PQ-Audit: A Formally Verified Minimax Calculus and Live Multi-Protocol Scanner for Post-Quantum and Classical Cryptographic Exposure

Fabien Pierret
Independent Researcher · WallStreetDebug Research
ORCID: 0009-0001-1223-2170 · Live Edge Scanner: https://pq.wallstreetdebug.com
Open-Source Code & Lean 4 Proofs (MIT): https://github.com/fabien-pierret/pq-audit

November 27, 2026

Abstract

In late 2026, the combination of finalized NIST post-quantum standards (FIPS 203/204/205 and NIST IR 8547), IETF RFC 10024 hybrid TLS 1.3 key exchange (`X25519MLKEM768`), Bitcoin draft BIP-360 (`P2MR`), and viral public discussion of AI-assisted cryptanalysis created intense demand among retail crypto holders and enterprises for clear, non-sensational cryptographic survival audits. Existing dashboards suffer from three structural flaws: (i) weighted-average (L_p) compliance scores mathematically conceal single-endpoint or single-UTXO compromises; (ii) on-chain scanners routinely misclassify unspent Taproot (`P2TR`), Ethereum EIP-7702 delegated EOAs (`0xef0100`), and Solana SPL Associated Token Accounts; and (iii) unverified migration advice omits self-change leakage and partial-sweep traps. We introduce **PQ-Audit**, a three-layer framework uniting: (1) a standalone, zero-dependency **Lean 4.36.0** formalization (`PQAuditCore.lean`, **35/35** public theorems, **0 `sorry`**, `-DwarningAsError=true`, standard kernel axioms only, audited by two independent referees) proving irreversible public-key reuse monotonicity, field-general classical ECDSA nonce-reuse recovery across both standard ($s_1 - s_2$) and BIP-62/EIP-2 low-S ($s_1 + s_2$) branches, dimension-free IFF uniqueness of minimax L_∞ scoring alongside universal simplex-L_p dilution blindness, full-wallet zero-leakage UTXO migration and authority inheritance invariants, and assumption-free Fréchet hybrid KEM combiner bounds; (2) the MIT-licensed Python scanner `pqaudit` and edge web application `pq.wallstreetdebug.com` (100% read-only with fail-closed private-key/seed rejection); and (3) a reproducible live empirical benchmark conducted on November 27, 2026 across **100 global/SME HTTPS domains** (OpenSSL 4.1.0) and **15 iconic public Bitcoin, Ethereum, and Solana wallets**. Empirically, **71.0%** (71/100) of audited domains already negotiate RFC 10024 `X25519MLKEM768` (Crypto/Web3 **95.0%**, Cloud/Big Tech **85.0%**, Dev/SaaS **80.0%**), whereas **Finance & Banking lags at 50.0%** and **Government & Academia at 45.0%**—including a live Grade-F non-PFS RSA TLS 1.2 finding (`stanford.edu`). On-chain, we observe over **405,600 BTC** sitting in reused exchange cold wallets, confirm funded unspent Taproot (`bc1p`) key-path exposure versus hash-shielded `bc1q`, and catch `vitalik.eth` live as an **EIP-7702 delegated EOA** (`0xef0100`) rather than a keyless smart contract.

1 Introduction: Rigorous Cryptographic Triage Without Quantum Hype

Public anxiety surrounding post-quantum cryptography (PQC) and AI-accelerated cryptanalysis peaked in November 2026 following high-profile commentary by Scott Aaronson [1] clarifying that while theoretical AI-assisted mathematical advances warrant attention, *no verified practical break of RSA-2048, `secp256k1`, or `Ed25519` exists today.* Likewise, public quantum cryptanalysis milestones remain at toy key sizes (e.g., breaking a 15-bit elliptic curve key in April 2026). Fear-driven messaging harms users by inducing rushed key migrations and fraudulent "quantum-safe wallet" scams.

Yet dismissing post-quantum hygiene altogether is equally flawed. Three concrete, deterministic, and currently measurable cryptographic risks exist *today*:

1. **Immediate classical compromises (Level 4, Grade F):** ECDSA duplicate-r nonce reuse on Bitcoin/Ethereum [3], expired/weak X.509 certificates, TLS 1.0/1.1, and non-PFS RSA TLS 1.2 key transport—requiring *zero* quantum hardware.
2. **Active Harvest-Now-Decrypt-Later (HNDL) confidentiality exposure (Level 3, Grade D):** Classical-only TLS 1.2/1.3 endpoints lacking IETF RFC 10024 hybrid ML-KEM (`X25519MLKEM768`, IANA `0x11EC`) [6, 9] expose recorded sessions whose secrecy lifetime X plus migration time Y exceeds the NIST IR 8547 2030/2035 horizon [8, 7].
3. **Permanent on-chain static public-key exposure (Level 3, Grade D):** Bitcoin `P2PK` outputs, reused `P2PKH`, `P2SH`, `P2WPKH`, and `P2WSH` addresses, unspent Taproot `P2TR` outputs [11] (whose locking script directly exposes tweaked curve point $Q = P + H_{\text{TapTweak}}(P\|m)G$), active Ethereum EOAs (nonce ≥ 1) and EIP-7702 delegated EOAs (`0xef0100`) [4], and on-curve Solana `Ed25519` wallets [5] (whose address *is* the raw public key).

We enforce strict **3-layer epistemic demarcation**: **Layer 1** (standalone Lean 4.36.0 machine-checked deterministic invariants in `lean/PQAuditCore.lean`), **Layer 2** (analytical cryptographic, HNDL, and mempool models), and **Layer 3** (reproducible live empirical probes of 100 global/SME domains and 15 public wallets).

2 Formal Model and Machine-Checked Theorems (Lean 4.36.0)

All deterministic theorems below are verified in `lean/PQAuditCore.lean` (**35/35** public declarations, **0 `sorry`**, zero Mathlib dependency, compiled with `-DwarningAsError=true`, SHA-256 `ece453e90a305b33...`) using standard Lean kernel axioms only (`propext`, `Classical.choice`, `Quot.sound`), audited by two independent referee agents (`lean/AUDIT_REPORT_2_AGENTS.md`).

2.1 Exposure Lattice, Typed Monotonicity, and Field-General ECDSA Recovery

Every cryptographic surface maps to an ordered five-level lattice $\mathcal{L} = \{0 < 1 < 2 < 3 < 4\}$: `pqShielded` (0), `hashCommitted` (1), `mempoolShort` (2), `longExposedStatic` (3), and `classicalCompromise` (4). Spend transitions are typed by `KeyScheme` in {`classicalEC`, `postQuantum`, `keyless`}, and structural key exposure is kept strictly orthogonal to active at-risk balance.

Theorem 1 (Typed Monotonicity & Field-General ECDSA Recovery — Lean 1A–1F)**.** *1.* ***Typed Spend Monotonicity (1A–1B):*** *Under `classicalEC`, any outgoing spend locks structural exposure to ≥ 3 irreversibly—no finite sequence of subsequent incoming deposits can restore level 1 or 0—and any `nonceReuse` event absorbs to level 4. Under `postQuantum` signatures (ML-DSA/SLH-DSA), spending preserves `pqShielded` (0).*

2. ***Field-General ECDSA Recovery with Low-S Branch (1C–1D, 0 kernel axioms):*** *Over* any *commutative field $(\mathbb{F}, K)$ (covering prime field $\mathbb{F}_n$ of `secp256k1` and $\mathbb{Q}$), given $r \neq 0$, distinct digests $z_1 \neq z_2$, and either same-sign equations $s_1 k = z_1 + rd$, $s_2 k = z_2 + rd$ or BIP-62/EIP-2 low-S opposite-sign equations $s_1 k = z_1 + rd$, $(-s_2)k = z_2 + rd$, the algebraic relations* derive *$k \neq 0$ and $s_1 \mp s_2 \neq 0$ (even when $s_1 = s_2$ under low-S!) and uniquely recover $k = (z_1 - z_2)/(s_1 \mp s_2)$ and $d = (s_1 k - z_1)/r$.*

3. ***Timestamped Mosca HNDL Irreversibility (1E–1F):*** *Classical sessions captured at $t_{\text{cap}} < t_{\text{upg}}$ remain retroactively compromised whenever $T_{\text{crqc}} < t_{\text{cap}} + X$, whereas post-upgrade RFC 10024 sessions face $Y = 0$ and post-quantum horizon T_{pq}.*

2.2 Dimension-Free Minimax IFF Uniqueness and Universal Simplex-L_p Blindness

Enterprise PQC readiness dashboards commonly aggregate endpoint compliance using weighted averages (L_1) or RMS norms (L_2). Extending the minimax framework of [10] to arbitrary multi-asset cryptographic portfolios $r \in [0,1]^K$ ($K \geq 1$):

