National Research Journal of Information Technology & Information Science
Volume No: 12, Issue No: 2, Year: 2025 (July- December)
PP: 634-648
ISSN: 2350-1278
Peer Reviewed & Refereed Journal (IF: 7.9)
Journal Website www.nrjitis.in

NON-ABELIAN GROUPS AS CRYPTOGRAPHIC FOUNDATIONS: MAPPING MATHEMATICAL HARDNESS TO SECURITY, EFFICIENCY, AND EMERGING COMPUTATIONAL CHALLENGES

Shashikumar R

Associate Professor, Department of Mathematics, Government First Grade College, Yelahanka

ABSTRACT

The search for cryptographic foundations beyond classical number-theoretic assumptions has stimulated sustained interest in non-Abelian groups, where non-commutativity enables computational problems and protocol structures that do not arise naturally in conventional Abelian settings. This paper critically synthesizes the mathematical, cryptographic, computational, and cryptanalytic literature on non-Abelian group-based cryptography and develops an integrative Hardness–Security–Efficiency–Viability (HSEV) framework. Rather than assuming that an algebraically difficult problem automatically constitutes a secure cryptographic primitive, the study distinguishes four progressively stronger requirements: mathematical problem hardness, computational hardness under realistic parameter distributions, cryptographic security under adversarial interaction, and practical viability under implementation constraints. Major problem families—including the conjugacy search, simultaneous conjugacy search, decomposition, subgroup membership, word, root extraction, and semidirect-product-related problems—are examined across braid groups, polycyclic groups, matrix groups, and related noncommutative structures. Historical evidence from braid-group cryptography demonstrates that apparent algebraic complexity can be weakened by length-based, representation-based, structural, and parameter-specific attacks. More recent research on polycyclic groups, semidirect products, and alternative group platforms illustrates both continuing mathematical potential and unresolved security questions. The analysis further situates group-based cryptography within the post-quantum landscape. Although group-based constructions remain an active research direction, current NIST post-quantum standards are founded principally on lattice- and hash-based constructions, indicating that non-Abelian approaches have not yet achieved comparable standardization maturity. The paper argues that future progress requires a shift from identifying nominally hard algebraic problems toward constructing parameterized problem distributions with demonstrable classical and quantum security, efficient representations, formal security reductions, and reproducible benchmarking. The resulting framework provides a structured research agenda for evaluating when non-commutativity constitutes a meaningful cryptographic resource rather than merely additional algebraic complexity.

Keywords: *non-Abelian groups; group-based cryptography; conjugacy search problem; braid groups; polycyclic groups; semidirect products; cryptanalysis; computational hardness; post-quantum cryptography; quantum security.*

1. INTRODUCTION

Public-key cryptography has historically relied on mathematical problems that exhibit a pronounced asymmetry between efficient legitimate computation and infeasible adversarial inversion. Integer factorization, discrete logarithms, and elliptic-curve discrete logarithms are canonical examples. The development of quantum algorithms capable, in principle, of

© Copyright @ Authors

ISSN: 2350-1278
Peer Reviewed & Refereed Journal (IF: 7.9)
Journal Website www.nrjitis.in

undermining major classical public-key assumptions has intensified research into alternative mathematical foundations.

Non-Abelian group theory represents one such direction. Unlike Abelian groups, in which ab = ba, a non-Abelian group admits elements for which:

$$ab \neq ba$$

Although this difference appears elementary, its computational implications can be substantial. Conjugation, centralizers, normal forms, subgroup membership, decomposition and group actions can produce search spaces and computational structures that have no direct counterpart in conventional commutative cryptographic constructions.

Early noncommutative cryptography gained particular visibility through braid-group protocols. The Anshel–Anshel–Goldfeld family and related constructions demonstrated how conjugation and commutators could provide mechanisms for key agreement. Subsequent research expanded the field toward polycyclic groups, matrix groups, graph groups, automaton groups, semidirect products and other algebraic platforms. Fine et al. (2011) characterized these developments as part of a broader research programme in noncommutative algebraic cryptography.

However, the history of this field also exposes a fundamental methodological problem. A mathematical problem may appear difficult in an abstract algebraic formulation but become substantially easier for the particular instances generated by a cryptographic protocol. Shpilrain (2003), for example, emphasized the importance of average-case behaviour and careful platform selection when evaluating conjugacy-based cryptosystems.

