A Survey of Public-Key Cryptography over Non-Abelian Groups

G. H. J. Lanel[†,*], T. M. K. K. Jinasena[††] and B. A. K. Welihinda[†],

kasun@sjp.ac.lk, kasuniwe@gmail.com

[†]Department of Mathematics, University of Sri Jayewardenepura, Gangodawila, Nugegoda, Sri Lanka

[††]Department of Computer Science, University of Sri Jayewardenepura, Gangodawila, Nugegoda, Sri Lanka

*(Corresponding Author: Dr. G.H.J. Lanel ghjlanel@sjp.ac.lk)

Summary

Non-abelian group based Cryptography is a field which has become a latest trend in research due to increasing vulnerabilities associated with the abelian group based cryptosystems which are in use at present and the interesting algebraic properties associated that can be thought to provide higher security. When developing cryptographic primitives based on non-abelian groups, the researchers have tried to extend the similar layouts associated with the traditional underlying mathematical problems and assumptions by almost mimicking their operations which is fascinating even to observe. This survey contributes in highlighting the different analogous extensions of traditional assumptions presented by various authors and a set of open problems. Further, suggestions to apply the Hamiltonian Cycle/Path Problem in a similar direction is presented.

Key words:

Cryptography, Diffie-Hellman, Discrete Logarithm Problem, El-Gamal, Hamiltonian Cycle/Path Problem, Non-abelian/Non-commutative.

1. Introduction

Cryptography, which is the science of secret communication has been a topic of interest from earliest days of history. There are two main types of Cryptography. They are Private-key Cryptography and Public-key Cryptography. The well-known public-key cryptosystems that are practically in use at present are Number theory based and theoretically use the structures and properties of abelian groups. A prominant discussion among experts, at present is, whether the security of these cryptosystems are breakable. Infact, it was proven, that their security will be easily broken if the quantum computers are invented.

With the discovery of more and more vulnerabilities, the attention is focused on introducing novel methods for Cryptography. One such direction is the use of non-abelian groups to develop cryptographic protocols. In this survey, we focus on the literature related to the non-abelian group based public-key cryptographic protocols.

Actually, our attention was directed towards non-abelian group based Cryptography, during a study of the Hamiltonian cycles in Cayley graphs. We have studied about the Cayley graphs of non-abelian groups of orders $p^n q$, p^2q^2 and p^2qr, where p, q, r are distinct primes and $n(\geq 2) \in \mathbb{Z}^+$. For related literature and a recent advancement in this direction see [1] and [2].

A Hamiltonian cycle in a Cayley graph represents a non-trivial relationship among the generating elements of the graph and it is well known among the mathematicians that the Hamiltonian Cycle Problem is a very difficult problem (NP-complete problem). This motivated us to think of applying the Hamiltonian Cycle Problem to the field of Cryptography. And we noticed, since we are using non-abelian groups, it will probably give an added advantage and security over the currently existing algorithms which only make use of the abelian properties. Thereby after initiating the literature survey, it was possible to see that, indeed the attention of scientists have already been enthralled towards non-abelian group based Cryptography. Such studies were actually started in 1980's [3].

As a main contribution of our work, we present and discuss important related literature during the past two decades. Refer [4] and [5] for past literature surveys on the same topic. We gather and present literature related to some significant schemes and several open problems not highlighted in those surveys, while keeping an emphasis on different variants of the traditional cryptographic assumptions extended to the non-abelian platforms, with the expectation that it will be a useful reference for academic scholars and undoubtably provoke enthusiasm in them due to the variated algebraic properties involved with the non-abelian groups. Moreover, we also present a novel motivation to view the Hamiltonian Cycle/Path Problem in relation to public-key cryptographic schemes.

The remainder of this paper is organized as follows. Firstly, Section II briefly introduces the most important and relevant basic concepts of Public-key Cryptography. Then, the Sections III to VI present the existing non-abelian group based cryptosystems which follow the concepts of traditional Discrete Logarithm Problem, non-abelian group based variants of Factorization Problems, Membership Search Problems and the Word Problem respectively. The next Section includes a short review on the famous Logarithmic signatures. The Section VIII is devoted to our discussion on future research directions. The final Section summarizes this paper and draws conclusions about the state of the art of this field.

Manuscript received April 27, 2021
Manuscript revised April 30, 2021
https://doi.org/10.22937/IJCSNS.2021.21.4.36

2. Fundamentals of Public-key Cryptography

The well-known mathematically hard problems used for Cryptography are the Integer Factorization Problem and the Discrete Logarithm Problem. Currently existing cryptographic schemes are based on assumptions such as the RSA assumption, strong RSA assumption [6] or the Elliptic Curve Discrete Logarithm Problem and uses protocols like the Diffie-Hellman key exchange, El-Gamal encryption scheme etc.

Definition 1 (Discrete Logarithm Problem (DLP) [5]). *Let G be a group. If $h, g \in G$ such that $h = g^x$ and h, g are known, find the integer x.*

Definition 2 (The RSA assumption [6]). *It is the assumption that, "Given a randomly generated RSA modulus n, an exponent r and a random $z \in \mathbb{Z}_N^*$, find y such that $y^r = z$ ".*

Eventhough many attempts have been made to develop cryptosystems using the non-abelian algebraic structures, a successful, practically usable non-abelian analogy of a cryptosystem is yet to be devised. The main method of handling non-abelian groups is Combinatorial Group theory, which involve the studying of groups using group presentations.

When considering the non-abelian platforms for Cryptography, the researchers have also found many novel mathematically hard problems which can be employed as the basis of necessary cryptographic assumptions such as the Conjugacy Problem, Conjugacy Search Problem etc.
The standard assumption of cryptographers in the past is that, an eavesdropper has access to all the information except the secret keys and random choices of the communicating parties. But the modern Cryptography has more demanding point of views such as the assumption that, an eavesdropper is unable to guess which two messages have been encrypted, once presented with a single challenging cipher-text, which is one of the encrypted messages.

3. Discrete Logarithm Problem

Many researches have output with various analogous problems that can follow the basic concepts of the traditional DLP. In this section, we discuss the related literature.

3.1 Conjugacy Problem and Conjugacy Search Problem

An outstanding property of the non-abelian cryptographic platforms is that it can take advantage of intractable problems in Quantum Computing, Combinatorial Group theory and Computational Complexity theory for their construction [3]. Due to its ability to resist quantum attacks, non-abelian group based Cryptography is expected to achieve higher security. Some mathematical problems offer significantly increased hardness when non-commutative groups are considered. For instance, there exists efficient quantum algorithms that can solve hidden subgroup problem in abelian groups but not in non-abelian groups.

Anshel-Anshel-Goldfeld and Ko-Lee cryptographic schemes are two of the very first introductions of non-abelian cryptosystems (introduced around the same time periods, in 1999 and 2000 respectively). The schemes are based on the difficulty of the Conjugacy Search Problem and Conjugacy Problem in the underlying groups respectively.

