A Masked Pure-Hardware Implementation of Kyber Cryptographic Algorithm

Tendayi Kamucheka, Alexander Nelson, David Andrews, Miaoqing Huang

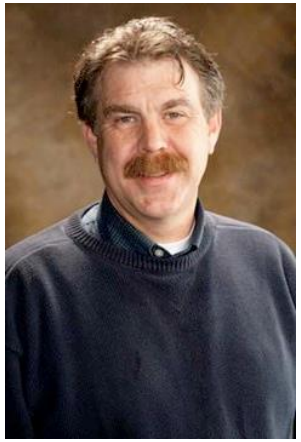
Acknowledgement: NIST – Award 60NANB20D016

About Us

- Computer Systems Design Lab & AESIR Lab at University of Arkansas – Computer Science & Computer Engineering Department

- Background – Hardware design, Embedded Systems, High Performance Computing, FPGAs, GPGPU



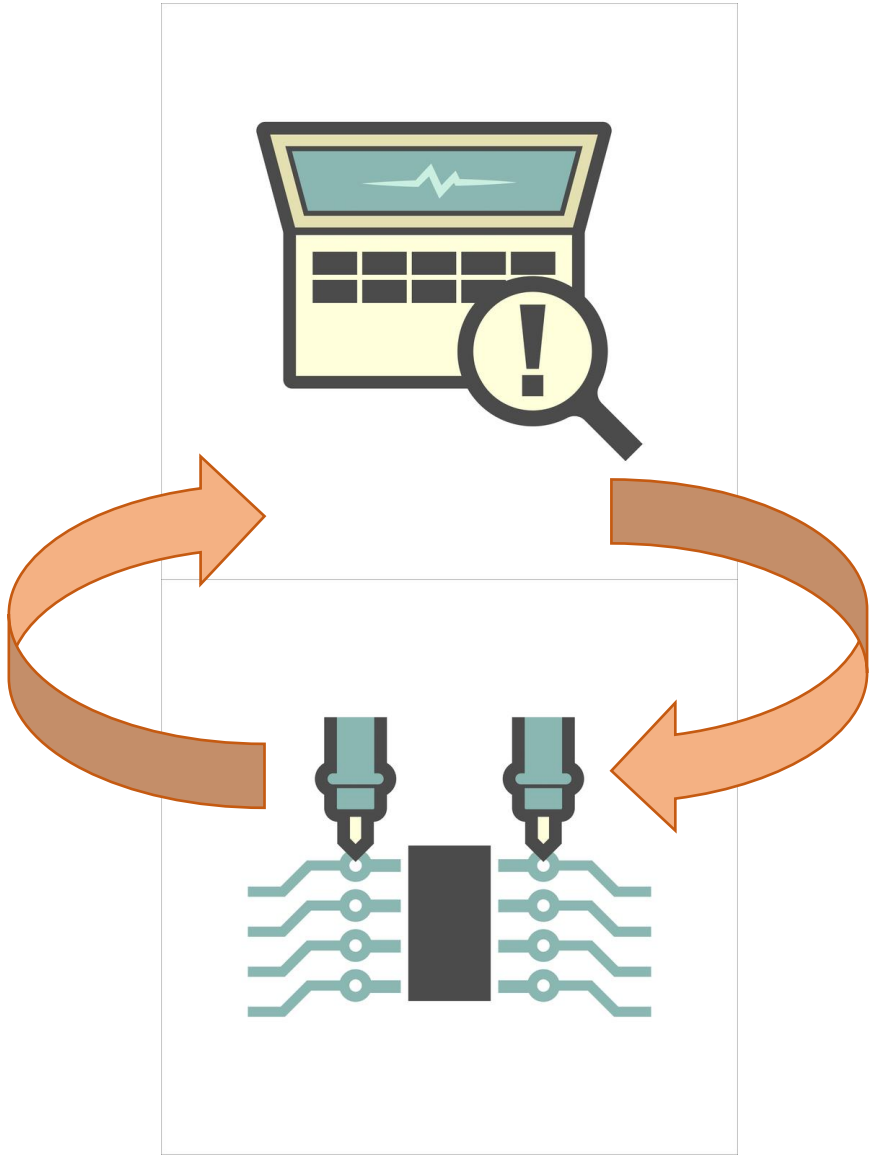



(Top) Tendayi Kamucheka, Alexander Nelson
(Bottom) David Andrews, Miaoqing Huang

