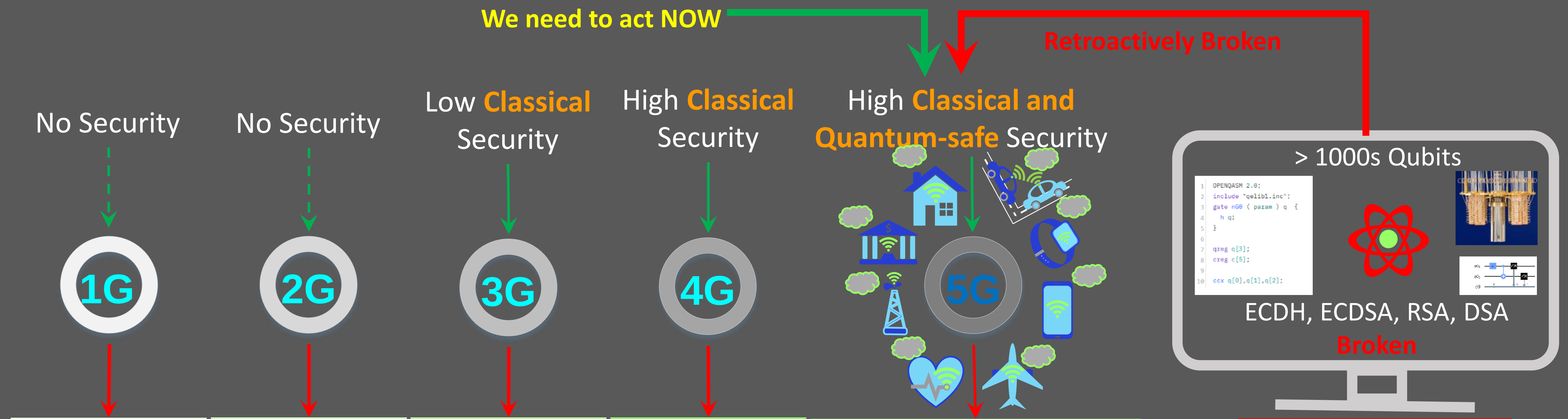
ETSI/IQC Quantum Safe Cryptography Event

Challenges of Deploying and Integrating PQC in Hyper-Scale IoTs in 5G and NextG

Reza Azarderakhsh

03/14/2023

PQC for IoT in 5G: New Attack Surface



We need to act NOW

Retroactively Broken

No Security

No Security

Low Classical Security

High Classical Security

High Classical and Quantum-safe Security

> 1000s Qubits

```
OPENQASM 2.0;
include "qelib1.inc";
gate nG0 ( param ) q  {
  h q;
}

qreg q[3];
creg c[5];

ccx q[0],q[1],q[2];
```

ECDH, ECDSA, RSA, DSA

Broken

1980s
Latency N/A
No Data

Analog Voice

Impact
None

1990s
300 – 1,000 ms
< 40 Kb/s

Digital Voice

Impact
- ✓Text messages to and from remote machines

2000s
100 – 500 ms
< 20 Mb/s

Wireless Internet

Impact
- ✓Video monitoring
- ✓Remote access to machines
- ✓Remote conditioning monitoring

2010s
< 25 ms
< 1 Gb/s

Mobile Broadband

Impact
- ✓Mobile technical services
- ✓Services via smartphones
- ✓Wireless networks

