An ECC with Probable Secure and Efficient Approach on Noncommutative Cryptography

Gautam Kumar and Hemraj Saini

Abstract An Elliptic Curve Cryptography (ECC) is used on the Noncommutative Cryptographic (NCC) principles. The security and strengths of the manuscript are resilient on these two cryptographic assumptions. The claims on the Noncommutative cryptographic scheme on monomials generated elements is considered be based on hidden subgroup or subfield problems that strengthen this manuscript, where original assumptions are hidden and its equivalents semiring takes part in the computation process. In relation to the same, the research gap is well designed on Dihedral orders of 6 and 8, but our contributions are in security- and length-based attacks enhancement over Dihedral order 12, reported in work done. We modeled the said strategies and represent the ideal security concerns for applications.

Keywords ECC · Noncommutative cryptography · Monomials generations · Length based attacks

1 Introduction

In cryptography, the security algorithm and its measures are playing important role responsiveness, which has been considered as an integral part of computer science. Cryptography is a combined discipline of mathematics, computer science, electrical engineering, and physics. It is one of the foundations that give guaranteed secure communication in the presence of adversaries. Where, the strength and powerful computing techniques are most useful to avoid the threats and supports challenges. A lot of applications are available in the realistic sense for showing the essential requirements that contain to avoid adversaries to occur, the assurance of legitimacy,

G. Kumar (✉)
KL University, Hyderabad 500075, TS, India
e-mail: gautam21ujrb@gmail.com

H. Saini
Jaypee University of Information Technology, Solan 173234, HP, India
e-mail: hemraj1977@yahoo.co.in

L. C. Jain et al. (eds.), *Data Communication and Networks*,
Advances in Intelligent Systems and Computing 1049,
https://doi.org/10.1007/978-981-15-0132-6_1

protection of information from confession, protected message communication systems involved in transmission(s), and storage of information(s). The cryptographic algorithms are shown appropriateness in the full-fledged measurements with the proposed and/or available resources. But instead of the same, from a research point of view, the motivational issues on the algorithms with more impulsiveness and arbitrariness fondness are a guide for future research with an assortment on comparatively more and strong responses. In essence of cryptography, these are termed as private-key and public-key authentication and key exchange.

An immense revolution came through the use of Public-Key Cryptography (PKC), proposed by Diffie and Hellman [1]. The PKC's techniques introduced further in various forms, where on a variety of special features in Elliptic Curve Cryptography (ECC) [2, 3] is attracted the most attention in the area of cryptography. It is well available in the literature to show with marginal enhancement on the lower communication as well as computation costs. ECC provides better security and performance than RSA/DSA algorithms for equivalent security strengths on shorter key sizes [we followed National Institute of Standard and Technology (NIST) guidelines released in 2012]. Today, ECC is considered being tenable above the key length of 224 bits up to the year 2031, corresponding to the same 256 bits key lengths unsusceptible beyond 2031 and above key lengths are not defined but is secure, (Table 1). This table is indicating the RSA algorithm using 2048 and 3072 keyed sized bits for the same security strength for 224-255 and 256-383 varied lengths keyed and its an obvious relative performance advancements indicators.

From research points of view, all PKC's approaches are generalized on commutative-based principles, but some of the researchers were looking into the fact to generalize the cryptographic approach on noncommutative basis, and the given name for the same is noncommutative cryptography or non-Abelion cryptography. It is one of the approaches based on noncommutative nature, where it is mathematically based on random arithmetic operation star (*) (holds on rotation and/or reflection) on any of the noncommutative group G of $(G, *)$, where group G may be any Group elements, Ring elements, Semiring elements, or some algebraic structural elements or its combinations. According to its noncommutative naturalness properties for two elements or combinations of [if considered order be appropriate] a and b operations of G are not resembles the same results, such as $a * b \neq b * a$. It can be achieved on the combined principles from physics and mathematics that are producing the noncommutative natural generalization.