UNIVERSITY OF ARKANSAS

Motivations

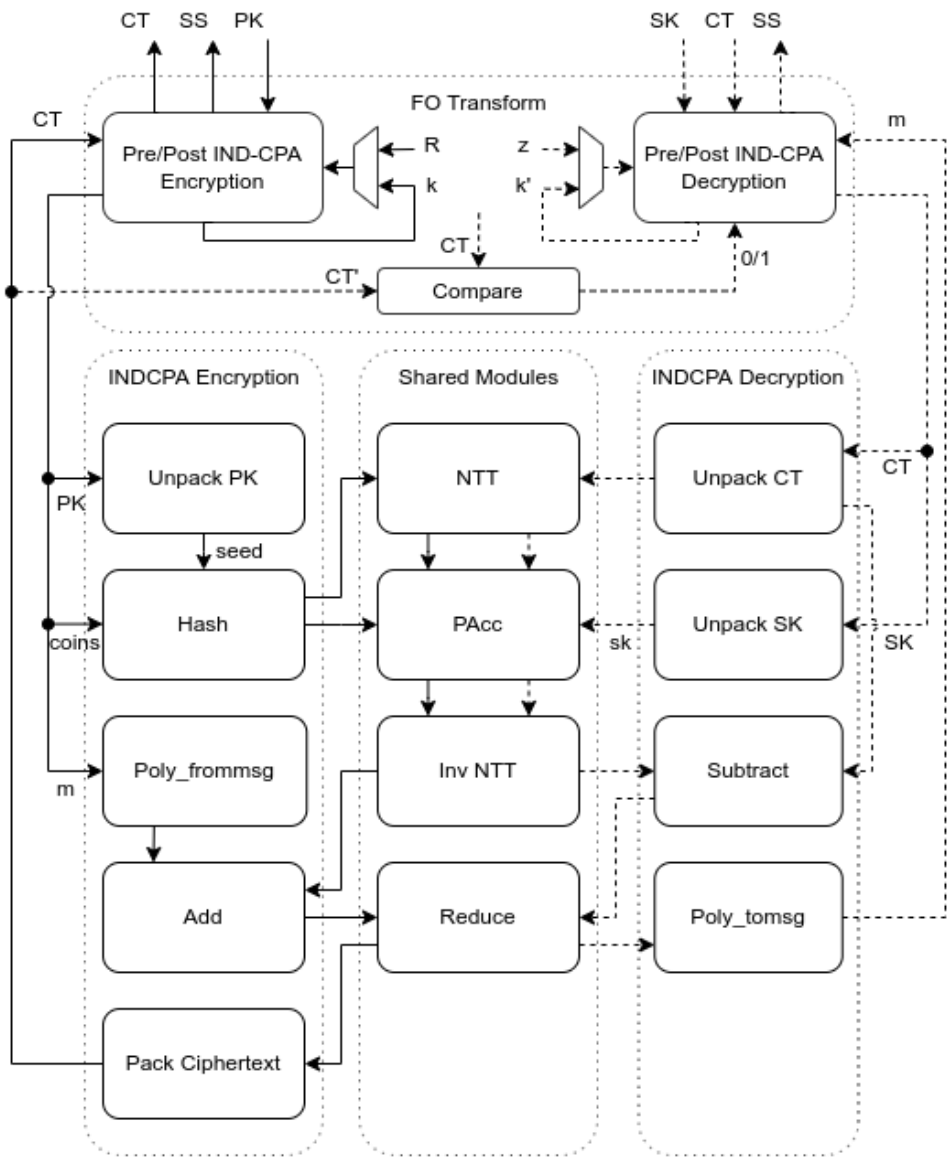
- Part of larger effort to set up testing lab for PQC algorithms
- Demonstrate an implementation agnostic approach to masking Kyber (& other lattice-based schemes) on FPGA
- Highlight measurable noise differences between hiding and hiding-plus-masking techniques



UNIVERSITY OF ARKANSAS

Design: Unmasked

- As close as possible to reference design
- Common modules are reused between encryption and decryption operations
- Some hiding techniques via loop unrolling for exposed modules

