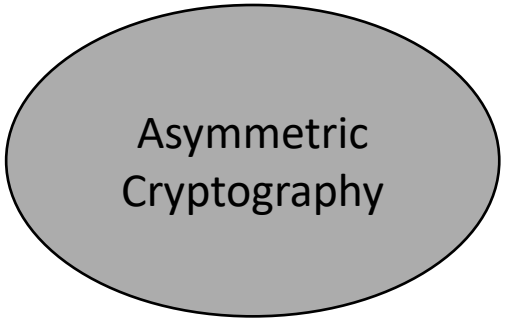
Sponge-based Authenticated Encryption: Security against Quantum Attackers

Christian Janson and Patrick Struck

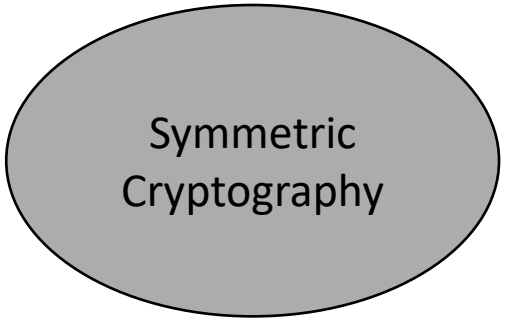
Universität Regensburg

PQCrypto 2022

Motivation



- Shor's algorithm breaks many underlying hardness assumptions
  - Post-quantum cryptography (lattices, codes, multivariate, hash, isogenies)
- Grover's algorithm provides speed-up for finding collisions
  - Double the output length of hash functions

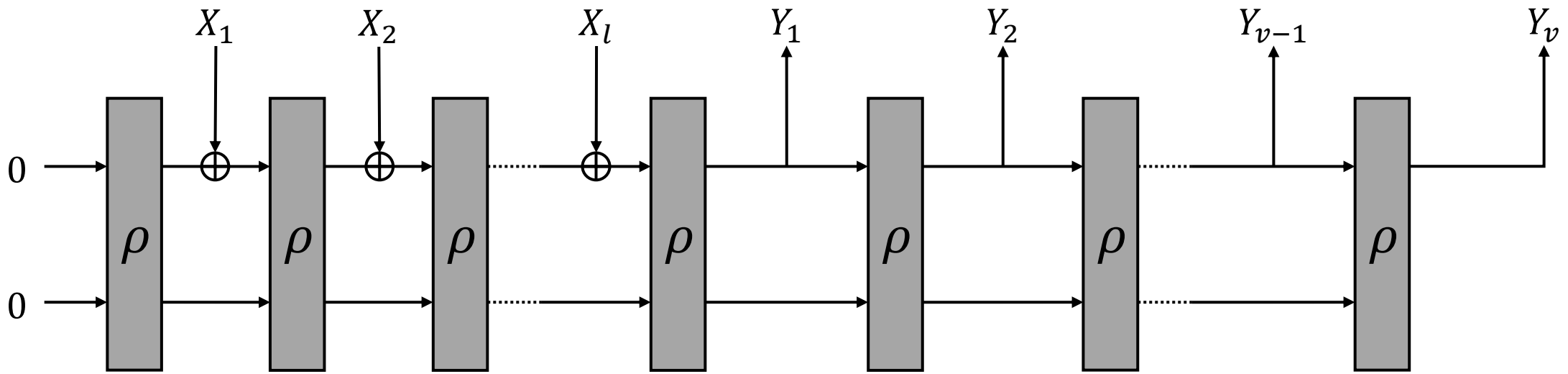


- Grover's algorithm provides speed-up for brute-force search of the key space
  - Double the key length
- [BSS22] shows that better attacks are possible
  - Analyzing security is important

[BSS22] Bonnetain, Schrottenloher, Sibleyras. Beyond quadratic speedups in quantum attacks on symmetric schemes. EUROCRYPT 2022

Sponge-based Authenticated Encryption

- SLAE: Sponge-based leakage-resilient authenticated encryption scheme [DJS19]
  - Designed to resist side-channel leakage
  - Design is closely related to/inspired by ISAP [DEMMU17]
  - Entirely based on T-Sponges, i.e., ρ is a random function



[DJS19] Degabriele, Janson, Struck. Sponges resist leakage: The case of authenticated encryption. ASIACRYPT 2019
[DEMMU17] Dobraunig, Eichlseder, Mangard, Mendel, Unterluggauer. ISAP – towards side-channel secure authenticated encryption. ToSC 2017

