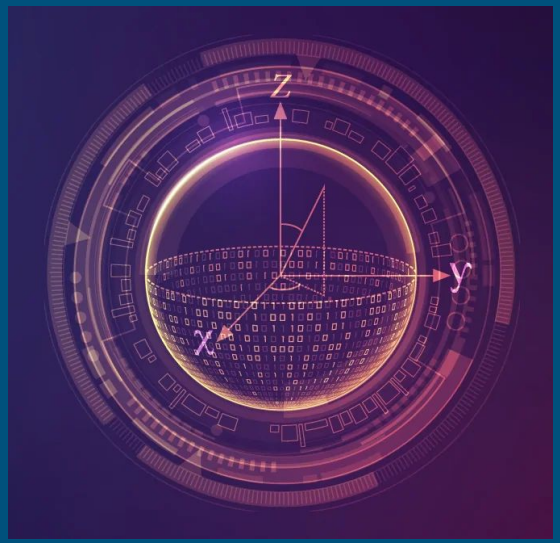
Post-Quantum Stateful Hash-Based Signature Scheme for Improving Bluetooth Security

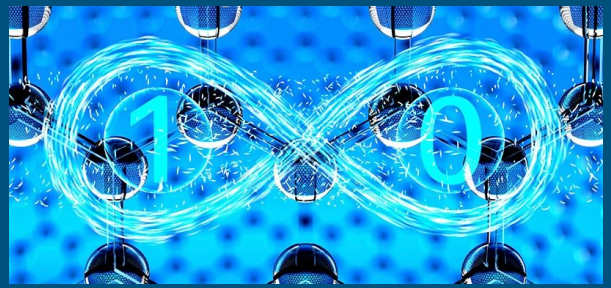
Andres Colon, Ian Lieu, Peter Anthony, Arron Lu

Advisor: Professor Mohamed El-Hadedy
Assistant Professor, ECE-department, College of Engineering
California State Polytechnic University, Pomona
Team: Post-Quantum on-Chip

Motivation

- Quantum Computers
- Post-Quantum
- Quantum Cryptography
- Hash-Based Signatures
- Shor's Algorithm
- Bluetooth Public-Key Exchange
- IoT/Low-Power Devices

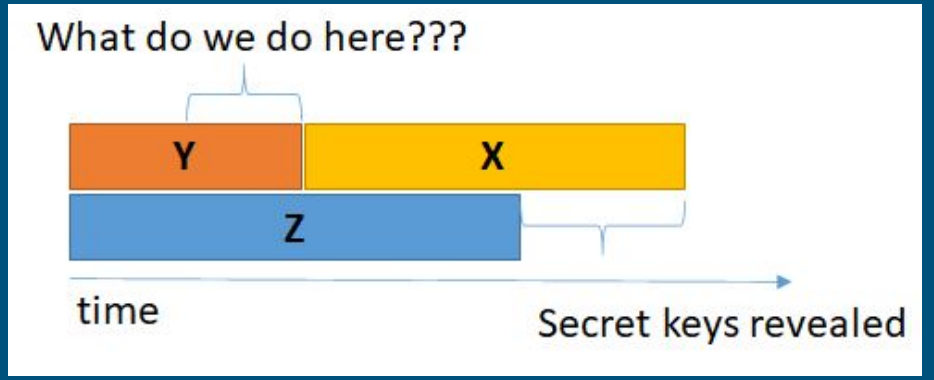




Post-Quantum

Mosca's Inequality Theorem:

If X + Y > Z, then security is broken



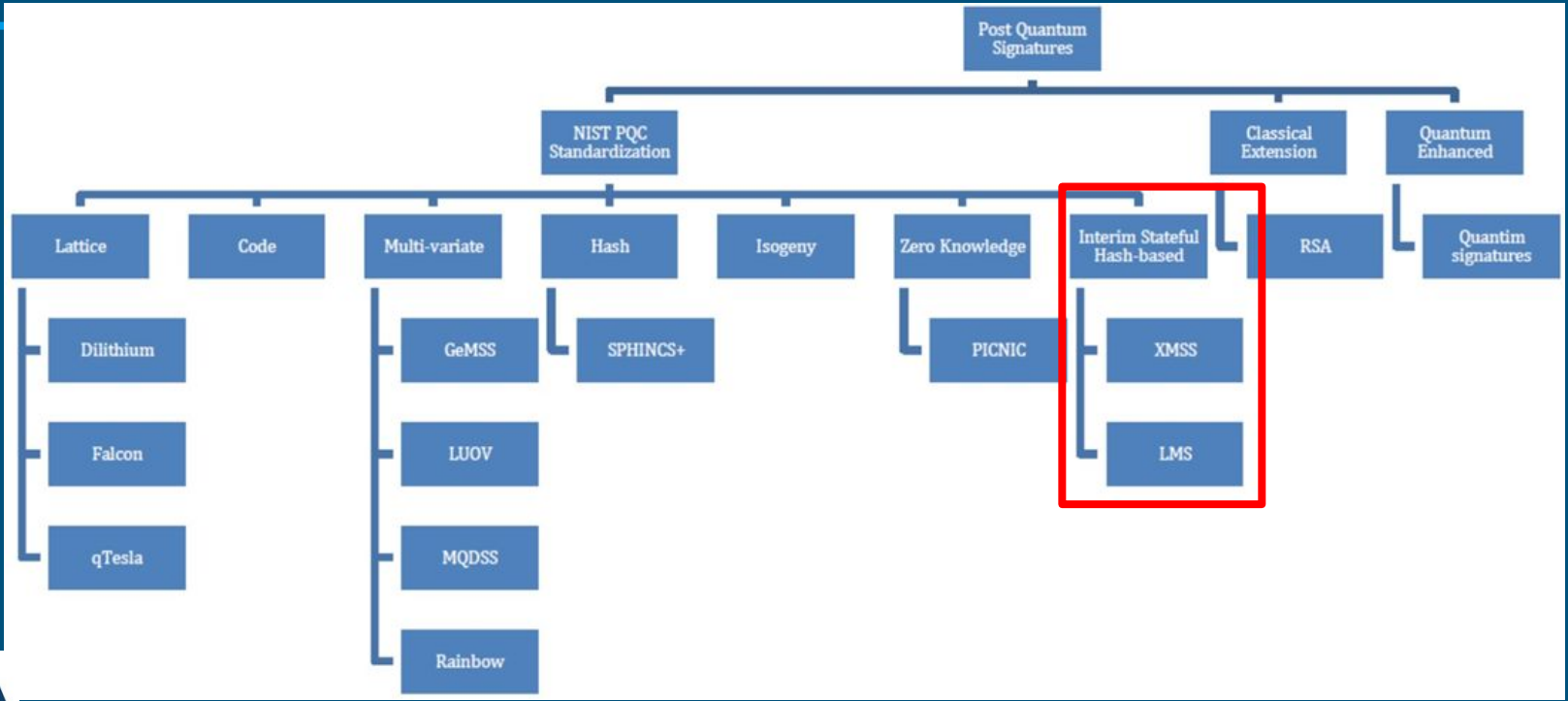
X: shelf life of existing security standards

Y: time to migrate from current crypto standards to a quantum-safe environment

Z: time for a large-scale quantum computer to be built

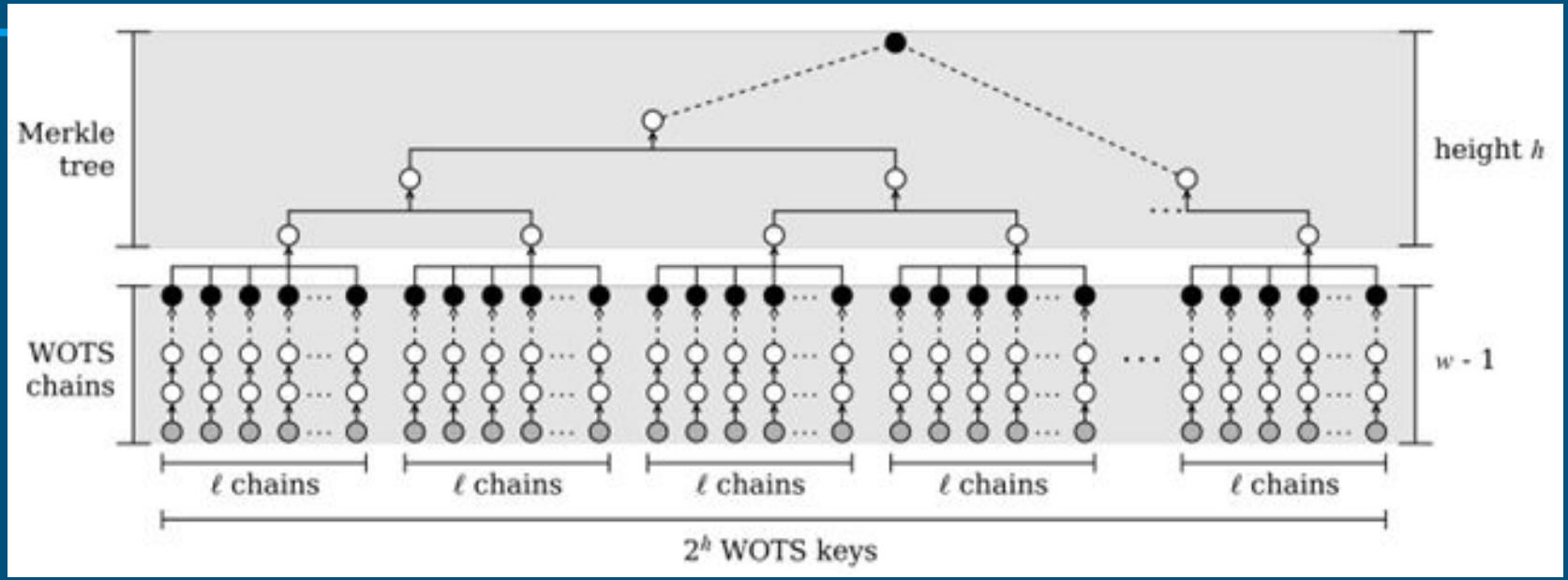
[1] Dr. Michele Mosca "Cybersecurity in a quantum world: will we be ready?"

