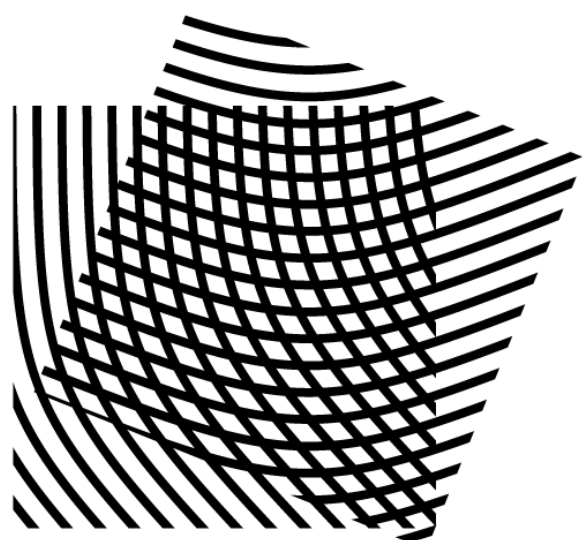


Lattice-Based Cryptography: beyond NIST Standardization

Suparna Kundu,

Ingrid Verbauwhede, Angshuman Karmakar

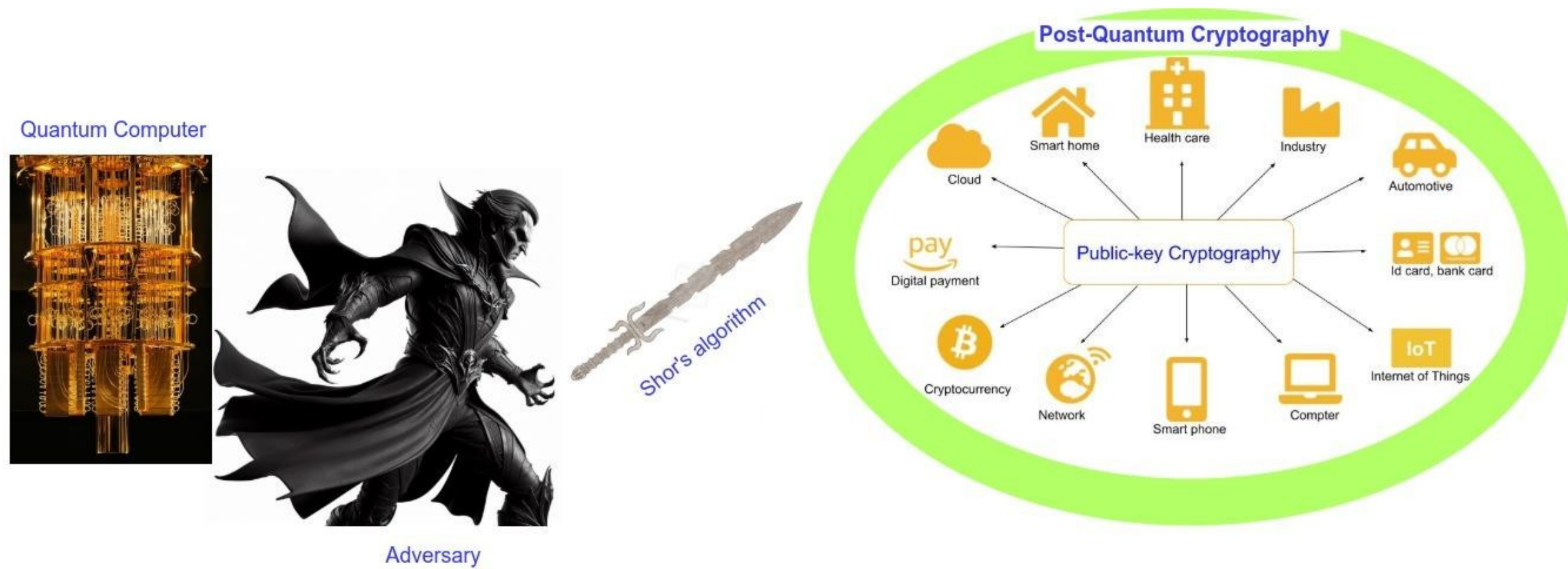
DATE 2025 PhD Forum, Lyon, France



COSIC

KU LEUVEN

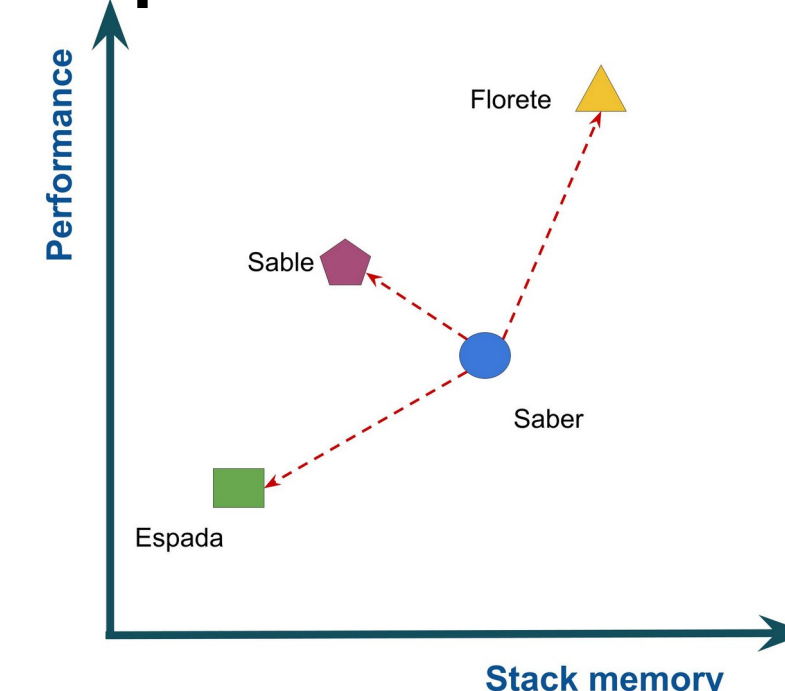
Introduction and background



- **NIST** initiated post-quantum standardization procedure and recently concluded
 - **KEM**: Kyber (aka ML-KEM), HQC
 - **DSA**: Dilithium, Falcon, SPHINCS+
- Relatively new and several deterrents for real-world deployment

Scabbard: A suite of PQ KEMs

- **Goal**: Use latest advancements in lattice-based (LWE and LWR) cryptography to create new / improve state-of-the-art KEMs
- **Contributions**:
 - **Florete**: Fast RLWR KEM
 - **Espada**: Compact, highly parallelizable MLWR KEM
 - **Sable**: compact MLWR KEM, modified Saber
 - Optimized for AVX2, μC , and HW-SW accelerators