The FGHF' Construction

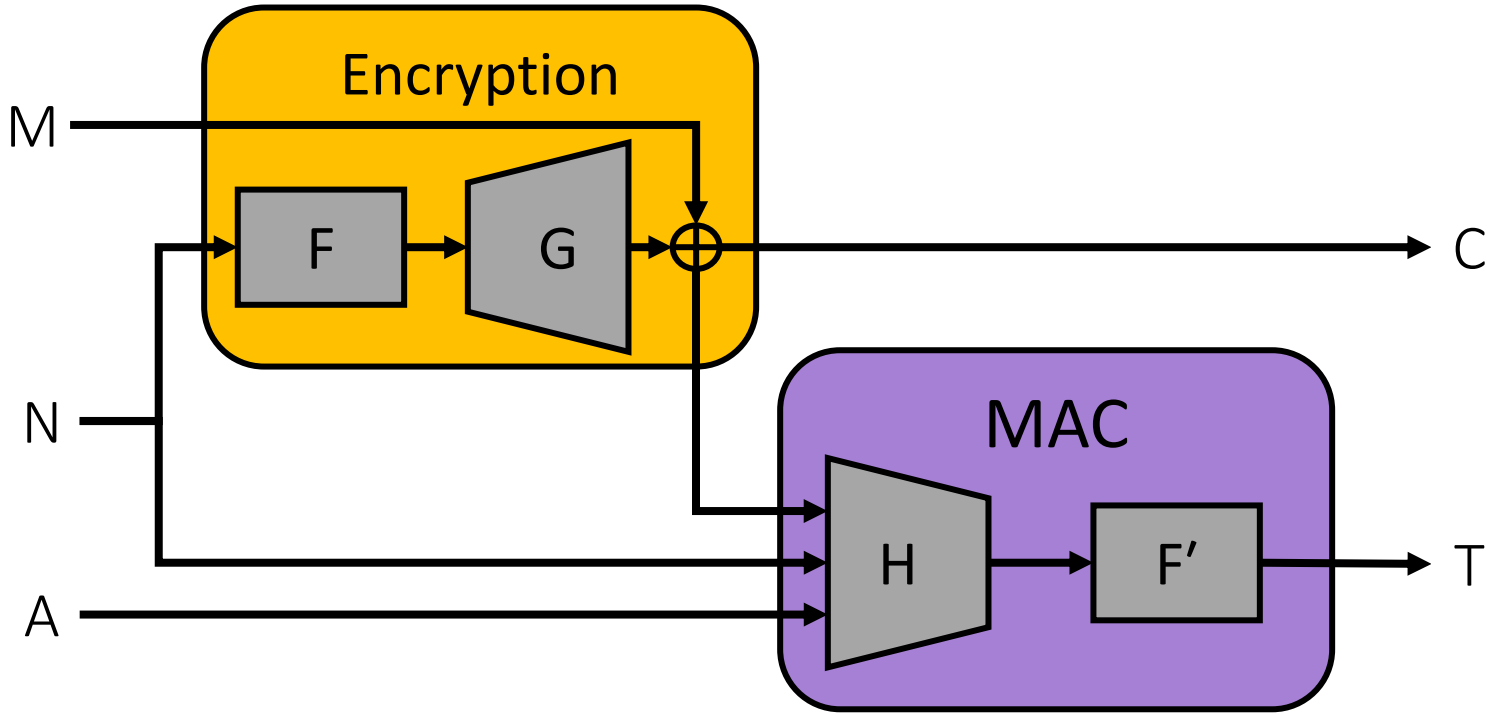
Construction follows the Encrypt-then-MAC paradigm