Theorem 2 (Minimax IFF, Simplex-L_p Blindness & Floor Score — Lean 2A–2I)**.** *1.* ***Global IFF Uniqueness (2D):*** *A normalized aggregator $S : [0,1]^K \to [0,1]$ satisfies both* Single-Surface Non-Compensation *($\exists i, r_i > \tau \Rightarrow S(r) > \tau$) and* Zero False-Alarm Calibration *($\forall i, r_i \leq \tau \Rightarrow S(r) \leq \tau$) for all $\tau \in [0,1]$* ***if and only if*** *$S(r) = \|r\|_\infty = \max_{1 \leq i \leq K} r_i$.*

2. ***Simplex Pigeonhole & Universal L_p Dilution Blindness (2E–2F):*** *Every simplex weight vector $w \in \Delta^{K-1}$ satisfies $w_j \leq 1/K$ for some coordinate j. Hence for every $K \geq 2$, every integer power $p \geq 1$, every simplex weight vector w, and every threshold $0 \leq \tau < 1$ with $1/K \leq \tau^p$, there exists a 100% single-surface breach $e_j \in [0,1]^K$ silently passed by L_p ($\sum_i w_i (e_j)_i^p \leq \tau^p$) yet strictly vetoed by $\|e_j\|_\infty = 1 > \tau$.*

3. ***Exact Grade Commutation & Conservative Floor Score (2G–2I):*** *Mapping risk thresholds $(0.15, 0.35, 0.55, 0.75)$ to survival grades $\{A, B, C, D, F\}$ commutes identically with $\max_i$, and the conservative integer score $S = \lfloor 100(1-R) \rfloor$ satisfies exact equivalences ($R \leq 0.15 \Leftrightarrow S \geq 85$, etc.), eliminating rounding contradictions (e.g., $R = 0.154 \Rightarrow S = 84$, Grade B).*

2.3 Full-Wallet UTXO Migration, ρ_{exp} Separation, and Authority Inheritance

Theorem 3 (Full-Wallet Sweep, ρ_{exp} Separation & Authority Inheritance — Lean 3A–3H)**.** *Modeling a complete post-migration wallet $W_{\text{post}} = W_{\text{unswept}} +\!\!+ U_{\text{out}}$ with value conservation $\sum U_{\text{out}} + \text{fee} = \sum U_{\text{in}}$ and $\sum U_{\text{out}} > 0$:*

1. ***Self-Change & Partial-Sweep Failure (3B):*** *Returning active change to any spent source address* or *leaving any exposed UTXO unswept locks $\max_{u \in W_{\text{post}}} E(u) \geq 3$.*

2. ***Clean Full-Sweep Reduction & Taproot Separation (3C–3D):*** *Sweeping 100% of exposed inputs into disjoint fresh hash-committed outputs drops stationary exposure strictly to ≤ 1 under `P2WPKH` (`bc1q`) or BIP-360 `P2MR` (`bc1z`) [2], whereas sweeping into unspent `P2TR` (`bc1p`) leaves stationary exposure at 3.*

3. ***Auxiliary Value Ratio ρ_{exp} Separation (3F):*** *While $\rho_{\text{exp}} = V_{\text{exposed}}/V_{\text{total}} \in [0,1]$ vanishes iff no active UTXO has rank ≥ 3, for every $\varepsilon > 0$ there exists a wallet with $\rho_{\text{exp}} < \varepsilon$ and an active Level 4 classical compromise.*

4. ***Authority Minimax Inheritance (3G):*** *For keyless surfaces (Solana off-curve PDAs/ATAs and Ethereum smart contracts), effective exposure $\max(E_{\text{direct}}, \max_{a \in \text{Auth}} E(a))$ equals 0 iff every controlling authority has exposure 0; any SPL ATA controlled by an on-curve `Ed25519` EOA inherits exposure ≥ 3 (Grade D).*

2.4 Assumption-Free Fréchet Hybrid KEM Combiner and TLS Path Veto

Theorem 4 (Fréchet Hybrid Combiner & Edge-to-Origin TLS Veto — Lean 4A–5B)**.** *1.* ***Assumption-Free Fréchet Bound (4A–4B):*** *Without assuming independence between classical and PQ breaks, any joint distribution $(p_{00}, p_{01}, p_{10}, p_{11})$ with combiner overhead $\varepsilon_{\text{comb}} \geq 0$ satisfies $\max(0, p_c + p_q - 1) \leq p_{11} \leq \min(p_c, p_q)$ and $p_{11} + \varepsilon_{\text{comb}} \leq \min(p_c, p_q) + \varepsilon_{\text{comb}}$. Under correlated failures (e.g., compromised shared CSPRNG), $p_{11} = \min(p_c, p_q)$ is attained with no strict gain; multiplicative reduction $\varepsilon_c \varepsilon_q < \min(\varepsilon_c, \varepsilon_q)$ requires independent break events and an ideal combiner.*