μC , Cortex-M4 results

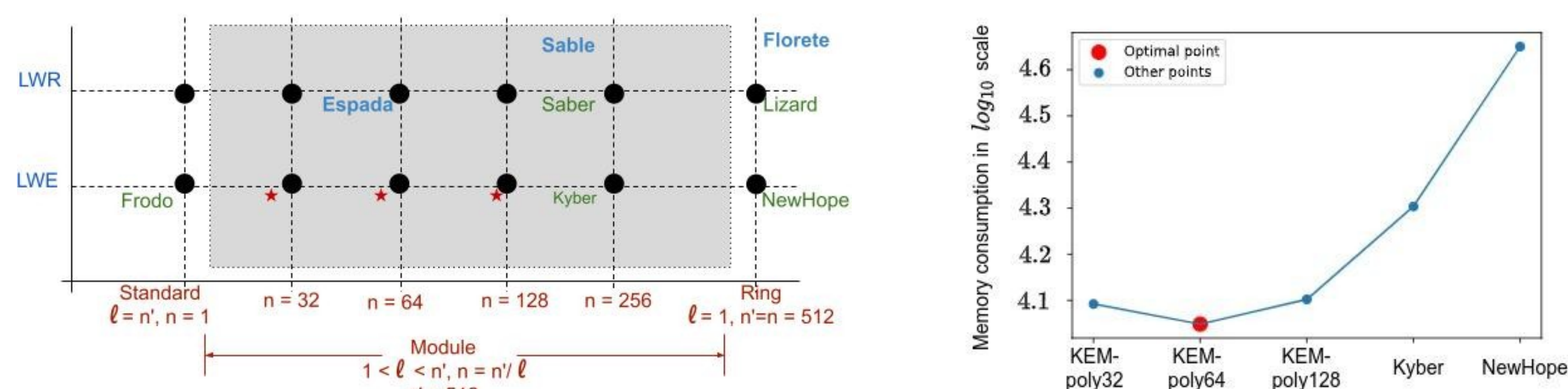
Florete: High Performance

Espada: Less Memory footprint

Sable: trade-off

Rudraksh: A lightweight PQ KEM

Prob: IoT devices have much less computing power, batteries, and other resources. Adding a KEM is tough

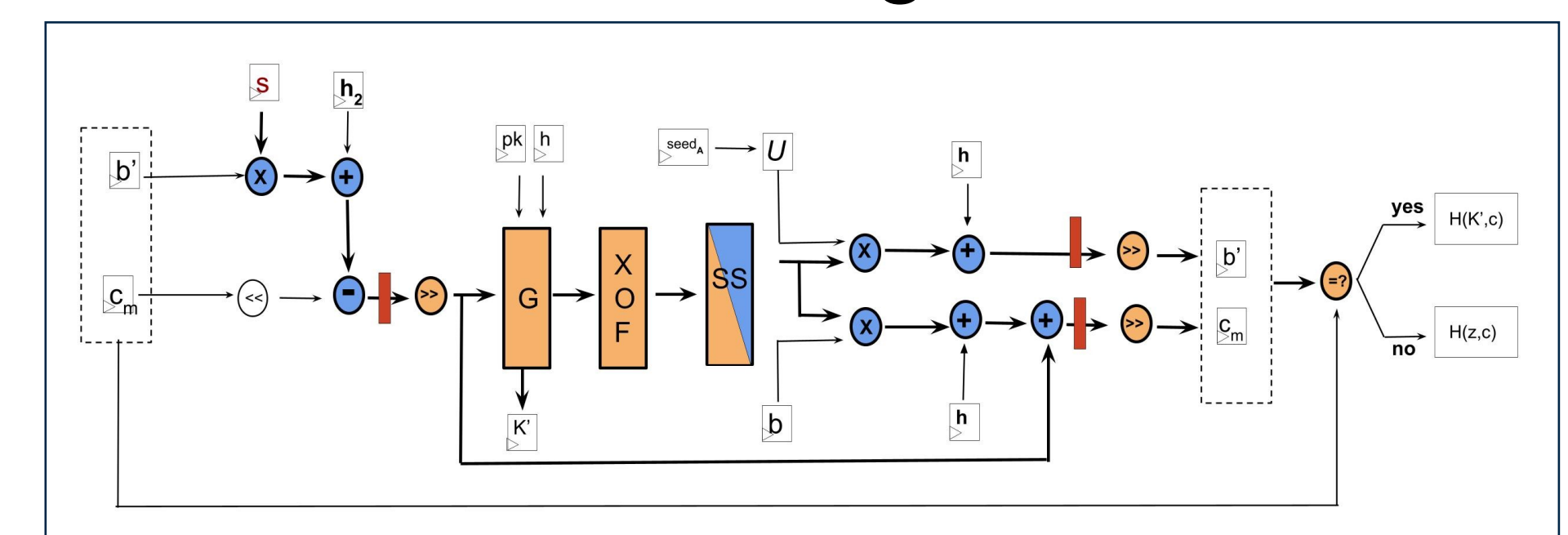


- We designed MLWE-based lightweight KEM Rudraksh at the **minima** of hardware requirement
- Application of ASCON: Used here as XOF
- **Results** compared to the state-of-the-art Kyber
 - **Area**: $\sim 3\times$ improvement
 - **Time-area-product**: $\sim 2\times$ improvement

