RISC-V-based Acceleration Strategies for Post-Quantum Cryptography

IVAN SARNO
UNIV. GRENOBLE ALPES
CEA, LIST
F-38000 GRENOBLE, FRANCE
IVAN.SARNO@CEA.FR

STEFANO DI MATTEO
UNIV. GRENOBLE ALPES
CEA, LETI
F-38000 GRENOBLE, FRANCE
STEFANO.DIMATTEO@CEA.FR

EMANUELE VALEA
UNIV. GRENOBLE ALPES
CEA, LIST
F-38000 GRENOBLE, FRANCE
EMANUELE.VALEA@CEA.FR

CYRILLE CHAVET
UNIV. GRENOBLE ALPES
GRENOBLE INP, TIMA
F-38000 GRENOBLE, FRANCE
CYRILLE.CHAVET@UNIV-GRENOBLE-ALPES.FR

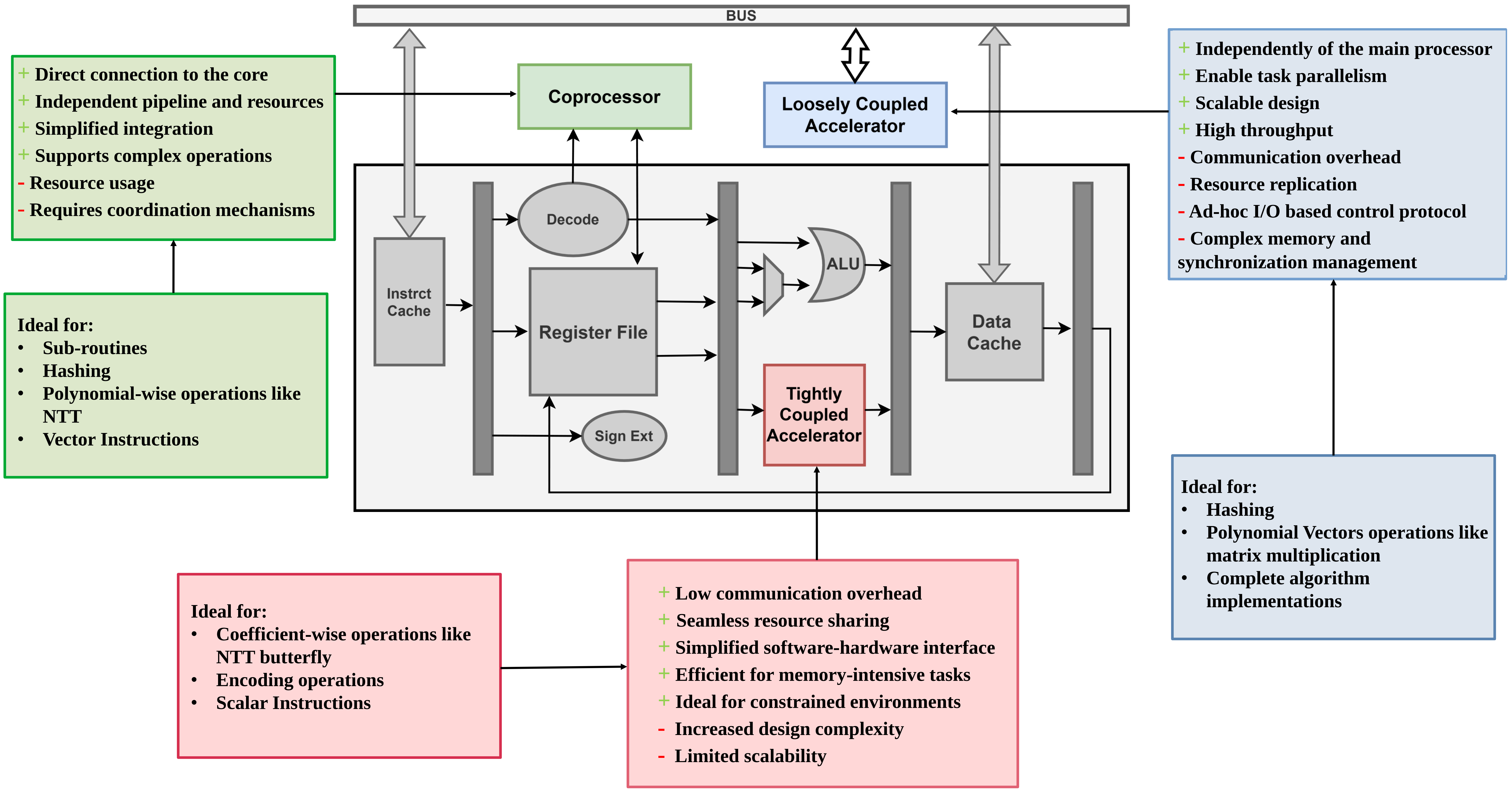
Context

The rise of quantum computing threatens current cryptographic systems, which could be broken using quantum algorithms. To address this, NIST has selected ML-KEM, ML-DSA, and SLH-DSA as future public key cryptography standards. SHA-3 hash function has been identified as a bottleneck for hash-based schemes, like SLH-DSA, and lattice-based ones, such as ML-KEM and ML-DSA, which also rely on NTT-based multiplication to speed up polynomial arithmetic. RISC-V is an open, modular ISA that supports custom instructions, enabling efficient domain-specific optimization. Its flexibility allows tailored acceleration strategies, making it suitable for cryptographic workloads beyond traditional accelerator approaches.