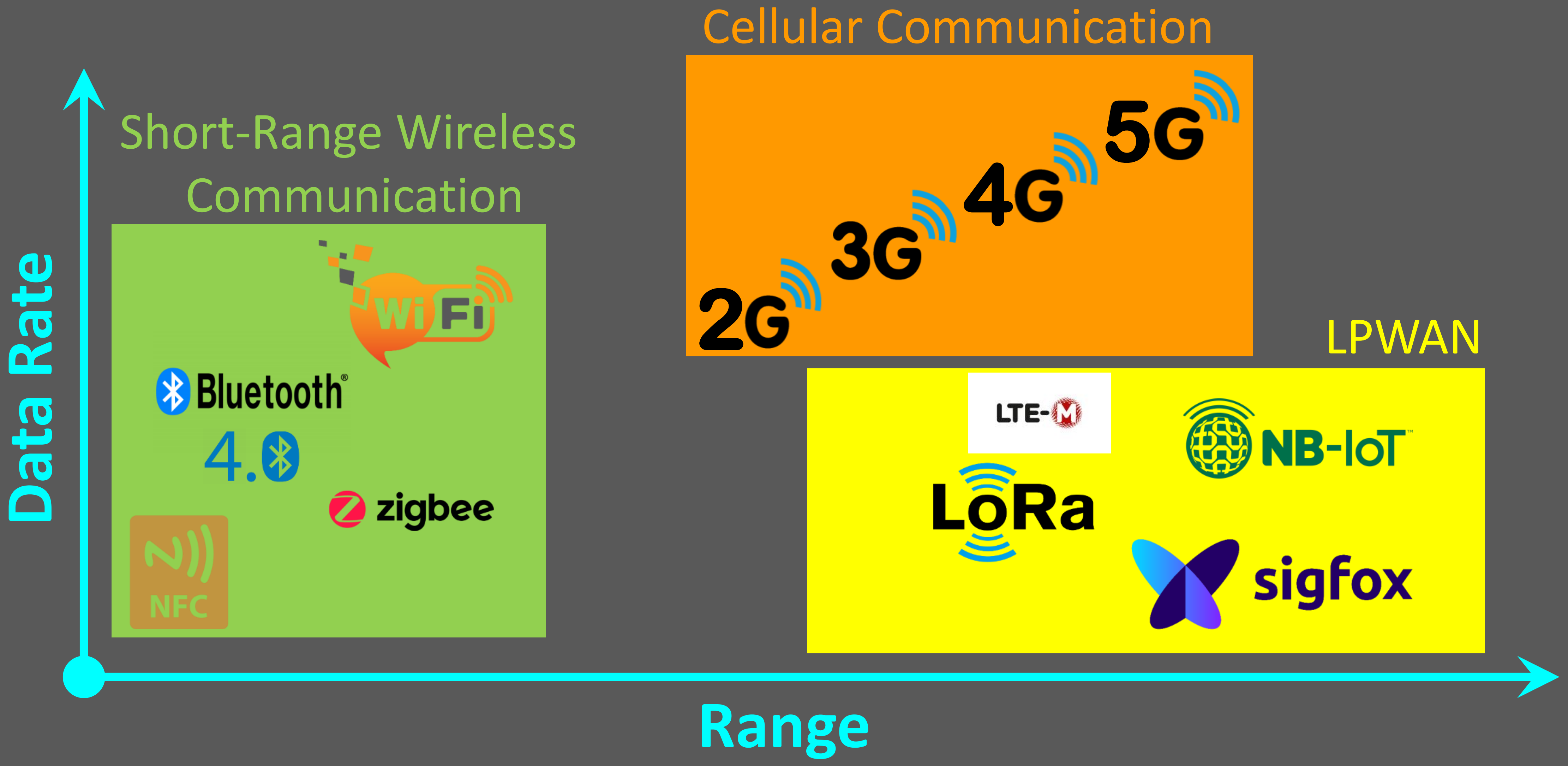
2020s
< 1 ms
< 20 Gb/s
Massive Connection + IoTs

Impact
- ✓Autonomous logistics
- ✓Robots and autonomous machines
- ✓Assisted work
- ✓Wireless backhaul
- ✓Real-time data analytics
- ✓Carbon footprint management

2030s
Large Quantum Computers

“Distribution Statement A – Approved for Public Release, Distribution Unlimited”

