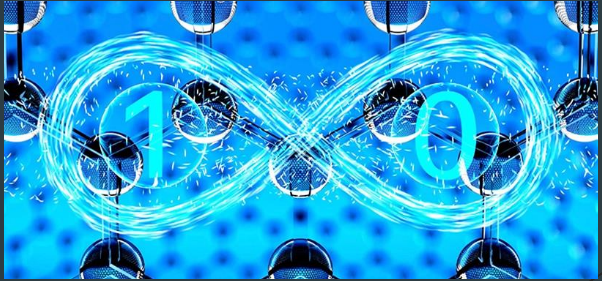
Post-Quantum Stateful Hash-Based Signature Scheme for Improving Bluetooth Security

Arron Lu, Ian Lieu, Peter Anthony, Andres Colon

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

Motivation

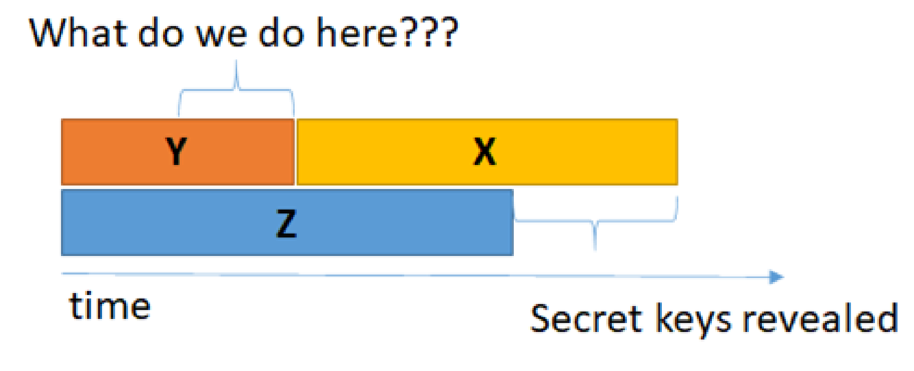
- Quantum Computers
- Post-Quantum
- Quantum Cryptography
- Hash-Based Signatures
- Shor’s Algorithm
- Bluetooth Public-Key Exchange
- IoT/Low-Power Devices



Post-Quantum

Mosca’s Inequality Theorem:

If $X + Y > Z$, then security is broken



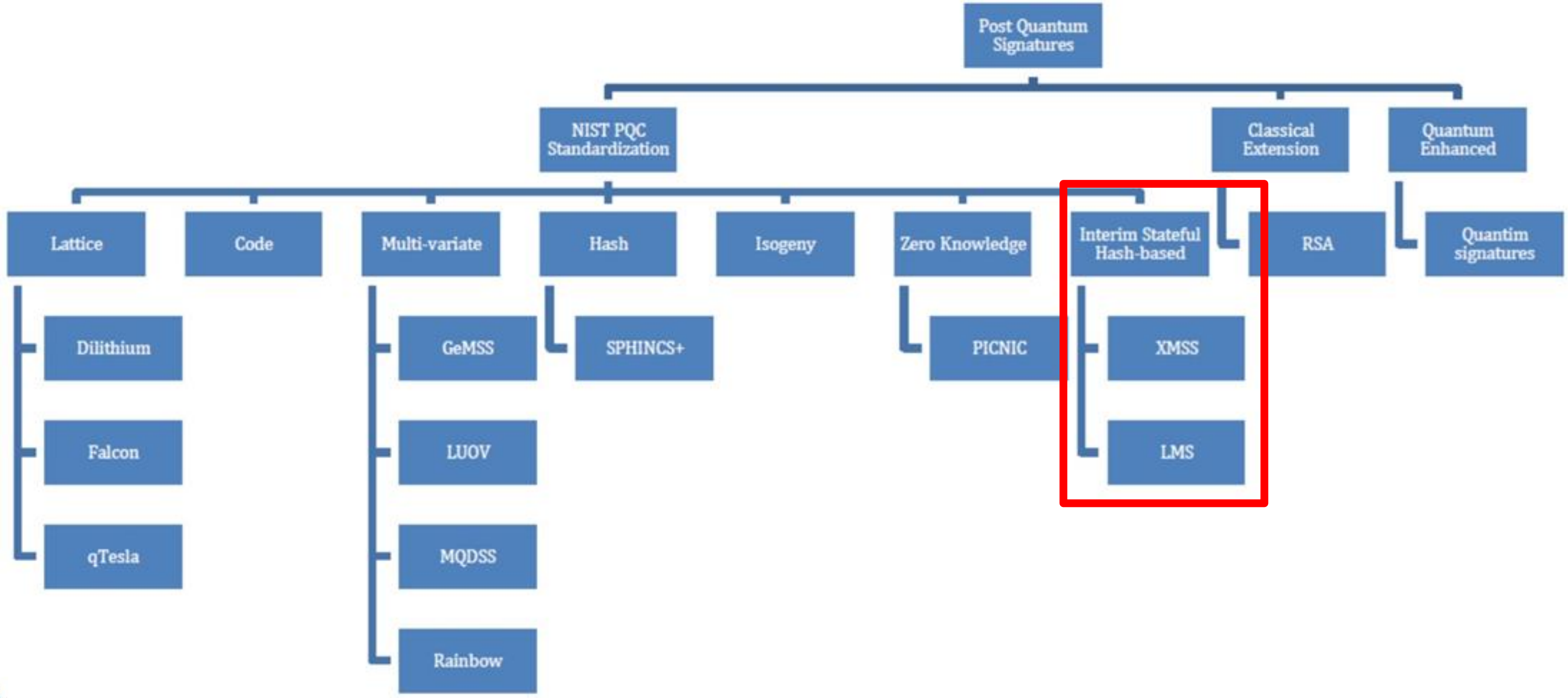
X: shelf life of existing security standards

