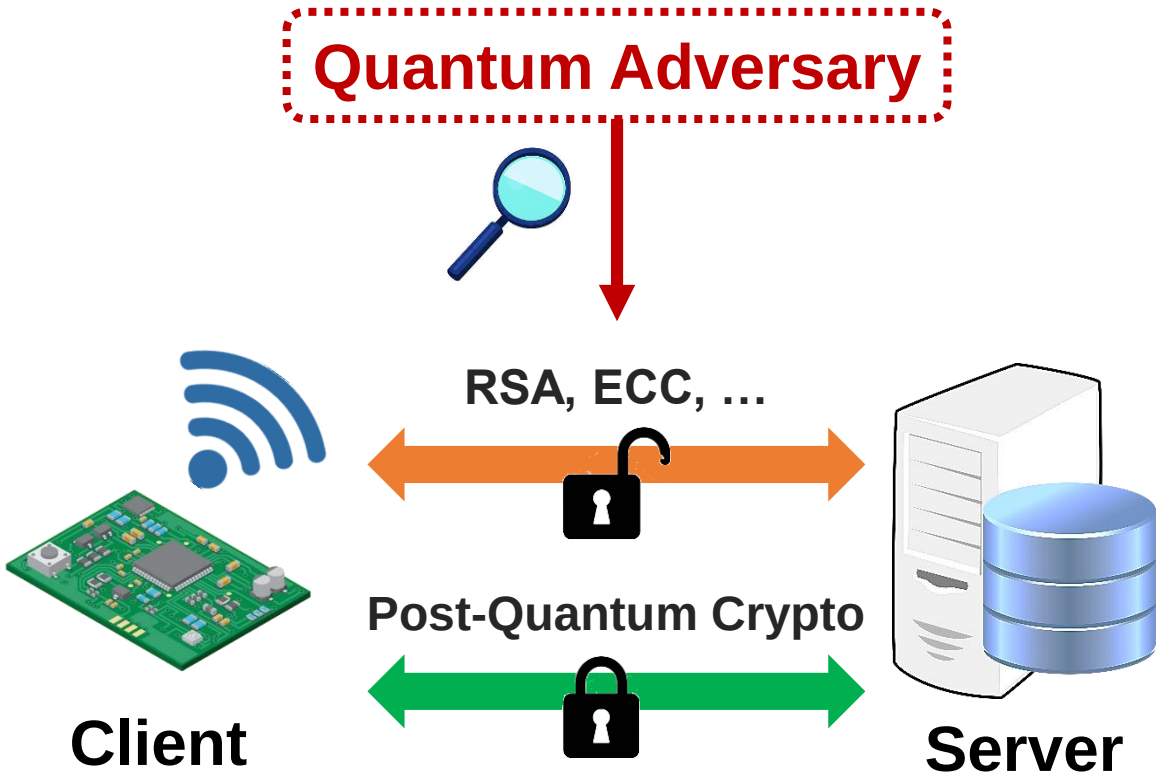
An Energy-Efficient Configurable Crypto-Processor for Post-Quantum Lattice-based Protocols

Utsav Banerjee, Tenzin S. Ukyab, Anantha P. Chandrakasan

Massachusetts Institute of Technology

Post-Quantum Cryptography



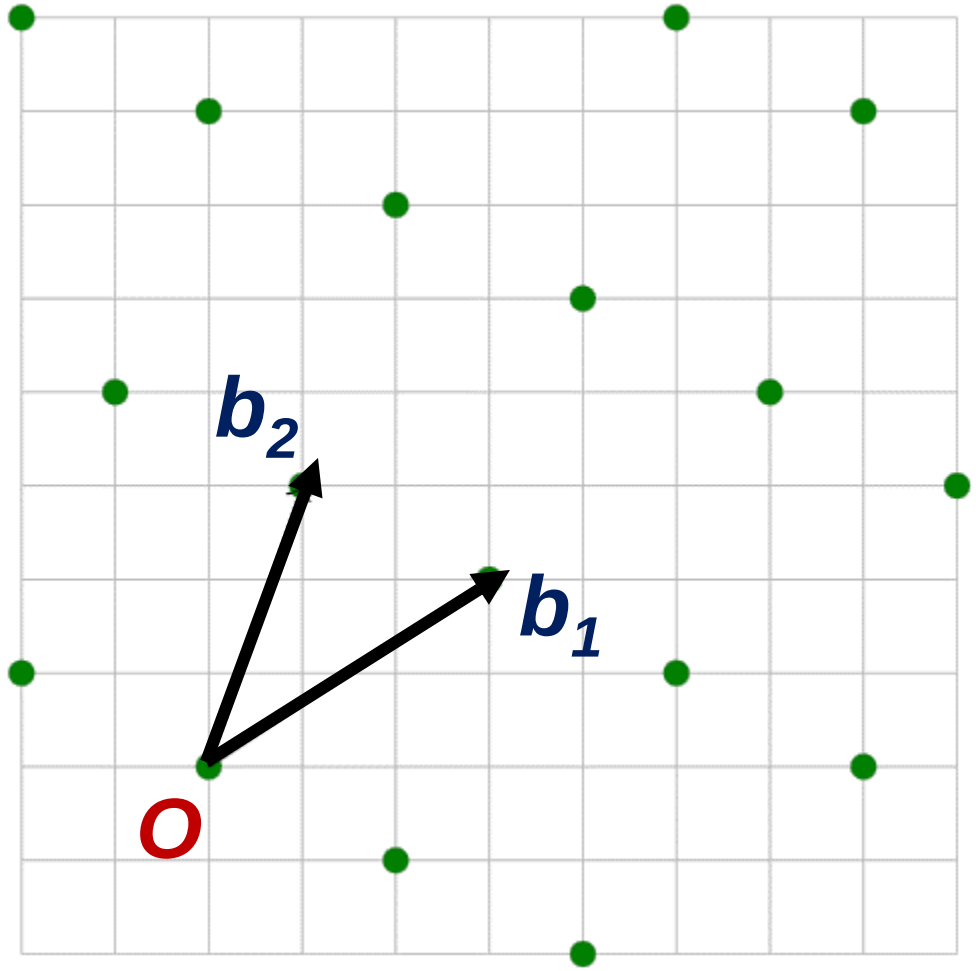
- Current public key cryptography vulnerable to quantum attacks
- NIST Post-Quantum Crypto (PQC) standardization in progress
- Round 2 has 26 candidates:
  - **Lattice-based (9 KEM + 3 Sign)**
  - Code-based (7 KEM)
  - Hash-based (1 Sign)
  - Multivariate (4 Sign)
  - Supersingular isogeny (1 KEM)
  - Zero-knowledge proofs (1 Sign)

Outline

- ❑ Lattice-Based Cryptography
- ❑ Efficient Hardware Implementation
- ❑ Chip Architecture
- ❑ Measurement Results
- ❑ Side-Channel Analysis