F — Fixed-input-length function

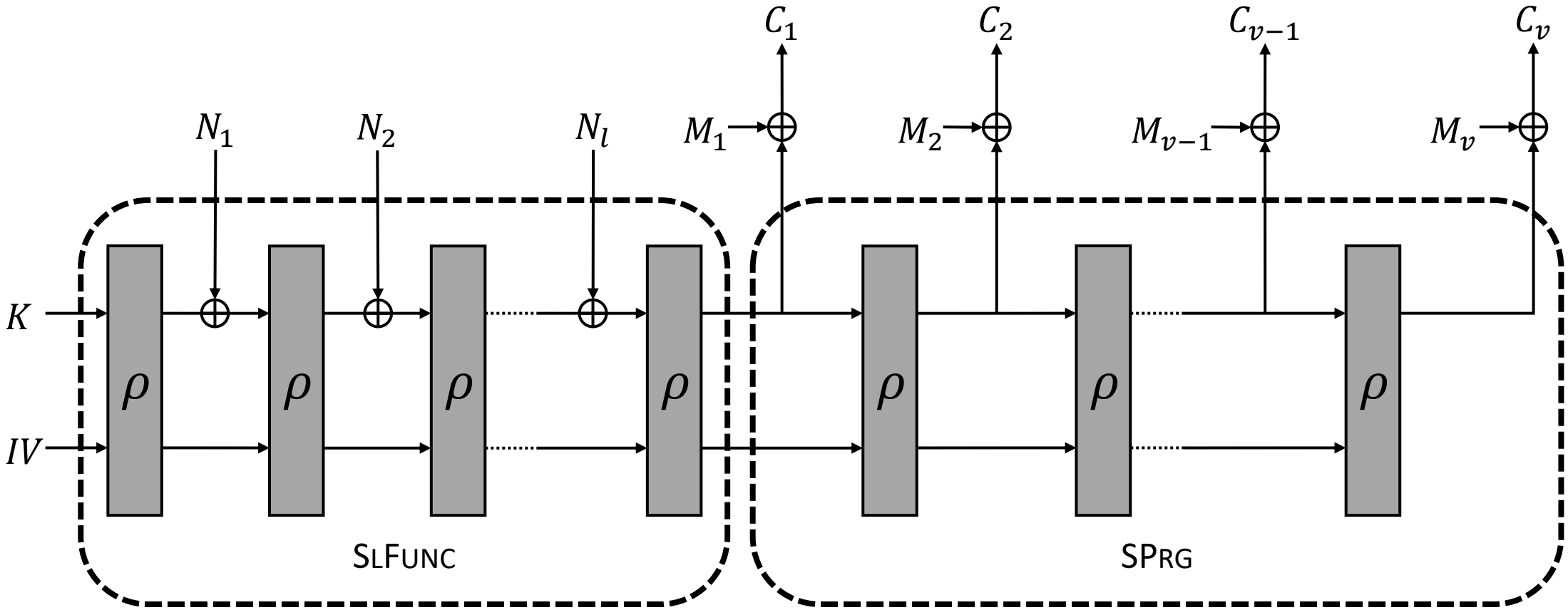
G — Pseudorandom generator

H — Vector hash function

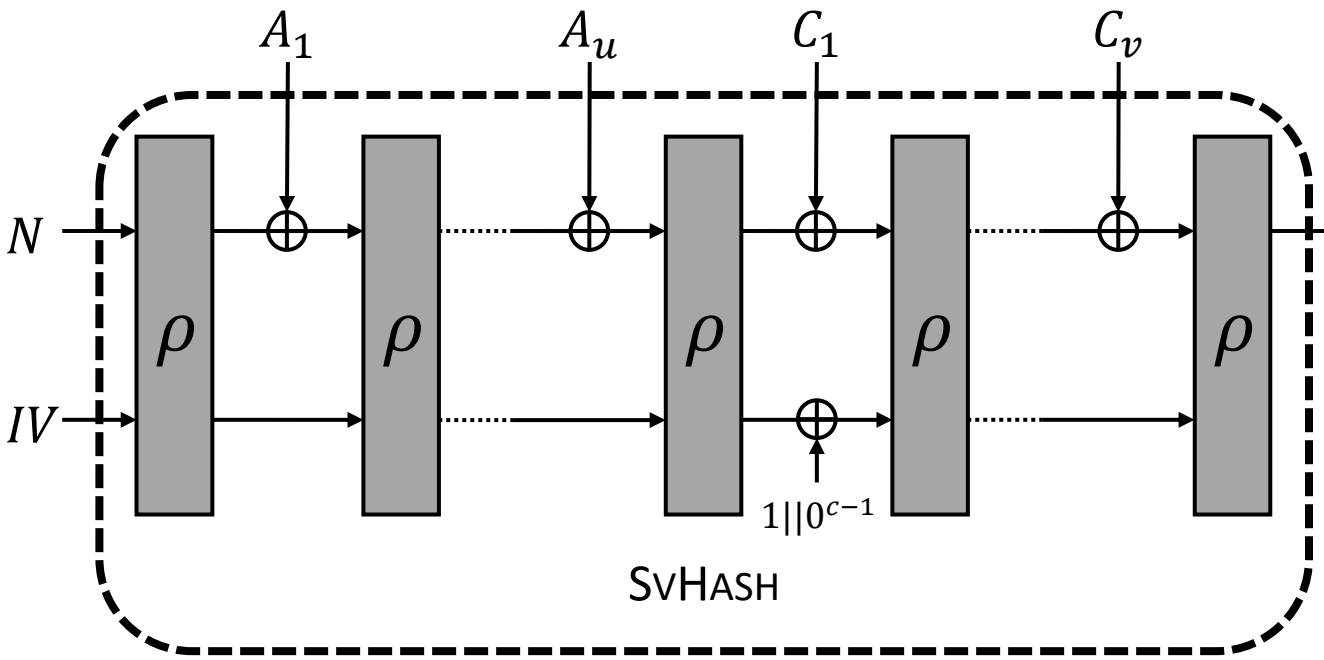
F' — Fixed-input-length function

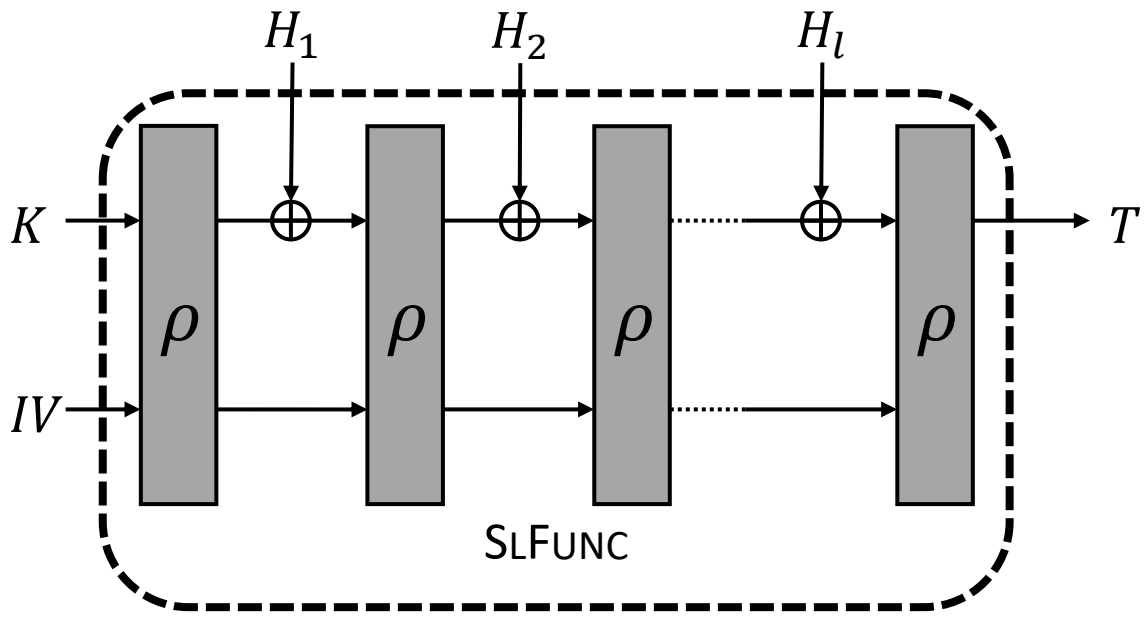


Sponge-based Encryption SLENC



