Cal Poly Pomona

Thoth: Open-Source Kubernetes Orchestration of Dilithium & Kyber for Quantum-Resilient Multi-Architecture Clusters

Mohamed El-Hadedy[1]
Reconfigurable Space Computing Lab, Cal Poly Pomona

Benny Cheng[2]
NAVSEA Warfare Centers Corona

Wen-Mei Hwu[3]
Coordinated Science Lab, UIUC

OSCAR2025, Japan – June 21

Why Thoth? Quantum Threats & Edge Constraints

Imminent quantum risk

- Shor's algorithm can break RSA/ECC in hours on ~4 000-qubit machine
- Today's TLS/SSH links become insecure overnight

PQC adoption gap

- NIST's CRYSTALS-Dilithium & Kyber are standardized

Edge constraints

- Resource-limited nodes (TRK1 RISC-V. Pi Zero)
- Tight power budgets (1 W per verifier)
- Real-time latency needs (< 15 ms end-to-end

Heterogeneous clusters

- Multi-architecture (RISC-V+ARM)
- Require unified, lightweight

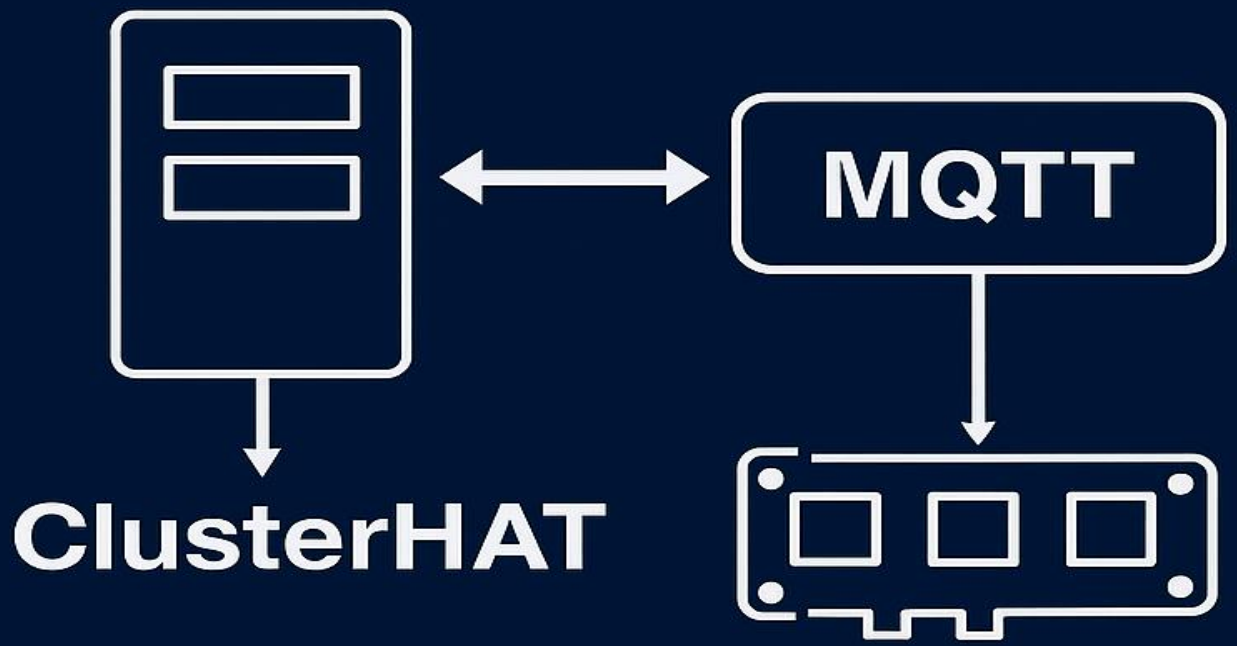
Thoth bridges this gap—delivering sub-7 ms PQC on resource-constrained, multi-architecture clusters.

Thoth System Architecture

Cal Poly Pomona

THOTH

Turing Pi 2.5



- Kubernetes master on TRK1 nodes
- Turing Pi 2.5 with 4 Compute Modules 4/4S
- MQTT for interconnect & messaging
- ClusterHAT with 4 Pi Zero verifiers

Performance Results

- Dilithium signing on Turing Pi (TRK1): 6.5 ms (avg)
- Kyber encapsulation on Turing Pi (TRK1): 6.7 ms (avg)
- Kyber decapsulation on Turing Pi (TRK1): 4,2 ms (avg)
- Dilithium verification on Turing Pi (TRK1): 3.5 ms (avg)
- Verification throughput on ClusterHAT (Pi Zero): 813 ops/s

813 ops/s

1.1 W

Impact & Future Work

Secure edge deployment

Cluster scaling & robustness

Integration with space systems

Opportunities abound – projected across defense, industrial, and aerospace domains.