FortifyIQ

# Protecting PQC Algorithms against Physical Attacks


**Yaacov Belenky**

Chief Innovation Officer
FortifyIQ

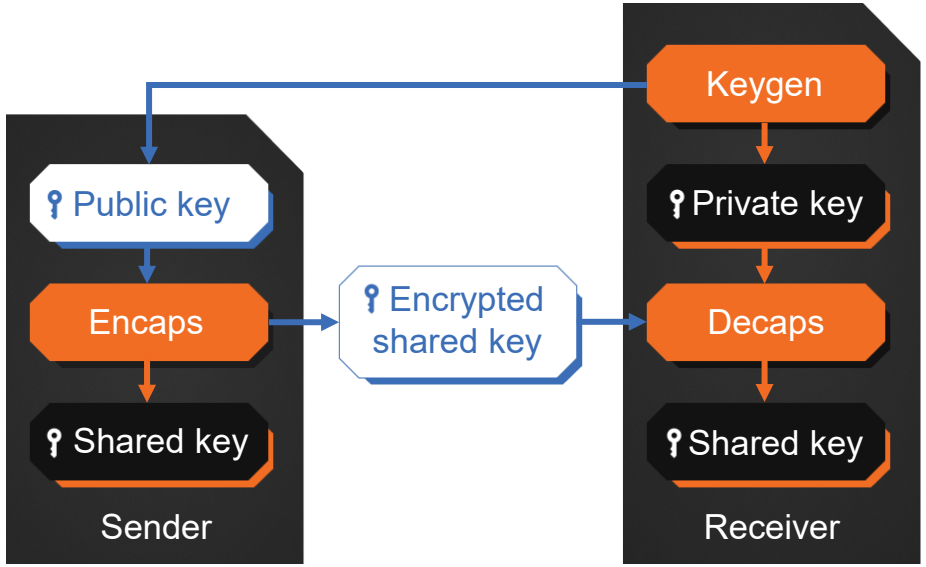

www.fortifyiq.com

# Why PQC Is *Urgent*

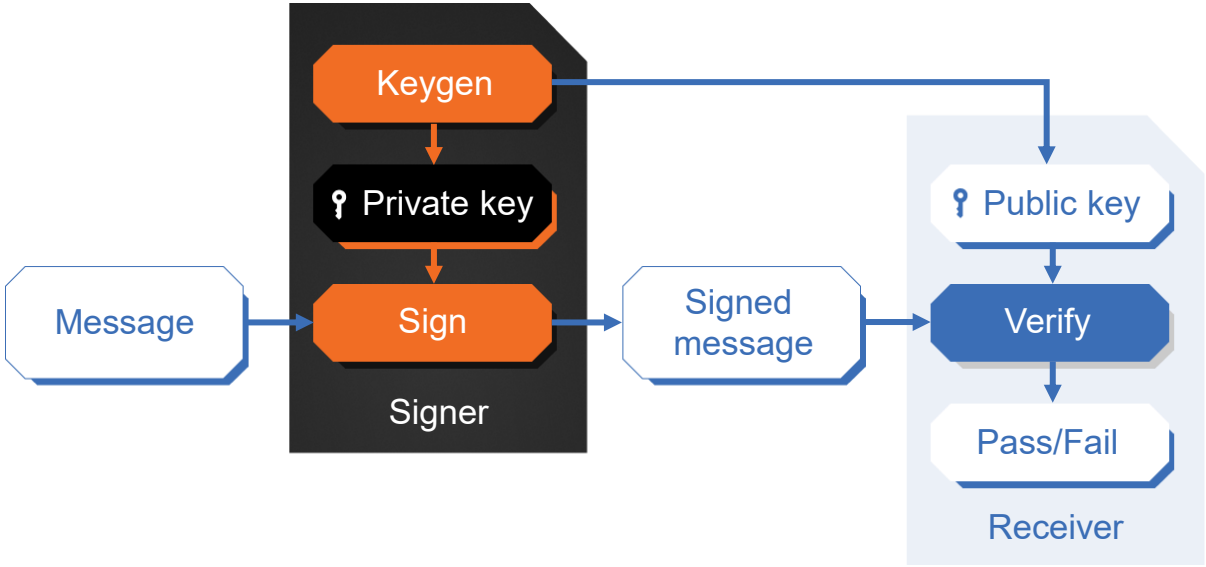
- All today's asymmetric cryptography algorithms are vulnerable to quantum computer attacks, regardless of the key size.
- "Harvest-now, decrypt-later" is happening.
- NSA (CNSA 2.0), BSI, and ANSSI mandate migration:
  - Deprecation in 2030
  - Disallowance in 2035
- Long-life systems: vehicles, satellites, industrial IoT, etc. must adopt PQC today.

