Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 28 (2025), No. 5-B, pp. 2049–2058
DOI : 10.47974/JDMSC-2422

Dihedral group order 12 noncommutative cryptography primitive generations

Gautam Kumar [§]
Department of Artificial Intelligence and Machine Learning
Manipal University Jaipur
Jaipur 303007
Rajasthan
India

Sonu Sharma [†]
Department of Computer Science and Engineering
Poornima University
Jaipur 303905
Rajasthan
India

Vijay Shankar Sharma *
Department of Computer and Communication Engineering
Manipal University Jaipur
Jaipur 303007
Rajasthan
India

Dharm Singh Jat [‡]
Department of Computer Science
Namibia University of Science & Technology
Windhoek 13388
Namibia

Abstract

Noncommutative Cryptography is one of the most interesting application fields for strengthening security concerns and a robust performance approach. The base of the same

[§] *E-mail:* gautam.kumar21ujrb@jaipur.manipal.edu
[†] *E-mail:* sonu.sharma@poornima.edu.in
* *E-mail:* vijayshankar.sharma@jaipur.manipal.edu (Corresponding Author)
[‡] *E-mail:* dsingh@nust.na

works on hidden subfield and hidden subgroup problem (HSP). We proposed cryptological working schemes using dihedral group order 12 approach, in this manuscript. The generation of cryptographic primitives on key exchange directly its monomials generation are having the potential advancement in the field of security achievements. The length-based attacks are advanced compared to its Dihedral Group Order 8, which has worked in part of extra special group.

Subject Classification: *Primary 94A60, Secondary 68M25.*

Keywords: *Cryptography, Noncommutative cryptography, Dihedral order 12, Length based attacks, ECC, Quantum cryptography.*

1. Introduction

Cryptology is a fundamental area in the disciple of computer science, where communication on data and storage data in secure fashion plays a pivotal role. Traditionally cryptology is a combined form of cryptography and cryptanalysis. The considered algorithm in the same acts a central role of its responsiveness. Security services such as authentication, integrity, confidentiality, access control & nonrepudiation are the backbone of the security and in addition to the same these enhance the business processes in respect to the security. The cryptographic schemes are applicable in most of the applications where there is security required and in most of the case there are working in full-fledged appropriateness in the same. But there are still to be many open areas where more arbitrariness and randomness may be possible too, in relation to the enhanced security services, by using the mathematical proofs.

2. Background

The noncommutative cryptographic primitives based on the structure of ring, semi-ring elements and group elements [1]. A quantum algorithm, in support of noncommutative discrete logarithmic problem (DLP) and integer factorization problem (IFP) are proposed by Shor's [2]. An exceptional case of DLP for hidden subfield or hidden subproblem problem is considered in 1996 by Kitaev's depicted in their framework [3]. In 2002, Stinson observed that most of the public-key cryptography coming in commutative, which may not be good enough in forthcoming. Then after, Goldreich and Lee advised other than the commutative generalization need to focus, here onwards a new field of noncommutative came into existence [4][5]. The DLP over hidden-subfield problem for ECC is recommended as harder problem [6][7].

3. Preliminaries

A. *Noncommutative $\mathbb{Z}$ Modular Assumptions*

Cao in 2007 worked on polynomials-based consideration over the noncommutative group, ring and semiring elements, the named structure known by $\mathbb{Z}$-modular structure $\mathbb{Z}$ ®, and further to be applicable on extended version of $\mathbb{Z}^{+}[r]$ *or* $\mathbb{Z}^{-}[r]$ for all integers either for positive or negative value assumptions

are on ring for additive $(R,.,1)$ and multiplicative $(R,+,0)$ as defined in this fashion. The co-efficient for positive and negative are defined as follows:

$(\mathrm{K})\mathrm{r} \cong \underbrace{\mathrm{r}+\cdots+\mathrm{r}}_{\mathrm{k\ times}}$ and $(\mathrm{k})\mathrm{r} \cong \underbrace{(-\mathrm{r})+\cdots+(-\mathrm{r})}_{-\mathrm{k\ times}}$, where as $(\mathrm{k})\mathrm{r}=0$ if $k=0$ is assumed. (1)

