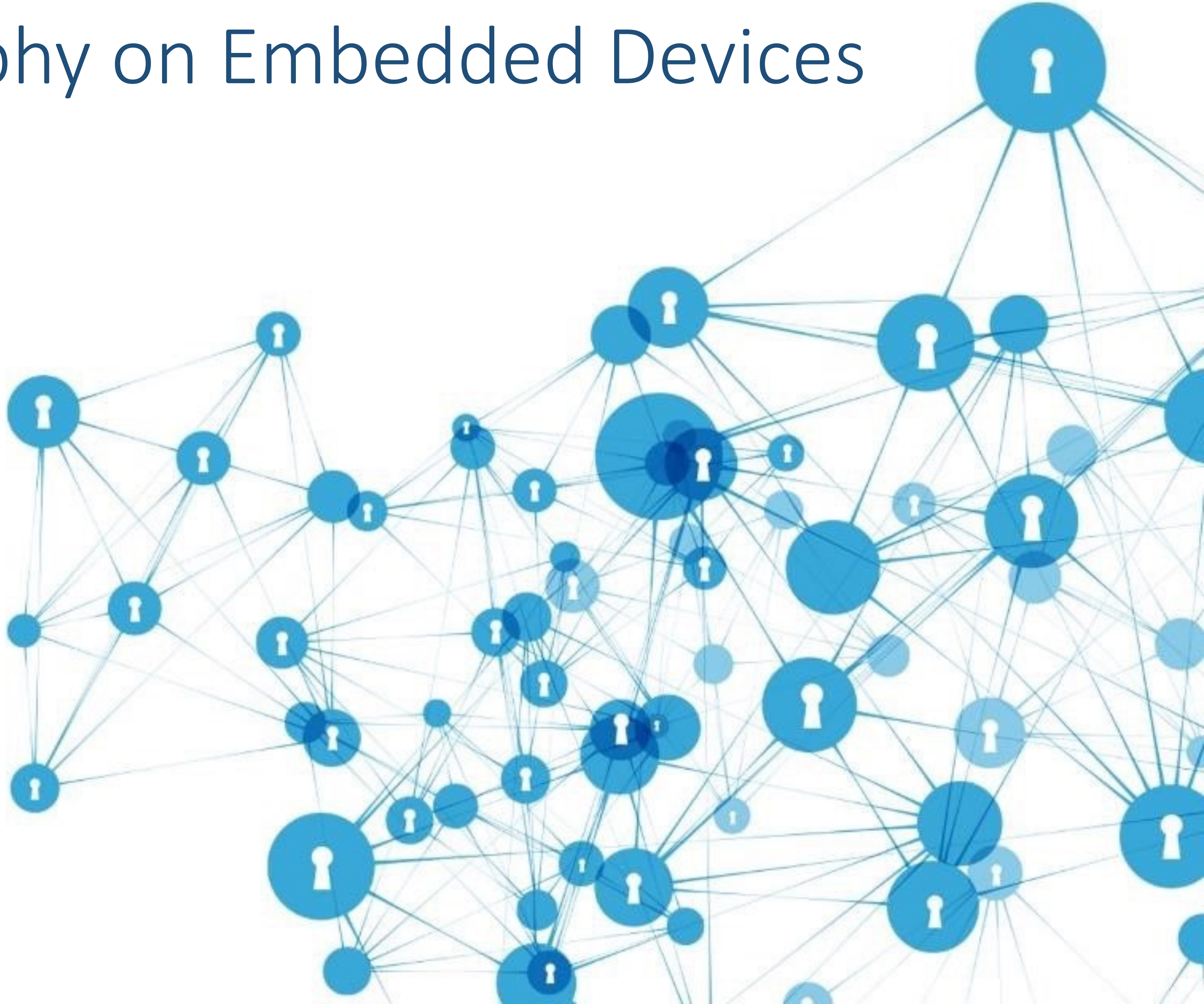
Requirements for Post-Quantum Cryptography on Embedded Devices for the IoT



NIST PQC Conference #3

June 2021

Derek Atkins, CTO

Veridify Security

The IoT needs PQC
(possibly more than the regular Internet)

- Long-lived devices
  - In some cases, devices deployed for 20-40 years!
- Embedded in critical infrastructure
  - Power grid, water treatment, transportation controls
- Even with firmware updates, it is hard to change a root of trust
- Need long-lived, trusted crypto *now*.

MCUs are smaller than they appear

- NIST has recommended a focus on the Arm® Cortex®-M4
- The IoT, however, uses many smaller MCUs
  - Arm® Cortex®-M0
  - RISC-V
  - ARC
  - AVR
  - etc.
- Less storage, less RAM, slower clocks
- Devices with these MCUs still require PQ security

Veridify Security

Current MCU resources

- Clock speeds as low as 8-24MHz
  - As high as 100-300MHz
- ROM/Flash as low as 16-32KB
- RAM as low as 4-16KB
- No floating point support
- Sometimes not even a 32x32 multiplier

MCU resource growth trends

- ROM/Flash is growing larger, faster than RAM
  - XMC1100: Cortex M0 with 64K Flash, 16K RAM
  - RSL10: Cortex M3 with 384K Flash, 32K RAM
  - PIC-8: 56K Flash, 4K RAM
- ROM/Flash sizes can get up to 1-2MB on the very large size
- RAM sizes top out around 64KB
- Financial/market pressures keep extending the use of small devices

Round 3 candidate requirements

- Source: PQM4 Metrics at github.com/mupq/pqm4
- Assumption: port to M3 or M0 wont significantly impact ROM/RAM
- Signatures:
  - Falcon: 160KB Code Size, 500B (0.5KB) RAM
    - Tradeoff: 80KB Code Size for 4-8KB RAM
  - Dilithum: 12-20KB Code Size, 40-70KB RAM
- KEMs:
  - Plenty of options in 5-10KB ROM and 3-24KB RAM

Veridify Security

Recommendations

- Consider devices smaller than Arm Cortex-M4
    - Specifically, at least Arm Cortex-M0, if not smaller
- Focus on smaller RAM vs. smaller ROM
    - Enables PQC to fit on more, smaller devices
- Based on these metrics, market would prefer:
    - Falcon over Dilithium for signatures
    - Saber or Kyber for a KEM, with Kyber taking precedence

Veridify Security

Veridify
Security

Your Partner in IoT Security

Company Headquarters
100 Beard Sawmill Road, Suite 300
Shelton, CT 06484 USA
+1.203.227.3151
info@veridify.com

California Office
75 East Santa Clara, Floor 6
San Jose, CA 95113 USA
+1.888.272.1977