Definition 3 (Conjugacy Problem (CP) [7]). *Given a group G and elements $x, y \in G$, decide whether there exists an element $g \in G$ such that $x^g = y$. i.e., $g^{-1}xg = y$.*

Definition 4 (Conjugacy Search Problem (CSP) [5]). *Let G be a non-abelian group. Let $g, h \in G$ be known such that $h = g^x$ for some $x \in G$. Find x. Here, g^x stands for $x^{-1}gx$.*

3.1.1 Anshel-Anshel-Goldfeld protocol:

Let G be a non-abelian group with a finite presentation, where elements can be represented using unique normal forms. Let $NF(g)$ denote the normal form of g, for any $g \in G$. Assume that for given normal forms of $x, y \in G$, the normal form for xy doesn't reveal either x nor y.
The protocol operates via the computation of the commutator, $[a, b] = a^{-1}b^{-1}ab$ as a shared secret key, by the communicating parties, Alice and Bob. Here, $a = W(a_1, \dots, a_n)$, $b = V(b_1, \dots, b_m)$ are the secret words chosen by Alice and Bob, from their randomly chosen, finitely generated subgroups of G, say $A =< a_1, \dots, a_n >$, $B =< b_1, \dots, b_m >$, respectively. The groups, A, B and the normal forms of the conjugates of the generating elements of A, B, i.e. $NF(a_j^b), j = 1, \dots, n$ and $NF(b_i^a), i = 1, \dots, m$ are made public by each of the parties, by using their respective private keys. Since, Alice knows a^b from Bob's shared computation, she can compute $a^{-1}a^b = a^{-1}(b^{-1}ab) = [a, b]$. Similarly, Bob knows b^a from Alice's shared computation, so he can compute $(b^a)^{-1}$ and hence, $(b^a)^{-1}b = (a^{-1}b^{-1}a)b = [a, b]$.

In [8], I. Anshel, M. Anshel, B. Fisher and D. Goldfeld had proposed key agreement protocols whose security is based on the difficulty of inverting one-way functions derived from hard problems in braid groups. And further in [9], I. Anshel, M. Anshel and D. Goldfeld analyze several examples of non-abelian key agreement protocols (KAPs) and discuss the axioms for non-abelian key agreement protocols, some intractable problems and requirements for Graph theory in KAP.

An analogue of the Anshel-Anshel-Goldfeld protocol based on the following Subgroup Conjugation Search Problem (SCSP) was discussed in [10].

Definition 5 (Subgroup Conjugation Search Problem (SCSP)). *Given a group G, subgroups H_1, H_2 of G, and two elements $f, g \in H_1$, find an element $h \in H_2$ such that $f = h^{-1}gh$, provided that at least one such h exist.*

The SCSP seems to be difficult if G is restricted to subgroups of the group $GL(V,R)$, which denote the group of all invertible R-linear transformations of the free R-module V and R is a finite commutative ring [10]. In order to clarify this the authors had discussed a special case of the SCSP when $G = AGL(V,R)$, the Linear Transporter Problem (Here, $AGL(V,R)$ is the group of all affine transformations of V [10]). Another novel cryptographic protocol was also proposed based on this problem.

Definition 6 ((Linear Transporter Problem (LTP)). *Let R be a commutative ring, V be an R-module and $G \leq GL(V,R)$. Given $u \in V$, and $v \in u^G = \{u^g | g \in G\}$, find $g \in G$ such that $v = u^g$.*

3.1.2 Ko-Lee protocol:

Let G be a non-abelian group with unique normal forms same as in the above protocol. Alice and Bob choose commuting subgroups A, B of G, random elements $a \in A$, $b \in B$ respectively, which will be kept as secrets. For a public element $g \in G$, $g^a = a^{-1}ga$ and $g^b = b^{-1}gb$ are computed by Alice and Bob and exchanged, which will be exponentiated by the secret elements of each party to acquire a shared secret key. In this protocol, $(g^b)^a = (g^a)^b$, due to the commuting property of the subgroups A and B chosen. While the security of novel cryptosystems is always an open question, the studies of Ko-Lee has brought up several new problems.

Q1. Can new primitives and cryptosystems be further developed, using the hard problems in braid groups? For instance, digital signature schemes.

Q2. What conditions make problems like, Generalized Conjugacy Search Problem and Conjugacy Decomposition Problem equivalent?

Q3. Identify new groups suitable to be used with one-way functions like Conjugacy Problem. Particularly, groups satisfying the properties,

- the Word Problem should be solvable by a fast algorithm (e.g.:- automatic groups),
- the Conjugacy Problem should be hard,
- should be easy to digitize the group element.

The Anshel-Anshel-Goldfeld and Ko-Lee protocols can be regarded as quite practical schemes, had a most suitable platform group been found. The main requirements in a platform group for any cryptosystem are the possibility to store and manipulate group elements efficiently and the underlying mathematical problem being hard in a majority of its instances.

The groups with short linear representations are obviously more vulnerable, since they can be subjected to linear attacks. Finite groups comprising of permutation representations of lower degrees could get subjected to attacks based on the theories of computational permutation group theory, whereas the groups with many normal subgroups can be reduced to quotients easily, and hence are vulnerable.

3.2 Generalized Discrete Logarithm Problem

Ivana Ilić [11] (see [7] for a detailed description) had used a Generalized DLP, which was originally introduced in [12] and had proven that it is weak in the projective special linear groups, $PSL(2,p)$, where p is an odd prime. However, recollect that even the ideas of using conjugates in the Anshel-Anshel-Goldfeld and Ko-Lee protocols can also be thought of as other ways of generalizing the DLP to non-abelian groups.

Definition 7 (Generalized DLP [12]).
Let G be a finite group generated by $\alpha_1, \dots, \alpha_t$. i.e. $G =< \alpha_1, \dots, \alpha_t >$. Denote by $\alpha = (\alpha_1, \dots, \alpha_t)$, the ordered tuple of generators of the group G. For a given $\beta \in G$, the Generalized DLP of β with respect to α is to determine a positive integer k and a (kt)- tuple of non-negative integers $x = (x_{11}, \dots, x_{1t}, \dots, x_{k1}, \dots, x_{kt})$ such that,

$$\beta = \prod_{i=1}^{k} (\alpha_1^{x_{i1}} \dots \alpha_t^{x_{it}})$$

This can be expressed using the notation $\beta = \alpha^x$. The (kt) –tuples, $(x_{11}, \dots, x_{1t}, \dots, x_{k1}, \dots, x_{kt})$ are known as the *generalized discrete logarithms* of β with respect to α.
When considering the group $G = PSL(2,p)$, two subgroups, say H and K generated by two non-commuting elements α and β of order p in G are required to be identified. Then, the group can be represented as $G = HKHK$. By assuming that, G is represented by matrices

from $SL(2,p)$ and taking $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $B = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$, to

be the generating elements such that $G =< A, B >$, the author shows that the solving of the Generalized DLP is equivalent to determining a non-negative integer tuple (i, j, k, l) such that,
$M = A^i B^j A^k B^l$, where $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G; a, b, c, d \in \mathbb{F}_p$.

This is then reduced to a system of equations which can be solved using Gröbner basis computations easily. Hence, it was concluded that the Generalized DLP in $PSL(2,p)$ is not hard. Further, using this, a Generalized Diffie-Hellman key exchange protocol and a Generalized El-Gamal encryption scheme was also proposed.

