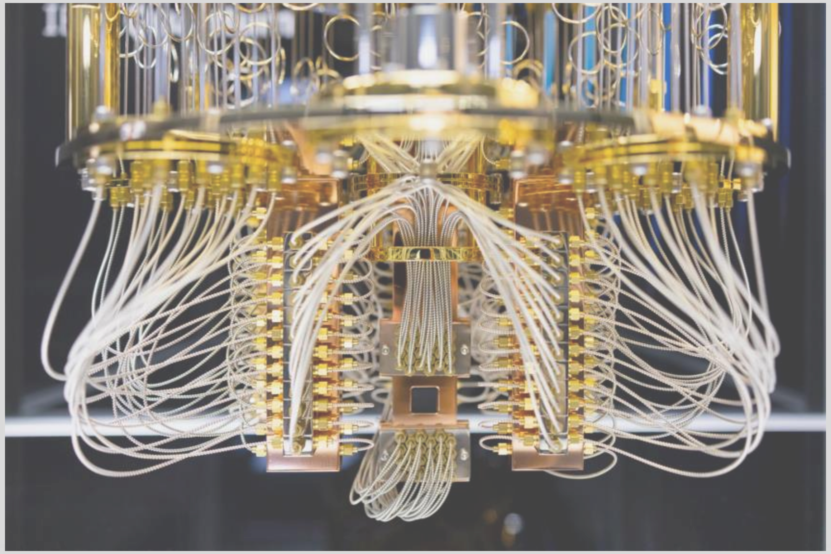
# Advancing Hardware Security in the Post-Quantum Cryptography Landscape: Challenges and Solutions

Qian Wang
UC Merced

# Quantum Computer Threat and Post Quantum Crypto Solutions



## 1000—10,000 qubits

IBM's quantum computing updates include the release of a 1,000-qubit quantum chip called Condor

Targets 2029 for the quantum computer to be operational. With more than 10,000 qubits

Around 4000-10000bit to break RSA2k

Around 2000-bit to break AES128

## Shor's Algorithm

Shor's algorithm [Shor'94] is expected to completely break RSA and ECC.