The critical distinction is therefore:

Mathematical Hardness ⇏ Cryptographic Security

More appropriately:

Algebraic Structure → Problem Instance → Computational Hardness → Security Assumption → Protocol Security → Implementation Viability

This distinction motivates the present paper. Rather than providing another catalogue of non-Abelian cryptosystems, this study asks a more fundamental question: under what conditions does the mathematical hardness associated with non-Abelian groups translate into demonstrable cryptographic security, acceptable computational efficiency, and resilience against emerging classical and quantum computational threats? The paper develops the Hardness–Security–Efficiency–Viability (HSEV) framework to address this question.

2. OBJECTIVES AND RESEARCH QUESTIONS

The study pursues four objectives:

- RO1: To systematically examine the mathematical structures and computational problems underlying non-Abelian cryptographic constructions.
- RO2: To map the relationship between group-theoretic hardness, cryptographic security and computational efficiency across major non-Abelian platforms.
- RO3: To analyse structural, heuristic, implementation-oriented and emerging computational attacks against non-Abelian cryptographic constructions.
- RO4: To formulate an integrative framework and research agenda for developing practically credible non-Abelian cryptographic systems.

© Copyright @ Authors

ISSN: 2350-1278
Peer Reviewed & Refereed Journal (IF: 7.9)
Journal Website www.nrjitis.in

Correspondingly, the analysis addresses four research questions:

- RQ1. Which properties make particular non-Abelian groups potentially suitable cryptographic platforms?
- RQ2. How reliably does mathematical hardness translate into cryptographic hardness?
- RQ3. What security–efficiency trade-offs characterize major non-Abelian platforms?
- RQ4. What theoretical and empirical requirements must be satisfied before group-based constructions can become credible components of post-quantum cryptography?

3. REVIEW METHOD AND ANALYTICAL ARCHITECTURE

This study adopts a critical integrative review rather than a purely descriptive literature review. Literature concerning noncommutative cryptography, braid groups, conjugacy problems, polycyclic groups, matrix groups, semidirect products, cryptanalysis, computational complexity and post-quantum cryptography was conceptually integrated.

The synthesis was organized around five analytical layers:

- Mathematical structure
- Computational hardness
- Cryptographic construction
- Adversarial security
- Practical efficiency and viability

The review deliberately distinguishes a historical proposal from evidence of contemporary security. This distinction is necessary because several influential non-Abelian constructions subsequently became targets of successful or partially successful cryptanalytic techniques.

The resulting unit of analysis is therefore not merely the group, but the combination:

$$\mathcal{C} = (G, P, D, \Theta, A, I)$$

where G = platform group; P = underlying computational problem; D = distribution of generated problem instances; Θ = parameter configuration; A = adversarial model; I = implementation.

This formulation is important because security is ultimately a property of the complete cryptographic construction, not simply of G.

4. MATHEMATICAL FOUNDATIONS OF NON-ABELIAN CRYPTOGRAPHY

4.1 Groups and Non-Commutativity

A group G consists of a set equipped with a binary operation satisfying closure, associativity, existence of an identity and existence of inverses. An Abelian group additionally satisfies:

$$xy = yx$$

for every x, y ∈ G. A non-Abelian group relaxes this condition. Hence there exist x, y ∈ G such that:

$$xy \neq yx$$

Cryptographically, this creates asymmetric algebraic expressions whose order cannot simply be rearranged. One important operation is conjugation:

© Copyright @ Authors

ISSN: 2350-1278
Peer Reviewed & Refereed Journal (IF: 7.9)
Journal Website www.nrjitis.in

$$y = x^{-1}gx$$

Given g, y, and the knowledge that they are conjugate, recovering an appropriate x constitutes a conjugacy search problem.

5. COMPUTATIONAL PROBLEMS AS CRYPTOGRAPHIC FOUNDATIONS

Non-Abelian cryptography encompasses several related hardness assumptions rather than one universal problem.