Masking lattice-based KEMs

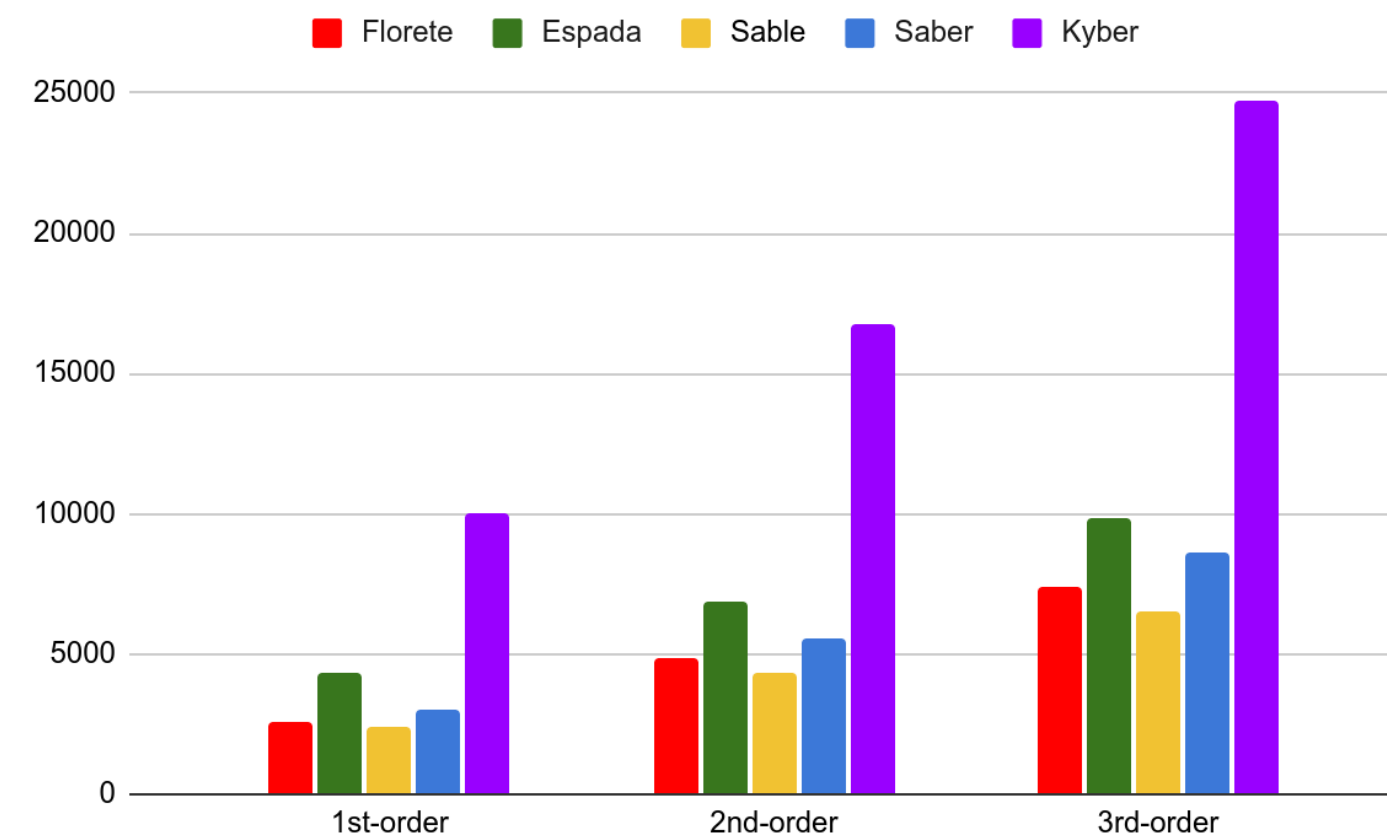
Prob: Lattice-based KEMs vulnerable against SCA