**Mitigation:** Replace all digital signature, key exchange and asymmetric encryption algorithms

## Grover's Algorithm

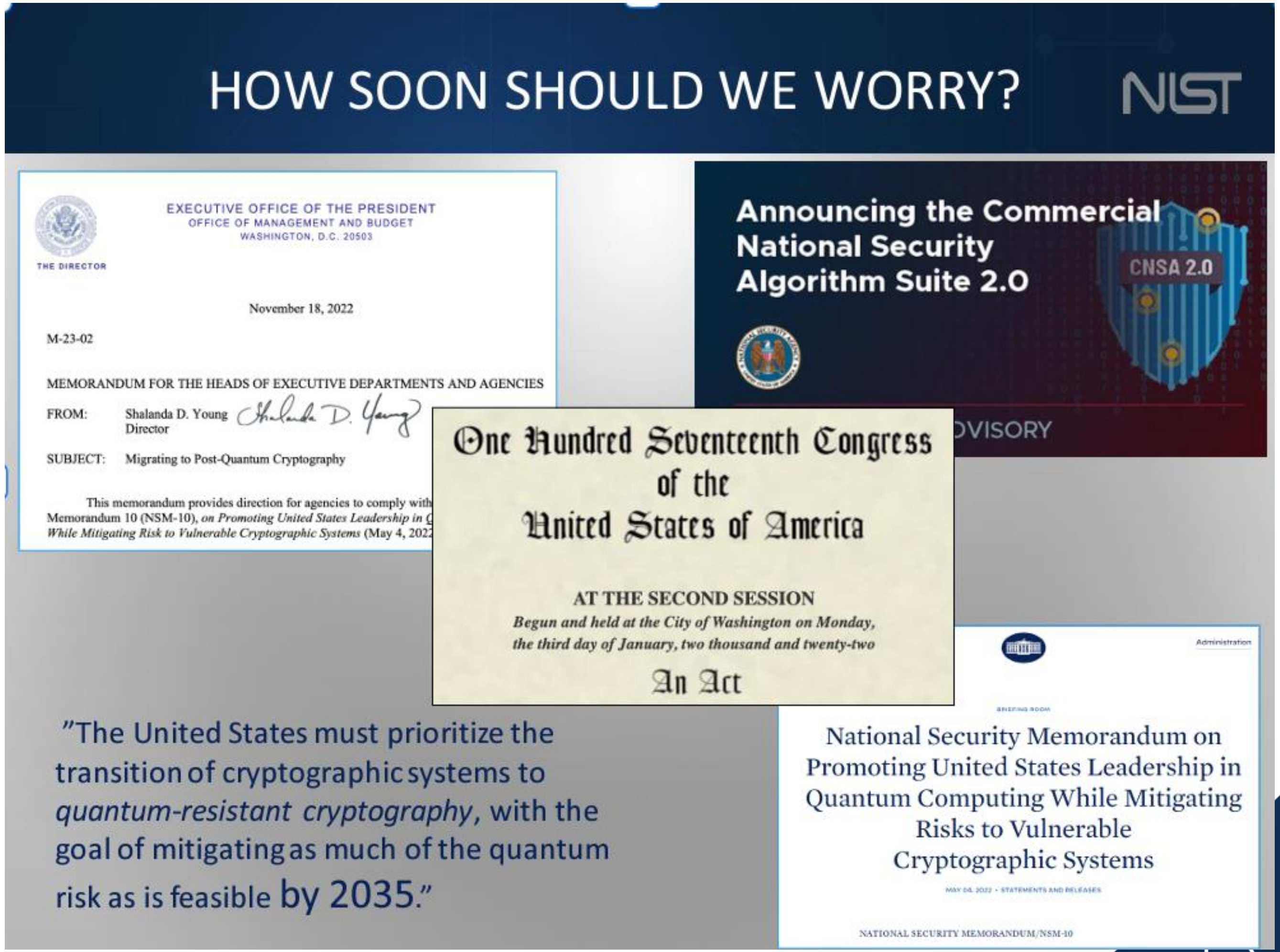
Grover's algorithm [Gro'96] is expected to break AES128 and SHA256.

**Mitigation:** Increase keys/parameters of algorithms (Ex: AES128 → AES256, SHA2-> SHA3)

# PQC Introduction

- Need to find cryptographic algorithms that are secure against attacks by both classical and quantum computers

- Clarification: Post-quantum cryptographic algorithms are supposed to be implemented in "classical" computers in the same way as RSA, DH, and ECDSA




From NIST'24 Workshop

UCMERCED

# NIST PQC Competition

- **2016** Criteria and requirements and Call for proposals
- **2017** Received 82 submissions and announced 69 **1st** round candidates
- **2018** NIST PQC Standardization Conference
- **2019** Announced 26 **2nd** round candidates
- **2020** Announced 7 **3rd** round finalists and 8 alternative candidates
- **2022** Announced **3rd** round selections (kyber, dilithium, falcon and sphincs+)
  And 4th round candidates
- **2022** called additional signatures
- **2023** released draft standards
- **2023** received 50 signature submissions and select 40 as first round
- **2024** publish the 1st set of PQC standards (summer)

# PQC Standardization Algorithms

## THE 1ST PQC DRAFT STANDARDS

- FIPS 203:  ML-KEM (KYBER)
- FIPS 204:  ML-DSA (DILITHIUM)
- FIPS 205:  SLH-DSA (SPHINCS+)
- FN-DSA (FALCON) – under development (will have other docs with more guidance/details)

More Security Mature

Less  Efficient

Hash-based schemes
Security: relies on well know security notions
Use: Digital Signature

Lattice-based schemes
Security: problems from lattice
Use: Encryption, Key Exchange, Signature

