ASIACRYPT 2021: 27th International Conference on the Theory and Application of Cryptology and Information Security, Singapore, December 6–10, 2021, Proceedings, Part II 27*, pp. 33-61. Springer International Publishing, 2021.

FIA on Decapsulation: Skip CT Comparison [XIU+21]



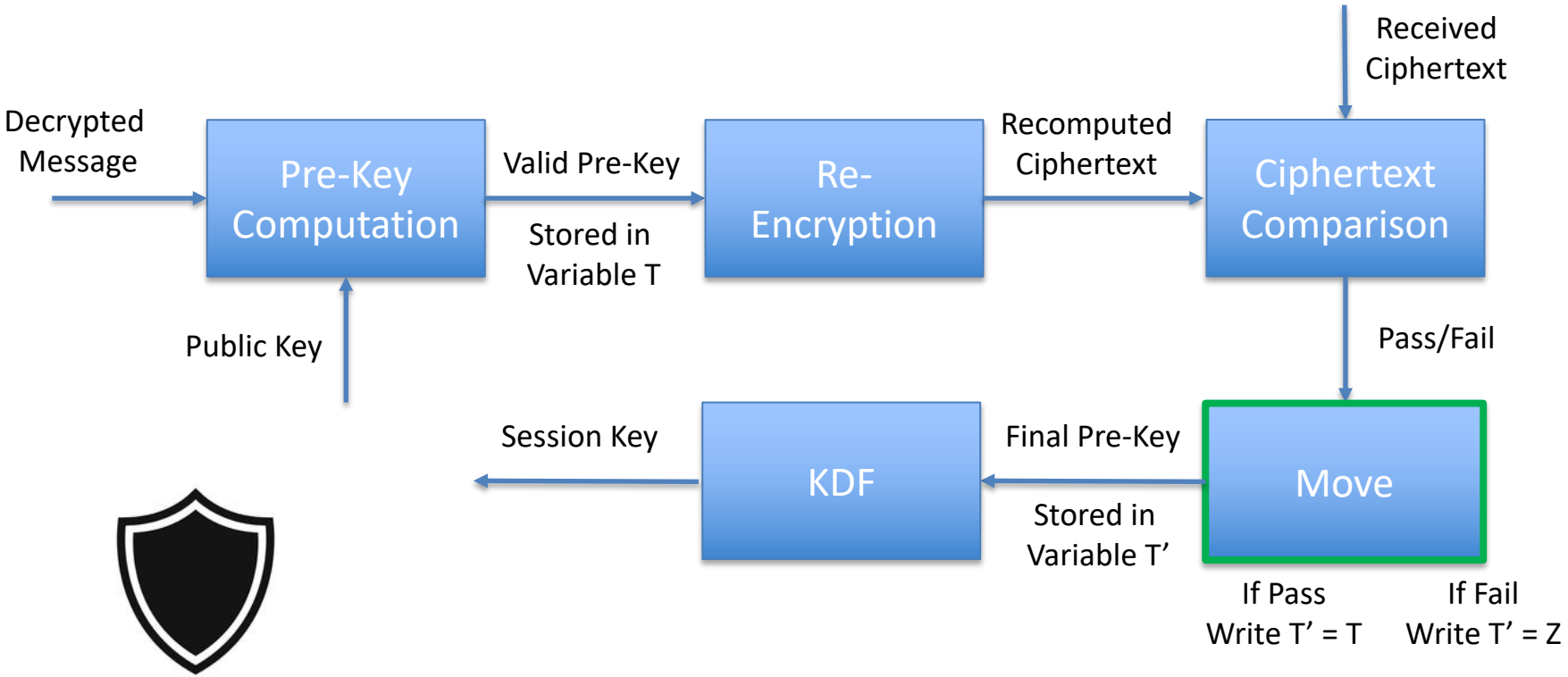
[XIU+21] Xagawa, Keita, Akira Ito, Rei Ueno, Junko Takahashi, and Naofumi Homma. "Fault-injection attacks against NIST's post-quantum cryptography round 3 KEM candidates." In *Advances in Cryptology–ASIACRYPT 2021: 27th International Conference on the Theory and Application of Cryptology and Information Security, Singapore, December 6–10, 2021, Proceedings, Part II 27*, pp. 33-61. Springer International Publishing, 2021.

FIA on Decapsulation: Skip CT Comparison [XIU+21]



[XIU+21] Xagawa, Keita, Akira Ito, Rei Ueno, Junko Takahashi, and Naofumi Homma. "Fault-injection attacks against NIST's post-quantum cryptography round 3 KEM candidates." In *Advances in Cryptology–ASIACRYPT 2021: 27th International Conference on the Theory and Application of Cryptology and Information Security, Singapore, December 6–10, 2021, Proceedings, Part II 27*, pp. 33-61. Springer International Publishing, 2021.

FIA on Decapsulation: Skip CT Comparison [XIU+21]

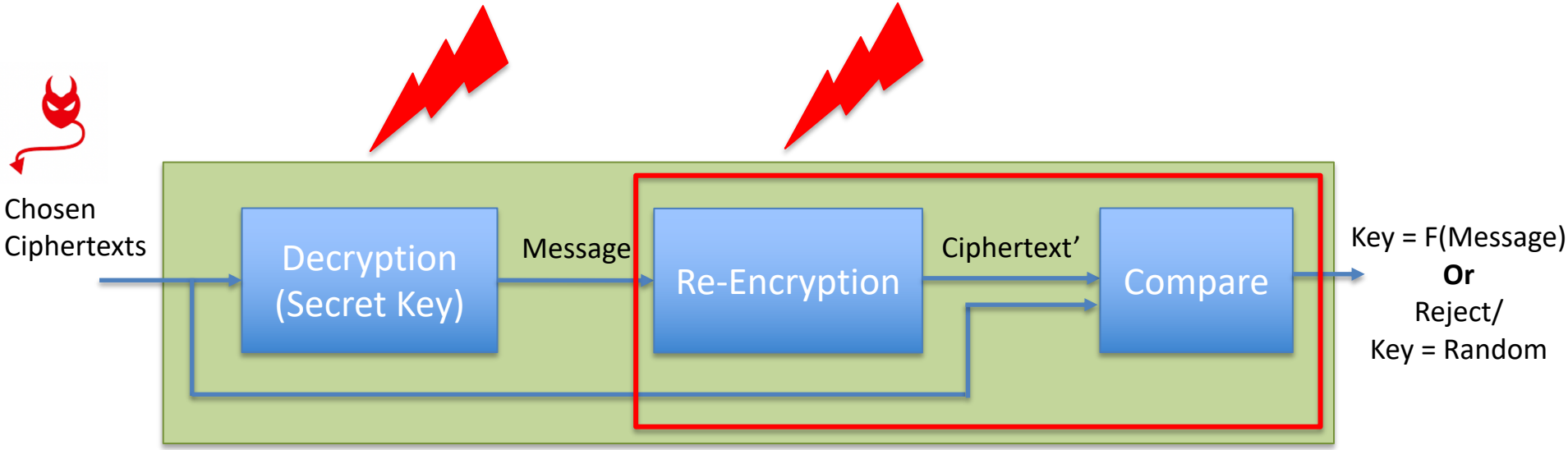


[XIU+21] Xagawa, Keita, Akira Ito, Rei Ueno, Junko Takahashi, and Naofumi Homma. "Fault-injection attacks against NIST's post-quantum cryptography round 3 KEM candidates." In *Advances in Cryptology–ASIACRYPT 2021: 27th International Conference on the Theory and Application of Cryptology and Information Security, Singapore, December 6–10, 2021, Proceedings, Part II 27*, pp. 33-61. Springer International Publishing, 2021.

FIA on Kyber Decaps: Summary

Attack Name	DUT_IO_Access	Type of Fault	Targeted_ or_Not	No. of Faults within Single Computation	Total No. of Faulty Computations	Countermeasure
Skip_CT_ Compare	Communicate_DUT _IO	Control	Targeted	1	Few thousand.	Protected Conditional Move

FIA on Decapsulation: Fault Assisted CCA [PP21,HPP21,D22]



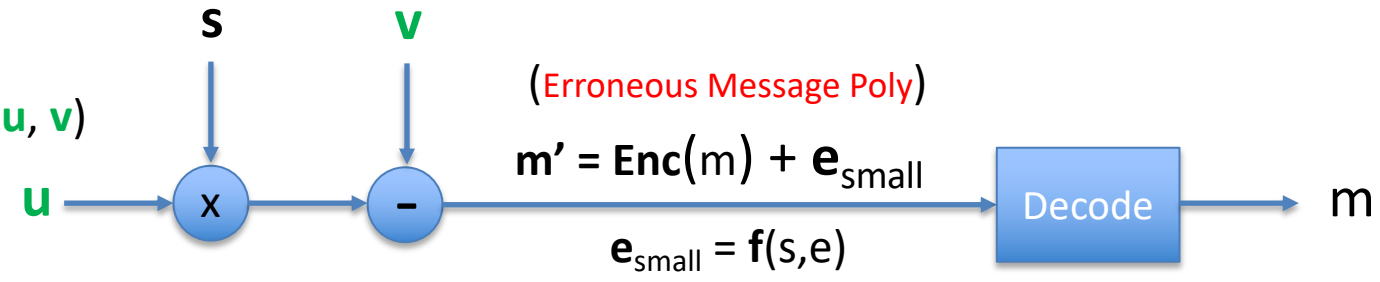
Modus Operandi: Inject Faults to realize a Decryption Failure (DF) Oracle

[PP21] Pessl, Peter, and Lukas Prokop. "Fault attacks on CCA-secure lattice KEMs." *IACR Transactions on Cryptographic Hardware and Embedded Systems* (2021): 37-60.
[HPP21] Hermelink, Julius, Peter Pessl, and Thomas Pöppelmann. "Fault-enabled chosen-ciphertext attacks on Kyber." In *Progress in Cryptology–INDOCRYPT 2021: 22nd International Conference on Cryptology in India, Jaipur, India, December 12–15, 2021, Proceedings 22*, pp. 311-334. Springer International Publishing, 2021.
[D22] Delvaux, Jeroen. "Roulette: A Diverse Family of Feasible Fault Attacks on Masked Kyber." *IACR Transactions on Cryptographic Hardware and Embedded Systems* (2022)

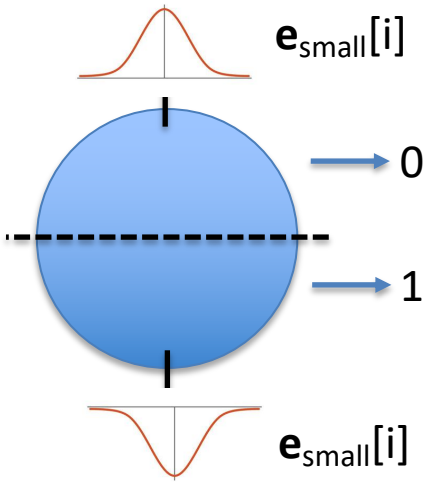
FIA on Decapsulation: Fault Assisted CCA [PP21,HPP21,D22]

Decryption

Chosen Ciphertext = (**u**, **v**)



Linear Relation



Knowledge of $\mathbf{e}_{small}[i] < 0$ or $\mathbf{e}_{small}[i] > 0$ for chosen-ciphertexts