Emerging Wireless Communication



Data Rate

Range

Short-Range Wireless Communication

Wi Fi

Bluetooth 4.0

zigbee

NFC

Cellular Communication

2G

3G

4G

5G

LPWAN

LTE-M

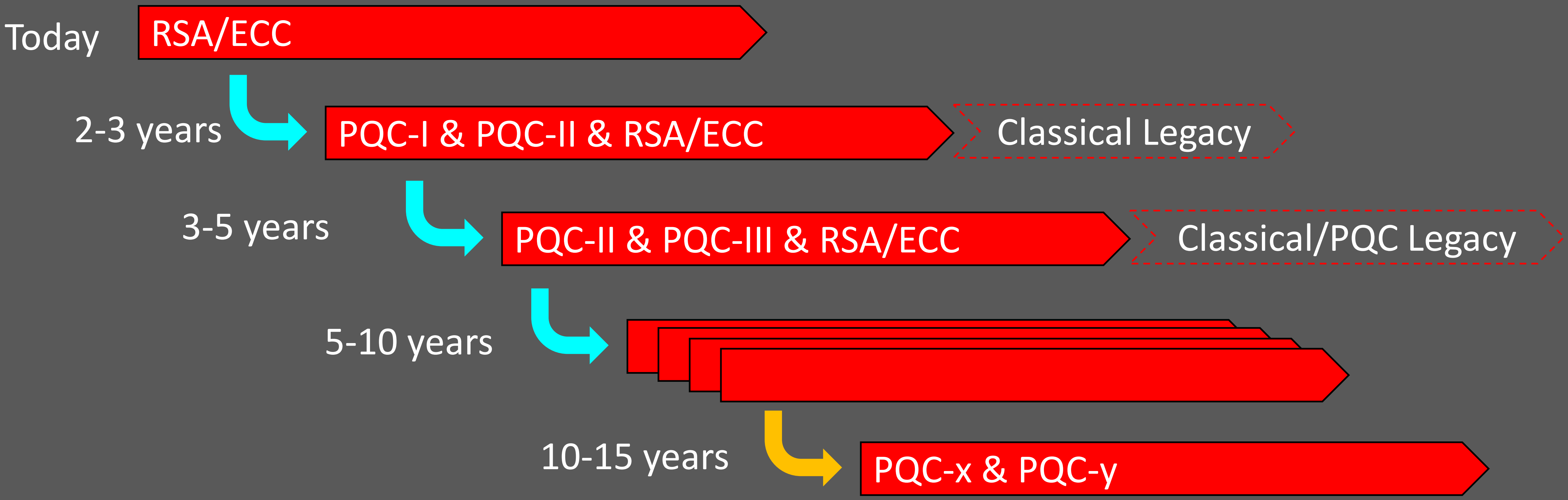
NB-IoT

LoRa

sigfox

Crypto-Agility & Multi-Stage Transition

PQSecure



Today

RSA/ECC

2-3 years

PQC-I & PQC-II & RSA/ECC

Classical Legacy

3-5 years

PQC-II & PQC-III & RSA/ECC

Classical/PQC Legacy

5-10 years

10-15 years

PQC-x & PQC-y

Hybrid:

- Classical and quantum security
- Backwards compatibility
- Continuous updates

“Crypto-Agility will be the Key to Managing Rapid Transitions in Security”

Companies will need:

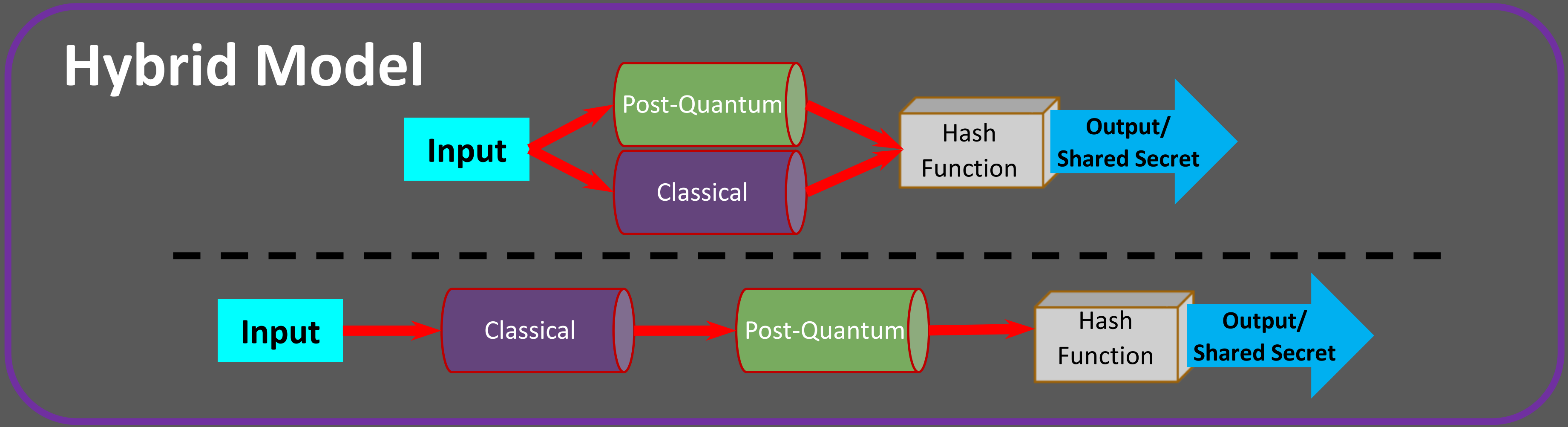
- Interoperability
- Diverse technical requirements
- Rapid update cycles

“Distribution Statement A – Approved for Public Release, Distribution Unlimited”