Less Security Mature

More Efficient

Many trade-offs of hash-lattice:
(un-)limited number of signatures vs.  efficient key generation vs.  signature size vs.  efficient sign/verify performance

# Hardware Security related PQC research

**System Implementation**
- Crypto Migration
- Various hardware platforms

**Side-channel Attack Resilience**
- Power, EM, Fault
- Micro-arch level attacks

**Performance Optimization**
- Parallelism
- Balance performance with power

**Associated Protocol updates**
- TLS protocols
- Bank Cards

UCMERCED

# System Implementation

*History shows that crypto migration takes a considerable amount of time*

- ECC: proposed by mid-1980’s + 2 decades to gain some adoption
- AES: 4 years of competition + more than a decade to gain wide adoption
- SHA-3: 5 years of competition + 6 years since publication. No wide adoption (yet?)

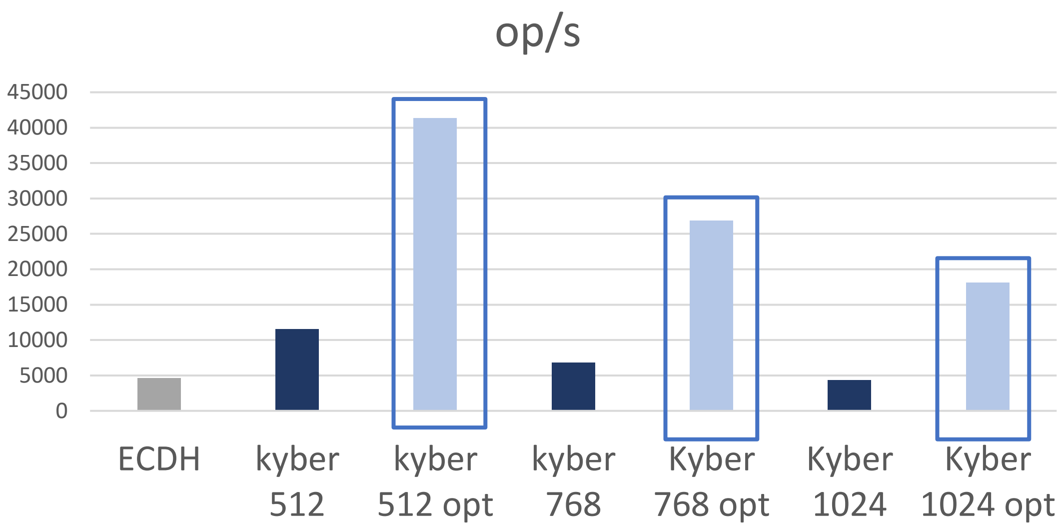
*Guided Timeline*

- NIST: Standardization of Algorithm *at 2024*
- NSA: NSA expects the transition to QR algorithms for NSS to be
complete *by 2035*
- Industry adoption: Long-term transition ?

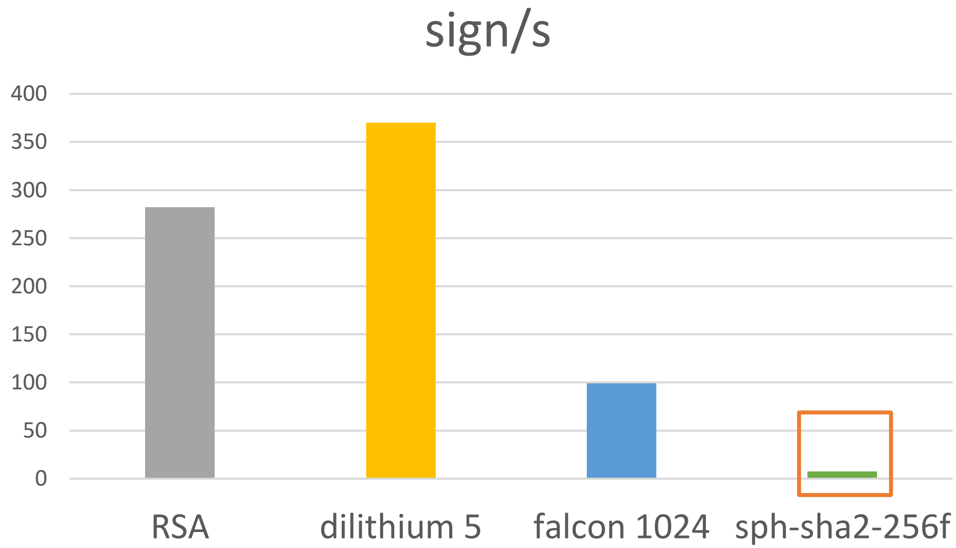
Google, for example, has already started implementing hybrid PQC algorithms in its products, signaling a move towards broader industry adoption