Lattices

Lattices – integer linear combinations of basis vectors



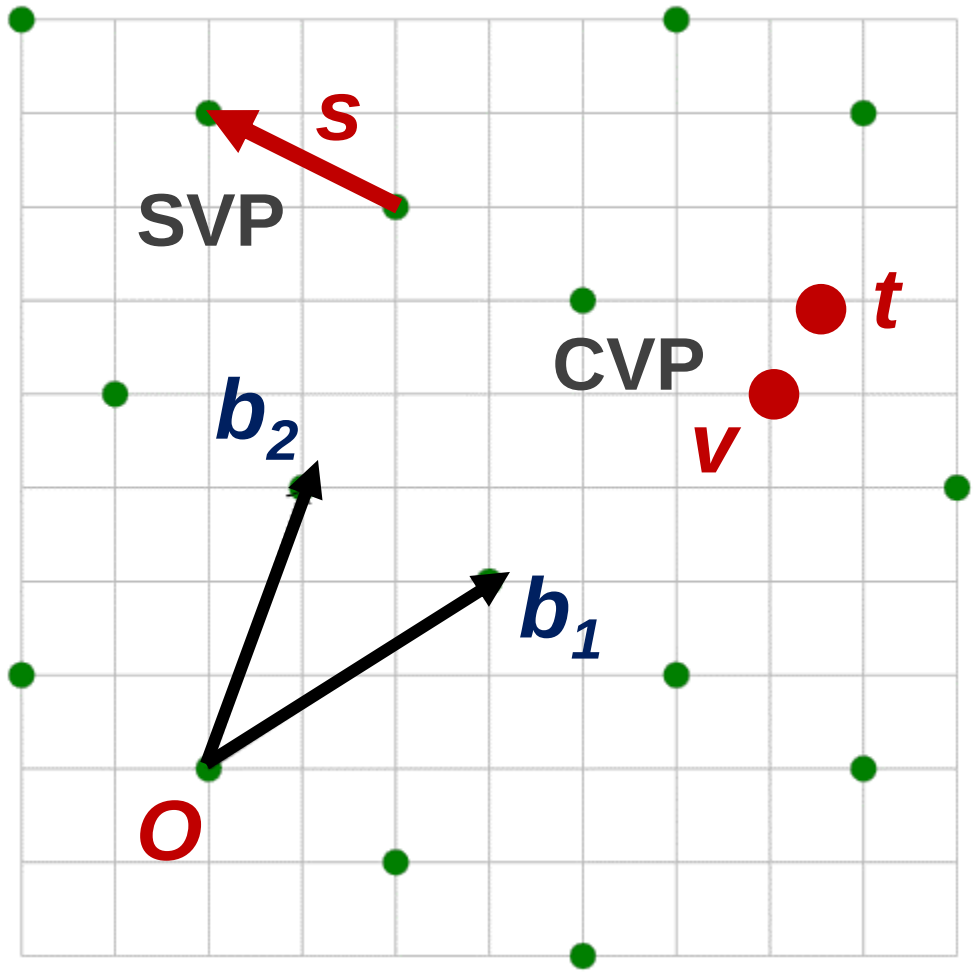
Lattices

Lattices – integer linear combinations of basis vectors

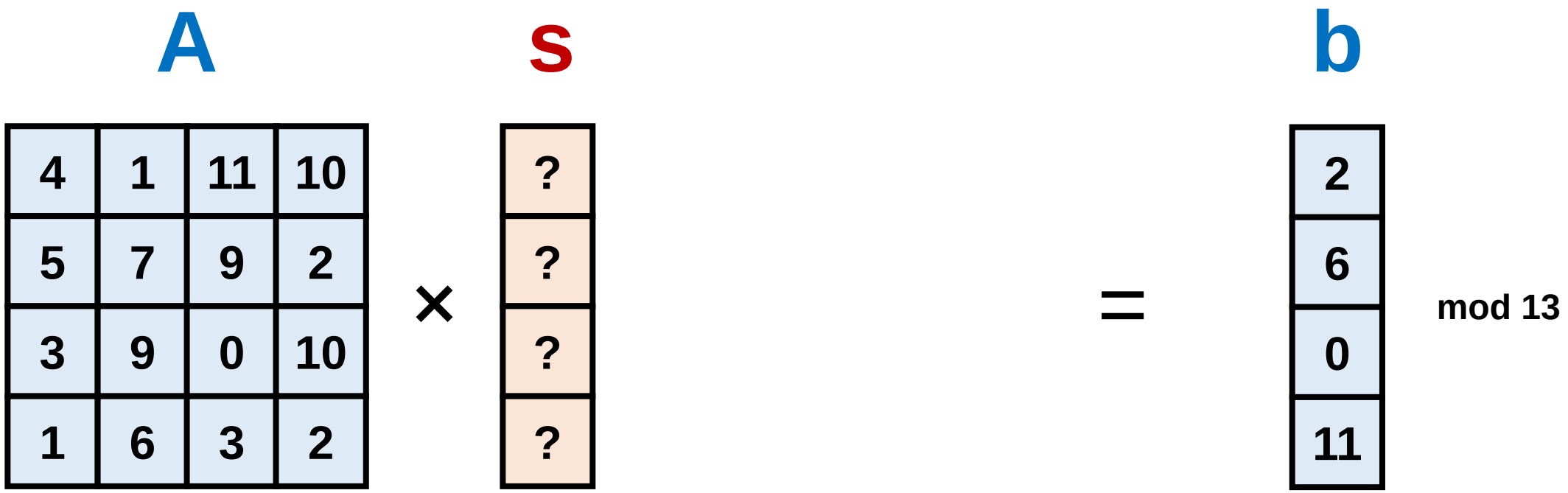
Shortest Vector Problem (SVP)

Closest Vector Problem (CVP)