Table 1. Principal Computational Problems in Non-Abelian Cryptography

Problem	General formulation	Cryptographic relevance	Principal concern
Word problem	Determine whether two words represent the same group element	Efficient legitimate computation	Must normally be efficiently solvable
Conjugacy decision	Determine whether x and y are conjugate	Structural primitive	Decision hardness alone may be insufficient
Conjugacy search	Recover g satisfying $y = g^{-1}xg$	Key agreement / authentication	Susceptible to structural and heuristic attacks
Simultaneous conjugacy	Recover common conjugator for multiple pairs	AAG-type systems	Multiple samples may leak structure
Decomposition	Find a, b satisfying y = axb	Key establishment	Centralizer information can matter
Subgroup membership	Determine / recover membership representation	Alternative hardness foundation	Representation may change complexity
Root extraction	Find x satisfying x^k = y	Signatures / authentication	Some braid constructions have been attacked
Semidirect discrete-log-like	Recover exponent / action information	Key exchange	Security depends strongly on group / action

Shpilrain and Ushakov proposed key establishment based on the decomposition problem:

$$w_1 = awb$$

with a and b drawn from appropriate subgroups and additional difficulty introduced through hidden subgroup or centralizer information.

The proliferation of such assumptions demonstrates one attraction of noncommutative cryptography: it offers a substantially broader hardness landscape than simply replacing one discrete logarithm group with another. But diversity of assumptions is not equivalent to security.

© Copyright @ Authors

ISSN: 2350-1278
Peer Reviewed & Refereed Journal (IF: 7.9)
Journal Website www.nrjitis.in

6. THE HARDNESS TRANSLATION PROBLEM

The central proposition developed in this review is that cryptographic hardness should be viewed as a translation process.

6.1 Level I: Mathematical Difficulty

At the first level, a problem may lack an efficient general algorithm or may exhibit strong worst-case complexity. This establishes theoretical interest but provides limited cryptographic evidence.

6.2 Level II: Instance Hardness

Cryptographic protocols do not generate arbitrary mathematical instances. They generate instances according to a parameterized probability distribution Dθ. Consequently:

$$H_worst\text{-}case(P) \neq H_cryptographic\text{-}instances(P, D\theta)$$

A problem containing exceptionally difficult instances may nevertheless be insecure if cryptographic key generation disproportionately produces easy ones. This was recognized early in assessments of group-based cryptography, where average-case complexity was identified as critical to meaningful security evaluation.

6.3 Level III: Adversarial Hardness

An attacker is not necessarily required to solve the original mathematical problem exactly. If the intended security assumption is P(x) = y, the adversary's objective may instead be to derive the shared secret, forge a signature or distinguish session keys without recovering x. Therefore:

$$Breaking\ protocol \not\equiv Solving\ underlying\ problem$$

This is one of the most important lessons from historical algebraic cryptanalysis.

6.4 Level IV: Implementation Hardness

Finally, a mathematically secure protocol may leak information through timing, memory access, serialization, non-uniform sampling, parameter generation, canonicalization, and implementation shortcuts. Hence practical security is better expressed as:

$$S = f(G, P, D, \Theta, \Pi, A, I)$$

where Π represents the protocol itself.

7. BRAID GROUPS: FOUNDATIONAL PLATFORM AND CAUTIONARY CASE

Braid groups became one of the most influential early platforms for non-Abelian cryptography. The braid group Bn can be presented through generators $\sigma_1, \sigma_2, \ldots, \sigma_{n-1}$ with relations including:

$$\sigma_i\sigma_j = \sigma_j\sigma_i \quad for\ |i - j| > 1$$

and the braid relation:

$$\sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1}$$

Their infinite, non-Abelian nature, together with algorithmic normal forms and apparently difficult conjugacy-related problems, initially made them attractive cryptographic candidates. Fine et al. identify braid-group constructions as formative developments in noncommutative cryptography.

© Copyright @ Authors

ISSN: 2350-1278
Peer Reviewed & Refereed Journal (IF: 7.9)
Journal Website www.nrjitis.in

However, braid cryptography also became a laboratory for cryptanalysis. Length-based methods attempt to exploit the tendency of candidate conjugators to modify measurable word lengths. Research subsequently demonstrated that such techniques can materially threaten particular braid-based parameter regimes and protocols.

The broader lesson is crucial:

Non-commutativity itself is not a security assumption.

