SURVIVING THE FO-CALYPSE:

SECURING PQC IMPLEMENTATIONS IN PRACTICE

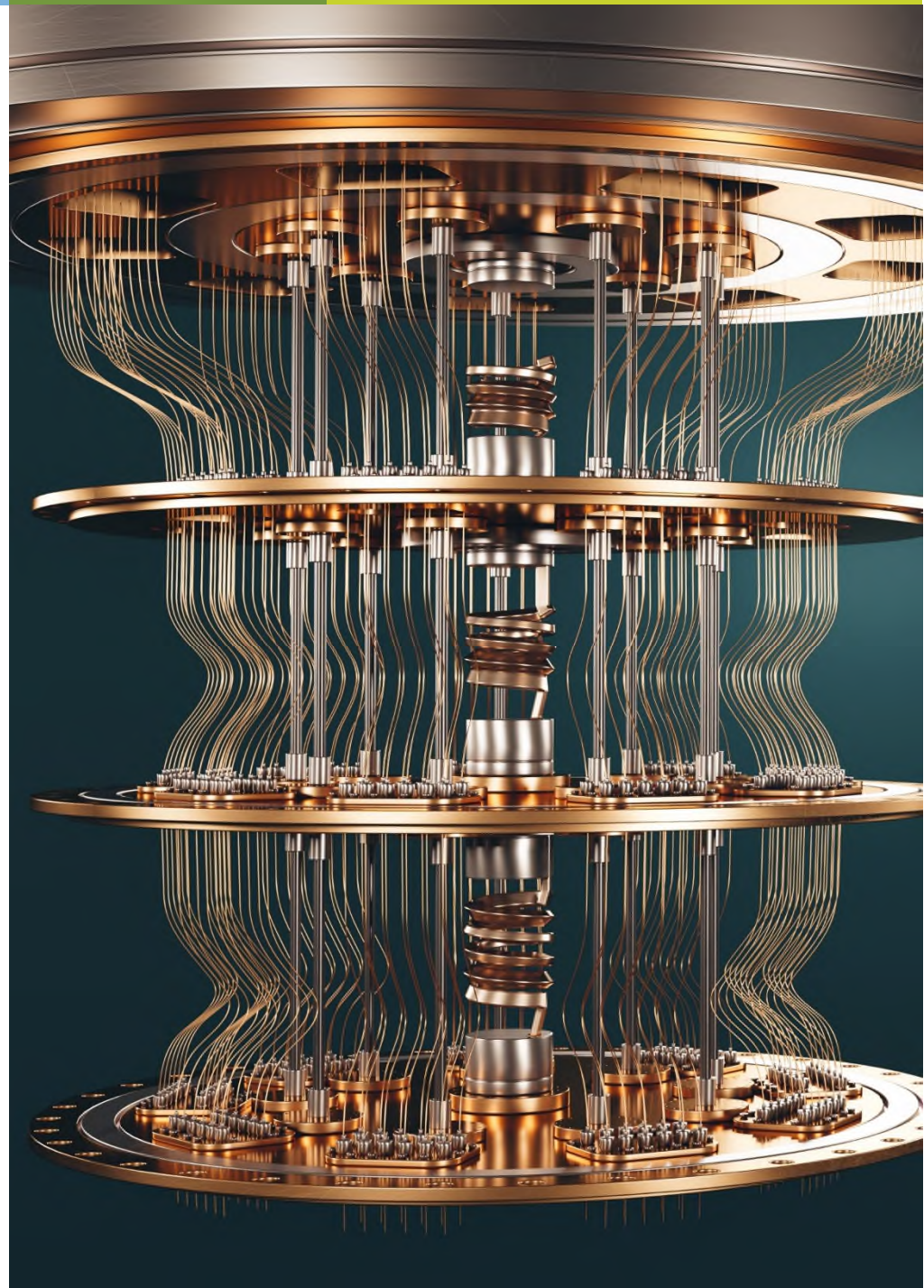
Melissa Azouaoui, Joppe W. Bos, Björn Fay, Marc Gourjon, Yulia Kuzovkova, Joost Renes, **Tobias Schneider**, Christine van Vredendaal

In Collaboration with UCLouvain:
Olivier Bronchain, Clément Hoffmann, François-Xavier Standaert

CONTACT: PQC@NXP.COM

REAL WORLD CRYPTO SYMPOSIUM, APRIL 2022

NXP | SECURE CONNECTIONS FOR A SMARTER WORLD



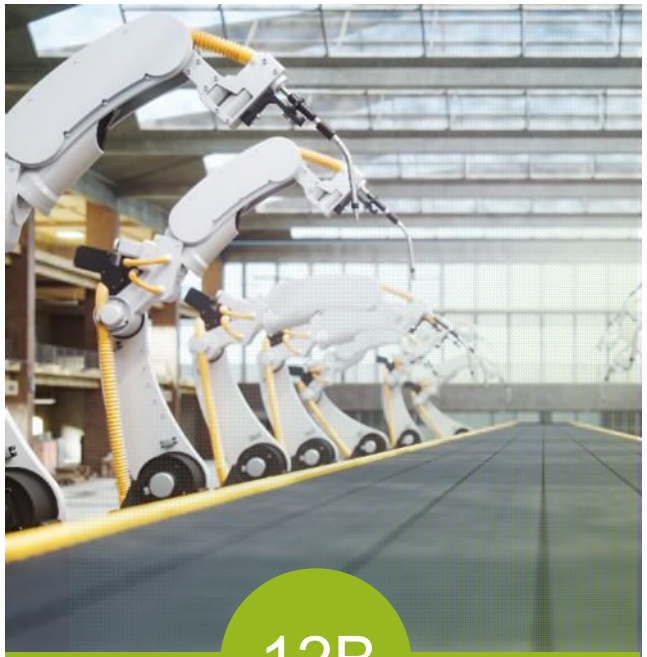
POST-QUANTUM CRYPTO IS ON THE HORIZON

AUTOMOTIVE

70%

70% connected cars by 2025

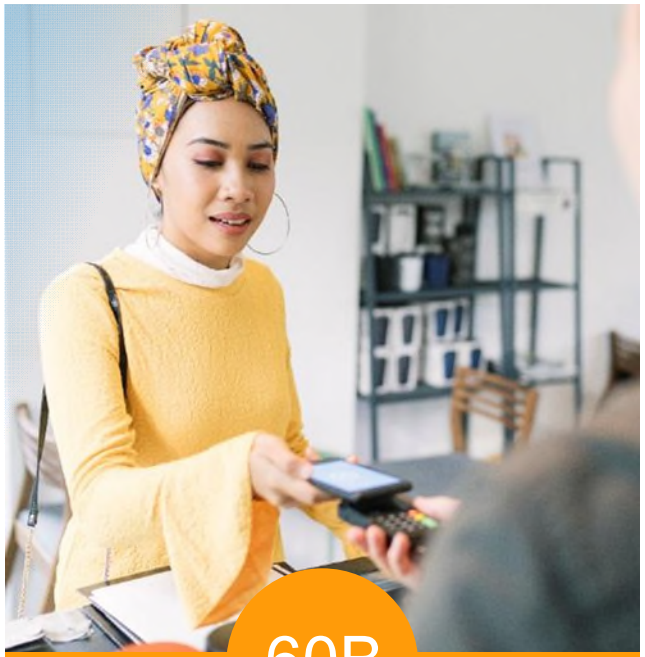
INDUSTRIAL & IOT



12B

IoT Edge & end nodes from **6B units** in 2021 to **12B units** in 2025

MOBILE



60B

Tagging **60B products** per year by 2025

COMMUNICATION INFRASTRUCTURE

40B

Secure anchors & services for **40B processors**

What is the impact on the billions of embedded devices?

1. Source: NXP, Strategy Analytics, Evercore, Ericsson, IDTechex,

CHALLENGES IN THE EMBEDDED WORLD

2021: General Challenges

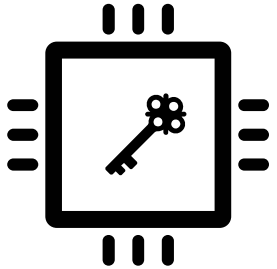
- OTA updates
- Secure boot
- Reuse existing co-pros

CHALLENGES IN THE EMBEDDED WORLD

2021: General Challenges

- OTA updates
- Secure boot
- Reuse existing co-pros

2022: Physical Security

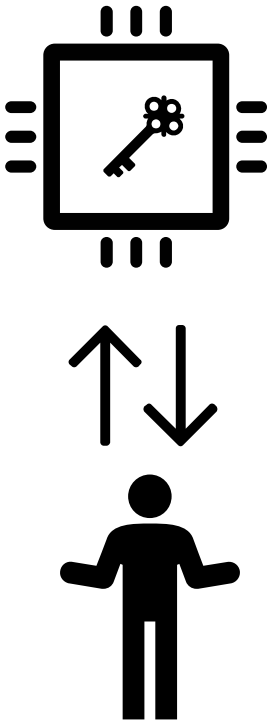


CHALLENGES IN THE EMBEDDED WORLD

2021: General Challenges

- OTA updates
- Secure boot
- Reuse existing co-pros

2022: Physical Security

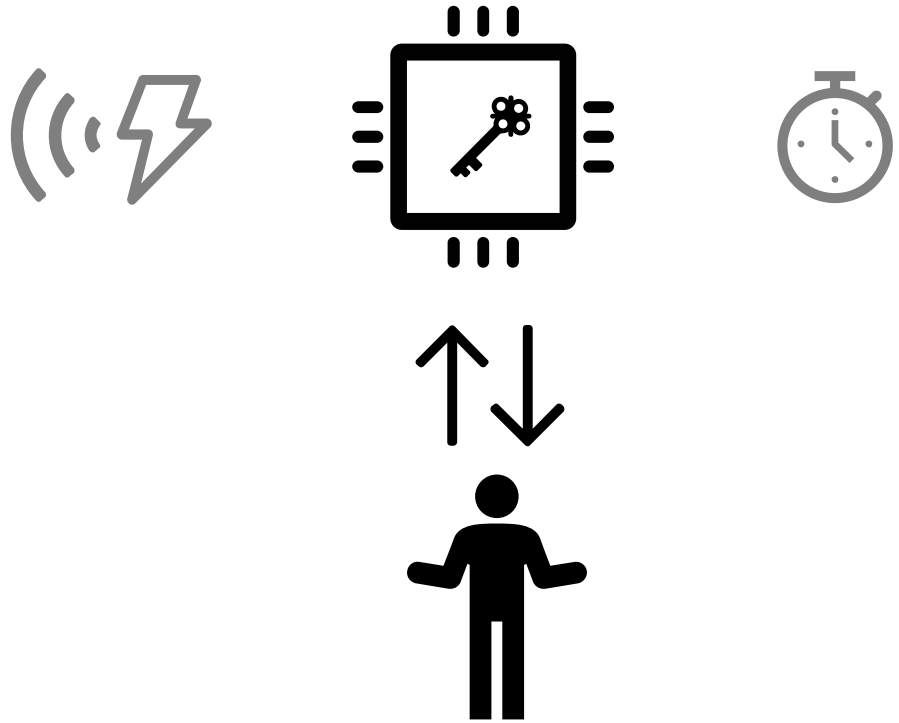


CHALLENGES IN THE EMBEDDED WORLD

2021: General Challenges

- OTA updates
- Secure boot
- Reuse existing co-pros

2022: Physical Security

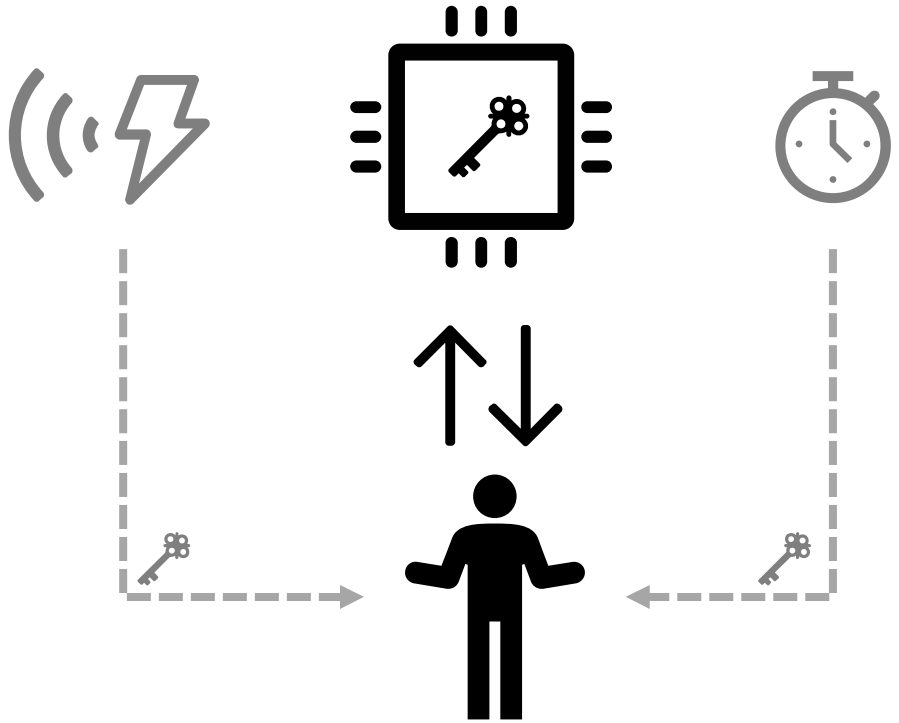


CHALLENGES IN THE EMBEDDED WORLD

2021: General Challenges

- OTA updates
- Secure boot
- Reuse existing co-pros

2022: Physical Security



Current Cryptography

CHALLENGES IN THE EMBEDDED WORLD

Attacks

Deep understanding in both academia and industry.

