1: Motivation

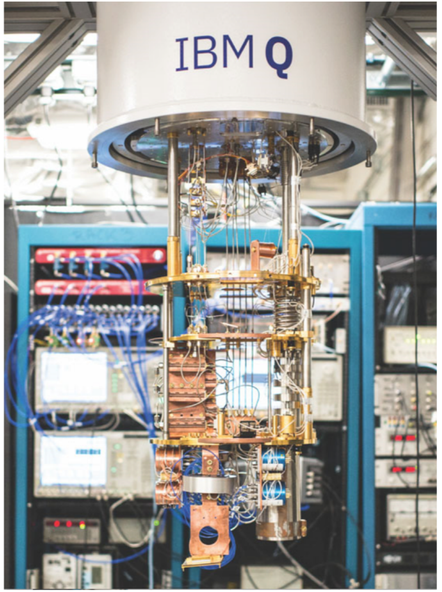
Why do we care about Post-Quantum Cryptography?

Modern cryptography

- Symmetric key crypto
- Public key crypto
- Hash functions

Modern cryptography

- Symmetric key crypto
- ~~Public key crypto~~
- Hash functions



2: Background

Ring-LWE and lattice-based digital signature scheme qTESLA

RLWE distribution

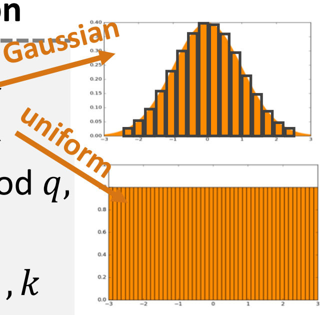
Sample $s, e_1, \dots, e_k \leftarrow_\sigma R_n$

$a_1, \dots, a_k \leftarrow_\$ R_n$

Compute $b_i = a_i s + e_i \bmod q$,

for $i = 1, \dots, k$

Return $(a_i, b_i), i = 1, \dots, k$



qTESLA keys

$sk = (s, e_1, \dots, e_k)$

$pk = (a_1, \dots, a_k, b_1, \dots, b_k)$

Decision-RLWE problem

$(a_i, b_i)_{i=1,\dots,k} \rightarrow \boxed{?}$

$\rightarrow (a_i, b_i) \leftarrow_{\text{RLWE}} R_{n,q} \times R_{n,q}$

$\rightarrow (a_i, b_i) \leftarrow_\$ R_{n,q} \times R_{n,q}$

Security of qTESLA:

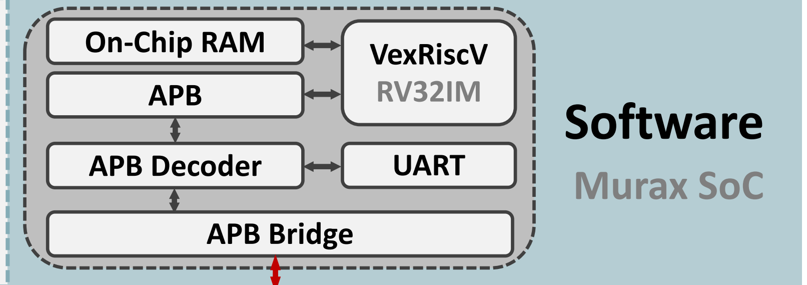
- Quantum-hard
- Reduction from Shortest Vector Problem

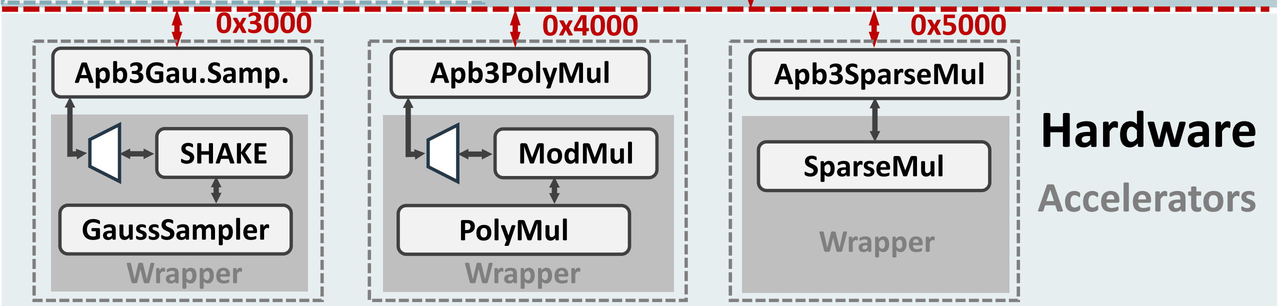
3: Hardware Prototype

SW/HW co-design for qTESLA based on RISC-V

Time-critical operations:

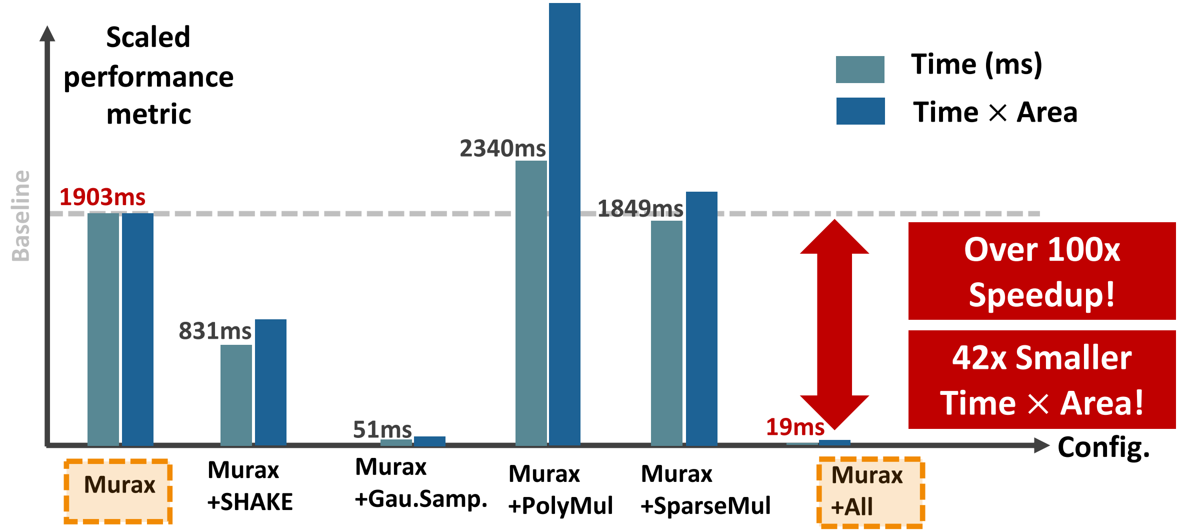
- Gaussian sampling
- Polynomial mult.
- Hash function
- Sparse polynomial mult.





4: Performance evaluation

Post-Quantum Cryptography running on hardware!



Performance of qTESLA key generation operation on different SW/HW co-design platforms