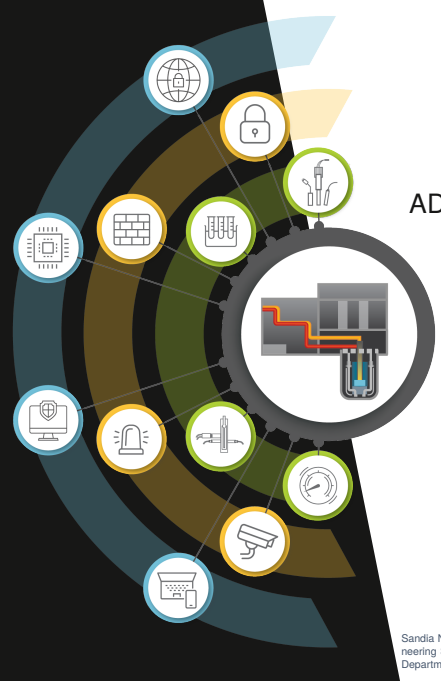


ADVANCED REACTOR SAFEGUARDS & SECURITY

Encryption Effects on Short Range Communication

Presented by

Christopher C. Lamb[1] **Greg White**[2]

[1]Sandia National Laboratories [2]Lawrence Livermore National Laboratory

April 28-30, 2026

SAND2026-20356C

Sandia National Laboratories is a multi-mission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC (NTESS), a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration (DOE/NNSA) under contract DE-NA0003525.

Sandia National Laboratories

U.S. DEPARTMENT OF ENERGY

Motivation: The Safety vs. Security Tension

- Digital I&C in nuclear plants introduces cybersecurity risks with no analog precedent
- Standards now mandate TLS for industrial protocol security:
  - IEC 62351-3 (power systems), Modbus/TCP Security, IEEE 1815 (DNP3)
  - Minimum: TLS 1.2 with X.509v3 mutual authentication
- Persistent objection from control system engineers:
  "Encryption is incompatible with real-time safety constraints"
- Result: limited adoption of cryptographic protections in nuclear OT

Prior Work and the Open Question

Lamb & Sandoval (IAEA CN313, 2023): TLS 1.2 over internet-connected endpoints

- Mean overhead: ≈ 5 ms — small
- Standard deviation: 40 ms–100 ms — large
- Cause attributed to wide-area network effects and remote CA round trips

2023 hypothesis: Local PKI on a dedicated local segment would substantially reduce timing variance.

This work:

- Tests that hypothesis directly in a controlled, isolated local environment
- Extends evaluation to TLS 1.3 and post-quantum hybrid key exchange (NIST FIPS 203)

Experimental Setup

Hardware

Role	Device
Client (A)	Raspberry Pi 5
Server (B)	Raspberry Pi 5
Network	Ubiquiti Flex

Isolated L2 segment — no external routing.
Cortex-A76, 4 GB RAM on each endpoint.

Two network media

- Wired: Cat 6 Ethernet
- Wireless: IEEE 802.11ac

Scale

- 196,000 request measurements
- 14 experimental configurations
- 1,000 iterations per payload size
- All client-side timing; no server-side metrics

Measurement Design

Why HTTP, not Modbus or DNP3?

- TLS operates *below* the application layer — cipher overhead is independent of protocol framing
- Payload *size* is the relevant variable, not protocol semantics

Payload sizes map to representative I&C messages:

Size	Representative message type
64 B	Modbus read holding registers response
256 B	DNP3 Class 0 poll response
512 B	IEC 61850 GOOSE trip frame
2048 B	OPC UA subscription notification

Payloads are randomly generated bytes to eliminate compression artifacts.

Cipher Suite Matrix

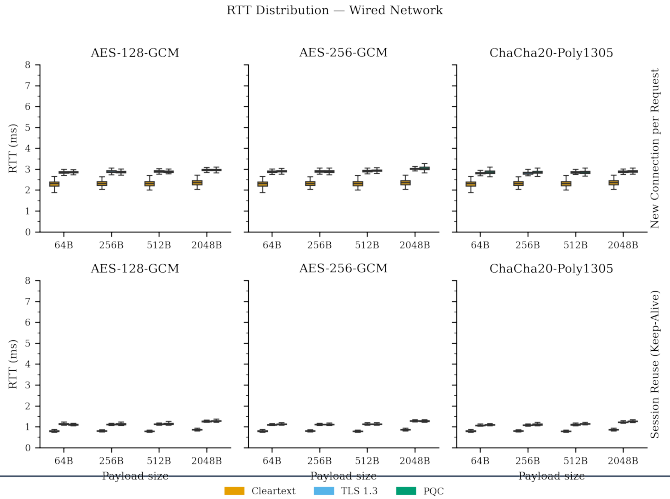
Three conditions × three AEAD cipher suites:

- **Cleartext baseline** — unencrypted, establishes the timing floor
- **TLS 1.3, classical** — ECDHE (X25519) key exchange
  - AES-128-GCM, AES-256-GCM, ChaCha20-Poly1305
  - Current state-of-practice upgrade path from TLS 1.2
- **TLS 1.3, post-quantum hybrid** — X25519MLKEM768
  - Classical ECDHE + ML-KEM-768 (NIST FIPS 203 / Kyber)
  - Secure against classical and quantum adversaries during transition

Two session modes per cipher:

- **New connection per request** — worst case; isolates handshake cost
- **Session reuse (keep-alive)** — isolates per-message encryption cost

Wired Network RTT Distributions



Wired RTT: Key Findings

Cleartext baseline:

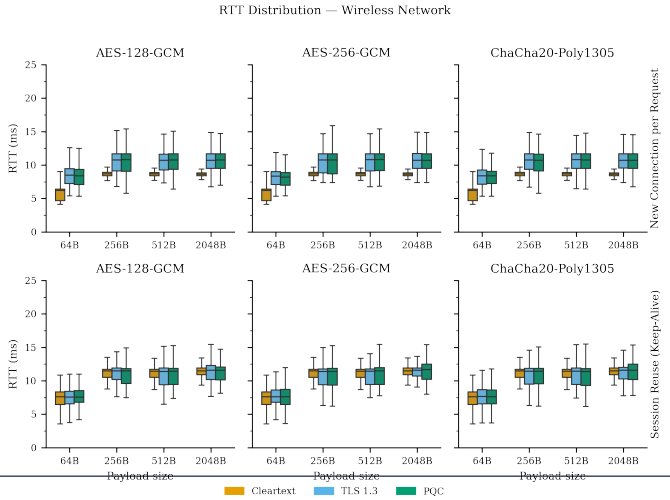
- No-reuse: 2.30–2.37 ms mean, std 0.13–0.17 ms
- Session reuse: 0.79–0.87 ms mean, std as low as 0.035 ms

TLS 1.3 overhead:

- No-reuse: 0.53–0.68 ms (all three cipher suites)
- Session reuse: 0.29–0.43 ms, std < 0.16 ms
- No operationally meaningful difference among the three cipher suites

2023 hypothesis confirmed. Local PKI eliminates variance: std is now 0.035–0.16 ms, versus 40–100 ms over WAN in the prior work.

Wireless Network RTT Distributions



Wireless RTT: The Session Reuse Effect

Without session reuse:

- TLS 1.3 added 2.29 ms mean overhead over wireless cleartext
- Std rose to 1.45–9.29 ms
- Multi-packet TLS handshake is vulnerable to 802.11 retransmissions — single event injects 50–220 ms spike
- 131 observations exceeded the 25 ms display threshold

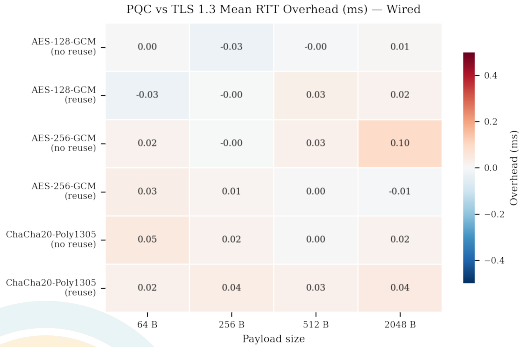
With session reuse:

- TLS overhead collapsed to 0.031 ms — **98% reduction**
- Std returned to 1.12–1.65 ms, matching cleartext
- All three conditions visually identical (bottom row of figure)

Session reuse eliminates wireless handshake vulnerability entirely.

