Reliability-Based Post-Quantum Digital Signature on Multi-Parametric Groups

Khivrenko Hlib Oleksandrovych[1]

[1]*Kharkiv National University of Radio Electronics, 14 Nauky Ave, Kharkiv UA-61166, Ukraine, hlib.khivrenko@nure.ua*

Abstract. *This paper addresses reliability and safety assurance for computer and information systems threatened by future quantum adversaries* [5]. *We outline a digital signature scheme over non-commutative multi-parametric groups (NMPGs) whose hardness relies on simultaneous conjugacy/decomposition problems rather than integer or lattice structures. The design is reliability-first: deterministic signing (to avoid RNG-induced failures), constant-time word-reduction kernels, explicit verification equations with localizable failure, and built-in assurance artifacts (known-answer tests, power-on self-tests, duplication checks, and fault handling aligned with FMEA). Parameter agility enables uplift without key-format churn, supporting long-lived deployments. While complementary to NIST-standardized PQC (and therefore useful for crypto-diversity), the proposal emphasizes engineering properties important in safety-critical contexts: predictable worst-case execution time, side-channel resilience practices, and evidence-friendly testing for certification.*

Keywords: *post-quantum cryptography; non-commutative groups; digital signatures; reliability engineering; safety assurance.*

I. Introduction and Problem statement

Ensuring the reliability and safety of computer and information systems under post-quantum threats requires cryptographic mechanisms with strong security guarantees, operational robustness, and engineering properties that support assurance cases and certification. While NIST-selected lattice and hash-based schemes are maturing, defense-in-depth motivates algorithmic diversity—especially constructions whose security does not reduce to structured lattices or integer factorization.

These theses propose and motivate a digital signature scheme built over non-commutative multi-parametric groups (NMPGs)—families of efficiently computable, finitely generated non-abelian groups controlled by several independent parameters (e.g., rank, relator density/length, automorphism complexity). The underlying hardness relies on simultaneous conjugacy/decomposition problems in these groups. Our objective is not merely cryptographic novelty but a reliability-first design: deterministic signing, clear failure modes, constant-time kernels, testability (KATs), and structured assurance artifacts suitable for safety-critical deployments.

Problem statement: Design a practical, ROM-secure (Random Oracle Model) signature over NMPGs that exposes tunable parameters for security and performance, avoids large-integer arithmetic (favoring constant-time word-reduction), and integrates reliability and safety assurance techniques (threat modeling, FMEA, KATs, side-channel controls) into the construction and its lifecycle.

II. Problem solution and Results

Let G be a non-abelian group with: efficiently solvable word problem and canonical normal form, intractable Simultaneous Conjugacy Search (SCS) and Decomposition/Factorization Search (DS) for appropriately distributed instances, efficient random generation within subgroups with bounded length and relator density. Families such as polycyclic or metabelian semidirect products or carefully parameterized Artin-type groups can be instantiated as NMPGs with parameter vector.

$$\lambda = (\mathrm{n}, \rho, \mathrm{L}, \nu, \sigma),$$

capturing generator count n, relator density ρ, word-length budget L, normal-form reduction complexity ν, and dispersion/entropy controls σ.

Signature construction (Σ-protocol $\rightarrow$ Fiat $-$Shamir)

We adopt a three-move identification protocol over conjugation that yields a non-interactive signature via Fiat–Shamir (Key generation, Sign, Verification):

1. Pick secret $a \in \mathrm{G}$ from distribution D_λ, choose public base tuple $g = (g_1, \dots, g_k)$. Publish $h = (h_i)$ with $h_i = a^{-1} g_i a$. Public key: (g, h), secret key a.
2. For message m, sample ephemeral $\mathrm{r} \leftarrow D_\lambda$ and compute commitment $t_i = r^{-1} g_i \mathrm{r}$. Compute challenge $\mathrm{c} = \mathrm{H}(\mathrm{m}, \mathrm{g}, \mathrm{h}, \mathrm{t})$ in a large domain. Response $s = ra^c$ (group product /exponent is repeated conjuration /power via normal forms). Signature $\sigma = (\mathrm{t}, \mathrm{s})$. Use deterministic $r = KDF(sk, H(m))$ (RFC6979-style) to eliminate RNG faults.
3. Recompute c. Check $s^{-1} g_i s = a^{-c} r^{-1} g_i r a^c = (a^{-1})^c t_i a^c$ which, using public (g, h), is equivalent to verifying the conjugation constraints derived from (t, s, c). All checks use canonical normal forms, failure is explicit and localizable.