3.2.1 Generalized Diffie-Hellman key exchange protocol:

A major problem faced in trying to achieve Diffie-Hellman key exchange is the inequality $(\alpha^x)^y \neq (\alpha^y)^x$ due to the non-abelian nature of elements. To overcome this, the operation of conjugation by elements was introduced to commute with the exponentiation by integers.

Theorem 1. [7] Let $G =< \alpha_1, \dots, \alpha_n >$ be a finite non-abelian group. Let $(\alpha_1, \dots, \alpha_n)^x$ denote the operation of exponentiation by integer x and for $g \in G$ let $(\alpha_1, \dots, \alpha_n)^g$ denote the operation of conjugation:

$$(\alpha_1, \dots, \alpha_n)^g = (\alpha_1^g, \dots, \alpha_n^g) = (g^{-1}\alpha_1 g, \dots, g^{-1}\alpha_n g)$$

Then, $((\alpha_1, \dots, \alpha_n)^x)^g = ((\alpha_1, \dots, \alpha_n)^g)^x$.

Key-exchange protocol:- Alice and Bob agree on a group $G =< \alpha_1, \dots, \alpha_n >$. Alice selects a random positive integer x, computes $g_a = (\alpha_1, \dots, \alpha_n)^x$ and sends it to Bob, where as Bob selects a random group element $g \in G$, computes $g_b = (\alpha_1, \dots, \alpha_n)^g$ and sends it to Alice. Then the two parties compute $g_b^x = ((\alpha_1, \dots, \alpha_n)^g)^x = k_A$ and $g_a^g = ((\alpha_1, \dots, \alpha_n)^x)^g = k_B$, respectively, which is the shared secret (by, Theorem 1, $k_A = k_B =$ *common secret key*).

3.2.2 Generalized El-Gamal encryption scheme:

A short description of the operation of a variant of the El-Gamal encryption scheme based on the Generalized DLP is as follows.

Key generation: Each entity ε selects non-abelian group $G =< \alpha_1, \dots, \alpha_n >$, random positive integer x_ε, computes $g_\varepsilon = (\alpha_1, \dots, \alpha_n)^{x_\varepsilon}$ and publishes g_ε and $(\alpha_1, \dots, \alpha_n)$, keeping x_ε a secret. In particular, Alice's secret key is x_a, and public key is $(g_a, (\alpha_1, \dots, \alpha_n))$, where $g_a = (\alpha_1, \dots, \alpha_n)^{x_a}$.

Encryption: To send a message to Alice, Bob obtains Alice's public-key pair $(g_a, (\alpha_1, \dots, \alpha_n))$, and writes the message m as an element of the group G. Then, for a random secret element $g \in G$, he computes $(\beta_1, \dots, \beta_n) = (\alpha_1, \dots, \alpha_n)^g$, and sends$((\beta_1, \dots, \beta_n), mg_a^g)$ to Alice.

Decryption: To decrypt, Alice uses x_a to compute $((\beta_1, \dots, \beta_n)^{x_a})^{-1}$ and multiplies on the right by mg_a^g.

$$mg_a^g((\beta_1, \dots, \beta_n)^{x_a})^{-1} = mg_a^g(((\alpha_1, \dots, \alpha_n)^g)^{x_a})^{-1}$$

$$= m((\alpha_1, \dots, \alpha_n)^{x_a})^g(((\alpha_1, \dots, \alpha_n)^g)^{x_a})^{-1} = m.$$

Further research on Generalized DLP could be through investigating along the below questions [12].

Q4. Analyzing whether there exists an appropriate algebra on the exponents and the direct applications of the Generalized DLP in encryption/signature primitives.

Q5. Determine computational complexity of Generalized DLP, respect to α.

Q6. Determine efficient methods/ways to factorize elements in concrete or abstract groups.

3.3 Protocols involving automorphisms

Usage of automorphisms of non-abelian groups for Cryptography was also apparent in several sources of literature. Based on the concept of the standard Diffie-Hellman key exchange protocol, A. Mahalanobis in 2018 [13], had studied regarding a possible analogous key exchange protocol using the abelian subgroups of the automorphism group of a non-abelian nilpotent group.
Similar efforts were also mentioned in [8], [14], [15] using braid groups, in [16], [17] using a family of finitely presented non-abelian groups and in [18], a description of a key exchange protocol similar to that in [13] can also be found. As described in [13], the definitions of General Discrete Logarithm Problem (GDLP) and General Diffie-Hellman Problem (GDHP) are as follows and the author had discussed two variants of key-exchange protocols.

Definition 8 (General DLP (GDLP)). *Let* $G =< a_1, a_2, \dots, a_n >$ *and* $f: G \to G$ *be a non-identity automorphism. Suppose one knows* $f(a)$ *and* $a \in G$*, then GDLP is to find* $f(b)$ *for any* $b \in G$.

Assuming the Word Problem (see Definition 20) is easy or presentation of the group is by means of generators, GDLP is equivalent to finding $f(a_i)$ for all i which in terms gives us a complete knowledge of the automorphism. In other words the cryptographic primitive GDLP is equivalent to, "finding the automorphism f from the action of f on only one element".

Definition 9 (General Diffie-Hellman Problem (GDHP)). *Let* $\phi, \psi: G \to G$ *be arbitrary automorphisms such that* $\phi\psi = \psi\phi$*, and assume one knows* $a, \phi(a)$ *and* $\psi(a)$*. Then GDHP is to find* $\phi(\psi(a))$.

Let G be a finitely presented group and S be an abelian subgroup of $Aut(G)$.

3.3.1 Key-exchange protocol 1:

1. Alice and Bob first select a group G, and an element $a \in G \setminus Z(G)$, where $Z(G)$ is the center of G and random automorphisms ϕ_A, ϕ_B from S, respectively, as the private keys. Each compute $\phi_A(a)$ and $\phi_B(a)$ respectively, and exchange.
2. Then Alice can compute $\phi_A(\phi_B(a))$, which is equal to $\phi_B(\phi_A(a))$ that can be computed by Bob. This is the shared secret key.

If the automorphisms used are automorphisms which fix conjugacy classes, such as the inner automorphisms, then the security of the scheme actually relies on the Conjugacy Problem. Suppose, $\phi_A(a) = x^{-1}ax$ and $\phi_B(a) = y^{-1}ay$ for some x, y, then $\phi_A(\phi_B(a)) = (yx)^{-1}a(yx)$. Hence, if the Conjugacy Problem is easy, for a known a, $\phi_A(a)$ and

$\phi_B(a)$, then the secret values x and y can be found by an eavesdropper.

3.3.2 Key-exchange protocol 2:

1. Alice and Bob choose a group G. Any $z_{\phi,g} \in Z(G)$ depends on ϕ and g for any central automorphism $\phi \in Aut(G)$ and $g \in G$.
2. First, Alice chooses a random non-central element $g \in G$ and $\phi_A \in S$. She computes $\phi_A(g)$ and sends to Bob.
3. For a random $\phi_B \in S$, Bob computes $\phi_B(\phi_A(g))$ and sends to Alice.
4. Then, Alice computes $\phi_A^{-1}(\phi_B(\phi_A(g)))$, which will give her $\phi_B(g)$.
5. Now, Alice has to pick another random $\phi_H \in S$ and compute $\phi_H(\phi_B(g))$ and $\phi_H(g)$. She sends $\phi_H(\phi_B(g))$ to Bob and keeps $\phi_H(g)$ private.
6. Bob computes $\phi_B^{-1}(\phi_H(\phi_B(g))) = \phi_H(g)$. Then $\phi_H(g)$ is the shared secret key.