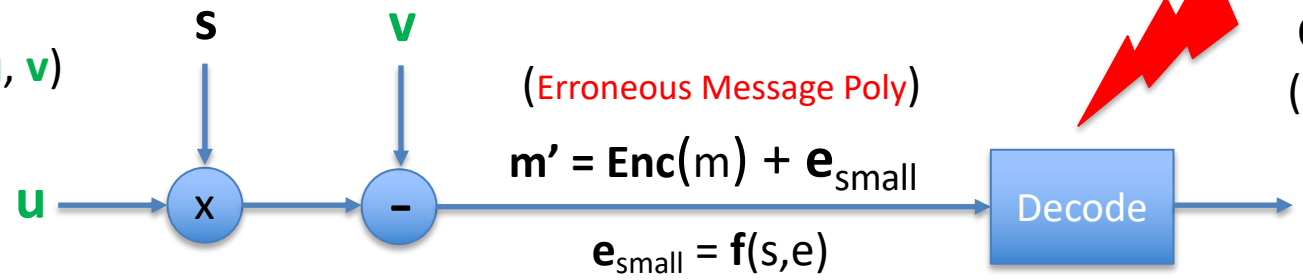
Modus Operandi:

Use faults to learn $\mathbf{e}_{small}[i] < 0$ or $\mathbf{e}_{small}[i] > 0$ for chosen-ciphertexts

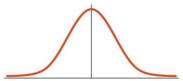
FIA on Decapsulation: Ineffective Fault Analysis [PP21]

Decryption

Ciphertext = (**u**, **v**)



Linear Relation

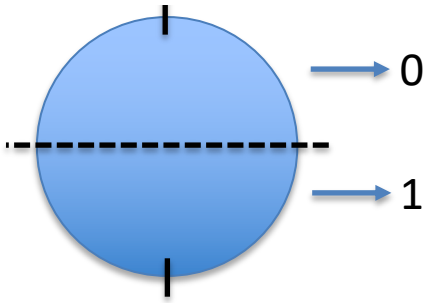


$\mathbf{e}_{small}[0] + \lfloor q/4 \rceil$

Effective Fault

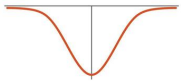
Bit Flip when $\mathbf{e}_{small}[0] < 0$
Decapsulation Failure

Can also tolerate error (1%)



Ineffective Fault

No Bit Flip when $\mathbf{e}_{small}[0] > 0$
Decapsulation Success



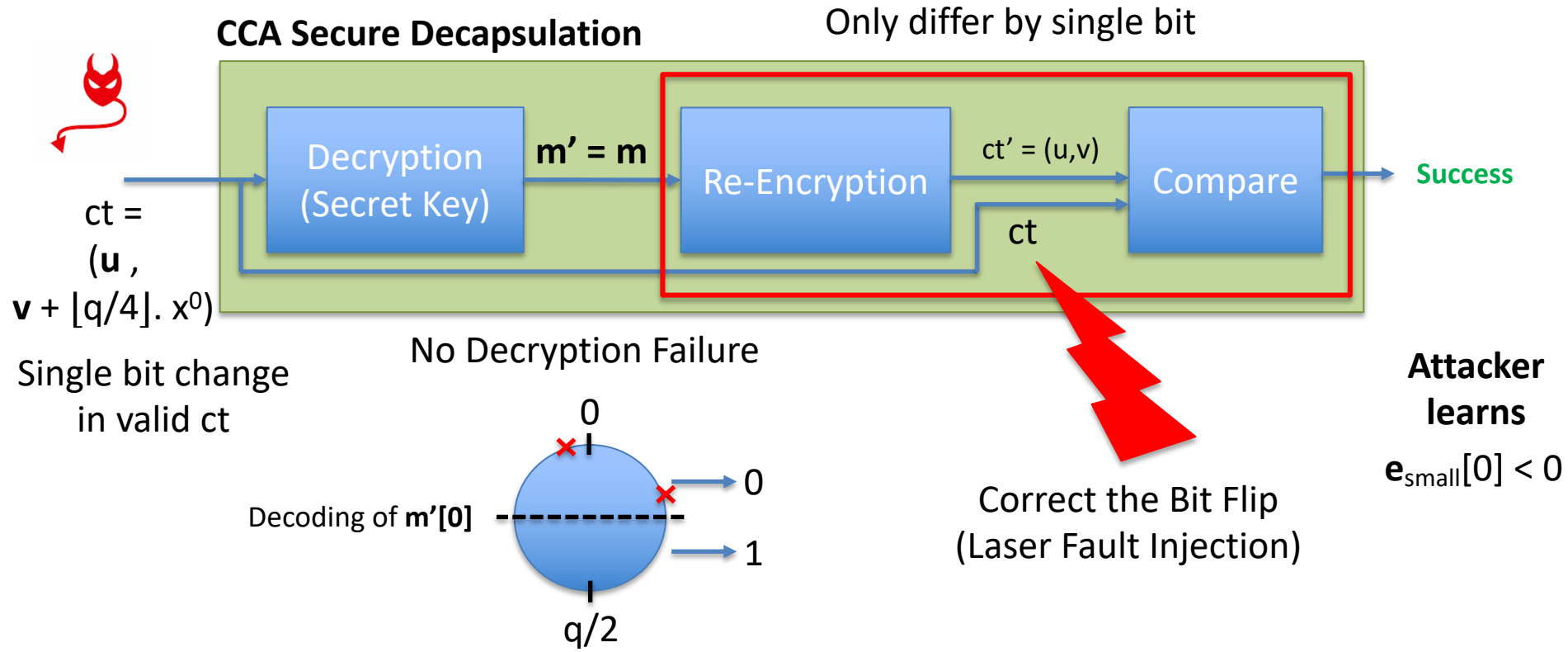
$\mathbf{e}_{small}[0] + \lfloor q/4 \rceil$

[PP21] Pessl, Peter, and Lukas Prokop. "Fault attacks on CCA-secure lattice KEMs." *IACR Transactions on Cryptographic Hardware and Embedded Systems* (2021): 37-60.

FIA on Kyber Decaps: Summary

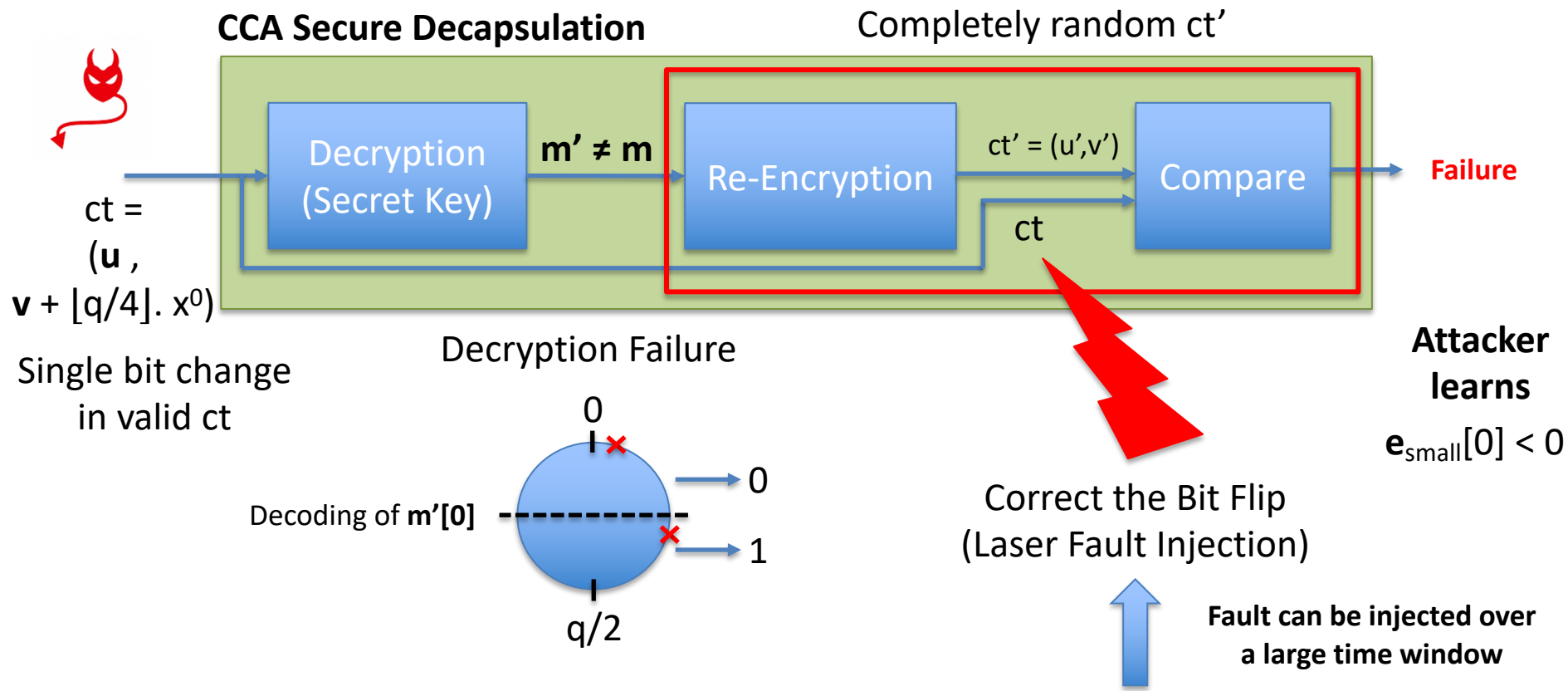
Attack Name	DUT_IO_Access	Type of Fault	Targeted_or_Not	No. of Faults within Single Computation	Total No. of Faulty Computations	Countermeasure
Skip_CT_Compare	Communicate_DUT_IO	Control	Targeted	1	Few thousands (1k-3k)	Protected Conditional Move
Ineffective_FIA	Communicate_DUT_IO	Control	Targeted	1	Few thousands (5k-7k)	Shuffle Message Decoding

FIA on Decapsulation: Fault Correction Attack [HPP21]



[HPP21] Hermelink, Julius, Peter Pessl, and Thomas Pöppelmann. "Fault-enabled chosen-ciphertext attacks on Kyber." In *Progress in Cryptology–INDOCRYPT 2021: 22nd International Conference on Cryptology in India, Jaipur, India, December 12–15, 2021, Proceedings 22*, pp. 311-334. Springer International Publishing, 2021.

FIA on Decapsulation: Fault Correction Attack [HPP21]



[HPP21] Hermelink, Julius, Peter Pessl, and Thomas Pöppelmann. "Fault-enabled chosen-ciphertext attacks on Kyber." In *Progress in Cryptology–INDOCRYPT 2021: 22nd International Conference on Cryptology in India, Jaipur, India, December 12–15, 2021, Proceedings 22*, pp. 311-334. Springer International Publishing, 2021.