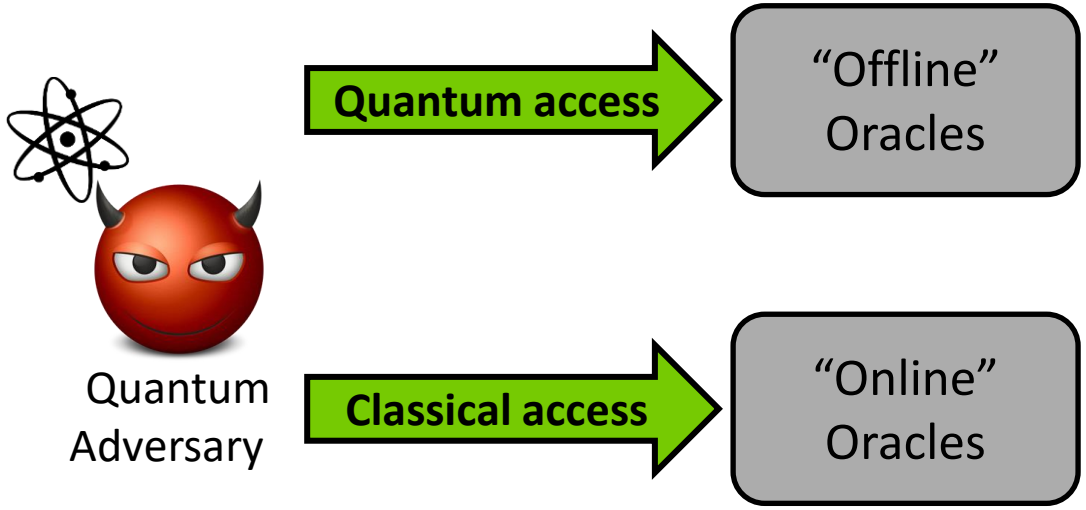
Sponge-based MAC SLMAC





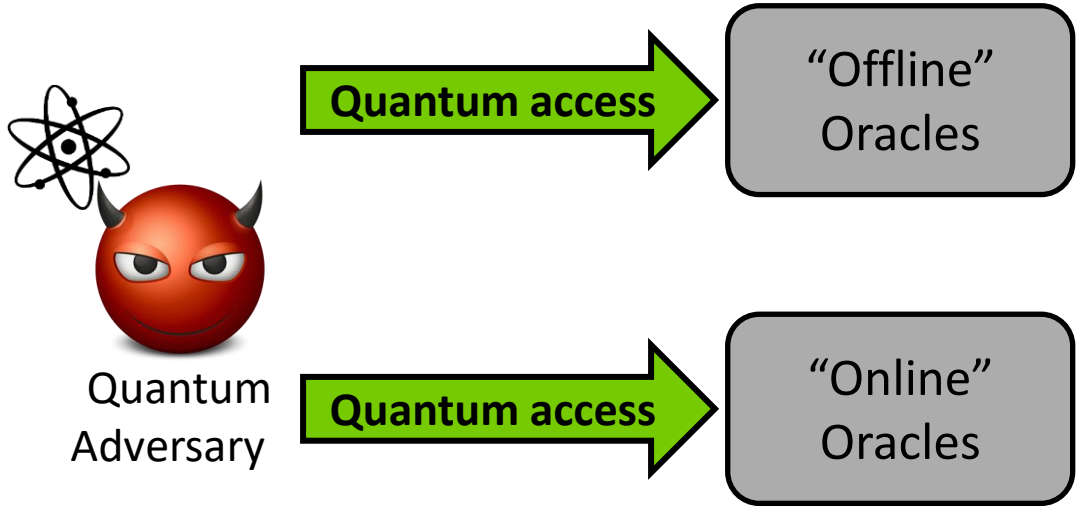
Security of SLAE against Quantum Attackers

Post-Quantum/Q1 Security



- Offline oracles: transformation ρ
- Online oracles: challenger provided oracles

