Journal of Data Acquisition and Processing
ISSN:1004-9037
https://sjcjycl.cn/
DOI: 10.5281/zenodo.777432

NONCOMMUTATIVE CRYPTOGRAPHY PRIMITIVES IN ALGEBRAIC STRUCTURES

C. Senthilnathan[1] and S. Karunanithi[2]1,2
P G & Research Department of Mathematics, Government Thirumagal Mills College, Tamil Nadu , India.
E-Mail: duriselvan@gmail.com[1], kap232008@gmail.com[2]

Abstract: This paper provides the concepts of non-commutative group embedded with cryptography, a true area, fascinate with advanced high end performance and security. The basis of this non-commutative group is recognized on the hidden subgroup computational problem. The main focal point in this paper is to ascertain the cryptographic schemes on the additional sub group (ASG). ASG is screening the suitable non-commutative platforms for the solution of cryptographic problems. The computational methodology is based on the random polynomials chosen by the communicating to the particular person through secured key exchange, encryption-decryption and authentication schemes. This group supports Diffie-Hellman algorithm (with hash function) to encrypt and decrypt.

Key Words: Non-commutative group, cryptography, Diffie-Hellman algorithm, semi ring, semi group.

1. Introduction

Cryptography, a discipline of computing, as well as the modeling, algorithms and security components and these components acts as a primary tool. This cryptography application contains the promise of legitimacy, the protection of information and therefore the system of communication protected messages for the essential wants. To reinforce security, scientific discipline schemes play a significant role in security responsiveness for several relevant applications round the world.

Absolutely the live scientific approaches shows an ideal work and the fondness of serenities with applied mathematics which motivates to proceed further. The Since then, various patterns and styles of PKC algorithms are projected and applied, wherever secured

data transformation is possible. This PKC is taken into account and the researchers are trying to find different schemes for encryption and decryption by grouping all security protocols into various groups and subgroups. Peter's et al [14], projected the discrete logarithm problem (DLP) and integer factorization problem (IFP) along with Diffie-Hellman crypt analysis. A framework by Kitaev et al in 1996 [9] analyzed a special case in DLP, referred to the hidden subgroup problem. Stinson et al determined, in 2002, about the foremost PKC to independent or commutative group, whose intention is the crypt keys are belonging to various groups. In line with the cryptographers themselves, to place scientific discipline protocols in one group and then create an appropriate subgroup. The rationale was cleared to introduce a replacement space of cryptography; this was completely depends on non-commutative cryptography [6] and the standard pattern for non-commutative cryptography are developed for numerous issues.

The structure of non-commutative cryptography relied on braid-based cryptography for protocol generalizations. Numerous different structures related to matrix groups, ring elements were later projected. The primitive methods and scientific discipline systems of non-commutative cryptography are supported algebraical structures of group, ring, semi-ring elements and so on. However these groups of matrix elements showed potential and optimal changes. In addition, the implementation in recent applications utilizes public key scientific crypt schemes in Diffie-Hellaman, RSA, and various cryptography algorithms which rely on number theory. They solve numerous issues like private and public key authentication schemes.

The basis of non-commutative cryptography relies on the operation * on the non-commutative group G of $(G,*)$ consisting of a group or a ring or a two-dimensional image or bounded algebraical structural elements [7]. The operations of two elements say a and b of G specified $a * b \neq b * a$ are acknowledged by non-commutative or non-abelian group [3, 4].

This paper is organized as follows. Section II deals with fundamentals of non-communicative cryptography related to ring and group. Few assumptions are made according to the secured data transfer. In section III, Non-commutative monomials and the original information (message) of the group and its elements are hide along with their ring or semi-ring elements, and these kinds of computations are considered as a special case. Section IV deals with the Diffie-Hellman key algorithmic process for the Non-commutative

Group G, along with Monomials with Non-commutative Basis - Encryption-Decryption Rule Algorithm. Finally section V concludes the paper.