# Acceleration and Optimization

KEM performance compared to default ECDH




Signature Performance compared to default RSA

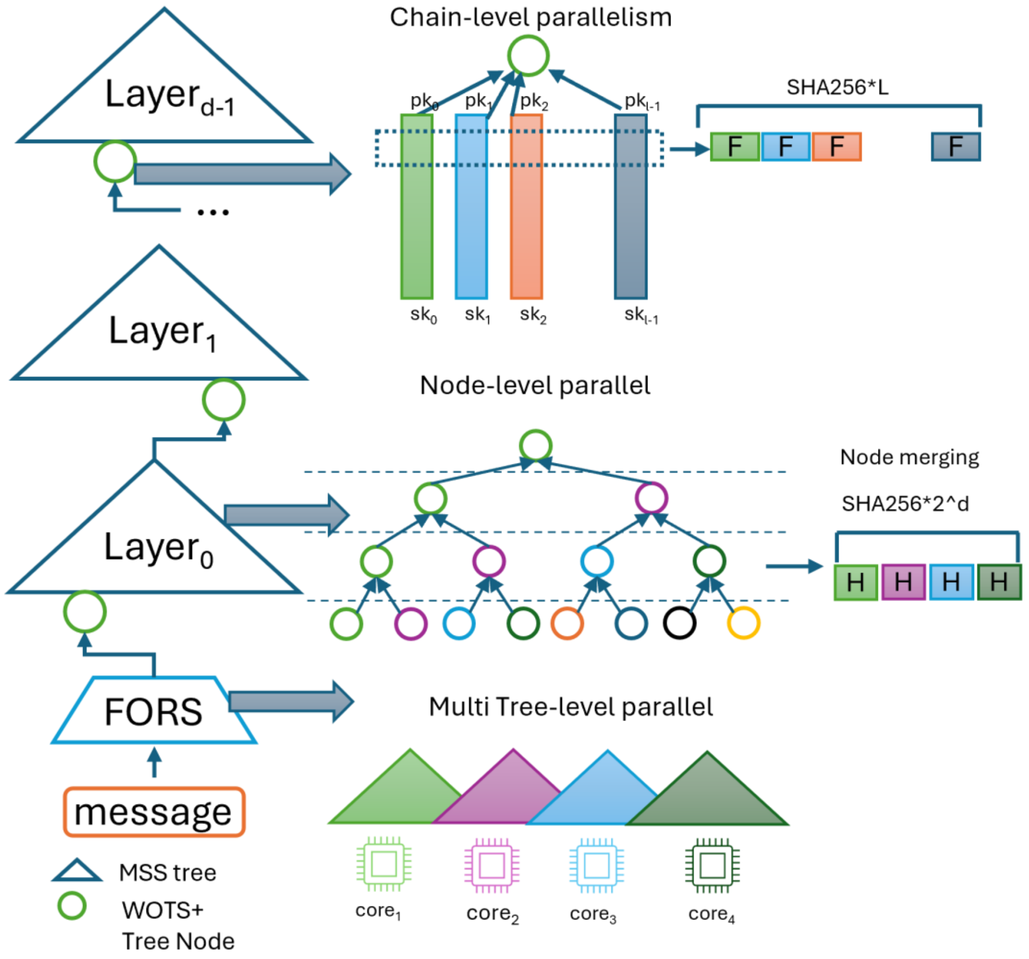



AVX2 optimization may gains x4 performance