8. ROOT EXTRACTION: A CONTEMPORARY ILLUSTRATION

The root extraction problem asks, given β ∈ Bn and k, to recover an appropriate α:

$$\alpha^k = \beta$$

It appears attractive because exponentiation can be straightforward while inversion may appear difficult. Yet Cumplido, Kahrobaei and Noce's 2024 examination of braid-group root-extraction cryptography concluded that the authentication and signature constructions analysed in their study were generally insecure and provided attacks against the schemes considered.

This provides a near-ideal illustration of the HSEV framework. A problem can possess algebraic interest and apparently difficult search behaviour, yet fail to yield:

a secure protocol construction.

Security analysis must therefore focus not only on solving P, but on every exploitable relationship introduced by the protocol.

9. POLYCYCLIC GROUPS

The limitations observed in early braid-based cryptography motivated investigation of alternative platforms. Eick and Kahrobaei proposed polycyclic groups partly because the word problem could be efficiently handled while conjugacy-related computation could be considerably more difficult.

Polycyclic groups possess several potentially useful characteristics:

- Finite presentations
- Algorithmically manageable normal forms
- Rich subgroup structures
- Non-commutativity
- Potentially complex conjugacy behaviour
- Exponential growth in relevant classes

Gryak and Kahrobaei's survey nevertheless makes clear that cryptanalytic techniques—including length-based and linear-decomposition methods—also need to be considered for these groups. The quantum resistance of relevant infinite polycyclic-group constructions remained an explicit open problem in that literature.

More recent research continues to investigate the complexity of conjugacy variants in polycyclic and matrix groups. A 2026 study, for example, shows that some restricted cases can reduce to computational problems such as discrete logarithms, reinforcing the importance of analysing the exact platform and parameter regime rather than relying on the generic name of the group family.

© Copyright @ Authors

ISSN: 2350-1278
Peer Reviewed & Refereed Journal (IF: 7.9)
Journal Website www.nrjitis.in

10. MATRIX GROUPS

Matrix groups provide another attractive platform because group operations can often be implemented using established computational linear algebra. Potential advantages include:

- Concise representations
- Efficient multiplication
- Established software support
- Controllable dimensions
- Compatibility with finite rings and fields

Grigoriev and Ponomarenko investigated public-key constructions over matrix groups relying on conjugacy and subgroup-membership problems. The same representation that improves implementation efficiency, however, may create cryptanalytic leverage. This produces a recurring tension:

Efficient representation ↔ *Potential structural leakage*

If group operations become matrices over a field or ring, apparently nonlinear group-theoretic relationships may sometimes become susceptible to linear-algebraic methods. Therefore, efficient representation should be treated simultaneously as a performance asset and a security attack surface.

11. SEMIDIRECT-PRODUCT CONSTRUCTIONS

Semidirect products offer another route for building noncommutative key-exchange mechanisms. Kahrobaei and Shpilrain developed a general framework based on extensions of groups or semigroups by automorphisms, with the choice of automorphism and platform affecting both security and efficiency. A semidirect-product construction can be represented schematically as:

$$G \rtimes_{\varphi} S$$

where the action φ introduces nontrivial interaction between components. Habeeb et al. demonstrated how this mechanism could generalize key exchange beyond the conventional commutative Diffie–Hellman structure.

The significance of semidirect products lies less in a single protocol than in their ability to generate families of candidate hardness assumptions through different combinations of groups, semigroups and automorphisms. The security question nevertheless remains unchanged: is recovering the secret information hard for the actual distribution of parameters and against the strongest known structural algorithms?

12. COMPARATIVE MAPPING OF MAJOR PLATFORMS

Table 2. Comparative Characteristics of Non-Abelian Cryptographic Platforms

Platform	Attractive property	Typical hardness basis	Major concern	Research status
Braid groups	Rich conjugacy structure	CSP / MSCP / root extraction	Length / structural / representation attacks	Historically important; construction-dependent
Polycyclic	Efficient normal	CSP / twisted	Linearization and	Active

© Copyright @ Authors

ISSN: 2350-1278
Peer Reviewed & Refereed Journal (IF: 7.9)
Journal Website www.nrjitis.in

groups	forms; complex structure	conjugacy	parameter-specific attacks	research
Matrix groups	Efficient computation	Conjugacy / membership	Linear algebra may expose structure	Platform-dependent
Semidirect products	Flexible group actions	Action / exponent recovery	Choice of automorphism may create weakness	Active research
Graph / related groups	Rich combinatorial structure	Multiple algorithmic problems	Limited maturity	Exploratory
Automaton groups	Complex algorithmic behaviour	Conjugacy / action problems	Implementation and analysis complexity	Exploratory

The table reveals that no single platform currently satisfies all desirable properties automatically.