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

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

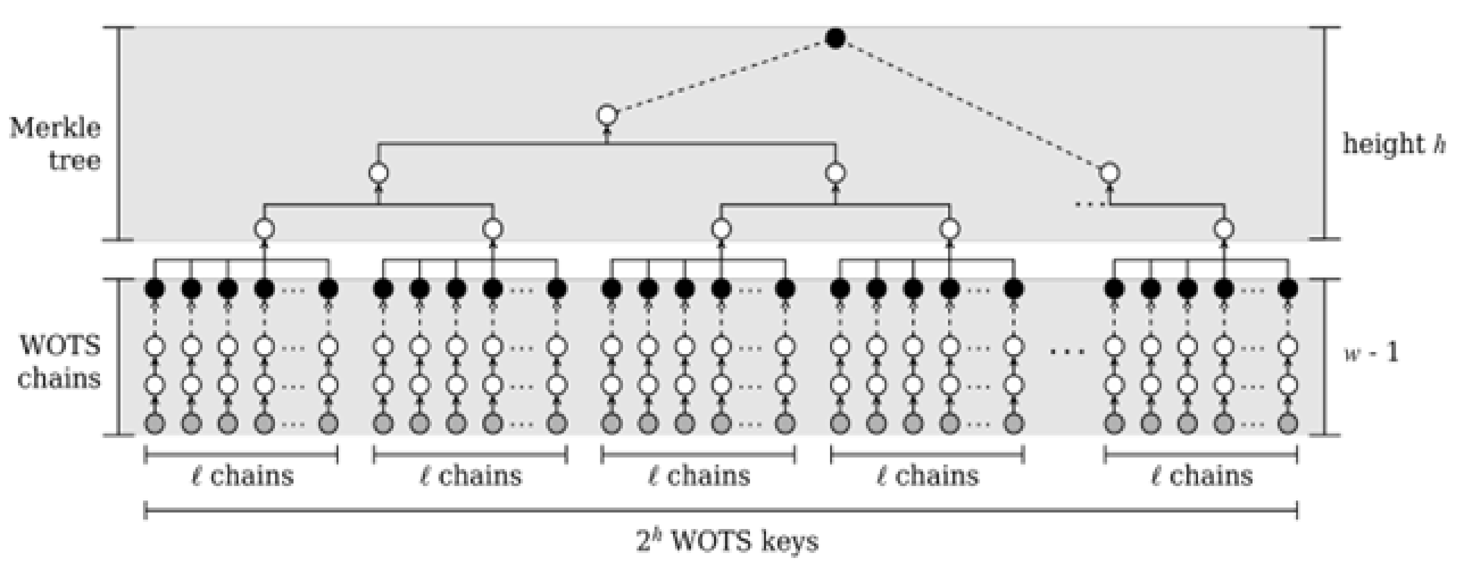
[1] Dr. Michele Mosca “Cybersecurity in a quantum world: will we be ready?”

