

SECURE AND SCALABLE HARDWARE FOR POST-QUANTUM CRYPTOGRAPHY AND FULLY HOMOMORPHIC ENCRYPTION

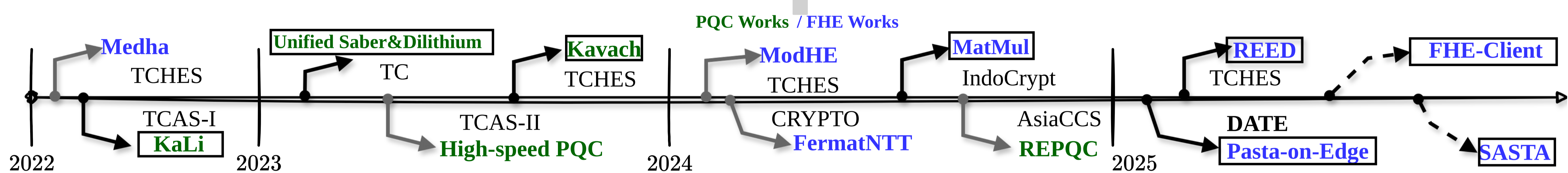
Aikata, Sujoy Sinha Roy

ISEC | Institute of Information Security - TU Graz



Pillar 1: Post-Quantum Cryptography (PQC)

- ❖ **Why PQC?** Classical cryptographic schemes like RSA and ECC are vulnerable to quantum attacks (e.g., using Shor's algorithm).
- ❖ **Foundation:** Schemes rely on problems that remain hard in a post-quantum world, such as **Lattice-Based Cryptography** (e.g., Kyber, Dilithium).
- ❖ **Challenges:** PQC schemes are still in their early stages of adoption, requiring well-defined **design methodologies** and rigorous **security analysis**.



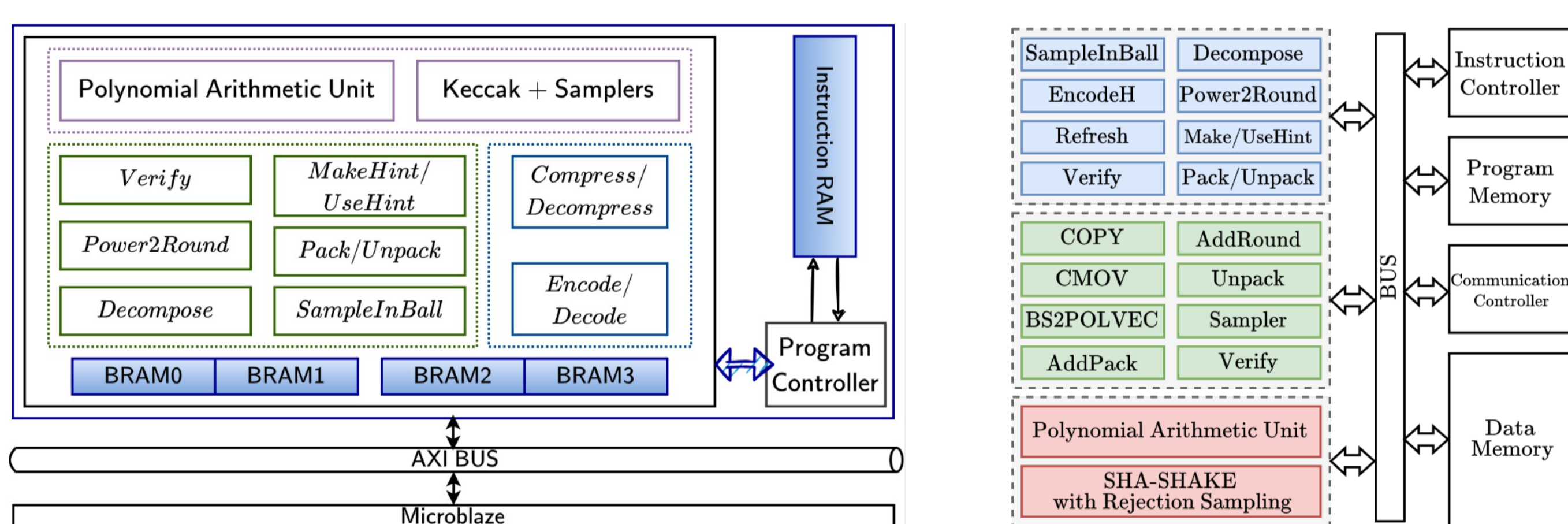
Pillar 2: Fully Homomorphically Encryption (FHE)