Current Cryptography

Countermeasures

Practically secure and certified implementations.

CHALLENGES IN THE EMBEDDED WORLD

Attacks

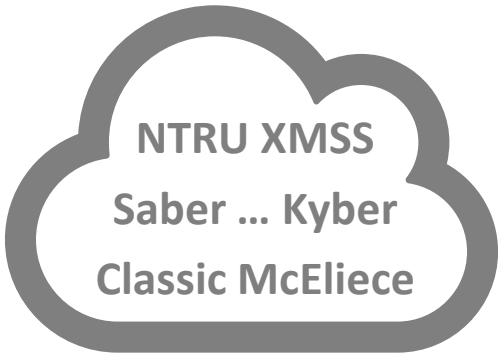
Deep understanding in both academia and industry.

Current Cryptography

Countermeasures

Practically secure and certified implementations.

Post-Quantum Cryptography



CHALLENGES IN THE EMBEDDED WORLD

Attacks

Deep understanding in both academia and industry.

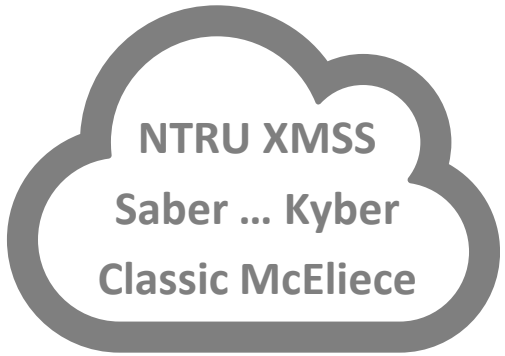
Current Cryptography

Countermeasures

Practically secure and certified implementations.

Post-Quantum Cryptography

Active research area resulting in increasingly powerful attacks.



Early stage of academic research.
Limited industrial results.

CHALLENGES IN THE EMBEDDED WORLD

Attacks	Current Cryptography	Countermeasures
Deep understanding in both academia and industry.	AES 3DES DSA … ECDSA RSA ECC	Practically secure and certified implementations.

What does it mean to secure PQC implementations in “practice”?

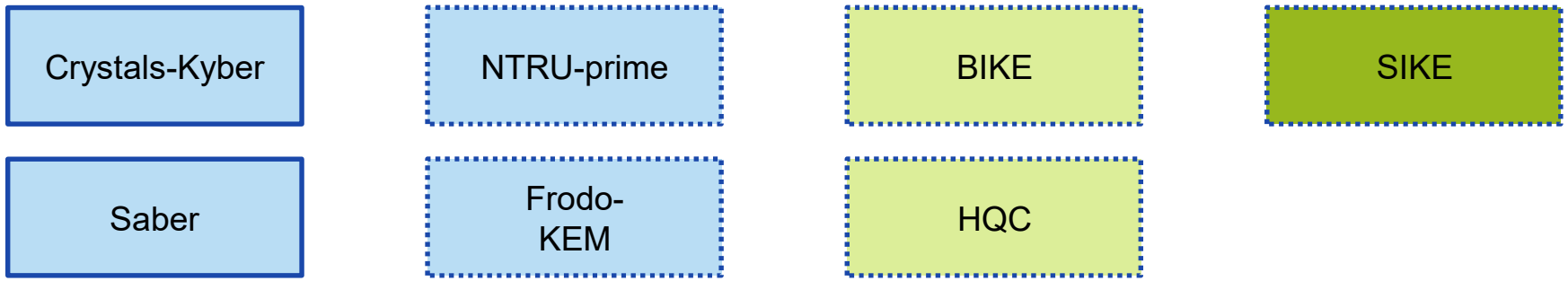
Active research area resulting in increasingly powerful attacks.	NTRU XMSS Saber … Kyber Classic McEliece	Early stage of academic research. Limited industrial results.

FO-CALYPSE?

SECURE CONNECTIONS
FOR A SMARTER WORLD

THE SCA PROBLEM OF THE FO-TRANSFORM

The Fujisaki-Okamoto (FO) transformation (or slight variants) underlies the IND-CCA security of many KEMs, e.g.:

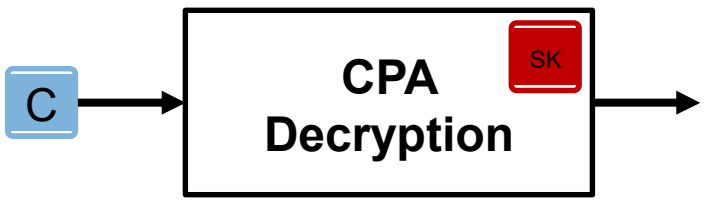


THE SCA PROBLEM OF THE FO-TRANSFORM

The Fujisaki-Okamoto (FO) transformation (or slight variants) underlies the IND-CCA security of many KEMs, e.g.:

Crystals-Kyber	NTRU-prime	BIKE	SIKE
Saber	Frodo-KEM	HQC	

Exemplary Decapsulation:

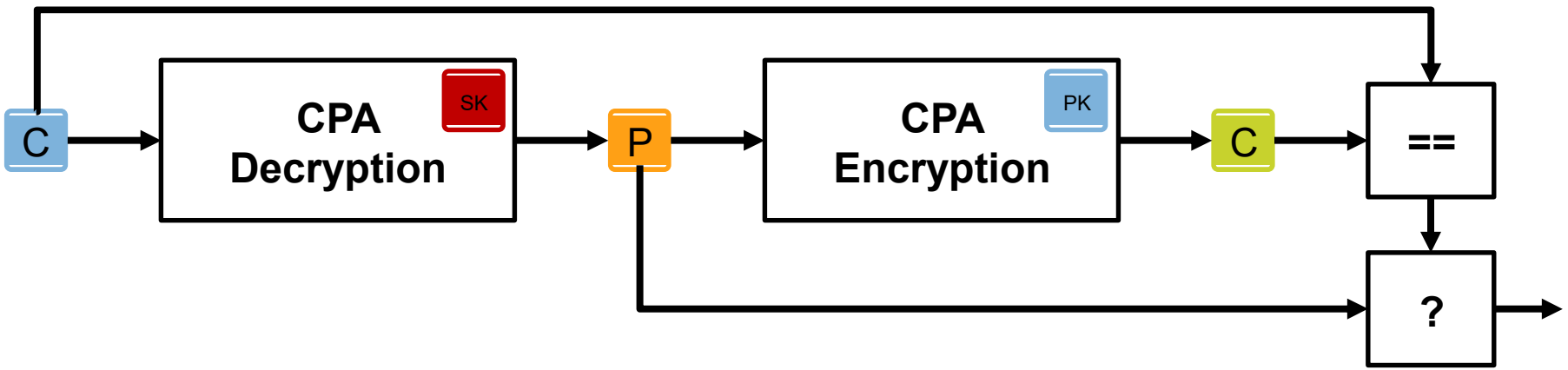


THE SCA PROBLEM OF THE FO-TRANSFORM

The Fujisaki-Okamoto (FO) transformation (or slight variants) underlies the IND-CCA security of many KEMs, e.g.:

Crystals-Kyber	NTRU-prime	BIKE	SIKE
Saber	Frodo-KEM	HQC	

Exemplary Decapsulation:

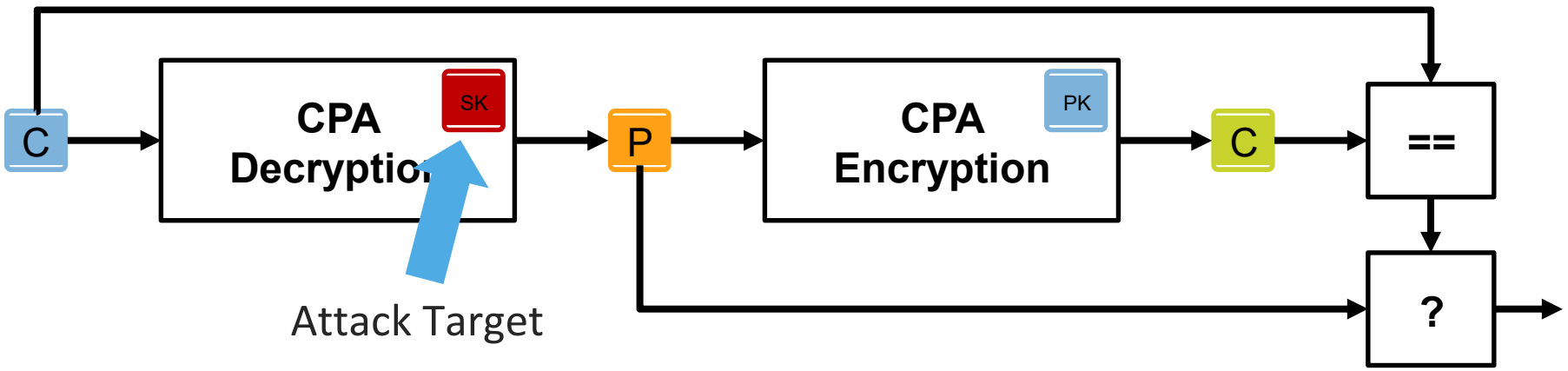


THE SCA PROBLEM OF THE FO-TRANSFORM

The Fujisaki-Okamoto (FO) transformation (or slight variants) underlies the IND-CCA security of many KEMs, e.g.:

Crystals-Kyber	NTRU-prime	BIKE	SIKE
Saber	Frodo-KEM	HQC	

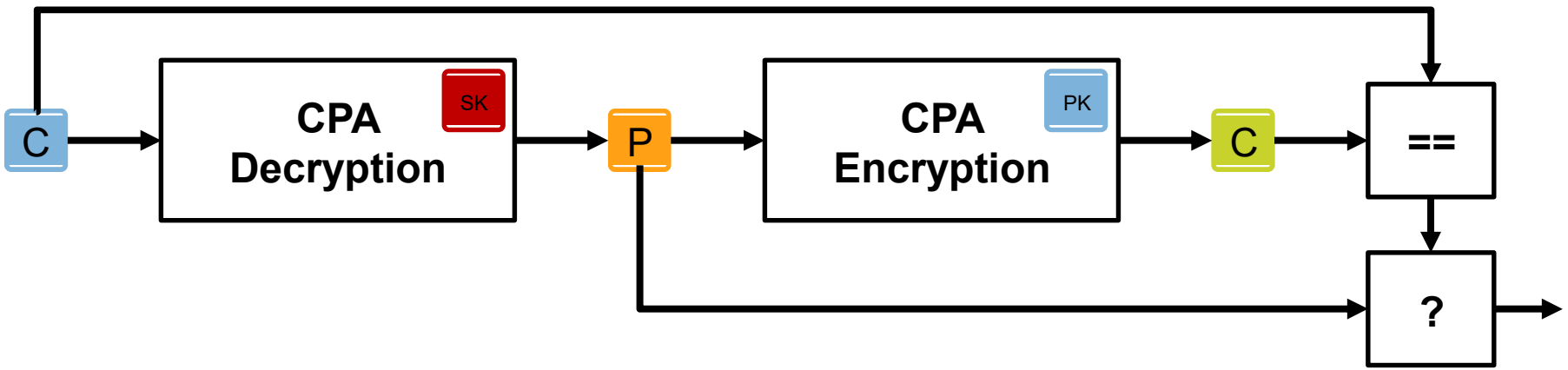
Exemplary Decapsulation:



THE SCA PROBLEM OF THE FO-TRANSFORM

Attack 1: Chosen Plaintext

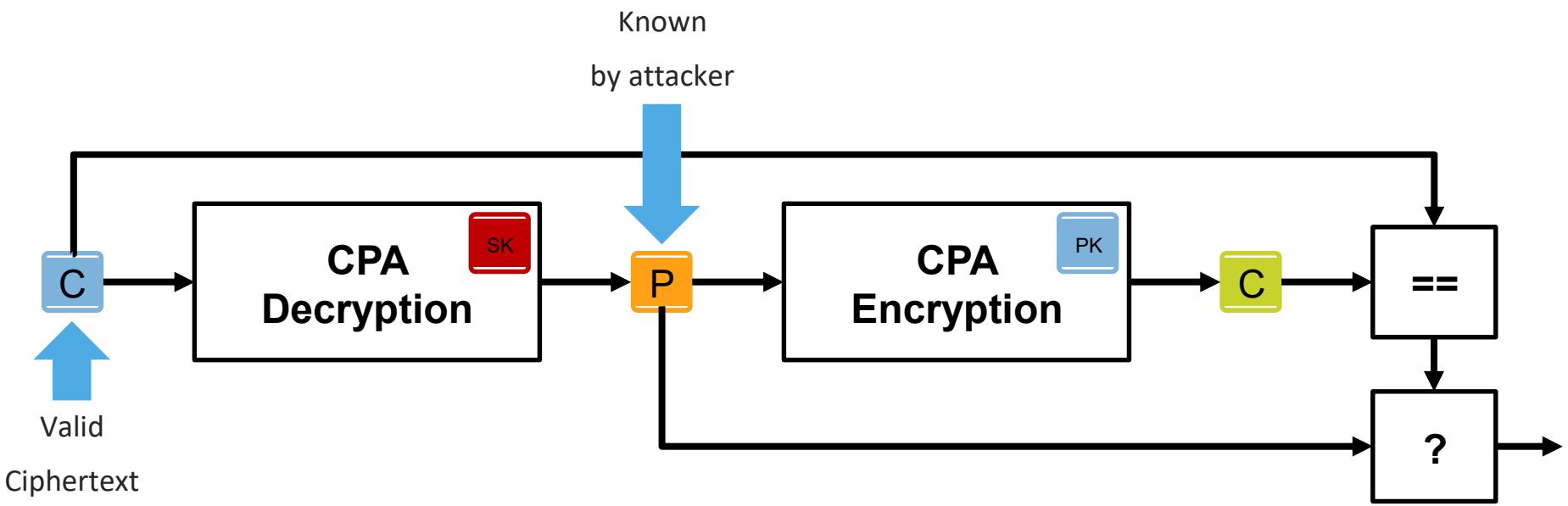
- Attacker inputs only valid ciphertexts



THE SCA PROBLEM OF THE FO-TRANSFORM

Attack 1: Chosen Plaintext

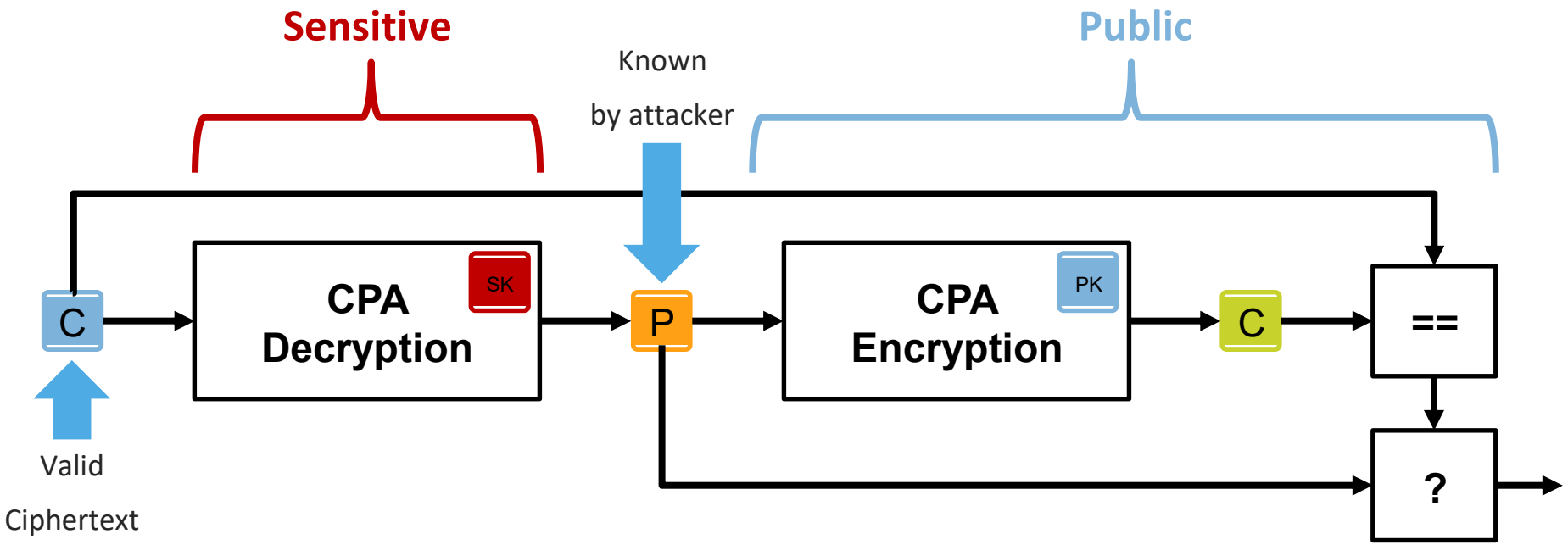
- Attacker inputs only valid ciphertexts



THE SCA PROBLEM OF THE FO-TRANSFORM

Attack 1: Chosen Plaintext

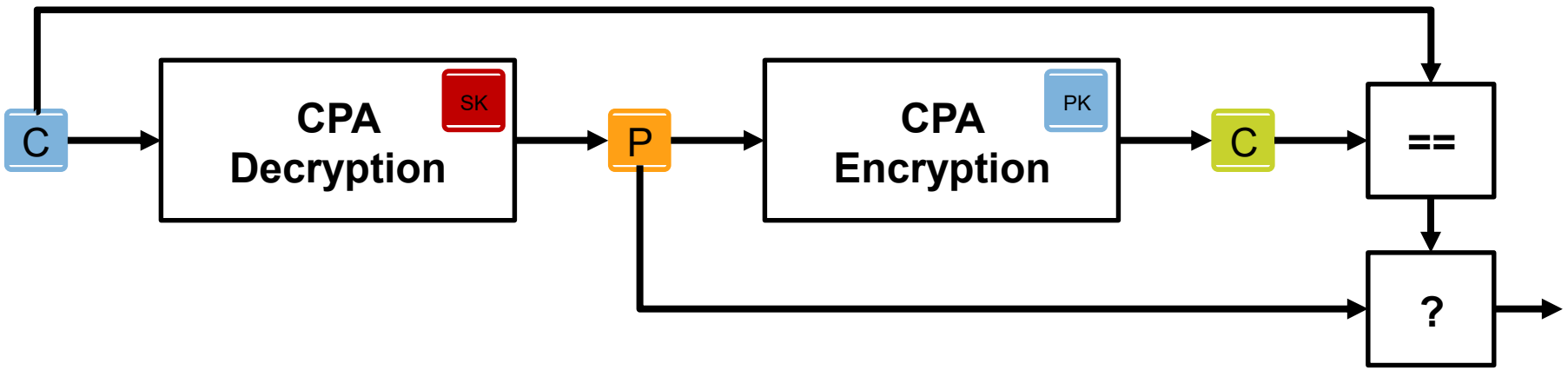
- Attacker inputs only valid ciphertexts
- Attack focuses on **CPA Decryption**, everything after (and including) P is public
- Only need to protect **CPA Decryption**



THE SCA PROBLEM OF THE FO-TRANSFORM

Attack 2: Chosen Ciphertext

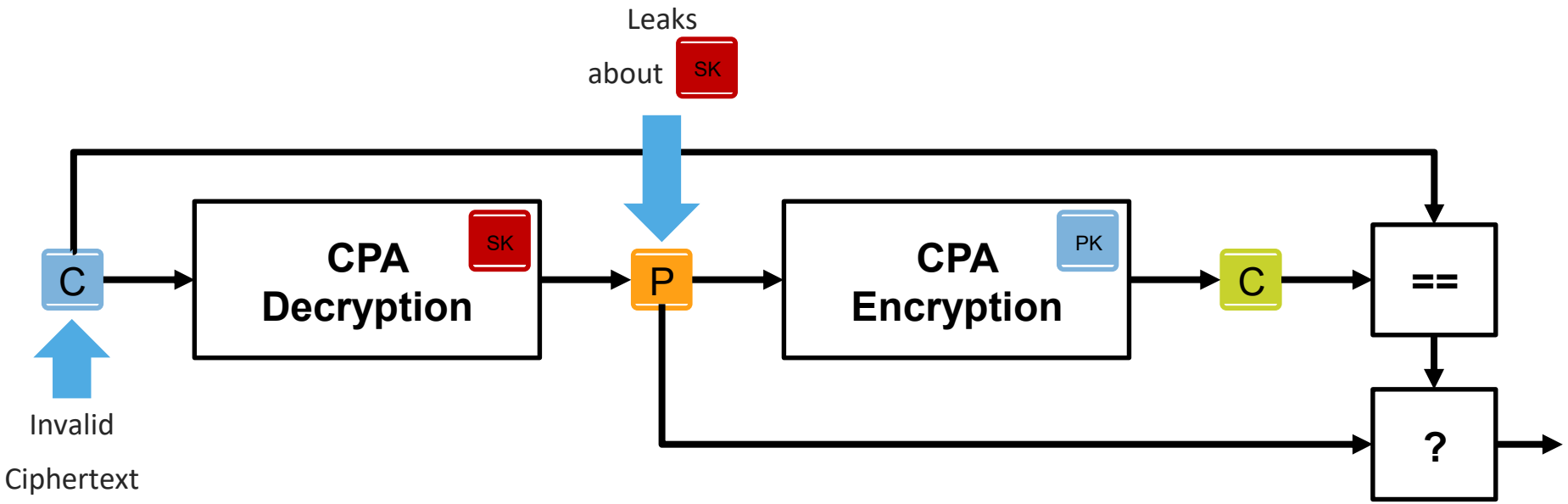
- Attacker inputs specially-crafted invalid ciphertexts



THE SCA PROBLEM OF THE FO-TRANSFORM

Attack 2: Chosen Ciphertext

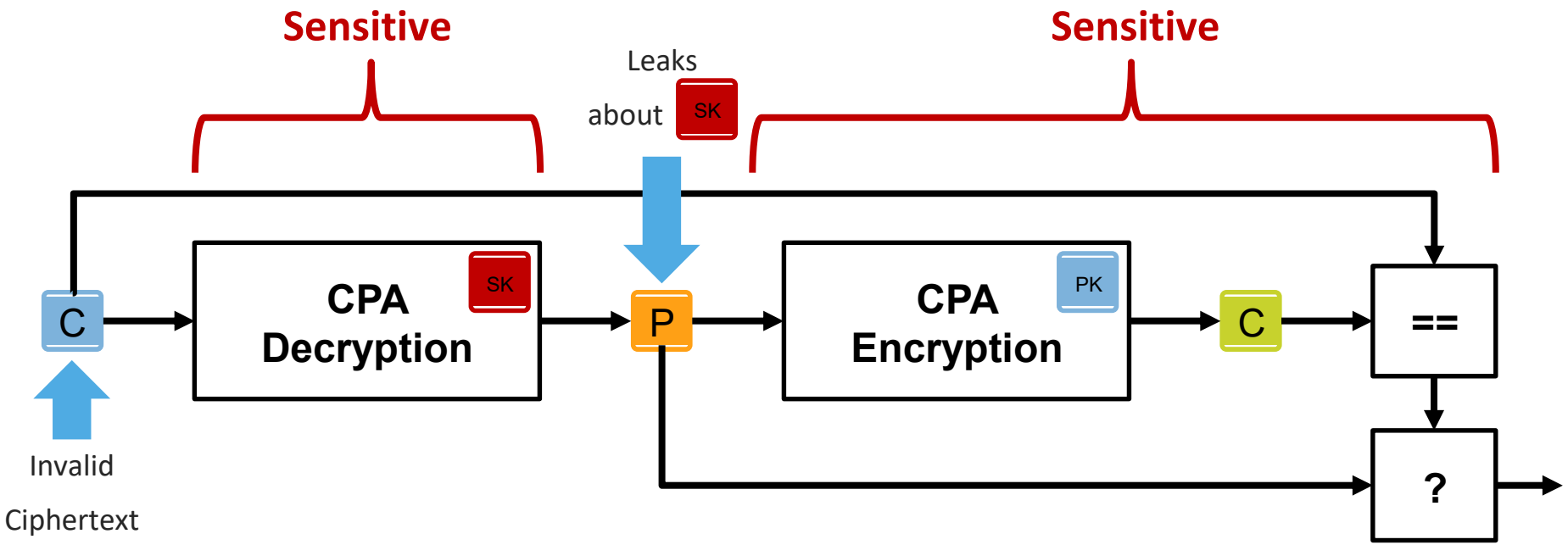
- Attacker inputs specially-crafted invalid ciphertexts



THE SCA PROBLEM OF THE FO-TRANSFORM

Attack 2: Chosen Ciphertext

- Attacker inputs specially-crafted invalid ciphertexts
- Attack focuses on **CPA Decryption +** everything after (and including) P is potentially sensitive
- Potentially **all (or most) modules** need to be hardened



THE SCA PROBLEM OF THE FO-TRANSFORM

Why is it bad?