Table 1 Equivalent security for RSA versus ECC

RSA	ECC	Protection from attack
1024	160–223	Until 2010
2048	224–255	Until 2031
3072	256–383	Beyond 2031
7680	384–511	–
15360	512+	–

1.1 Related Work and Associated Issues

Noncommutative cryptographic approach keeps a solid backbone security enrichments and better performances than the existing approaches. Using noncommutative cryptography implementations in a number of applications are based on PKC's approaches such as on RSA/DSA, Diffie–Hellman, and ECC algorithms. For the cryptographic purposes, these are working efficiently in session-key establishment, en/decryption and/or in authentication systems on noncommutative too. The discrete logarithmic is acting as an intermediary strength near to non-negligible solutions. On behalf of the open opinion on security experts, a brief observation is presented here.

For solving a discrete logarithm problem (DLP) and integer factorization problem (IFP), Shor in 1994 [4] is given a competent algorithm on the quantum basis, so likely a representation of possible security breach on commutative-based cryptography. Further, Kitaev [5] considered the same as a special case on its DLP, and analyzed on its significance, called hidden subfield or subgroup problem (HSP). The general ideas from Paeng et al. [6], Joux and Nguyen [7], and Cocks [8] are one of the important steps in making the finite Abelian group's decision separations on cryptographic groups and its equivalents on quadratic residues. Magliveras et al. [9] designed PKC's using one-way functions and trapdoors infinite groups, therefore in 2002, Stinson observed sensibly on most of the PKCs that only belong on Abelian or commutative approach, whose forthcoming future intention may be susceptible in the arena. On behalf of same, Goldreich and Lee suggested don't put all the cryptographic generalizations in single "commutative group" only. Therefore, the reason was a clear indication to look at alternative cryptography for specific purposes; this was the opening of noncommutative cryptography. Noncommutative cryptography is a generalization of a commutative approach in such a way that it doesn't follow the commutative case properties, but those are analogous to be the commutative cases. Afterward, there are session-key establishment, en/decryption, and authentication schemes on noncommutative are generalized on a variety of schemes [10, 11]. HSP over elliptic curve cryptography-DLP (ECC-DLP) is comprehensively resolved by Proos and Zalka [12]. Lee [13] in 2004 organized quantum algorithms well on the random HSP for Noncommutative group elements and it was reporting well, with respect to braid group based attacks [14]. Further, Rotteler [15] suggested to use HSP over noncommutative with proven evidence are much harder and better in the adversaries presence. Cao et al. [16] used polynomials functions to build cryptographic scheme over noncommutative semirings or ring elements. Further, the protocol application was based on non-Abelian given by Kubo [17] on Dihedral order 6, which has been considered the initial order for this group and its construction is based on revolutions of three-dimensional approaches. Reddy et al. [18] build signature schemes over modular method on noncommutative groups and semirings. Moldovyan and Moldovyan [19] constructed the cryptographic implementations on four dimensions; the major intention was to generalize the security enhancement. Myasnikov and Ushakov [20] have the crypt analyzed on encrypted texts and the authentication schemes on the

hardness tests of the Conjugacy search problem on monoids elements. An algorithm is devised to solve the same problems and got anxious on the strategies. Svozil [21] recognized the metaphorical structures with hidden variable indecisiveness on non-contextual elements that can't be figured out on cryptanalysis, and it doesn't any assembled proofs. Kumar and Saini [22] have shown the cryptographic applications on extra special group (ESG) that provides more robustness and unpredictable behavior as compared to all the known schemes using Noncommutative Cryptography on the extra special group (ESG) and applied the same in cryptographic schemes generations. Where the center of ESG is cyclic and its quotient belongs to nontrivial, i.e., the resultants are not equal to zero or identity to its group elements. Transitions from group elements to its equivalent semiring elements finish finitely on monomials (the proposed assumptions for a group and semiring elements are unique and irreversible on the proposed group) and contain all the algorithmic properties. It is designed the authentication and integrity schemes on Mono-morphism for a group and semiring elements on Dihedral Order 8 of ESG. Also, ESG defaults contain the authentication and integrity schemes on Heisenberg and Quaternion groups and finally it is illustrated on the exponential growth on Length Based Attacks and predicted almost to be unpredictable.