2. ***Edge-to-Origin TLS Gap Veto (4C):*** *Even when a CDN edge negotiates RFC 10024* `X25519MLKEM768` *($r_{\text{edge}} \leq 0.15$, Grade A), a classical-only origin hop ($r_{\text{origin}} > 0.55$, Grade D/F) forces end-to-end path risk* $\max(r_{\text{edge}}, r_{\text{origin}}) = r_{\text{origin}}$ *and a mandatory* ≥ 3*-tier grade drop.*

3. ***Exhaustive Calibration (5A–5B):*** *All 18 canonical surface risk constants lie in* $[0, 1]$*, map to their exact target grades, and satisfy strict inter-level lattice separation ($E = 0 < E = 1 < E = 2 < E = 3 < E = 4$).*

3 Live Empirical Benchmark (27 November 2026)

Using the MIT-licensed `pqaudit` scanner on an Apple Mac Studio M4 Max (benchmark script `sim/run_all_benchmarks.py`, runtime **7.91 s**, JSON SHA-256 `d0bab98a156b5e13`), we conducted two live real-world measurements plus two controlled algorithmic verifications.

3.1 Top-100 Global and SME HTTPS Domains (OpenSSL 4.1.0 Live Probes)

We probed 100 major domains equally stratified across five sectors ($n = 20$ each) offering RFC 10024 hybrid groups `X25519MLKEM768`, `SecP256r1MLKEM768`, `SecP384r1MLKEM1024`, `X25519`, `P-256`, and `P-384`. All **100/100** endpoints completed live TLS handshakes (Table 1, Figure 1).

Table 1: Live RFC 10024 Hybrid `X25519MLKEM768` Adoption Across 100 Global & SME Domains (27 Nov 2026).

Sector	Audited	TLS 1.3	RFC 10024	HSTS	PQ Share
Crypto & Web3	20	20	19	13	**95.0%**
Cloud & Big Tech	20	19	17	17	**85.0%**
Dev, SaaS & Retail	20	20	16	19	**80.0%**
Finance & Banking	20	16	10	16	**50.0%**
Gov & Academia	20	16	9	15	**45.0%**
Total (5 Sectors)	**100**	**91**	**71**	**80**	**71.0%**

Overall, **71.0%** (71/100) negotiated `TLSv1.3 / X25519MLKEM768` (Grade A), closely corroborating macro browser telemetry while uncovering a stark sectoral chasm: **95.0%** of Crypto/Web3 frontends (largely Cloudflare-fronted; self-hosted `mempool.space` remains classical TLS 1.3) and **85.0%** of Cloud/Big Tech are HNDL-shielded at the edge, whereas **50.0% of major Finance & Banking domains** (including `stripe.com`, `jpmorgan.com`, `chase.com`, `mastercard.com`, `morganstanley.com`, `citigroup.com`, `ubs.com`, `blackrock.com`, `fidelity.com`, and `schwab.com`) and **55.0% of Government & Academia domains** (`nasa.gov`, `nih.gov`, `irs.gov`, `europa.eu`, `service-public.fr`, `hal.science`, `mit.edu`, `harvard.edu`, `ethz.ch`, `wikipedia.org`) still negotiate classical-only TLS 1.3 (`15 X25519`, `5 prime256v1`) or TLS 1.2 (`9` domains). Notably, `stanford.edu` negotiated **TLS 1.2 static RSA (`AES128-GCM-SHA256`, no ECDHE/PFS)**, triggering a real-world **Grade F (8/100)** classical finding.

3.2 Live Read-Only On-Chain Audit of 15 Iconic Public Wallets

We audited 15 public mainnet Bitcoin, Ethereum, and Solana addresses read-only via Mempool/Blockstream and public JSON-RPC endpoints (Figure 2):

- **Bitcoin (7 wallets):** Reused institutional cold wallets—Binance P2SH (`34xp4v...`, **248,597.59 BTC**) and Bitfinex P2WSH (`bc1qgd...`, **157,010.08 BTC**)—score **Grade D (26/100)** due to permanent on-chain public-key exposure, alongside Satoshi's Genesis Block-0 `P2PK` address (`1A1zP1...`, 57.72 BTC, **Grade D, 28/100**). Crucially, a real funded unspent