- ❖ **Why FHE?** Conventional encryption protects data at rest and in transit but exposes it during computation. FHE enables secure computations.
- ❖ **Foundation:** Most efficient FHE schemes rely on **Lattice-Based Cryptography**, for e.g., BGV and CKKS (supports approximate arithmetic for ML).
- ❖ **Challenges:** FHE operations are costly and memory-intensive, necessitating **acceleration** and **security analysis** for practical use.

Architecture Design Methodology

➤ **KaLi** - the *first-of-its-type* unified hardware architecture for PQC, with both-KEM (CRYSTALS-Kyber) and DSA (CRYSTALS-Dilithium), on 28nm.

➤ This state-of-the-art work reports **0.26 mm²** and **10× better performance**. We also offer this a full-fledged IP.

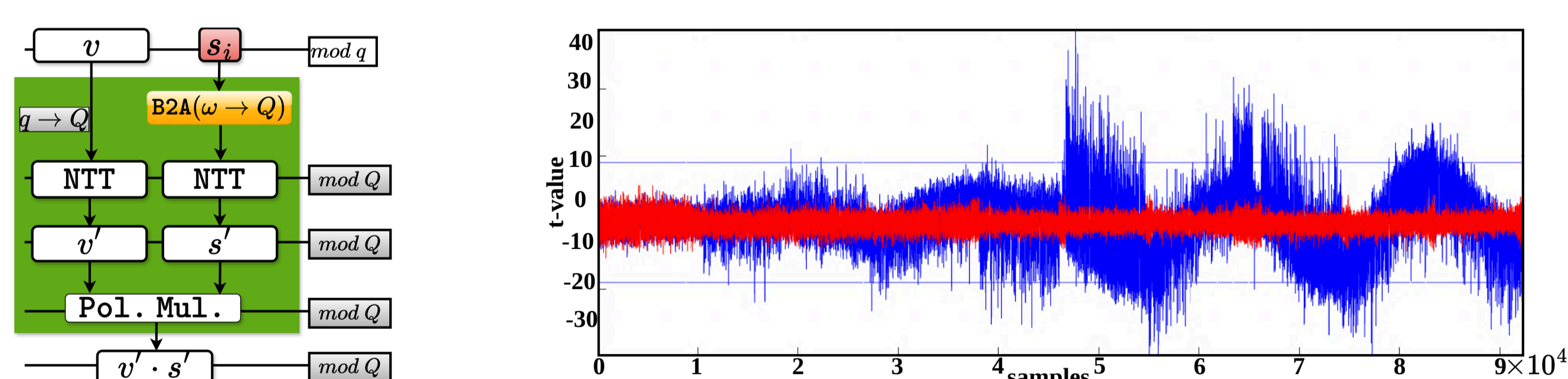


The **KaLi** and **SabDil** instruction set processor, which support **all security levels** stated by NIST.

Security Analysis

➤ **Kavach** develops novel techniques for **masked polynomial multiplication** to protect against side-channel attacks, validated through extensive TVLA tests.