Post-Quantum Signatures



[2] Teik Guan Tan, Jianying Zhou, A survey of Digital Signing in the post Quantum Era (Singapore University of Technology and Design, Singapore)

LMS: Leighton-Micali Signatures



[3] Campos, Kohlstadt, Reith, Stottinger, “LMS vs XMSS: Comparison of Stateful Hash-Based Signature Schemes on ARM Cortex-M4”

Hash

- SHA-1
- SHA-2 256/512
- SHA-3 (SHAKE)
- Lightweight Hash (LWC: Lightweight Cryptography)
  - GAGE Hash Function

Gage Security Range Greater Than: 2^{112} or 2^{128}
Low-End IoT Device Security Range: 2^{80} – 2^{96}

Percentage of Time Spent on Hashing

	HSS	XMSS^{MT}	SIMPLE
key gen	92%		85%
sign	92%		85%
verify	94%		85%

[3] Campos, Kohlstadt, Reith, Stottinger, "LMS vs XMSS: Comparison of Stateful Hash-Based Signature Schemes on ARM Cortex-M4"

Bluetooth

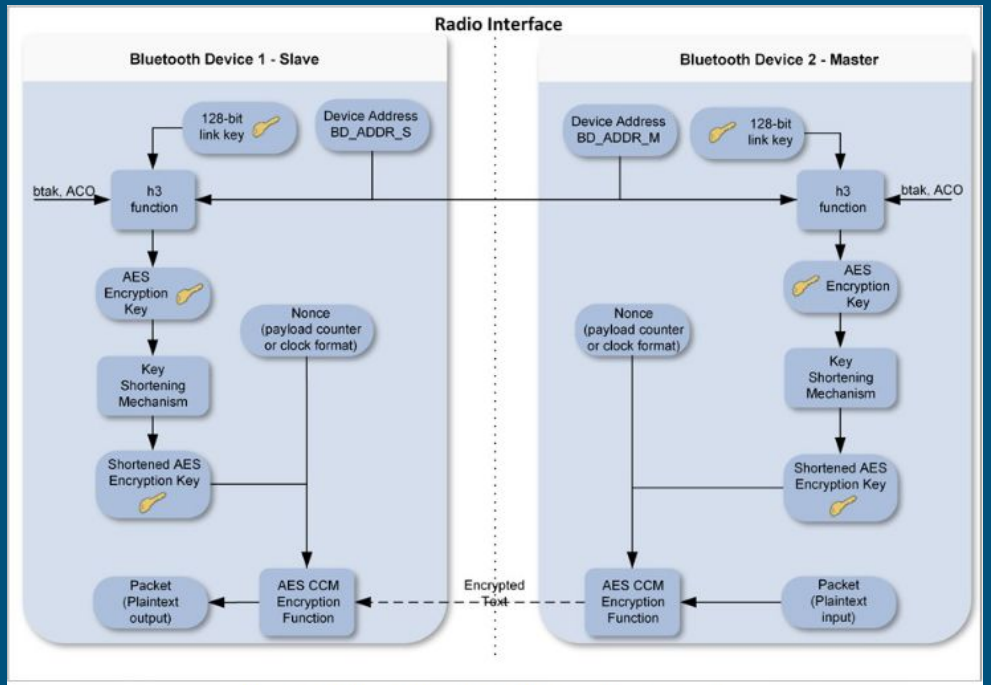


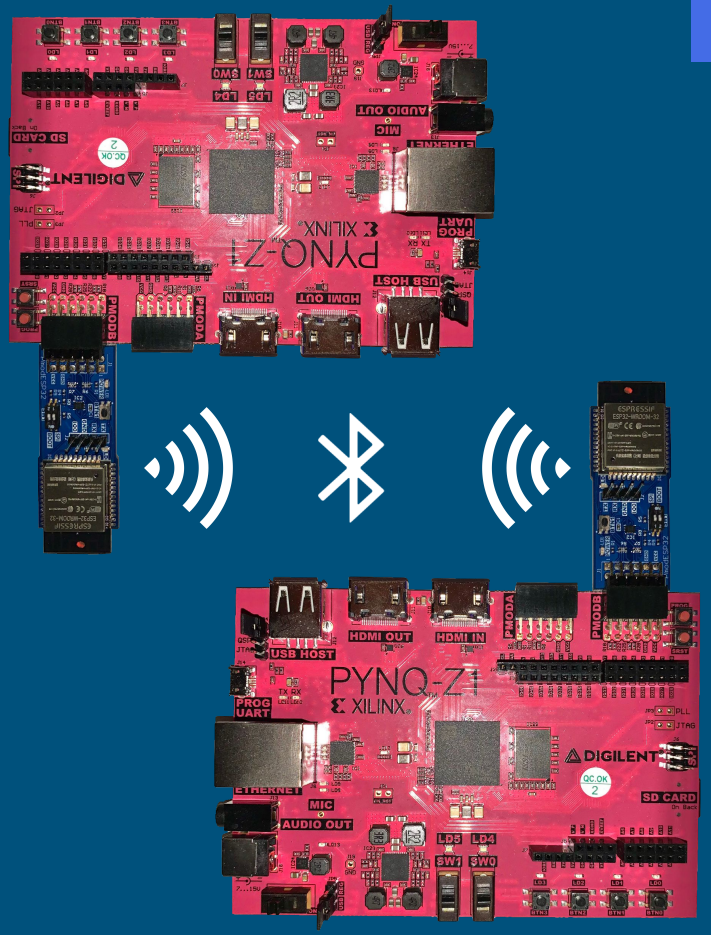
Figure 3-8. Bluetooth AES-CCM Encryption Procedure

[4] “NIST Special Publication 800-121 Revision 2, Guide to Bluetooth Security”

Our Goal

- IoT Communication with Post-Quantum Security
- Hash-Based Signature Scheme Acceleration

- PYNQ-Z1 SoC
- ESP-WROOM-32 (ESP32) Pmod



Test Results: LMS

Implementation	Function	Run Time
Desktop (SHA-256)	Key Generation	5 minutes
	Signing	< 1 second
	Verifying	< 1 second
PYNQ-Z1 (SHA-256)	Key Generation	3 hours
	Signing	1 minute
	Verifying	< 1 second
Desktop (SHA-3)	Key Generation	7 minutes
	Signing	3 seconds
	Verifying	< 1 second

LMS Functions

```
ubuntu@arm:~/hash-sigs$ ./demo
Usage:
 ./demo genkey [keyname]