13. FROM HARDNESS TO SECURITY: THE HSEV FRAMEWORK

The principal theoretical contribution of this review is the Hardness–Security–Efficiency–Viability framework.

Stage 1: Platform Suitability

A platform G should provide: efficient group operations, efficient normal representation, efficient legitimate key generation, large effective key spaces, and hard inverse/search problems.

Stage 2: Distributional Hardness

For security parameter λ, $x \leftarrow D\lambda$ should generate instances that remain difficult for realistic adversaries. This shifts attention from $\max_x T_A(x)$ toward the adversarial performance over cryptographically generated distributions.

Stage 3: Cryptographic Reduction

A mature construction should ideally establish that a successful attack on Π implies a solution to an assumed-hard P, under a clearly defined security model. Without such a reduction, empirical resistance remains useful evidence but does not constitute the same form of assurance.

Stage 4: Efficiency

Let E = (T_K, T_E, T_D, M, C, K_s), where T_K, T_E, T_D denote key-generation, encryption/encapsulation and decryption/decapsulation time; M denotes memory; C communication cost; and K_s key size. A theoretically secure construction with prohibitive E has limited practical viability.

Stage 5: Emerging-Adversary Resilience

Security evaluation must finally consider:

$$A = A_classical \cup A_heuristic \cup A_structural \cup A_quantum \cup A_implementation$$

© Copyright @ Authors

ISSN: 2350-1278
Peer Reviewed & Refereed Journal (IF: 7.9)
Journal Website www.nrjitis.in

Only after traversing these stages should a construction be described as practically promising.

14. SECURITY–EFFICIENCY TRADE-OFF

Security and efficiency are not independent. Increasing parameters may make attacks more expensive but simultaneously increase public-key size, private-key size, multiplication cost, normal-form computation, bandwidth, and storage requirements. The design problem can therefore be expressed as a constrained optimization:

$$\max_{\Theta} S(\Theta) \quad \text{subject to} \quad T(\Theta) \le T_{max},\ M(\Theta) \le M_{max},\ C(\Theta) \le C_{max}$$

The relevant question is consequently not "Is the conjugacy problem hard?" but rather "Does this distribution of conjugacy instances at this parameter level provide the targeted security margin while meeting specified computational and communication constraints?" That is a substantially stronger cryptographic question.

15. CRYPTANALYTIC THREAT TAXONOMY

Table 3. Threats to Non-Abelian Cryptographic Constructions

Attack family	Exploited feature	Consequence
Brute-force search	Insufficient key entropy	Secret recovery
Length-based attack	Correlation between secret operations and word length	Candidate secret reconstruction
Centralizer attack	Structural subgroup information	Reduced search space
Linear decomposition	Linear representation of group action	Algebraic secret / key recovery
Representation attack	Faithful or exploitable mapping	Converts group problem into easier domain
Parameter attack	Weak sampling / short words / special structure	Easy cryptographic instances
Protocol attack	Information leaked by protocol equations	Break without solving assumed problem
Quantum attack	Quantum algorithmic structure	Reduced asymptotic security
Side-channel attack	Implementation leakage	Secret extraction without algebraic solution

The experience of braid-group cryptanalysis demonstrates why this broader attack taxonomy is necessary. The AAGL/Algebraic Eraser family, for example, has been subjected to parameter- and structure-specific cryptanalysis rather than merely generic attacks on the abstract underlying group problem.

16. NON-ABELIAN CRYPTOGRAPHY IN THE QUANTUM ERA

The post-quantum question requires particularly careful terminology. A cryptosystem is not quantum-resistant simply because it avoids integer factorization or conventional discrete logarithms.

Group-based cryptography remains an active post-quantum research direction. Kahrobaei, Flores and Noce survey several group families and identify unresolved questions surrounding their quantum security. A 2024 American Institute of Mathematics workshop was explicitly devoted to rigorous security analysis, quantum analysis and the development of post-quantum group-based primitives. There have also been contemporary constructions, including group-based signature research appearing in PQCrypto proceedings.

