Error Resilience in the Number-Theoretic Transform

PQC acceleration for safety critical applications

Mohamed Abdelmonem

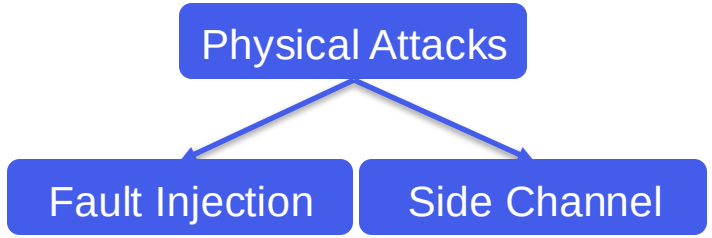
2024-10-25

Motivation

Post-Quantum Cryptography: Algorithms based on **classical** operations that resist attacks from quantum computers

Hard problems:

- Lattice based
- Code based
- Hash based
- Multivariate based
- Isogeny based

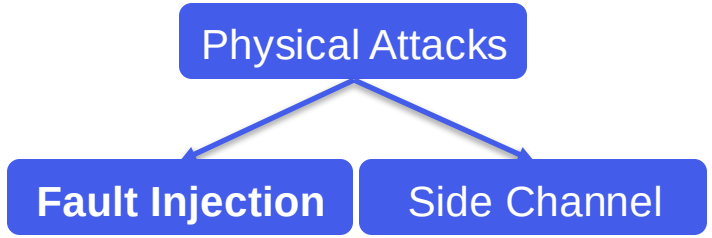


Motivation

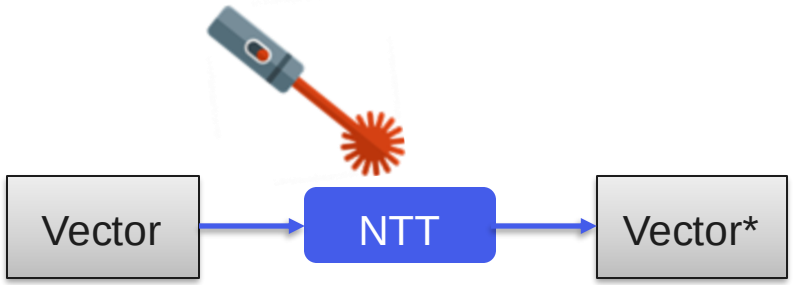
Post-Quantum Cryptography: Algorithms based on **classical** operations that resist attacks from quantum computers

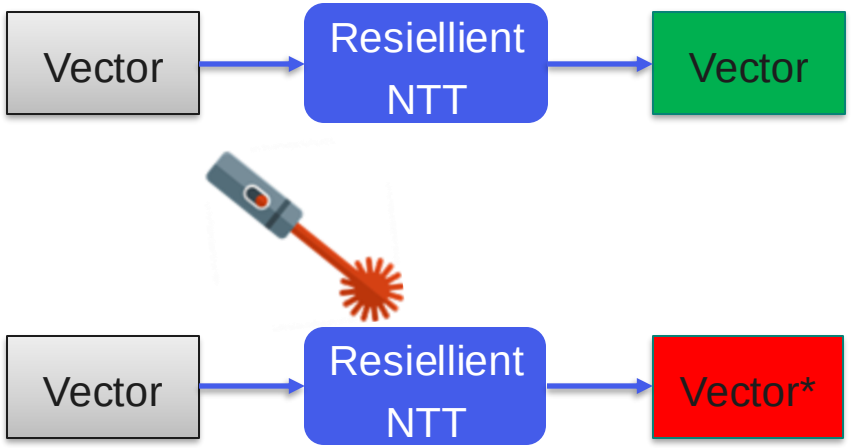
Hard problems:

- **Lattice based**
- Code based
- Hash based
- Multivariate based
- Isogeny based



Example





Number Theoretic Transform

- **Module-Lattice-Based**
  - Use polynomial ring $R_q = \mathbb{Z}_q[X]/\phi(x)$ instead of $\mathbb{Z}_q$
  - Better efficiency
  - Same security