FIA on Decapsulation: Fault Correction Attack [HPP21]

- Compute Hash of Ciphertext and Compare with Hash
  - Inject fault before ciphertext sent to hash function
  - Reduces Attack Surface, but does not prevent attack

- Attack of [HPP21] improved in Roulette Attack [D22]:
  - **Larger Attack Surface**:
    - Operations in Re-Encryption: Sampler, INTT
  - **Relaxed Fault Models**:
    - Set-to-0, random faults, arbitrary bit flips, instruction skips
  - **Allows larger errors:**
    - ≅ 25%

[D22] Delvaux, Jeroen. "Roulette: A Diverse Family of Feasible Fault Attacks on Masked Kyber." *IACR Transactions on Cryptographic Hardware and Embedded Systems* (2022)

FIA on Kyber Decaps: Summary

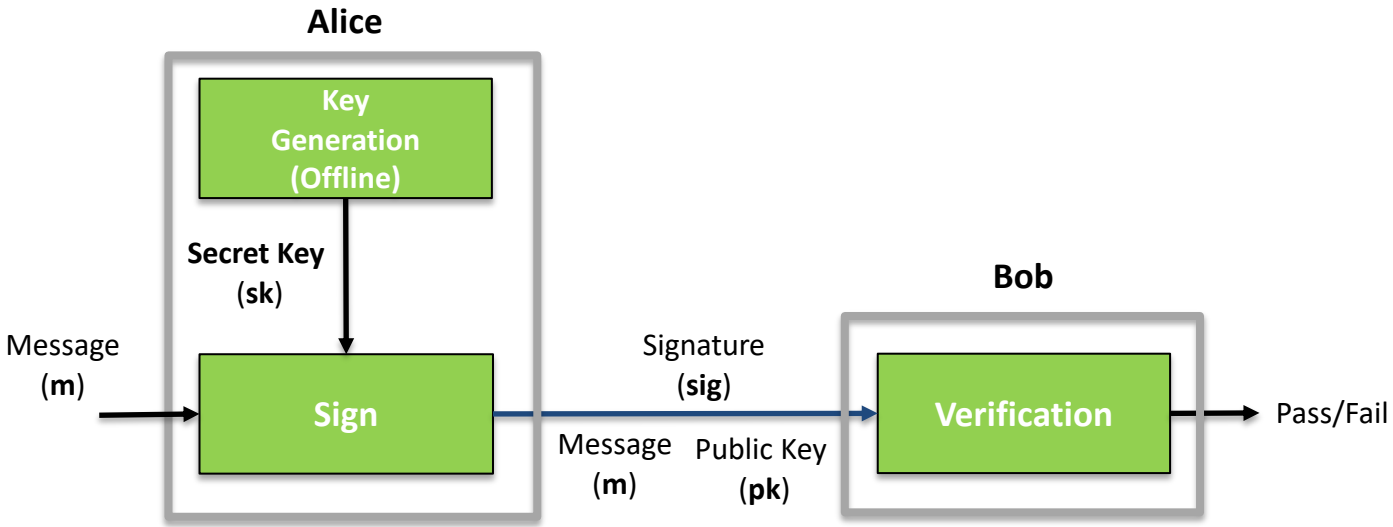
Attack Name	DUT_IO_Access	Type of Fault	Targeted_or_Not	No. of Faults within Single Computation	Total No. of Faulty Computations	Countermeasure
Skip_CT_ Compare	Communicate_DUT _IO	Control	Targeted	1	Few thousands (1k-3k)	Protected Conditional Move
Ineffective_FIA	Communicate_DUT _IO	Control	Targeted	1	Few thousands (5k-7k)	Shuffle Message Decoding
Fault_Correction _Attack_1	Communicate_DUT _IO	Control	Targeted (Bit Flip)	1	Few thousands (5k-7k)	Redundancy
Fault_Correction _Attack_2	Communicate_DUT _IO	Control	Targeted (More Relaxed Fault Models)	1	Few tens-hundred thousands (10k-100k)	Redundancy

Open Research Directions: Development of Algorithmic Countermeasures against fault assisted DF oracle attacks

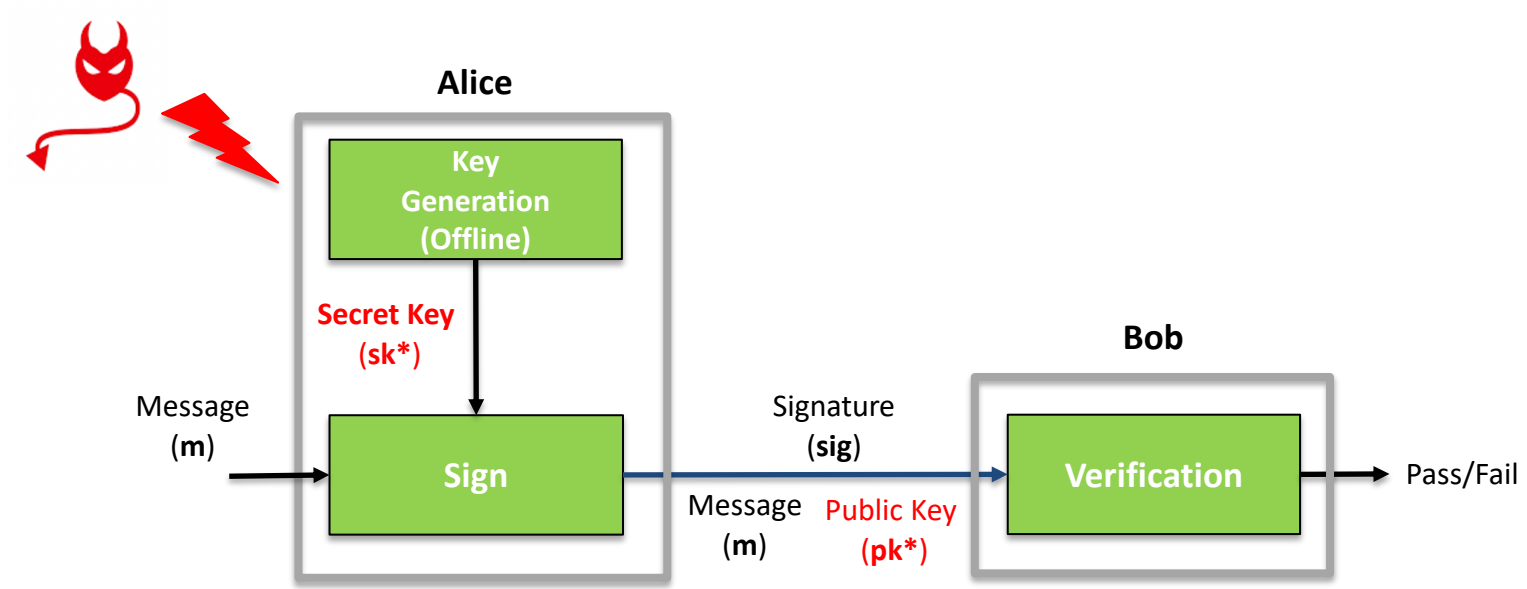
Outline

- ❑ FIA on Kyber:
  - ❑ FIA on Key Generation
  - ❑ FIA on Decapsulation
- ❑ **FIA on Dilithium**
  - ❑ **FIA on Signing**
  - ❑ **FIA on Verification**
- ❑ Conclusion

Signature Scheme: Background

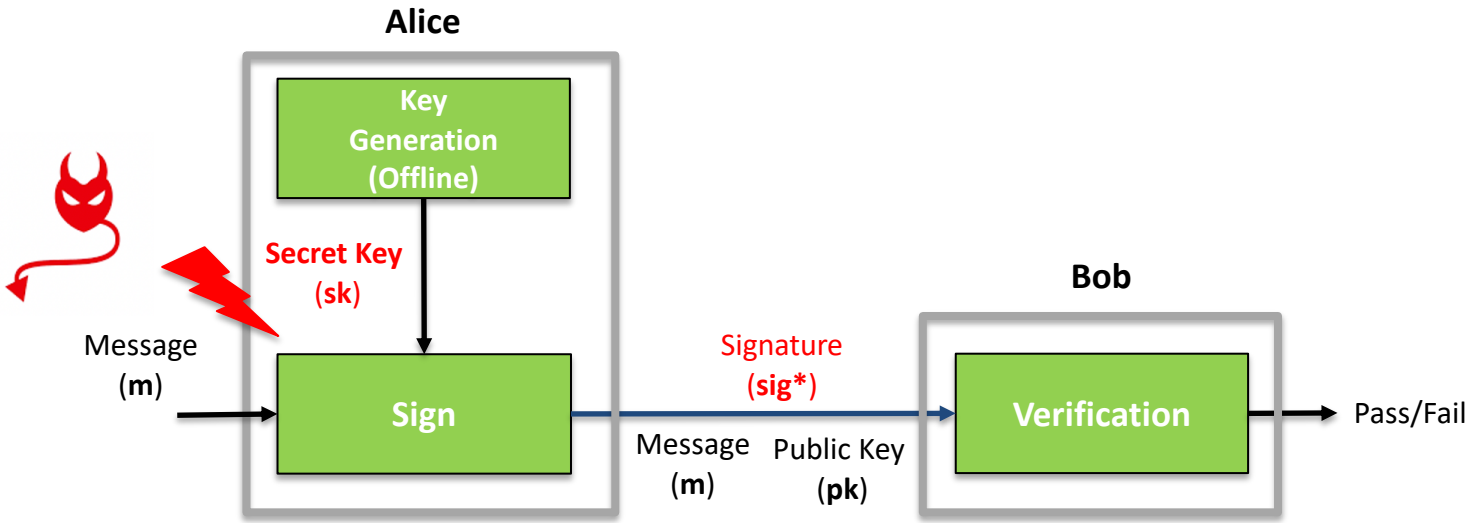


Signature Scheme: Attacking Alice



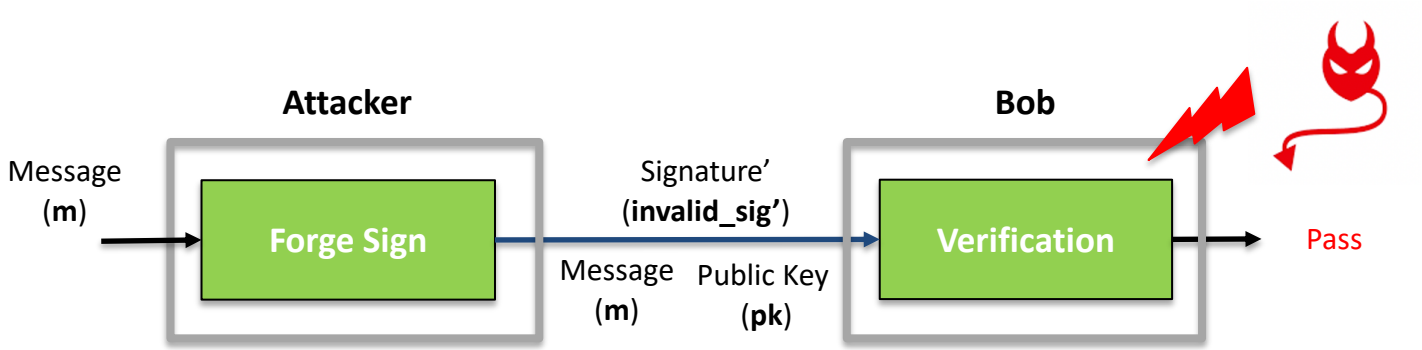
- Single execution to target Key Generation: Key Recovery Attack
  - Recover Secret key from Faulty but valid Public Key
  - But, key generation mostly done offline (PKI Infrastructure)

Signature Scheme: Attacking Alice



- Multiple Executions to target Signing Procedure:
  - Single/Multiple faulty signatures used to recover secret key
  - Most attractive target for attacker