For central automorphisms, ϕ_A and ϕ_B, $\phi_A(g) = gz_{\phi_{A,g}}$. If G is special (i.e. $Z(G) = [G,G] = \Phi(G)$, where $[G,G]$ is the commutator subgroup of G and $\Phi(G)$ is the Frattini subgroup of G), then, $\phi_B(gz_{\phi_{A,g}}) = gz_{\phi_{B,g}}z_{\phi_{A,g}}$ from which $z_{\phi_{B,g}}$ can be computed. Since, $\phi_H(\phi_B(g)) = gz_{\phi_{B,g}}z_{\phi_{H,g}}$ is public, $gz_{\phi_{H,g}}$ can be computed using $z_{\phi_{B,g}}$ and the scheme can be broken. However, this attack is possible only if the group is special.
The author introduces a signature scheme as well, where as it is generally difficult to devise signature schemes using non-abelian groups.

3.3.3 A signature scheme based on the conjugacy problem as mentioned in [13]:

Let G be a group with commuting inner automorphisms.

1. Alice chooses $\beta = a^{-1}\alpha a$ and publishes α and β, while keeping a as a secret.
2. To sign a text $x \in G$, she picks an arbitrary $k \in G$ and compute $\gamma = k\alpha k^{-1}$ and δ such that, $x = (\delta k)(a\gamma)^{-1}$.

   Note that, $x\alpha x^{-1} = (\delta k)(a\gamma)^{-1}\alpha((\delta k)(a\gamma)^{-1})^{-1}$

   $= (\delta k)\gamma^{-1}a^{-1}\alpha a\gamma k^{-1}\delta^{-1} = \delta\gamma^{-1}a^{-1}k\alpha k^{-1}a\gamma\delta^{-1}$

   (since inner automorphisms commute)

   $= \delta\gamma^{-1}a^{-1}\gamma a\gamma\delta^{-1} = \delta a^{-1}\gamma a\delta^{-1}$

   $= \delta(k\beta k^{-1})\delta^{-1}$ $(\gamma = k\alpha k^{-1} \Longrightarrow a^{-1}\gamma a = k\beta k^{-1})$
3. Alice sends x and $k\delta$ to Bob.
4. Bob computes $L = x\alpha x^{-1}$ and $R = \delta k\beta(\delta k)^{-1}$. If $L = R$, the message is authentic, otherwise it is not.

3.3.4 The MOR cryptosystem:

The MOR cryptosystem is another well-known cryptosystem which had attracted the attention of many scholars, that makes use of automorphisms (See [19], [20], [21] and [22] for further analytical details). It can be identified as a straight forward generalization of the traditional El-Gamal cryptosystem.
Let $G =< \alpha_1, \dots, \alpha_t >$ be a finite non-abelian group and ϕ_g be an inner automorphism of G. $\phi_g(x) = g^{-1}xg, \forall x \in G$. We know that, $\phi_g^m(x) = g^{-m}xg^m$, for any $m \in \mathbb{Z}^+$. The MOR cryptosystem introduced in [22] involves computing and publishing of a sequence of values like ϕ_g and ϕ_g^m (i.e. $\{\phi_g(\alpha_i)\}_{i=1}^t$ and $\{\phi_g^m(\alpha_i)\}_{i=1}^t$), by the communicating parties, where $g \in G$ and $m \in \mathbb{Z}^+$ will be kept as secrets.
A. Mahalanobis, in [22] had proposed the group of unitriangular matrices over a finite field as a suitable non-abelian platform for the MOR cryptosystem. There, the composition of inner, diagonal and central automorphisms were considered as the group of automorphisms. The author has also encouraged future research focusing on the following questions.
Q7. Is the security of the MOR and El-Gamal cryptosystems equivalent?
Q8. Is it computationally more expensive than the El-Gamal cryptosystem?

In the following year, A. Mahalanobis [23] had given an explicit discussion regarding the use of p-groups for the MOR cryptosystem. He had shown that a better cryptosystem in comparison to the existing El-Gamal cryptosystem can not be built using the p-groups. In [24], the same author had studied the security of the MOR cryptosystem in special linear groups over the finite fields and had shown that it has better security than the traditional El-Gamal cryptosystem when special linear groups are considered.

Free groups are widely used in computer science and many modern cryptosystems rely on the hardness of computational problems over finite free groups. Articles [4], [25] and [26] includes informative descriptions regarding the free group cryptosystems.

Definition 10. *A group is a "free group" if no relation exists between its generators (other than the relationship between an element and its inverse which is required as one of the defining properties of a group).*

3.3.5 Moldenhauer protocol:

In [27], a public-key cryptosystem following the format of the conventional El-Gamal encryption scheme was developed based on the automorphisms of a free group

$F =< X| >$, where X is a free generating set with $|X| = q$ by Moldenhauer et al.. There,

Public parameters: The group $F =< X| >$, a freely reduced word $a \neq 1$ in the free group F and an automorphism $f: F \to F$ of infinite order.

Encryption and Decryption procedure:

1. Alice chooses (privately) a natural number n and publishes the element $f^n(a) = c \in S^*$ (S^* is the set of all freely reduced words with letters in $X \cup X^{-1}$).
2. Bob picks (privately) a random $t \in \mathbb{N}$ and his message $m \in S^*$. He calculates the freely reduced elements,

   $m \cdot f^t(c) = c_1 \in S^*$ and $f^t(a) = c_2 \in S^*$ and sends the cipher text $(c_1, c_2) \in S^* \times S^*$ to Alice.
3. Alice computes, $c_1 \cdot f^n(c_2)^{-1} = m \cdot f^t(c) f^n(c_2)^{-1}$

   $= m \cdot f^t(f^n(a)) f^n(f^t(a))^{-1} = m \cdot f^{t+n}(a)(f^{n+t}(a))^{-1} = m$

   to recover the message.

3.3.6 Paeng et al. cryptosystem:

Paeng et al. in 2001 [28] had put forward another cryptosystem using the automorphisms of non-abelian groups. A speciality of this system is that it involves faster encryption and decryption than most other well-known public-key cryptosystems and also could give rise to a signature scheme.

Let G be a non-abelian group with non-trivial center $Z(G)$, where $Z(G)$ is not small, $g \in G$ and $Inn(g)$ denote an inner automorphism. Suppose $\{\alpha_i\}$ is a set of generators of G. For a communicating party, say Alice, the public key is $\{Inn(g), Inn(g^a)\}$ and the private key is a. A sequence of values, quite similar to that in the MOR cryptosystem is made public to be used for encryption. i.e. $(Inn(g^a))^b$ ($\{(Inn(g^a))^b(\alpha_i)\}$) for an arbitrarily chosen value b. A message m will be encrypted as, $E = Inn(g^{ab})(m) = (Inn(g^a))^b(m)$ and $\phi = Inn(g^b)$ (i.e. $\{Inn(g^b)(\alpha_i)\}$) and (E, ϕ) will be sent to Bob.