➡ Fast arithmetic on $R_q = \mathbb{Z}_q[X]/\phi(x)$ necessary

- Schoolbook-Multiplication” $O(n^2)$ operations
- Fast Multiplication $O(n \log(n))$ operations

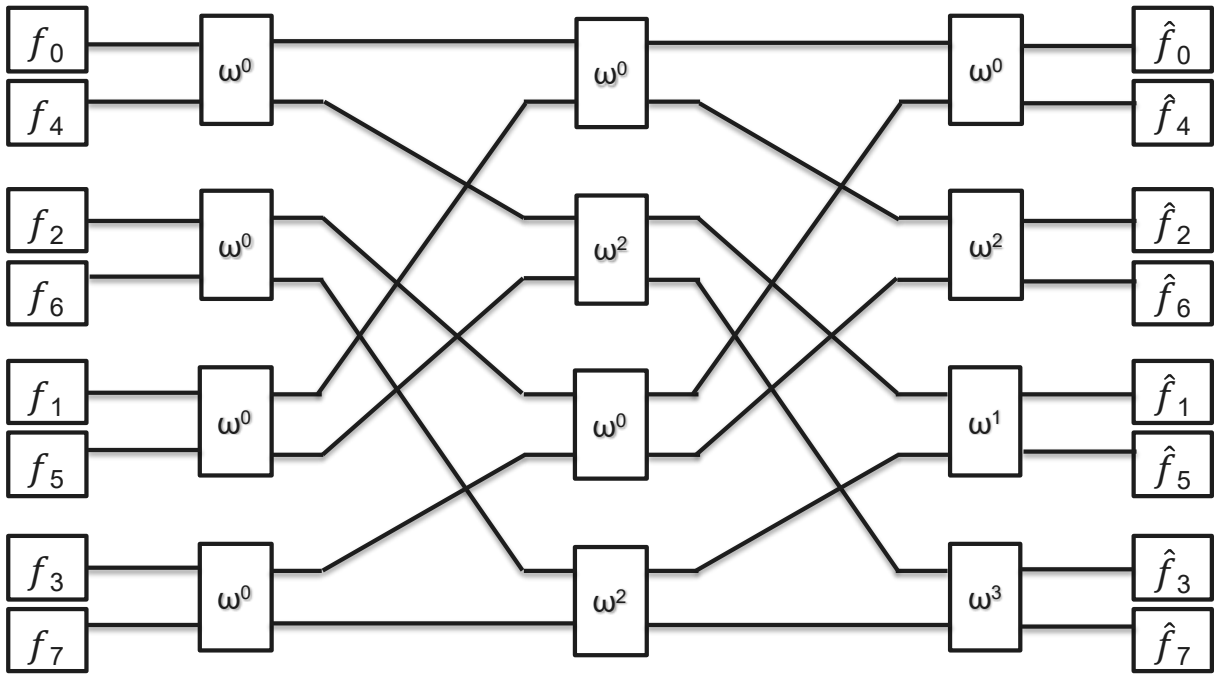
- **Fast Multiplication**

Calculate product as

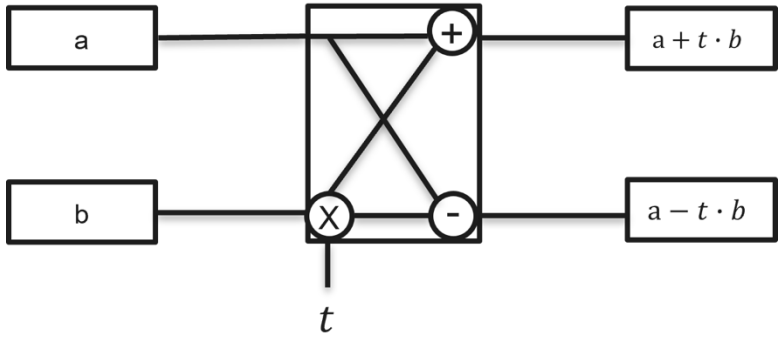
$$f \times g = NTT^{-1}\big(NTT(f) \circ NTT(g)\big)$$