II Preliminaries

Non-commutative discipline approaches the features of a robust situation as well as chaotic situation in the security enhancements. N. R. Wagner et al, in 1985 [16] projected chaotic problems on semi group elements for public key cryptography (PKC). However J.C. Birget et al [2] detected a method which projects the consequences of the PKC. Braid-based cryptography (compact key) was projected by I. Anshel et al. [1]. The premise was faced complexity in computing algebraic structures, and they used compact key as a platform for PKC. Later on, K.H. Ko et al in 2000 [10] extended the braid-based cryptography. Moreover, the domain into consideration successfully implemented by P. Dehornoy et al in 2004 [5]. In 2001, S.H. Paeng et al [13] also proceed with a new PKC based on non-abelian finite groups. His method on applying DLP in the group of inner automorphism involves the realization of conjugation. In the meantime, the growth of finite fields was notable within the pure mathematics according to S.S. Magliveras et al [11]. Later, few authors confirmed an honest generality on factorization of convincing homomorphic cryptosystem; these were originally created for non-abelian group. Grigoriev et al [8] comprehensively solved the membership issues on matrices.

Arithmetic key exchange is illustrated by B . Eick et al in 2004 [6] and they propose an innovative cryptosystem on polycyclic groups. A group G is named a polycyclic series with cyclic aspects; in different words, $G_i \,/\, G_{i+1}$ is recurring for $i = 1, \dots, n$. V. Shpilrain et al in 2005 [15] were come out with Thompson's group may be a sensible proposal to make to build PKC. In 2005, A. Mahalanobis [12] did not discriminate the Diffie-Hellman key exchange protocol from a cyclic group to a non-abelian group. Further he focused the nil potent group and the quotient $H_i \,/\, H_{i+1}$ fall in the middle of H_i / H_{i+1} .

In general public key cryptography on the scalar multiplication of polynomials on the non-commutative ring R was bringing out enormous applications for example few applied mathematicians are developed a theme and is working on modulo prime integers. The derived Z modular structure over the ring is $Z(r)$ is applied into positive $Z^{+}[r]$ and / or negative $Z^{-}[r]$ on the non-commutative ring, where r ∈ R.

The integral constant polynomial in non-commutative additive characterization in ring is defined as $(R, +, 0)$ and for multiplicative non-commutative is defined as $(R, \cdot, 1)$ and the scalar multiplication on R is k $\in Z^+$ and $r \in R$:

$$(k)r \cong r + \cdots + r_{\ k\ times}. \tag{1}$$

Further, for $k \in Z^-$ we have,

$$(k)r \cong (-r) + \cdots + (-r)_{\ -k\ times}. \tag{2}$$

For scalar $k = 0$, and probably $(k)r = 0$.

Proposition 2.1: Scalar multiplication of the non-commutative property follows

$(a)r \cdot (b)s \neq (b)s \cdot (a)r$, when $r \neq s$.

Consider the polynomial $f(x) = a_0 + a_1x + \cdots + a_nx^n \in Z^+$, for all x and r □ R, then

$$f(r) = \sum_{i=0}^{n} (a_i)^{r^i} = a_0 \cdot 1 + a_1 \cdot x + \cdots + a_n \cdot x^n \tag{3}$$

Suppose that r is indeterminate; then the polynomial over $f(r)$ may be a univariable polynomial found in R. The univariable polynomial over R is denoted by $Z^+[r]$, then $f(r)$ is defined as follows:

$$f(r) = \sum_{i=0}^{n} (a)_i^{\ r^i}$$

$$h(r) = \sum_{j=0}^{m} (b)_j^{\ r^j} \tag{4}$$

Again, if $n \geq m$, then

$$\sum_{i=0}^{n} (a_i)^{r^i} + \sum_{j=0}^{m} \left(b_j\right)^{r^j} = \sum_{i=0}^{m} (a_i + b_i)^{r^i} + \sum_{i=m+1}^{n} (a_i)^{r^i} \tag{5}$$

by applying distributive law we get,

$$\sum_{i=0}^{n} (a_i)^{r^i} + \sum_{j=0}^{m} \left(b_j\right)^{r^j} = \sum_{i=0}^{n+m} (p_i)^{r^j} \tag{6}$$

where,

$$p_i = \sum_{j=0}^{i} \left(a_i b_{i-j}\right)^{r^j} = \sum_{j+k=i} \left(a_j\right)(b_k) \tag{7}$$

Theorem 2.2: If $f(r) \cdot h(r) = h(r) \cdot f(r)$, for every $f(r)$ and $h(r) \in Z^{+}[r]$.