Proposition 1: Scalar multiplication in noncommutative is $(\mathrm{a})\mathrm{r} * (\mathrm{b})\mathrm{s} \neq (\mathrm{b})\mathrm{s} * (\mathrm{a})\mathrm{r}$ when, $\mathrm{s} \neq \mathrm{r}$, with coefficient of $\mathrm{f}(\mathrm{x}) = \mathrm{a}_0 + \mathrm{a}_1\mathrm{x} + \cdots \mathrm{a}_\mathrm{n}\mathrm{x}^\mathrm{n} \in \mathrm{Z}^+$, for all x, attained as:

$$\mathrm{f}(\mathrm{r}) = \sum_{\mathrm{i}=0}^{\mathrm{n}} (\mathrm{a}_\mathrm{i})^{\mathrm{r}^\mathrm{i}} = \mathrm{a}_0.1 + \mathrm{a}_1.\mathrm{x} + \cdots + \mathrm{a}_\mathrm{n}.\mathrm{x}^\mathrm{n} \quad (2)$$

B. *Cryptographic Assumptions on noncommutative*

The difficulty level to defend the noncommutative depends to two assumptions:

(i) **Conjugacy Decisional Problem (CDP):** It is a decision problem on group G for two values a and b then determine then find out to exists x for some value in G to obtain as $\mathrm{b} = \mathrm{a}^\mathrm{x}$ or its inverse multiplicative as $\mathrm{b} = \mathrm{x}^{-1}\mathrm{ax}$ to represent a conjugative for group G

(ii) **Conjugacy Search Problem (CSP):** For two values a and b on G group, there is availability x in some group G for $\mathrm{b} = \mathrm{a}^\mathrm{x}$ or its inverse multiplication to exists for $\mathrm{b} = \mathrm{x}^{-1}\mathrm{ax}$.

For the CDP/CSP assumptions do not exist for polynomial based cryptography, where its probabilistic natured polynomial to solve this problem having the special consideration, in this regard.

4. Dihedral Group order 12 Cryptographic Approach

A Dihedral Group of order 12, denoted by D_6 is regular hexagon for a group of symmetries elements. It is constructed using 6 rotations and 6 reflections, in a total of 12 elements. Using the same with mathematical foundation and well formed in algebraic structure are interesting to use in the cryptographic primitives' generations. The same is alternatives offering for ECC and RSA algorithm to use the non-abelian cryptography. For understanding D_6 structure the elements are: $a^0, a^1, a^2, a^3, a^4, a^5, a^6, b, ba, ba^2, ba^3, ba^4, ba^5$, where a is rotation by $60^0$and b is reflection. The same is obtained by the cyclic rotations & its corresponding reflections are the base point to form the cryptographic primitives' generations.

For the understanding purpose, a polygon hexagon structure as certain thickness is considered and placed one of the letter alphabet "F". To form a movement of polygon with 6 phases are visible and noted down its assumptions as in the form of rotations and reflections, Fig. 1 & 2. For illustration revolve it through 60° clock-wise, let's entitle it to 'a'. Now take a reflection and say it 'b'. In case of initial consideration or no movements represented as e.

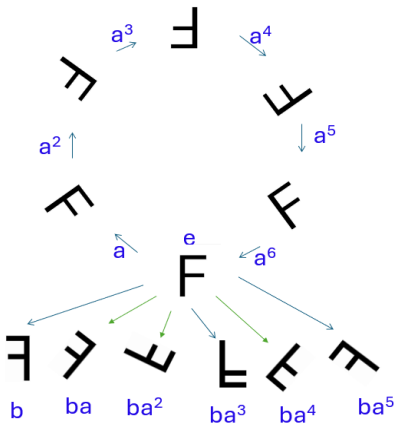

Figure 1
Dihedral Order D_6 Variations Generation

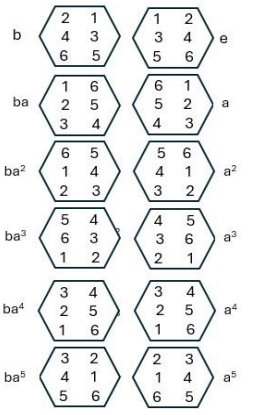

Figure 2
Dihedral Order D_6 mathematical notations

A Cayley table 1 has finite set elements shown with all the applicable permutations represented in table. It is significance in the creation of cryptographic primitives that may be most valuable in constructing a secure and efficient scheme. It supports in algebraic model creation, provides a strong diffusion and confusion, resistance to known attacks and useful in post-quantum cryptosystems generation. The dihedral group order D_6 has shown in Table 2.