where $\circ$ is the elementwise multiplication

Number Theoretic Transform

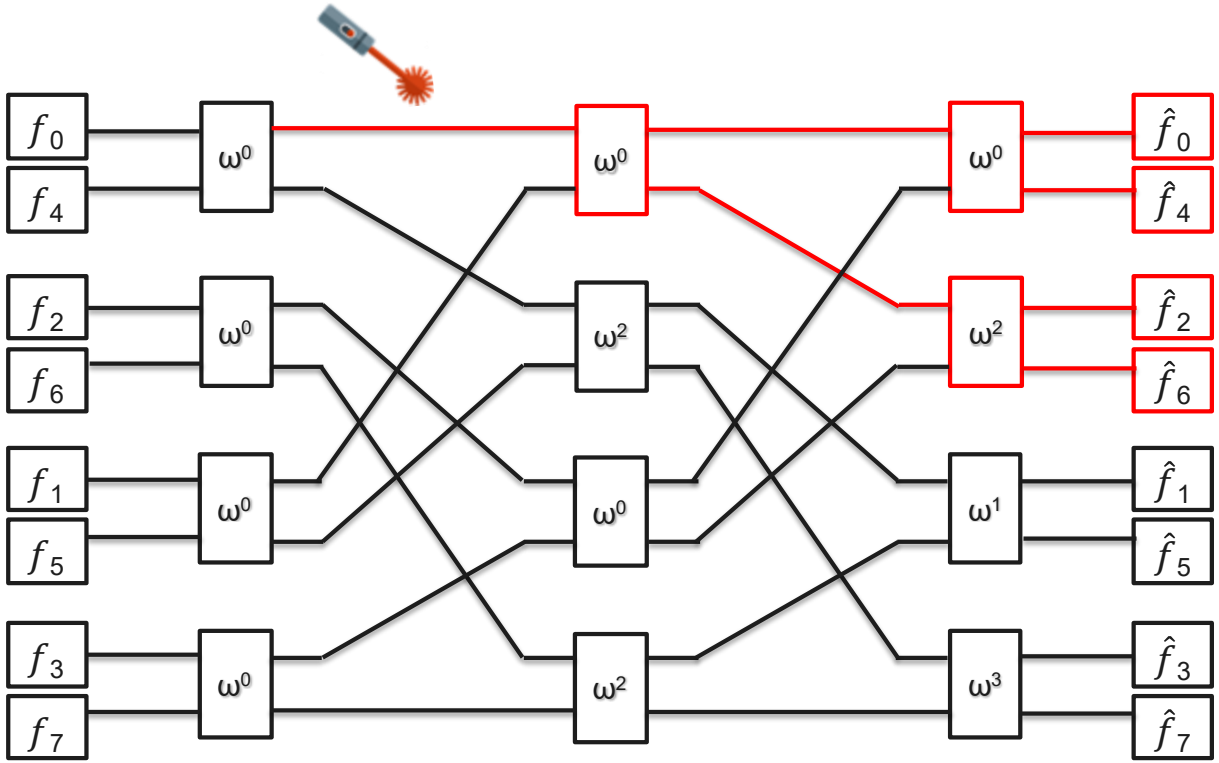


General structure of an NTT

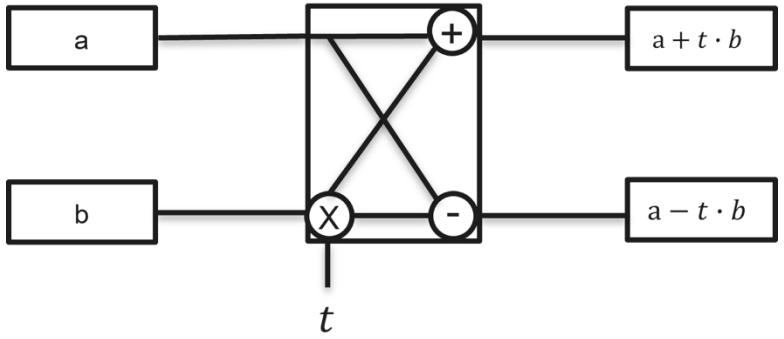