 ./demo genkey [keyname] [parameter set]
 ./demo sign [keyname] [files to sign]
 ./demo verify [keyname] [files to verify]
 ./demo advance [keyname] [amount of advance]
```

Specifications:

Desktop: Intel Core i7-6700K CPU @ 4.00GHz, 16GB DDR4

PYNQ-Z1: Cortex-A9 ARM Processor @650MHz, 512MB DDR3

Future Works

LMS

- Replace Open-SSL SHA-256 in software with a SHA-256 hardware core
- Develop a lightweight hash compatible with LMS

Bluetooth

- Implement a fully functioning Btstack onto bluetooth device
- Replace authentication model, AES to LMS

References

1. Dr. Michele Mosca “Cybersecurity in a quantum world: will we be ready?”
2. Teik Guan Tan, Jianying Zhou, “A survey of Digital Signing in the post Quantum Era” (Singapore University of Technology and Design, Singapore)
3. Campos, Kohlstadt, Reith, Stottinger, “LMS vs XMSS: Comparison of Stateful Hash-Based Signature Schemes on ARM Cortex-M4”
4. “NIST Special Publication 800-121 Revision 2, Guide to Bluetooth Security”

https://github.com/Reconfigurable-Computing-CalPoly-Pomona/postquantum_crypto_signature-

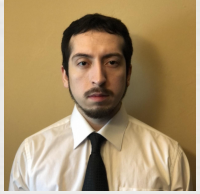
Acknowledgement

This research was supported in part by:

- Xilinx Inc.
- Center for Cognitive Computing Systems Research (C^3SR)
- US Air Force Research Laboratory, Academy Center for Cyberspace

Ian Lieu

Arron Lu



Peter Anthony

Andres Colon

Prof. M. El-Hadedy

Questions?

Ian Lieu

Arron Lu

Prof. M. El-Hadedy

http://www.recoiot.com/

Andres Colon

Peter Anthony

https://github.com/Reconfigurable-Computing-CalPoly-Pomona/postquantum_crypto_signature-