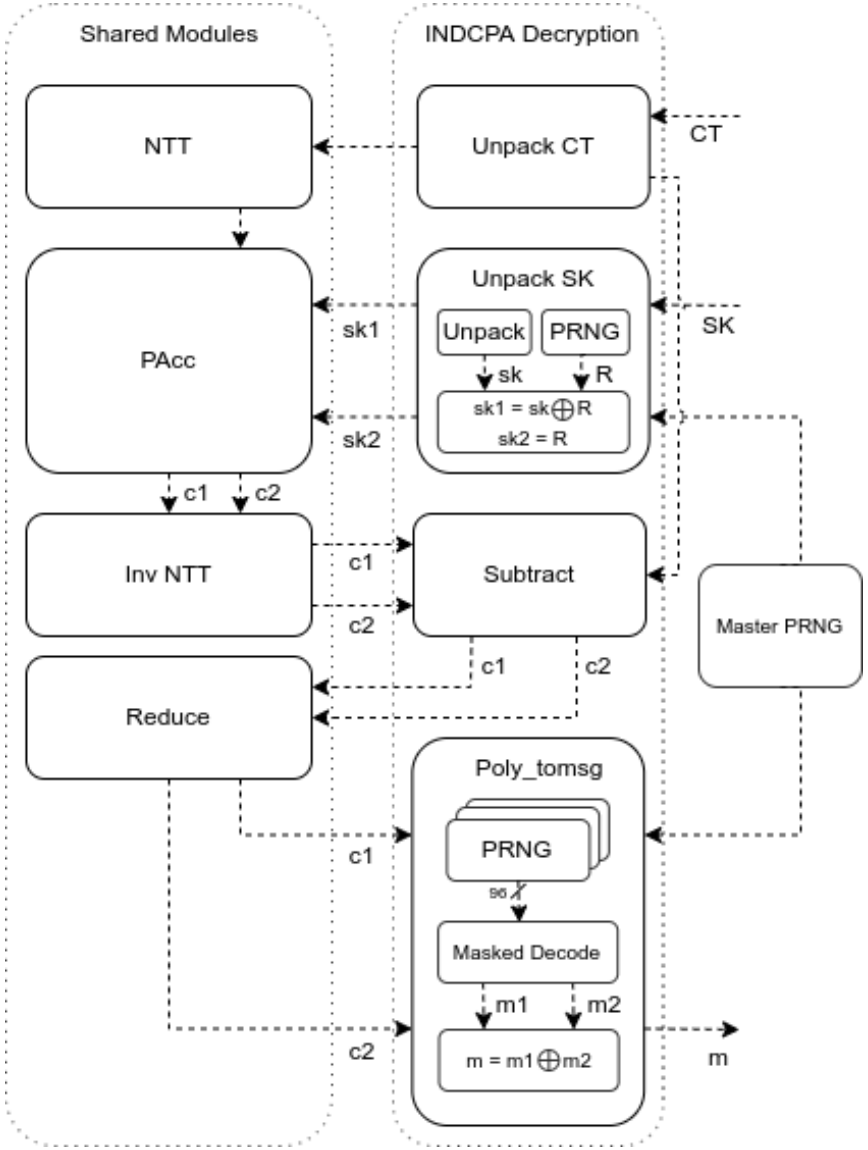


Re-use, Re-use, Re-use!!!

UNIVERSITY OF ARKANSAS

Design: Masked

- First-order masking applied to the Decryption algorithm with the reuse of common modules
- Series of PRNGs produces random inputs
- Overall algorithm avoids directly handling secret keys during decryption operation
  - $sk_1 = sk + R$
  - $sk_2 = R$
  - $m = m_1 + m_2$



Measurements & Setup

- Equipment:
  - Tektronix MDO 3 Series oscilloscope
- Platform: Xilinx Virtex-7 (VC707)
- Measured 5, 10, and 20k traces from VCCAUX_IO & VCCBRAM $\boldsymbol{V}$ & $\boldsymbol{I}$ power rails
- Results shown are 20k random vs. fixed inputs for unmasked and masked inputs

Power Rail	Traces
	(Un)masked
VCCAUX_IO (V)	5, 10, 20k
VCCAUX_IO (I)	5, 10, 20k
VCCBRAM (V)	5, 10, 20k
VCCBRAM (I)	5, 10, 20k

UNIVERSITY OF ARKANSAS

Evaluation

- Standard TVLA for evaluation
  - Leakage threshold set to ± 4.5
  - Pass/Fail per point
- Welch's t-test is a statistical test that highlights differences between two datasets
- TVLA is **not** a security guarantee – but the magnitude of t-values gives an idea of (signal to noise) SNR ratio