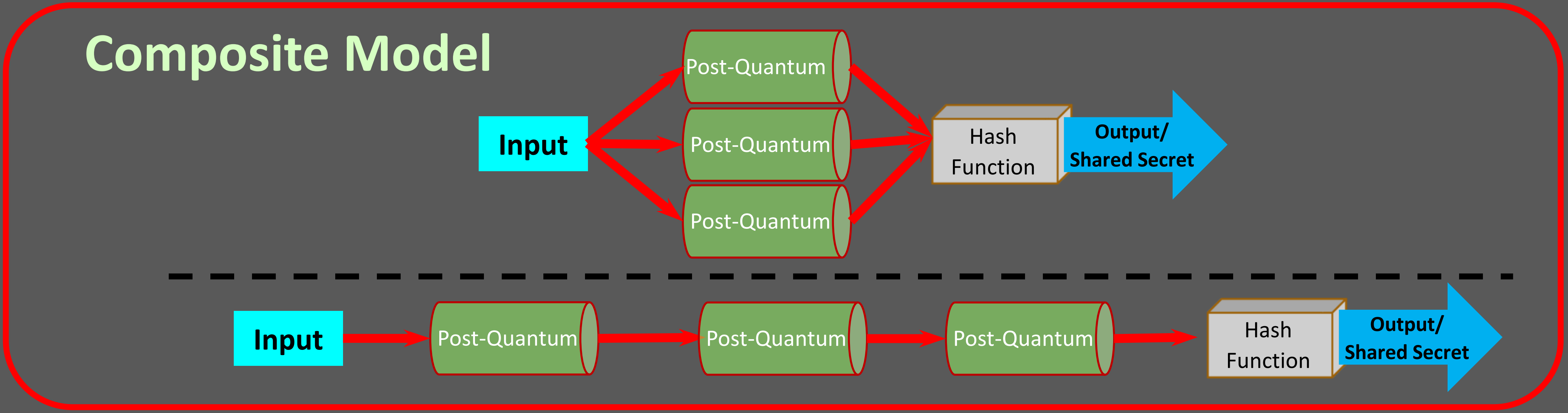
Implementing hybrid/composite Sys.

PQSecure

Hybrid Model



Composite Model



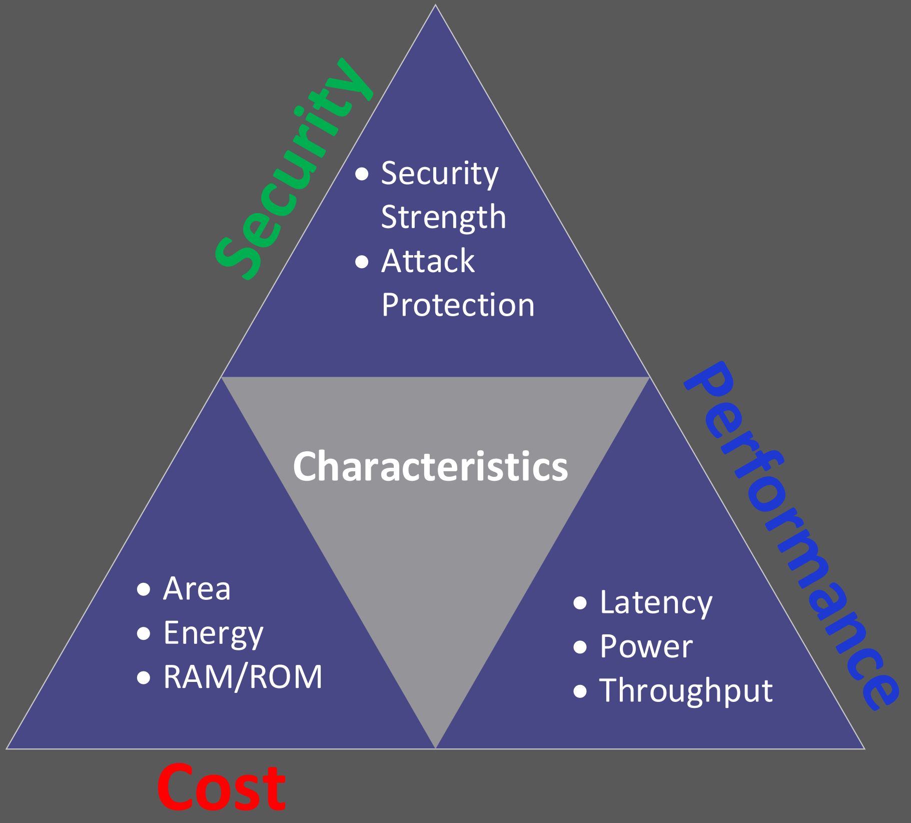
"Distribution Statement A – Approved for Public Release, Distribution Unlimited"