Table 1
Cayley Table

		1	2	3	4	5	6	7	8	9	10	11	12
		e	a	a^2	a^3	a^4	a^5	b	ba	ba^2	ba^3	ba^4	ba^5
1	e	e	a	a^2	a^3	a^4	a^5	b	ba	ba^2	ba^3	ba^4	ba^5
2	a	a	a^2	a^3	a^4	a^5	b	ba	ba^2	ba^3	ba^4	ba^5	e
3	a^2	a^2	a^3	a^4	a^5	b	ba	ba^2	ba^3	ba^4	ba^5	e	a
4	a^3	a^3	a^4	a^5	b	ba	ba^2	ba^3	ba^4	ba^5	e	a	a^2
5	a^4	a^4	a^5	b	ba	ba^2	ba^3	ba^4	ba^5	e	a	a^2	a^3
6	a^5	a^5	b	ba	ba^2	ba^3	ba^4	ba^5	e	a	a^2	a^3	a^4
7	b	b	ba	ba^2	ba^3	ba^4	ba^5	e	a	a^2	a^3	a^4	a^5
8	ba	ba	ba^2	ba^3	ba^4	ba^5	e	a	a^2	a^3	a^4	a^5	b
9	ba^2	ba^2	ba^3	ba^4	ba^5	e	a	a^2	a^3	a^4	a^5	b	ba
10	ba^3	ba^3	ba^4	ba^5	e	a	a^2	a^3	a^4	a^5	b	ba	ba^2
11	ba^4	ba^4	ba^5	e	a	a^2	a^3	a^4	a^5	b	ba	ba^2	ba^3
12	ba^5	ba^5	e	a	a^2	a^3	a^4	a^5	b	ba	ba^2	ba^3	ba^4

The idea of the same applied to the composition of twelve different but interrelated operation for D_6.

5. Polynomial Based Non-commutative Cryptographic Approach

Cryptology works in a similar fashion like RSA and ECC, but noncommutative uses the secret key chosen as a polynomial form base, and uses the global parameters as group, ring and semiring elements for cryptographic techniques to apply. This is part of the post-quantum cryptography consideration that provides services against quantum adversaries. The algorithm is presented as follows, in fig 3:

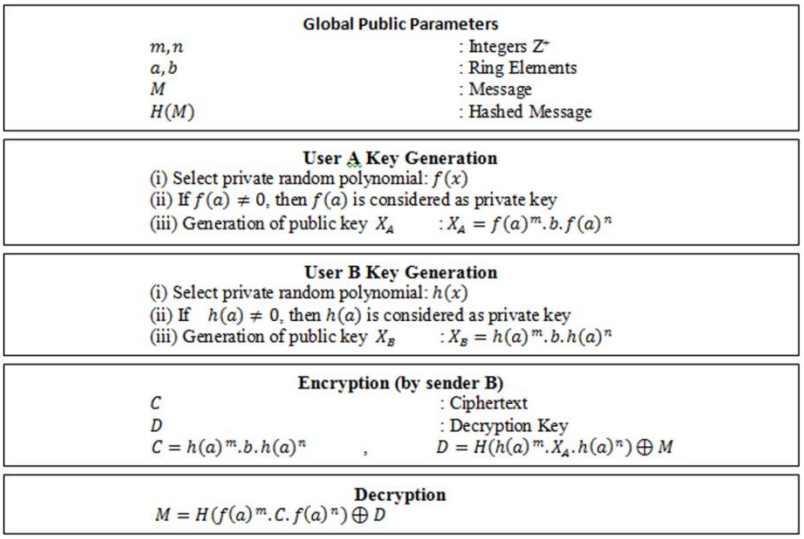

Figure 3
Encryption-Decryption Algorithm on Non-commutative Group and Ring

The above method described is suited for general noncommutative rings. The method below is a generalization of non-commutative group's semi-rings using the similar ways, here from the cryptographic point of view the group elements are used in computation but for the verification purpose semi-ring elements uses [8]. This is known by mono-morphisms problem and/or part of hidden sub-field and hidden subgroup problems.