Proof: Here, the ring r may be a set of the ring R that applies to the polynomial functions of $f(r)$ and $h(r)$, for any $Z^{+}[r]$. This ring is additionally satisfies the following properties:

(i) Closure : if a and b belong to the ring, then ab is also in ring.

(ii) Associative law : $a(bc) = (ab)c$ for all a, b, c.

(iii) Distributive laws: $a(b + c) = ab + ac \; or \; (a + b)c = ac + bc$ for all a, b, c.

(iv) Commutative multiplication: $ab = ba$ for all a, b.

(v) Multiplicative identity: $a \cdot 1 = 1 \cdot a = a$ for all a.

Based on these properties, the proof of the proposition is obvious by (i), (iii) and (iv).

Cryptographic Assumptions

The following assumptions are made according to the secured data transfer:

(A_1) Consider the two group of elements a and b, to compute a random, such that $b = a^x$ and to provide a similar conjugacy multiplicative inverse as $b = x^{-1}ax$.

(A_2) Consider the two group of elements a and b, to compute an element x in G, such that $b = a^x$ and to provide a similar conjugacy multiplicative inverse as $b = x^{-1}ax$.

In (A_2), when we apply x on one group of elements then the output becomes $a \rightarrow b^x$, a one way operation function, i.e. inverse or reversible is obviously not possible. But (A_1) accepts the elements of any group, ring or semi-ring part in multi way operation function, i.e. inverse or reversible is also possible.

III Non-commutative monomials

The polynomials in the Z modular methods are restricted to call monomials. Further the original information (message) of the group and its elements are hide along with their ring or semi-ring elements, and these kinds of computation needs to be considered as a special case. These kinds of elements are processed through Diffie-Helamn algorithm, RSA

algorithm and so on. In addition to this public-key coding schemes are applied into secured data transfer.

Let $(G, \cdot, 1)$ be a non-commutative monomial for an element $a \in G$, the other group element being $b \in G$, such that $a \cdot b = b \cdot a$; then the group a is assumed to be invertible and not all elements of G are invertible. If the inverse of a exists then it will be unique and is denoted as a^{-1}. The positive power of a is defined as follows: $a^n = a + \cdots + a_{\ n\ times}$ for n > 1. If b is that the inverse of a, then $a^{-1} = b + \cdots + b_{\ n\ times}$ for n > 1. According to the assumption (A_2) this can be extended into monomials G, as $\forall a \in G$ and $\forall x \in G^{-1}, xax^{-1}$ may be a conjugate of a, and x is called the conjugator of (a, xax^{-1}).

Definition 3.1 (Conjugation Search problem (CSP)): Let G be a non-commutative monomial; and the elements $a, b \in G$ so that $b = xax^{-1}$ and for any unknown element $x \in G^{-1}$.

Definition 3.2 : Suppose S may be a non-empty set, $F : S \times S \to S$ may be a well-defined function, and denote $F(a, b)$ by $F_a(b)$. If $F_r(F_s(p)) = F_{F_{r(s)}}(F_r(p))$, where $p, r, s \in S$, then $F \cdot (\cdot)$ be known as a left self-distributive system.

Theorem 3.3: Let G be a non-commutative monomial, the function F in the conjugate follows as $F : G^{-1} \times G \to G, (a, b) \to aba^{-1}$ and is a left self-distributive system.

Proof: By Definition 3.2, according to left self-distributive system, if $F_r(s)$ is written like r □ s; then $r * (s * p) = (r * s) * (r * p)$, wherever "□" remains left self-distributive. The proof of those observations follows from left to right as follows:

$$F_r(F_s(p)) = F_r(s * p) = r * (s * p) = (r * s) * (r * p) = F_r(s) * F_r(p) = F_{F_r(s)}(F_r(p)).$$

Here you satisfy the operate F on $F_r(F_s(p)) = F_{F_r(s)}(F_r(p))$ as a left self-distributive system. Therefore, the proof of Theorem 3.3 is predicated on these observations.