Post-Quantum Signatures



[2] T. G. Tan, J. Zhou, “A survey of Digital Signing in the post Quantum Era” (Singapore University of Technology and Design, Singapore)

LMS: Leighton-Micali Signatures

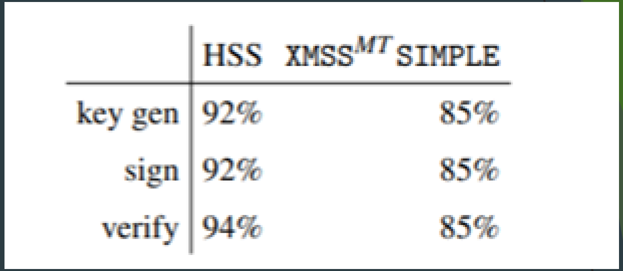


[3] F. Campos, T. Kohlstadt, S. Reith, M. Stottinger, “LMS vs XMSS: Comparison of Stateful Hash-Based Signature Schemes on ARM Cortex-M4”

Hash

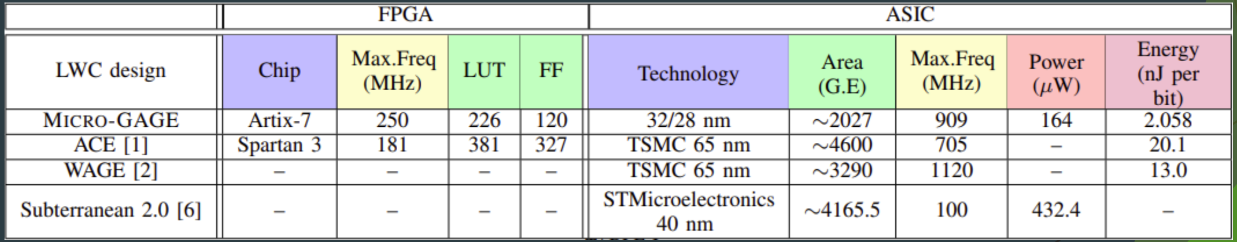
- SHA-1
- SHA-2 (256/512)
- SHA-3 (SHAKE)
- Lightweight Hash (LWC: Lightweight Cryptography)
  - GAGE Hash Function
    - Security Range Greater Than: 2^{112} or 2^{128}
    - Low-End IoT Device Security Range: 2^{80} – 2^{96}

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"



	FPGA				ASIC				
LWC design	Chip	Max.Freq (MHz)	LUT	FF	Technology	Area (G.E)	Max.Freq (MHz)	Power (μW)	Energy (nJ per bit)
MICRO-GAGE	Artix-7	250	226	120	32/28 nm	∼2027	909	164	2.058
ACE [1]	Spartan 3	181	381	327	TSMC 65 nm	∼4600	705	–	20.1
WAGE [2]	–	–	–	–	TSMC 65 nm	∼3290	1120	–	13.0
Subterranean 2.0 [6]	–	–	–	–	STMicroelectronics 40 nm	∼4165.5	100	432.4	–

[4] **M. El-Hadedy**, M. Margala, S. Mosanu, D. Gligoroski, J. Xiong, W-M. Hwu "Micro-GAGE: A Low-power Compact GAGE Hash Function Processor for IoT Applications", 27th IEEE International Conference on Electronics, Circuits, Systems (ICECS2020), Glasgow, Scotland, November 23-25, 2020