Signature Scheme: Attacking Bob

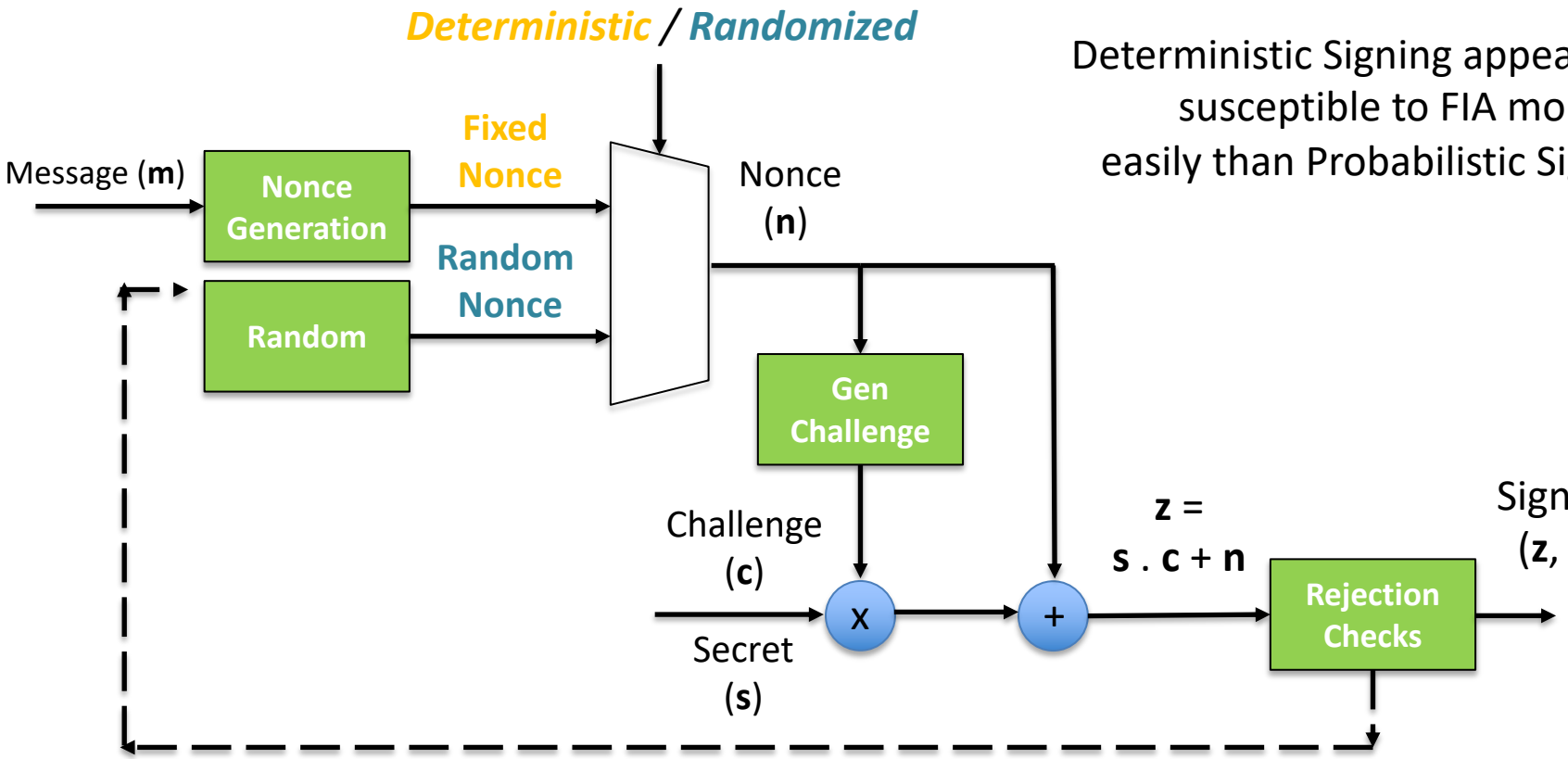


- Single Execution to bypass Signature Verification:
  - Application: Secure Boot

Outline

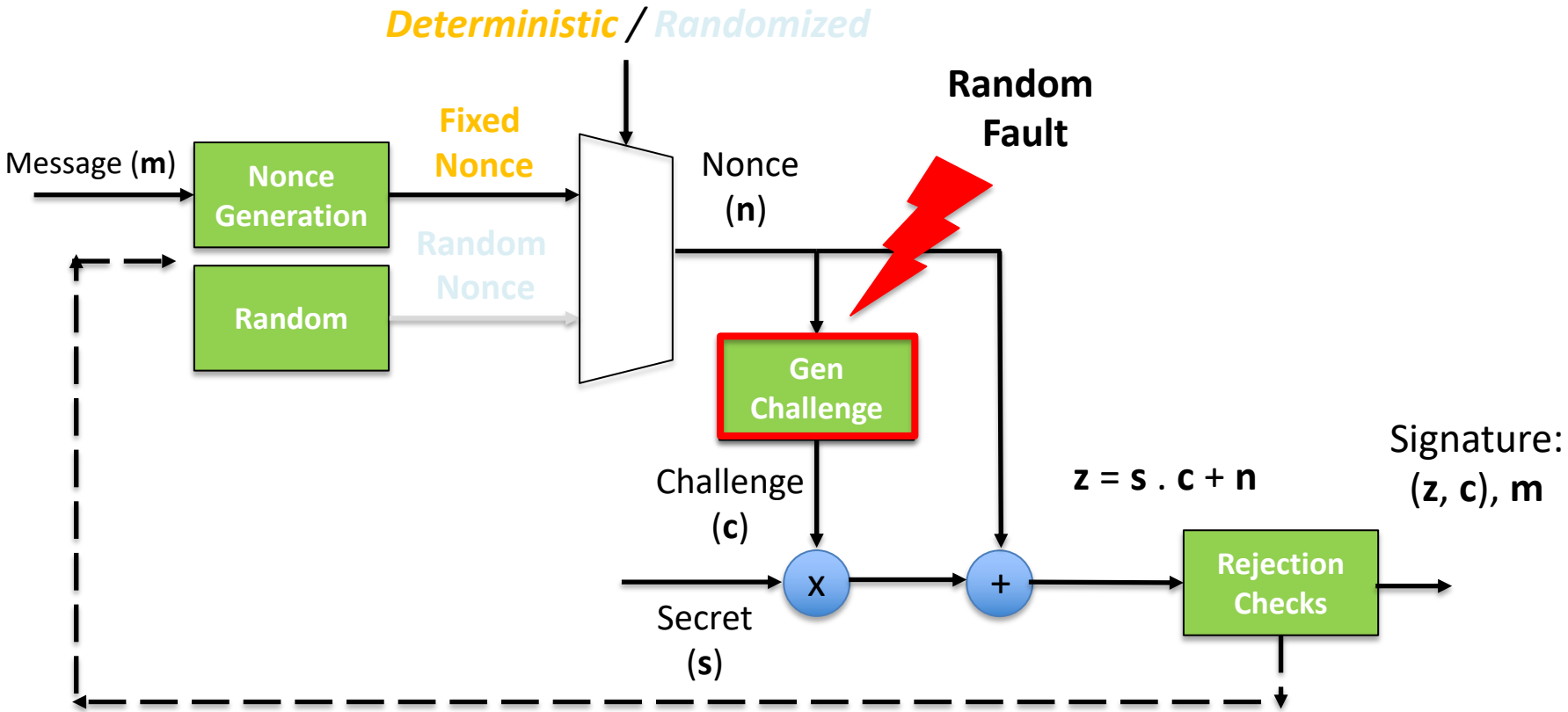
- ❑ FIA on Kyber:
  - ❑ FIA on Key Generation
  - ❑ FIA on Decapsulation
- ❑ **FIA on Dilithium**
  - ❑ **FIA on Signing**
  - ❑ FIA on Verification
- ❑ Conclusion

FIA on Signing Procedure: Background



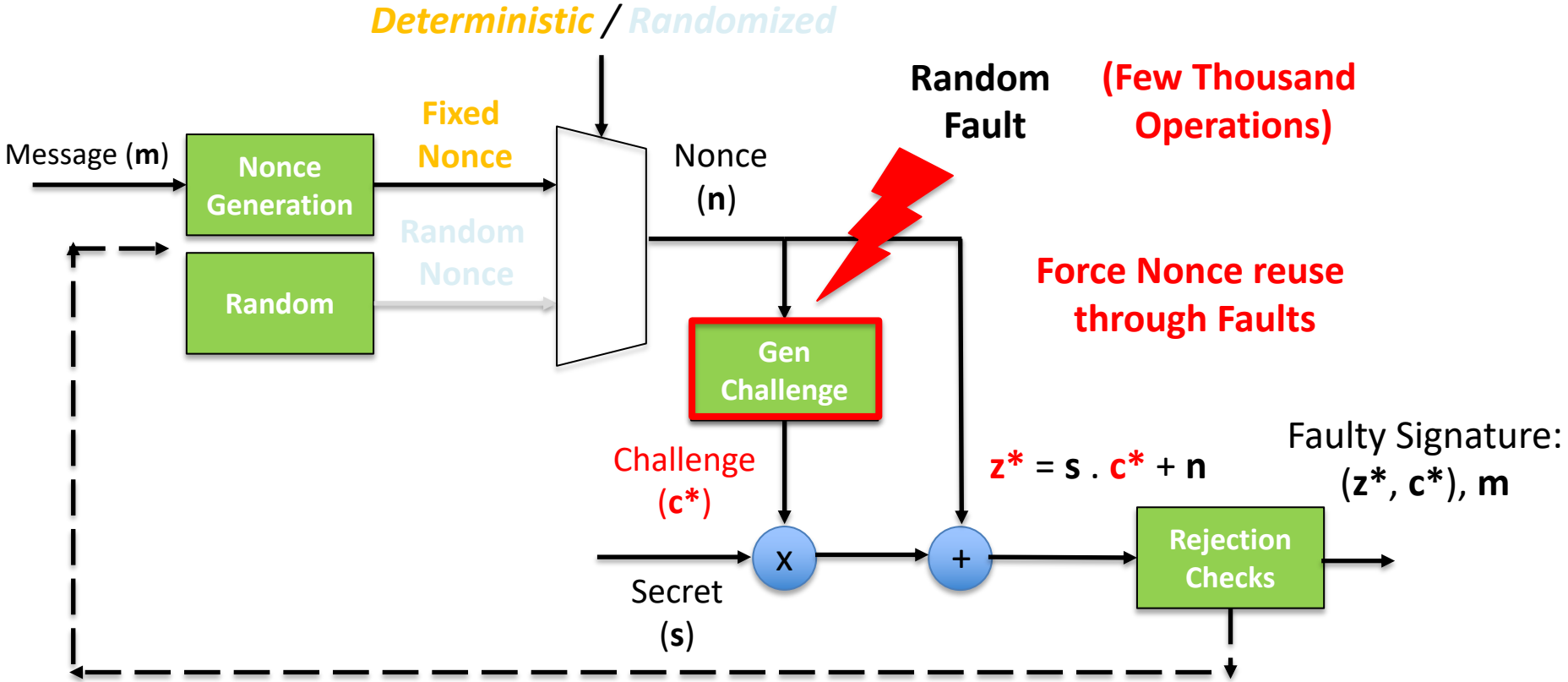
Deterministic Signing appears to be susceptible to FIA more easily than Probabilistic Signing!

FIA on Signing Procedure: DFA (Deterministic) [BP18]



[BP18] Bruinderink, Leon Groot, and Peter Pessl. "Differential fault attacks on deterministic lattice signatures." *IACR Transactions on Cryptographic Hardware and Embedded Systems* (2018): 21-43.

FIA on Signing Procedure: DFA (Deterministic) [BP18]



[BP18] Bruinderink, Leon Groot, and Peter Pessl. "Differential fault attacks on deterministic lattice signatures." *IACR Transactions on Cryptographic Hardware and Embedded Systems* (2018): 21-43.