THE SCA PROBLEM OF THE FO-TRANSFORM

Why is it bad?

- ☑ Millions of Points of Interest
- ☑ Low number of leakage classes (worst case = 2)
- ☑ Easy to build templates

THE SCA PROBLEM OF THE FO-TRANSFORM

Why is it bad?

- ☑ Millions of Points of Interest
- ☑ Low number of leakage classes (worst case = 2)
- ☑ Easy to build templates

Most recently at TCHES-2022:

Curse of Re-encryption: A Generic Power/EM Analysis on Post-Quantum KEMs

Rei Ueno[1,2,3], Keita Xagawa[4], Yutaro Tanaka[1,2], Akira Ito[1,2], Junko Takahashi[4] and Naofumi Homma[1,2]

Quantifying the Curse

SECURE CONNECTIONS
FOR A SMARTER WORLD

QUANTIFYING THE CURSE

How bad is it?

A lot of attacks published.

Some countermeasures.

QUANTIFYING THE CURSE

How bad is it?

A lot of attacks published.

+

Some countermeasures.

||

What do we need in “practice”?

QUANTIFYING THE CURSE

How bad is it?

A lot of attacks published.

+

Some countermeasures.

||

What do we need in “practice”?

Systematic Study of Decryption and Re-Encryption Leakage: the Case of Kyber

Melissa Azouaoui[1], Olivier Bronchain[2], Clément Hoffmann[2], Yulia Kuzovkova[1], Tobias Schneider[1], François-Xavier Standaert[2]

CASE STUDY: WORST CASE ANALYSIS

Target: 1M traces SCA security

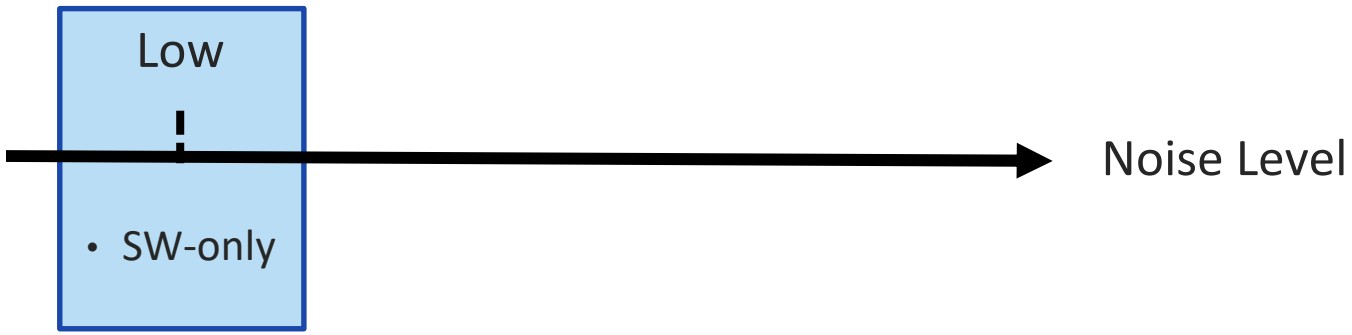
CASE STUDY: WORST CASE ANALYSIS

Target: 1M traces SCA security

Noise Level

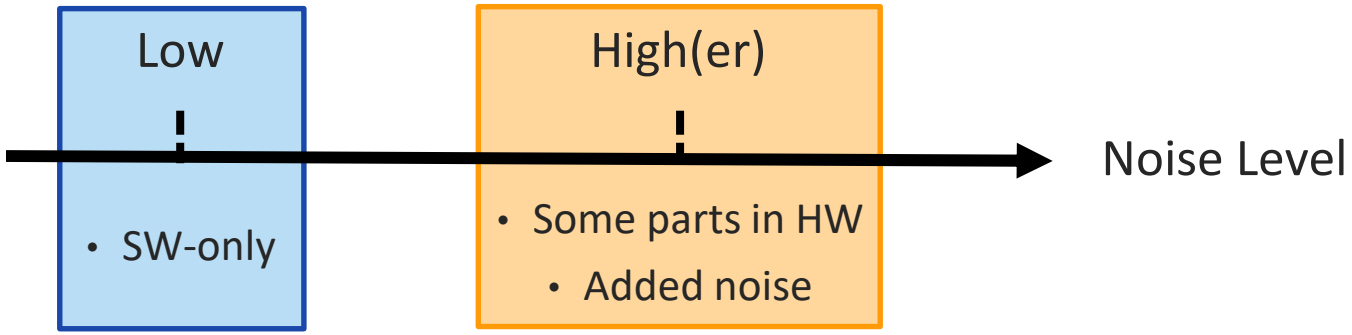
CASE STUDY: WORST CASE ANALYSIS

Target: 1M traces SCA security



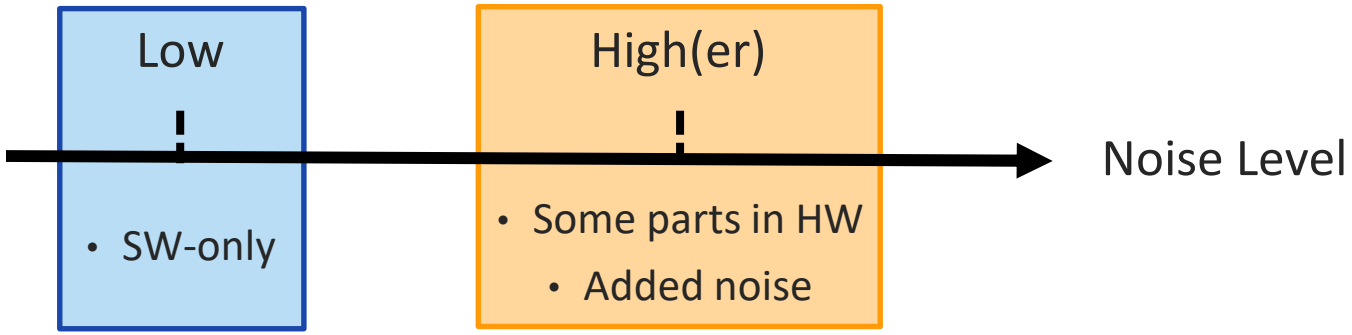
CASE STUDY: WORST CASE ANALYSIS

Target: 1M traces SCA security



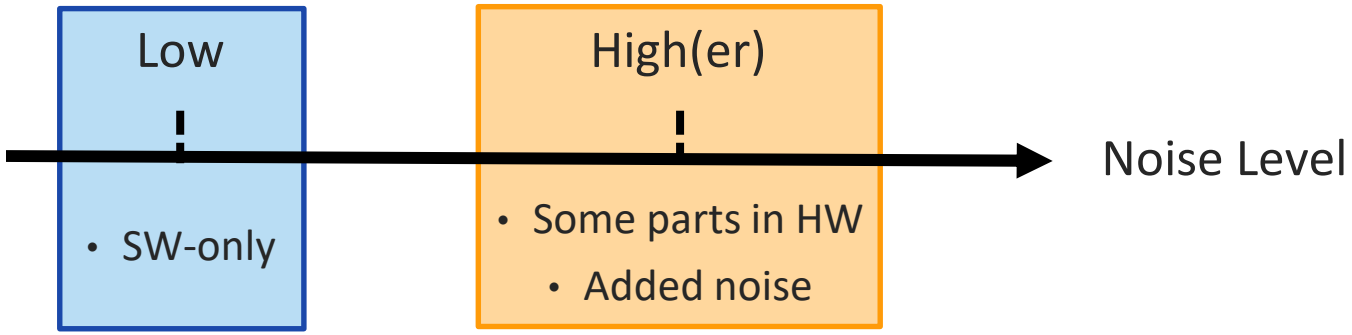
CASE STUDY: WORST CASE ANALYSIS

Target: 1M traces SCA security



CASE STUDY: WORST CASE ANALYSIS

Target: 1M traces SCA security

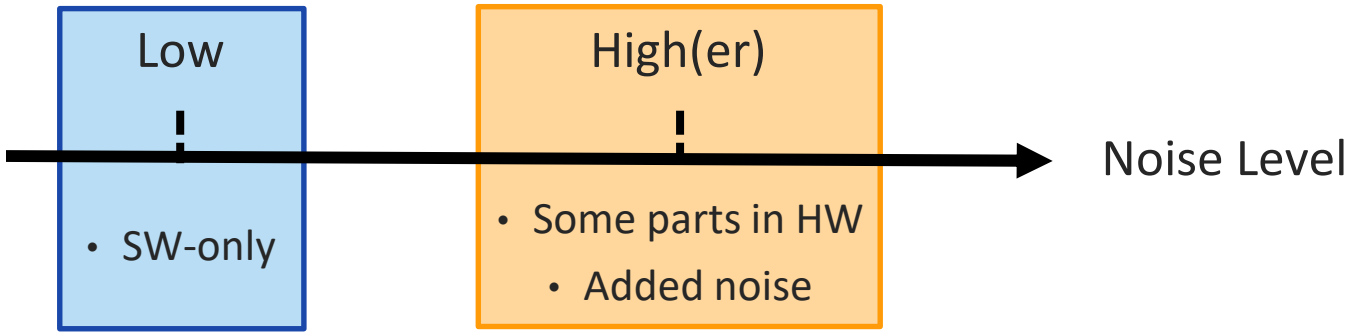


Count leaking variables for **Known Ciphertext** Attack

Count leaking variables for **Chosen Ciphertext** Attack

CASE STUDY: WORST CASE ANALYSIS

Target: 1M traces SCA security

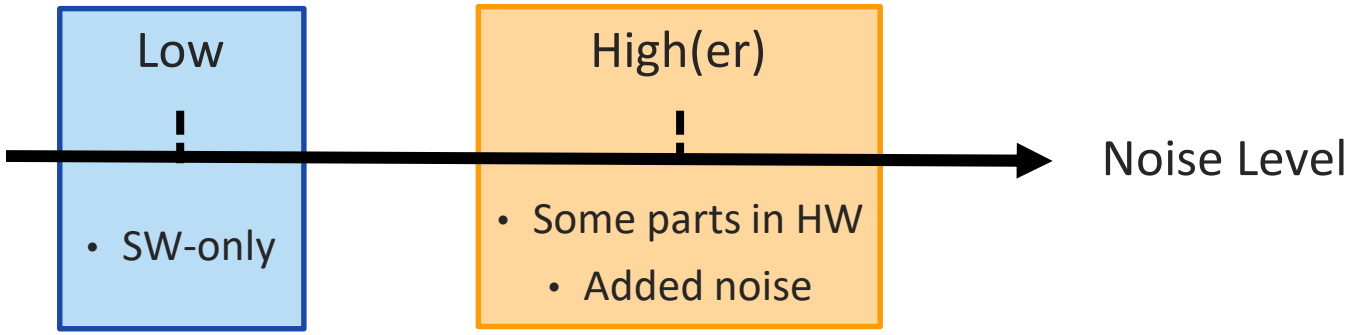


Count leaking variables for **Known Ciphertext** Attack → **Estimate** the **number of traces** required for an attack

Count leaking variables for **Chosen Ciphertext** Attack → **Estimate** the **number of traces** required for an attack