In the ROM, existential unforgeability against chosen-message attacks (EUF-CMA) reduces to the hardness of SCS/DS in G under D_λ and collision resistance of H. The non-abelian structure frustrates known quantum speedups (no Shor-style reduction is known for generic conjugacy search in these platforms), providing a complementary hardness assumption to lattice and hash families.

Efficiency and footprint (qualitative)

All operations are on group words; no big-integer arithmetic is required. Complexity is dominated by normal-form reductions $O(\nu * \mathrm{L})$. Public key contains k conjugates, signature contain k commitments plus one response element. With moderate k and bounded L, keys and signatures are kilobyte-scale and amenable to embedded firmware signing

and audit-log protection. Parallelizable reductions and precomputed rewrite tables support predictable latency—crucial for safety-critical systems where bounded worst-case execution time (WCET) matters. Security depends on concrete hardness for the selected G and distributions. A conservative deployment demands up-to-date cryptanalysis, leakage evaluations (TVLA), and side-channel reviews. The ROM proof model does not capture all real-world hash behaviors. We therefore mandate robust hash instantiation and domain separation. Parameter selection must balance footprint and assurance margins.

Reliability Evaluation and Safety Assurance

The adversarial environment presumes a chosen-message forger with quantum capabilities, full visibility of public transcripts, and the ability to induce computation faults and observe physical leakages unless mitigations are enforced. The operational environment must therefore bind the scheme's algebraic soundness to engineering practices that prevent nonce misuse, bound timing behavior, detect transient faults, and reject malformed inputs without undefined states.

III. Conclusions

We present a reliability-oriented digital signature scheme over non-commutative multi-parametric groups that (1) diversifies post-quantum assumptions, (2) integrates deterministic signing, constant-time kernels, KATs, and structured fault handling, and (3) exposes parameter agility for evolving assurance needs. The approach aligns with safety-critical engineering: clear verification equations, explicit failure modes, and evidence-friendly testing. Future work includes tight quantum-resistance analyses for concrete NMPG families, formal proofs beyond ROM, side-channel verification (TVLA), and comprehensive parameter recommendations derived from conservative cryptanalysis. Reliability targets are expressed through parameters and measurements rather than checklists. The parallel Fiat–Shamir construction offers a tunable soundness margin via the number of rounds ℓ with security error $2^{-\ell}$ providing conservative headroom for safety-critical deployments. Deterministic nonce derivation from a keyed PRF tied to $H(m)$ removes dependence on external entropy sources and collapses the probability of catastrophic nonce reuse to zero under standard PRF assumptions; domain separation ensures that signatures bound to distinct contexts cannot be replayed across protocols. To support certifiable timing behavior, the implementation of normal-form reduction $NF(\cdot)$ is written in a constant-time style with length-oblivious control flow, enabling measurement and proof of a worst-case execution time for verification. Fault tolerance is achieved by computing each verification equality under two independent reduction strategies and comparing the resulting normal forms, a mismatch constitutes a detected fault and triggers fail-closed behavior with precise localization to the offending round and coordinate. Known-answer vectors and property-based identities over the chosen group supply continuous self-test evidence, while leakage assessments such as TVLA provide empirical support for constant-time claims. EUF-CMA security is argued through standard Fiat–Shamir extraction over the simultaneous conjugacy platform, side-channel robustness is supported by constant-time coding and empirical leakage testing, and reliability is evidenced by WCET bounds, deterministic nonce generation, explicit failure localization, and comprehensive self-tests.

REFERENCES

[1] A. Fiat, A. Shamir, "How to prove yourself: practical solutions to identification and signature problems" CRYPTO 1986, LNCS.

[2] P.W. Shor, "Algorithms for Quantum Computation: Discrete Logarithms and Factoring" FOCS, 1994.

[3] NIST CSRC, "Selected Algorithms & PQC Status (incl. 2025 HQC selection)", 2025.

[4] Cumplido, M., Kahrobaei, D. & Noce, M. "The Root Extraction Problem in Braid Group-Based Cryptography." La Matematica 3, 1207–1217. https://doi.org/10.1007/s44007-024-00117-x, 2024.

[5] G. H. J. Lanel., "A Survey of Public-key Cryptography over Non-abelian Groups" IJCSNSJ, 2021.