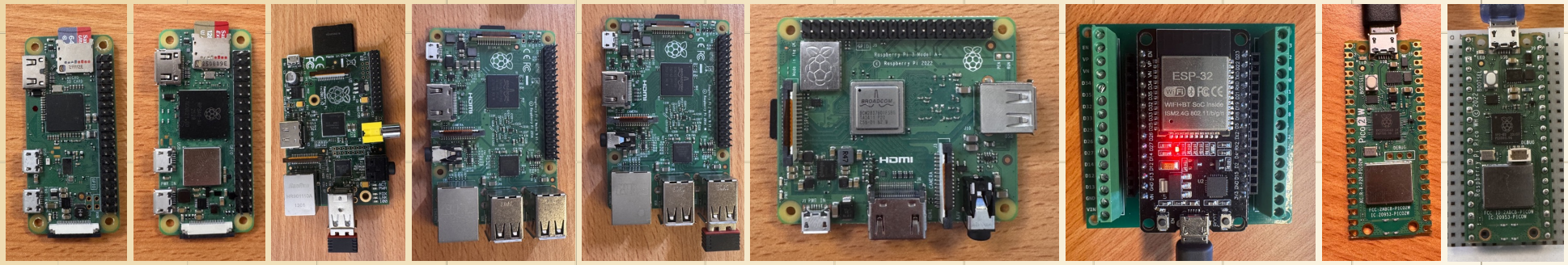
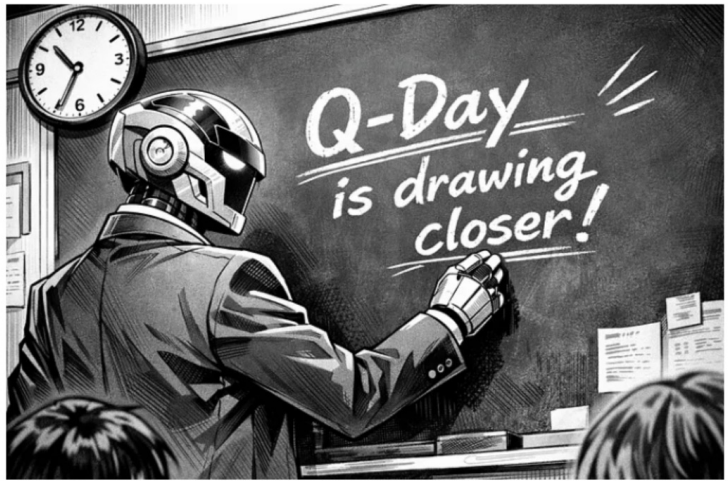
OpenSSL CONFERENCE

# *Practical Viability of NIST Post-Quantum Algorithms on Constrained ARM Devices and Microcontrollers: A Timing and Energy Study*



- *Why PQC?*
- **Q-day getting nearer, government timelines already tightening.**
- **UK 2031 · EU 2035 · US 2030**