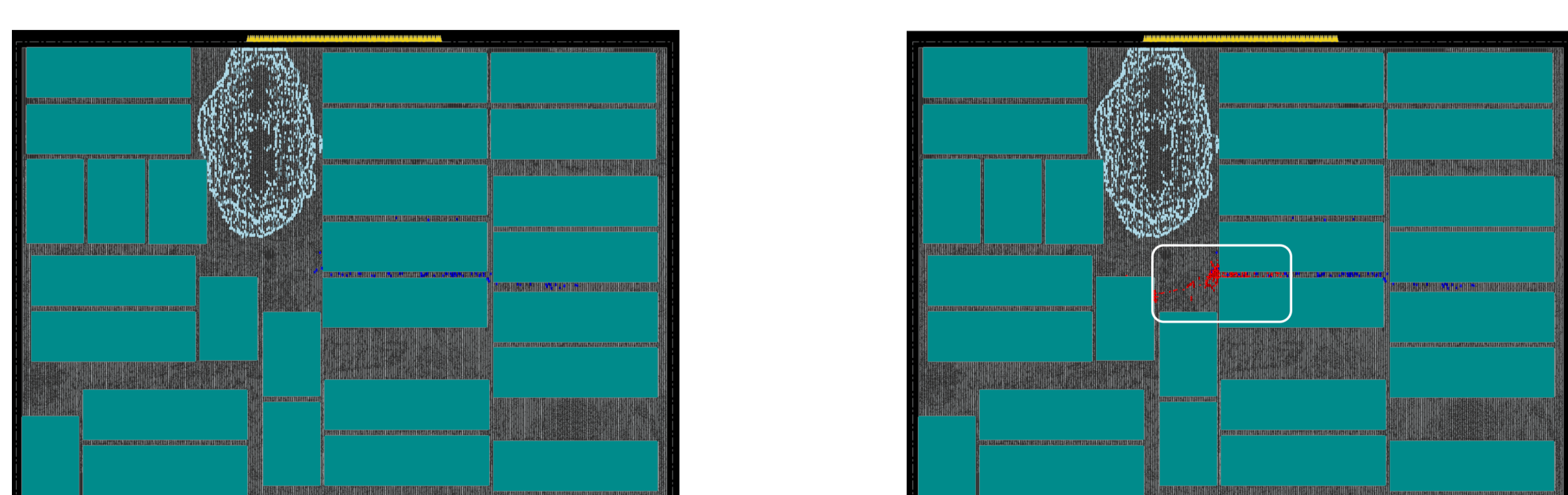
➤ The work enables **side-channel protected implementations** while retaining the performance benefits of compact multipliers.



The Kavach **masking technique** and **TVLA results** before (in blue) and after (in red) **masking**.

➤ **REPQC** is a **reverse engineering** algorithm which enables the insertion of stealthy **Hardware Trojan Horses** on PQC scheme CRYSTALS-Dilithium.

➤ **HTHs** increase the accelerator's layout density by as little as **0.1%** can be inserted without any impact on the performance of the circuit.

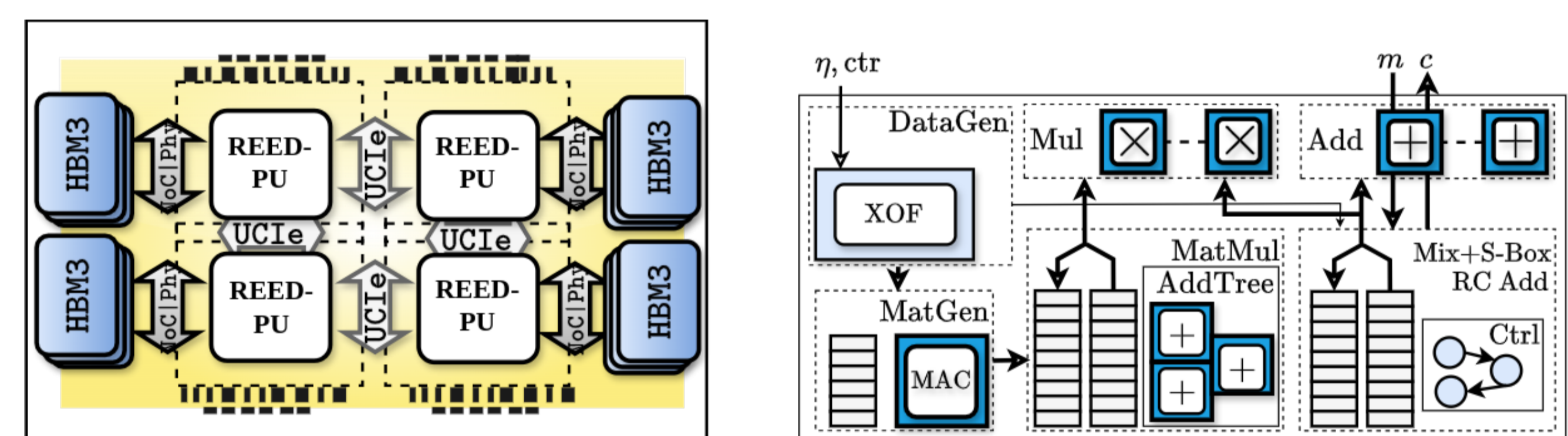


The **KaLi** processor in plain form (left) and with **Hardware Trojan** (right in red).