The scheme is efficient and successful once the $Inn(g^a)$ is expressed with small bits and even though the scheme has the outlook of the El-Gamal cryptosystem, it is possible to keep the random b value fixed unlike in the El-Gamal scheme. The reason for this is the inability to obtain $m_1^{-1}m_2$ from $Inn(g^b)(m_1)$ and $Inn(g^b)(m_2)$ for any two messages $m_1, m_2 \in G$, to find the key value b.

3.4 Protocols involving Matrix groups

Using the elements of $GL(2, \mathbb{Z}_n)$, Bates, Meyer and Pulickal [29] had proven the security of Cayley-Purser algorithm against the Brute Force attack and an attack on the public-key parameters (an attack made to acquire the private-key). The authors had also introduced a novel public-key exchange protocol. The steps of the Cayley-Purser algorithm introduced by S. Flannery [30] has quite a simple attire, so we will outline it here for an interested reader.

Consider $GL(2, \mathbb{Z}_n)$, where $n = pq$ with $p = 2p' + 1$ and $q = 2q' + 1$; p, q, p', q' are primes, and p, q are distinct safe primes as mentioned. Assume that, the messages are converted to matrices in $GL(2, \mathbb{Z}_n)$. The receiver of the message, computes $B = C^{-1}A^{-1}C$ and $G = C^r$ are computed, where $n = pq$, p, q are suitably large safe primes, $A, C \in GL(2, \mathbb{Z}_n)$ are random non-commuting elements and $r \in \mathbb{N}$ is random. The sender of the message, encrypt a message M as $M' = KMK$, where $D = G^s$, $E = D^{-1}AD$, $K = D^{-1}BD$ and $s \in \mathbb{N}$ is random. The matrix E acts as the enciphering key. The receiver, upon obtaining the encrypted message, compute $K^{-1}M'K^{-1} = K^{-1}(KMK)K^{-1} = M$.

A different construction of a public-key cryptosystem using a type of a block upper triangular matrices was investigated by Á lvarez et al. [31] in 2009. The set $\Theta = \left\{\begin{bmatrix} A & X \\ 0 & B \end{bmatrix} \middle| A \in Gl_r(\mathbb{Z}_p), B \in GL_s(\mathbb{Z}_p), X \in Mat_{r\times s}(\mathbb{Z}_p)\right\}$,forms a non-abelian group under the operation of product of matrices. Here, p is a prime number, $r, s \in \mathbb{N}$, $Mat_{r\times s}(\mathbb{Z}_p)$ is the set of $r \times s$ matrices over $\mathbb{Z}_p$ and $GL_r(\mathbb{Z}_p), GL_s(\mathbb{Z}_p)$ are the sets of invertible $r \times r$ and $s \times s$ matrices over $\mathbb{Z}_p$, respectively. When a matrix $M \in \Theta$ is raised to a power $h \in \mathbb{Z}^+$:

$$M^h = \begin{bmatrix} A^h & X^h \\ 0 & B^h \end{bmatrix}, \text{ where } X^h = \begin{cases} 0, & if\ h = 0 \\ \sum_{i=1}^{h} A^{h-i}XB^{i-1}, & if\ h \geq 1 \end{cases}$$

A key-exchange scheme was established by showing that a construction of keys obtained from the simplification of a computation involving matrix multiplications and matrix exponentiations following the above definitions are equal. This construction is dependent on the analogous DLP considered for matrices (See [31]). The same author had made further contributions in [32] and [33]. In 2006, Climent et al. [34] had proposed another cryptosystem using non-abelian matrix groups and in 2010 Pathak and Sanghi [35] studied in the same direction resulting in a novel public-key cryptosystem and a key-exchange protocol.

Menezes and Wu [36] had proven that, the DLP over $GL(n, \mathbb{F}_p)$ can be reduced in probabilistic polynomial time to the DLP over small finite extension fields of $\mathbb{F}_p$. This shows that there is no particular advantage in trying to use DLP over $GL(n, \mathbb{F}_p)$, than the field of integers modulo p.

Furthermore, a reputed key-agreement protocol using the matrices is the "Stickel's scheme" introduced by E. Stickel [37]. He had made use of a certain subgroup of $GL(n, \mathbb{F}_p)$ as the platform for the scheme rather than considering the entire group $GL(n, \mathbb{F}_p)$. V. Shipilrain [38] had suggested an

improvement for this scheme by proposing $Mat_n(R)$, where R is a finite ring as a more secure platform.

4. Factorization Problems

The non-abelian factorization problems were enlightened with the introduction of braid group based cryptosystems [15] and Conjugacy Search Problem based constructions [39]. We should remark here, that the braid group based Cryptography is a significant area where many researchers have studied and made contributions over the decades. Even though infinite groups such as braid groups had been under major attention, finite groups are expected to have more useful aspects.

In 2011, Baba, Kotyada and Teja [40] had proposed a non-commutative Factorization Problem and a related cryptosystem (the BKT scheme). The cryptographic assumptions as proposed by them can be stated as follows.

Definition 11 (Factorization Problem (FP) [40]). *Let G be any finite group with identity e. Let $g,h \in G$ be two random elements so that $< g > \cap < h > = \{e\}$. The Factorization Problem with respect to G, g, h, denoted by $FP_{g,h}^{G}$, is to split the given product $g^x h^y \in G$ into a pair $(g^x, h^y) \in G^2$, where x and y are arbitrary integers picked at random.*

If G is abelian and the orders of g and h are known, where $gcd(|g|, |h|) = 1$, the FP can be reduced to the DLP in G. If $|g|$ and $|h|$ have common factors the FP is much harder. If G is non-abelian and g, h are non-commuting, the best known method to solve the FP is the naïve method, which is to consider all the possible pairs of (x, y) one by one. This is regarded to be infeasible for very large values of $|g|$ and $|h|$. The traditional Diffie-Hellman Problem, which has two types; Computational and Decisional can be defined as follows.

Definition 12 (Computational Diffie-Hellman Problem [7]). *Given a finite cyclic group generated by element α, and given α^x and α^y, find α^{xy}.*

Definition 13 (Decision Diffie-Hellman Problem [7]). *Given a finite cyclic group generated by element α of order n, and given α^x, α^y and α^z, determine whether $z \equiv xy \bmod(n)$.*

If the DLP can be solved, then both the Computational Diffie-Hellman Problem and the Decision Diffie-Hellman Problem can be solved. If the Computational Diffie-Hellman Problem can be solved, then so can the Decision Diffie-Hellman Problem.

In [40], a more generalized expression of the Diffie-Hellman Problems can be found, which can be easily used for non-abelian groups as well. We mention here the Computational version of the problem:

Definition 14 (Computational Diffie–Hellman (CDH) Problem). *Let G be any finite group with identity e. Let $g, h \in G$ be two random elements so that $< g > \cap < h > = \{e\}$. The computational Diffie–Hellman (CDH) problem with respect to G, g, h, denoted by $CDH_{g,h}^{G}$, is to recover $g^{a+c}h^{b+d}$ from the given pair $(g^a h^b, g^c h^d) \in G^2$, where a, b, c, d are arbitrary integers picked at random.*

The BKT scheme:

1. Key-generation: Let G be a non-abelian group and $g, h \in G$ be non-commuting elements such that $|g| = k, |h| = l$. The public-key = $(G, g, h, g^x h^y)$ and private-key = $(g^x, h^y) \in G^2$, where x, y are random integers are to be securely destroyed after the generation of the keys.
2. Encryption: Let $m \in G$ be a plain-text message.