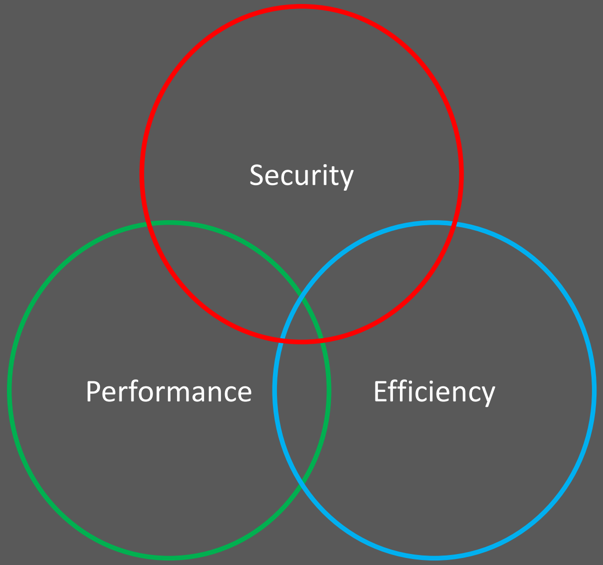
PQC Sizes

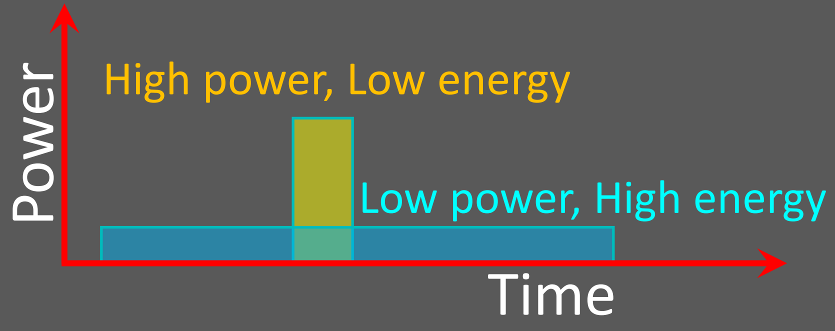
Algorithm	Secret Key Bytes	Public Key Bytes	Ciphertext/Signature Key Bytes
CRYSTALS-Kyber	1,632	800	768
CRYSTALS-Dilithium	2,528	1,312	2,420
FALCON	1,281	897	666
SPHINCS+	32	64	7,856
BIKE	281	1,541	1,573
Classic McEliece	6,492	261,120	128
HQC	2,289	2,249	4,481
XMSS	2,144	64	2,500
LMS	1,820	56	8,684

“Distribution Statement A – Approved for Public Release, Distribution Unlimited”

No one-size-fits-all for Today’s Devices



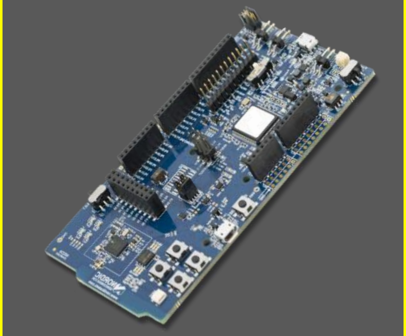




“Distribution Statement A – Approved for Public Release, Distribution Unlimited”

IoT Devices with Crypto HW Accelerators

NORDIC SEMICONDUCTOR



nRF5280
Arm® Cortex^{TM}-M4
@ 64 MHz
Arm CryptoCell CC310
HW Crypto Engine:
AES, Hash, RSA/ ECC, etc.

life.augmented

STM32L5xx
Arm® Cortex®-M33
TrustZone®
@ 110 MHz
HW Crypto Engine:
AES/ DES3, MD5/
SHA/SHA2. RNG etc.

TEXAS INSTRUMENTS

CC2642R
ARM® Cortex® -M4F
@ 48 MHz
HW Crypto Engine:
AES/ DES/ DES3, SHA2,
RNG, RSA/ ECC, etc.

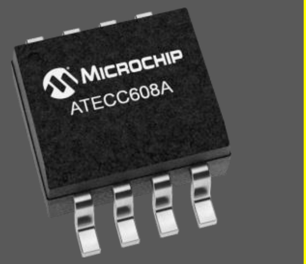
SILICON LABS

EFM32
ARM Cortex-M4
@ 40MHz
HW Crypto Engine:
AES, Hash, ECC, etc.

NXP

LPC55S6x
Arm® Cortex®-M33
TrustZone®
@ 150 MHz
HW Crypto Engine:
AES, SHA2, RNG, etc.