Quantum/Q2 Security



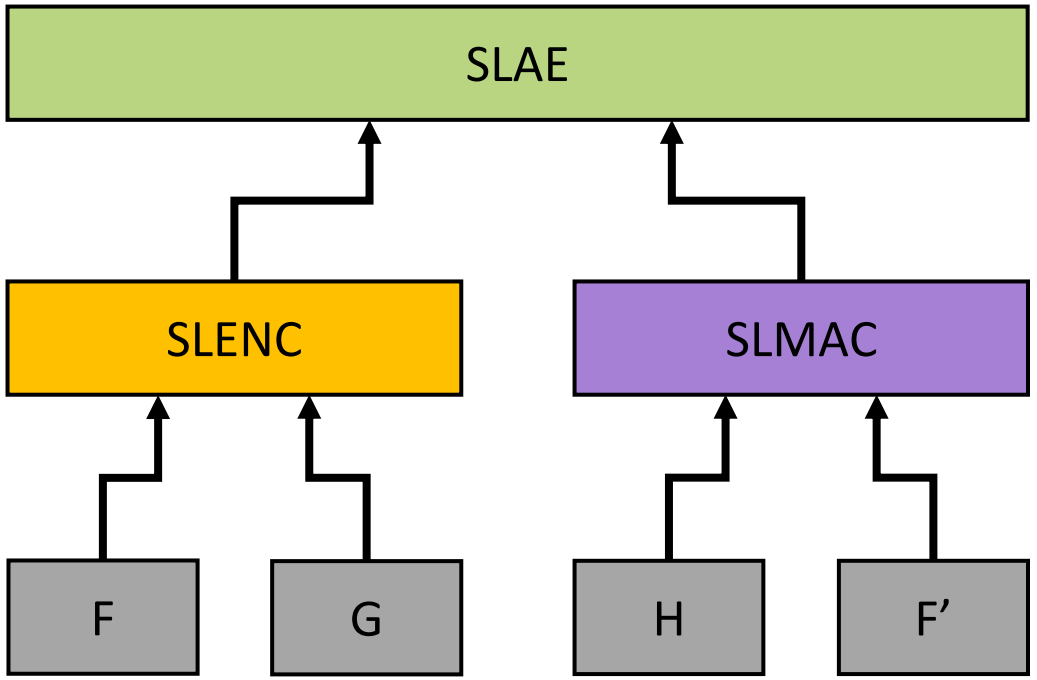
- Only consider SLENC
- Several security notions
  - INDqCPA [BZ13]
  - qINDqCPA [GHS16,MS16]

[BZ13] Boneh, Zhandry. Secure signatures and chosen ciphertext security in a quantum computing world. CRYPTO 2013
[GHS16] Gagliardoni, Hülsing, Schaffner. Semantic security and indistinguishability in the quantum world. CRYPTO 2016
[MS16] Mossayebi, Schack. Concrete security against adversaries with quantum superposition access to encryption and decryption oracles. arXiv 2016

Post-Quantum/Q1 Security of SLAE

- Leakage-resilient security of SLAE reduces to the leakage-resilient security of the underlying components

- Post-quantum security of SLAE also reduces to the post-quantum security of the underlying components



Post-Quantum/Q1 Security

- Post-quantum security of the pseudorandom function:
  - O2H Lemma

$$Adv^{PRF}(A) \leq \frac{q_F^2 + q_F}{2^{n+1}} + 2q\sqrt{\frac{2^v}{2^n}}$$

- Post-quantum security of the pseudorandom generator:
  - O2H Lemma

$$Adv^{PRG}(A) \leq \frac{2lq}{\sqrt{2^c}}$$

- Post-quantum security of the hash function:
  - [CGHSU18]

$$Adv^{CR}(A) \leq \sqrt{\epsilon_1} + l\epsilon_2 + \epsilon_3,$$

where $\epsilon_1 \leq (q+1)^2 2^{-c+4}, \epsilon_2 \leq q^3\left(\frac{\delta'+324}{2^{c-1}}\right) + 7\delta\sqrt{\frac{3(q+4)^3}{2^c}}, \epsilon_3 \leq q^3\left(\frac{\delta'+324}{2^{w+1}}\right) + 7\delta\sqrt{\frac{3(q+4)\text{^}3}{2^{w+2}}}$

[CGHSU18] Czajkowski, Groot Bruinderink, Hülsing, Schaffner, Unruh. Post-quantum security of the sponge-construction. PQCrypto 2018

Quantum/Q2 Security

- Several notions [BZ13,GHS16,MS16]