Sphincs+ ~ x100 slower than the RSA and the other PQC SIG

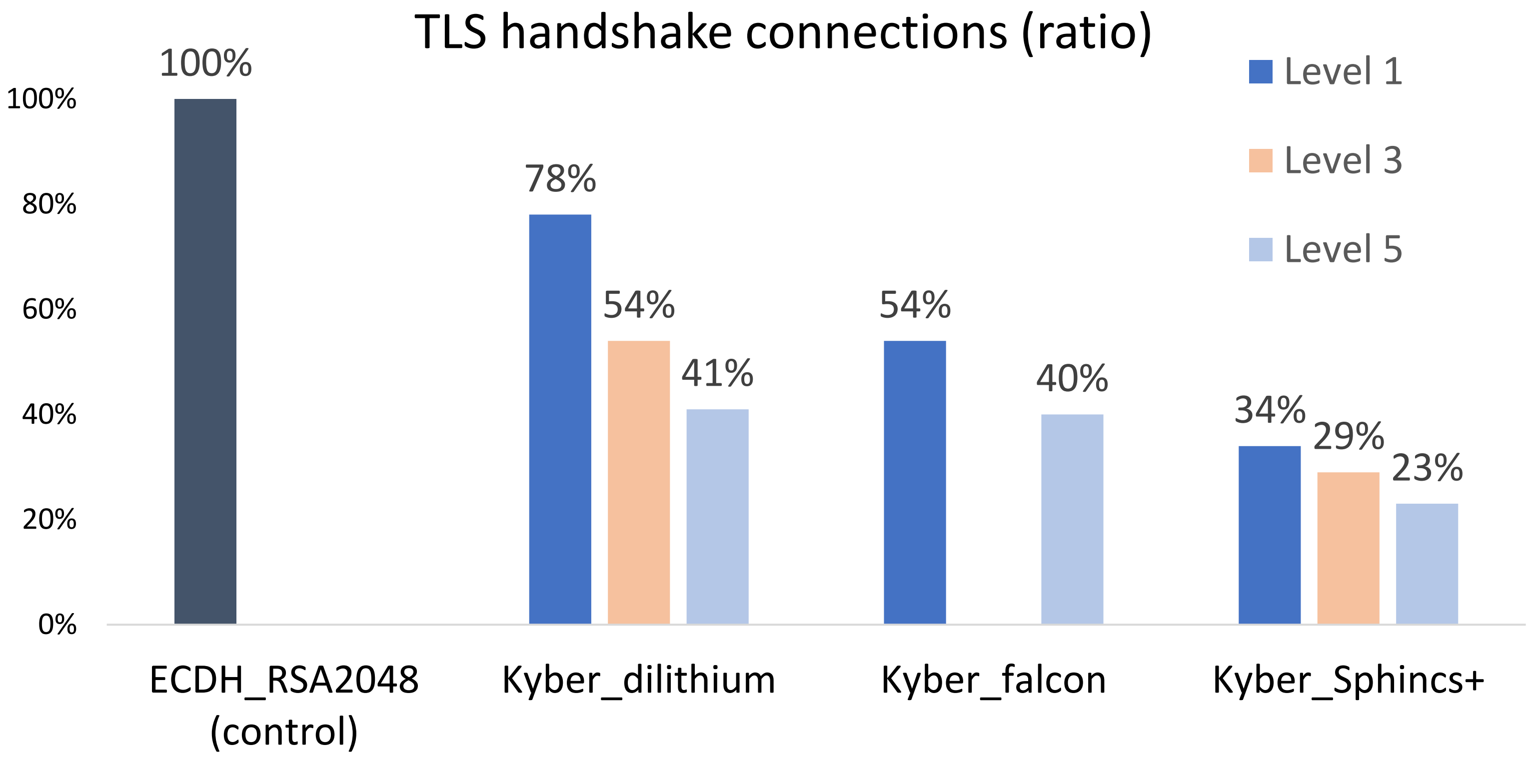
# Acceleration and Optimization

Hash-based Schemes, such as Sphincs+ lowest Performance due to thousands hash calls