≈ 2^N time complexity for N dimensions



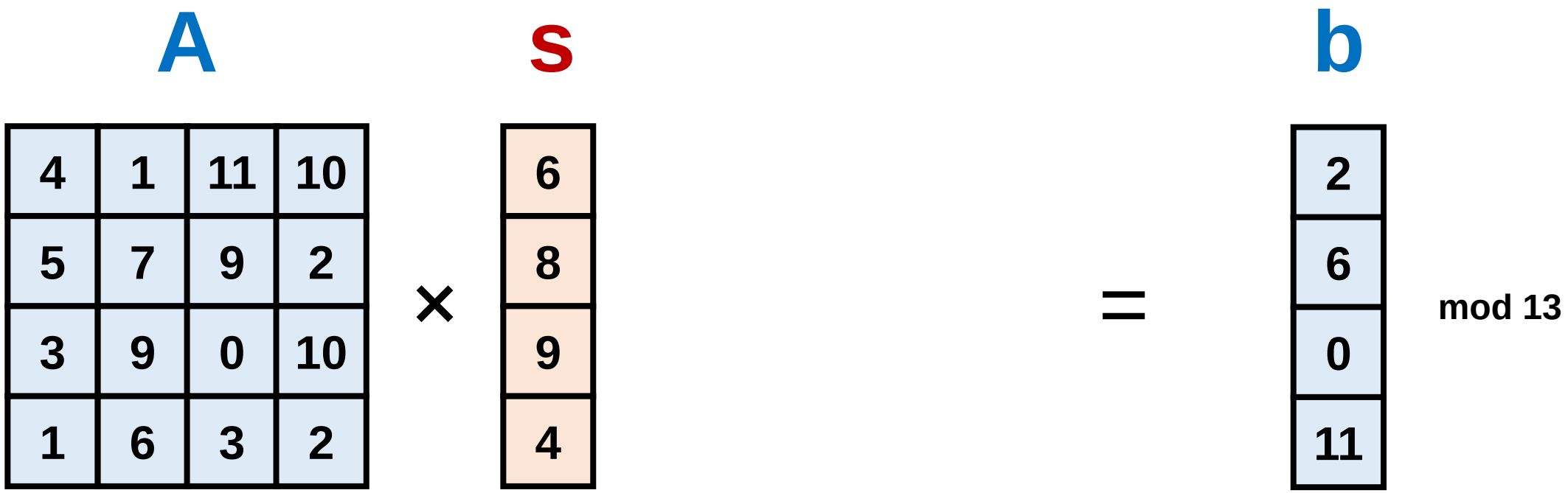
Learning with Errors



$As = b$

Given blue, find red

Learning with Errors

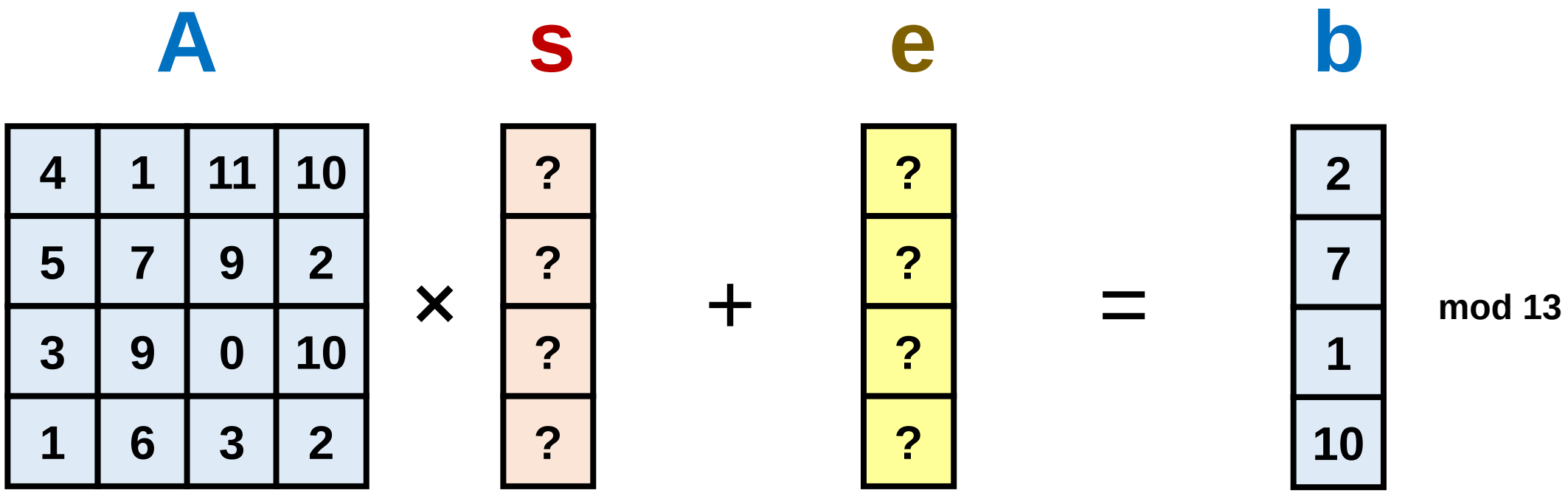


$As = b$

Given blue, find red

Easy

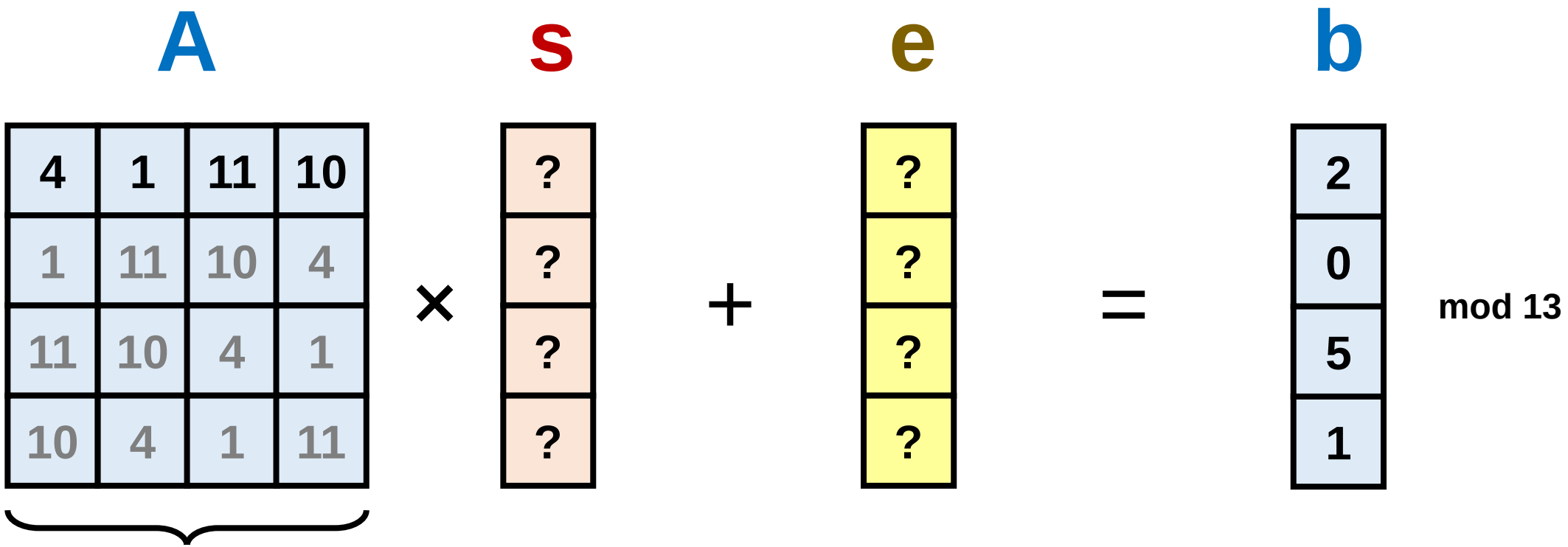
LWE



As + e = b Given blue, find red **Hard**

Storage = $O(N^2)$ and Computation = $O(N^3)$

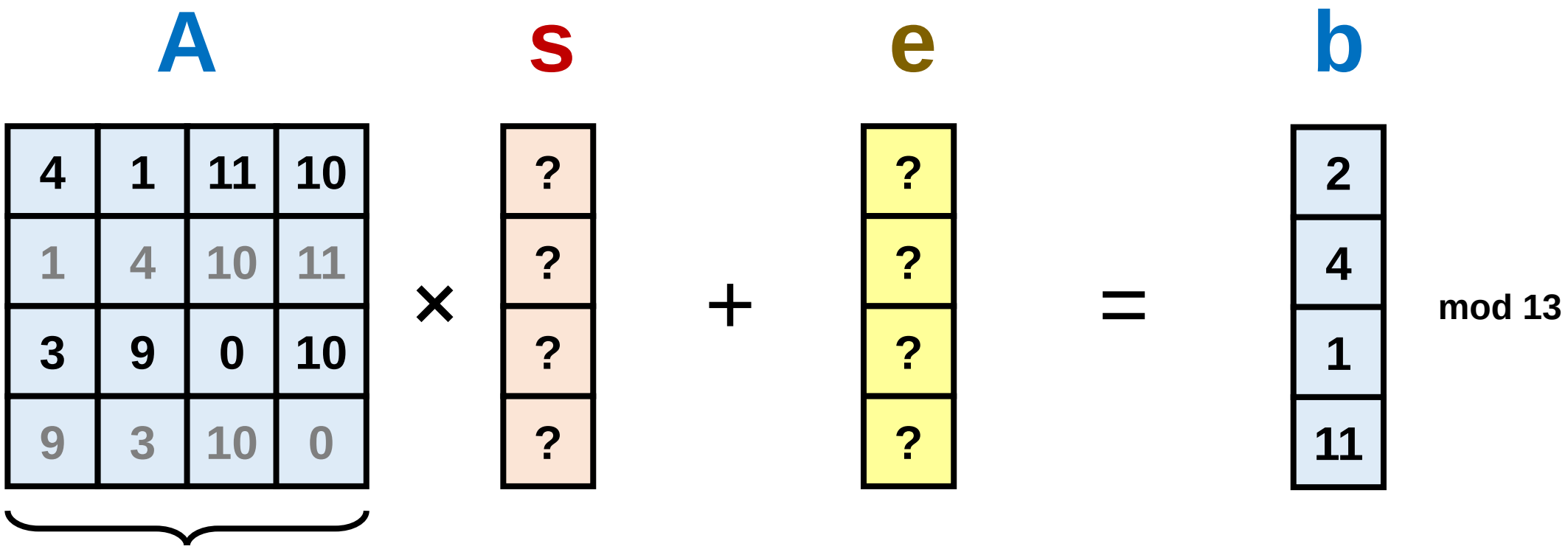
Ring-LWE