The definition for a given non-commutative group $(G,.,1_G)$ and elements of rings $(R,+,.,1_R)$, its monomorphism is defined in $\tau(G,.,1_G) \to (R,.,1_R)$. The mapping on τ^{-1}: $\tau(G) \to G$ works well on mono-morphism and for $a,b \in G$, if $\tau(a) + \tau(b) \in \tau(G)$, can assign a new element $c \in G$ as $c \triangleq \tau^{-1}(\tau(a) + \tau(b))$ and its quasi-sum on variables depicted on $c = a \boxplus b$ [31]. In a similar way, for $k \in R$ and $a \in G$, if $k * \tau(a) \in \tau(G)$, then further to new assignment as quasi-multiple a for $d \in G$ as $d \triangleq \tau^{-1}(k.\tau(a)$, denoted by $d = k \boxtimes a$.

The monomorphism τ holds a linear equality as follows: $\tau(k \boxtimes a \boxplus b) = \tau\big((k \boxtimes a) \boxplus b\big)$

Theorem 3: *A variable* $a \in G$ *and for any* $f(x)$ *and* $h(x) \in Z[x]$, *then* $\tau\big(f(a)\big) = f\big(\tau(a)\big)$ *and* $f(a) * h(a) = h(a) * f(a)$, *if* $h(a)$ *and* $f(a)$ *are well work on the same.*

Lemma 1: *The variability generation since* $\{-1, 0, 1\}$ *modulo prime on negative for monomials elements ring.*

Proof: [By inspection]

A. *Key Exchange on Monomials for Non-commutative Algorithm*

The parameters of the algorithm work on monomials for key exchange, available in Fig 4, where the assumptions given are as follows:

$$m = 16, n = 55, a = \begin{pmatrix} 1 & 2 & 3\,4 & 5 & 6 \\ 4 & 1 & 2\,3 & 6 & 5 \end{pmatrix}, b = \begin{pmatrix} 1 & 2 & 3\,4 & 5 & 6 \\ 1 & 4 & 3\,5 & 6 & 2 \end{pmatrix}$$

and $\mathfrak{T} : (\mathrm{G}, ., 1_{\mathrm{G}}) \to (\mathrm{R}, ., 1_{\mathrm{R}})$ in its monomials relative. The assumed group elements from G_1 to G_{12} and for ring elements, for monomials purpose, from R_1 to R_{12}. The assignment for group to ring assigned as $\mathrm{G}_1 \to \mathrm{R}_1, \mathrm{G}_2 \to \mathrm{R}_2, \mathrm{G}_3 \to \mathrm{R}_3, \mathrm{G}_4 \to \mathrm{R}_4, \mathrm{G}_5 \to \mathrm{R}_5, \mathrm{G}_6 \to \mathrm{R}_6, \mathrm{G}_7 \to \mathrm{R}_7, \mathrm{G}_8 \to \mathrm{R}_8, \mathrm{G}_9 \to \mathrm{R}_9, \mathrm{G}_{10} \to \mathrm{R}_{10}, \mathrm{G}_{11} \to \mathrm{R}_{11}, \mathrm{G}_{12} \to \mathrm{R}_{12}$ for computational purposes. We have group and ring elements as follows:

$$G_1 = \begin{pmatrix} 1\,2\,3\,4\,5\,6 \\ 1\,2\,3\,4\,5\,6 \end{pmatrix}, G_2 = \begin{pmatrix} 1\,2\,3\,4\,5\,6 \\ 6\,1\,2\,3\,4\,5 \end{pmatrix}, G_3 = \begin{pmatrix} 1\,2\,3\,4\,5\,6 \\ 5\,6\,1\,2\,3\,4 \end{pmatrix}, G_4 = \begin{pmatrix} 1\,2\,3\,4\,5\,6 \\ 4\,5\,6\,1\,2\,3 \end{pmatrix},$$