# Ideal World – Black Boxes, Perfect Security

## (for PQC Algorithms – Including Quantum Adversaries)

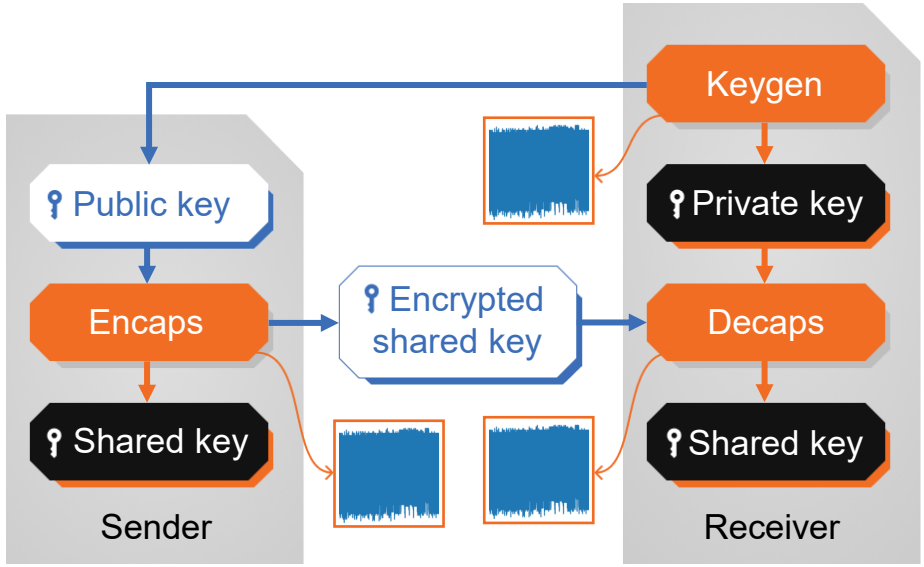



Secure Key Establishment
(e.g., ML-KEM)