Challenges: Accelerating SHA-3 hash function family and NTT-based polynomial multiplication while avoiding excessive memory consumption, data exchange latency, or data path complexity.

Contribution: We present the main acceleration approaches for PQC primitives leveraging RISC-V flexibility, comparing performance and FPGA area usage.

Acceleration Strategies



+ Direct connection to the core
+ Independent pipeline and resources
+ Simplified integration
+ Supports complex operations
- Resource usage
- Requires coordination mechanisms

Ideal for:
- Sub-routines
- Hashing
- Polynomial-wise operations like NTT
- Vector Instructions

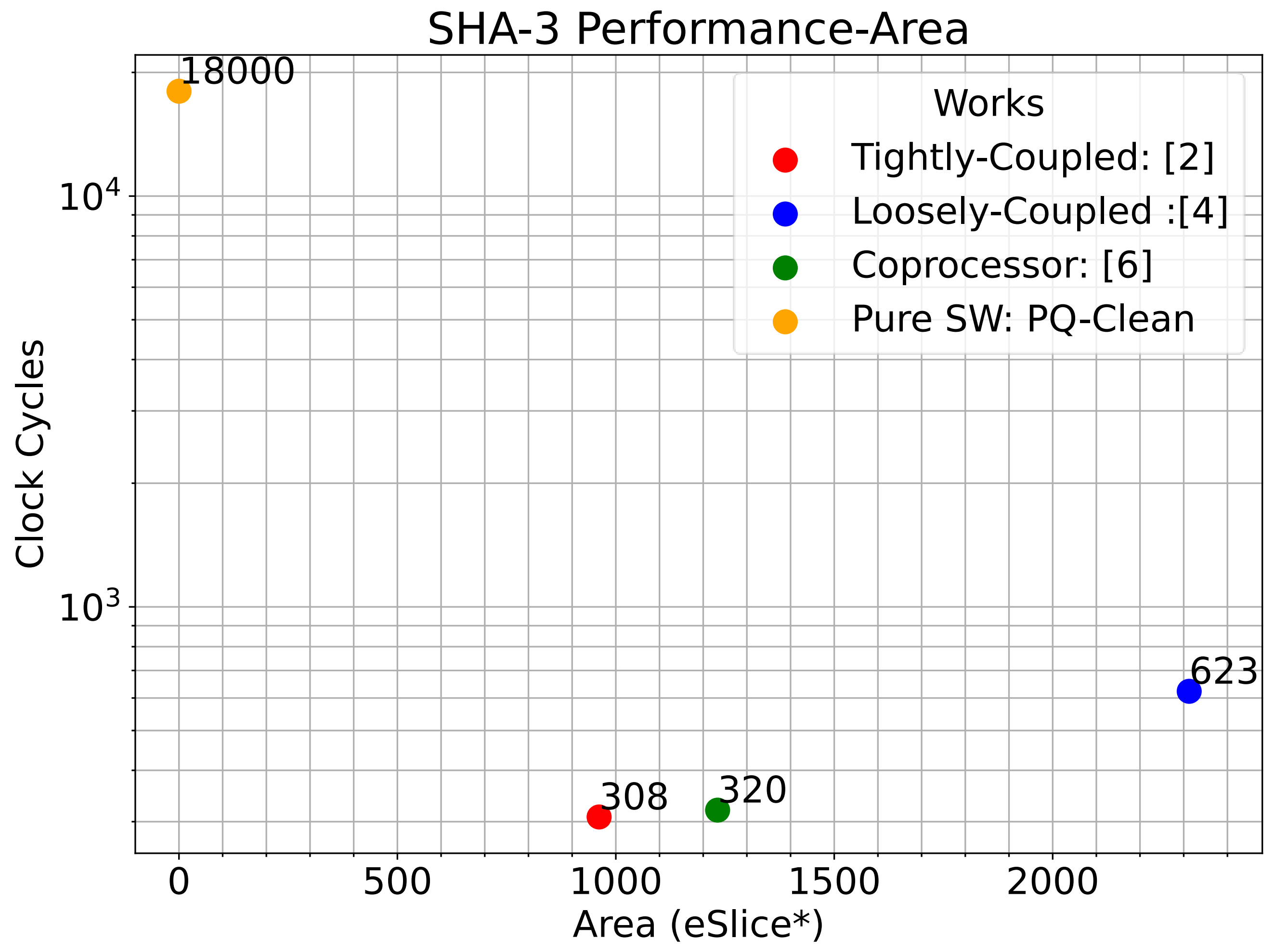
+ Independently of the main processor
+ Enable task parallelism
+ Scalable design
+ High throughput
- Communication overhead
- Resource replication
- Ad-hoc I/O based control protocol
- Complex memory and synchronization management