   Cipher-text= $(g^{x+x'}h^{y+y'}, g^{x'}h^{y'}m) = (\tau_1, \tau_2) \in G^2$,

   x', y' are random arbitrary integers.
3. Decryption: $m = h^y \tau_1^{-1} g^x \tau_2 \in G$

The BKT scheme can be regarded as the first such scheme to directly utilize non-commutativity of the underlying algebraic systems, not only for defining related cryptographic assumptions but also for hiding messages. In [41], the authors present several attacks against the BKT scheme and propose two novel public-key encryption schemes based on the non-abelian Factorization problems.

Hong et al. [3] in 2006, had proposed two hard problems which they had named as Non-abelian Factoring (NAF) Problem and Non-abelian Inserting (NAI) Problem, to present a brand new public-key encryption scheme.

Definition 15 (Non-abelian Factoring (NAF) Problem [3]). *Let $\mathbb{M} = M_n(p)$ be a semigroup with respect to multiplication operation, and $\mathbb{G} = GL_n(p)$ the general linear group with respect to multiplication operation. Let $R, T \in \mathbb{M}$ $(R \neq T)$ be two random nilpotent matrices. The Factoring Problem with respect to $\mathbb{G}, R, T$, denoted by $NAF_{exp^R, exp^T}^{\mathbb{G}}$, is to factor the given product $exp^{xR} exp^{yT} \in \mathbb{G}$, into a pair $(exp^{xR}, exp^{yT}) \in \mathbb{G}^2$.*

The statement of the problem is quite similar to the Computational Diffie-Hellman Problem in [41].

Definition 16 (Non-abelian Inserting (NAI) Problem [3]). *Let $\mathbb{M} = M_n(p)$ be a semigroup with respect to multiplication operation, and $\mathbb{G} = GL_n(p)$ the general linear group with respect to multiplication operation. Let $R, T \in \mathbb{M}$ $(R \neq T)$ be two random nilpotent matrices. The non-abelian inserting (NAI) problem with respect to $\mathbb{G}, R, T$, denoted by $NAI_{exp^R, exp^T}^{\mathbb{G}}$, is to recover $exp^{(a+c)R} exp^{(b+d)T}$ from the given random pair $(exp^{aR} exp^{bT}, exp^{cR} exp^{dT}) \in \mathbb{G}^2$.*

Eventhough, the problem of computing t for a given $exp^{tX} \in \mathbb{G}$ and $X \in \mathbb{M}$ is solved, the NAF is difficult since R and T are considered to be non-commuting and hence so are the exp^{xR} and exp^{yT}. Furthermore, the choice of sufficiently large p values also contribute to the hardness.
The authors in [42], had suggested several novel intractable conjugated problems related to the Factorization Problem, that can be used as underlying one-way trapdoor problems, namely "Subgroup Conjugator Searching Problem, Subgroup Conjugacy Deciding Problem, Conjugated Computational Diffie-Hellman Problem, Conjugated Decisional Diffie-Hellman Problem" and "Gap Conjugated Computational Diffie-Hellman Problem". The authors have called these as *conjugacy systems* and have proposed an encryption scheme, signature scheme and a signcryption scheme (a data security technology used to protect confidentiality and achieve authenticity) based on them. Moreover, they have recommended future research in the problems of,
Q9. Investigating more efficient platforms for implementing the newly proposed schemes.
Q10. Investigation of possible reductions from the hardness of the related conjugated problems to the hardness of the underlying problems.

5. Membership Search Problem

5.1 Roman'kov's schemes

Vitaly Roman'kov [43] in 2018, had shown general presentations for algebraic cryptographic schemes using two protocols. Many cryptographic schemes that use two sided multiplications in the existing literature are proven to be specific cases of the first general protocol and the author had discussed two instances of Membership Search Problem. He had used an efficient decidability of the problem in an algebraic system to show the vulnerability of both the protocols.
If linear spaces are considered,

Definition 17 (Membership Search Problem (first version)). *Given a linear space V over a field $\mathbb{F}$ and a subspace W, which is given by a basis $W_1, \dots, W_r$, and an element $u \in W$, find the linear representation of the form $u = \sum_{i=1}^{r} \alpha_i w_i, \alpha_i \in \mathbb{F}$.*

If groups are considered,

Definition 18 (Membership Search Problem (second version)). *Given a group G and a subgroup H, given by a generating set $h_1, \dots, h_r$, and an element $g \in H$, find a group word $u(h_1, \dots, h_r)$ such that $g = u(h_1, \dots, h_r)$.*

5.1.1 General scheme 1:

Let G be an algebraic system with associative multiplication (for example, a group). Two communicating parties, say Alice and Bob, choose private-key parameters, $(c, c') = (a, a')$ and $(c, c') = (b, b')$ respectively. They compute and sequentially publish elements of the form $\phi_{c,c'}(f) = cfc'$, where $c, c' \in G$ and $f \in G$ is a previously built element. The exchanged key is,

$$k = \phi_{c_l,c_l'}\left(\phi_{c_{l-1},c_{l-1}'}\left(\dots\left(= \phi_{c_1,c_1'}(g)\right)\right)\right) = c_l c_{l-1} \dots c_1 g c_1' \dots c_{l-1}' c_l'$$

where g is a given element of G $(f = g)$.
A and B are finitely generated subgroups of G used to construct transformations of the form $\phi_{c,c'}$ and $(a, a') \in A$, $(b, b') \in B$. However, the author himself had proven that the security of protocols having the format of general scheme 1 is breakable, without the knowledge of the private-keys, by some natural assumptions.

5.1.2 General scheme 2:

The second general scheme uses endomorphisms or automorphisms and most of the public-key exchange protocols in Algebraic Cryptography that uses automorphisms actually represent specific cases of this general scheme.
Let G be an algebraic system with associative multiplication as before. Establish a set of public elements, $g_1, g_2, \dots, g_k \in G$. Alice and Bob choose private-key parameters $\phi_i \in A$ and $\phi_j \in B$ respectively, where A and B are finitely generated subgroups of $Aut(G)$. Then, they compute and sequentially publish the elements of the form $\phi(f)$, where $f \in G$ is a previously built element and ϕ is the private automorphism. The exchanged key is, $k = \phi_l(\phi_{l-1}(\dots(\phi_1(g))))$, where $g \in G$ is the previously built element.

Shpilrain and Zapata in 2006 [44] had described a cryptosystem based on the computational difficulty of a variant of a Subgroup Membership (Search) Problem.

Definition 19 (Subgroup Membership (Search) Problem). *Given a group G, a subgroup H generated by $h_1, \dots, h_k$ and an element $h \in H$, find an expression of h in terms of $h_1, \dots, h_k$.*

6. Word Problem

Wagner and Magyarik [45] had investigated regarding the Word Problem during a very initial stage of this field of study, viz. around 1984. Even though, it does not give a provably secure, practical cryptosystem, this can be regarded as a very useful opening to the non-abelian group based cryptography during that era.