Breakdown into core operations

Number Theoretic Transform



General structure of an NTT

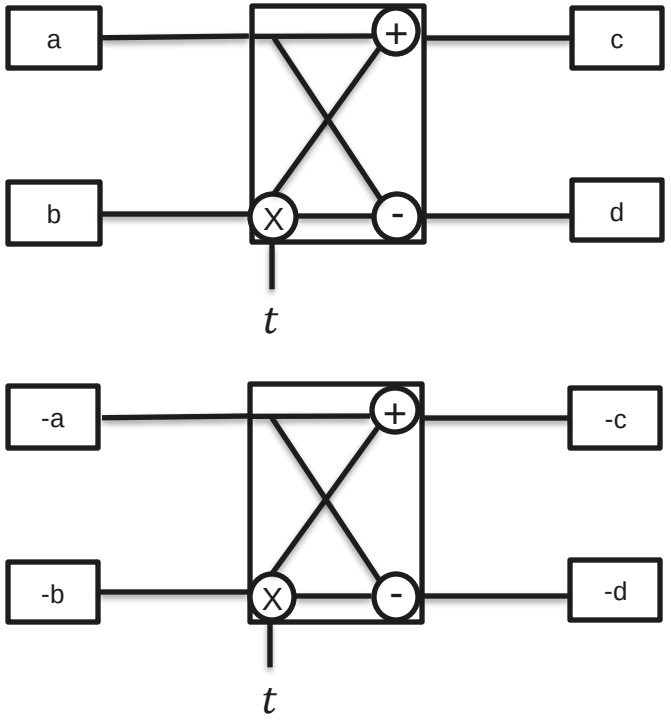


Breakdown into core operations

Recomputing (Sarker 2019)