Ideal for:
- Hashing
- Polynomial Vectors operations like matrix multiplication
- Complete algorithm implementations

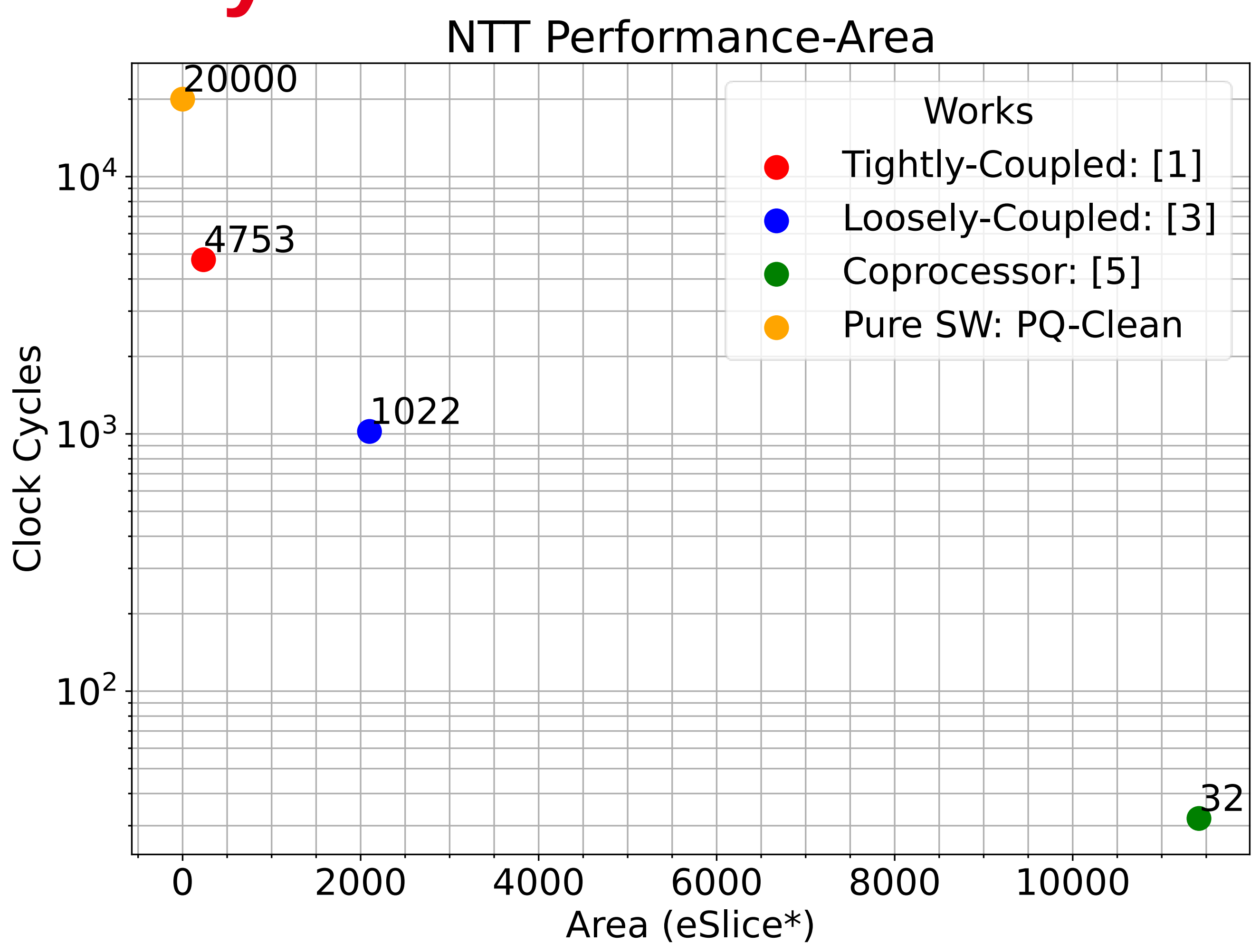
Ideal for:
- Coefficient-wise operations like NTT butterfly
- Encoding operations
- Scalar Instructions