Architecture Design Methodology

➤ **REED** is a pioneering **multi-chiplet FHE accelerator** that addresses the limitations of monolithic works. We benchmark **DNN Training** to showcase utility.

➤ Implemented on 7nm technology, REED occupies **96.7 mm²** and achieves up to **2,991× speedup** over a CPU while reducing development costs by **50%**.



The **REED** chiplet-based FHE accelerator architecture and **PASTA** HHE edge-architecture.

➤ **Pasta-on-Edge** is a **RISC-V SoC** architecture for the **FHE client**. It reduces the communication and computation overhead using **Hybrid HE (HHE)**.

➤ It reports up to **97× better performance** compared to prior FHE-client acceleration works and occupies **1.8 mm²** on 130nm tech.

Security Analysis and Application

➤ **SASTA** is a novel **Differential Fault Analysis (DFA)** attack technique on HHE enabling schemes where a **single fault** can lead to complete key recovery.

➤ We demonstrate an **end-to-end key recovery** on ATXmega128D4-AU.

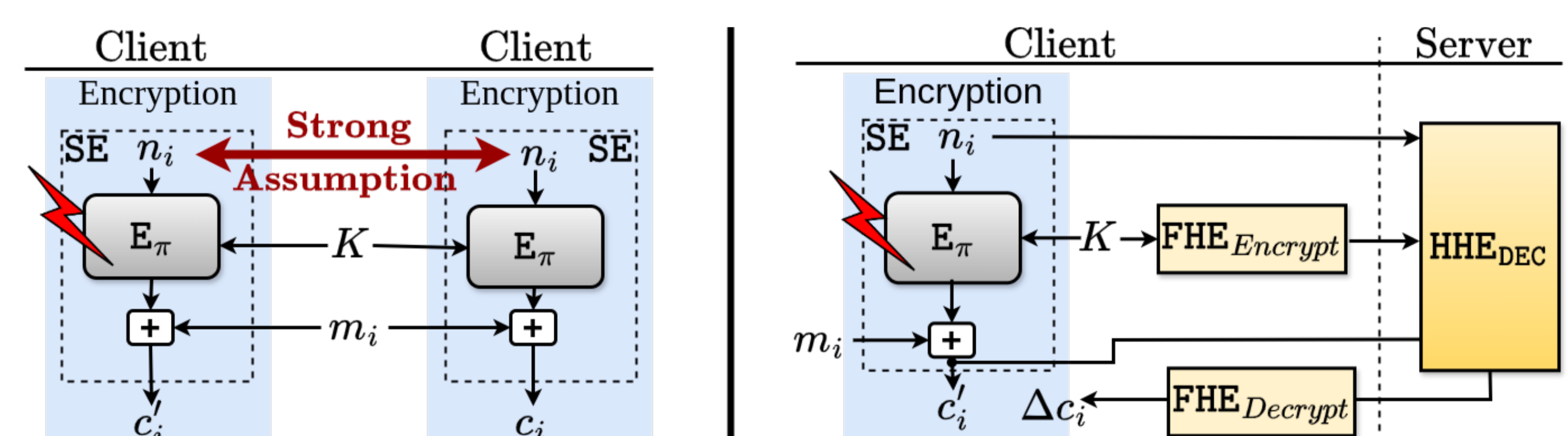


Figure depicting how the Standard DFA (left) differs from the **SASTA-DFA** (right).

➤ **MatMul** optimizes FHE-based matrix mult for **privacy-preserving NN**.

➤ The method lowers the **asymptotic complexity** from $\mathcal{O}(d)$ to $\mathcal{O}(\log d)$.

Conclusion.

Security and Privacy are a continuous pursuit, not a final destination.

This work proposes several secure and efficient architecture design techniques to ensure security and privacy are foundational and not optional.

➤ **What's Next?** Verifiability using Zero-Knowledge! (also **Lattice-Based** 😊)