# System Adoption

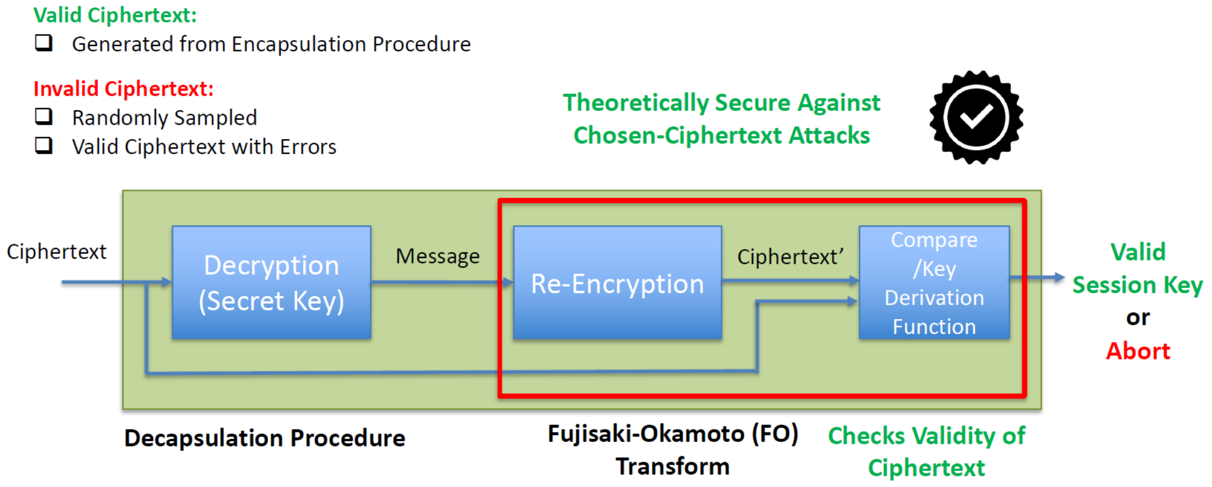
TLS Handshake performance on Cortex A72

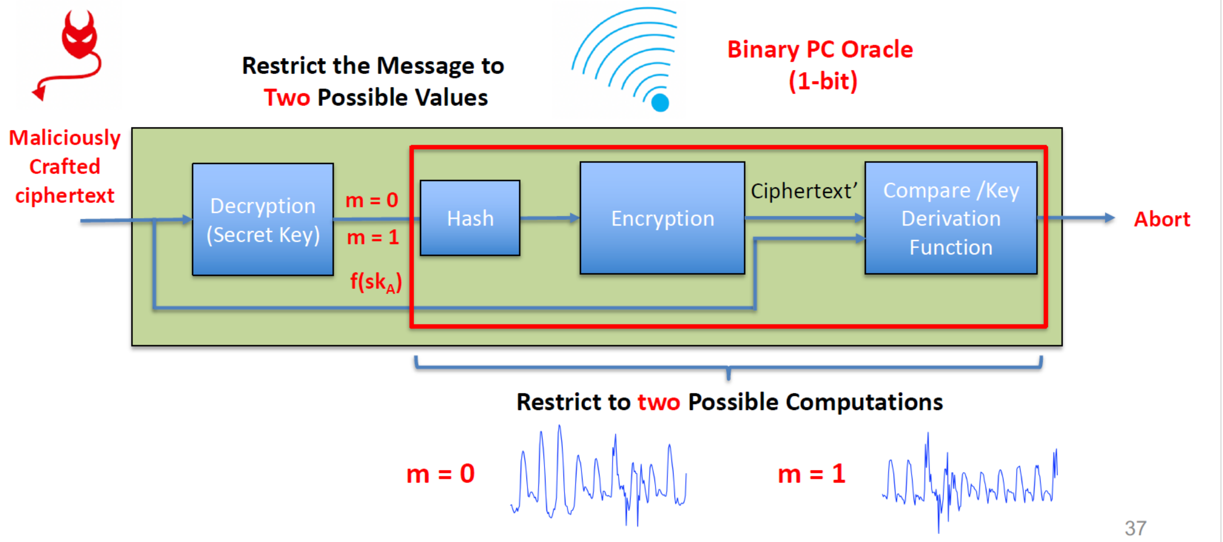



Signature and Ciphertext size are the bottleneck of PQC adoption in protocol

# Side-channel evaluation on Kyber

## Power Side channel on FO transform



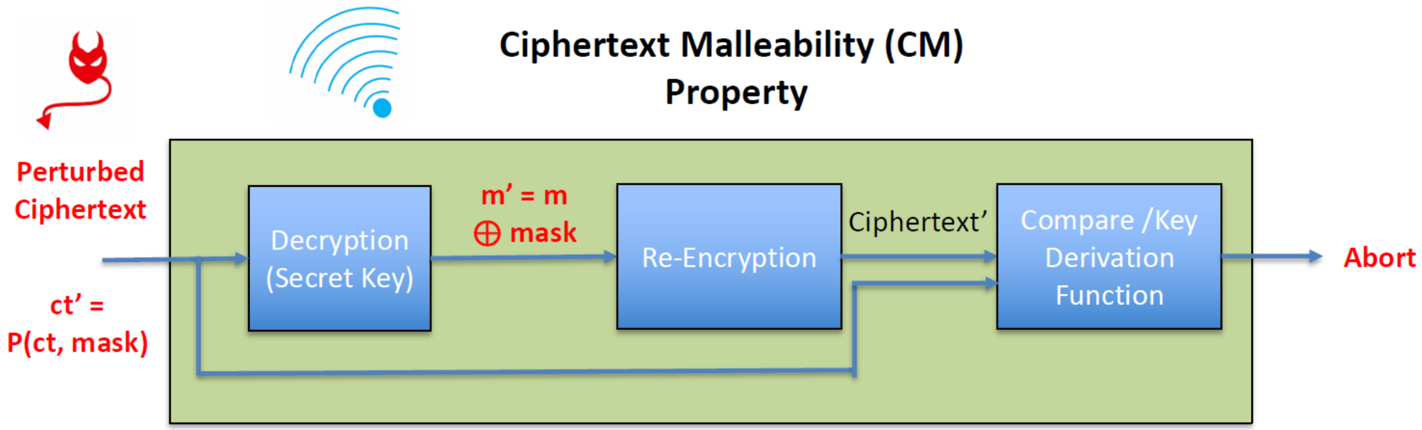

The FO transform mainly involves re-encryption after decryption which enables to detect invalid or maliciously formed ciphertexts and return failure upon detection.

Side-channel pattens reveals the difference in power of m=0, v.s., m=1. thus reveals the function of f(sk), off-line analysis could retrieve the full key.