$$G_5 = \begin{pmatrix} 1\,2\,3\,4\,5\,6 \\ 3\,4\,5\,6\,1\,2 \end{pmatrix}, G_6 = \begin{pmatrix} 1\,2\,3\,4\,5\,6 \\ 2\,3\,4\,5\,6\,1 \end{pmatrix}, G_7 = \begin{pmatrix} 1\,2\,3\,4\,5\,6 \\ 6\,5\,4\,3\,2\,1 \end{pmatrix}, G_8 = \begin{pmatrix} 1\,2\,3\,4\,5\,6 \\ 5\,4\,3\,2\,1\,6 \end{pmatrix},$$

$$G_9 = \begin{pmatrix} 1\,2\,3\,4\,5\,6 \\ 4\,3\,2\,1\,6\,5 \end{pmatrix}, G_{10} = \begin{pmatrix} 1\,2\,3\,4\,5\,6 \\ 3\,2\,1\,6\,5\,4 \end{pmatrix}, G_{11} = \begin{pmatrix} 1\,2\,3\,4\,5\,6 \\ 2\,1\,6\,5\,4\,3 \end{pmatrix},$$

$$G_{12} = \begin{pmatrix} 1\,2\,3\,4\,5\,6 \\ 1\,6\,5\,4\,3\,2 \end{pmatrix}$$

$$R_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, R_2 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, R_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, R_4 = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix},$$

$$R_5 = \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}, R_6 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, R_7 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, R_8 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$

$$R_9 = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}, R_{10} = \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}, R_{11} = \begin{pmatrix} 1 & -1 \\ -1 & 0 \end{pmatrix}, R_{12} = \begin{pmatrix} -1 & 0 \\ -1 & 0 \end{pmatrix}$$

The random polynomial is chosen for user A as an example, $f(x) = 4x^2 + x + 2$, & on $f(a) \neq 0$, then the sender user A computes as follows: $f(a) = \tau^{-1}\left(f(\tau(a))\right)$

$$= \tau^{-1}\left(4\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}^2 + \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} + 2\right)$$

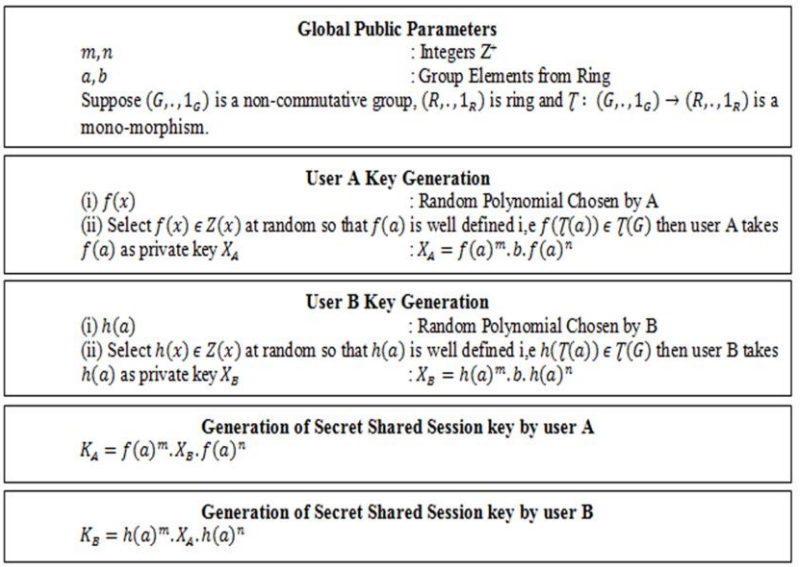

Figure 4
Monomials Key-exchange on Non-commutative Ring

$$= \tau^{-1}\left(\begin{pmatrix} -2 & 3 \\ 1 & -2 \end{pmatrix} mod\ (-2)\right) \qquad [\because \text{Lemma 1}]$$

$$= \tau^{-1}\begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix} \xrightarrow{R_5 \to G_5} G_5 = \begin{pmatrix} 1 & 2 & 3\,4 & 5 & 6 \\ 3 & 4 & 5\,6 & 1 & 2 \end{pmatrix}$$