© Copyright @ Authors

ISSN: 2350-1278
Peer Reviewed & Refereed Journal (IF: 7.9)
Journal Website www.nrjitis.in

Nevertheless, research activity must be distinguished from standardization maturity. NIST finalized three initial PQC standards in August 2024:

- FIPS 203 — ML-KEM
- FIPS 204 — ML-DSA
- FIPS 205 — SLH-DSA

ML-KEM and ML-DSA are lattice based, while SLH-DSA is hash based. NIST subsequently selected HQC for additional standardization, and its PQC programme remains active.

Thus, as of September 2026, group-based non-Abelian cryptography should be characterized as an active alternative research programme, not as a standardized replacement for the currently deployed PQC portfolio.

17. ARTIFICIAL INTELLIGENCE AND AUTOMATED CRYPTANALYSIS

A further emerging challenge concerns computational search enhanced by machine learning and automated reasoning. Historically, many attacks on group-based systems rely on heuristics:

$$h(x) \rightarrow \textit{estimate of proximity to secret}$$

Machine learning potentially transforms this into:

$$h\theta(x) = \textit{learned estimator from generated attack data}$$

Future AI-assisted cryptanalysis could therefore investigate:

- Learned length functions
- Secret-word prediction
- Adaptive search heuristics
- Reinforcement-learning-guided conjugator search
- Automatic parameter weakness detection
- Neural representations of Cayley graphs
- Automated theorem proving
- Symbolic–neural algebraic search

At present, these possibilities should be treated primarily as a research agenda, not evidence that AI has broken non-Abelian cryptography generally. The more important methodological implication is that empirical hardness evaluations should increasingly assume adaptive adversaries capable of learning from large numbers of generated instances.

18. THE HARDNESS–SECURITY GAP

The synthesis reveals what may be termed the Hardness–Security Gap (HSG). Define conceptual hardness as H_M, observed computational hardness as H_C, and effective cryptographic security as S_C. A naive assumption is:

$$H_M \approx H_C \approx S_C$$

Historical evidence suggests instead that:

$$H_M \geq H_C \geq S_C$$

© Copyright @ Authors

ISSN: 2350-1278
Peer Reviewed & Refereed Journal (IF: 7.9)
Journal Website www.nrjitis.in

can frequently occur because additional structure, instance distributions and protocol leakage create shortcuts. The gap can be conceptualized as:

$$HSG = H_M - S_C$$

Although this expression is conceptual rather than a directly standardized security metric, it highlights a useful design principle:

Good cryptographic design minimizes the gap between claimed mathematical hardness and demonstrable adversarial security.

19. PROPOSED INTEGRATED MODEL

The complete conceptual model derived from the review proceeds through the following stages, in sequence:

1. Non-Abelian algebraic structure
2. Platform selection
3. Hard computational problem
4. Instance distribution
5. Parameterization
6. Cryptographic construction
7. Security analysis (structural, heuristic, quantum, protocol, side-channel) and Efficiency analysis (time, memory, key size, communication) — conducted in parallel
8. Security–efficiency frontier
9. Practical viability
10. Standardization readiness

The framework deliberately places standardization readiness at the end, rather than treating mathematical novelty as evidence of deployment readiness.

20. MAJOR RESEARCH GAPS

The synthesis identifies seven particularly important gaps.

Table 4. Research Gaps and Future Directions

Gap	Existing limitation	Required research
G1: Average-case complexity	Worst-case hardness often dominates discussion	Distribution-specific complexity analysis
G2: Security reductions	Many schemes rely on heuristic assumptions	Formal reductions under established models
G3: Parameter methodology	Parameters often platform-specific	Standardized security-level parameter generation
G4: Quantum complexity	Classical hardness does not establish quantum hardness	Dedicated quantum algorithms and lower-bound research
G5: Benchmarking	Inconsistent performance reporting	Reproducible cross-platform benchmarks

© Copyright @ Authors

ISSN: 2350-1278
Peer Reviewed & Refereed Journal (IF: 7.9)
Journal Website www.nrjitis.in

G6: AI-assisted cryptanalysis	Limited systematic evidence	Learned / adaptive cryptanalytic frameworks
G7: Implementation security	Algebra dominates literature	Constant-time, side-channel and implementation studies

21. RESEARCH AGENDA

21.1 From Problems to Problem Distributions

Future research should stop treating statements such as "the conjugacy search problem is hard" as sufficient security justification. The more meaningful object is (G, P, Dλ, Θ). Hardness should be evaluated across millions of cryptographically generated instances wherever feasible.