1.2 Motivation and Our Contribution

The issue related to security enhancement is one of the most motivational concerns, where monomials with semiring structures and Dihedral orders are presented on potential advantages to keep away the assumptions from various attacks. The monomials structured foundation is, in general, uses the equivalent semiring elements consideration takes part in the computation process, whereas main group parameters work in hidden, and it is based on polynomial modular reductions.

Our contribution highlights the monomials generations on the three dihedral orders of 6, 8, and 12. The Dihedral 6 is already presented so we didn't take into considerations, and Dihedral order 8 monomials generations for key-exchange, encryption–decryption, and authentication schemes presented in [22]. The virtual consideration for Dihedral order 12 is considered in the manuscript. In last, we have presented a scenario for length based attacks in order to investigate into Monomials Cryptographic generation approach.

1.3 Manuscript Organization

The manuscript is organized into subsequent sections, in the next section, it is presented with cryptographic assumptions on modular polynomials and further its hypothesis is presented on group and ring elements, in brief. In Sect. 3, preliminary knowledge of dihedral order 6 and 8 are presented from mathematical points of view

in justification of proposed strategies, which releases the significant contribution our proposed cryptography. In Sect. 4, a length-based attacks scenario is presented on input sequence generation and further presents scenario on attacks by the adversaries in reverse to find the original key. This represents security strength guarantees on enlarged search species.

2 Preliminaries

2.1 Noncommutative Assumptions on $\mathbb{Z}$ Modular Strategies

A PKCs over the Noncommutative cryptography on polynomials with the semiring R elements is proposed by Cao et al. [16], and this scheme is generalized with the name of $\mathbb{Z}$-modular approach. The notation for a $\mathbb{Z}$-modular structure on ring r is $\mathbb{Z}(r)$, and its structural applications available on $\mathbb{Z}^{+}[r]$ for positive elements on noncommutative R and it is as well as applicable on negative $\mathbb{Z}^{-}[r]$, where $r \in R$ is not certain on general and monomials, where group and semiring are comprehensively applicable on $\mathbb{Z}$-modular.

2.2 The Basis of Noncommutative Cryptographic Algorithm

The concerns on security strengths are based on the following two assumptions:

(i) **Conjugacy Decisional Problem (CDP)**: The definition of CDP says on given two group elements a and b of group *G*, using the random secret chosen x to generate the other group elements that satisfies for $b = a^{x}$ or to generate the Conjugacy multiplicative inverse of: $b = x^{-1}ax$. It works in the forward direction.

(ii) **Conjugacy Search Problem (CSP)**: For a group G of elements a and b, that try to finds a secret *x* if there exists x in G such that $b = a^{x}$ or $b = x^{-1}ax$. It is a reverse process to determine the random secret key as *x*.

CSP is considered to be a one-way hash function generation, i.e., the designed algorithm(s) are not able to determine the other group elements values such as $a \rightarrow b^{x}$. In modern cryptography on Noncommutative, generalized assumption is completed enough to frustrate the cryptographers. Also, CSP is well known for its unrealistic nature to solve the same probably on polynomial time.

2.3 Monomials Used in $\mathbb{Z}$ Modular Method

The $\mathbb{Z}$-Modular method is constrained to be monomials on the chosen polynomials on secrets parameters, i.e., original information of group elements are hidden with its equivalents ring/semiring elements on polynomials functions. Such participation Conjugacy assumptions are viewed as a special case. Conjugacy Search Problem is proposed under these considerations.