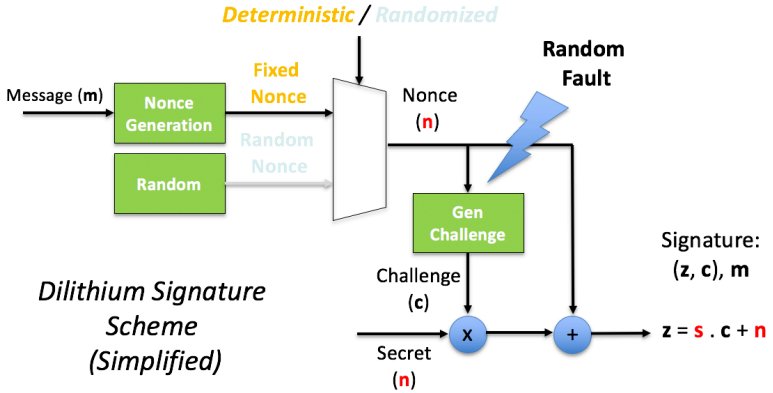
FIA on Signing Procedure: DFA (Deterministic) [BP18]

Valid Sig. **Faulty Sig.**

$z = s \cdot c + n$ $z^* = s \cdot c^* + n$

$(z - z^*) = s \cdot (c - c^*)$

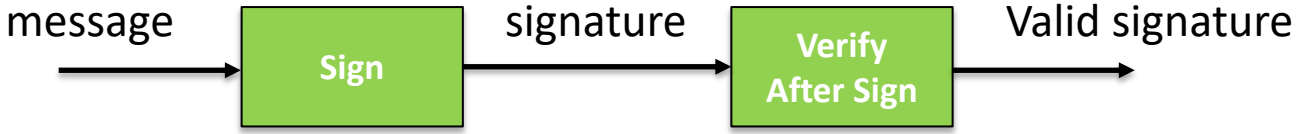
$s = (z - z^*).(c - c^*)^{-1}$



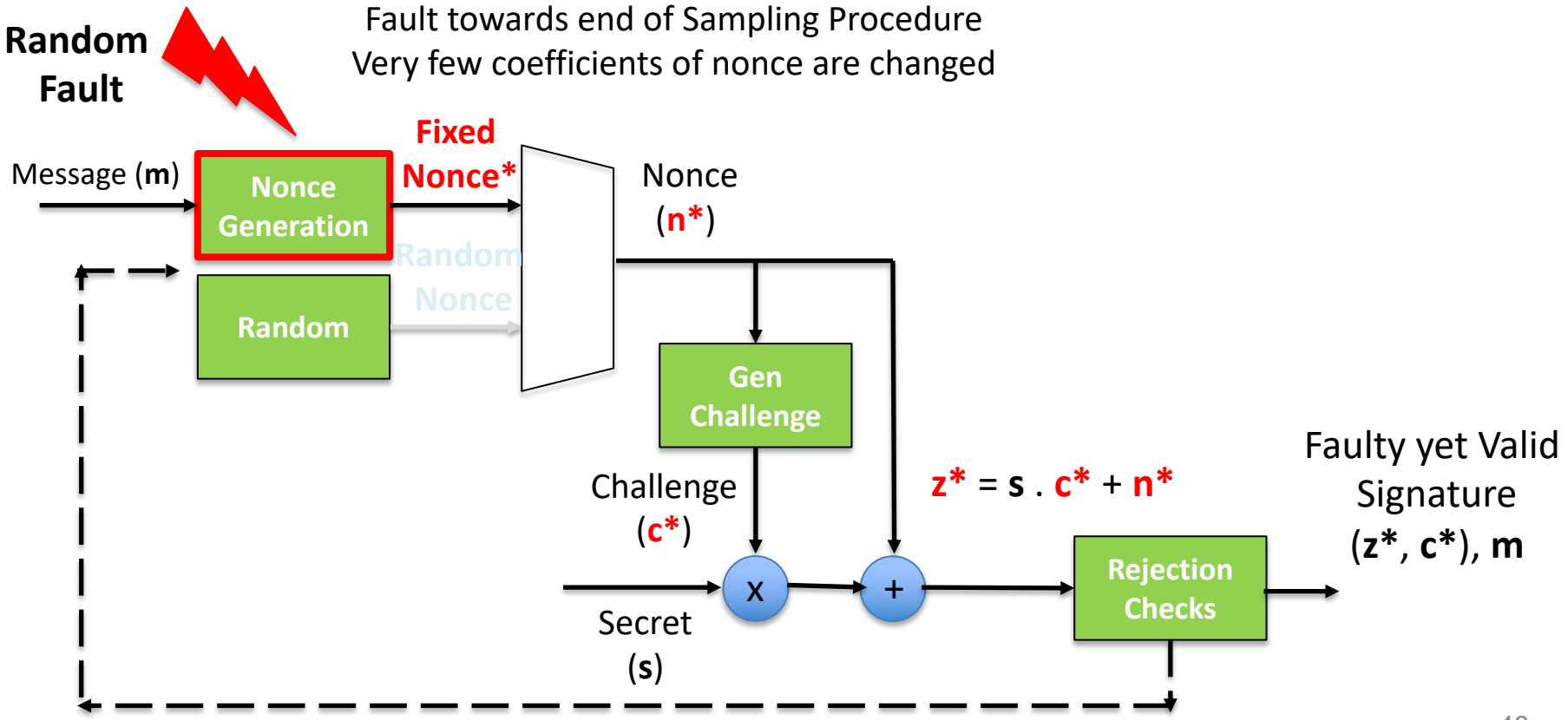
60% operations are vulnerable to DFA

Mitigation

Verify the generated Signatures

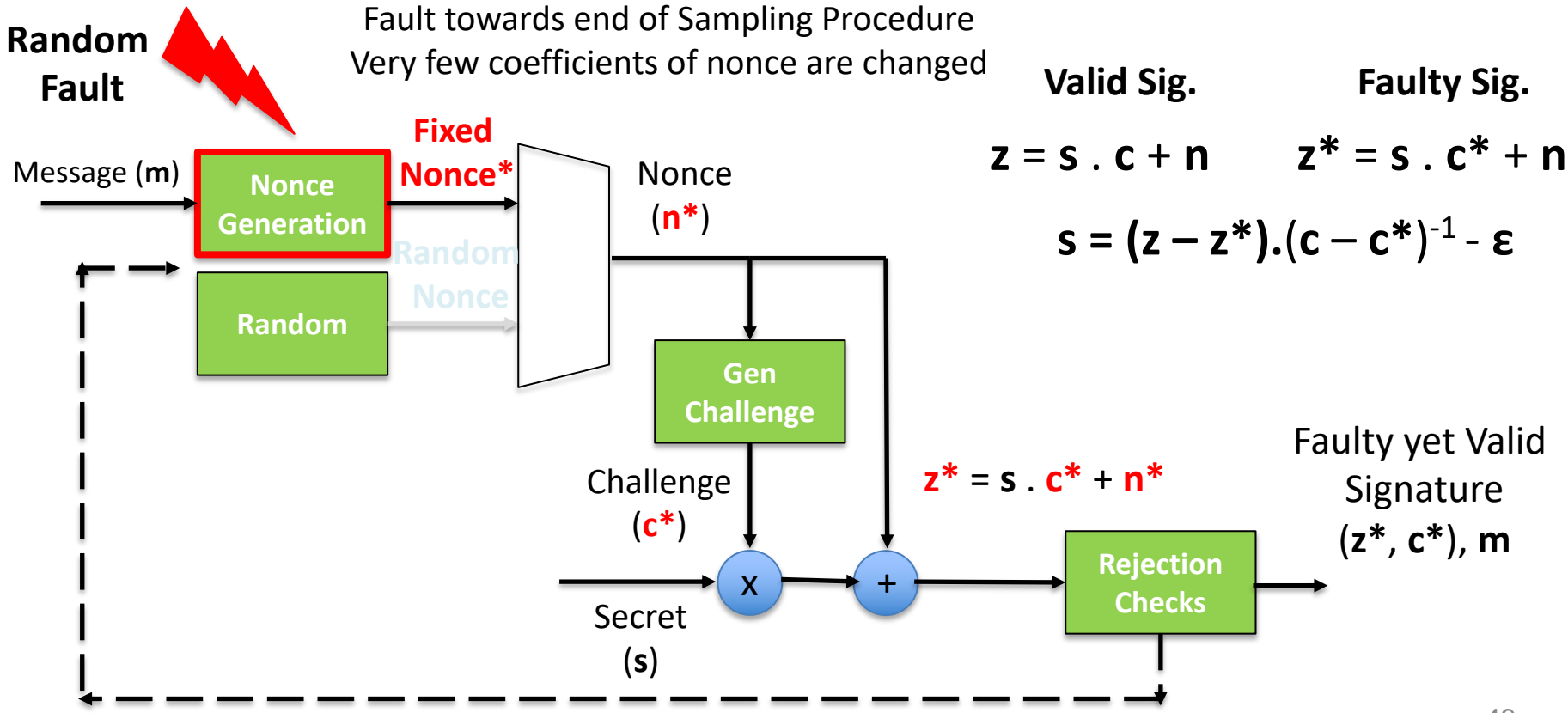


FIA on Signing Procedure: DFA (Deterministic) [BP18]



[BP18] Bruinderink, Leon Groot, and Peter Pessl. "Differential fault attacks on deterministic lattice signatures." *IACR Transactions on Cryptographic Hardware and Embedded Systems* (2018): 21-43.

FIA on Signing Procedure: DFA (Deterministic) [BP18]

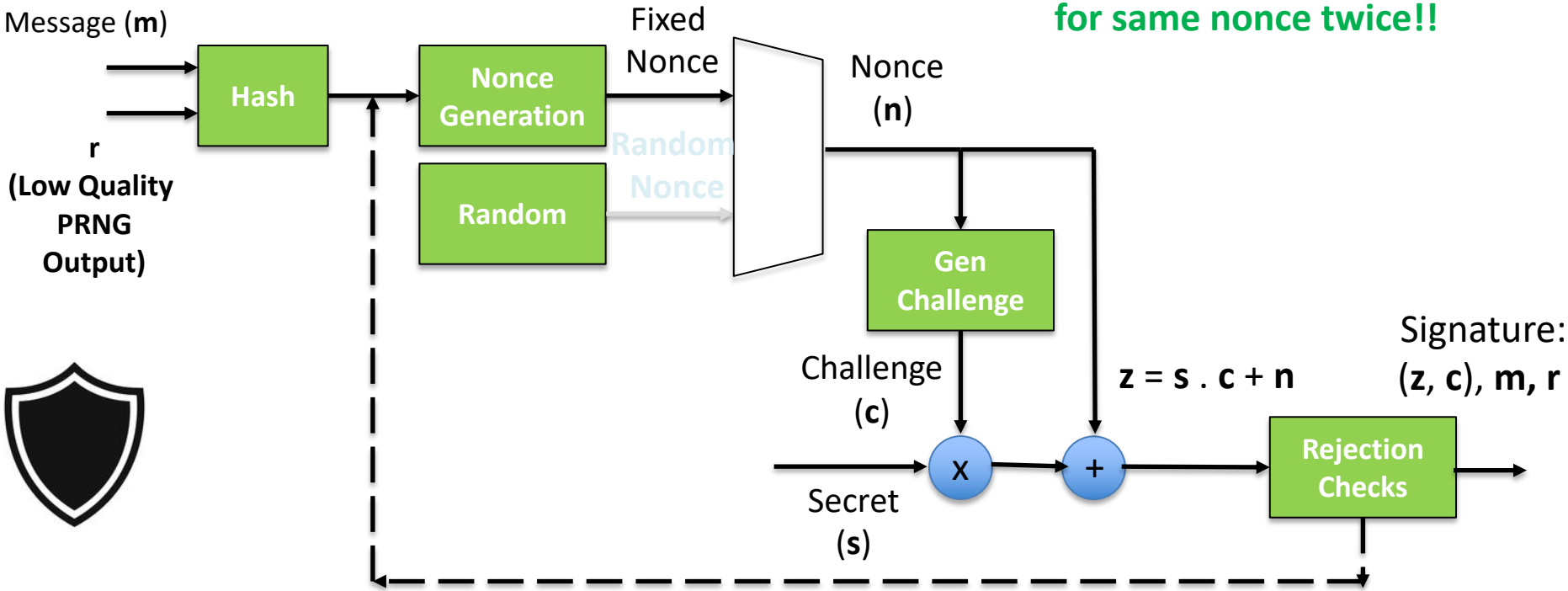


[BP18] Bruinderink, Leon Groot, and Peter Pessl. "Differential fault attacks on deterministic lattice signatures." *IACR Transactions on Cryptographic Hardware and Embedded Systems* (2018): 21-43.