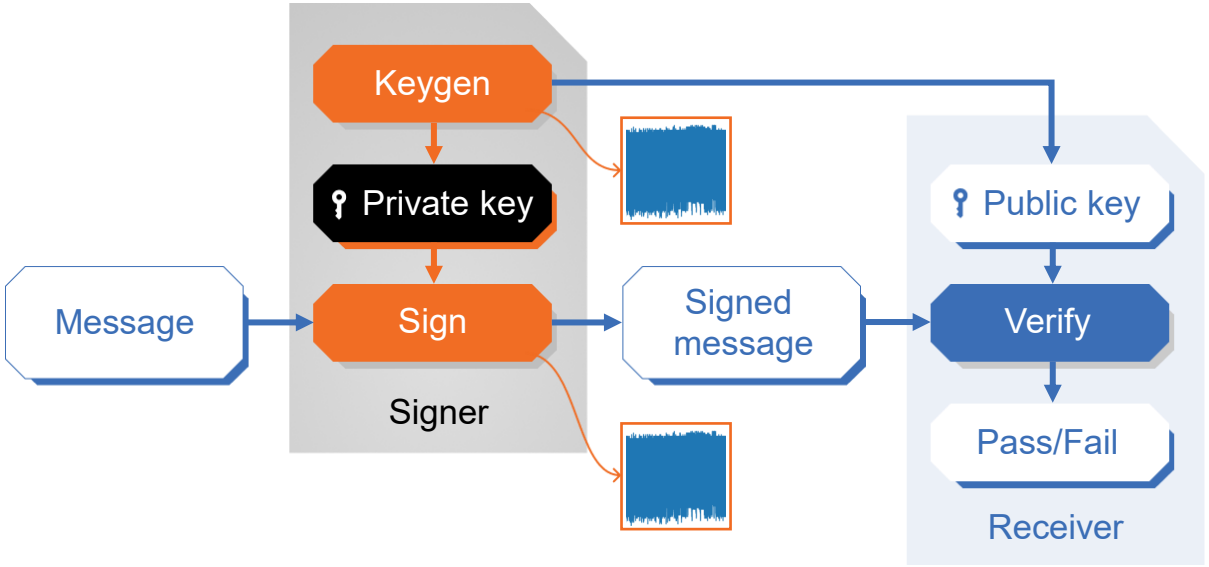



Digital Signing and Verification
(e.g., ML-DSA)

# Real World – Grey Boxes, Side-Channel Leakages

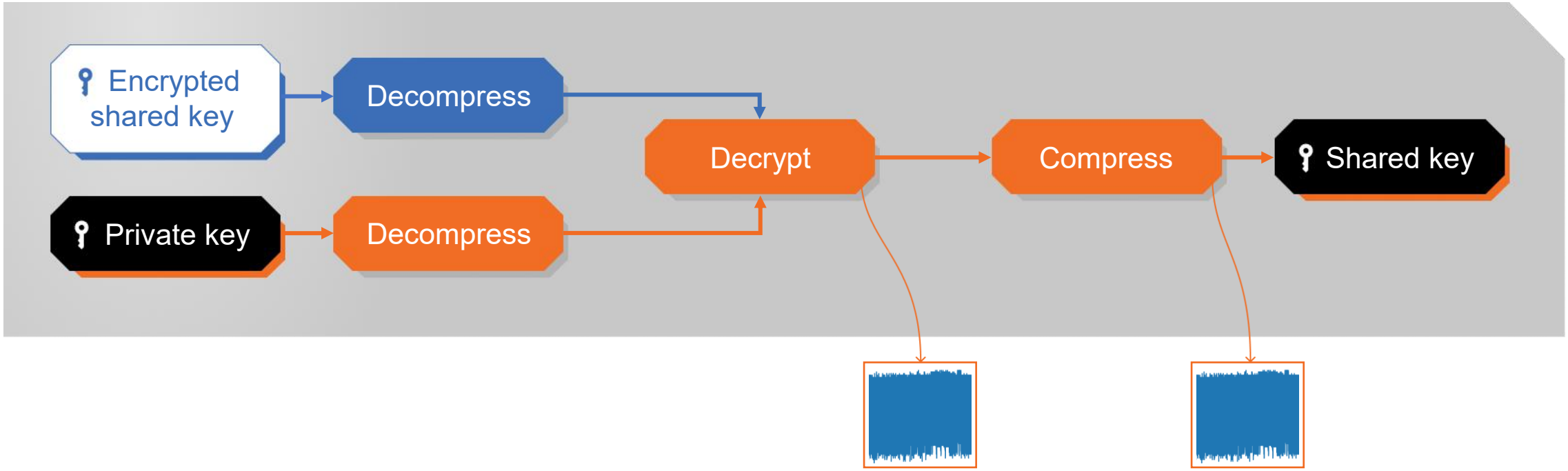



Secure Key Establishment
(e.g., ML-KEM)