3 The Preamble to Dihedral Orders

3.1 Dihedral Orders 6

The dihedral is a virtual concept works on a finite set of group elements. After defined operations on it, the group elements show some specific variations that make the unique nature for cryptographic uses. The first initiated step for the noncommutative or non-Abelian group is dihedral order 6, denoted by D_3, given by Uno and Kano in [23]. In which, three colored blocks such as Red, Green, and Blue is considered as an assumption, where three actions applies as "a: swap the first block and second block from left to right, b: swap the second and third block from left to right, e: leave the block as they are, and if two actions then do the operation from right to left as specified". The set of operations works is as follows:

e: RGB $\rightarrow$ RGB or (), a: RGB $\rightarrow$ GRB, b: RGB $\rightarrow$ RBG, ab: RGB $\rightarrow$ BRG, ba: RGB $\rightarrow$ GBR, aba: RGB $\rightarrow$ BGR

Here, the block operations are represented in the form of mathematics, with considerations on R = 1; G = 2; B = 3 and arranged the same in various group elements. Further, equivalent ring elements are assigned to group elements. It shows the center of group element results on a cyclic rotation having its quotient belongs to nontrivial elements, where variables or terms that don't result on the identity or zero elements.

$$\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}\rightarrow\begin{pmatrix}1&0\\0&1\end{pmatrix},\quad\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}\rightarrow\begin{pmatrix}0&1\\1&0\end{pmatrix},\quad\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}\rightarrow\begin{pmatrix}1&1\\1&1\end{pmatrix},$$
$$\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\rightarrow\begin{pmatrix}0&1\\1&1\end{pmatrix},\quad\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}\rightarrow\begin{pmatrix}1&1\\1&0\end{pmatrix},\quad\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}\rightarrow\begin{pmatrix}1&0\\1&1\end{pmatrix}$$

The cryptographic schemes such as key-agreement, encryption–decryption, and its authentication have presented on general and monomials generations in [24], and interested authors can go in detail with this reference.

3.2 Dihedral Order 8

The initial order for Dihedral order 8, denoted by D_4 is available in [25] and the use of this order for the cryptographic purpose is presented in [22]. These consist of the operations on the cyclic subgroup generation by rotations and reflections. For virtualization point of view Dihedral order 8 represented with an on a square of glass with the alphabetic letter "F". In the same, some defined operations have been considered, such as *e* acts as an initial assumption likely be an identity element, *a* is used for a rotation by 90° and *b* is used for reflection. To make use of cryptographic aspects, square movement makes a difference on 0°, 90°, 180°, 270° [clockwise rotations], are taken into its considerations and reflections on the other hand, as shown in Fig. 1.

This virtual concept we apply for numeric consideration for the use of cryptographic purposes. Another way to represent the dihedral order 8 concepts is still possible. The schematic representation is based on the square glass on three operations e, a, b and its corresponding mixed operations, represented in Fig. 2.

Finally, consider these group elements in a group from G_1 to G_8, like e, a, a^2, a^3, b, ba, ba^2, ba^3, which have been used in cryptography for its specific uses such as session-key generation, en/decryption as part of its resultant. A similar idea for the same has assumed for Dihedral 12 on group elements from G_1 to G_{12}, detailed decryption is not available here, but we have considered. Interested authors may refer from Kumar and Saini [22].