Circulant Matrix $\Rightarrow$ Storage = $O(N)$

Circular Convolution $\Rightarrow$ Computation = $O(N \log_2 N)$

Module-LWE



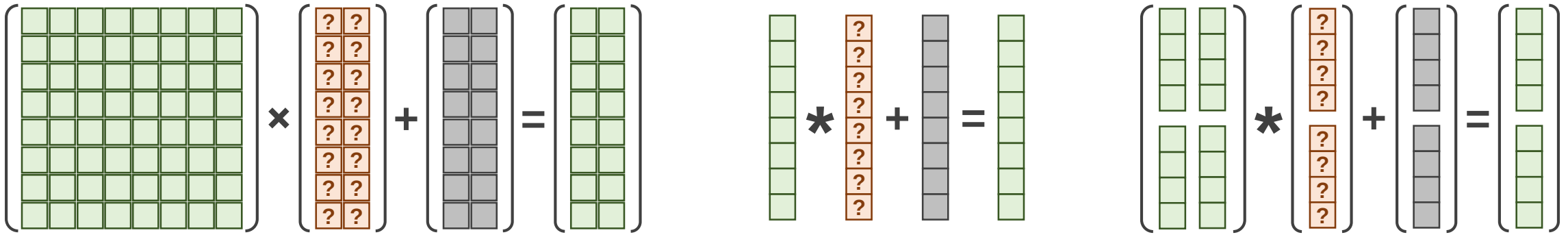
Matrix of Circulant Matrices

Security: Ring-LWE ≤ Module-LWE ≤ LWE

Efficiency: LWE << Module-LWE < Ring-LWE

Computational Requirements

- **Learning with Errors (LWE) and its variants:**



LWE
(Standard Lattices)

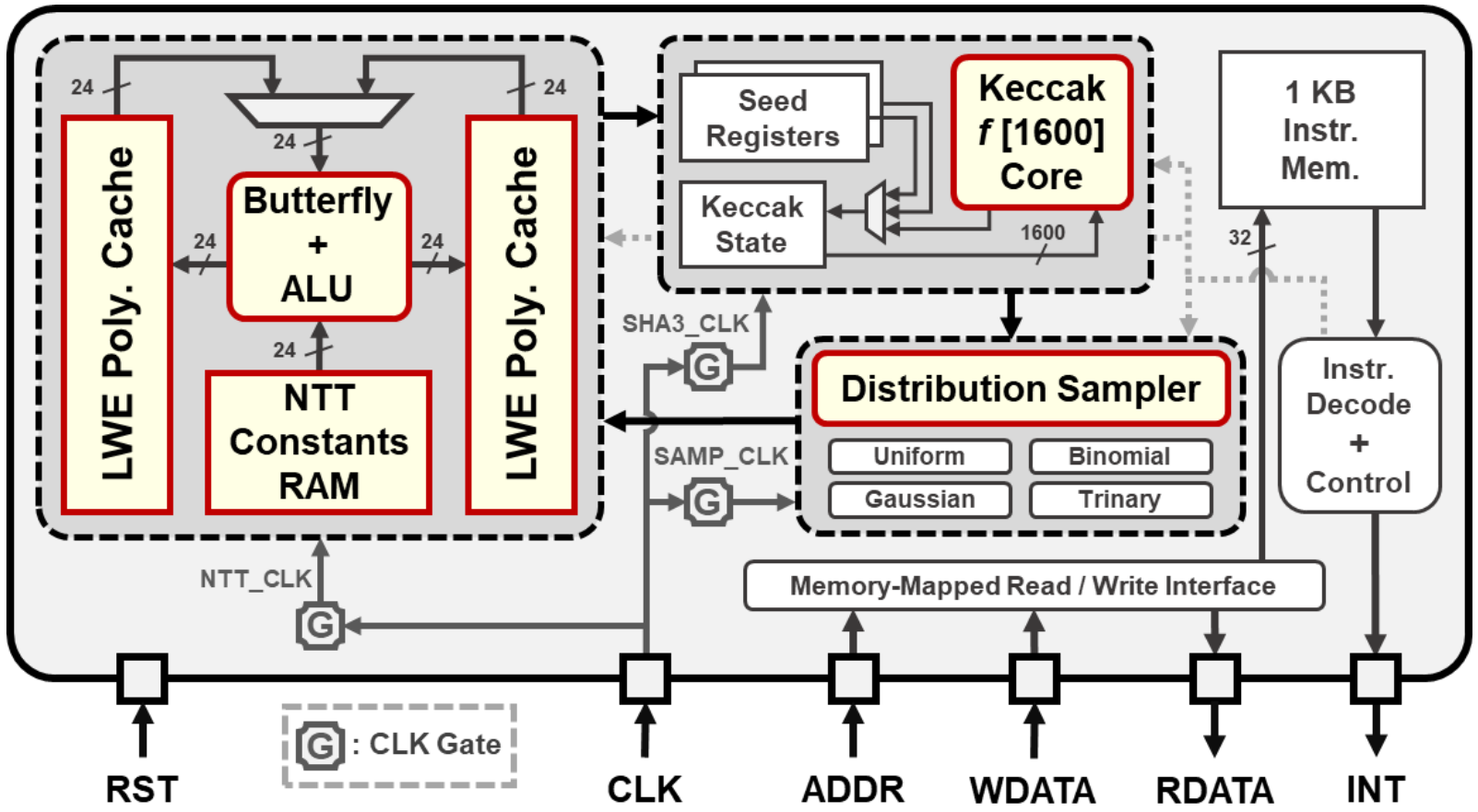
Ring-LWE
(Ideal Lattices)