$$t = \frac{X_A - X_B}{\sqrt{\frac{S_A^2}{N_A} + \frac{S_B^2}{N_B}}}$$

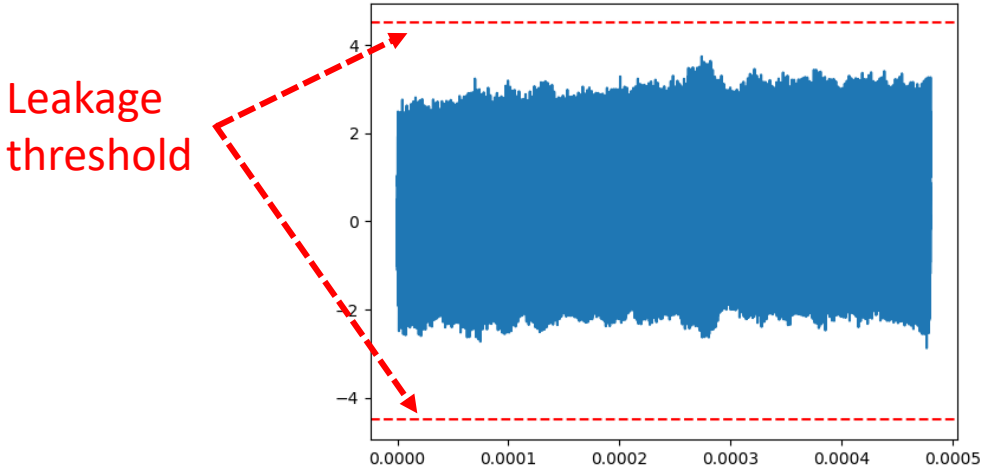
Where:

X_A = sample mean for each point across time

S_A = standard deviation

N_A = cardinality

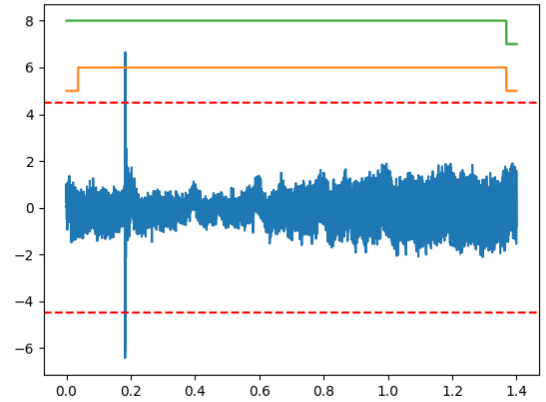
NOT a bulletproof test!



UNIVERSITY OF ARKANSAS

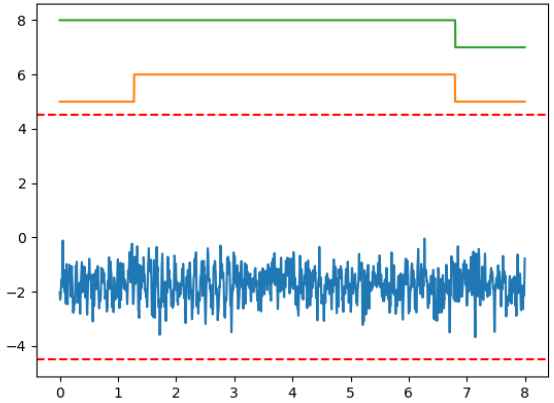
Results

Hiding Only

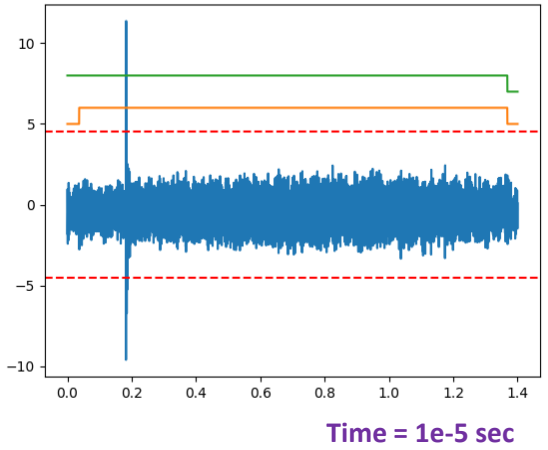


Unmasked VCCAUX_IO (V)

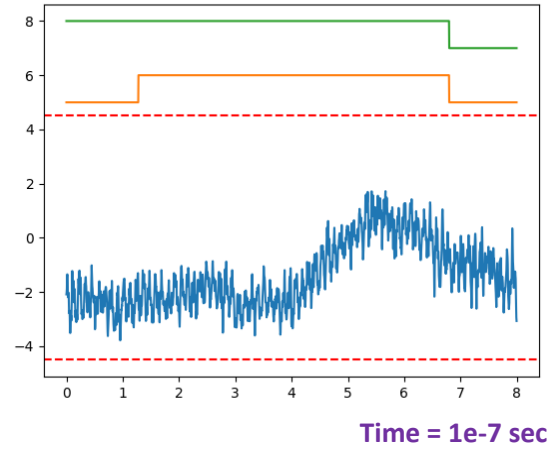
Hiding + Masking



Masked VCCAUX_IO (V)