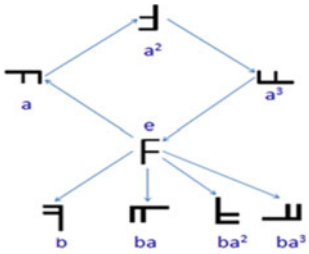

Fig. 1 Symmetries of Dihedral order-8

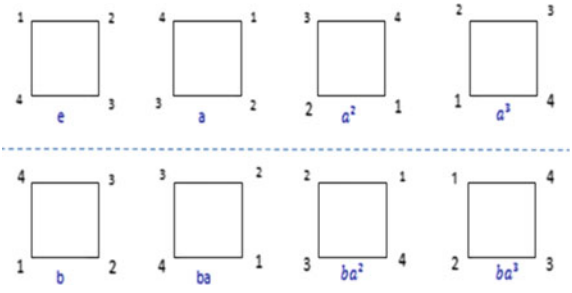

Fig. 2 Schematic representation on Dihedral 8

4 The Investigation into Length Based Attacks and Its Proposal

Length based attacks (LBA) is an approach to determine the user secret key; it works on word lengths, it is related to LBA, in Ruinskiy et al. [26], and in Myasnikov and Ushakov [27]. It is presented on Dihedral order 6 [24]. In these regards, it is one of the reverse procedures that try to recover the factors of conjugates. A good approach results in finding its Conjugator in the form of its group elements generation. The procedure is generating the Conjugators as follows for the Dihedral order of 6, 8, and 12, Fig. 3. On the input sequence and Dihedral order 6, there are 6 group elements and on the successful completion of this task a total of 36 elements to satisfy for the same. Similarly, for Dihedral 8, there are 8 group elements and a total of 64 elements. Finally, for the Dihedral 12 (hexagon element), there are 12 group elements and a total of 144 elements to satisfy for the same.

Our proposed approach is based on complexity enhancement for cryptographers (or complication) on Dihedral order of 6, 8, and 12. The group elements are $S_G = \left\{g_1^{\pm 1}, g_2^{\pm 1}, g_3^{\pm 1}\right\}$ for order 6, $S_G = \left\{g_1^{\pm 1}, g_2^{\pm 1}, g_3^{\pm 1}, g_4^{\pm 1}\right\}$ for order 8 and $S_G = \left\{g_1^{\pm 1}, g_2^{\pm 1}, g_3^{\pm 1}, g_4^{\pm 1}, g_5^{\pm 1}, g_6^{\pm 1}\right\}$ for order 12. The generation of input sequence on input $y = g_1 g_2^{-1} g_3 g_4^{-1}$, for length $n = 4$ for all the three orders as follows. On the assumption of any sequence of chosen input(s), perform operations on likely be on the 2k-ary tree. Where it does starts with an initial assumption word *e*, and generation of any further word/group elements depends on successful proceeding is one of the probable of its child generalized nodes. The successful accomplishment is based on chosen input y_n to length $y = y_1 y_2 \ldots . y_n$ traces likely as presented in Fig. 3. The nth-level contains elements on $(2k)^n$ leaf nodes. The leaf node of each one group is a potential element in any of y. The proposed work is difficult in finding its traces back on its cryptanalysis and/or decomposition of an encrypted message. The supporting group provides an unpredictable and robustness behavior on center and resultants in midair is/are rotates cyclic. Further, the assumptions are unique, irreversible and appropriate in sustaining to algorithmic properties. Therefore, for the proposed orders, it is assumed secure in reference to brute-force search.

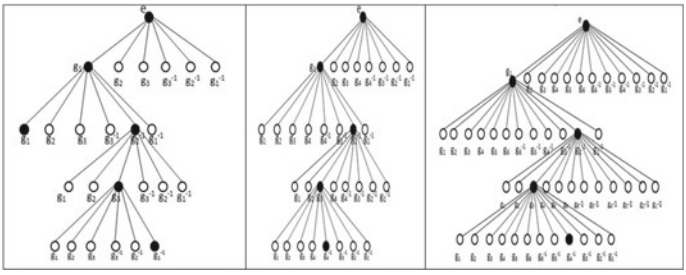

Fig. 3 The process of generating $y = g_1 g_2^{-1} g_3 g_4^{-1}$ on Dihedral 6, 8 and 12

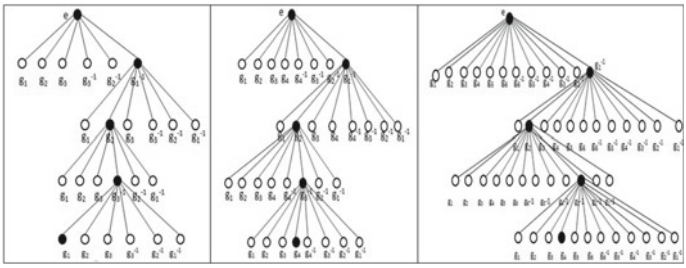

Fig. 4 Decomposition of length $y = g_1 g_2^{-1} g_3 g_4^{-1}$ on Dihedral 6, 8 and 12