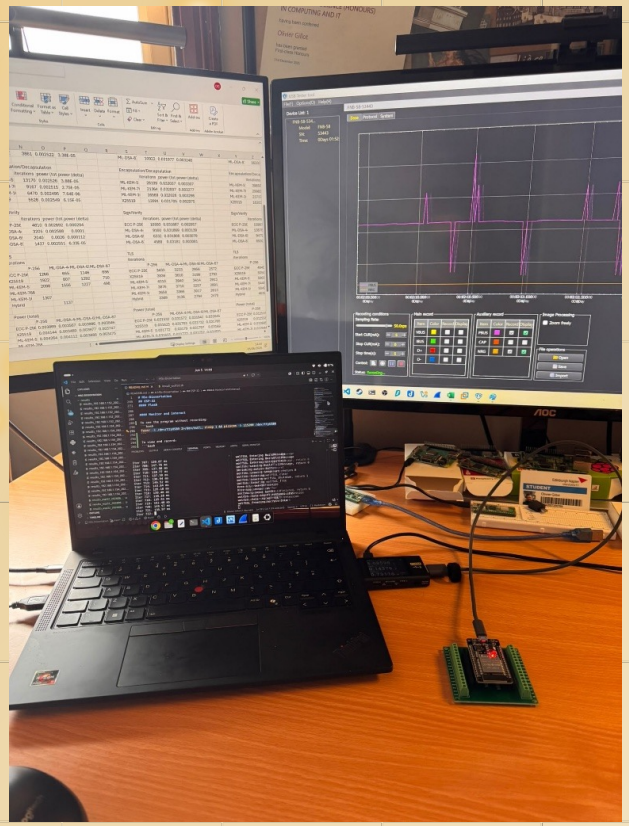



Member-only story

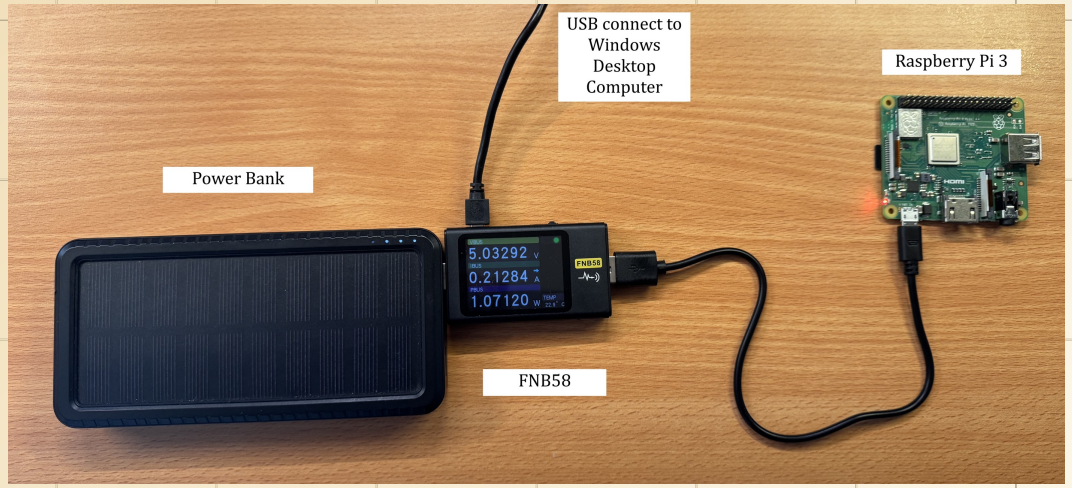
Cybersecurity + Cryptography +

## Q-Day Gets Nearer?

Prof Bill Buchanan OBE FRSE Follow 2 min read · Mar 8, 2026

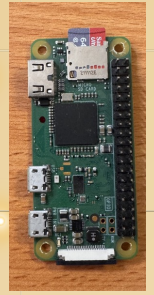


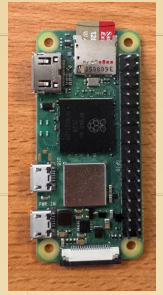
FNB58 allows for recording of up to 100 samples per second with the two metrics we're interested in: Watts (instant snapshot), Energy (Wh/Joules), consumption over time.



# • *Devices tested*

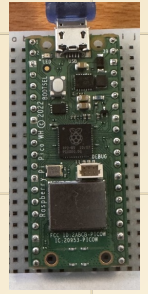
Pi Zero 1 & 2



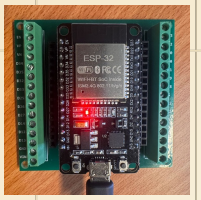


Pi 1, 2 (v1.1), 2 (v1.2), 3

Pico W 1 & 2



ESP32



# Key Generation
# X25519 vs ML-KEM-768

| Device | Library | Specs | x25519 | ML-KEM-768 |
|---|---|---|---|---|
| Pico W | wolfSSL | RP2040, dual-core Cortex-M0+ @ 133MHz, 264KB SRAM | | |
| Pico 2 W | wolfSSL | RP2350, dual-core Cortex-M33 @ 150MHz, 520KB SRAM | | |
| ESP32 | wolfSSL | Xtensa LX6, dual-core @ 240MHz, 520KB SRAM | | |
| Pizero WH | OpenSSL | ARM1176 single-core @ 1GHz (32-bit, ARMv6), 512MB RAM | | |
| Pi 1 | OpenSSL | ARM1176 single-core @ 700MHz (32-bit, ARMv6), 512MB RAM | | |
| Pi 2 (v1.1) | OpenSSL | Cortex-A7 quad-core @ 900MHz (32-bit, ARMv7), 1GB RAM | | |
| Pi 2 (v1.2) | OpenSSL | Cortex-A53 quad-core @ 900MHz (64-bit, ARMv8), 1GB RAM | | |
| Pizero 2 WH | OpenSSL | Cortex-A53 quad-core @ 1GHz (64-bit, ARMv8), 512MB RAM | | |
| Pi 3 | OpenSSL | Cortex-A53 quad-core @ 1.2GHz (64-bit, ARMv8), 1GB RAM | | |