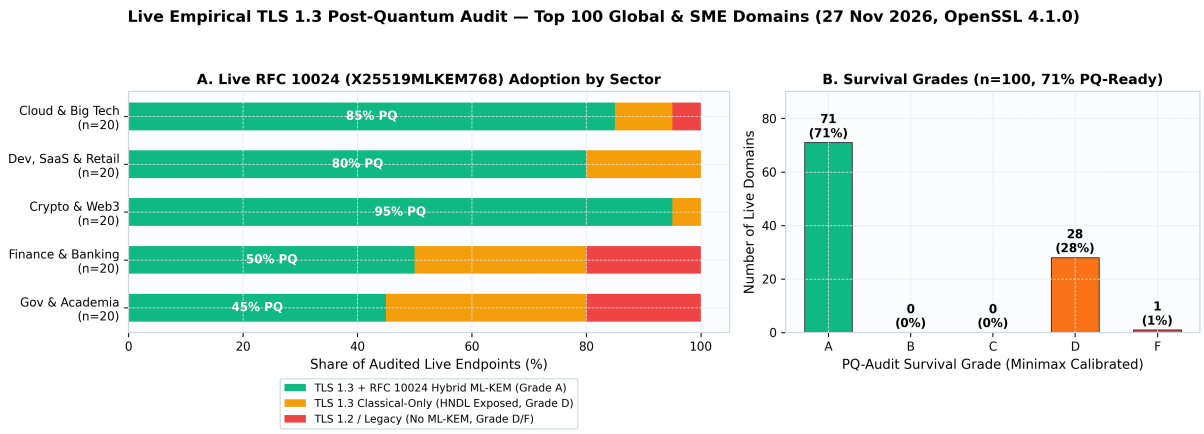


Figure 1: Live OpenSSL 4.1.0 empirical audit of 100 global/SME domains on November 27, 2026: RFC 10024 `X25519MLKEM768` adoption by sector (Panel A) and calibrated survival grade distribution (Panel B).

Taproot address (`bc1prg...`, 1.02 BTC, `spent_txo_count=0`) scores **Grade D (36/100)** due to its exposed tweaked key Q, whereas unspent SegWit `P2WPKH` (`bc1qaz...`, 94,643.49 BTC) and unspent legacy `P2PKH` (`1FeexV...`, 79,957.27 BTC) earn **Grade B (78/100)**.

- **Ethereum (4 wallets):** `vitalik.eth` (`0xd8dA...`, 5.80 ETH) was detected live with 23-byte bytecode starting with `0xef0100`—an **EIP-7702 delegated EOA** [4]—and properly graded **D (32/100)**, preventing the false Grade A emitted by naive `code != 0x` scanners. The Ethereum Beacon Deposit Contract (93.98M ETH) and Foundation Multisig (4,774.55 ETH) score **Grade A (85/100)** as keyless contracts (subject to Theorem 3G authority audit), and an unspent nonce = 0 EOA scores **Grade B (78/100)**.
- **Solana (4 accounts):** Active on-curve `Ed25519` treasuries (9.30M SOL and 66.08 SOL) score **Grade D (34/100)**, whereas an off-curve PDA vault (34.60 SOL) and the executable SPL Token Program score **Grade A (88/100)**.

3.3 Minimax vs. L_p Dilution, Mosca HNDL, and UTXO Sweep Verification

Across **1,000 simulated** $K = 10$ **enterprise stacks** ($\tau = 0.55$, 9 Grade-A RFC 10024 endpoints plus 1 Grade-F legacy endpoint), L_1, L_2, and L_3 compliance averages suffer a **100.0% silent breach bypass rate**, whereas PQ-Audit Minimax (L_∞) achieves **0.0% bypass** (Figure 3). Figure 4 maps the Mosca HNDL urgency contours against NIST 2030/2035 milestones alongside Theorem 4A's assumption-free Fréchet hybrid combiner envelope. Figure 5 confirms Theorems 3B–3D across five UTXO sweep topologies (clean atomic `bc1q`/`bc1z` sweeps drop exposure $3 \to 1$, while Taproot `bc1p`, self-change, and partial sweeps fail at ≥ 3) and quantifies the Gamma mempool confirmation tail ($m = 1$: mean **10.02 min**, p99 **45.54 min** vs. $m = 8$: mean **79.92 min**, p99 **159.57 min**). Figure 6 summarizes PQ-Audit's 8/8 cryptographic assurance coverage relative to existing tools.