FIA on Signing Procedure: DFA (Deterministic)

New Proposal (This Talk):

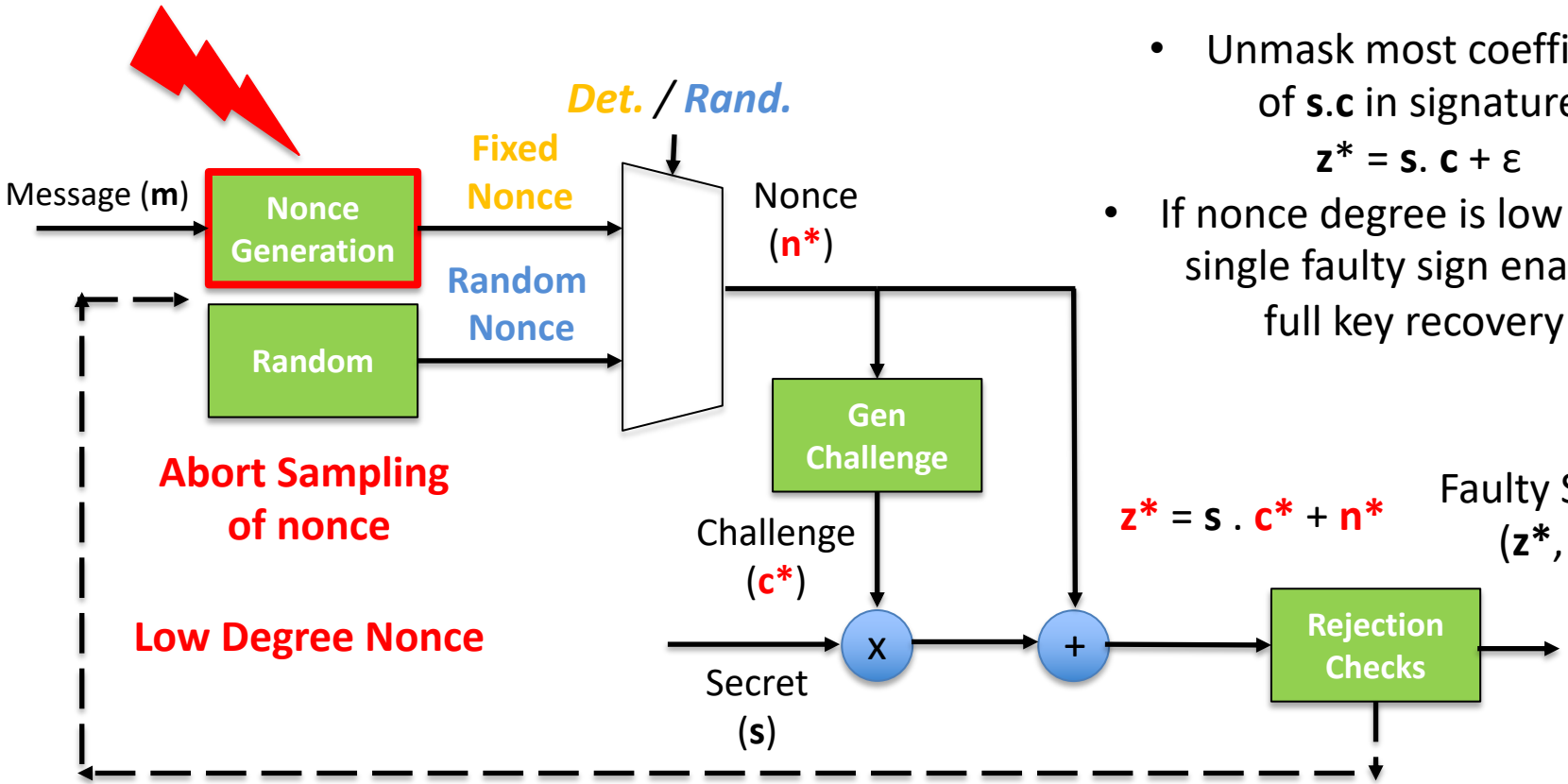
Attacker does not observe signatures for same nonce twice!!



FIA on Dilithium Signing: Summary

Attack Name	DUT_IO_Access	Type of Fault	Targeted_or_Not	No. of Faults within Single Computation	Total No. of Faulty Computations	Countermeasure
Generic_DFA	Communicate_DUT_IO	Data/ Control	Non_Targeted	1	1	Verify_after_Sign Redundancy (Nonce Sample)

FIA on Signing Procedure: Loop Abort Fault [EFG+18]



- Unmask most coefficients of **s.c** in signature
  $\mathbf{z}^* = \mathbf{s}.\mathbf{c} + \varepsilon$
- If nonce degree is low enough, single faulty sign enables full key recovery

[EFG+18] Espitau, Thomas, Pierre-Alain Fouque, Benoît Gérard, and Mehdi Tibouchi. "Loop-abort faults on lattice-based fiat-shamir and hash-and-sign signatures." In *Selected Areas in Cryptography–SAC 2016: 23rd International Conference, St. John's, NL, Canada, August 10-12, 2016, Revised Selected Papers 23*, pp. 140-158. Springer International Publishing, 2017.

FIA on Signing Procedure: Loop Abort Fault [EFG+18]

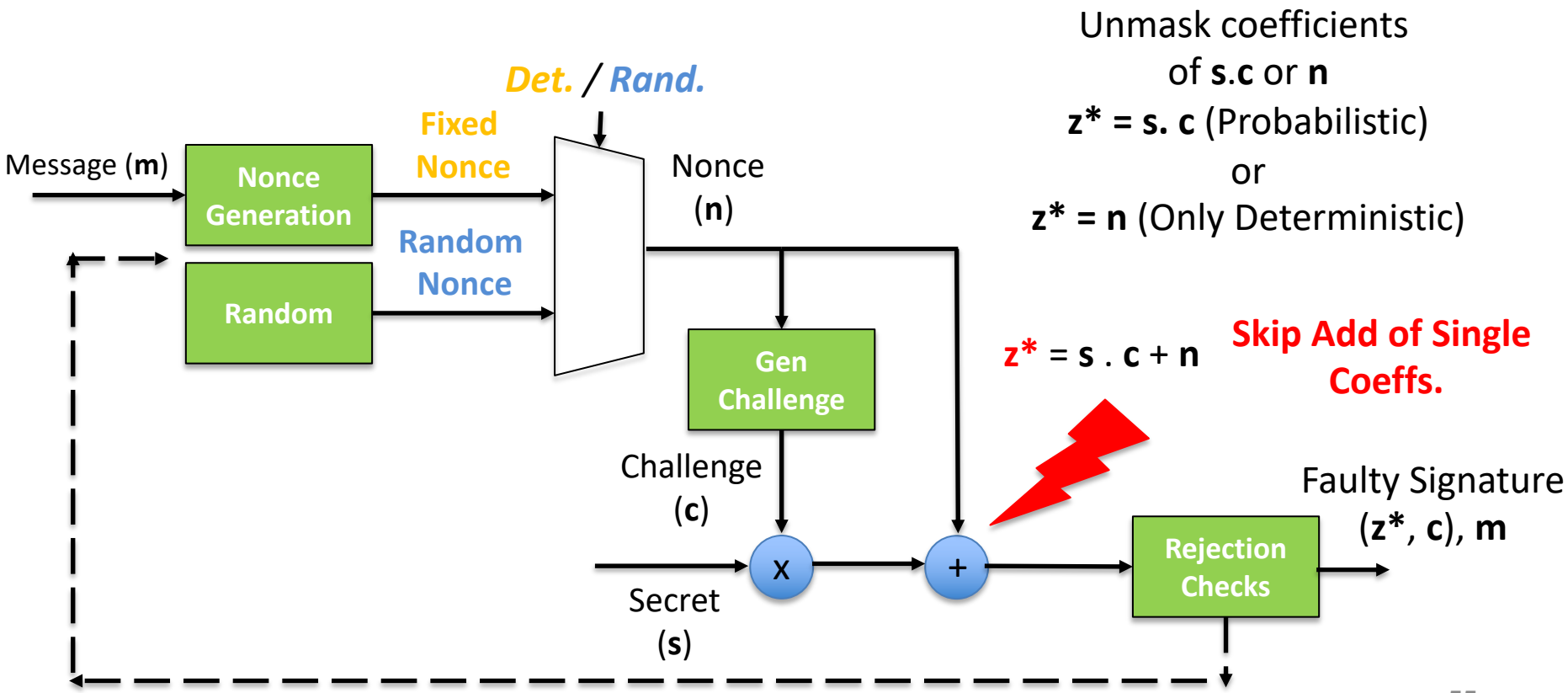
- Initializing nonce to random values and then sample
- Sanity Check of Nonce
  - Check for high number of zeros
  - Entropy Check

[EFG+18] Espitau, Thomas, Pierre-Alain Fouque, Benoît Gérard, and Mehdi Tibouchi. "Loop-abort faults on lattice-based fiat-shamir and hash-and-sign signatures." In *Selected Areas in Cryptography–SAC 2016: 23rd International Conference, St. John's, NL, Canada, August 10-12, 2016, Revised Selected Papers 23*, pp. 140-158. Springer International Publishing, 2017.