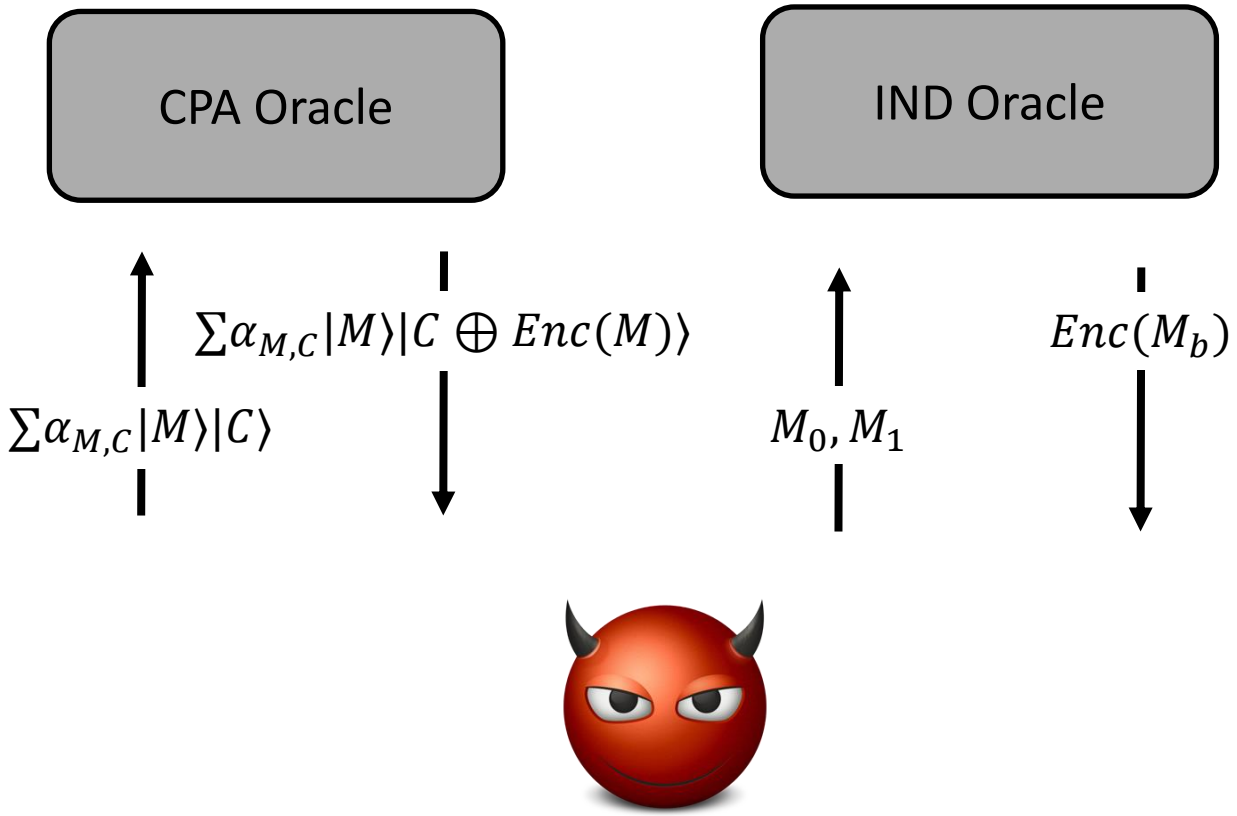
- All consider the randomness (the nonce) to be classical
  - Challenger measures the nonce and rejects a query if a nonce repeats
  - For classical nonces this is equivalent to nonce-respecting adversaries

[BZ13] Boneh, Zhandry. Secure signatures and chosen ciphertext security in a quantum computing world. CRYPTO 2013
[GHS16] Gagliardoni, Hülsing, Schaffner. Semantic security and indistinguishability in the quantum world. CRYPTO 2016
[MS16] Mossayebi, Schack. Concrete security against adversaries with quantum superposition access to encryption and decryption oracles. arXiv 2016

INDqCPA Security

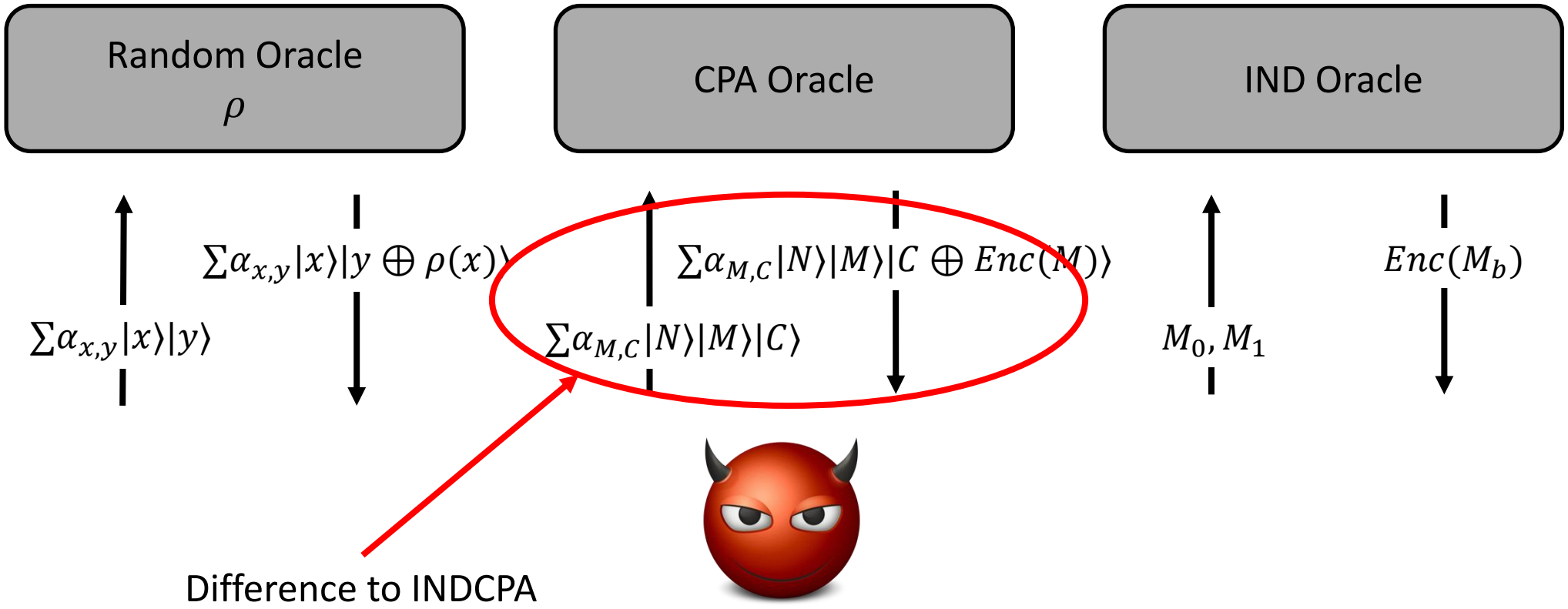
- Boneh and Zhandry [BZ13]