The generation of public key X_A, and send them to user B:

$$X_A = (f(a)^m * b * f(a)^n)$$

$$= \begin{pmatrix} 1 & 2 & 3\,4 & 5 & 6 \\ 3 & 4 & 5\,6 & 1 & 2 \end{pmatrix}^{16} * \begin{pmatrix} 1 & 2 & 3\,4 & 5 & 6 \\ 1 & 4 & 3\,5 & 6 & 2 \end{pmatrix} * \begin{pmatrix} 1 & 2 & 3\,4 & 5 & 6 \\ 3 & 4 & 5\,6 & 1 & 2 \end{pmatrix}^{55}$$

$$= \begin{pmatrix} 1\,2\,3\,4\,5\,6 \\ 2\,3\,4\,5\,6\,1 \end{pmatrix}$$

Moving further, for the end user B, a polynomial chosen as random as $h(x) = 3x^4 + x^3 + 4x^2 + 3x + 4$ and secret ket computation:

$$h(a) = \tau^{-1}\left(h(\tau(A))\right)$$

$$= \tau^{-1}\left(3\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}^4 + \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}^3 + 4\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}^2 + 3\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} + 4\right)$$

$$= \tau^{-1}\left(\begin{pmatrix} 3 & 6 \\ 2 & 3 \end{pmatrix} mod\ (-2)\right) \qquad [\because \text{Lemma 1}]$$

$= \tau^{-1}\begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix} \xrightarrow{R_7 \to G_7} \begin{pmatrix}1 & 2 & 3\,4 & 5 & 6\\ 6 & 5 & 4\,3 & 2 & 1\end{pmatrix}$ and now for the key exchange user B send the public key to user A and vice-versa as: $X_B = h(a)^m * b * h(a)^n$

$$= \begin{pmatrix}1 & 2 & 3\,4 & 5 & 6\\ 6 & 5 & 4\,3 & 2 & 1\end{pmatrix}^{16} * \begin{pmatrix}1 & 2 & 3\,1 & 2 & 3\\ 1 & 4 & 3\,5 & 6 & 2\end{pmatrix} * \begin{pmatrix}1 & 2 & 3\,4 & 5 & 6\\ 6 & 5 & 4\,3 & 2 & 1\end{pmatrix}^{55}$$

$$= \begin{pmatrix}1\,2\,3\,4\,5\,6\\ 4\,5\,6\,1\,2\,3\end{pmatrix}$$

To extract the session key for user A works as:

$K_A = f(a)^m . X_B . f(a)^n$

$$= \begin{pmatrix}1 & 2 & 3\,4 & 5 & 6\\ 4 & 1 & 2\,3 & 6 & 5\end{pmatrix}^{16} * \begin{pmatrix}1 & 2 & 3\,4 & 5 & 6\,4\\ 4 & 5 & 6\,2 & 1 & 2\,3\end{pmatrix} * \begin{pmatrix}1 & 2 & 3\,4 & 5 & 6\\ 4 & 1 & 2\,3 & 6 & 5\end{pmatrix}^{55}$$

$= \begin{pmatrix}1 & 2 & 3\,4 & 5 & 6\\ 4 & 5 & 6\,1 & 2 & 3\end{pmatrix}$ and in a similar way extract for receiver B user as:

$K_B = h(a)^m * X_A * h(a)^n$

$$= \begin{pmatrix}1 & 2 & 3\,4 & 5 & 6\\ 4 & 1 & 2\,3 & 6 & 5\end{pmatrix}^{16} * \begin{pmatrix}1\,2\,3\,4\,5\,6\\ 2\,3\,4\,5\,6\,1\end{pmatrix} * \begin{pmatrix}1 & 2 & 3\,4 & 5 & 6\\ 4 & 1 & 2\,3 & 6 & 5\end{pmatrix}^{55}$$

$$= \begin{pmatrix}1 & 2 & 3\,4 & 5 & 6\\ 4 & 5 & 6\,1 & 2 & 3\end{pmatrix}$$

6. Comparative Strength Dihendral Order 8 vs. Dihendral Order 12 on Basic Length Based Attacks

Security strength on length-based attacks on noncommutative cryptographic systems is a way to recover the secret conjugators in group length find [9]. The proposed work is in the relation to earlier Dihedral order 8 group, part of extra special group having the significant work. Here is comparative analysis presented between the proposed work of Dihedral order 12 and Dihedral order 8.