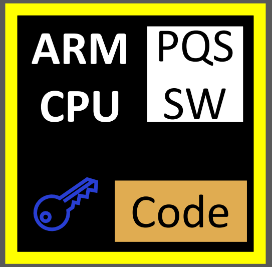
MICROCHIP



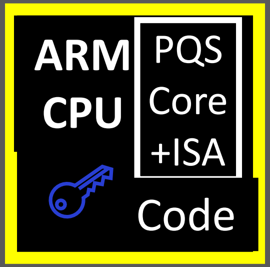
ATECC608A
Crypto Co-Processor
HWCrypto Engine:
AES, SHA2, ECDH,
ECDSA etc.
SCA protection

"Distribution Statement A – Approved for Public Release, Distribution Unlimited"

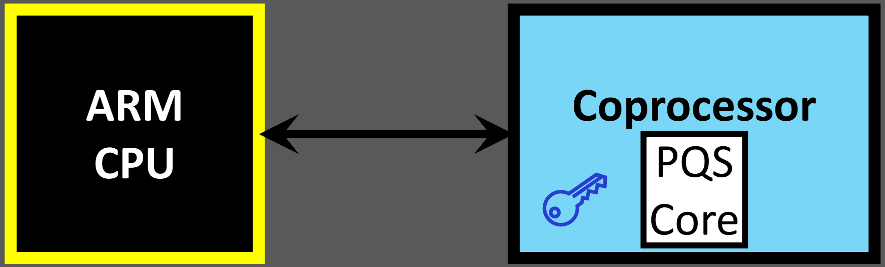
PQSecure’s Design Choices



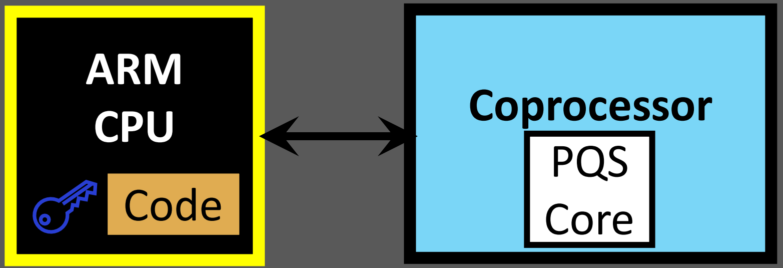
(a) SW only design
(e.g., ARM Cortex-M4)



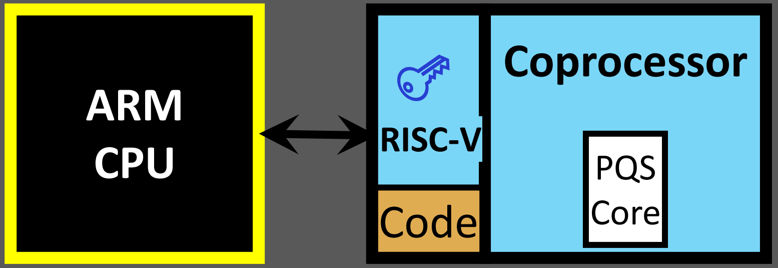
(b) Custom Instructions design
(e.g., ARM Cortex-M33)



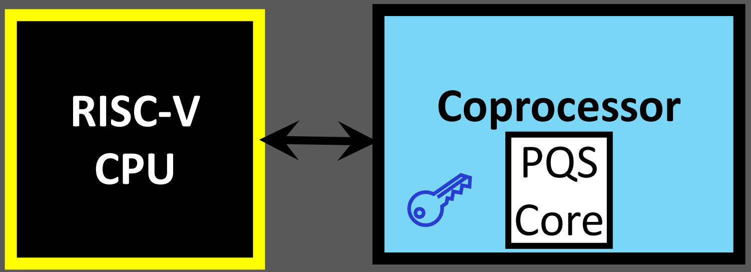
(c) HW only design with
ASIC or FPGA prototype