Especially, when an attacker(s) tries to determine with equal child nodes, such as *P* and *Q* in same length, then the procedure have been created in such a fashion to fall for the same with insignificant solution. The general observation for Dihedral order 6, six candidates group elements forms at each level, so the time complexity work in the form to attack on the proposed strategy is $O(6^{2n})$ for all n word length, on the success or failure attempts. Next on average, 8 candidates (in Dihedral order 8) elements in each level for one group element, so the time complexity of this strategy is $O(8^{2n})$ for all n word length, on the success or failure attempts. Finally on average, 12 candidates (in Dihedral order 12, denoted by D_6) elements in each level for each group element, the time complexity of the attack algorithm is $O(12^{2n})$ for n length words, either on failure or success proceedings. The attack procedure is considered to be reversed searching the instance on the 2k-ary tree. In reference to shown Fig. 4, the decomposition on any lengths, the dark nodes are considered to be target nodes that forms paths, where this technique is suitable to find the path if it successful works. Therefore, we are able to enhance the robustness properties on its orders and accelerate the unpredictable behavior for cryptographic purposes. Its practical feasibility of the proposed idea is keeping a lot of benefits in noncommutative matrix operations on a finite group. Theoretically, the proposed approach is working; therefore interested authors and/or security agencies may apply this principle in various cryptographic applications, such as mobile techniques, online services, cloud in security, Internet of Things (IOT).

5 Conclusion and Future Scope

Due to tremendous demands on secured tools and techniques for various applications, our considered approach is one of the prime research concerns. The manuscript claims the Noncommutative cryptographic scheme on monomials generated elements. The monomials working principles are acting on Dihedral order of 6, 8, and 12. In regards to security and performance, these are reporting an immense contribution in the field of cryptography and making the proposal stronger based on the hidden subgroup

or subfields problem. For the adversary, the attacks like length based, cryptanalysis, and brute-force are likely being negligible to find.

As the proposed approach itself is a representation of polynomial functions that doesn't reveal secrets and/or finding polynomial for attacker is hard to find. The deployment considerations for applications are on high demand, designing for accelerating the algorithms, also in the area of security, is in tremendous demands.