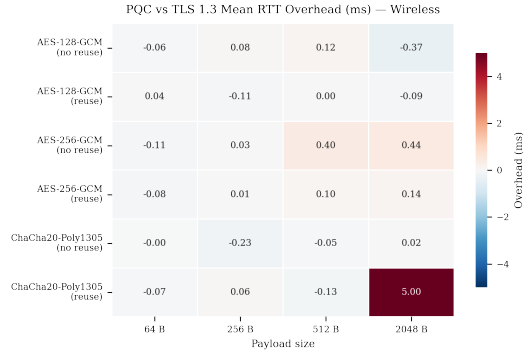
Post-Quantum Overhead: X25519MLKEM768 vs. X25519

Wired



All cells within ± 0.1 ms.
Inconsistent sign across cells — noise, not signal.

Wireless



One anomalous cell (wireless interference burst during collection).
All other cells $\leq \pm 0.05$ ms.

Statistical Analysis: Mann-Whitney U

Bonferroni-corrected Mann-Whitney U tests, 48 comparisons per group:

TLS 1.3 vs. Cleartext

- 38 of 48 significant ($p_{\text{corr}} < 0.05$)
- Handshake overhead is real and detectable at $n{=}1000$
- 10 non-significant: wireless reuse configurations, where medium variance masks the TLS cost

PQC vs. TLS 1.3

- 20 of 48 significant
- Max effect size: 0.096 ms
- At $n{=}1000$, the test resolves differences well below any operationally meaningful threshold

Statistical significance $\neq$ operational significance.
No practically relevant RTT difference is attributable to ML-KEM-768.

Resource Utilization

CPU — no-reuse condition (wired):

- Cleartext: 5.8% mean
- TLS 1.3 / PQC: ≈48% mean — 8× increase from handshake computation
- Bimodal distribution: alternating handshake bursts and inter-request idle time

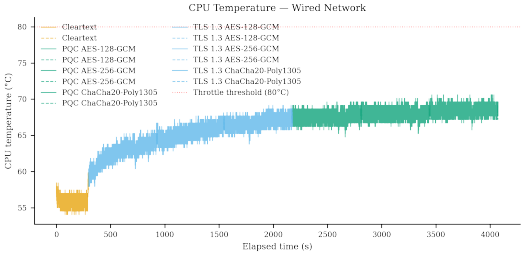
CPU — session reuse:

- All three conditions converge to ≈55–56% on wired, 13–17% on wireless
- **No cipher-dependent variation** — per-message symmetric encryption adds no measurable CPU cost

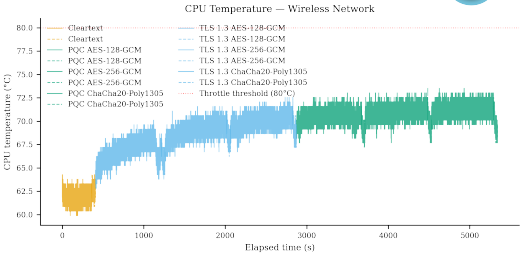
Memory: 121 MB–125 MB RSS; stable across all conditions, no growth within runs

Processor Temperature

Wired



Wireless



- Temperature increased monotonically across sequential runs — cumulative thermal loading across the full campaign
- Wired peak: $70.6\,°$C; wireless peak: $73.5\,°$C — both well below the $80\,°$C throttle threshold
- No cipher suite produced a discernibly different thermal trajectory at equivalent CPU utilization

What Actually Drives I&C Latency

Network medium dominates — not cipher suite:

- Wired cleartext reuse: 0.82 ms mean
- Wireless cleartext reuse: 10.19 ms mean
- $12.4\times$ difference from 802.11 MAC overhead alone

The critical comparison:

- TLS 1.3 overhead on wired: 0.34 ms
- Irreducible wireless std (reuse): 1.35 ms
- **Encryption cost $<$ wireless jitter**

On dedicated wired I&C infrastructure:

- Encryption is **not** the latency bottleneck
- Cipher suite and key exchange algorithm choice are engineering non-issues
- Network medium selection has far greater impact on timing determinism

Conclusions

1. **TLS 1.3 with session reuse imposes negligible overhead**
   0.29–0.43 ms on wired SMR I&C networks; std below 0.16 ms
2. **Post-quantum hybrid cryptography is operationally ready**
   X25519MLKEM768 carries no performance penalty on current embedded hardware; PQC migration can proceed without reservation
3. **Session management is the critical design decision**
   Session reuse reduces wireless TLS overhead by 98% and eliminates handshake-induced variance
4. **Network medium matters more than cipher suite**
   Wired vs. wireless choice dominates I&C latency by more than an order of magnitude

Future work: multi-node reactor network topologies, mutual TLS certificate authentication, protocol-specific measurements under concurrent traffic

Questions

?