CASE STUDY: WORST CASE ANALYSIS

Target: 1M traces SCA security



Count leaking variables for **Known Ciphertext** Attack

Estimate the **number of traces** required for an attack

Count leaking variables for **Chosen Ciphertext** Attack

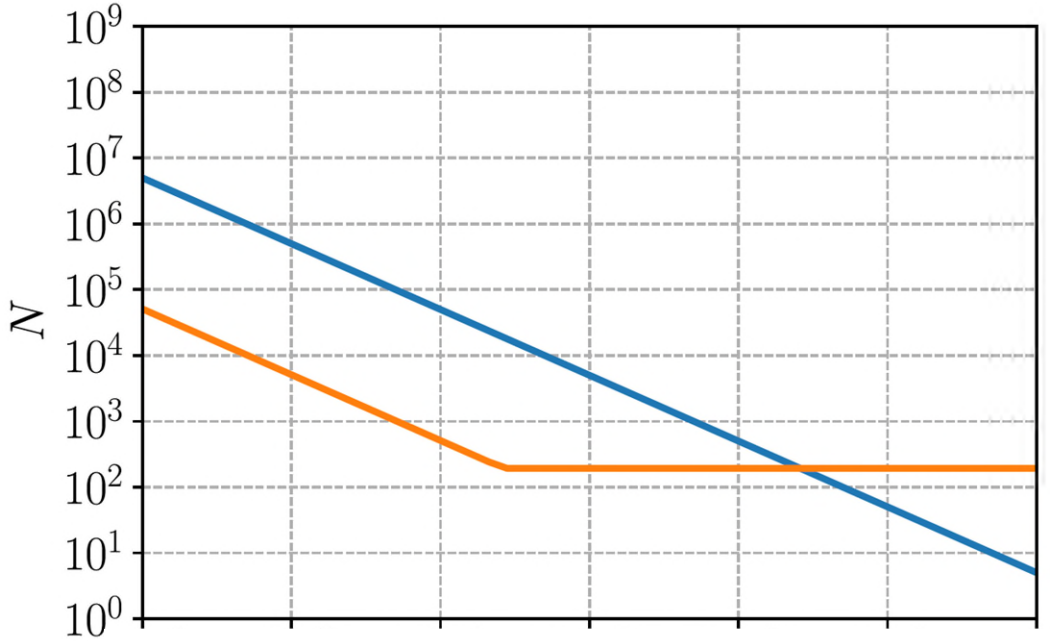
Estimate the **number of traces** required for an attack

Compare for different **noise levels**

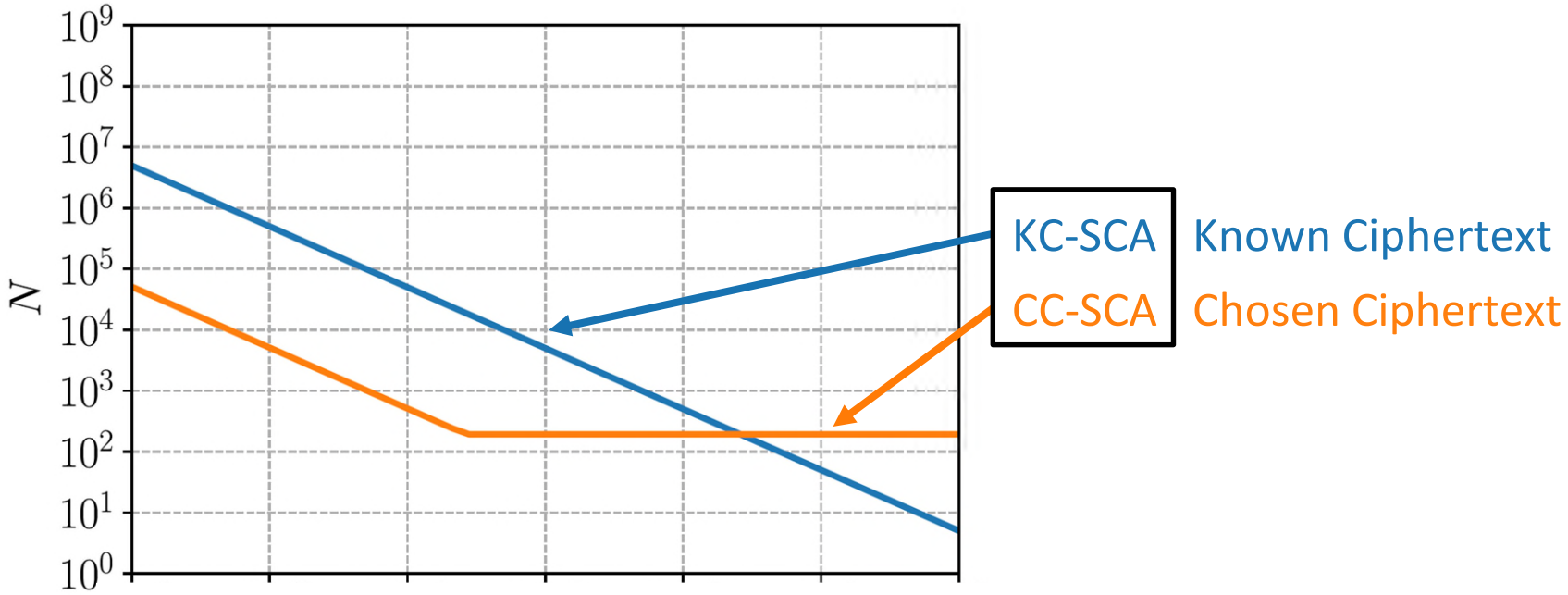
KYBER

Disclaimer: Not a replacement for practical evaluations!