4 Conclusion and Open-Source Availability

PQ-Audit bridges formal verification and accessible real-world security: 100% of its mathematical rigor (35 machine-checked Lean 4 theorems, field-general ECDSA low-S algebra, exact RFC 8032 `Ed25519` curve checks, EIP-7702 detection, and RFC 10024 TLS 1.3 ML-KEM probing) runs silently beneath a single read-only search bar at `https://pq.wallstreetdebug.com` and MIT package `pqaudit` (`https://github.com/fabien-pierret/pq-audit`). All source code, Lean 4 proofs, raw JSON datasets, and figure scripts are publicly archived for full reproducibility.

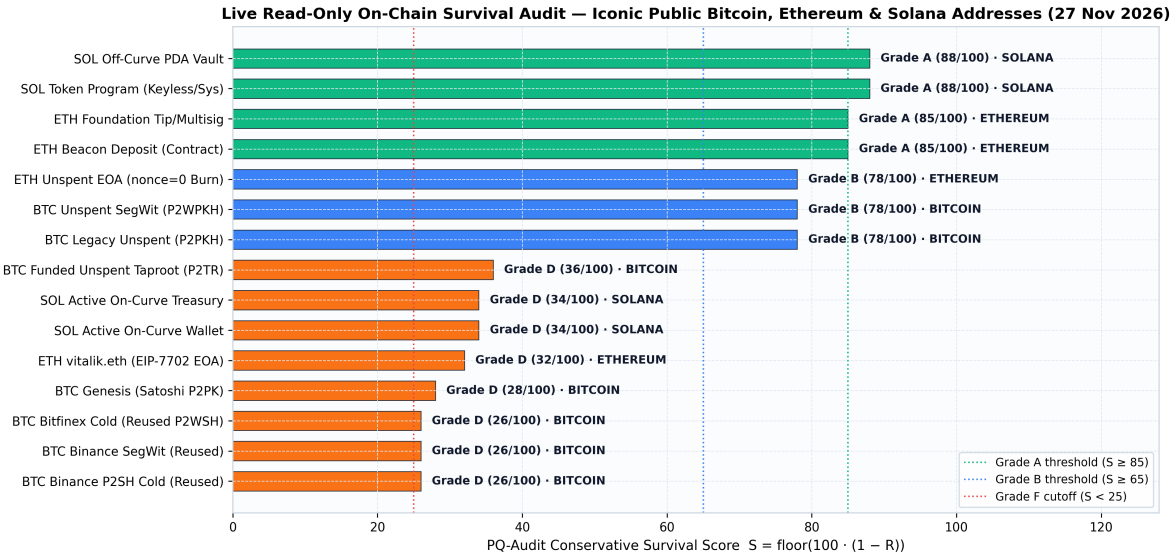


Figure 2: Live read-only on-chain survival audit across 15 public Bitcoin, Ethereum, and Solana addresses (27 Nov 2026), highlighting reused BTC cold wallets, unspent `P2TR` vs `P2WPKH`, and live EIP-7702 detection on `vitalik.eth`.

References

[1] Scott Aaronson. Notes on AI-driven mathematics and cryptanalysis rumors. Shtetl-Optimized Blog, November 2026.

[2] Hunter Beast, Ethan Heilman, and Isabel Foxen Duke. BIP-360: Pay-to-merkle-root (P2MR). Bitcoin Improvement Proposals (Draft merged Feb. 2026), 2026.

[3] Michael Brengel and Christian Rossow. Identifying key leakage of bitcoin users. In *Research in Attacks, Intrusions, and Defenses (RAID)*, pages 623–643, 2018.

[4] Vitalik Buterin, Sam Wilson, Ansgar Dietrichs, and Matt Garnett. EIP-7702: Set EOA account code. Ethereum Improvement Proposals (Pectra Upgrade), 2025.

[5] Simon Josefsson and Ilari Liusvaara. Edwards-curve digital signature algorithm (EdDSA). IETF RFC 8032, January 2017.

[6] Kris Kwiatkowski, Panos Kampanakis, Bas Westerbaan, and Douglas Stebila. Post-quantum traditional (PQ/T) hybrid key agreement mechanisms for TLS 1.3. IETF Standards Track, RFC 10024 (X25519MLKEM768 IANA 0x11EC), August 2026.

[7] Dustin Moody, Ray Perlner, Andrew Regenscheid, Angela Robinson, and David Cooper. Transition to post-quantum cryptography standards. NIST Internal Report NIST IR 8547, National Institute of Standards and Technology, October 2026.

[8] Michele Mosca. Cybersecurity in an era with quantum computers: Will we be ready? *IEEE Security & Privacy*, 16(5):38–41, 2018.