- Encryption oracles
  - Quantum access to the CPA oracle
  - Classical access to the IND oracle



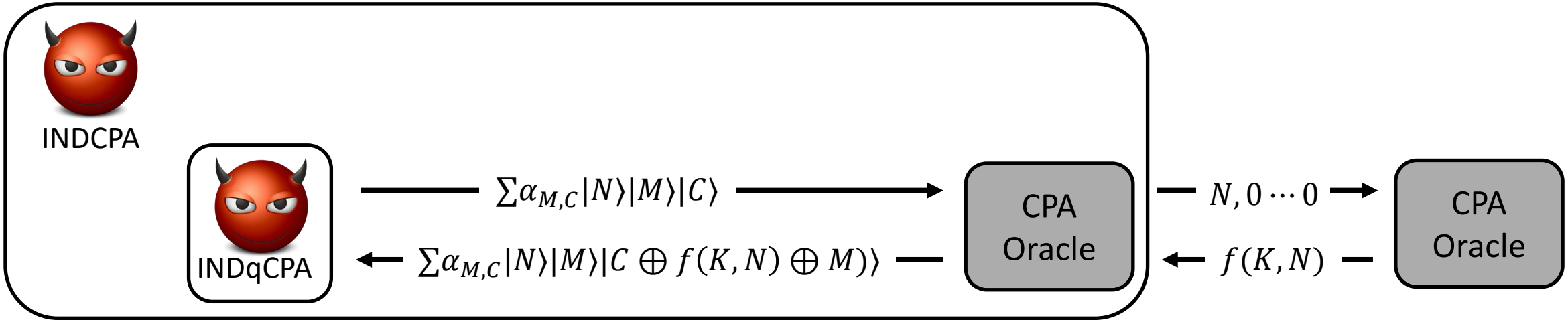
[BZ13] Boneh, Zhandry. Secure signatures and chosen ciphertext security in a quantum computing world. CRYPTO 2013

INDqCPA Security of SLENC



INDqCPA Security of SLENC

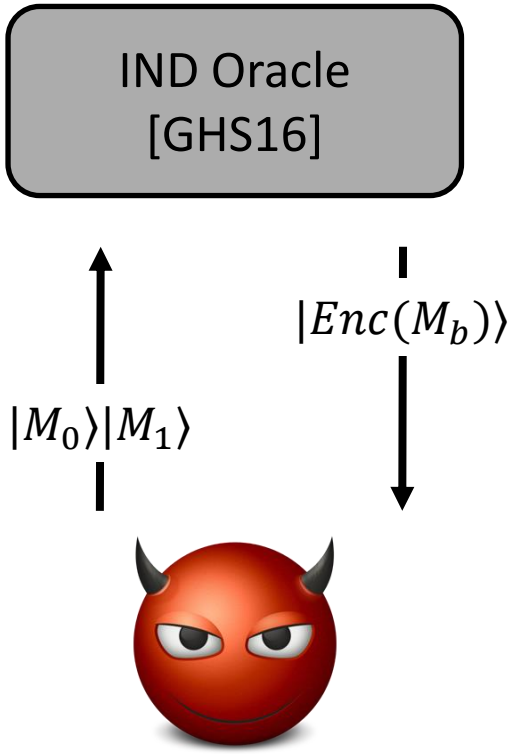
- SLENC is a stream cipher
  - $Enc(K, N, M) = f(K, N) \oplus M$
- [ATTU16] shows that INDCPA (Q1) security implies INDqCPA (Q2) security for stream ciphers
  - Keystream only depends on the key and the nonce, hence it is classical