21.2 Parameterized Security

Group-based systems need parameter methodologies analogous to mature cryptographic families. Parameters should correspond explicitly to target security levels and quantified attack costs.

21.3 Quantum Cryptanalysis Before Quantum Claims

Every proposed "post-quantum" non-Abelian system should undergo dedicated analysis against:

- Hidden-subgroup-type approaches
- Quantum walks
- Amplitude amplification
- Quantum linear algebra
- Representation-theoretic algorithms
- Hybrid classical–quantum attacks

A recent 2026 proposal based on Mihailova subgroups of braid groups claims resistance to known classical and quantum attacks. Because it is a recent proposal, however, such claims require sustained independent cryptanalysis before being interpreted as mature evidence of security.

21.4 Security–Efficiency Frontiers

Comparative research should report not merely execution speed but the Pareto frontier:

$$\mathcal{P} = \{(S, E) : \nexists\, (S', E') \text{ dominating } (S, E)\}$$

This would enable meaningful comparison with standardized PQC constructions.

21.5 Hybrid Cryptographic Architectures

A realistic near-term direction may involve hybridization rather than replacement. For example:

$$K = KDF(K_{standard\text{-}PQC} \,\|\, K_{group\text{-}based})$$

Such architectures could provide cryptographic diversity, although their security and interoperability must be analysed formally rather than assumed from combining primitives.

© Copyright @ Authors

ISSN: 2350-1278
Peer Reviewed & Refereed Journal (IF: 7.9)
Journal Website www.nrjitis.in

21.6 Open Cryptanalytic Competitions

Group-based proposals would benefit from:

- Open implementations
- Public parameter sets
- Reference vectors
- Attack challenges
- Reproducible benchmark suites
- Independent security evaluation

Cryptanalytic scrutiny should be regarded as part of maturation rather than evidence of failure.

22. DISCUSSION

Three broad conclusions emerge from the literature.

First, non-commutativity is a cryptographic resource but not a security guarantee. It enables conjugation, centralizers, decomposition, complex group actions and richer protocol structures, thereby expanding the mathematical design space.

Second, platform selection is inseparable from security. The abstract complexity of a problem cannot compensate for exploitable representations, weak instance distributions or protocol-specific leakage. The historical evolution of braid cryptography illustrates this especially clearly.

Third, the field should move from hardness-driven cryptography toward evidence-driven cryptography. The traditional development pathway is often:

Interesting group → apparently difficult problem → new protocol

A more mature pathway would be:

Security objective → formal adversarial model → candidate assumption → distributional hardness → security reduction → cryptanalysis → benchmarking → implementation validation

This inversion of priorities may be the most important strategic requirement for the next generation of non-Abelian cryptography.

23. THEORETICAL CONTRIBUTIONS

The paper contributes to the literature in four ways.

First, it integrates mathematical hardness, protocol security and implementation efficiency rather than studying these dimensions separately.

Second, it proposes the HSEV framework, distinguishing mathematical hardness, distributional computational hardness, adversarial security, efficiency and deployment viability.

Third, it conceptualizes the Hardness–Security Gap, explaining why nominal problem complexity can systematically overstate effective cryptographic security.

© Copyright @ Authors

ISSN: 2350-1278
Peer Reviewed & Refereed Journal (IF: 7.9)
Journal Website www.nrjitis.in

Fourth, it develops a forward-looking research architecture incorporating quantum cryptanalysis, AI-assisted cryptanalysis, parameter engineering and reproducible benchmarking.

Collectively, these contributions shift the central research question from "Which non-Abelian problems are difficult?" to "Which parameterized non-Abelian problems remain demonstrably difficult when embedded in efficient cryptographic protocols and exposed to realistic classical, quantum, structural and implementation-level adversaries?"