Module-LWE
(Module Lattices)

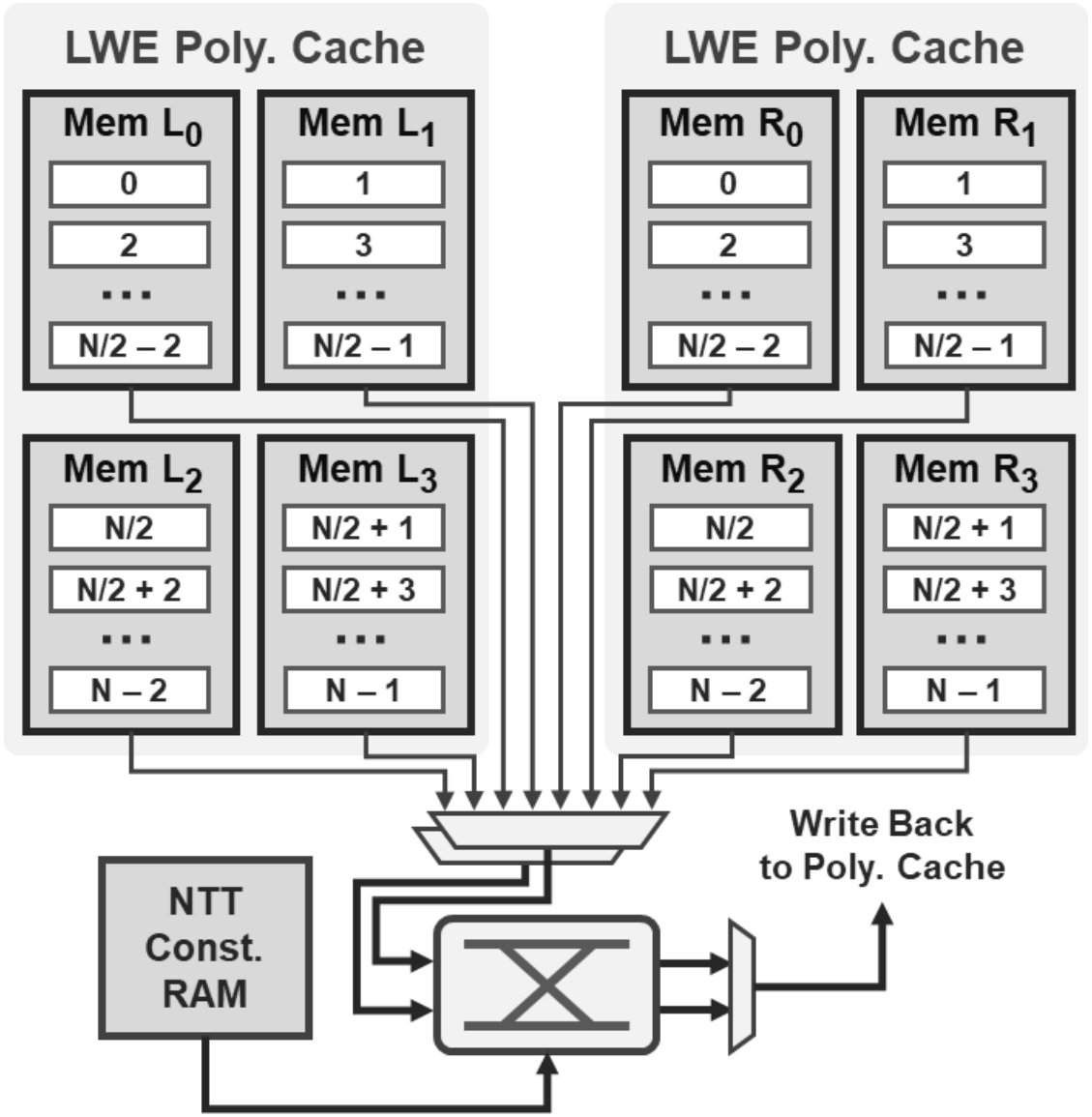
- **Computational requirements (apart from standard arithmetic):**
  - Modular arithmetic over various small primes
  - Polynomial arithmetic for Ring-LWE and Module-LWE
  - Sampling of matrices and polynomials from discrete distributions

Sapphire Crypto-Processor

- Energy-efficient configurable lattice-crypto-processor

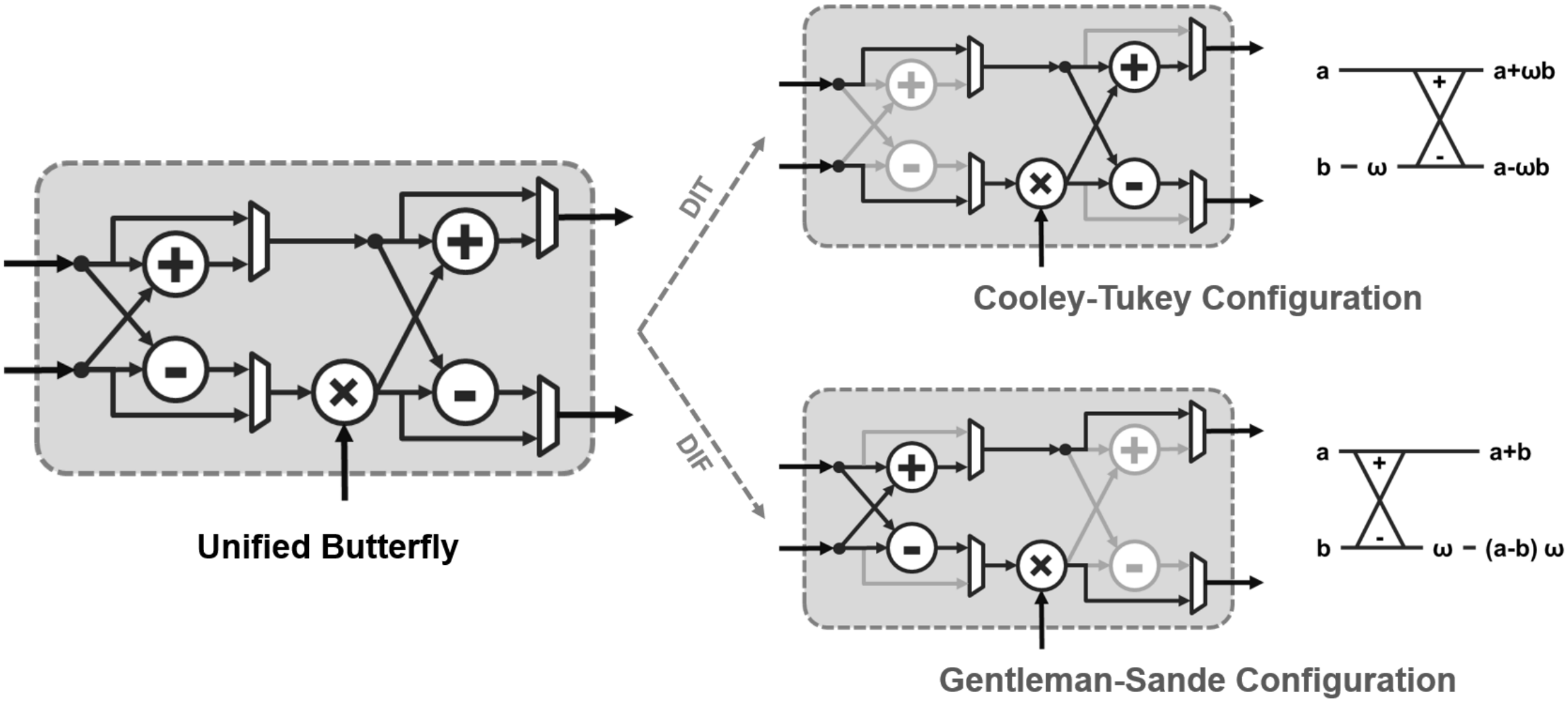


Area-Efficient NTT



- NTT memory banks using 2-port SRAMs have large area overheads
- Proposed 1-port SRAM-based NTT
- Based on constant geometry FFT data-flow
  [Pease, J. ACM, 1968]
- Polynomials split into four 1-port SRAMs
- Achieves > 30% area savings without loss in throughput