FIA on Dilithium Signing: Summary

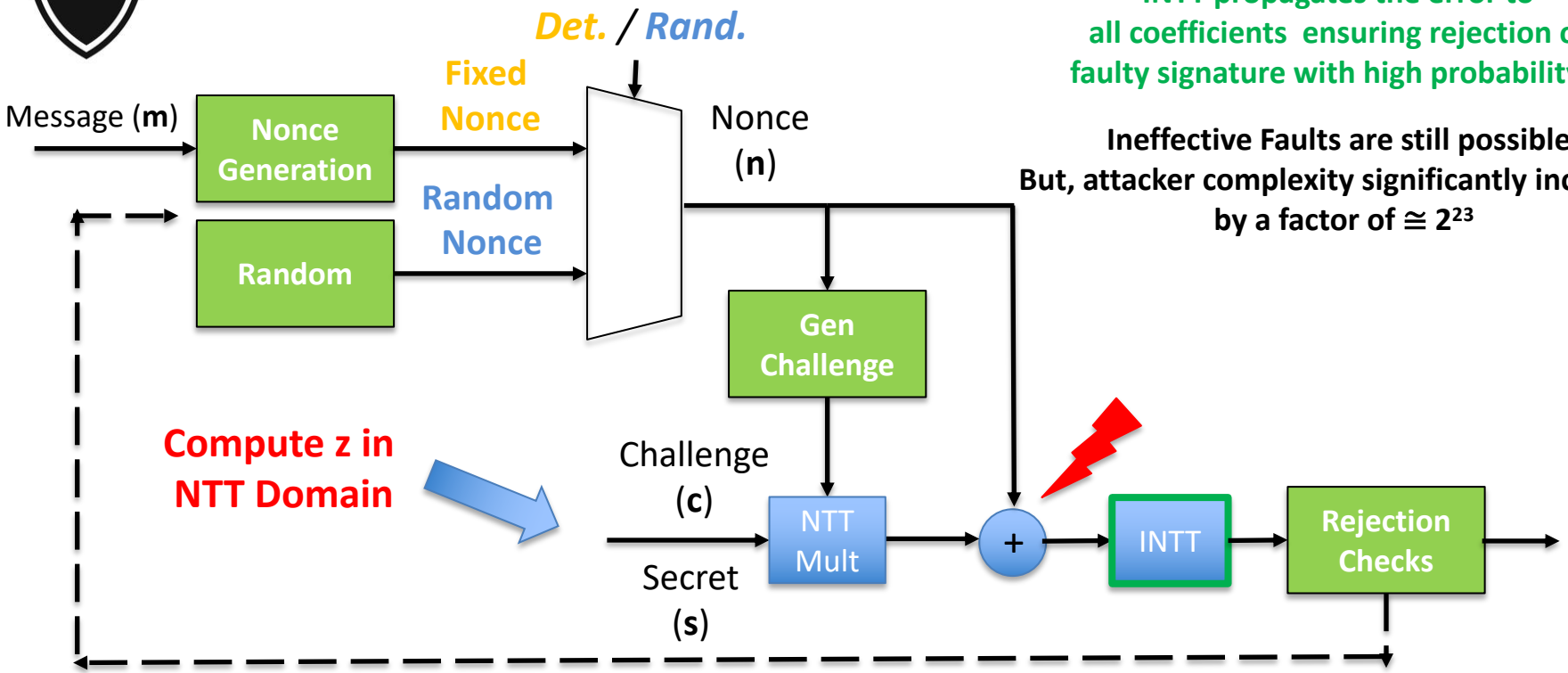
Attack Name	DUT_IO_Access	Type of Fault	Targeted_or_Not	No. of Faults within Single Computation	Total No. of Faulty Computations	Countermeasure
Generic_DFA	Communicate_DUT_IO	Data/ Control	Non_Targeted	1	1	Verify_after_Sign Redundancy (Nonce Sample)
Loop_Abort	Observe_DUT_IO	Control	Targeted	1	1	Redundancy (Nonce Sample) Sanity Check on Nonce Random Initialization

FIA on Signing Procedure: Skip Addition [RJH+19]



[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.

FIA on Signing Procedure: Skip Addition [RJH+19]



INTT propagates the error to all coefficients ensuring rejection of faulty signature with high probability!!!

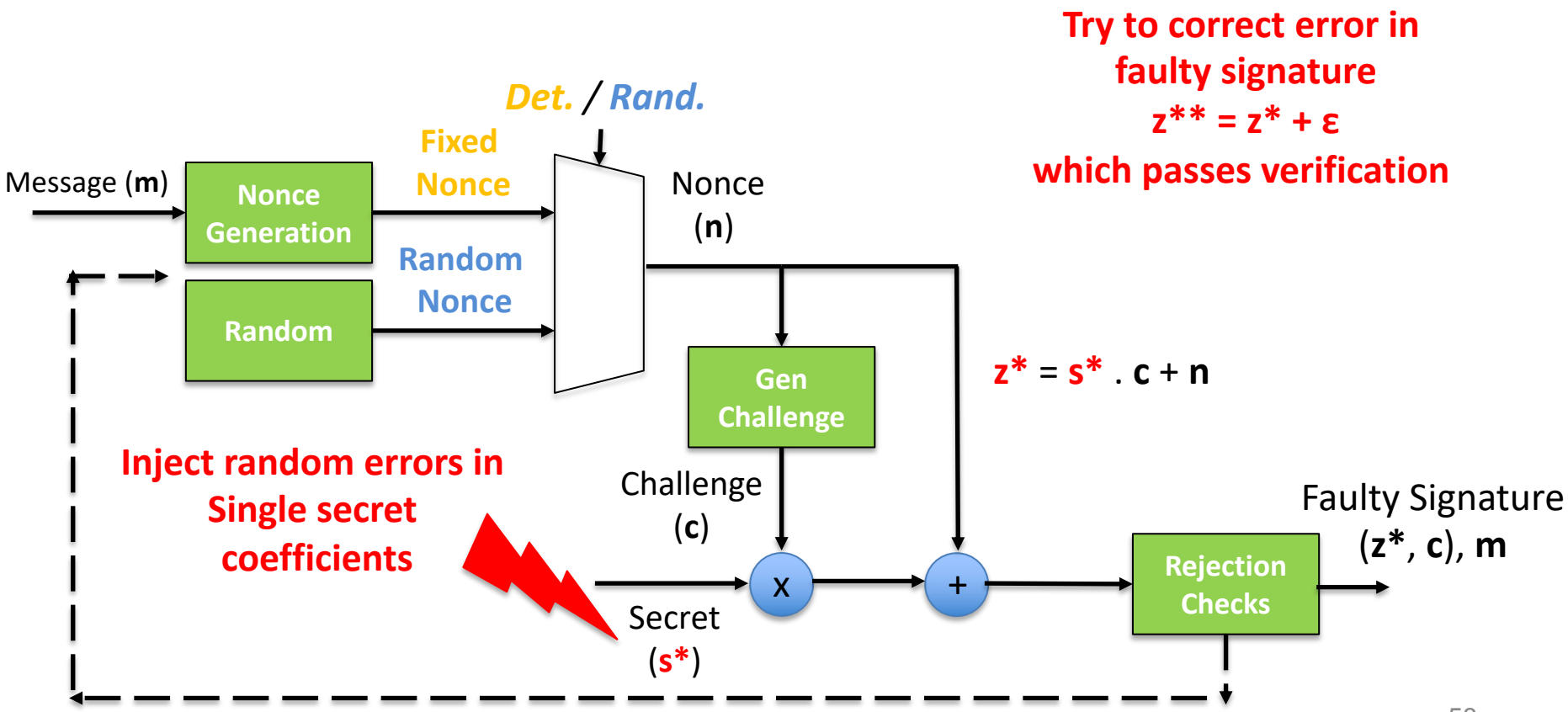
Ineffective Faults are still possible!
But, attacker complexity significantly increases by a factor of $\cong 2^{23}$

[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.

FIA on Dilithium Signing: Summary

Attack Name	DUT_IO_Access	Type of Fault	Targeted_or_Not	No. of Faults within Single Computation	Total No. of Faulty Computations	Countermeasure
Generic_DFA	Communicate_DUT_IO	Data/ Control	Non_Targeted	1	1	Verify_after_Sign Redundancy (Nonce Sample)
Loop_Abort	Observe_DUT_IO	Control	Targeted	1	1	Redundancy (Nonce Sample) Sanity Check on Nonce Random Initialization
Skip_Addition	Communicate_DUT_IO/Observe_DUT_IO	Data/ Control	Targeted	1	Few thousand	Verify After Sign Redundancy (Final Addition) NTT Addition

FIA on Signing Procedure: Erroneous Secret Key [IMS+22]

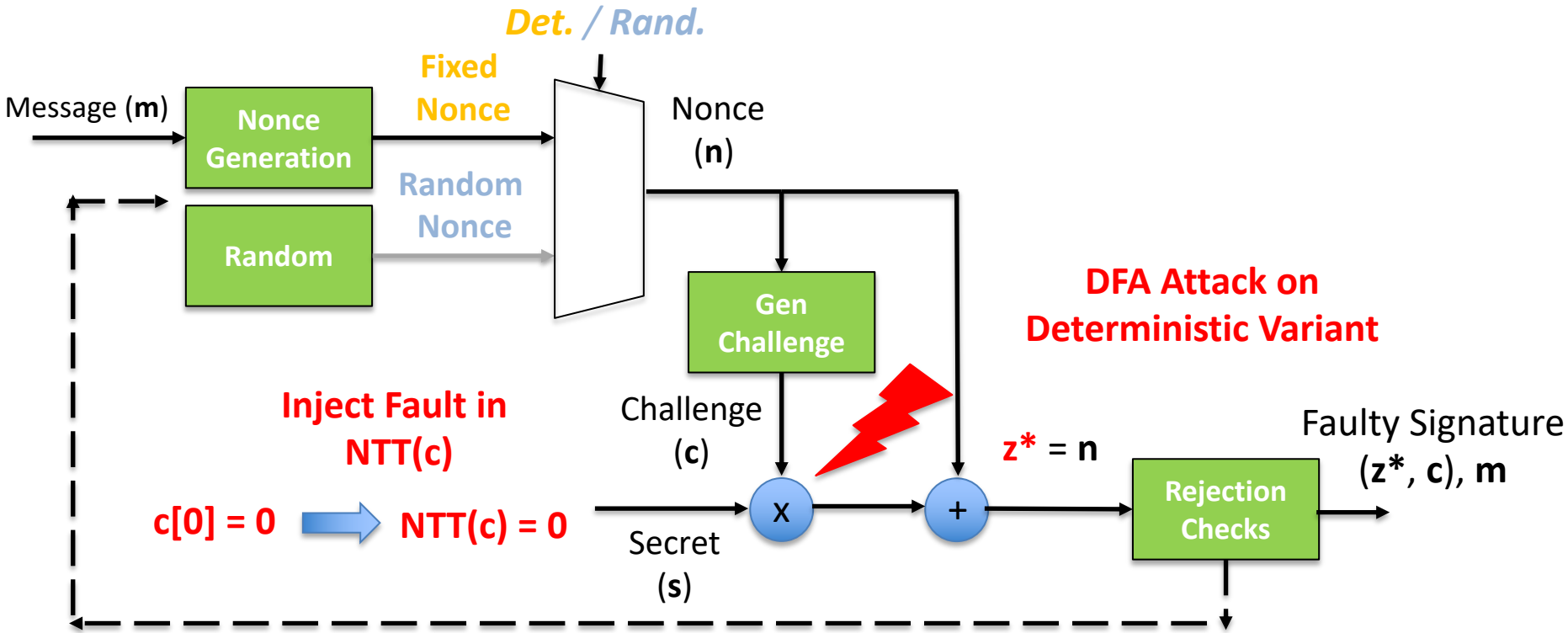


[IMS+22] Islam, Saad, Koksal Mus, Richa Singh, Patrick Schaumont, and Berk Sunar. "Signature Correction Attack on Dilithium Signature Scheme." In *2022 IEEE 7th European Symposium on Security and Privacy (EuroS&P)*, pp. 647-663. IEEE, 2022.