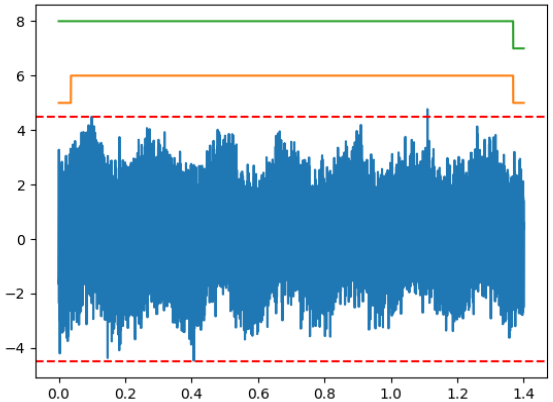


Unmasked VCCAUX_IO (I)



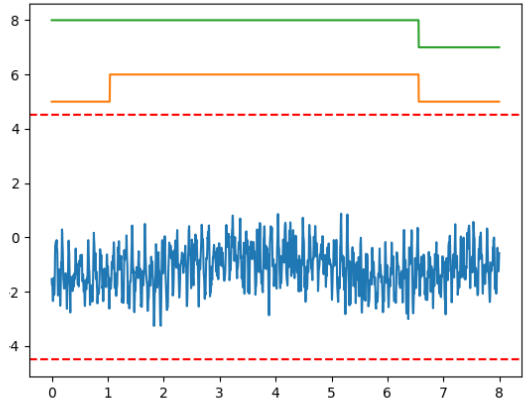
Masked VCCAUX_IO (I)

Hiding Only

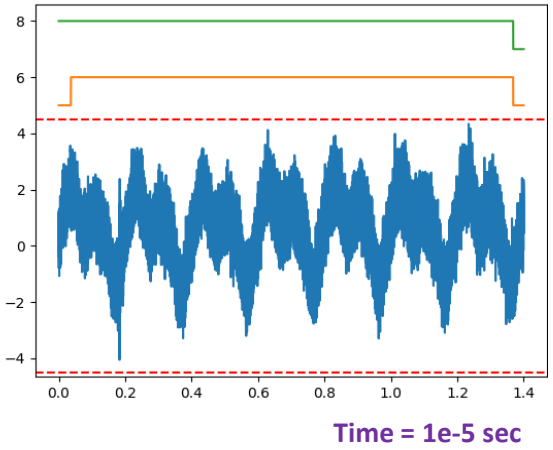


Unmasked VCCBRAM (V)

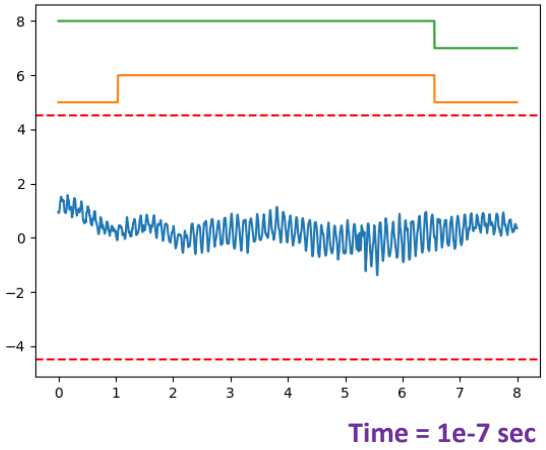
Hiding + Masking



Masked VCCBRAM (V)



Unmasked VCCBRAM (I)



Masked VCCBRAM (I)

Conclusions

- Demonstrated an implementation agnostic design for masking Kyber
- Demonstrated effectiveness of 1st-order masking for Kyber on FPGA

- **Critique:**
  - Remove decoupling capacitors for cleaner signal and better measurements

- **Future work:**
  - Continued developed of testing capabilities of testing platform

UNIVERSITY OF ARKANSAS

Questions?

- Contact info:
  - Tendayi Kamucheka – tfkamuch@uark.edu

  - Computer Systems Design Lab (Lab P.I.s)
    - Miaoqing Huang – mqhuang@uark.edu
    - David Andrews – dandrews@uark.edu
  - AESIR Lab (Lab P.I.)
    - Alexander Nelson – ahnelson@uark.edu

UNIVERSITY OF ARKANSAS