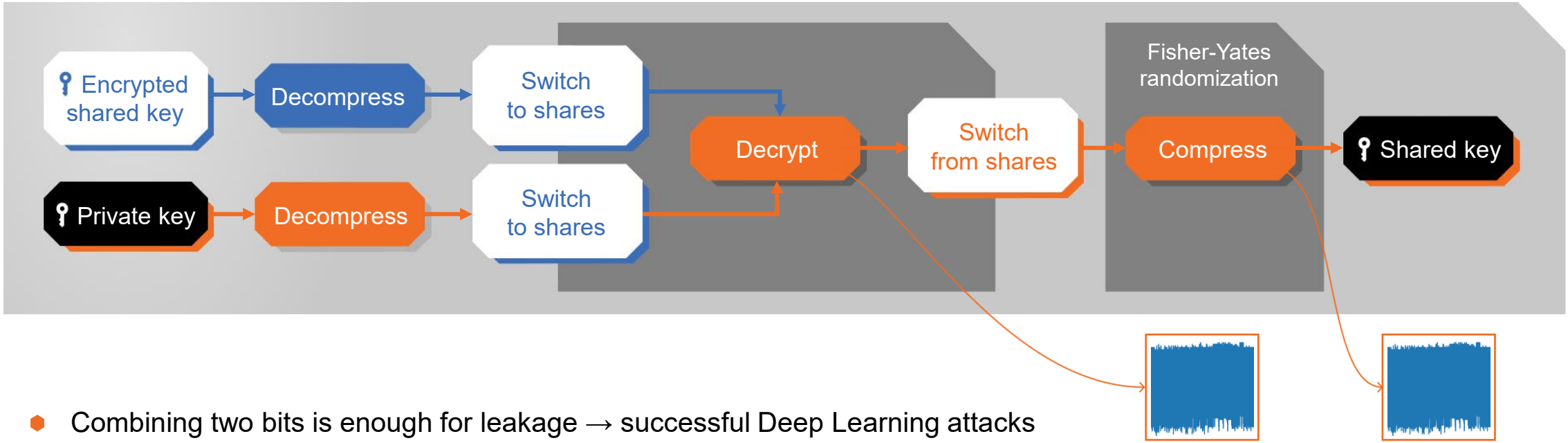



Digital Signing and Verification
(e.g., ML-DSA)

# Unprotected Kyber Decapsulation



# Kyber Decapsulation Protected Using Shares



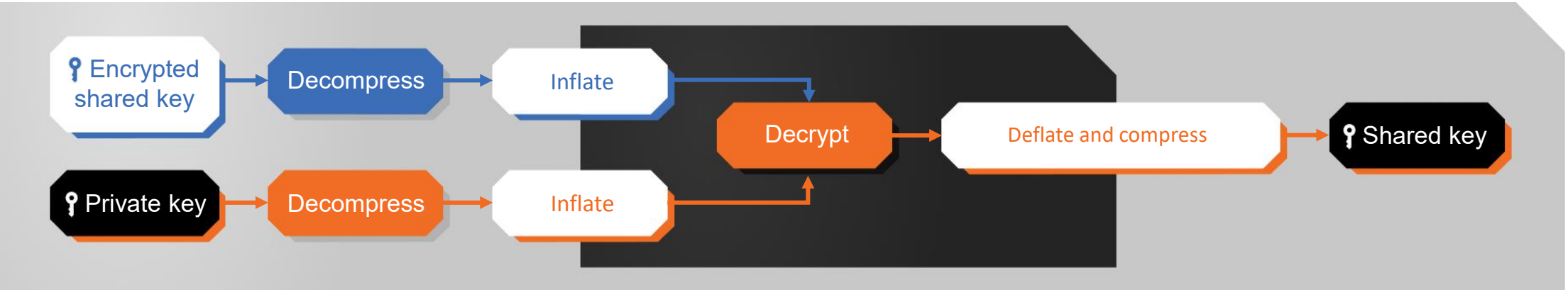

- Combining two bits is enough for leakage → successful Deep Learning attacks
- No protection of the compression in decaps and decompression in encaps
- The suggested protections (the Fisher-Yates randomization) have been successfully attacked
- Very significant performance degradation, especially in SW implementations