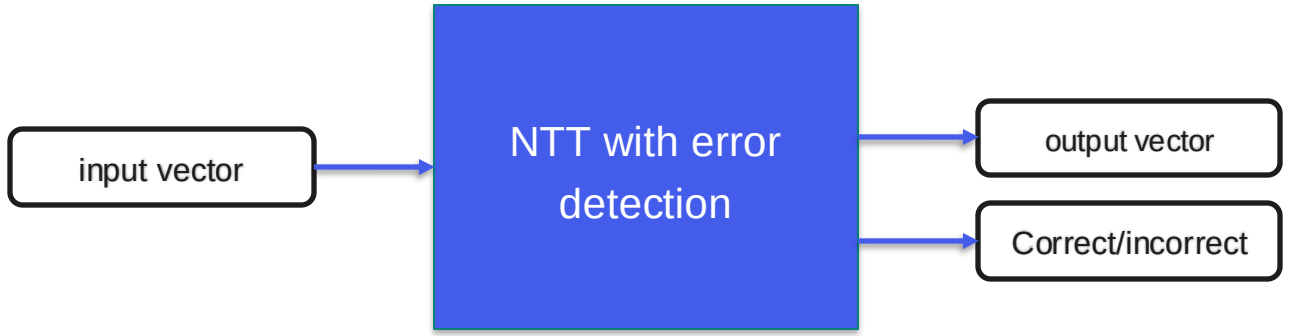
Techniques in the Literature

- Each butterfly operations is done twice → compare results



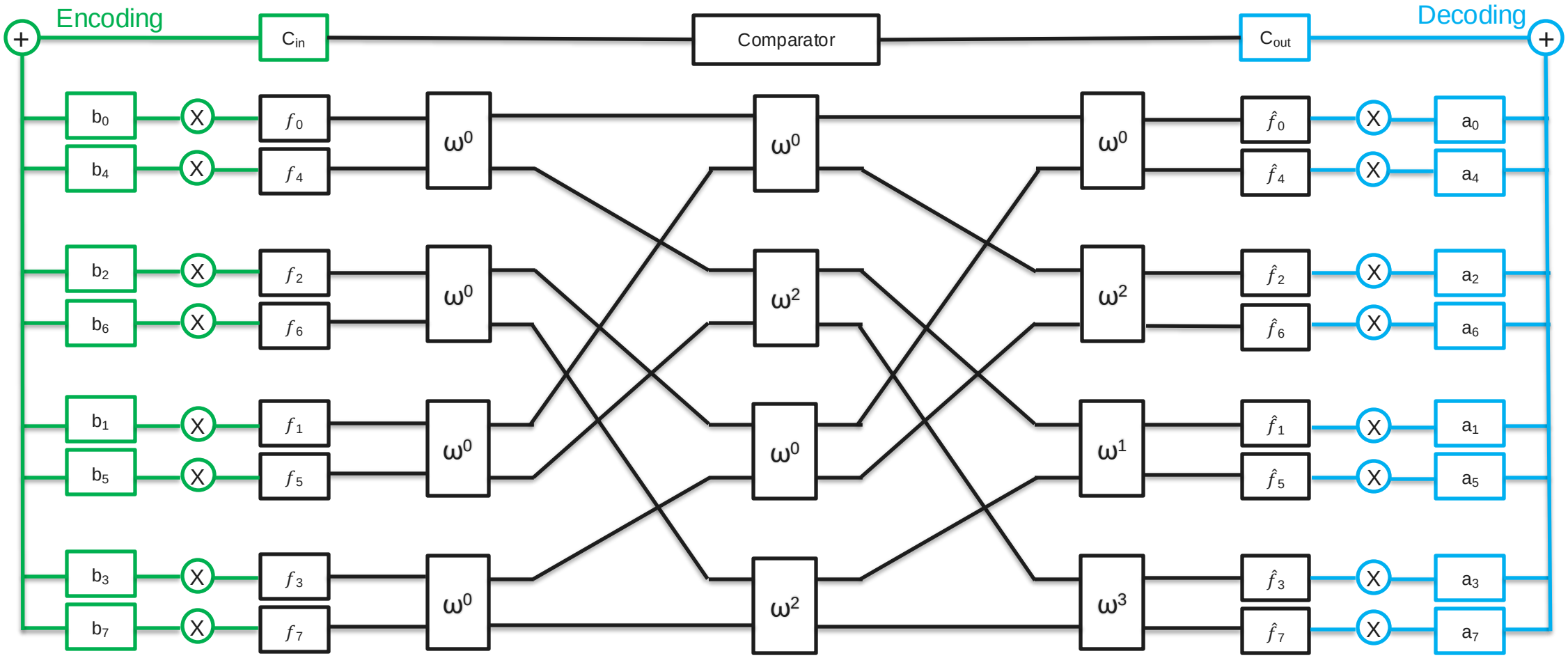
- Disadvantages:
  - high overhead
  - tests only butterfly calculations