Sol: Masking prevents DPA
Ex: LWR KEM



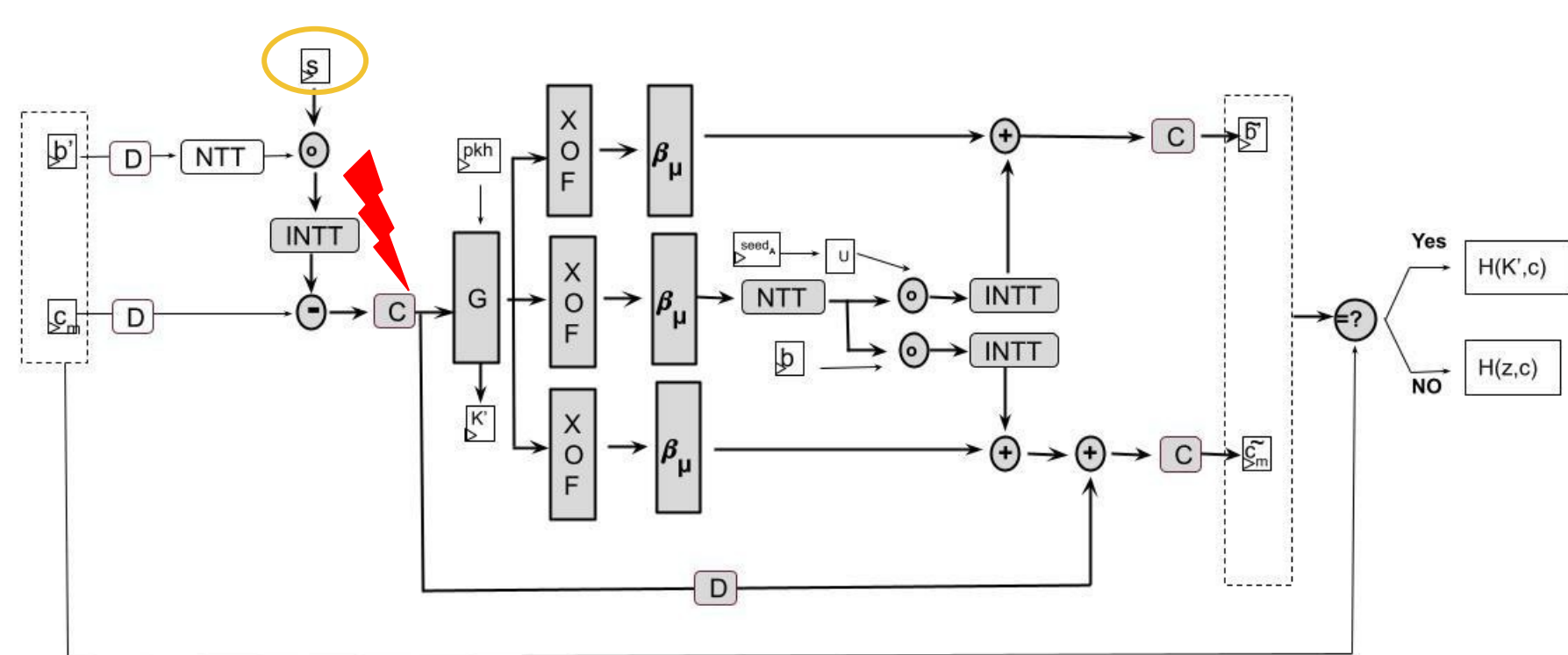
Legend for masking types:

- Arithmetic masking
- Both masking
- Boolean masking
- A2B conversion



- After masking LWR KEM outperforms LWE KEM
- Due to **power-of-2 moduli**
- LWR-KEM has less non-linear components

Cross-attacks on PQ KEMs



- Real-world adversaries are not limited to SCA
- We show a **fault attack** on masked Kyber and Saber
 - **Attack location**: Compression operation
 - **Fault type**: Stuck-at-1 bit fault
- This attack applicable to any LWE-based schemes
- Even to higher-order masked implementations
- **Attack on Kyber-512**: Only 10% successful fault injection and 1.9 M faults

Conclusion

- Improvements in post-quantum KEM designs
 - **Scabbard**: Improved SOTA LWR KEMs
 - **Rudraksh**: Lightweight KEM curated for resource constrained devices

- DPA secure implementations of LWE/LWR KEMs
 - **Masked LWR KEMs outperforms LWE KEMs**

- Cross-attacks on lattice-based KEMs
 - **It is first of its kind on PQC**

Bridged the gap between the theory and practice of PQC by addressing many open problems