# Attacks on Unprotected Implementations and Protected Implementations Using Shares

- Side-Channel and Fault Attacks on ML-KEM and ML-DSA – an introduction into ML-KEM and ML-PQC, countermeasures, and 6 side-channel attacks, 2 of them on protected implementations
- A Chosen-Ciphertext Side-Channel Attack on Shuffled CRYSTALS-Kyber – an attack on protected (shuffled) ML-KEM
- Secret Key Recovery Attacks on Masked and Shuffled Implementations of CRYSTALS-Kyber and Saber – an attack on protected (masked and shuffled) ML-KEM
- … and many others

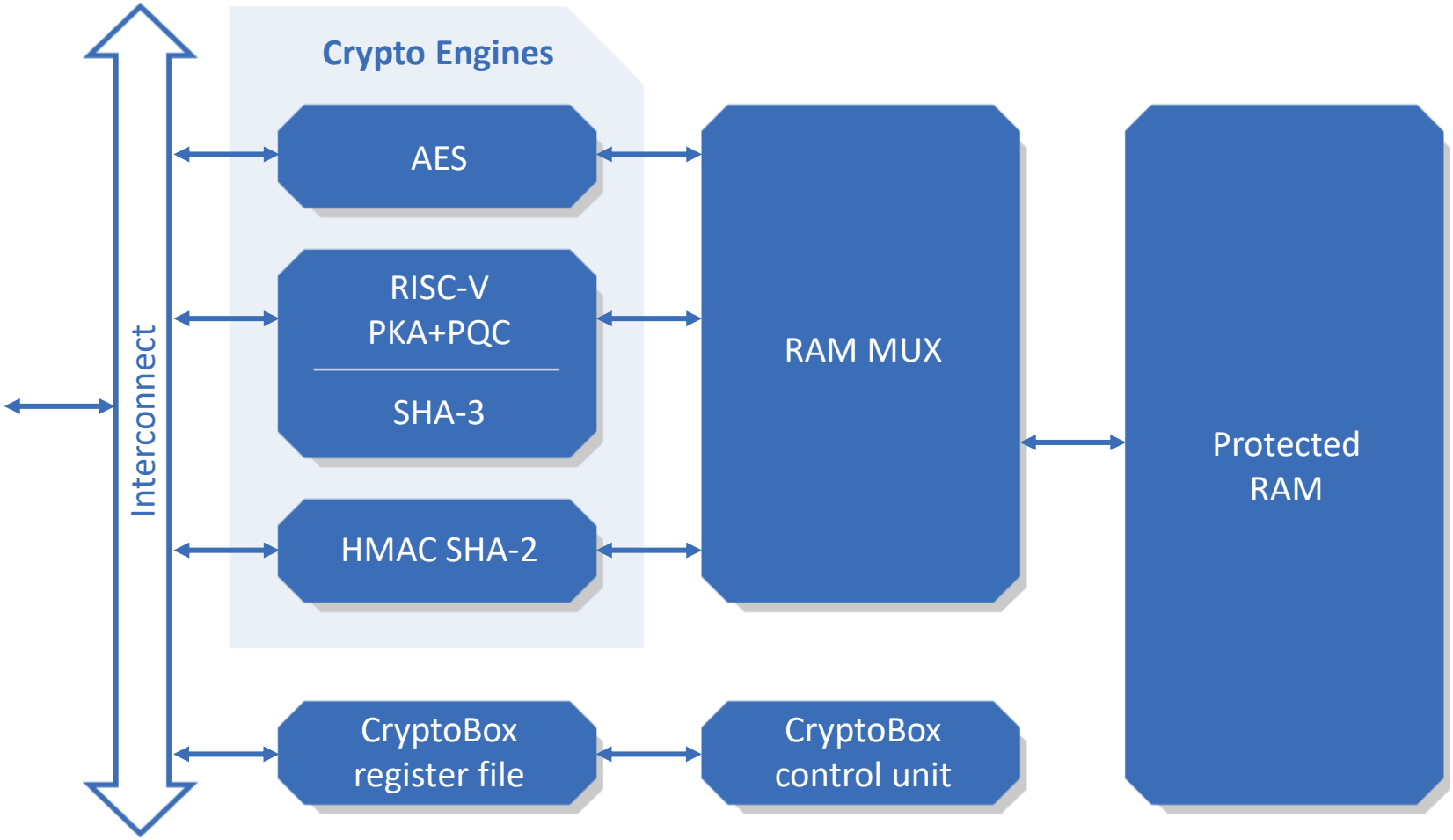
# FortifyIQ – Kyber Decapsulation Protected Using “Inflation” (patent pending)