Proposition 3.4: Let F be a left self-distributive system defined on a non-commutative monomial G; then there exist $a \in G^{-1}$ and $b, c \in G$, then the following subsequent conditions are well defined:

(i) $F_a(a) = a.$

(ii) $F_a(b) = c \Leftrightarrow F_{a^{-1}}(c) = b.$

(iii) $F_a(bc) = F_a(b)F_a(c).$

Proof: Proof of (i): Since $aaa^{-1} = a$, so $F_a(a) = a.$

Proof of (ii): $F_a(b) = c \ yields \rightarrow aba^{-1} = c \ yields \rightarrow a^{-1}ca = b \ yields \rightarrow F_{a^{-1}}(c) = b$

Proof of (iii):$F_a(bc) = a(bc)a^{-1} = (aba^{-1})(aca^{-1}) = F_a(b)F_a(c).$

This proof follows the symmetrical assumptions on non-commutative cryptography. The symmetries are generalized as follows:

(A_3) Given (a, b) ∈G and m, n ∈G, such that $b = x^m \cdot a \cdot x^n.$

(A_4) Given (a, b) ∈G, S⊆G, and x∈Z, such that $b = x^m \cdot a \cdot x^n.$

Further if the subset S is large enough, then the membership function doesn't get sufficient data from $x^m \cdot a \cdot x^n.$

IV Diffie-Hellman Process for the Non-commutative Group G

The problem of computing non-commutative group through Diffie-Hellman reference to its subset S determines $a^{x_1x_2}$ or $a^{x_2x_1}$ for known a, a^{x_1}, and a^{x_2}, where $x \in G$, $x_1, x_2 \in S$. In general the commutative law extracts the property that if $x_1 \in G(x_2)$, then $a^{x_1x_2} = a^{x_2x_1}$. Note that discrete logarithm problem in (A_4) over G is traceable. However the converse is not true.

The process of the coding and cryptography module for the monomial rule is conferred in dihedral order eight, as follows:

Monomials with Non-commutative Basis - Encryption-Decryption Rule Algorithm

Global Public Parameters: m, n: IntegersZ^+

a, b: Components of the Ring Group

p, q: Primes

g: Generating Function

M: Message

Assume that $(G, \cdot, 1_G)$ be a non-commutative group, $(R, \cdot, 1_R)$ be a ring and $\tau: (G, \cdot, 1_G) \rightarrow (R, \cdot, 1_R)$ be a monomorphism

User A Key Generation

(i) $f(x)$ could be a random polynomial chosen by A.

(ii) f(x) ∈ Z(x) be a random function, in order that f(a) is well defined; that is, f(τ(A)) ∈τ(G); then user A takes f(a) as personal key and this key is defined as X_A : $X_A = f(a)^m \cdot b \cdot f(a)^n$.

User B Key Generation

(i) *h*(a) could be a random polynomial chosen by B.

(ii) Select *h*(x) ∈ Z(x) randomly in order that *h*(a) is well defined; i.e. h(τ(A)) ∈τ(G); then user B takes *h*(a) as private key and this key is defined as X_B : $X_B = h(a)^m \cdot b \cdot h(a)^n$.

Encryption (User B)

C : Cipher text - sender public key

D: Decryption key - $H(h(a)^m \cdot X_A \cdot h(a)^n) * M$

Decryption (User A)

Original message M': $H(h(a)^m \cdot C \cdot h(a)^n) * M$

The computational rule is defined over two random primes p and q, such that q / p −1 ≠ 0, and also the generating function g is associated with degree order of q and also the message M. This computational rule is numerically illustrated as follows:

$$m = 12, n = 19,$$

$$a = (1\ 2\ 3\ 2\ \ 3\ 4\ 1\ 4\ )$$

$$b = (1\ 2\ 1\ 4\ \ 3\ 4\ 3\ 2\ )$$

Hence $p = 23, q = 11, g = 6,$ and $M = 17$. The random polynomial $f(x) = 2x^5 - 5x^2 + 3$ is chosen by user A; the private key is as follows:

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

$$= {}^{-1}(2 \cdot (0\ -1\ 1\ 0)^5 - 5 \cdot (0\ -1\ 1\ 0)^2 + 3)$$

$$= {}^{-1}\left((8\ 1\ 5\ 8)\ mod(-2)\right)$$

$$= \tau^{-1}(0\ -1\ 1\ 0)\ R_5 \to G_5 \Rightarrow (1\ 2\ 4\ 3\ \ 3\ 4\ 2\ 1\ ).$$

The public key X_A is generated as follows:

$$X_A = f(a)^m \cdot b \cdot f(a)^n$$

$$= (1\ 2\ 4\ 3\ \ 3\ 4\ 2\ 1\ )^{12} \cdot (1\ 2\ 1\ 4\ \ 3\ 4\ 3\ 2\ ) \cdot (1\ 2\ 4\ 3\ \ 3\ 4\ 2\ 1\ )^{19}$$

$$= (1\ 2\ 3\ 2\ \ 3\ 4\ 1\ 4\ )$$

Proceeding further, select user B and consider the random polynomial $h(x) = 9x^4 + x^3 + 4x^2 + 9x + 4$ and computes private key as

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

$$= \tau^{-1}(9(0\ -1\ 1\ 0)^4 + (0\ -1\ 1\ 0)^3 + 4(0\ -1\ 1\ 0)^2 + 9(0\ -1\ 1\ 0) + 4)$$

$$= \tau^{-1}\left((9\ -4\ 12\ 9)\ mod(-2)\right)$$

$$= \tau^{-1}(-1\ 0\ 0\ -1)\ R_7 \to G_7 \Rightarrow (1\ 2\ 2\ 1\ \ 3\ 4\ 4\ 3\ ).$$

The public key generation for user B is defined as X_B

$$X_B = h(a)^m \cdot b \cdot h(a)^n$$

$$= (1\ 2\ 2\ 1\ \ 3\ 4\ 4\ 3\ )^{12} \cdot (1\ 2\ 1\ 4\ \ 3\ 4\ 3\ 2\ ) \cdot (1\ 2\ 2\ 1\ \ 3\ 4\ 4\ 3\ )^{19}$$

$$= (1\ 2\ 2\ 3\ \ 3\ 4\ 4\ 1\ )$$

Then the hash function is defined at

$H: (1\ 2\ _1\ _2\ 3\ 4\ _3\ _4) \rightarrow \left(g^{2^0\cdot\sigma_1+2^1\cdot\sigma_2+2^2\cdot\sigma_3+2^3\cdot\sigma_4}\right)$ mod p.

Suppose that user B is that the sender, then public key is treated as Cipher text. The cryptographic decryption key D is defined for the hash function is

$$D = H(h(x)^m \cdot X_A \cdot h(x)^n) * M$$

$$= H\left((-1\ 0\ 0\ -1)^{12} . (0\ -1\ 1\ 0) . (-1\ 0\ 0\ -1)^{19}\right) * 17$$

$$= H\big((0\ 1\ -1\ 0)\big) * 17\ R_2 \rightarrow G_2 \Rightarrow \left(\left(g^{2^0\cdot 4+2^1\cdot 1+2^2\cdot 2+2^3\cdot 3}\right) mod\ p\right) * 17$$

$$= \left(\left(6^{2^0\cdot 4+2^1\cdot 1+2^2\cdot 2+2^3\cdot 3}\right) mod\ 23\right) * 17$$

$$= \left((6^{38})\ mod\ 23\right) * 17 = 6 * 17 = 23.$$

Now Receiver A decrypts the encrypted message as follows:

$$= H(f(x)^m \cdot Cipher \cdot f(x)^n) * D$$

$$= H\left((0\ -1\ -1\ 0)^{12} . (-1\ 0\ 0\ -1) . (0\ -1\ -1\ 0)^{19}\right) * 23$$

$$= H\big((0\ 1\ -1\ 0)\big) * 23\ R_2 \rightarrow G_2 \Rightarrow \left(\left(g^{2^0\cdot 4+2^1\cdot 1+2^2\cdot 2+2^3\cdot 3}\right) mod\ p\right) * 23$$