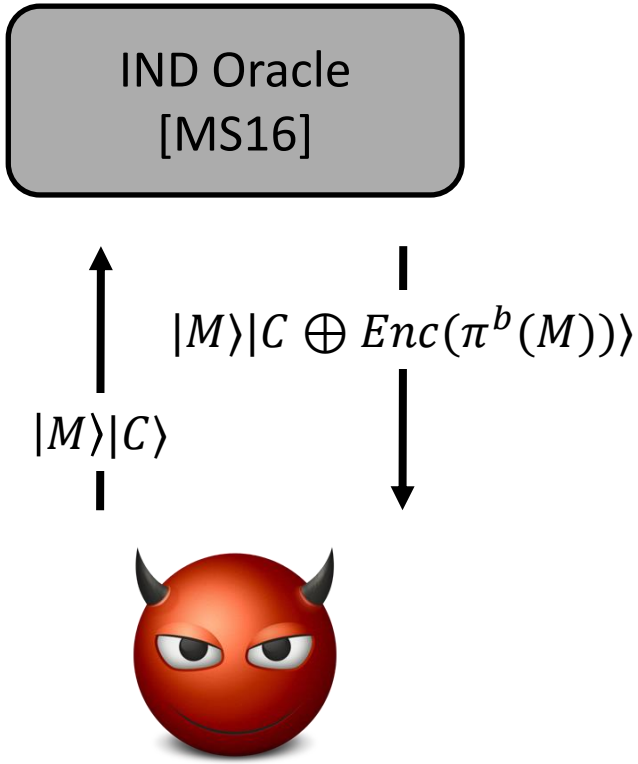


[ATTU16] Anand, Targhi, Tabia, Unruh. Post-quantum security of the cbc, cfb, ofb, and xts modes of operation. PQCrypto 2016

qINDqCPA Security of SLENC

- Two security notions



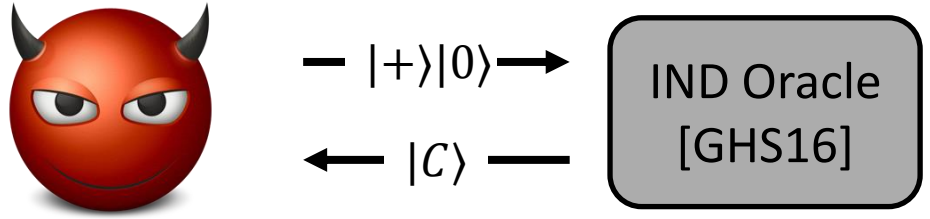


[GHS16] Gagliardoni, Hülsing, Schaffner. Semantic security and indistinguishability in the quantum world. CRYPTO 2016
[MS16] Mossayebi, Schack. Concrete security against adversaries with quantum superposition access to encryption and decryption oracles. arXiv 2016

qINDqCPA Security of SLENC

- SLENC is insecure due to being a stream cipher
  - Generic attack [GHS16]
  - "Quasi-length-preserving" encryption

- If $b = 0$: $|C\rangle = |+\rangle$
- If $b = 1$: $|C\rangle = |R\rangle$, for some random R



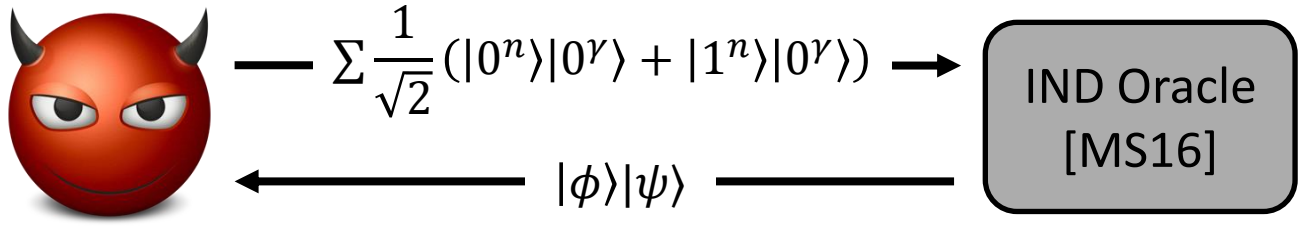
- Distinguishable by Hadamard+Measurement

[GHS16] Gagliardoni, Hülsing, Schaffner. Semantic security and indistinguishability in the quantum world. CRYPTO 2016

qINDqCPA Security of SLENC

- SLENC is insecure due to being a stream cipher
  - Attack given in [CEV20]

- If $b = 0$ (no permutation applied):
  - Hadamard+Measurement yields x and y s.t. $par(x) = par(y)$ with probability 1
- If $b = 1$ (permutation applied):
  - Hadamard+Measurement yields x and y s.t. $par(x) = par(y)$ with probability $^1/_2$



[CEV20] Chevalier, Ebrahimi, Vu. On security notions for encryption in a quantum world. ePrint 2020

Summary/Open Problems

- Security analysis of SLAE against quantum attackers
  - Post-quantum/Q1 security
  - Quantum/Q2 security
- Extend the results to ISAP
  - P-Sponge instead of a T-Sponge
- Post-quantum security + side-channel leakage

Thank You!

patrick.struck@ur.de

ePrint 2022/139