[9] National Institute of Standards and Technology. Module-lattice-based key-encapsulation mechanism standard (ML-KEM). Federal Information Processing Standards Publication FIPS 203, U.S. Department of Commerce, August 2024.

[10] Fabien Pierret. Proof-CI: Necessary and sufficient conditions for formally verified minimax evaluators preventing drift and reward hacking in recursive self-improvement. CERN Zenodo DOI 10.5281/zenodo.24614087; HAL hal-05886244v1, November 2026.

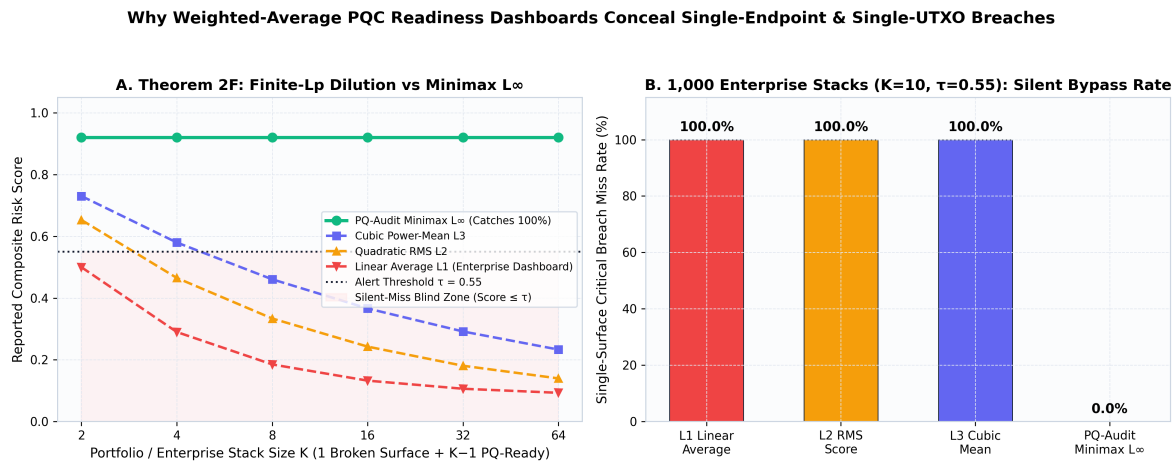


Figure 3: Verification of Theorem 2F: L_1, L_2, and L_3 enterprise dashboards miss 100.0% of single-surface Grade-F breaches across 1,000 $K = 10$ stacks ($\tau = 0.55$), whereas PQ-Audit Minimax L_∞ blocks 100.0%.

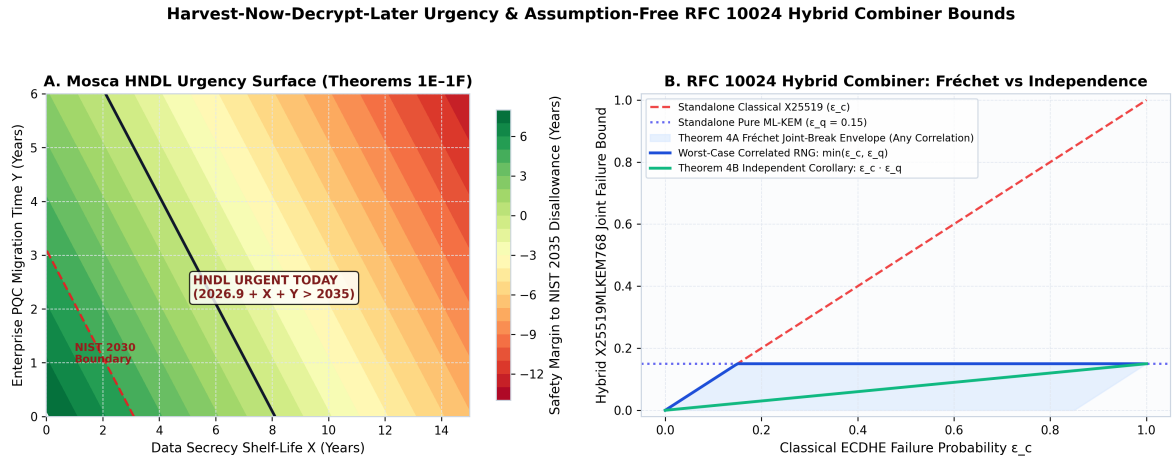


Figure 4: Mosca HNDL urgency surface relative to NIST IR 8547 2030/2035 milestones (Panel A) and Theorem 4A/4B Fréchet hybrid combiner envelope vs. correlated-RNG tightness (Panel B).