# Key Generation
# X25519 vs ML-KEM-768 (wolfSSL only)

| Device | Library | Specs | x25519 | ML-KEM-768 |
|---|---|---|---|---|
| Pico W | wolfSSL | RP2040, dual-core Cortex-M0+ @ 133MHz, 264KB SRAM | | |
| Pico 2 W | wolfSSL | RP2350, dual-core Cortex-M33 @ 150MHz, 520KB SRAM | | |
| ESP32 | wolfSSL | Xtensa LX6, dual-core @ 240MHz, 520KB SRAM | | |
| Pizero WH | wolfSSL | ARM1176 single-core @ 1GHz (32-bit, ARMv6), 512MB RAM | | |
| Pi 1 | wolfSSL | ARM1176 single-core @ 700MHz (32-bit, ARMv6), 512MB RAM | | |
| Pi 2 (v1.1) | wolfSSL | Cortex-A7 quad-core @ 900MHz (32-bit, ARMv7), 1GB RAM | | |
| Pi 2 (v1.2) | wolfSSL | Cortex-A53 quad-core @ 900MHz (64-bit, ARMv8), 1GB RAM | | |
| Pizero 2 WH | wolfSSL | Cortex-A53 quad-core @ 1GHz (64-bit, ARMv8), 512MB RAM | | |
| Pi 3 | wolfSSL | Cortex-A53 quad-core @ 1.2GHz (64-bit, ARMv8), 1GB RAM | | |

# Signing
# Ed25519 vs ML-DSA-65

| Device | Library | Specs | Ed25519 | ML-DSA-65 |
|---|---|---|---|---|
| Pico W | wolfSSL | RP2040, dual-core Cortex-M0+ @ 133MHz, 264KB SRAM | | |
| Pico 2 W | wolfSSL | RP2350, dual-core Cortex-M33 @ 150MHz, 520KB SRAM | | |
| ESP32 | wolfSSL | Xtensa LX6, dual-core @ 240MHz, 520KB SRAM | | |
| Pizero WH | OpenSSL | ARM1176 single-core @ 1GHz (32-bit, ARMv6), 512MB RAM | | |
| Pi 1 | OpenSSL | ARM1176 single-core @ 700MHz (32-bit, ARMv6), 512MB RAM | | |
| Pi 2 (v1.1) | OpenSSL | Cortex-A7 quad-core @ 900MHz (32-bit, ARMv7), 1GB RAM | | |
| Pi 2 (v1.2) | OpenSSL | Cortex-A53 quad-core @ 900MHz (64-bit, ARMv8), 1GB RAM | | |
| Pizero 2 WH | OpenSSL | Cortex-A53 quad-core @ 1GHz (64-bit, ARMv8), 512MB RAM | | |
| Pi 3 | OpenSSL | Cortex-A53 quad-core @ 1.2GHz (64-bit, ARMv8), 1GB RAM | | |

# *Signing SLH-DSA*

| Device | Library | Specs | Signing time |
|---|---|---|---|
| Pico W | wolfSSL | RP2040, dual-core Cortex-M0+ @ 133MHz, 264KB SRAM | |
| Pico 2 W | wolfSSL | RP2350, dual-core Cortex-M33 @ 150MHz, 520KB SRAM | |
| ESP32 | wolfSSL | Xtensa LX6, dual-core @ 240MHz, 520KB SRAM | |
| Pizero WH | OpenSSL | ARM1176 single-core @ 1GHz (32-bit, ARMv6), 512MB RAM | |
| Pi 1 | OpenSSL | ARM1176 single-core @ 700MHz (32-bit, ARMv6), 512MB RAM | |
| Pi 2 (v1.1) | OpenSSL | Cortex-A7 quad-core @ 900MHz (32-bit, ARMv7), 1GB RAM | |
| Pi 2 (v1.2) | OpenSSL | Cortex-A53 quad-core @ 900MHz (64-bit, ARMv8), 1GB RAM | |
| Pizero 2 WH | OpenSSL | Cortex-A53 quad-core @ 1GHz (64-bit, ARMv8), 512MB RAM | |
| Pi 3 | OpenSSL | Cortex-A53 quad-core @ 1.2GHz (64-bit, ARMv8), 1GB RAM | |

# TLS: Hybrid vs Full PQC

| | Pico 2 | ESP32 |
|---|---|---|
| Hybrid (ML-KEM-768/x25519) for keys. Ed25519 for signature. | | |
| ML-KEM-768 for keys. ML-DSA-65 for signature. | | |

# *Key Takeaways*

- **So, what does 30 minutes with nine live devices actually tell us?**
- **1. OpenSSL and wolfSSL differ in implementation, not concept.**
- **2. ML-KEM and ML-DSA aren't just viable on constrained hardware, they're often the better choice, although on microcontrollers, only some variant may be available.**
- **3. SLH-DSA works even on microcontrollers, with only Pico 1 as the exception.**
- **4. The IETF-recommended hybrid's real-world cost depends on implementation, not just algorithm choice.**

This talk was based on my published paper and my current active research, under the supervision of Prof. Bill Buchanan:
Energy Consumption of Post-Quantum Cryptography on Constrained and General-Purpose Architectures, MDPI Cryptography, 2026