Bluetooth

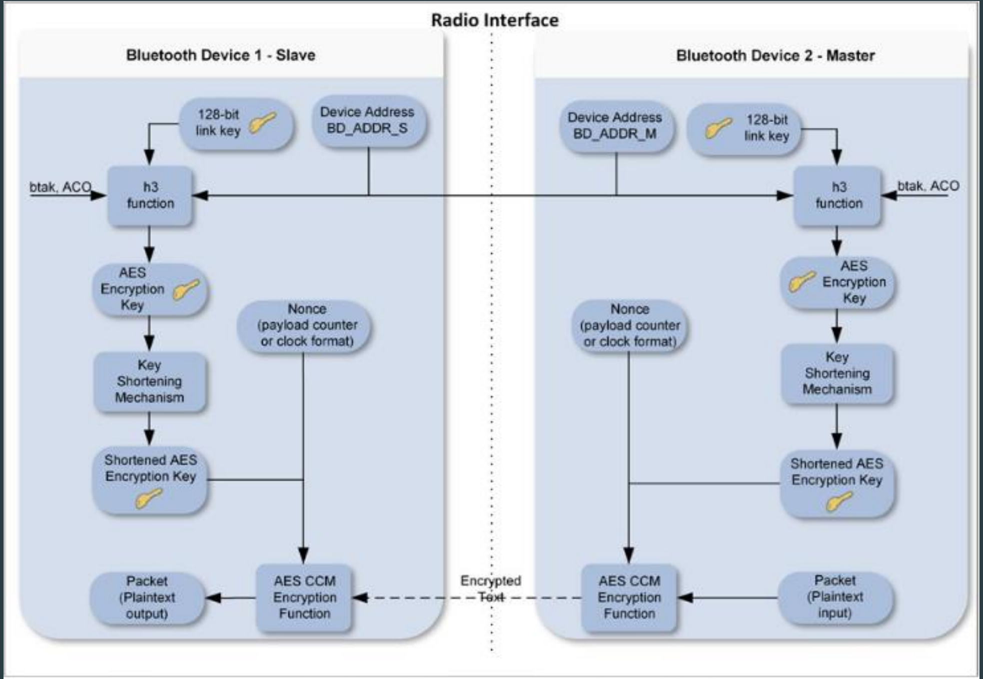

Radio Interface
Bluetooth Device 1 - Slave
128-bit link key
Device Address BD_ADDR_S
btak, ACO
h3 function
AES Encryption Key
Nonce (payload counter or clock format)
Key Shortening Mechanism
Shortened AES Encryption Key
Packet (Plaintext output)
AES CCM Encryption Function
Encrypted Text
Bluetooth Device 2 - Master
Device Address BD_ADDR_M
128-bit link key
h3 function
btak, ACO
AES Encryption Key
Nonce (payload counter or clock format)
Key Shortening Mechanism
Shortened AES Encryption Key
AES CCM Encryption Function
Packet (Plaintext input)

Figure 3-8. Bluetooth AES-CCM Encryption Procedure

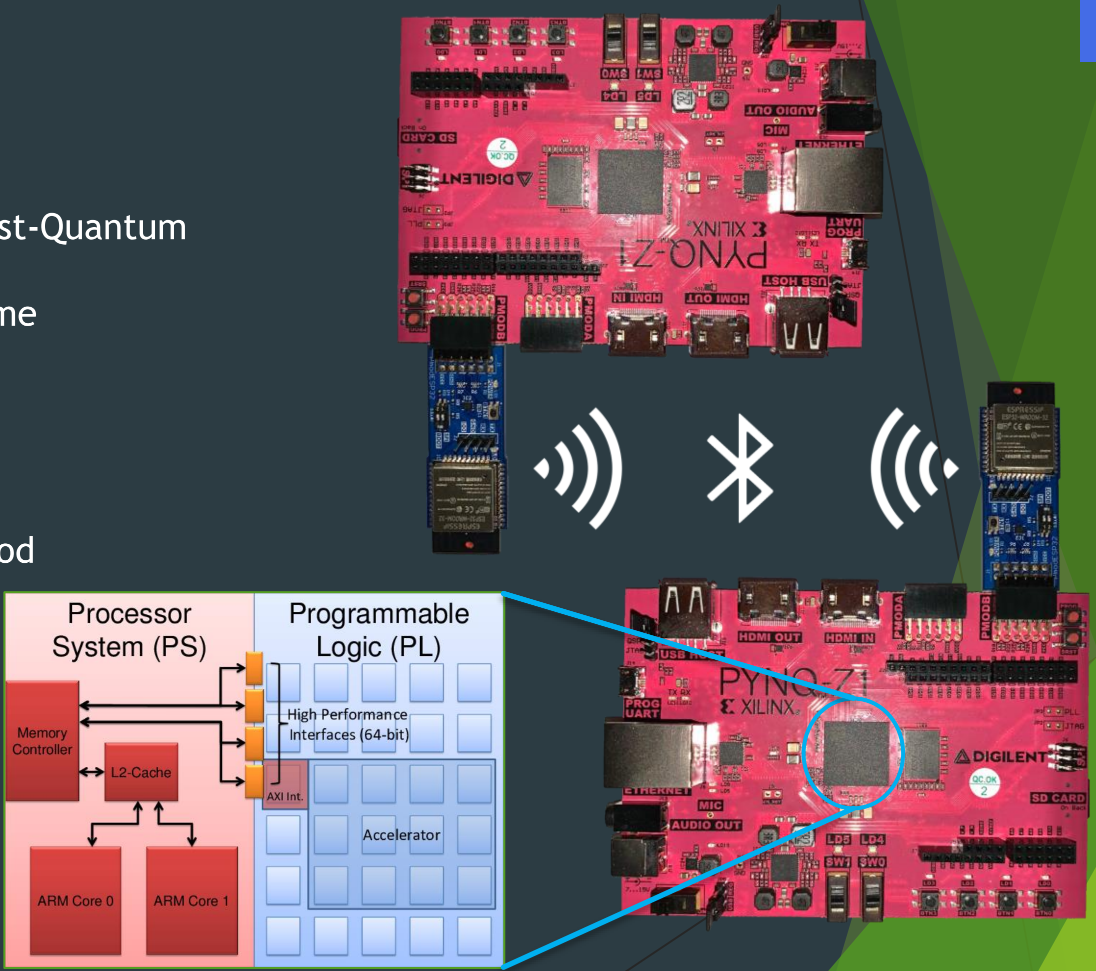
[5] “NIST Special Publication 800-121 Revision 2, Guide to Bluetooth Security”