Definition 20 (Word Problem [46]). *An element of the group is given as the product of generators. One is required to give a method whereby it may be decided in finite number of steps, whether this word is identity or not.*

The Word Problem hold similarities to the Knapsack Problem, in that they both can be viewed as "natural"

problems for public-key cryptosystems [45]. The word problem provides immediate and direct public encryption and difficulty to insert a trapdoor allowing the decryption. A very general and basic approach to handling the Word Problem can be described as below.

Let $G =< x_1, x_2, \dots, x_n | r_1 = e, r_2 = e, \dots, r_m = e >$, where r_i are the relations representing the group G. Let G' be another group obtained by adding more relators, $s_1 = e, s_2 = e, \dots, s_p = e$ to that in G. Then $G' \cong G/N$ [45]. A natural mapping (quotient mapping), $\Omega: G \to G'$ can be defined as follows.

For $x \in G$, let w be any word representing x. Then $\Omega(x)$ is the equivalence class of w within G'. If x and y are equivalent in G, then $\Omega(x)$ and $\Omega(y)$ are equivalent in G'.

For a trapdoor function to work, the $w_1, w_2 \in G$, which will be taken as a part of the public-key must have the property that, $\Omega(w_1)$ and $\Omega(w_2)$ are not equivalent in G'. To decrypt means, to determine which of $\Omega(w_1)$ and $\Omega(w_2)$, a word $\Omega(\mathrm{y})$ is equivalent to. i.e. to solve the Word Problem in G'.

Garzon and Zalcstein [47] had suggested a cryptosystem based on the Word Problem in Grigorchak groups, which can be regarded as a conceptual cryptographic scheme. An attack on this was presented by the authors of [48]. Furthermore, they had analyzed a security issue in another public-key cryptosystem; the Birget-Magliveras-Wei (BMW) cryptosystem [49] which is a cryptosystem based on the logarithmic signatures.

In [50], Grigorchuk had presented a very general construction to transform any one-way infinite sequence of a 4-generator group in to Word Problem. Literally, he had aquired this result during an investigation regarding the question, whether every finitely generated group has polynomial or exponential growth. An interesting further research direction would be to,

Q11. [48] Investigate the well studied instances of the Word Problem in finitely presented groups for cryptographic applications.

7. Logarithmic signatures

Another interesting atypical invention related to non-abelian group based Cryptography is the so called Logarithmic signature. This gives another way to generalize the conventional DLP. We will not go to an in-depth discussion on this topic, since [5] presents a detailed review.

Definition 21. Let G be a finite group and $S \subset G$ be a subset of G and s, be a positive integer. Let $A_i = [\alpha_{i1}, \dots, \alpha_{ir_i}]$ be a finite sequence of elements of G of length $r_i > 1$, for all $1 \leq i \leq s$, $\alpha = [A_1, \dots, A_s]$ be the ordered sequence of A_i. α is called a cover for S if any $h \in S$ can be written as a product $h = h_1 \dots h_s$, where $h_{\alpha_{ik_i}} \in A_i$. When such a decomposition is unique for every $g \in S$, then α is defined to be a "Logarithmic signature" for S.

Magliveras, Stinson and Trung [51] had developed the well-known MST_1 and MST_2 cryptosystems using the Logarithmic signatures based on the finite permutation groups. A MST_3 cryptosystem based on the Suzuki 2-groups was later proposed by Lempkun et al. [52]. An inspiring challenge to confront by the new researchers is the following problem.

Q12. Explore the potential of Logarithmic signatures for finite groups as a basis for practical and secure public-key encryption schemes.

The Cramer-Shoup cryptosystem is a generalization of the El-Gamal key exchange problem, which is provably secure against adaptive chosen cipher-text attacks. This scheme, which utilizes the basic concepts of the RSA assumption has been the limelight of many studies during the era. An extension of the Cramer-Shoup scheme to non-abelian groups was discussed by Kahrobaei and Anshel in 2013. See [53] for explicit details.

Moreover, Kahrobaei and Khan [19] had proposed another interesting generalization of El-Gamal key exchange over polycyclic groups using conjugates.

8. Future research: using Hamiltonian cycles/paths in Cayley graphs for Cryptography

A Hamiltonian path is a path which visits every vertex of a graph exactly once. When there is an edge between the starting and the ending vertices, it is known as a Hamiltonian cycle. Finding a Hamiltonian cycle or a path in most of the graphs is considered as one of the most difficult mathematical problems and is known as the Hamiltonian Cycle Problem (HCP) or the Hamiltonian Path Problem (HPP) respectively.

A Cayley graph is a type of a vertex-transitive graphs which can encode the abstract structures of groups clearly and faithfully. This property of Cayley graphs is extremely useful in studying group structures visually. A vertex-transitive graph is a graph X, where for any two vertices $v_1, v_2 \in V(X)$, there exists an automorphism of X which maps v_1 to v_2 ($V(X)$ is the set of vertices of X).

The RSA assumption is one of the most important concepts in the field of Cryptography. The RSA assumption can be written as "it is computationally difficult to find a non-trivial relation in the RSA group, $(\mathbb{Z}/pq\mathbb{Z})^*$ ".

Cycles in a Cayley graph correspond to relations among generating elements of the graph. Hence, the problem of finding Hamiltonian cycles in a Cayley graph correspond to a problem of finding non-trivial relationships between the generating elements of a graph. Moreover, if the product of a sequence of elements corresponding to a Hamiltonian path is considered, it becomes equal to another element in the group. A sequence of generating elements raised to integer

valued exponents, representing a Hamiltonian cycle or a Hamiltonian path can act as a good secret key for a communicating party.

By viewing the notion of the RSA assumption in relation with the difficulty of finding Hamiltonian cycles in Cayley graphs, a variant of the RSA assumption can be stated as follows.

"It is computationally difficult to find a non-trivial relation in the Cayley graph of a finite group which optimizes conditions corresponding to a Hamiltonian cycle".

It can be expected that the cryptographic protocols built upon assumptions like above, are more stronger and better due to the use of non-abelian groups (in abelian groups Hamiltonian Cycle/Path Problem are not difficult) and the very strong assumption based on the difficulty of finding Hamiltonian cycles/paths in Cayley graphs.

9. Conclusion

Many researches in the field of Modern Cryptography have been attracted towards non-abelian group based cryptosystems, due to the presence of more complex algebraic structures and the expectation that they will offer higher security when confronted with Quantum Computational approaches. Mathematically hard problems giving rise to one-way trapdoor functions in non-abelian groups have been studied and extended to different variants of the traditional cryptographic assumptions such as the DLP. The most common future research directions for all the non-abelian group based cryptosystems are,

Q13. Investigate more suitable platform groups for the execution of the respective cryptographic protocols.

Q14. Analysis and discovery of methods to improve the security and efficiency of the protocols.

We propose the Hamiltonian Cycle/Path Problem, particularly in Cayley graphs as a suitable intractable problem for future studies with relevant to development of novel public-key cryptosystems.

Acknowledgements

We would like to express our warm thanks to the Editor and the Reviewers of the open access journal IJCSNS, for their kind comments and support during the publication of this manuscript.