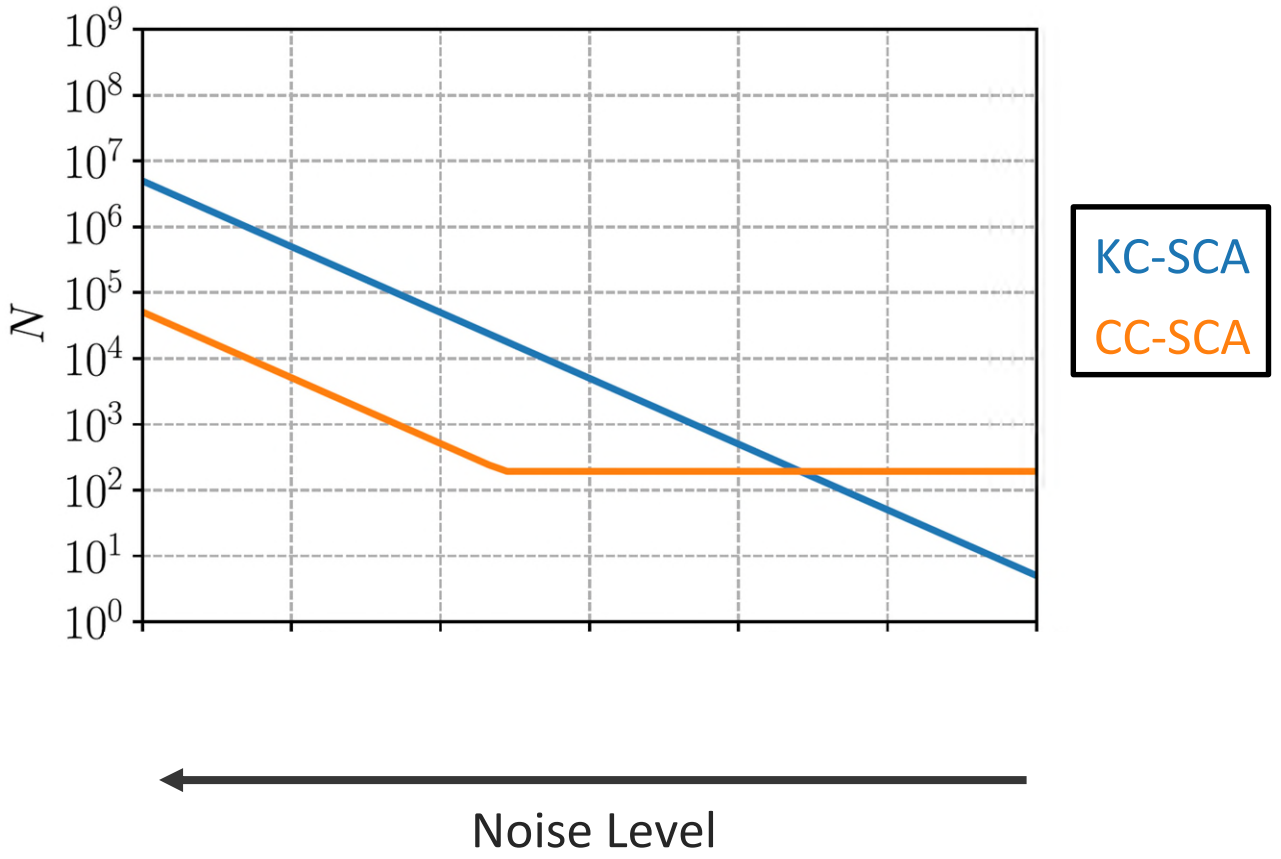
CASE STUDY: UNPROTECTED KYBER



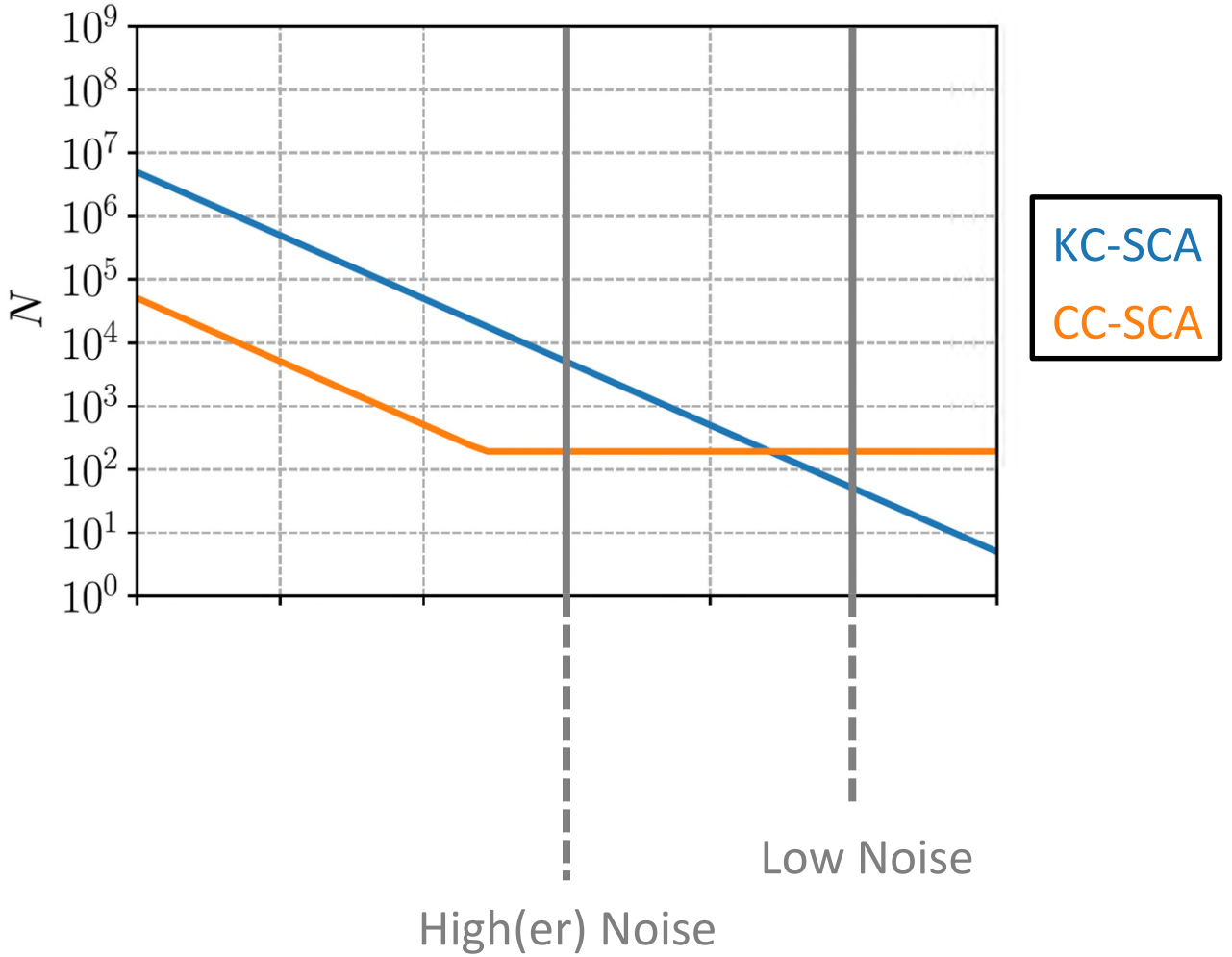
CASE STUDY: UNPROTECTED KYBER



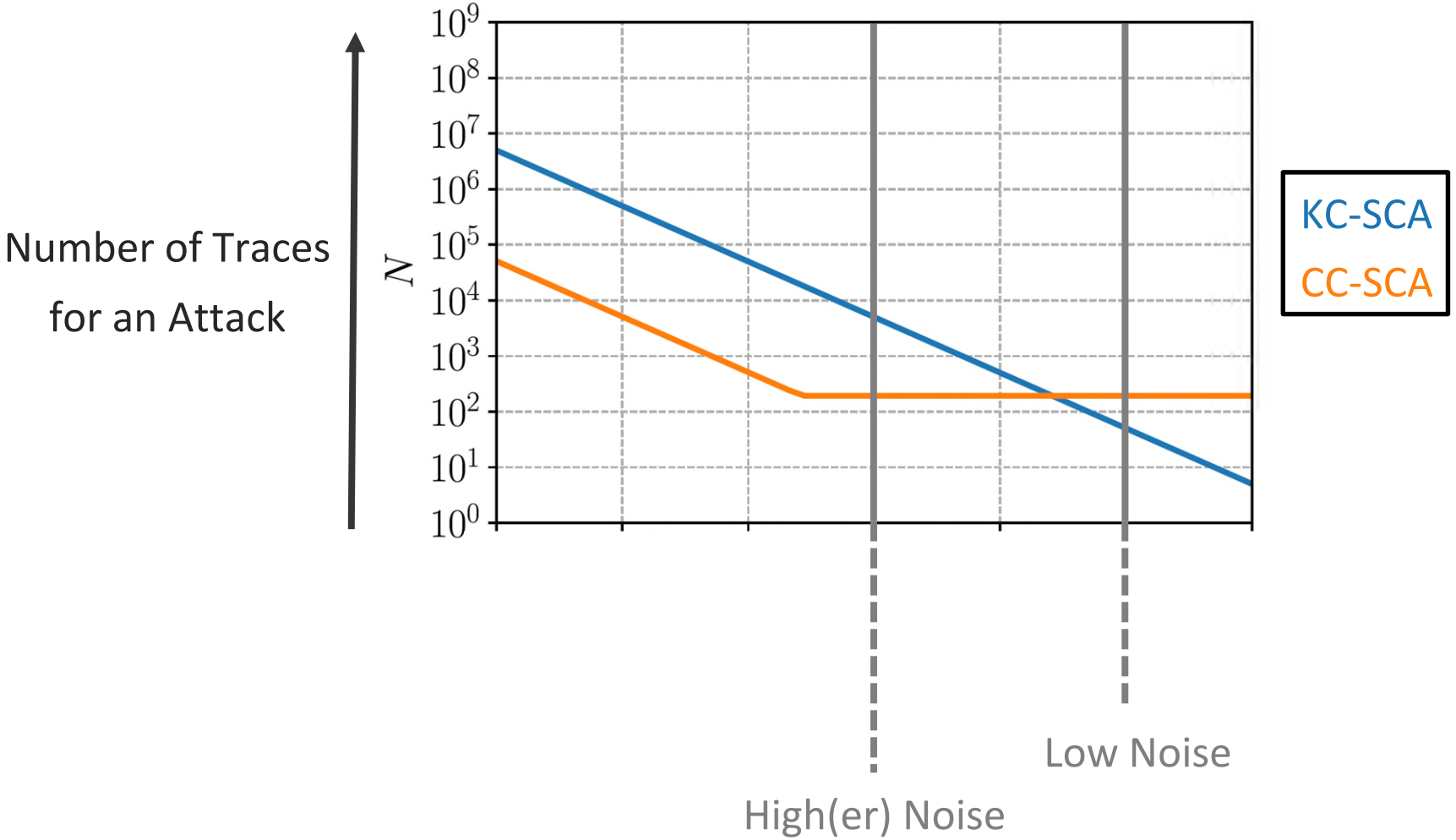
CASE STUDY: UNPROTECTED KYBER



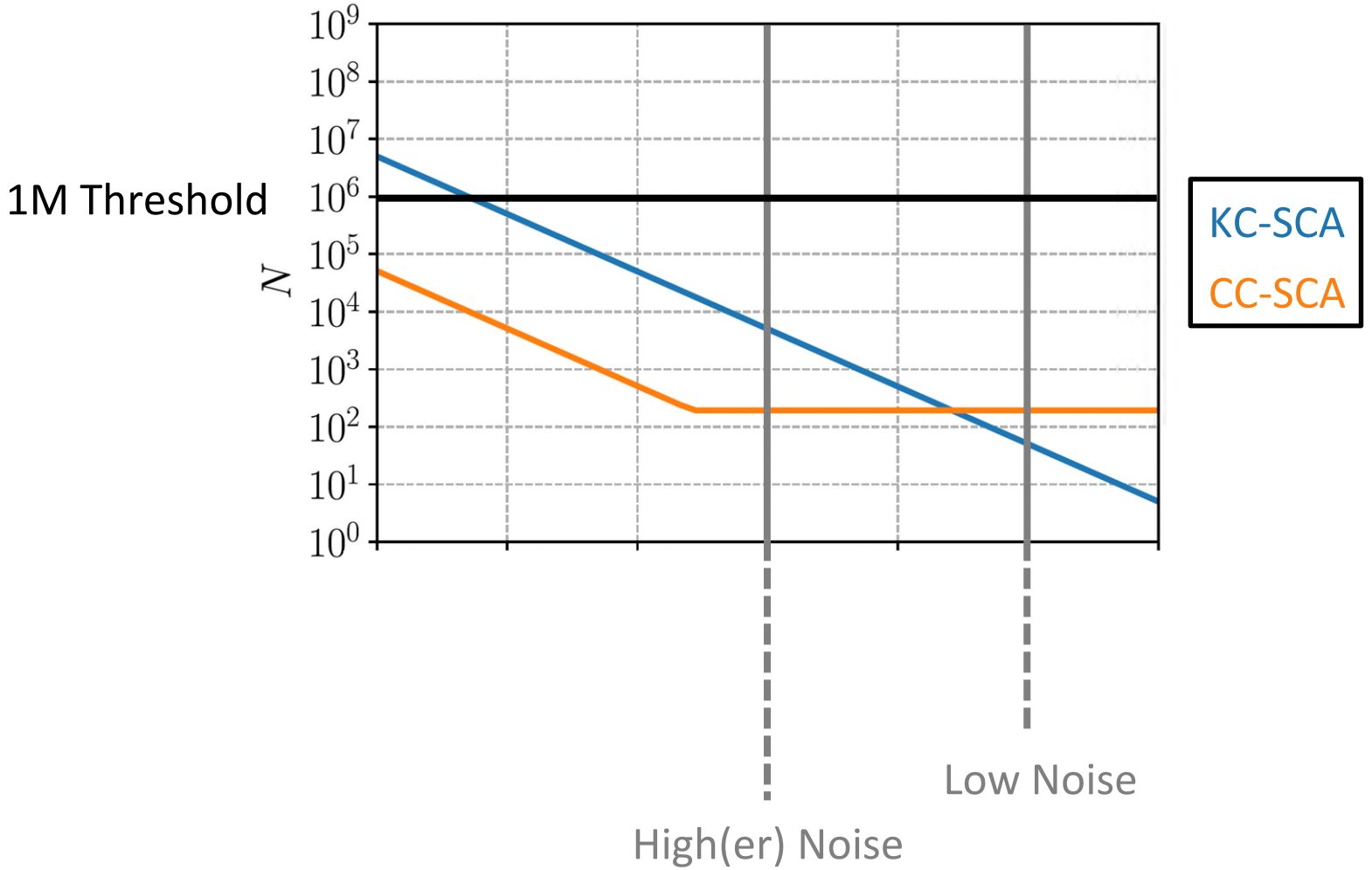
CASE STUDY: UNPROTECTED KYBER



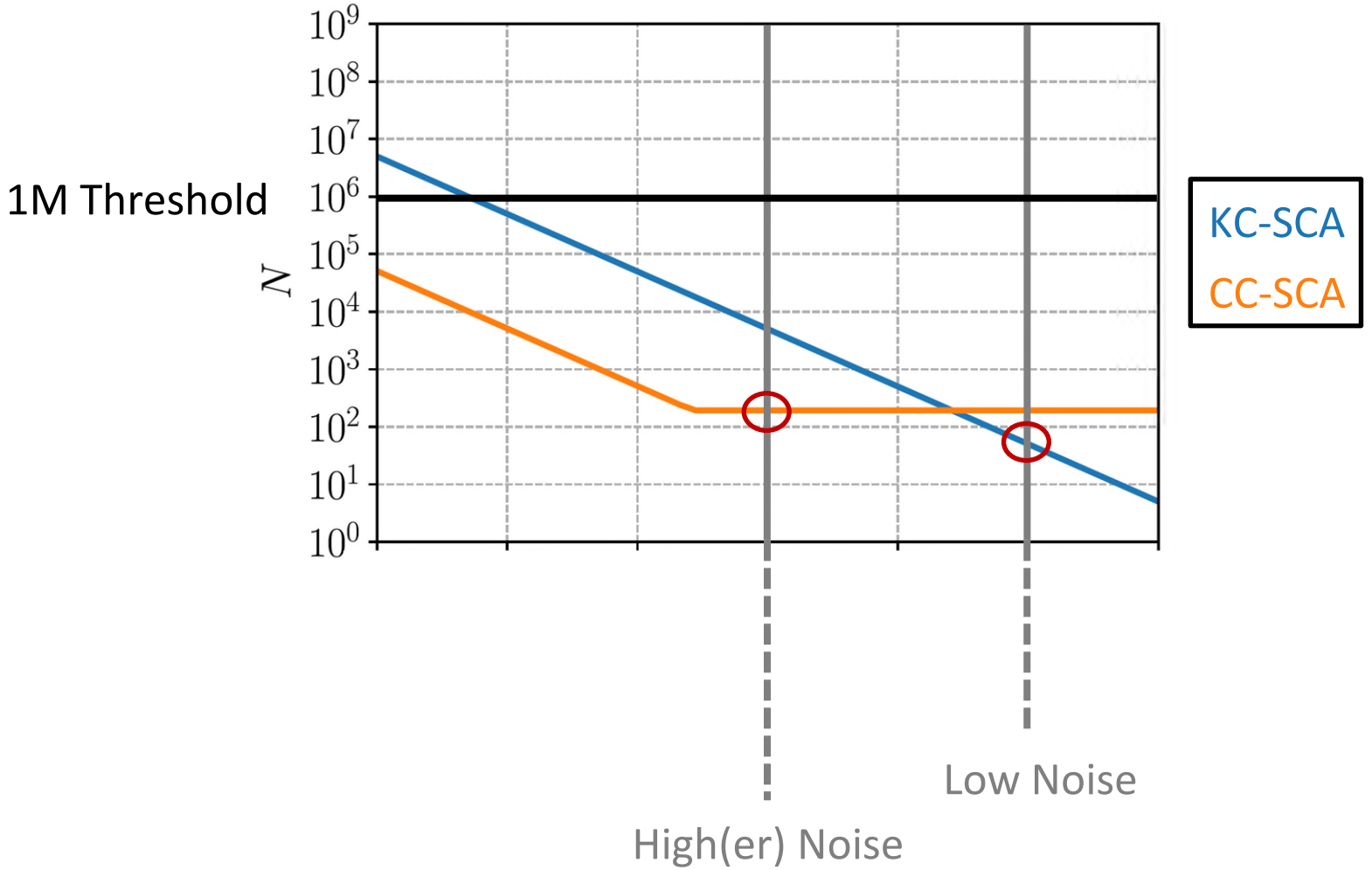
CASE STUDY: UNPROTECTED KYBER



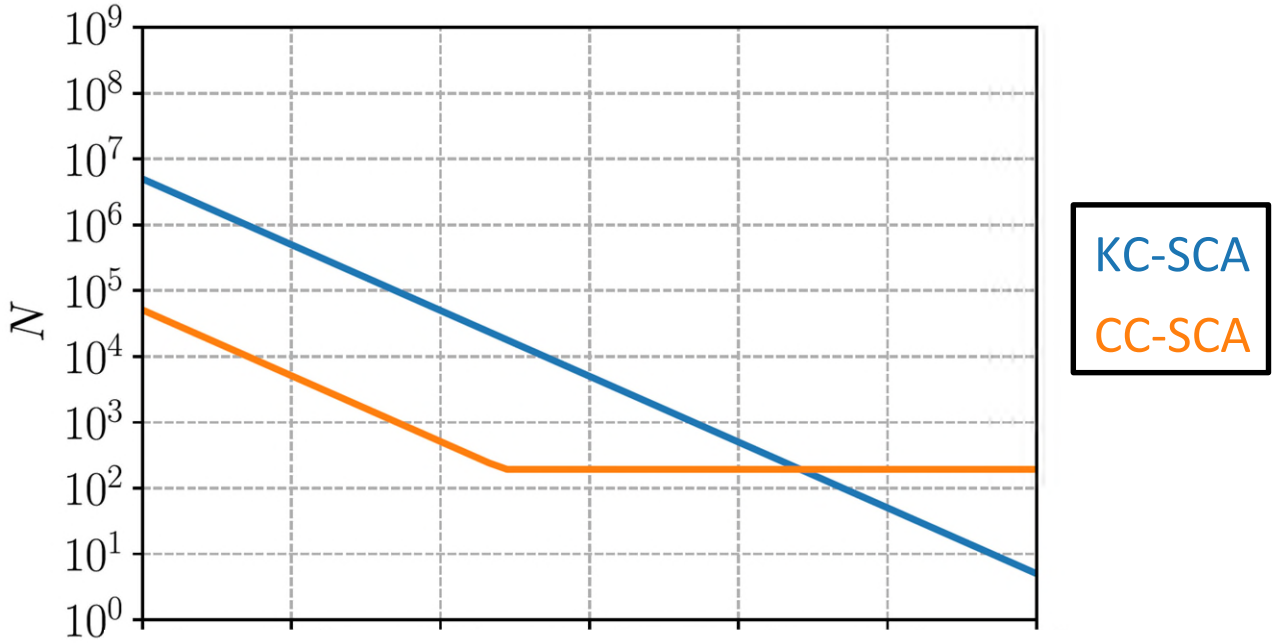
CASE STUDY: UNPROTECTED KYBER



CASE STUDY: UNPROTECTED KYBER

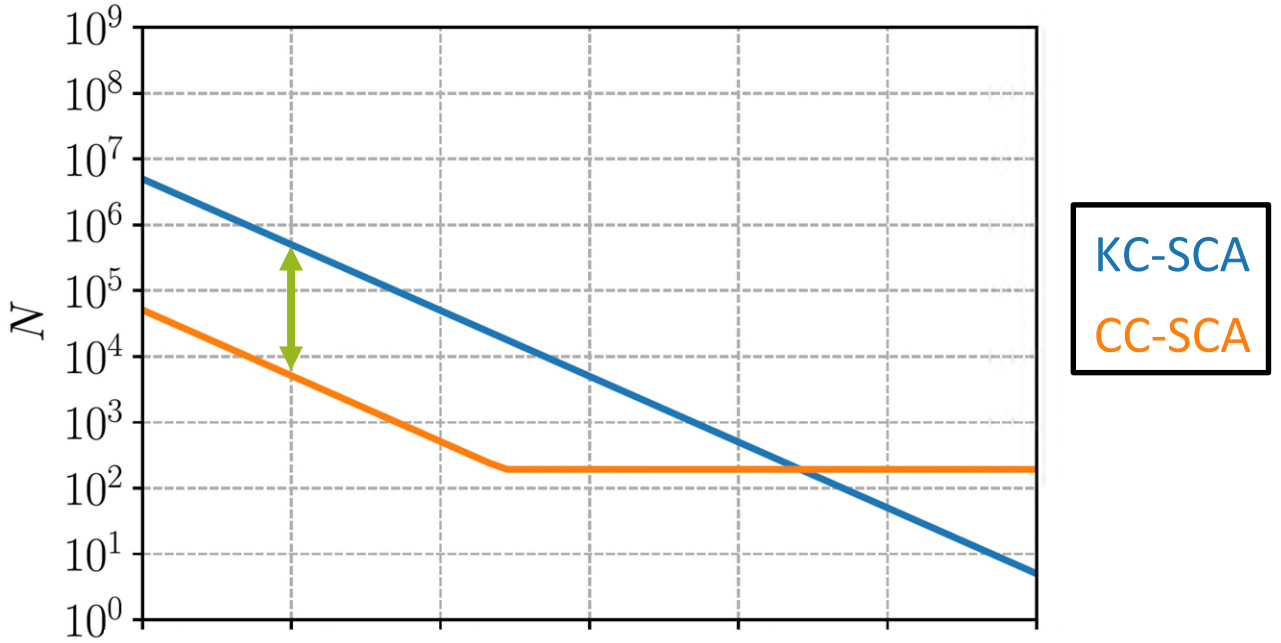


CASE STUDY: UNPROTECTED KYBER



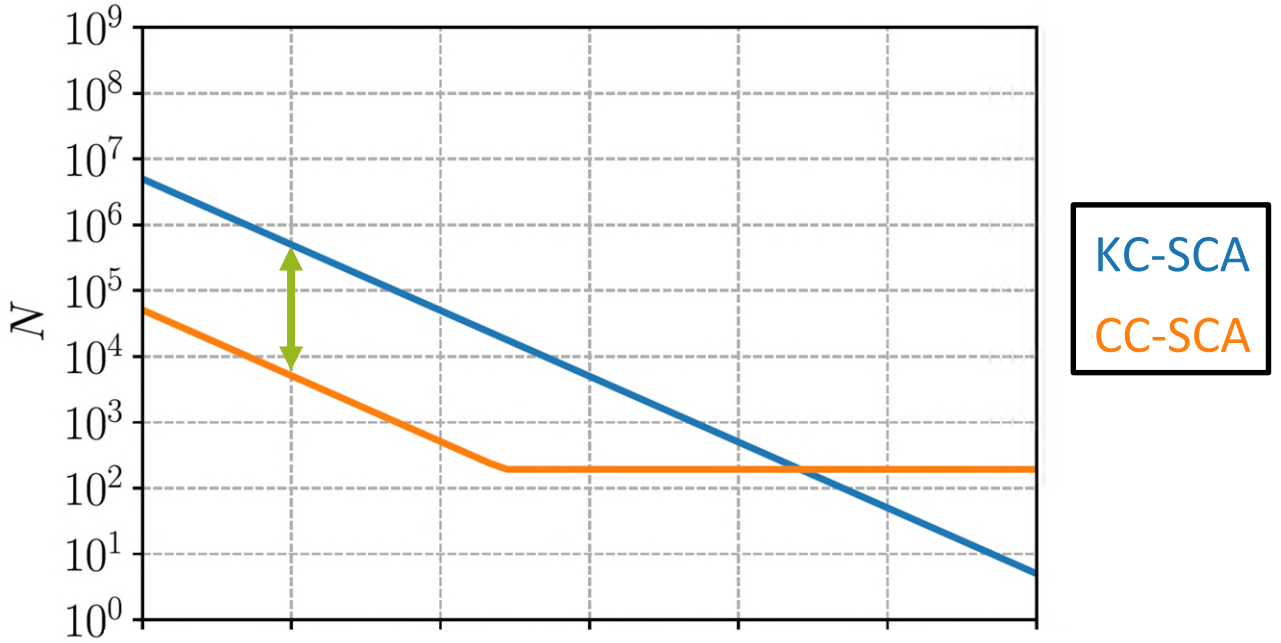
- Unprotected Kyber is (unsurprisingly) not sufficient for both noise levels

CASE STUDY: UNPROTECTED KYBER



- Unprotected Kyber is (unsurprisingly) not sufficient for both noise levels