(d) HW/SW co-design with HW in ASIC/
FPGA and SW in ARM Cortex-M4

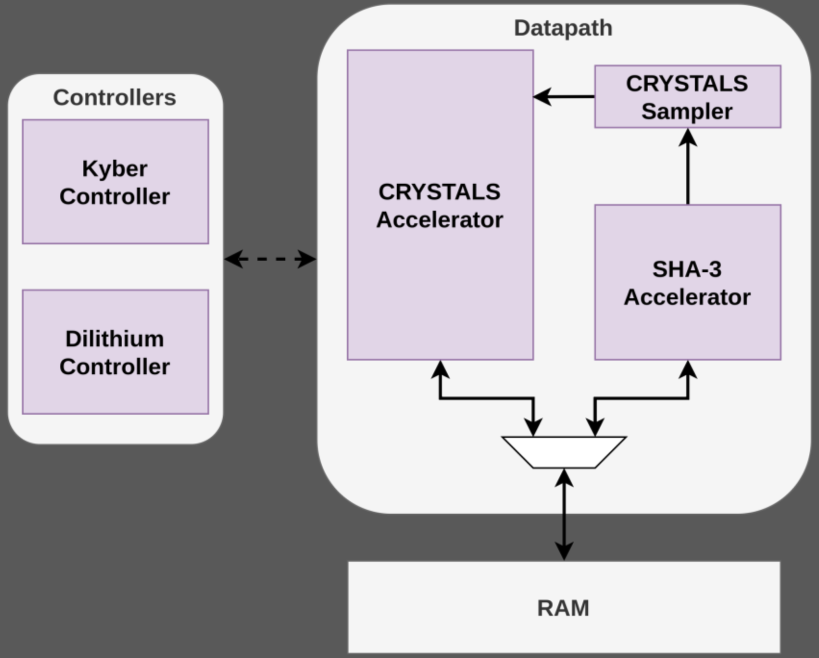


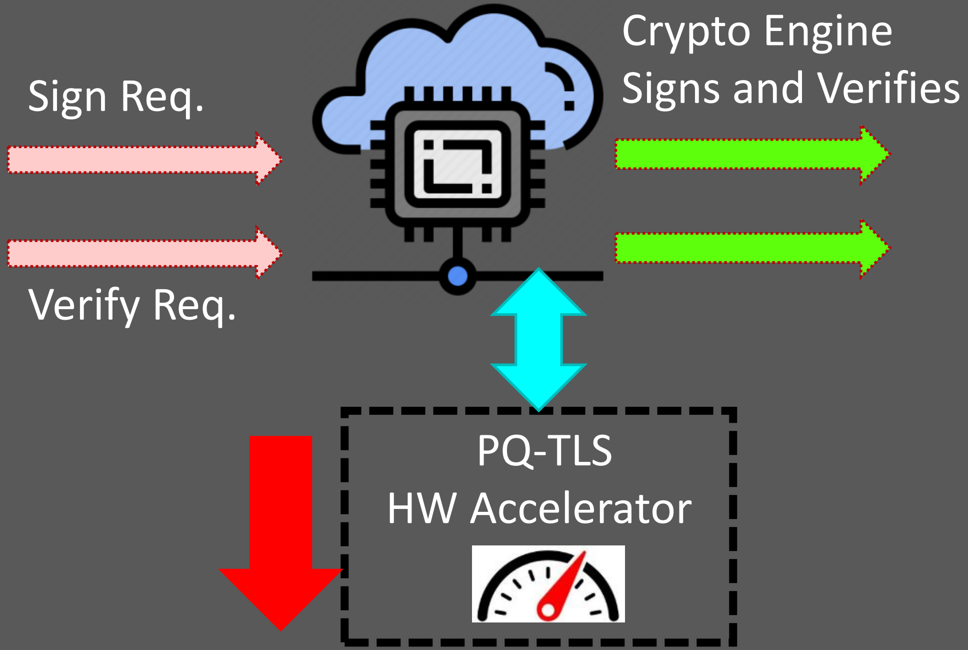
(e) HW/SW RISC-V (or custom) with
ASIC or FPGA



(f) HW only with RISC-V with ASIC or
FPGA

Integration into TLS



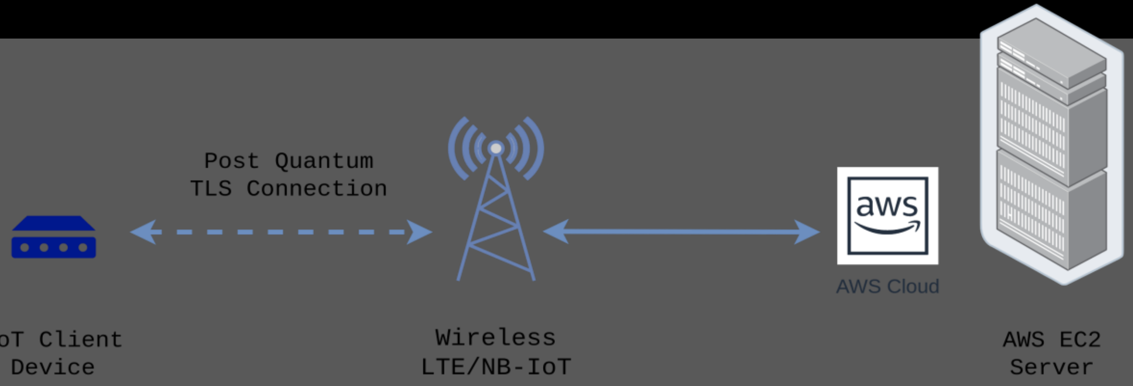


- Performance for both algorithms is the same as separate modules
- Combined module uses ~30% fewer resources