# Side-channel evaluation on Kyber

## Countermeasures

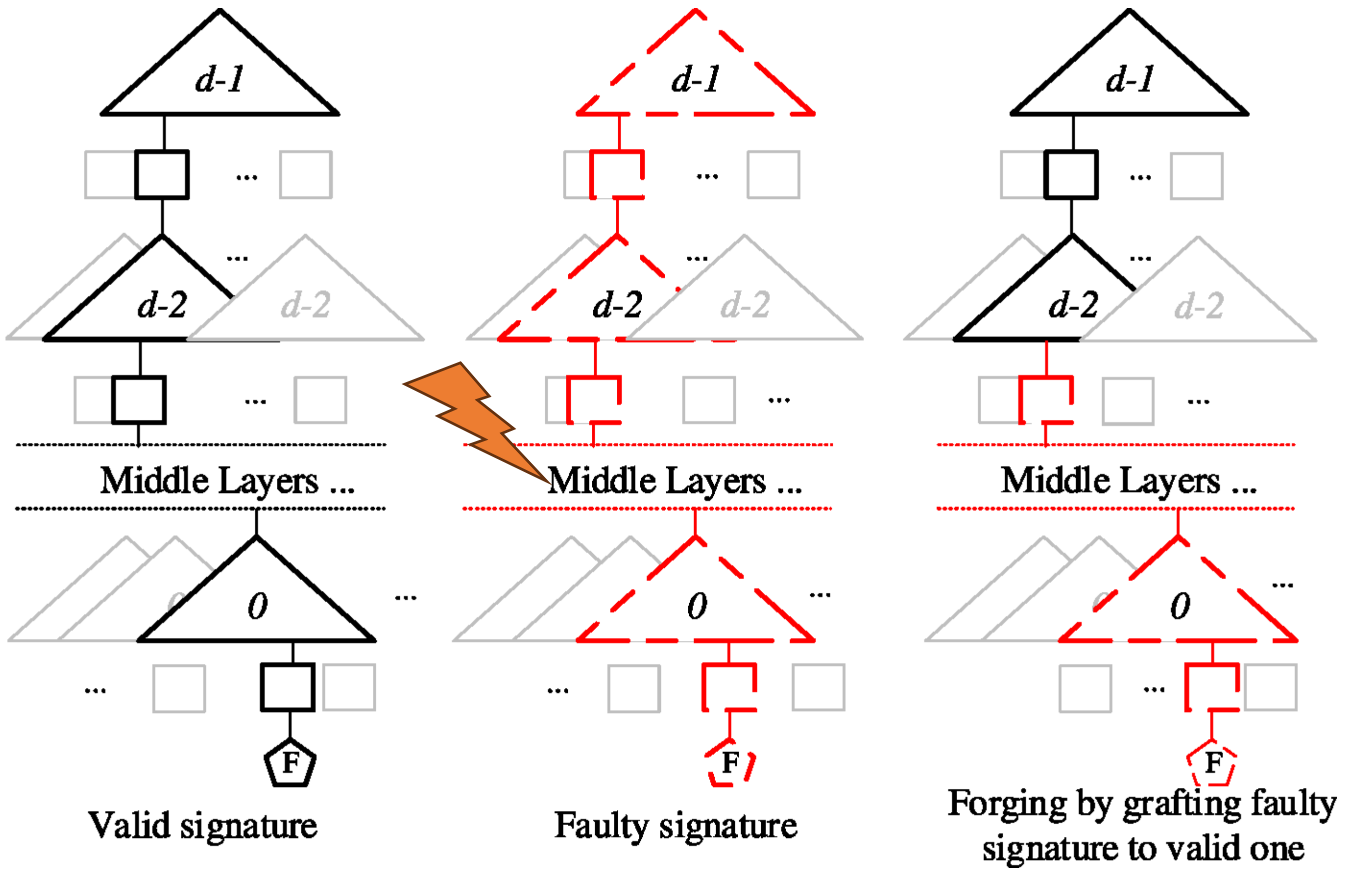
Let Encrypt(m) = ct




Masking the intermediate result?
Overhead of implementation: x4 –x5 times slower (20-25%).
Fast arithmetic masks available on embedded system but not on general platforms.

# Fault attacks on Hash-based Scheme

Reconstruct tree to forgery the valid signatures



# Final Remarks

- PQC transition is an unprecedented move and Industry perspective is critical for wide adoption
    - Ease of deployment
    - Scalability
    - Maintenance
- Hash-based or Lattice-based
    - Simple & well-understood is better than complex & less-understood
    - Diversity is needed
- Security analysis evaluate with cost of security
    - Side-channel attacks


UCMERCED