[11] Pieter Wuille, Jonas Nick, and Anthony Towns. BIP-341: Taproot: SegWit version 1 spending rules. Bitcoin Improvement Proposals, 2020.

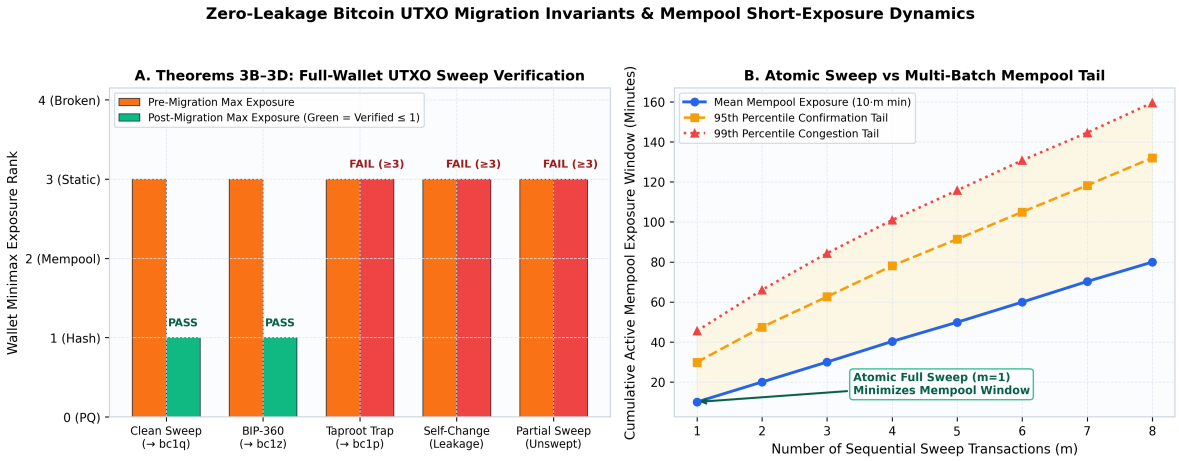


Figure 5: Full-wallet UTXO migration verification across five topologies (Panel A, Theorems 3B–3D) and cumulative Bitcoin mempool short-exposure window for $m = 1 \ldots 8$ sequential sweep batches (Panel B).

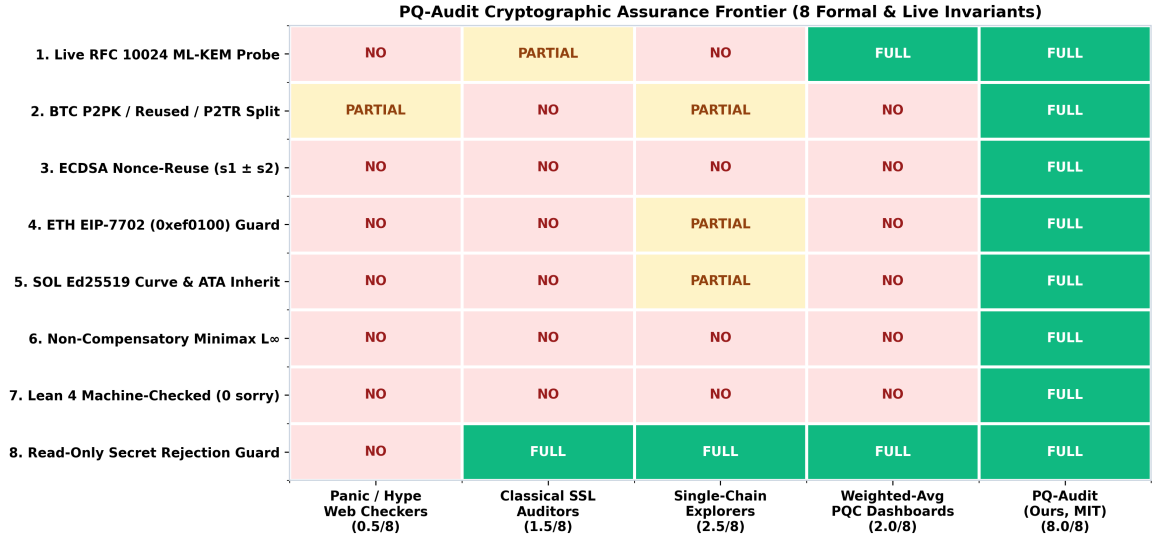


Figure 6: Eight-invariant cryptographic assurance frontier comparing PQ-Audit (8.0/8) against existing panic checkers, classical SSL auditors, single-chain explorers, and weighted-average PQC dashboards.