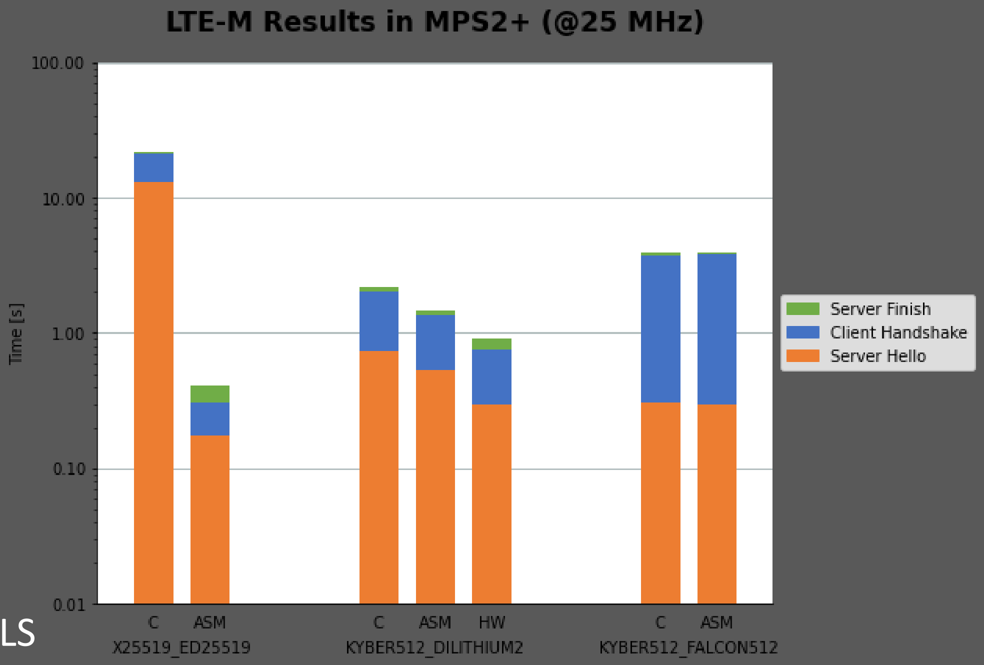
“Distribution Statement A – Approved for Public Release, Distribution Unlimited”

TLS Integration to IoT: SW/HW Cellular

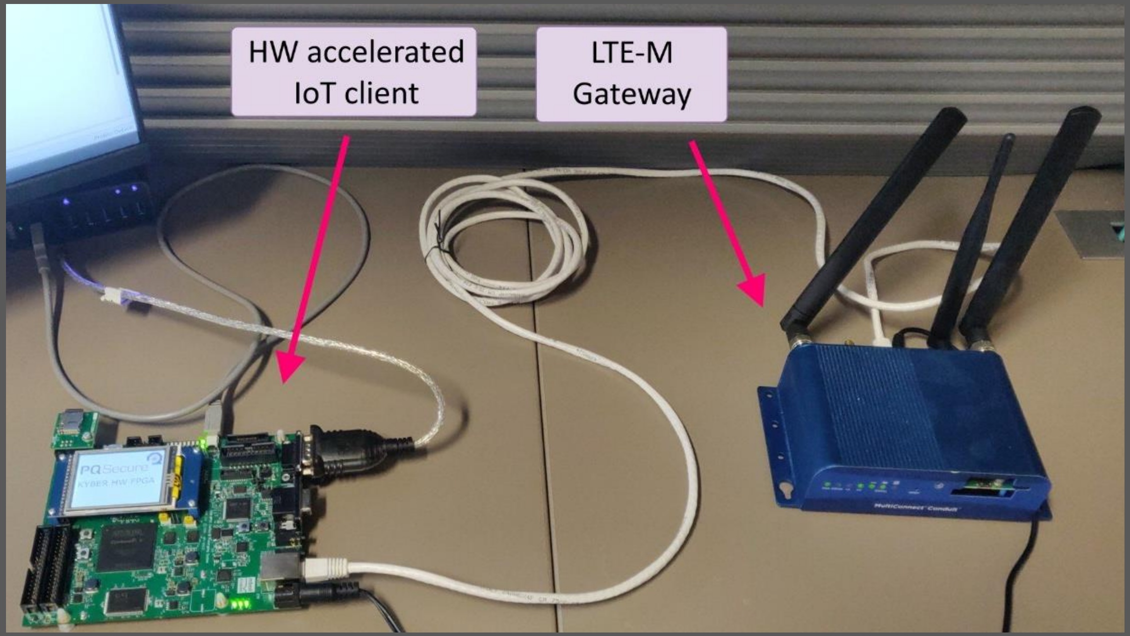
NRF9160 Cellular IoT LTE/M



TLS 1.2 in mbedTLS



“PQSecure Inside” embedded



HW acceleration makes computations ~ x50 faster

“Distribution Statement A – Approved for Public Release, Distribution Unlimited”

Questions?

Dr. Reza Azarderakhsh

razarder@pqsecurity.com

in @PQSecure

@PQSecure

www.pqsecurity.com

"Distribution Statement A – Approved for Public Release, Distribution Unlimited"