Table 2

Comparative Study Dihedral order 8 and 12, with impact of Length Based Attacks

Property	D_4 (Dihedral order 8)	D_6 (Dihedral order 12)	Impact on LBA Resistance
Group Order	8	12	Higher order makes more key space
Number of Elements	8 (4 rotations each by 90^0 + 4 reflections)	12 (6 rotations each by 60^0+ 6 reflections)	D_6 provides more diversity
Group Size and Key Space	8 Elements having the smaller key space compared to 12 Elements having the higher key space	Larger set of elements implies more potential conjugators and targets.	More secure against brute force

Word/Element Diversity	Less non-trivial subgroups and less complex normal form expressions. Less conjugacy classes and less variability in length growth under conjugation.	More non-trivial subgroups and more complex normal form expressions. More conjugacy classes and more variability in length growth under conjugation.	Harder to predict in D_6
Structural Symmetry and Predictability	Highly symmetric with less variation in conjugacy action.	More structural complexity due to higher order of rotation	Higher complexity and less predictable
Empirical Results	Larger and more complex non-abelian groups tend to resist LBAs better. D_6 performs slightly better than D_4 under basic LBAs	Larger and more complex non-abelian groups tend to resist LBAs better. D_6 performs slightly better than D_4 under basic LBAs	Shows better resistance
Conjugacy complexity	Low	Higher	More classes reduce LBA success rate

7. Conclusion

This manuscript is having the idea behind a noncommutative cryptography primitives' generation, based on dihedral group order 12. The security strength and robustness of the proposed work on hidden subgroup or subfield problem (HSP). The cryptographic primitive's generation works on key exchange as well as monomials cryptographic point of view. A comparative study is presented on dihedral order 8 and 12 with hardness to decipher on the length-based attacks.

References

[1] V. V. Anh and K. S. Govindarajan, "On Noncommutative Cryptographic Schemes Using Semigroup Structures," *Journal of Discrete Mathematical Sciences and Cryptography*, Vol. 16, No. 2–3, pp. 145–158 (2013). DOI: 10.1080/09720529.2013.11891245

[2] Peter W. Shor, "Algorithms for Quantum Computation: Discrete logarithms and Factorings," In Proceedings of the 35th Annual Sym-

posium on Foundations of Computer Science, pp. 124-134 (1994), DOI:10.1109/SFCS.1994.365700

[3] Alexei Kitaev, "Quantum Measurements and the Abelian Stabilizer Problem. Electronic Colloquium on Computational Complexity," Vol. 3 (1996), DOI: http://eccc.hpi-web.de/eccc-reports/1996/TR96-003/index.html

[4] John Proos and Christof Zalka, "Shor's Discrete Logarithm Quantum Algorithm for Elliptic Curve," *Quantum Information & Computation,* Vol. 3, pp. 317-344 (2003), DOI: http://dl.acm.org/citation.cfm?id=2011531

[5] P. Vijayakumar and C. Duraisamy, "Quantum Resistant Noncommutative Public Key Cryptography Using Matrix Groups," *Journal of Discrete Mathematical Sciences and Cryptography*, Vol. 21, No. 5, pp. 1095–1110 (2018). DOI: 10.1080/09720529.2018.1492247

[6] Martin Rotteler, "Quantum Algorithm: A Survey of Some Recent Results," Information Forensic Entw., Vol. 21, pp. 3-20 (2006), DOI: http://link.springer.com/content/pdf/10.1007%2Fs00450-006-0008-7.pdf

[7] Iris Anshel, Michael Anshel, and Dorian Goldfeld, "A Linear Time Matrix Key Agreement Protocol over Small Finite Fields," AAECC (2006), DOI: http://link.springer.com/content/pdf/10.1007/s00200-006-0001-1.pdf

[8] Dmitriy N. Moldovyan and Nikolay A. Moldovyan, "A New Hard Problem over Non-commutative Finite Groups for Cryptographic Protocols," Lecture Notes in Computer Science, Springer-Verlag Heidelberg, New York. Vol. 6258, pp. 183-194, Vol. 6258 (2010), DOI: 10.1007/978-3-642-14706-7_14

[9] James Hughes and Allen Tannenbaum, "Length-Based Attacks for Certain Group Based Encryption Rewriting Systems," *Institute for Mathematics and Its Application* (2000), DOI: http://purl.umn.edu/3443

Received November, 2024