- There is a gap of roughly **x100** between the attacks for high(er) noise

CASE STUDY: UNPROTECTED KYBER



- Unprotected Kyber is (unsurprisingly) not sufficient for both noise levels
- There is a gap of roughly **x100** between the attacks for high(er) noise

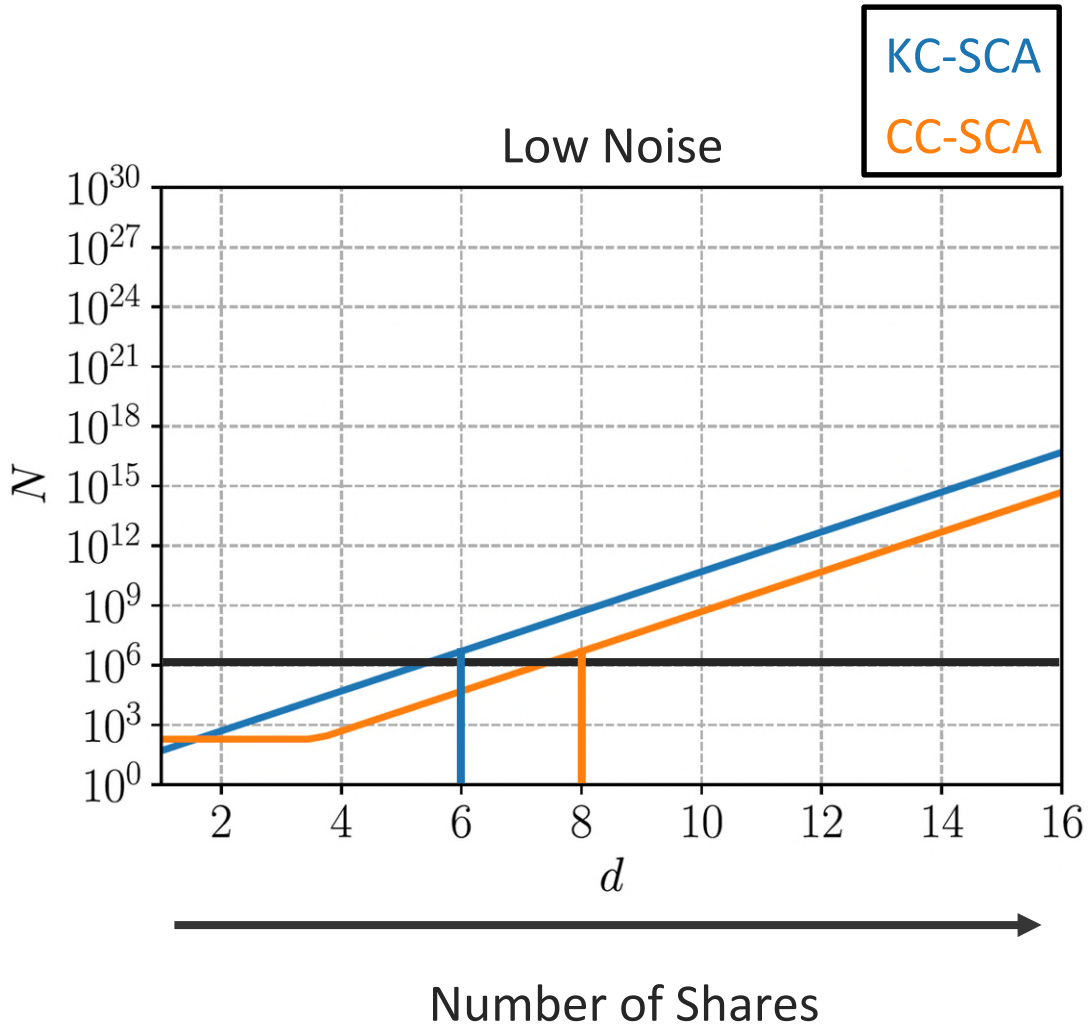
Can this be overcome through masking?

CASE STUDY: MASKED KYBER

Split variables into *d* **shares**.

Higher *d* = Higher security + Increased cost

Pre-Quantum: Certified industrial solutions **d = 2-3**



CASE STUDY: MASKED KYBER

Split variables into *d* **shares**.

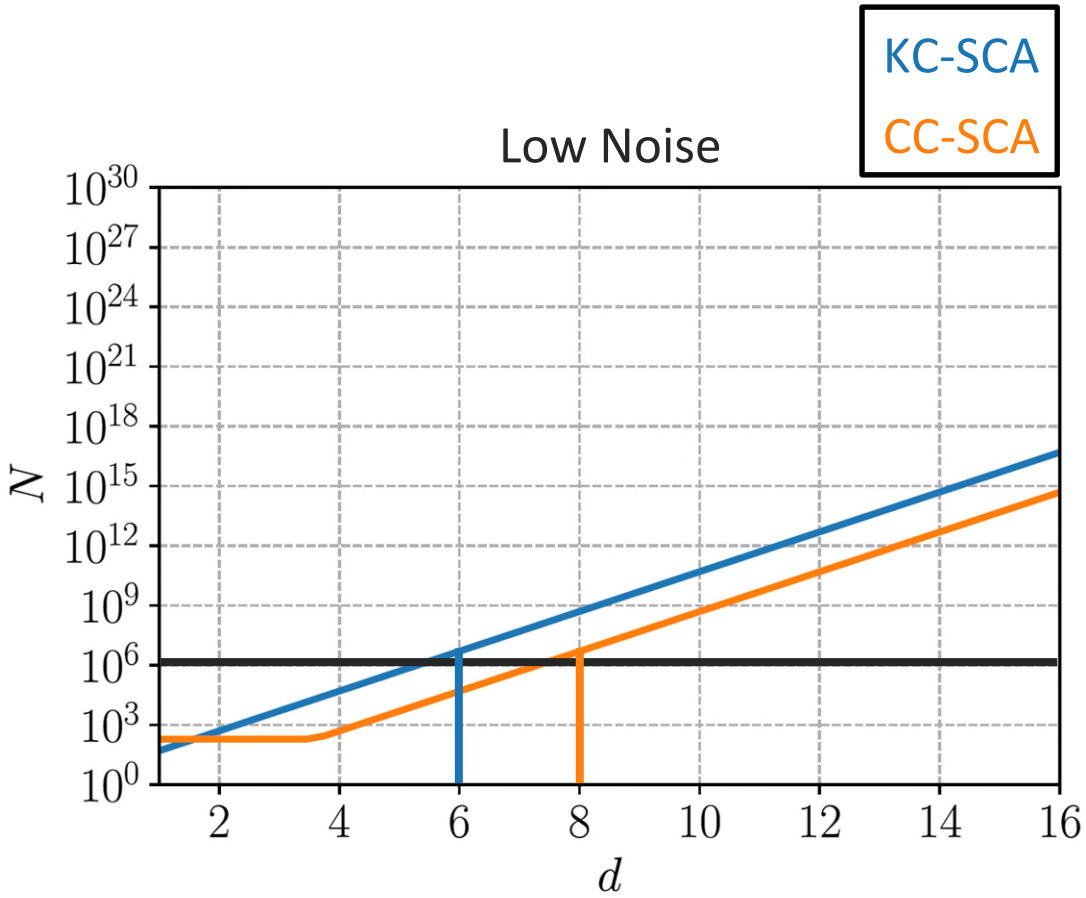
Higher *d* = Higher security + Increased cost

Pre-Quantum: Certified industrial solutions **d = 2-3**

For **low noise**:

- Known ciphertext ➔ d = 6
- Chosen ciphertext ➔ d = 8

FO leakage causes an increase of **2** shares.