Our Goal

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

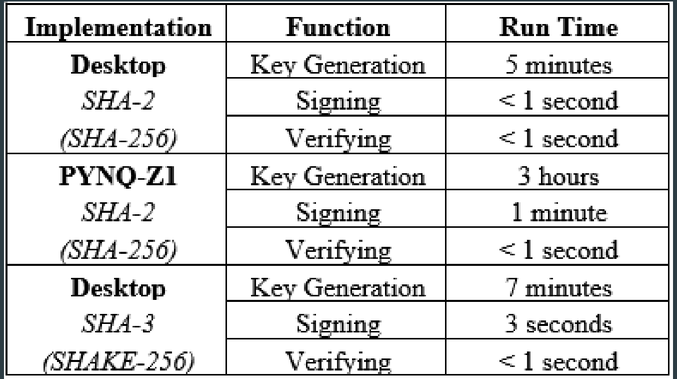
Hardware:

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



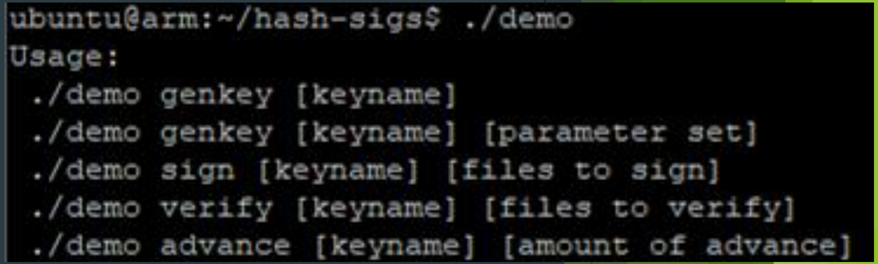
[6] J. Monson, “Implementing high-performance, low power FPGA-based optical flow accelerators in C”

Test Results: LMS



Implementation	Function	Run Time
Desktop *SHA-2* *(SHA-256)*	Key Generation	5 minutes
	Signing	< 1 second
	Verifying	< 1 second
PYNQ-Z1 *SHA-2* *(SHA-256)*	Key Generation	3 hours
	Signing	1 minute
	Verifying	< 1 second
Desktop *SHA-3* *(SHAKE-256)*	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

Demo

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. T. G. Tan, J. Zhou, “A survey of Digital Signing in the post Quantum Era” (Singapore University of Technology and Design, Singapore)
3. F. Campos, T. Kohlstadt, S. Reith, M. Stottinger, “LMS vs XMSS: Comparison of Stateful Hash-Based Signature Schemes on ARM Cortex-M4”
4. **M. El-Hadedy**, M. Margala, S. Mosanu, D. Gligoroski, J. Xiong, W-M. Hwu “Micro-GAGE: A Low-power Compact GAGE Hash Function Processor for IoT Applications”, 27th IEEE International Conference on Electronics, Circuits, Systems (ICECS2020), Glasgow, Scotland, November 23-25, 2020
5. “NIST Special Publication 800-121 Revision 2, Guide to Bluetooth Security”
6. J. Monson, “Implementing high-performance, low power FPGA-based optical flow accelerators in C”

CalPoly Pomona

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

Acknowledgement

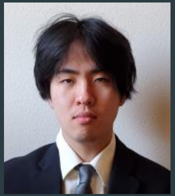
This research was supported in part by:

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

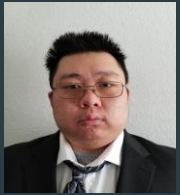
C3SR center for cognitive computing systems research

IBM | ILLINOIS

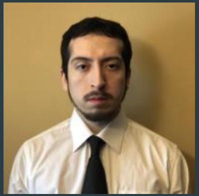
RECOIOT RECONFIGURABLE INTERNET OF THINGS



Ian Lieu



Arron Lu



Peter Anthony

Andres Colon

Prof. M. El-Hadedy

http://www.recoiot.com/

CalPoly Pomona