Unified Butterfly

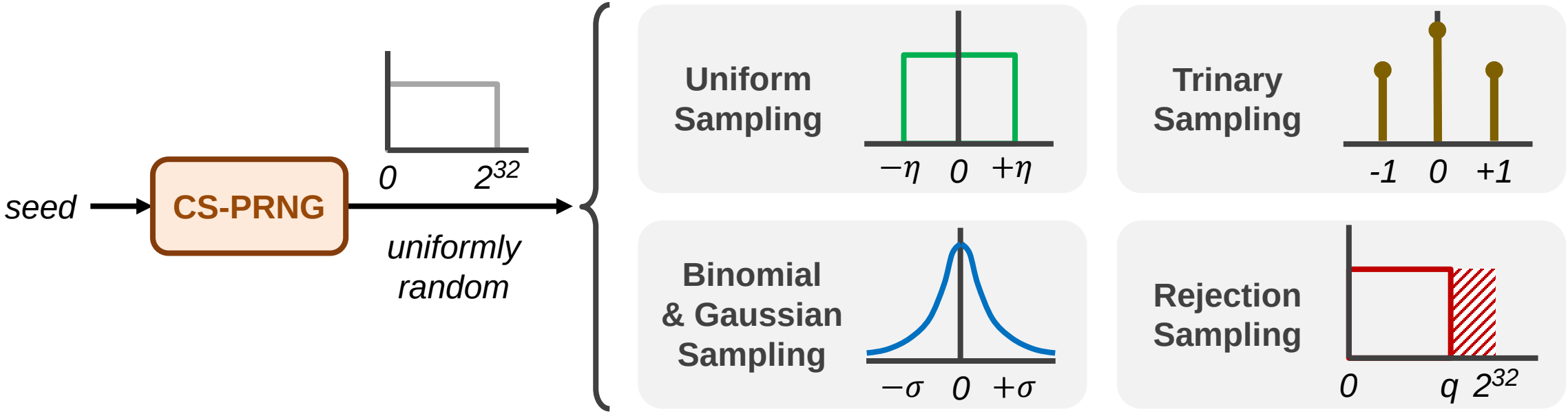


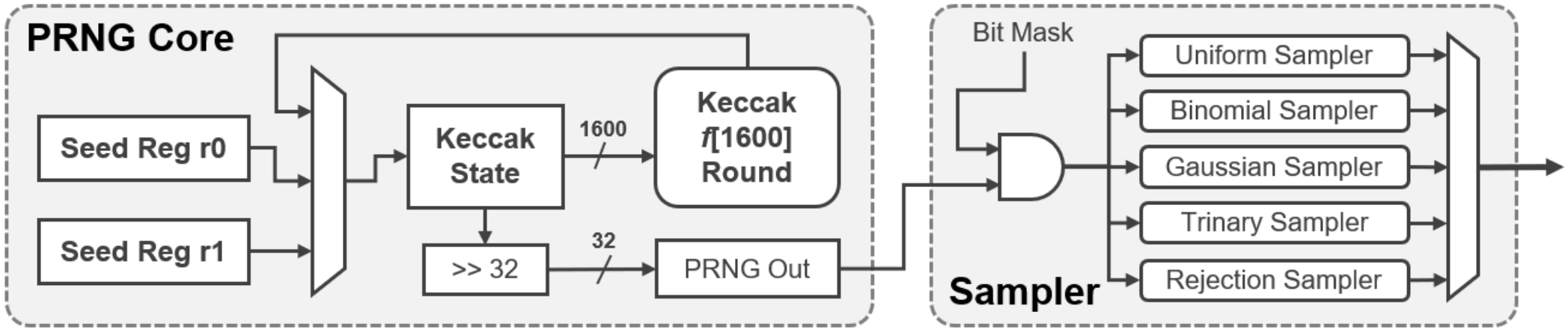
Unified Butterfly

Cooley-Tukey Configuration

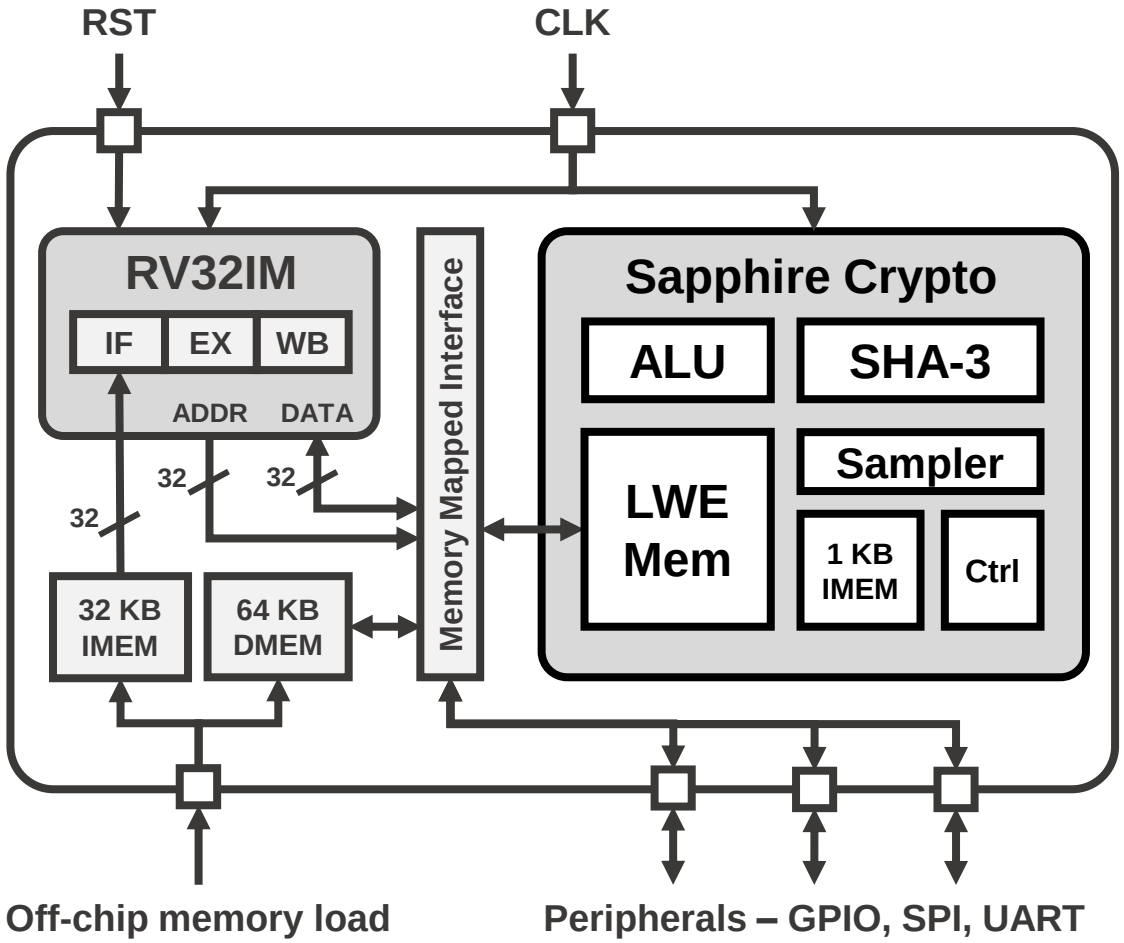
Gentleman-Sande Configuration

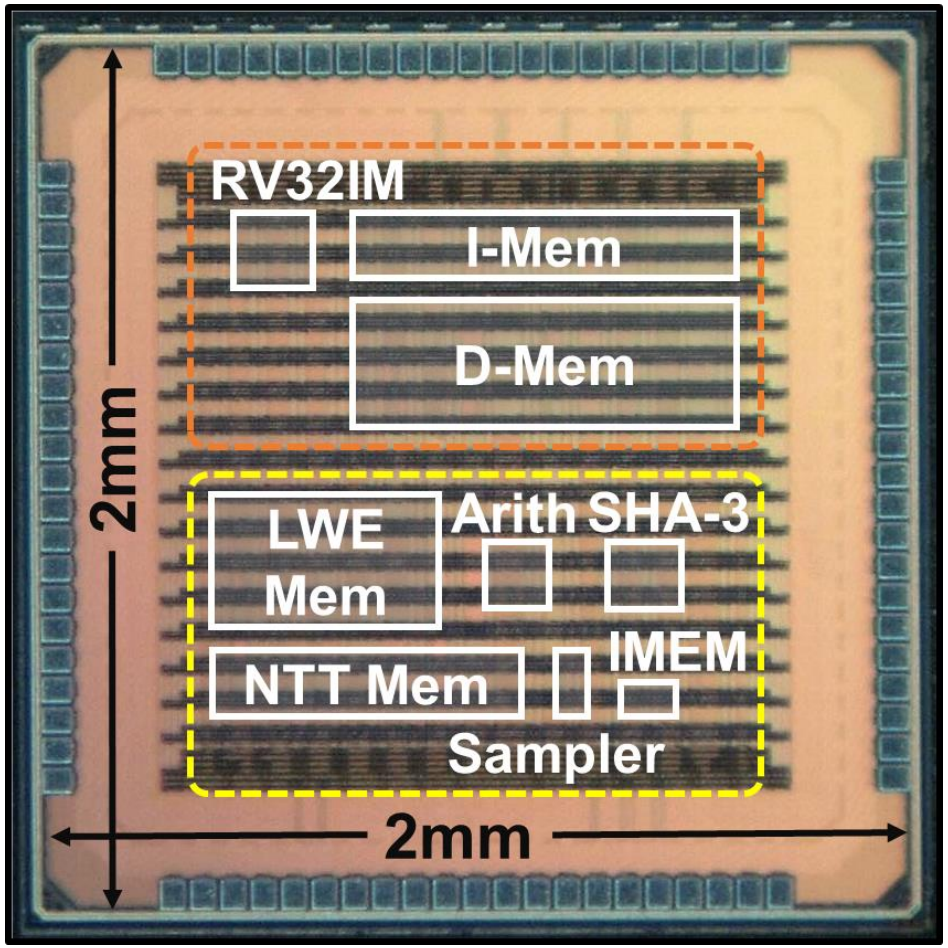
Energy-Efficient Sampler





Test Chip Overview





Chip Micrograph

Protocol Implementations

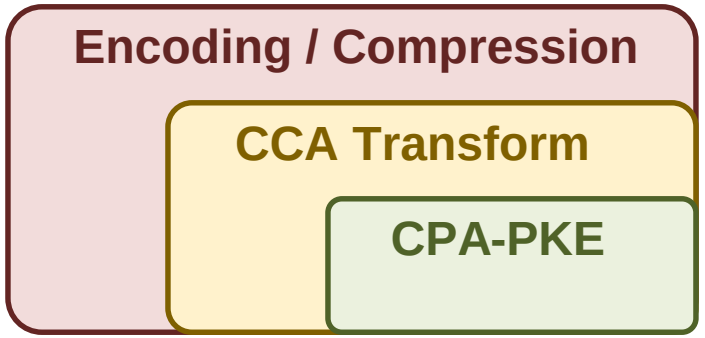
- NIST PQC Round 2 protocols implemented on test chip:

CCA-KEM	LWE	Frodo
	Ring-LWE	NewHope
	Module-LWE	CRYSTALS-Kyber

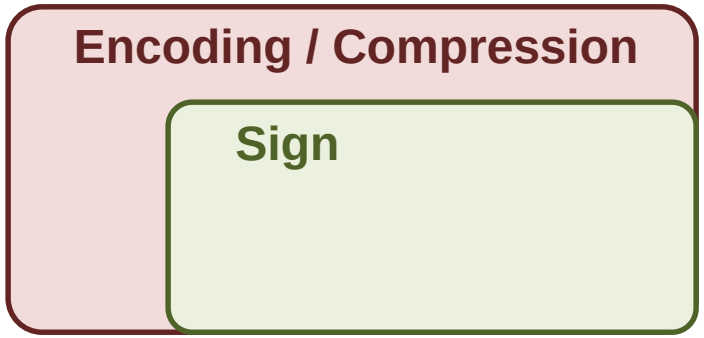
Signature	Ring-LWE	qTesla
	Module-LWE	CRYSTALS-Dilithium

- Computations shared between software and crypto hardware:

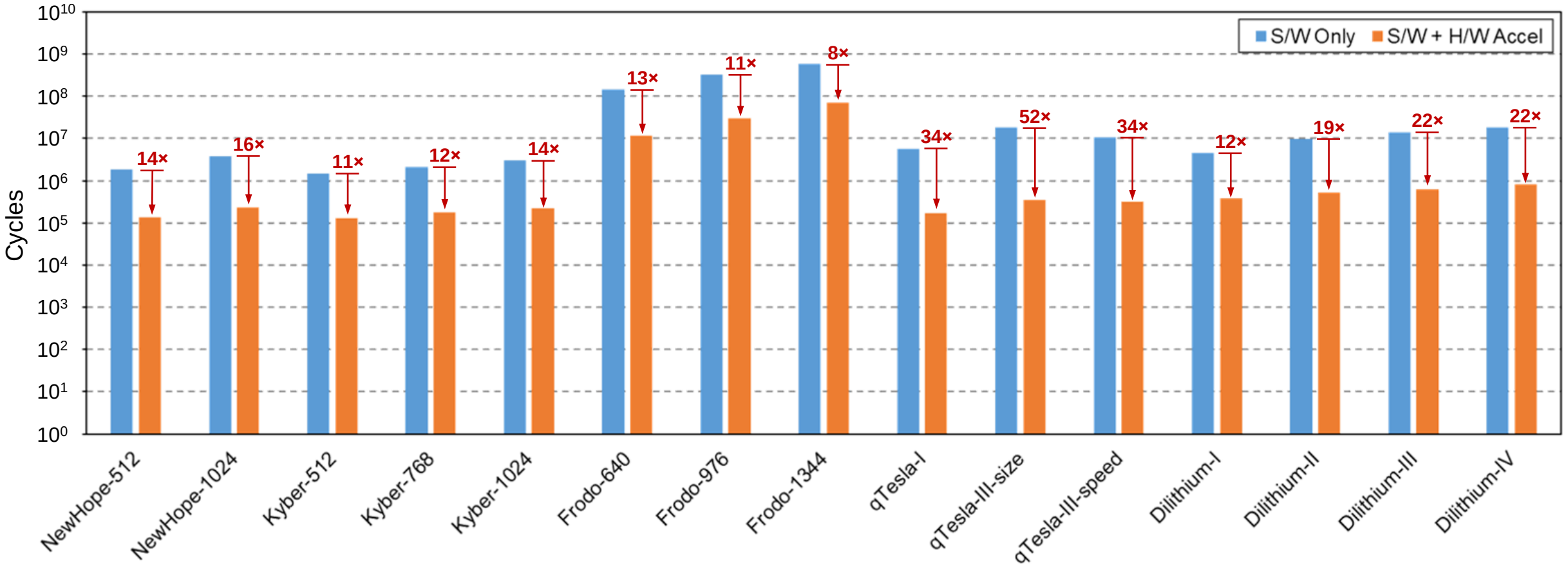
CPA-PKE / CCA-KEM:



Sign:



Protocol Evaluation Results

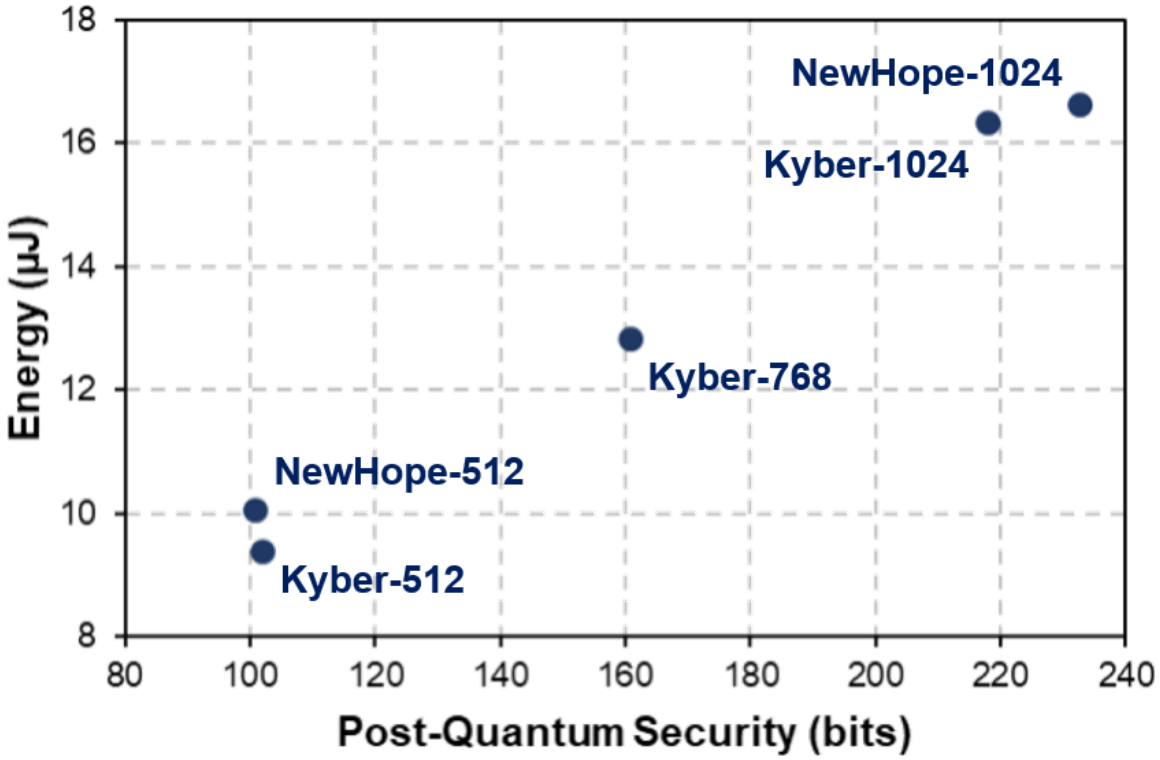


** Cycle counts for CCA-KEM-Encaps and Sign*

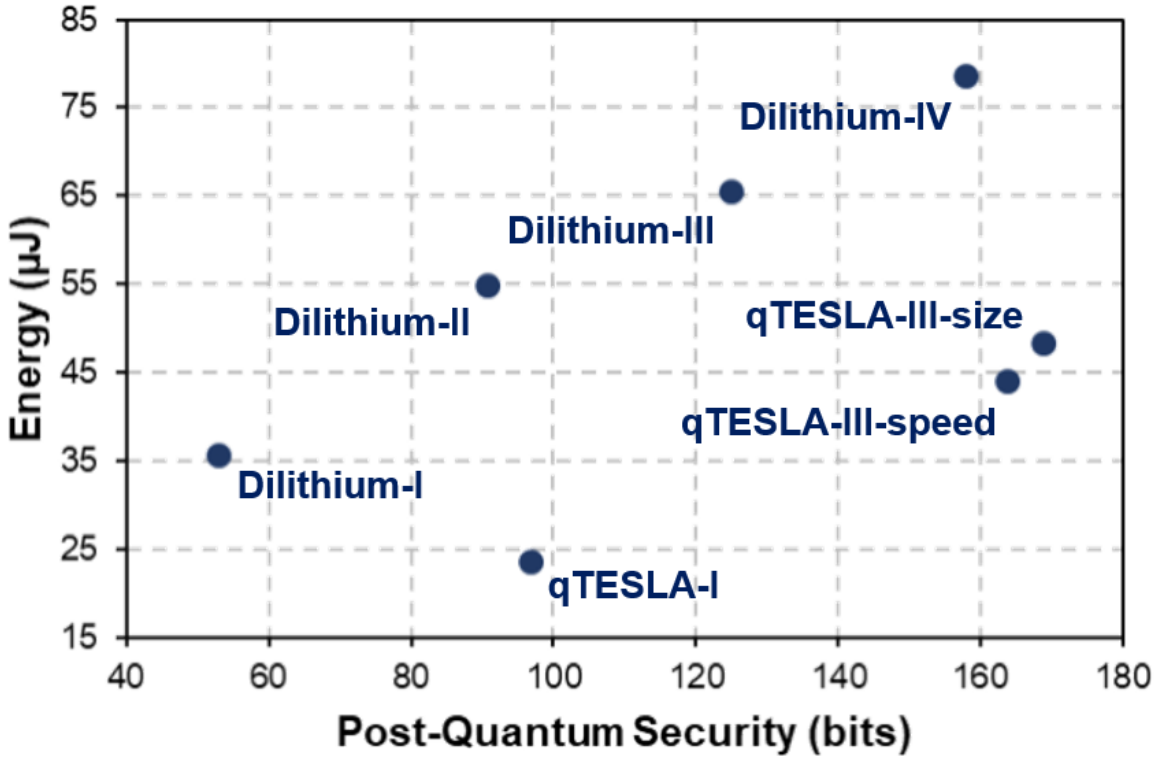
Order of magnitude improvement in energy-efficiency and performance