## You do not need to choose between secure, fast and compact anymore!




- Any pair or triplet of bits contains only a negligible information
- Decompression and inflation are merged where necessary, and so are deflation and compression
- Excellent PPA:
  - In HW: Tradeoff between matching or exceeding the performance of a naïve implementation and minimizing the area
  - In SW (compared to a naïve implementation):
    - Significantly smaller data RAM size
    - The same code size
    - Performance on par

# FortifyIQ's CryptoBox



## Eliminate DPA&FIA Vulnerabilities


## IP Cores

### FortiCrypt

**AES XP**
Ultra High Bandwidth IP Core

**AES SX**
Balanced IP Core

**AES ULP**
Ultra Low Power IP Core

**AES UC**
Ultra Compact IP Core

### FortiMac

**HMAC SHA2-XP**
High-Performance IP Core

**HMAC SHA2**
IP Core

### FortiPKA

**FortiPKA**
Public Key Accelerator

**FortiPKEx**
Public-Private Keys Exchanger

**FortiPKA+PQC***
Hybrid PKA and PQC Accelerator

### FortiPQC

**ML-KEM**
(Kyber)*

**ML-DSA**
(Dilithium)*

*fully customized solution

## Cryptographic Toolboxes

### FortiCryptoBox
Orchestrated by RISC-V

**FortiCryptoBOX-UC**
Ultra Compact Package of PKA, AES, and HMAC Accelerators

**FortiCryptoBOX-XP**
Ultra High-Performance Package of PKA, AES and HMAC Accelerators

- FortiCrypt
- FortiMac
- FortiPKA
- FortiPQC

**FortiCryptoBOX-PQC**
Ultra Compact Package of PKA+PQC, AES, and HMAC Accelerators

## Roots of Trust

### FortiTrust

**Forti-IoT**
Ultra Compact RoT

**Forti-AI***
Ultra High-Performance Package of PKA, AI RoT

**Forti-Chiplet***
Chiplet RoT

**Forti-Cloud***
Cloud RoT

**Forti-General**
Configurable General Purpose RoT

FortiCryptoBox
- FortiCrypt
- FortiMac
- FortiPKA
- FortiPQC

## FortiEDA
### Pre-Silicon Security Verification

Side Channel Studio — SCOPE IQ — SCORE IQ

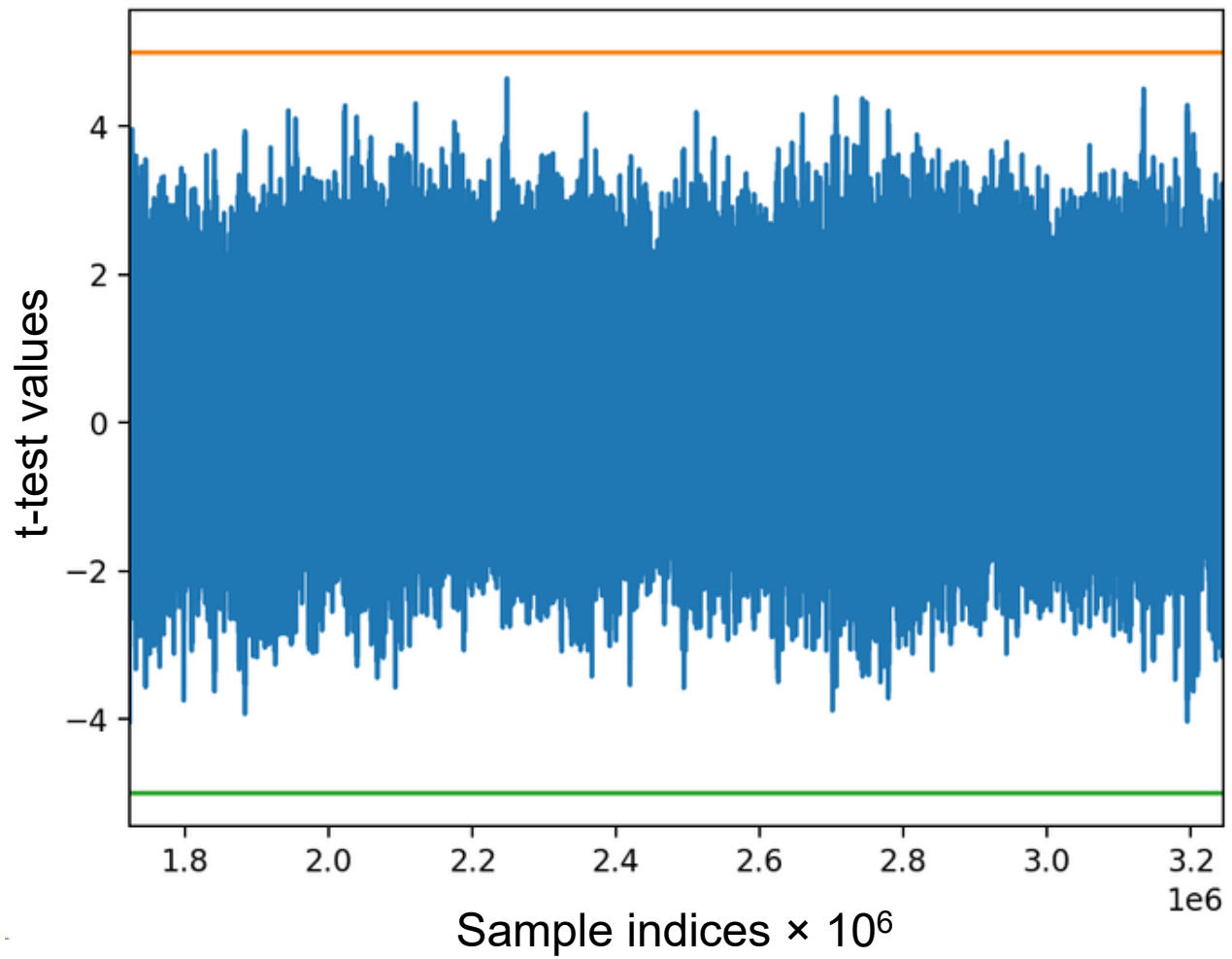
Fault Injection Studio — FAST IQ — FIRE IQ

## FortiCryptoLibraries

- FortiAES
- FortiMac
- FortiECC/RSA
- FortiML-KEM
- FortiML-DSA

FortifyIQ

# TVLA Assessment of FortiPQC Library Kyber (ML-KEM) Using FortiEDA



# Thank you!

info@FortifyIQ.com

81 Washington Street, Suite #307
Salem, MA 01970
USA

www.fortifyiq.com