$$= \left(\left(6^{2^0\cdot 4+2^1\cdot 1+2^2\cdot 2+2^3\cdot 3}\right) mod\ 23\right) * 23$$

$$= \left((6^{38})\ mod\ 23\right) * 23 = 6 * 23 = 17.$$

V Conclusion

In this paper, non-commutative cryptography with group and ring and semi ring are considered. Random polynomial was chosen with monomial and this monomial was applied in encryption and decryption techniques with two users. The basis of this non-commutative group is recognized on the hidden subgroup or subfield problem. The random polynomials chosen by the communicating to the particular person through secured key exchange, encryption-decryption and authentication schemes. This group supports Diffie-Hellman algorithm along with hash function non-commutative cryptography primitives in algebraic structures

References

[1] M. Anshel, and D. Goldfeld, “An algebraic method for public-key cryptography,” Mathematical Research Letters, vol. 6, no. 3, pp. 287–291, 1999.

[2] J.C. Birget, S. S. Magliveras, and M. Sramka, “On public key cryptosystems based on combinatorial group theory,” Tatra Mountains Mathematical Publications, vol. 33,pp. 137–148, 2006.

[3] Z.Cao, “Noncommutative cryptography” in New Directions of Modern Cryptography, CRC Press, New York, NY, USA, 2013.

[4] Z. Cao, X. Dong, and L.Wang, “New public key cryptosystems using polynomials over noncommutative rings ,” Journal of Cryptology—IACR, vol. 9, pp. 1–35, 2007.

[5] P. Dehornoy, “Braid-based cryptography,” Contemporary Mathematics, vol. 360, pp. 5–33, 2004.

[6] B. Eick and D. Kahrobaei, “Polycyclic groups: a new platform for cryptology?” https://arxiv.org/abs/math/0411077v1.

[7] Gautam Kumar and Hemraj Saini, Novel Noncommutative Cryptography Scheme Using Extra Special Group, Security and Communication Networks Volume 2017, Article ID 9036382, 21 pages, https://doi.org/10.1155/2017/9036382.

[8] D. Grigoriev and I. Ponomarenko, “Homomorphic public-key cryptosystems over groups and rings,” https://arxiv.org/abs/cs/ 0309010v1, 2003.

[9] A. Kitaev, “Quantum Measurements and the Abelian Stabilizer Problem. Electronic Colloquium on Computational Complexity,” Vol. 3, 1996, http://eccc.hpi-web.de/ecccreports/ 1996/TR96-003/index.html.

[10] K.H.Ko, S. J. Lee, J.H. Cheon, J.W.Han, J.-S.Kang, and C.Park, “New publickey cryptosystem using braid groups,” in CRYPTO 2000, M. Bellare, Ed., vol. 1880 of Lecture Notes in Computer Science, pp. 166–183, Springer, Berlin, Germany, 2000.

[11] S. S. Magliveras, D. R. Stinson, and T. van Trung, “New approaches to designing public key cryptosystems using one way functions and trapdoors in finite groups,” Journal of Cryptology, vol. 15, no. 4, pp. 285–297, 2002.

[12] A. Mahalanobis, The diffie-hellman key exchange protocol, its generalization and nilpotent groups [Ph.D. dissertation], Florida Atlantic University, Boca Raton, USA, 2005.

[13] S.H. Paeng, K.-C. Ha, J. H. Kim, S. Chee, and C. Park, “New public key cryptosystem using finite non abelian groups,” in Advances in Cryptology—CRYPTO 2001.

[14] W. S. Peter, “Algorithms for quantum computation: discrete logarithms and factorings,” in Proceedings of the 35th Annual Symposium on Foundations of Computer Science, pp. 124–134, 1994.

[15] V. Shpilrain and A. Ushakov, “Thompson’s group and public key cryptography,” in Applied Cryptography and Network Security, pp. 151–163, 2005.

[16] N. R.Wagner and M. R. Magyarik, “A public-key cryptosystem based on the word problem,” in Advances in Cryptology—Proceedings of CRYPTO 84, G. R. Blakley and D. Chaum, Eds., vol. 196 of Lecture Notes in Computer Science, pp. 19– 36, Springer, Berlin, Germany, 1985.