Protocol Evaluation Results

CCA-KEM-Encaps

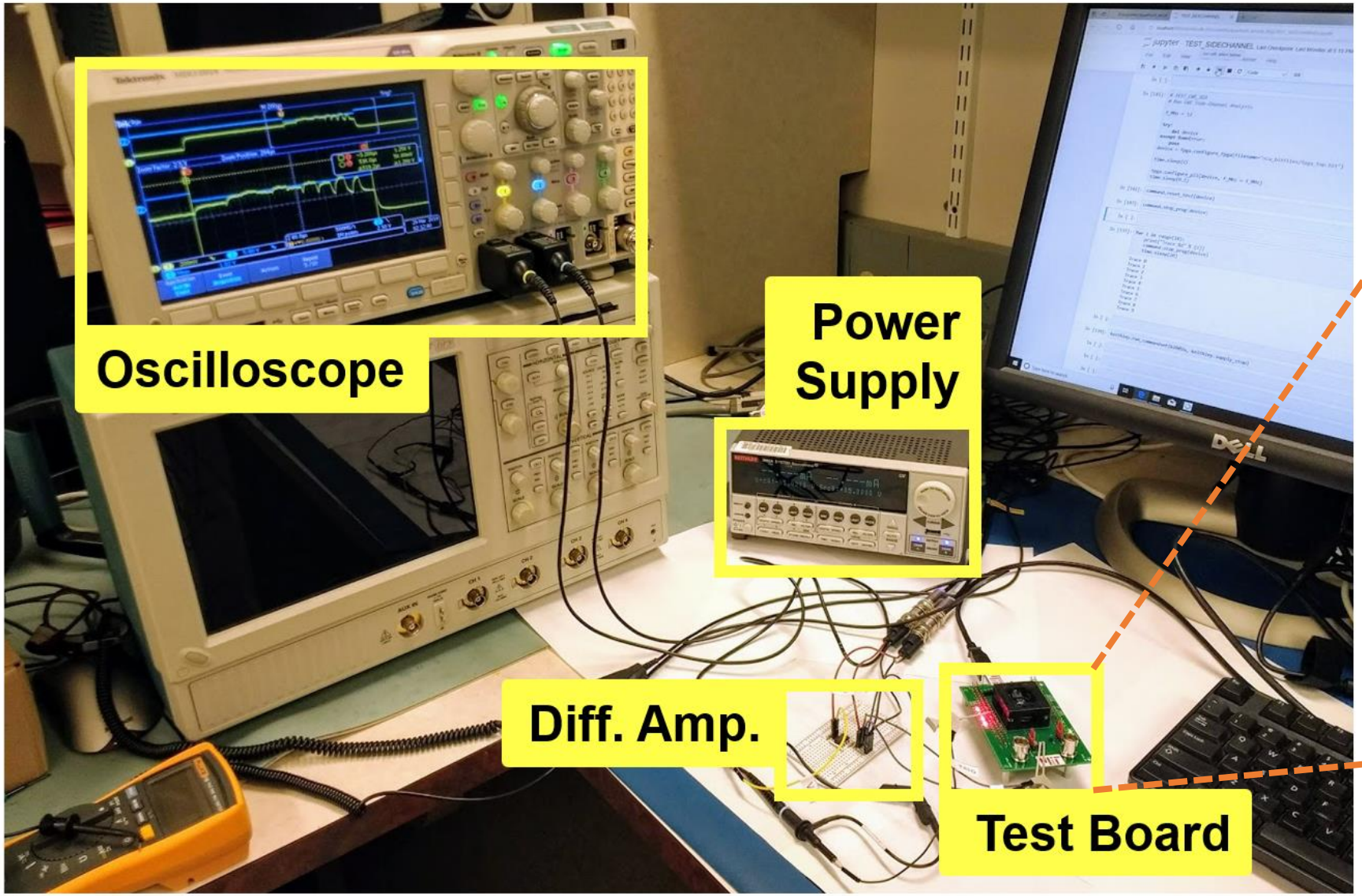


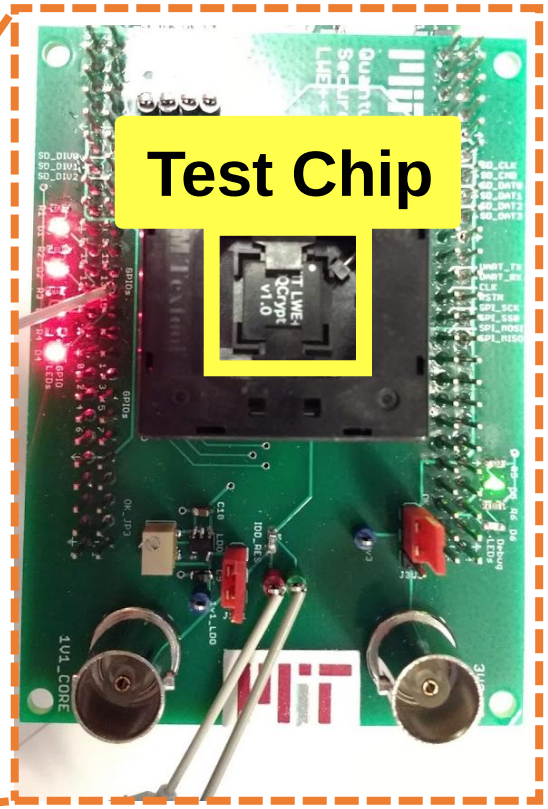
Sign



** Measured using test chip operating at 1.1 V and 72 MHz*

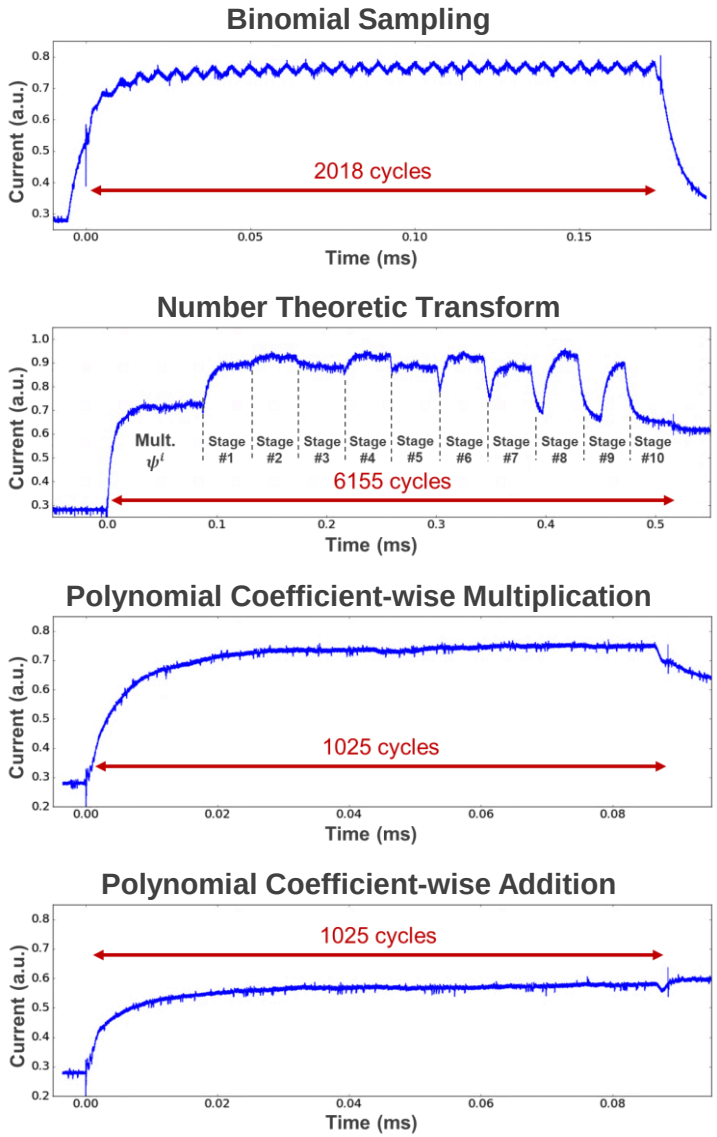
Side-Channel Analysis Setup





Timing and SPA Side-Channels

- All key building blocks **constant-time by design**
- Energy consumption of sampling and polynomial arithmetic follows a narrow distribution with coefficient of variation ≤ 0.5% ($= \sigma/\mu$)
- SPA attacks target polynomial arithmetic:
  - Number Theoretic Transform
  - Coefficient-wise Multiplication
  - Coefficient-wise Addition
- **SPA resistance of polynomial arithmetic** evaluated using difference-of-means test with 99.99% confidence interval



Masking for DPA Security

- Crypto core is programmable, hence **masking can also be implemented**
- Masked NewHope-CPA-PKE-Decrypt based on additively homomorphic property:

[Reparaz et al, PQCrypto, 2016]

1. Generate secret message μ_r
2. Encrypt μ_r to its corresponding ciphertext $c_r = (\hat{u}_r, v'_r)$
3. Compute $c_m = (\hat{u} + \hat{u}_r, v' + v'_r)$ where $c = (\hat{u}, v')$ is the original ciphertext
4. Decrypt c_m to obtain $\mu_m = \mu \oplus \mu_r$ where μ is the original message
5. Recover original message as $\mu = \mu_m \oplus \mu_r$

- Masked decryption using same hardware; 3× slower than unmasked version
- Masking increases decryption failure rate, which can be resolved by decreasing std. dev. σ of error distribution (at the cost of slightly lower security level)

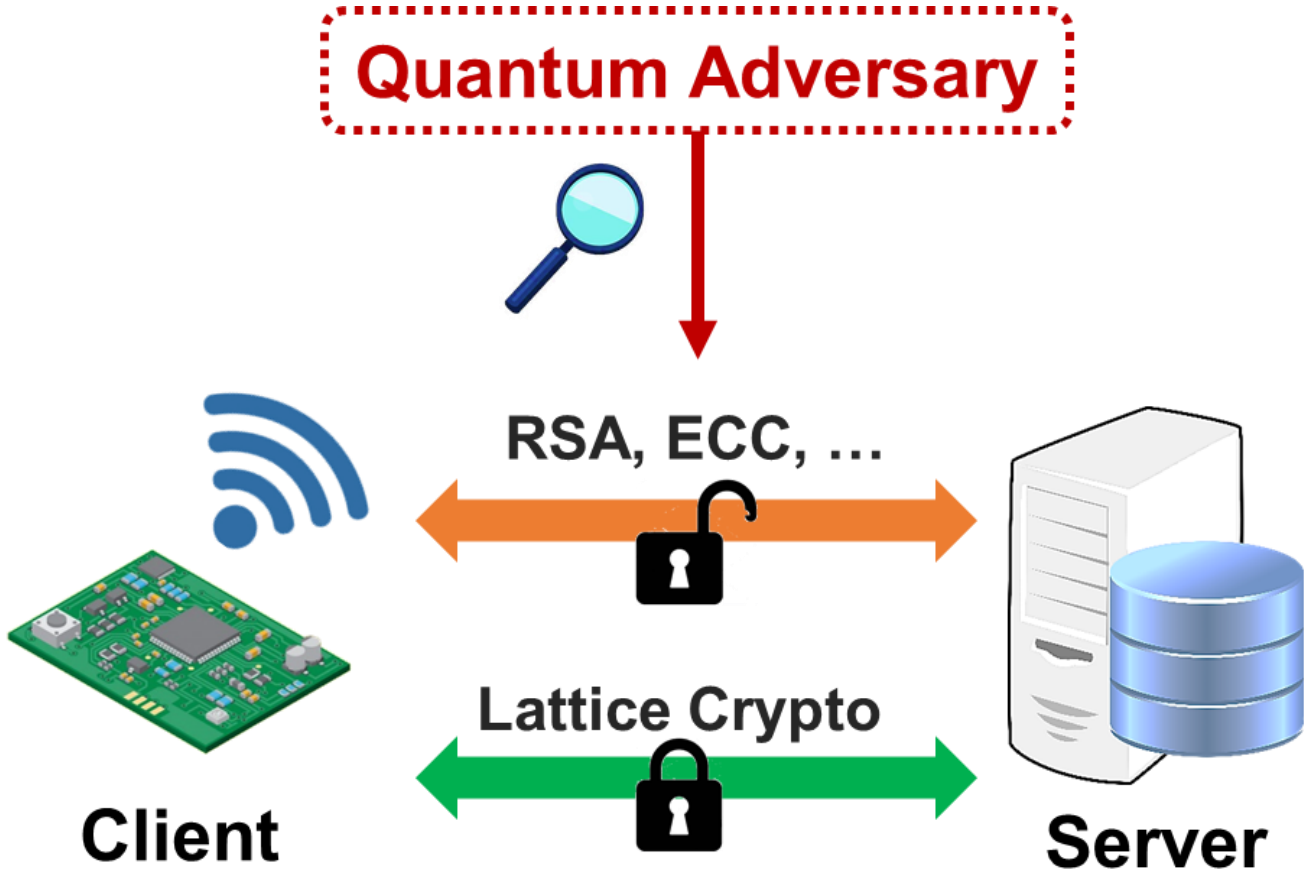
Conclusion

- Configurable crypto-processor for LWE, Ring-LWE and Module-LWE protocols
- Area-efficient NTT, energy-efficient sampler and flexible parameters
- ASIC demonstration of NIST Round 2 CCA-KEM and signature protocols: Frodo, NewHope, Kyber, qTesla, Dilithium
- Order of magnitude improvement in performance and energy-efficiency compared to state-of-the-art software and hardware
- Hardware building blocks constant-time and SPA-secure by design; masking can also be implemented for DPA security

Acknowledgements

- Texas Instruments for funding
- TSMC University Shuttle Program for chip fabrication

Questions



References

1. L. Chen et al., “Report on Post-Quantum Cryptography,” *NIST Technical Report*, no. 8105, Apr. 2016.
2. G. Alagic et al., “Status Report on the First Round of the NIST Post-Quantum Cryptography Standardization Process,” *NIST Technical Report*, no. 8240, Jan. 2019.
3. C. Peikert, “A Decade of Lattice Cryptography,” in *Now Publishers - Foundations and Trends in Theoretical Computer Science*, vol. 10, no. 4, pp. 283-424, Mar. 2016.
4. M. C. Pease, “An Adaptation of the Fast Fourier Transform for Parallel Processing,” in *Journal of the ACM*, vol. 15, pp. 252-264, Apr. 1968.
5. S. Gueron and F. Schlieker, “Speeding up R-LWE Post-Quantum Key Exchange.” in *Cryptology ePrint Archive*, Report 2016/467, May 2016.
6. O. Reparaz, R. de Clercq, S. S. Roy, F. Vercauteren and I. Verbauwhede, “Additively Homomorphic Ring-LWE Masking,” in *Post-Quantum Cryptography (PQCrypto)*, pp. 233-244, Feb. 2016.
7. https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Round-2-Submissions
8. U. Banerjee, A. Pathak and A. P. Chandrakasan, “An Energy-Efficient Configurable Lattice Cryptography Processor for the Quantum-Secure Internet of Things,” in *IEEE International Solid-State Circuits Conference (ISSCC)*, pp. 46-48, Feb. 2019.
9. U. Banerjee, T. S. Ukyab and A. P. Chandrakasan, “Sapphire: A Configurable Crypto-Processor for Post-Quantum Lattice-based Protocols,” in *IACR Transactions on Cryptographic Hardware and Embedded Systems (TCHES)*, vol. 2019, pp. 17-61, Aug. 2019.