References

1. W. Diffie, M.E. Hellman, New directions in cryptography. IEEE Trans. Inf. Theory **22**, 644–654 (1976). https://doi.org/10.1109/TIT.1976.1055638
2. V.S. Miller, Use of elliptic curves in cryptography. Adv. Cryptol. **218**, 417–426 (1986), dl.acm.org/citation.cfm?id=704566
3. N. Koblitz, Elliptic curve cryptosystems. Math Comput. **48**, 203–209 (1987). https://doi.org/10.1090/S0025-5718-1987-0866109-5
4. P.W. Shor, Algorithms for quantum computation: discrete logarithms and factorings, in *Proceedings of the 35th Annual Symposium on Foundations of Computer Science* (1994), pp. 124–134. https://doi.org/10.1109/sfcs.1994.365700
5. A. Kitaev, Quantum measurements and the Abelian stabilizer problem, in *Electronic Colloquium on Computational Complexity* (1996), http://eccc.hpi-web.de/eccc-reports/1996/TR96-003/index.html
6. S.H. Paeng, K.C. Ha, J.H. Kim, S. Chee, C. Park, New public key cryptosystem using finite non abelian groups. Lect. Notes Comput. Sci. **2139**, 470–485 (2001)
7. A. Joux, K. Nguyen, Separating decision Diffie-Hellman from Diffie-Hellman in cryptographic groups. Cryptology ePrint Archive, Report 2001/003 (2001), http://eprint.iacr.org/
8. C. Cocks, An identity based encryption scheme based on quadratic residues. Lect. Notes Comput. Sci. **2260**, 360–363 (2001)
9. S.S. Magliveras, D.R. Stinson, T.V. Trung, New approaches to designing public key cryptosystems using one-way functions and trapdoors in finite groups. J. Cryptol. **15**(4), 285–297 (2002)
10. K.H. Ko, D.H. Choi, M.S. Cho, J.W. Lee, New signature scheme using conjugacy problem. IACR Cryptology ePrint Archive 2002:168 (2002)
11. D. Grigoriev, I.V. Ponomarenko, On non-abelian homomorphic public-key cryptosystems. J. Math. Sci. (2002), cs.CR/0207079, arXiv:cs/0207079
12. J. Proos, C. Zalka, Shor's discrete logarithm quantum algorithm for elliptic curve. Quantum Inf. Comput. **3**, 317–344 (2003), http://dl.acm.org/citation.cfm?id=2011531
13. E. Lee, Braid groups in cryptology. ICICE Trans. Fundam. E**87**-A(5), 986–992 (2004)
14. D. Grigoriev, I. Ponomarenko, Constructions in public-key cryptography over matrix groups (2005), CoRR, abs/math/0506180, arXiv:math/0506180
15. M. Rotteler, Quantum algorithm: a survey of some recent results. Inf. Forensic Entw. **21**, 3–20 (2006), http://link.springer.com/content/pdf/10.1007%2Fs00450-006-0008-7.pdf
16. Z. Cao, X. Dong, L. Wang, New public key cryptosystems using polynomials over noncommutative rings. Int. J. Cryptol. Res. **9**, 1–35 (2007), https://eprint.iacr.org/2007/009.pdf
17. J. Kubo, The dihedral group as a family group, in *Quantum Field Theory and Beyond*, ed. by W. Zimmermann, E. Seiler, K. Sibold (World Science Publication, Hackensack, NJ, 2008), pp. 46–63, http://www.worldscientific.com/worldscibooks/10.1142/6963
18. P.V. Reddy, G.S.G.N. Anjaneyulu, D.V.R. Reddy, M. Padmavathamma, New digital signature scheme using polynomials over noncommutative groups. Int. J. Comput. Sci. Netw. Secur. **8**, 245–250 (2008), http://paper.ijcsns.org/07_book/200801/20080135.pdf

19. D.N. Moldovyan, N.A. Moldovyan, A new hard problem over noncommutative finite groups for cryptographic protocols, in *Lecture Notes in Computer Science*, vol. 6258 (Springer, Heidelberg, New York, 2010), pp. 183–194
20. A.D. Myasnikov, A. Ushakov, Cryptanalysis of matrix conjugation schemes. J. Math. Cryptol. **8**, 95–114 (2014). https://doi.org/10.1515/jmc-2012-0033
21. K. Svozil, Non-contextual chocolate balls versus value indefinite quantum cryptography. Theoret. Comput. Sci. **560**, 82–90 (2014)
22. G. Kumar, H. Saini, Novel noncommutative cryptography scheme using extra special group. Secur. Commun. Netw. **2017**, 1–21 (2017)
23. M. Uno, M. Kano, Visual cryptography schemes with dihedral group access structure, in *Proceedings of ISPEC'07* (Springer, 2007), pp. 344–359, http://dl.acm.org/citation.cfm?id=1759542
24. Z. Cao, New Directions of modern cryptography, in *Noncommutative Cryptography* (CRC Press, 2013)
25. B.C. Hall, *Lie Groups, Lie Algebras, and Representations: An Elementary Introduction* (Springer, New York, 2003), http://link.springer.com/book/10.1007%2F978-0-387-21554-9
26. D. Ruinskiy, A. Shamir, B. Tsaban, Length-based cryptanalysis: the case of Thompson's group. J. Math. Cryptol. **1**, 359–372 (2007). https://doi.org/10.1515/jmc.2007.018
27. A.D. Myasnikov, A. Ushakov, Length based attack and braid groups: cryptanalysis of Anshel-Anshel-Goldfeld key exchange protocol, in *Lecture Notes in Computer Science*, vol. 4450 (Springer, Heidelberg, 2007), http://link.springer.com/chapter/10.1007%2F978-3-540-71677-8_6