FIA on Dilithium Signing: Summary

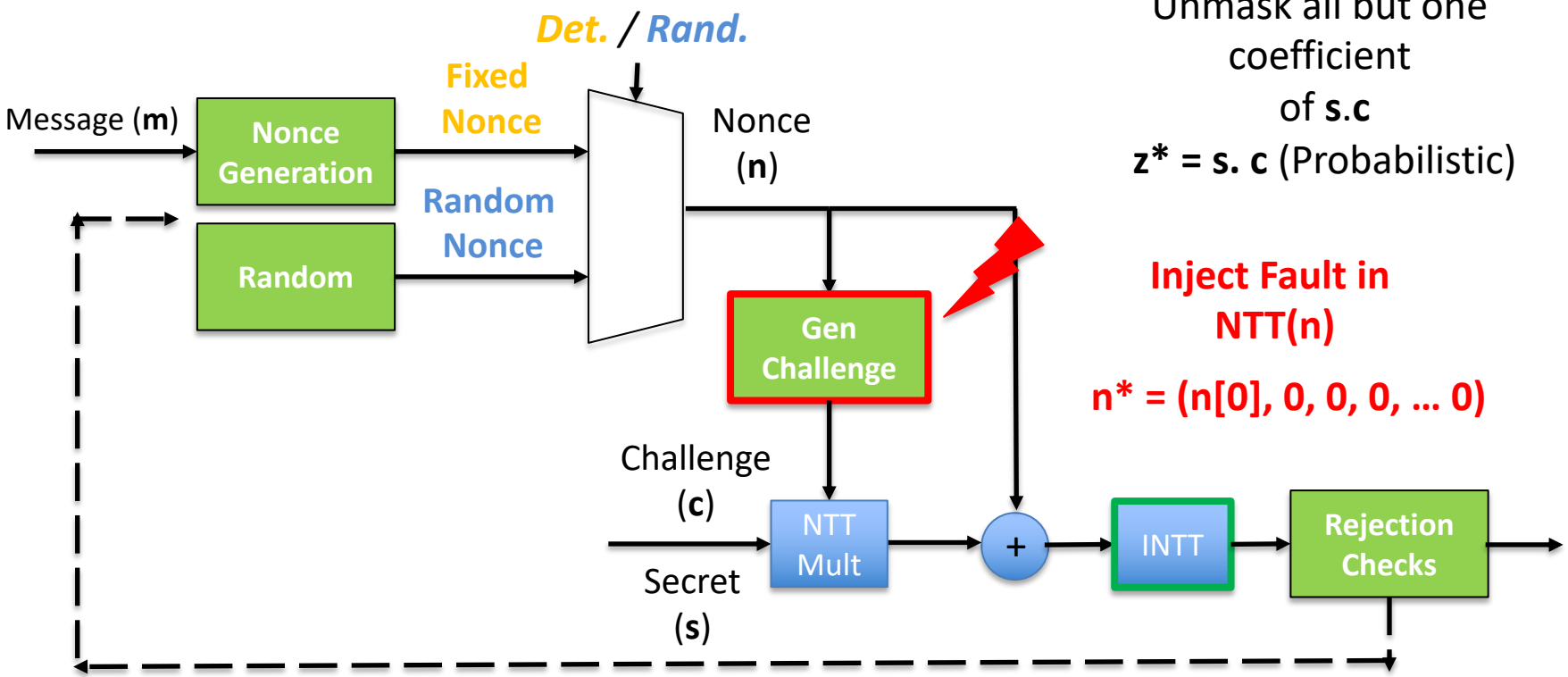
Attack Name	DUT_IO_Access	Type of Fault	Targeted_or_Not	No. of Faults within Single Computation	Total No. of Faulty Computations	Countermeasure
Generic_DFA	Communicate_DUT_IO	Data/ Control	Non_Targeted	1	1	Verify_after_Sign Redundancy (Nonce Sample)
Loop_Abort	Observe_DUT_IO	Control	Targeted	1	1	Redundancy (Nonce Sample) Sanity Check on Nonce Random Initialization
Skip_Addition	Communicate_DUT_IO/Observe_DUT_IO	Data/ Control	Targeted	1	Few thousand	Verify After Sign Redundancy (Final Addition) NTT Addition
Erroneous_ Secret_Key	Observe_DUT_IO	Data	Targeted	1	Few thousand	Verify After Sign

FIA on Signing Procedure: NTT Fault Attack [RYB+23]



[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.

FIA on Signing Procedure: NTT Fault Attack [RYB+23]



[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.

FIA on Dilithium Signing: Summary

Attack Name	DUT_IO_Access	Type of Fault	Targeted_or_Not	No. of Faults within Single Computation	Total No. of Faulty Computations	Countermeasure
Generic_DFA	Communicate_DUT_IO	Data/ Control	Non_Targeted	1	1	Verify_after_Sign Redundancy (Nonce Sample)
Loop_Abort	Observe_DUT_IO	Control	Targeted	1	1	Redundancy (Nonce Sample) Sanity Check on Nonce Random Initialization
Skip_Addition	Communicate_DUT_IO/Observe_DUT_IO	Data/ Control	Targeted	1	Few thousand	Verify After Sign Redundancy (Final Addition) NTT Addition
Erroneous_ Secret_Key	Observe_DUT_IO	Data	Targeted	1	Few thousand	Verify After Sign
NTT_Fault_ Attack	Communicate_DUT_IO/Observe_DUT_IO	Data	Targeted	1	1	Sanity Check on Twiddle Constants or NTT outputs

Outline

- ❑ FIA on Kyber:
  - ❑ FIA on Key Generation
  - ❑ FIA on Decapsulation
- ❑ **FIA on Dilithium**
  - ❑ FIA on Signing
  - ❑ **FIA on Verification**
- ❑ Conclusion

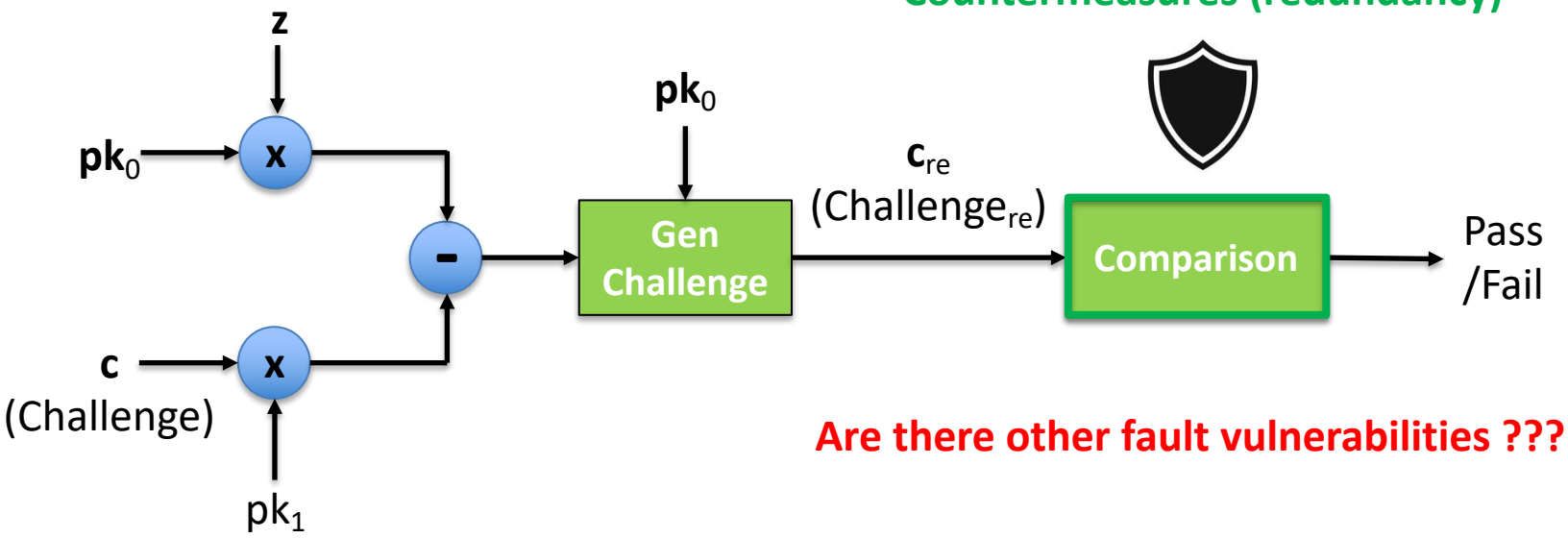
FIA on Verification Procedure

Signature: (z, c) , m

Public Key: (pk_0, pk_1)

Most Obvious Target

Can be fortified with known Countermeasures (redundancy)

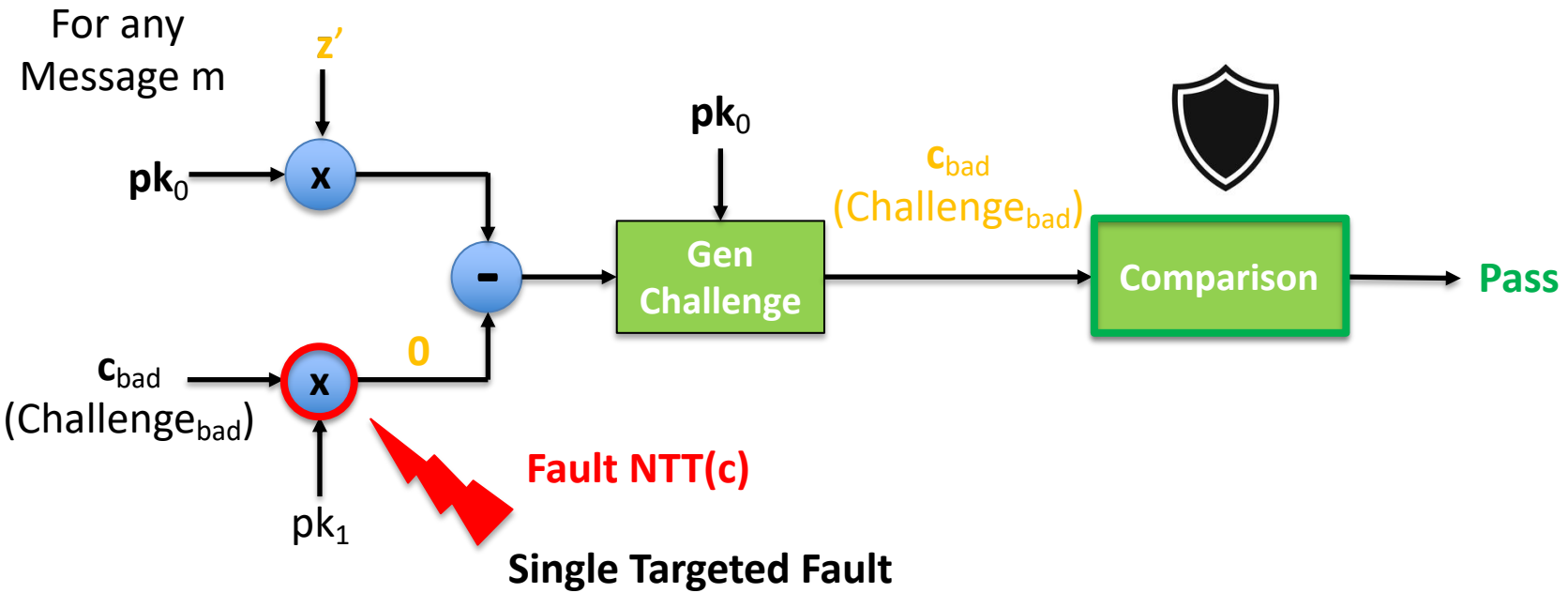


Are there other fault vulnerabilities ???

FIA on Verification: NTT Fault Attack [RYB+23]

Signature: (**z**, **c**) , **m**

Public Key: ($\mathbf{pk}_0$, $\mathbf{pk}_1$)



[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

- ❑ FIA on Kyber:
  - ❑ FIA on Key Generation
  - ❑ FIA on Decapsulation
- ❑ FIA on Dilithium
  - ❑ FIA on Signing
  - ❑ FIA on Verification
- ❑ **Conclusion and Open Questions**

Conclusion

- Variety of FIA are possible on unprotected Kyber and Dilithium
  - Non-Monolitic nature of scheme: Arithmetic Domain, Boolean Domain
- Underlying algorithmic features and implementation choices render them susceptible to SCA and FIA
- Questions:
  - Should we use dedicated countermeasures for every attack?
  - Can we exploit algorithmic features for efficient and low-cost countermeasures?
- Refer to [RDB+22] for a systematic study of SCA, FIA of Kyber and Dilithium (NIST PQC Standards)

[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).

"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!

Prasanna Ravi,
Temasek Labs, NTU Singapore

E-mail: prasanna.ravi@ntu.edu.sg
GitHub: https://github.com/PRASANNA-RAVI