+ Low communication overhead
+ Seamless resource sharing
+ Simplified software-hardware interface
+ Efficient for memory-intensive tasks
+ Ideal for constrained environments
- Increased design complexity
- Limited scalability

State Of The Art Analysis



The tightly-coupled in [2] performs a full SHA-3 round by using floating-point registers to store the SHA-3 state. Loosely-coupled [4] and coprocessor [6] designs for SHA-3 yield similar improvements; they differentiate because of data transfer latency and interface logic overhead.
**eSlice= 128*BRAMs + 60*DSPs + 0.25*LUTs + 0.125*FF*



The tightly-coupled accelerator in [1] propose custom instruction for NTT butterfly. The loosely-coupled accelerator by [3] provides a mid-performance polynomial NTT acceleration using four butterfly units, and a high-speed slave interface to minimize I/O latency. [5] proposes a highly parallel (32 butterfly units) and high-performance NTT coprocessor with a large resource footprint.

References

[1] Miteloudi K. et al. “PQ. V. ALU. E: Post-quantum RISC-V Custom ALU Extensions on Dilithium and Kyber”. In: International Conference on Smart Card Research and Advanced Applications. 2023.

[2] Fritzmann T. et al. “RISQ-V: Tightly Coupled RISC-V Accelerators for Post-Quantum Cryptography”. In: IACR Transactions on Cryptographic Hardware and Embedded Systems (2020).

[3] Rafael Carrera Rodriguez et al.Hardware Implementa-tion and Security Analysis of Local-Masked NTT for CRYSTALS-Kyber. Cryptology ePrint Archive, Paper2024/1194. 2024.

[4] Diamante Simone Crescenzo et al. “Hardware Accelerator for FIPS 202 Hash Functions in Post-Quantum Ready SoCs”. In: 2024 IEEE 30th International Symposium on On-Line Testing and Robust System Design (IOLTS). 2024.

[5] Yifan Zhao et al. “A high-performance domain-specific processor with matrix extension of RISC-V for module-LWE applications”. In: IEEE Transactions on Circuits and Systems I: Regular Papers 69.7 (2022), pp. 2871–2884.

[6] Zhenjiang Wang et al. “An Instruction Extension BasedSHA-3 Algorithm Co-Processor Design Scheme”. In: 2023 3rd International Symposium on Computer Technology and Information Science (ISCTIS). 2023.