CASE STUDY: MASKED KYBER

Split variables into *d* **shares**.

Higher *d* = Higher security + Increased cost

Pre-Quantum: Certified industrial solutions **d = 2-3**

For **low noise**:

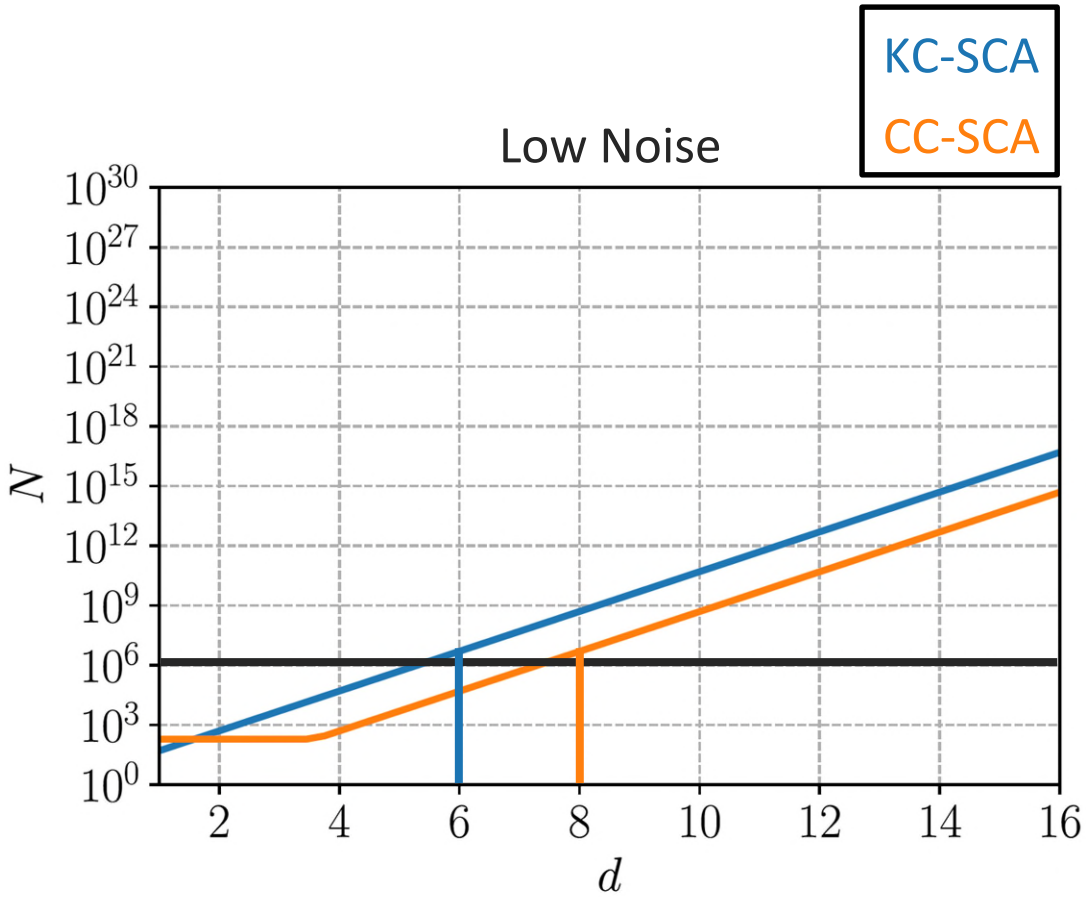
- Known ciphertext ➔ d = 6
- Chosen ciphertext ➔ d = 8

FO leakage causes an increase of **2** shares.

For **high(er) noise**:

- Known ciphertext ➔ d = 2
- Chosen ciphertext ➔ d = 3

FO leakage causes an increase of **1** share.



Survival in the FO-CALYPSE

SECURE CONNECTIONS
FOR A SMARTER WORLD

SURVIVAL STRATEGIES

Higher-Order Masking

Case Study: Higher-order masked Kyber (M4) from [BGR+21]
(with adapted A2B)

Overhead compared to unprotected (d=1):

d=2	d=3	d=4	d=5	d=6	d=7
3.5x	64x	110x	197x	293x	397x

[BGR+21] Bos et al.: Masking Kyber, TCHES-2021

SURVIVAL STRATEGIES

Higher-Order Masking

Case Study: Higher-order masked Kyber (M4) from [BGR+21]
(with adapted A2B)

Overhead compared to unprotected (d=1):

d=2	d=3	d=4	d=5	d=6	d=7
3.5x	64x	110x	197x	293x	397x

High(er)

[BGR+21] Bos et al.: Masking Kyber, TCHES-2021

SURVIVAL STRATEGIES

Higher-Order Masking

Case Study: Higher-order masked Kyber (M4) from [BGR+21]
(with adapted A2B)

Overhead compared to unprotected (d=1):

d=2	d=3	d=4	d=5	d=6	d=7
3.5x	64x	110x	197x	293x	397x

18x → High(er)

[BGR+21] Bos et al.: Masking Kyber, TCHES-2021

SURVIVAL STRATEGIES

Higher-Order Masking

Case Study: Higher-order masked Kyber (M4) from [BGR+21]
(with adapted A2B)

Overhead compared to unprotected (d=1):

d=2	d=3	d=4	d=5	d=6	d=7	
3.5x	64x	110x	197x	293x	397x	N/A*
18x	High(er)			?		Low

* For this specific implementation + board.

Requires further stack usage optimization.

[BGR+21] Bos et al.: Masking Kyber, TCHES-2021

SURVIVAL STRATEGIES

Higher-Order Masking

Case Study: Higher-order masked Kyber (M4) from [BGR+21]
(with adapted A2B)

Overhead compared to unprotected (d=1):

d=2	d=3	d=4	d=5	d=6	d=7	N/A*
3.5x	64x	110x	197x	293x	397x	Low

18x → High(er)

? → Low

* For this specific implementation + board.

Requires further stack usage optimization.

Leakage caused by the FO significantly increases deployment costs of affected KEMs

[BGR+21] Bos et al.: Masking Kyber, TCHES-2021

SURVIVAL STRATEGIES

Alternative Solution: Encrypt-then-Sign KEM *(work-in-progress)*

Replace FO check by **signature verification** for some use cases

- Uses less shares because no FO leakage
- Verification only with public values (no SCA protection)

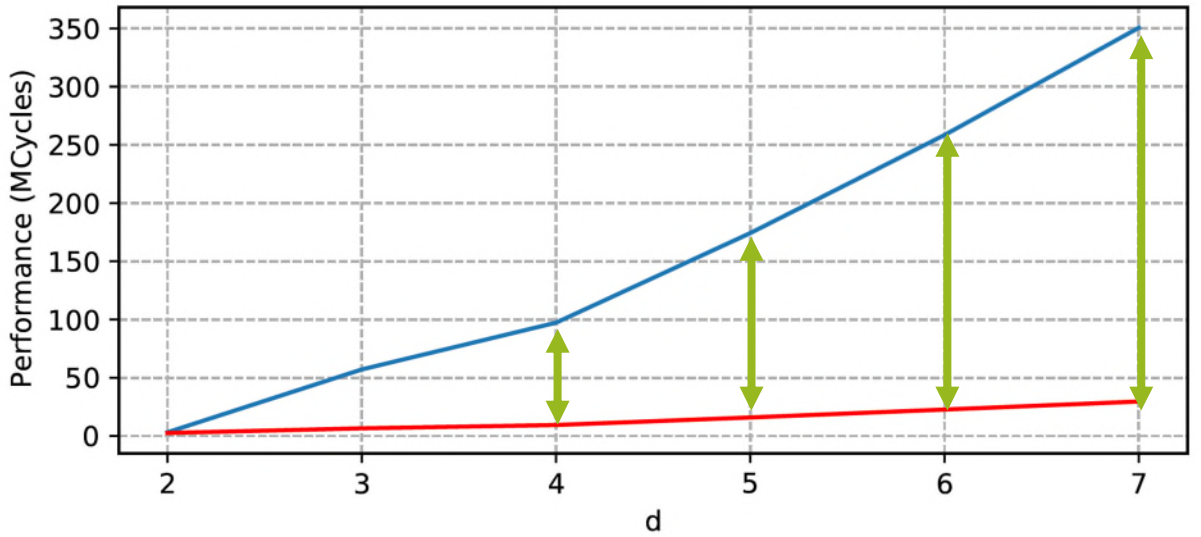
SURVIVAL STRATEGIES

Alternative Solution: Encrypt-then-Sign KEM *(work-in-progress)*

Replace FO check by **signature verification** for some use cases

- Uses less shares because no FO leakage
- Verification only with public values (no SCA protection)

Example: Kyber + Dilithium



Speed-Up

~10x

SURVIVAL STRATEGIES

Alternative Solution: Adapt the FO before standardization

Add a mechanism to avoid SCA-relevant chosen ciphertexts.

- Filter low-entropy ciphertexts [XPR+20]
- Does not cover border-failure SCA strategies

[XPR+20] Xu et al.:
Magnifying Side-Channel Leakage of Lattice-Based Cryptosystems with Chosen Ciphertexts: The Case Study of Kyber, IEEE-TC 2021

SURVIVAL STRATEGIES

Alternative Solution: Adapt the FO before standardization

Add a mechanism to avoid SCA-relevant chosen ciphertexts.

- Filter low-entropy ciphertexts [XPR+20]
- Does not cover border-failure SCA strategies

Randomize the re-encryption.

- Determinism a big factor in the SCA on the FO.
- Would reduce number of variables that can be (easily) predicted.

[XPR+20] Xu et al.:
Magnifying Side-Channel Leakage of Lattice-Based Cryptosystems with Chosen Ciphertexts: The Case Study of Kyber, IEEE-TC 2021

SURVIVAL STRATEGIES

Alternative Solution: Adapt the FO before standardization

Add a mechanism to avoid SCA-relevant chosen ciphertexts.

- Filter low-entropy ciphertexts [XPR+20]
- Does not cover border-failure SCA strategies

Randomize the re-encryption.

- Determinism a big factor in the SCA on the FO.
- Would reduce number of variables that can be (easily) predicted.

Replace it with something completely new.

- Discussion zero-knowledge proof alternative [ABH+21]

[XPR+20] Xu et al.:
Magnifying Side-Channel Leakage of Lattice-Based Cryptosystems with Chosen Ciphertexts: The Case Study of Kyber, IEEE-TC 2021

[ABH+21] Azouaoui et al.:
Systematic Study of Decryption and Re-Encryption Leakage: the Case of Kyber, COSADE 2022

CONCLUSIONS

FO leakage will complicate the integration of PQC KEM’s.

CONCLUSIONS

FO leakage will complicate the integration of PQC KEM's.

Will it make it impossible?

Probably not in noisy environments.

CONCLUSIONS

FO leakage will complicate the integration of PQC KEM's.

Will it make it impossible?

Probably not in noisy environments.

But it comes at a price.

Further research required.

CONCLUSIONS

FO leakage will complicate the integration of PQC KEM's.

Will it make it impossible?

Probably not in noisy environments.

But it comes at a price.

Further research required.

CONTACT: PQC@NXP.COM | NXP.COM/PQC

PQC-FORUM: PQC-FORUM/C/IVBJKCYTOOG

THANK YOU.

QUESTIONS?

SECURE CONNECTIONS
FOR A SMARTER WORLD

SECURE CONNECTIONS
FOR A SMARTER WORLD