- Our goal:
  - Test the whole NTT block with less overhead



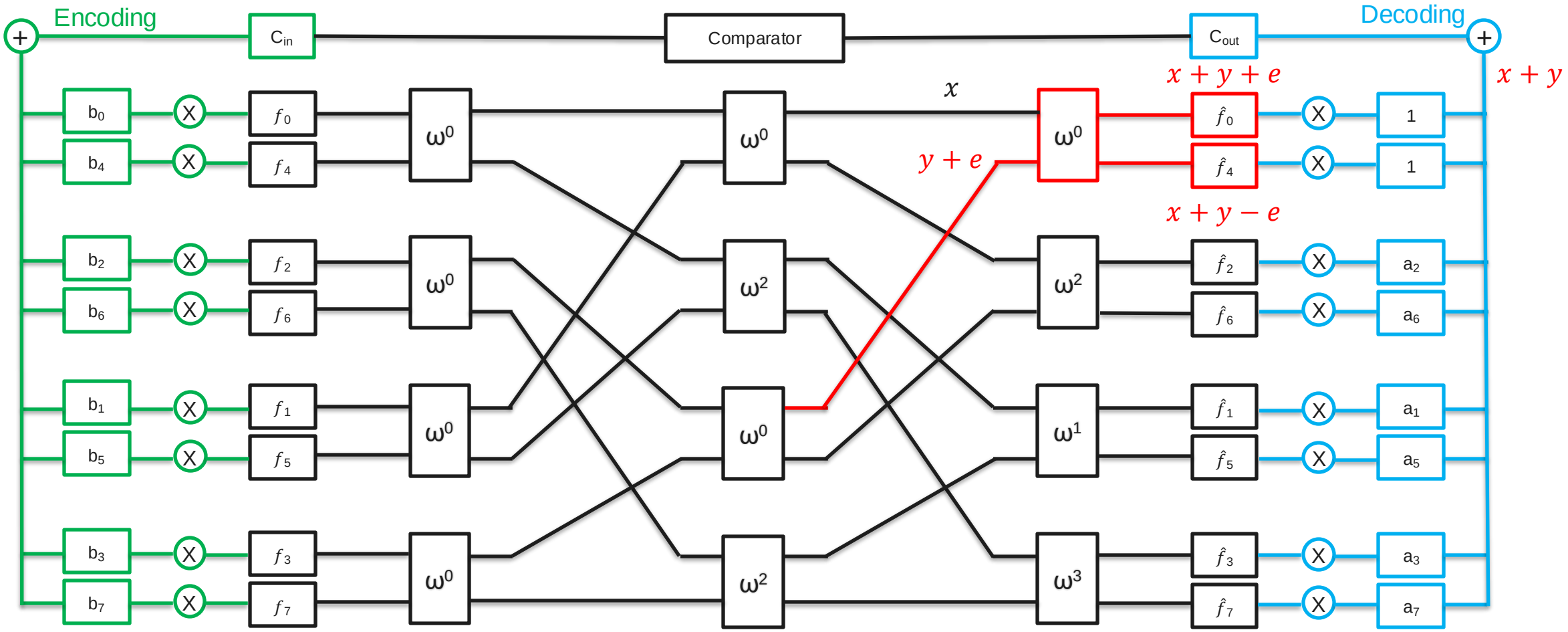
Weighted Checksums (Tao, Hartmann, and Chen 1990 and Wang and Jha 1994)

Applying methods known for FFT



Weighted Checksums (Tao, Hartmann, and Chen 1990 and Wang and Jha 1994)