24. CONCLUSION

Non-Abelian groups constitute a mathematically rich foundation for cryptographic research. Their noncommutative structure supports conjugacy, decomposition, subgroup membership, root extraction, semidirect actions and other computational problems that significantly enlarge the design space available beyond classical commutative cryptography.

Yet the accumulated literature demonstrates that mathematical complexity and cryptographic security are fundamentally different propositions. The experience of braid-group cryptography is particularly instructive. Problems once regarded as promising foundations have encountered length-based, structural, representation-oriented and protocol-specific attacks. Contemporary analyses of braid root-extraction schemes reinforce the lesson that the apparent hardness of an underlying algebraic operation cannot independently establish security.

Polycyclic groups, matrix groups, semidirect products, graph-related structures and other platforms continue to offer important research possibilities. The field remains active in the quantum era, including dedicated research programmes examining group-based post-quantum constructions. However, current standardization provides an important benchmark: NIST's deployed PQC foundations presently center on ML-KEM, ML-DSA and SLH-DSA, while additional algorithms continue through the standardization process.

The future of non-Abelian cryptography therefore depends less on discovering another algebraically difficult problem than on demonstrating that hardness survives instance generation, representation, protocol composition, cryptanalysis, quantum computation, implementation and performance constraints simultaneously.

The governing principle emerging from this study can consequently be expressed as:

Algebraic Hardness + Distributional Hardness + Provable Security + Cryptanalytic Resilience + Computational Efficiency = Cryptographic Viability

Non-Abelian groups should therefore be regarded neither as inherently secure nor as historically exhausted. They represent a high-potential but validation-intensive cryptographic research domain, whose future depends on closing the gap between elegant mathematics and demonstrable security.

REFERENCES

1. Anshel, I., Anshel, M., Fisher, B., & Goldfeld, D. (2001). New key agreement protocols in braid group cryptography. In Topics in cryptology—CT-RSA 2001 (pp. 13–27). Springer. https://doi.org/10.1007/3-540-45353-9_2
2. Cumplido, M., Kahrobaei, D., & Noce, M. (2024). The root extraction problem in braid group-based cryptography. La Matematica, 3, 1207–1217. https://doi.org/10.1007/s44007-024-00117-x

© Copyright @ Authors

ISSN: 2350-1278
Peer Reviewed & Refereed Journal (IF: 7.9)
Journal Website www.nrjitis.in

3. Eick, B., & Kahrobaei, D. (2004). Polycyclic groups: A new platform for cryptology? arXiv.
4. Fine, B., Habeeb, M., Kahrobaei, D., & Rosenberger, G. (2011). Aspects of nonabelian group based cryptography: A survey and open problems. arXiv.
5. Grigoriev, D., & Ponomarenko, I. (2005). Constructions in public-key cryptography over matrix groups. arXiv.
6. Gryak, J., & Kahrobaei, D. (2016). The status of polycyclic group-based cryptography: A survey and open problems. Groups, Complexity, Cryptology, 8(2). https://doi.org/10.1515/gcc-2016-0013
7. Habeeb, M., Kahrobaei, D., Koupparis, C., & Shpilrain, V. (2013). Public key exchange using semidirect product of (semi)groups. arXiv.
8. Kahrobaei, D., Flores, R., & Noce, M. (2022). Group-based cryptography in the quantum era. arXiv.
9. Kahrobaei, D., & Shpilrain, V. (2016). Using semidirect product of (semi)groups in public key cryptography. arXiv.
10. Myasnikov, A. D., & Ushakov, A. (2008). Cryptanalysis of Anshel–Anshel–Goldfeld–Lemieux key agreement protocol. arXiv.
11. National Institute of Standards and Technology. (2024). FIPS 205: Stateless hash-based digital signature standard. https://doi.org/10.6028/NIST.FIPS.205
12. National Institute of Standards and Technology. (2024). NIST releases first 3 finalized post-quantum encryption standards.
13. National Institute of Standards and Technology. (2026). Post-quantum cryptography: Publications.
14. Shpilrain, V. (2003). Assessing security of some group based cryptosystems. arXiv.
15. Shpilrain, V., & Ushakov, A. (2006). A new key exchange protocol based on the decomposition problem. In Algebraic methods in cryptography. American Mathematical Society. https://doi.org/10.1090/conm/418/07954

© Copyright @ Authors