GtC = ME: Multi-Domain, Energy-Anchored Cryptography with P^3 Visibility for Quantum-Resistant Digital Signatures

Abstract: Quantum computing threatens classical cryptographic systems by efficiently solving the mathematical problems underlying conventional digital signatures. While quantum-resistant schemes offer algebraic protection, they rely solely on mathematical hardness. This paper introduces **GtC = ME**, a multi-domain cryptographic framework that combines **Water (G), Land (t), and Cognition (C) keys** with **energy/matter attestations (E)** and a **P^3 visibility model** (Personal, Private, Public per domain). This layered approach ensures that digital actions are cryptographically secure, physically anchored, and policy-governed. GtC = ME is compatible with existing post-quantum schemes and provides enhanced security, auditability, and flexible governance.

Thesis: 1. Multi-Domain Security – Combining G, t, and C keys prevents single-point compromise. 2. Physical Anchoring (E) – Energy attestations link cryptographic identities to observable reality, adding a layer of protection beyond algebraic hardness. 3. Policy-Controlled Visibility (P^3) – Each domain's data/action can be Personal, Private, or Public, forming a profile that governs access and authorization. 4. Quantum-Resistant Compatibility – The framework can wrap PQ signature schemes for algebraic resilience. 5. Auditability and Governance – Actions and attestations are verifiable and tied to CoI policy, enabling accountability.

Background: The Quantum Threat - Shor's algorithm threatens RSA, ECC, and Diffie-Hellman by solving factoring/discrete log efficiently. - Existing quantum-resistant schemes rely on mathematical hardness alone. - They lack physical anchoring, making them theoretically vulnerable to new classes of attacks or insider compromise.

Conceptual Model: GtC = ME

Domains: - G (Water): Mobility, fluid identity elements. - t (Land): Location, fixed operational elements. - C (Cognition): Intent, policy or human decision-making keys.

Energy Attestation (E): - Real-world measurements (sensor readings, hardware attestations, timestamps, nonces). - Provides a cryptographic anchor tying digital signatures to the physical world.

P^3 Visibility: - Each domain carries a visibility mode: Personal, Private, or Public. - Forms a P^3 profile: {G: P_G, t: P_t, C: P_C} with 27 possible combinations. - Controls who can view or act upon data, respecting ownership and CoI policies.

Operational Mechanism: 1. Domain Key Generation – Each domain generates a keypair; optionally PQ-based. 2. Energy Attestation (E) – Sensors/HSMs issue signed measurements including timestamp, nonce, and metadata. 3. Identity Binding – Combine public keys + E_attest digest into a canonical identifier: GtC_id = Hash(G_pub || t_pub || C_pub || E_anchor). 4. Community Bind Credential – CoI signs GtC_id, P^3 profile, and policy rules. 5. Action Signing – Actions include latest E_attest, GtC_id, and required domain signatures. 6. Verification – Check energy attestation integrity, domain signatures per Bind policy, P^3 visibility rules, thresholds, emergency overrides, and revocation status.

Evidence of Feasibility: - Layered Hardness: Even if domain keys are stolen, E_attest prevents full impersonation. - Compatibility: Can wrap PQ signature schemes like Dilithium or SPHINCS+. - Auditability: Actions are verifiable against CoI policies; logs tie signatures to real-world evidence. - P^3 Enforcement: Visibility rules enforced per-domain; JSON schema provides canonical structure for Binds and Actions.

Example P^3 Profile: { "G": "public", "t": "private", "C": "personal" }

Tested Theses: 1. Multi-Domain Security: Compromise of one domain key does not allow GtC forgery. ✅2. Physical Anchoring: E_attest prevents signature-only attacks. ✅3. P^3 Visibility: Per-domain visibility enforced; item cannot be less restrictive than Bind. ✅4. Quantum-Resistant Compatibility: Works with post-quantum signature schemes. ✅5. Auditability: Full cryptographic and physical evidence trail for verification. ✅

Conclusion: GtC = ME provides a multi-layered cryptographic solution: combines domain-separated keys, energy anchoring, and visibility policy (P^3); wraps existing and future quantum-resistant schemes without altering their mathematical foundation; ensures resilience, auditability, and policy governance; offers a pragmatic path toward long-term, 1,000-year digital identity and signature systems.

Credits: - Author: Joseph A. Sprute (ERES Maestro) - Affiliation: ERES Institute for New Age Cybernetics - Contributors: GPT-5 research assistance, Project PERCMARC, NAC integration frameworks

References: 1. Alallayah, F. S. (2024). A Solution for Constructing Quantum-Resistant Digital Signature Schemes. ResearchGate. https://www.researchgate.net/publication/387699245 2. Shor, P. W. (1994). Algorithms for quantum computation: discrete logarithms and factoring. Proc. 35th Annual Symposium on Foundations of Computer Science. 3. Bernstein, D. J., Buchmann, J., & Dahmen, E. (2009). Post-Quantum Cryptography. Springer. 4. National Institute of Standards and Technology (NIST). (2022). Post-Quantum Cryptography Standardization: Round 3 Report. 5. Sprute, J. A. (2025). ERES Cybernetics: Ethical Substrates for 1,000-Year Governance. ERES Institute Publications.