Applying methods known for FFT



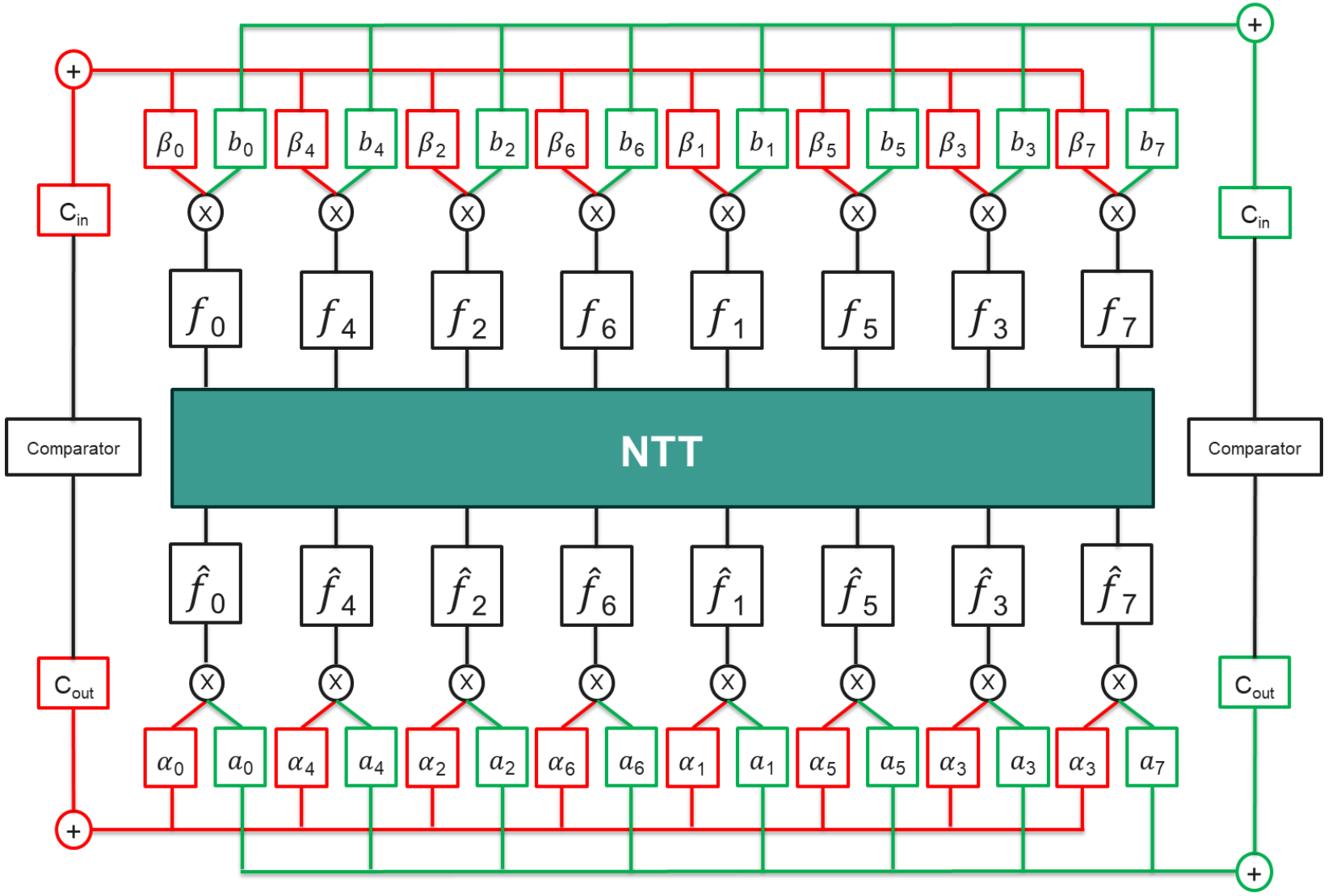
a_0 *and* a_4 *can not be the same*

Our work

- Derive conditions on **a's** to detect **one and two Faults in NTT network**
- One Fault:
  - show that **a** exists that meets these conditions for the parameter sets of **Dilithium, Falcon and Kyber**
  - we provide an efficient implementation that requires only $\boldsymbol{N}$ ***extra multiplications*** (recomputing $\boldsymbol{N/2\ log\ N}$ extra multiplications)

Scheme	Dilithium	Kyber	Falcon I	Falcon V
Overhead	0.25	0.286	0.222	0.2

Two error detection



Our work

- Derive conditions on **a's** to detect **one and two Faults in NTT network**
- One Fault:
  - show that **a** exists that meets these conditions for the parameter sets of **Dilithium, Falcon and Kyber**
  - we provide an efficient implementation that requires only $\boldsymbol{N}$ ***extra multiplications*** (recomputing $\boldsymbol{N/2\ log\ N}$ extra multiplications)

Scheme	Dilithium	Kyber	Falcon I	Falcon V
Overhead	0.25	0.286	0.222	0.2

- Two Faults:
  - show that **a's** exist that meet these conditions for the parameter sets of **Dilithium**
  - upper bound: about $\boldsymbol{N^2}$restrictions on $\boldsymbol{a_i} \in \mathbb{Z}_q^N$

Scheme	Ring degree N	N^2	Modulus q
Dilithium	256	65536	$<$ 8380417
Kyber	256	65536	$>$ 3329
FALCON I	512	262144	$>$ 12289
FALCON V	1024	1048576	$>$ 12289

Future work

- Find **a's** that also work for Kyber and Falcon

- Error correction

- Find Fault injection attacks and countermeasures on other PQC schemes
  - 40 new NIST **Additional Digital Signature Schemes** in Round 1