References

[1] G. H. J. Lanel, H. K. Pallage, J. K. Ratnayake, S. Thevasha, and B. A. K. Welihinda, "A survey on Hamiltonicity in Cayley graphs and digraphs on different groups," Discrete Math. Algorithms Appl., vol. 11, no. 05, p. 1930002, 2019, doi: 10.1142/s1793830919300029.

[2] G. H. J. Lanel, T. M. K. K. Jinasena, and B. A. K. Welihinda, "Hamiltonian Cycles in Cayley Graphs of Semidirect Products of Finite Groups," Eur. Mod. Stud. J., vol. 04, no. 03, pp. 1–19, 2020.

[3] H. Hong, J. Shao, L. Wang, H. Ahmad, and Y. Yang, "Public Key Encryption in Non-Abelian Groups," ArXiv Prepr. ArXiv160506608, 2016.

[4] B. Fine, M. Habeeb, D. Kahrobaei, and G. Rosenberger, "Aspects of nonabelian group based cryptography: a survey and open problems," JP J. Algebra Number Theory Appl., 2011.

[5] T. C. Lin, "A study of non-abelian public key cryptography," Int. J. Netw. Secur., vol. 20, no. 2, pp. 278–290, 2018.

[6] R. Cramer and V. Shoup, "Signature schemes based on the strong RSA assumption," ACM Trans. Inf. Syst. Secur. TISSEC, vol. 3, no. 3, pp. 161–185, 2000, doi: 10.1145/357830.357847.

[7] I. Ilic, "The Discrete Logarithm Problem in Non-abelian Groups," Computing, vol. 1, p. 1, 2010.

[8] I. Anshel, M. Anshel, B. Fisher, and D. Goldfeld, "New key agreement protocols in braid group cryptography," 2001, pp. 13–27, doi: 10.1007/3-540-45353-9_2.

[9] I. Anshel, M. Anshel, and D. Goldfeld, "Non-abelian key agreement protocols," Discrete Appl. Math., vol. 130, no. 1, pp. 3–12, 2003, doi: 10.1016/s0166-218x(02)00585-1.

[10] D. Grigoriev and I. Ponomarenko, "Constructions in public-key cryptography over matrix groups," ArXiv Prepr. Math0506180, 2005, doi: 10.1090/conm/418/07949.

[11] I. Ilic and S. S. Magliveras, "Weak discrete logarithms in non-abelian groups," J. Comb. Math. Comb. Comput., vol. 74, p. 3, 2010.

[12] L. C. Klingler, S. S. Magliveras, F. Richman, and M. Sramka, "Discrete logarithms for finite groups," Computing, vol. 85, no. 1–2, p. 3, 2009, doi: 10.1007/s00607-009-0032-0.

[13] A. Mahalanobis, "The Diffie-Hellman key exchange protocol and non-abelian nilpotent groups," Isr. J. Math., vol. 165, no. 1, pp. 161–187, 2008, doi: 10.1007/s11856-008-1008-z.

[14] I. Anshel, M. Anshel, and D. Goldfeld, "An algebraic method for public-key cryptography," Math. Res. Lett., vol. 6, no. 3, pp. 287–291, 1999, doi: 10.4310/mrl.1999.v6.n3.a3.

[15] K. H. Ko, S. J. Lee, J. H. Cheon, J. W. Han, J. S. Kang, and C. Park, "New public-key cryptosystem using braid groups," 2000, pp. 166–183, doi: 10.1007/3-540-44598-6_10.

[16] J. Birman, "Braids, links, and mapping class groups, volume 82 of Annals of Math," Stud. Princet. Univ. Press, 1974, doi: 10.1515/9781400881420.

[17] P. Dehornoy, "Braid-based cryptography," Contemp Math, vol. 360, pp. 5–33, 2004, doi: 10.1090/conm/360/06566.

[18] V. Shpilrain and G. Zapata, "Combinatorial group theory and public key cryptography," Appl. Algebra Eng. Commun. Comput., vol. 17, no. 3–4, pp. 291–302, 2006, doi: 10.1007/s00200-006-0006-9.

[19] I. S. Lee, W. H. Kim, D. Kwon, S. Nahm, N. S. Kwak, and Y. J. Baek, "On the security of MOR public key cryptosystem," 2004, pp. 387–400.

[20] S. H. Paeng, "On the security of cryptosystem using automorphism groups," Inf. Process. Lett., vol. 88, no. 6, pp. 293–298, 2003, doi: 10.1016/j.ipl.2003.09.001.

[21] C. Tobias, "Security analysis of the MOR cryptosystem," 2003, pp. 175–186.

[22] A. Mahalanobis, "A simple generalization of the ElGamal cryptosystem to non-abelian groups," Commun. Algebr., vol.

36, no. 10, pp. 3878–3889, 2008, doi: 10.1080/00927870802160883.
[23] A. Mahalanobis, "A note on using finite non-abelian p-groups in the MOR cryptosystem," ArXiv Prepr. Cs0702095, 2007.
[24] A. Mahalanobis, "A simple generalization of the ElGamal cryptosystem to non-abelian groups II," Commun. Algebra, vol. 40, no. 9, pp. 3583–3596, 2012, doi: 10.1080/00927872.2011.602998.
[25] W. Magnus, A. Karrass, and D. Solitar, Combinatorial group theory: Presentations of groups in terms of generators and relations. Courier Corporation, 2004.
[26] G. Baumslag, Topics in combinatorial group theory. Birkhäuser, 2012.
[27] A. I. S. Moldenhauer and G. Rosenberger, "Cryptosystems using automorphisms of finitely generated free groups," ArXiv Prepr. ArXiv160302328, 2016.
[28] S. H. Paeng, K. C. Ha, J. H. Kim, S. Chee, and C. Park, "New public key cryptosystem using finite non Abelian groups," 2001, pp. 470–485, doi: 10.1007/3-540-44647-8_28.
[29] C. Bates, N. Meyer, and T. Pulickal, "Cryptographic applications of nonabelian groups," Math Ariz. Edu Asp2008crypto Pdf, 2008.
[30] M. Cohen, S. Flannery, and D. Flannery, "In Code: A Mathematical Journey, by Sarah Flannery and David Flannery," Am. Math. Mon., vol. 109, no. 10, p. 929, 2002, doi: 10.2307/3072480.
[31] R. Álvarez, L. Tortosa, J. Vicent, and A. Zamora, "A non-abelian group based on block upper triangular matrices with cryptographic applications," 2009, pp. 117–126, doi: 10.1007/978-3-642-02181-7_13.
[32] R. Álvarez, F. M. Martinez, J. F. Vicent, and A. Zamora, "A new public key cryptosystem based on matrices," WSEAS Inf. Secur. Priv., vol. 3639, 2007.
[33] R. Álvarez, L. Tortosa, J. F. Vicent, and A. Zamora, "Analysis and design of a secure key exchange scheme," Inf. Sci., vol. 179, no. 12, pp. 2014–2021, 2009, doi: 10.1016/j.ins.2009.02.008.
[34] J. J. Climent, E. Gorla, and J. Rosenthal, "Cryptanalysis of the CFVZ cryptosystem," Adv. Math. Commun., vol. 01, no. 01, pp. 1–11, 2007, doi: 10.3934/amc.2007.1.1.
[35] H. K. Pathak and M. Sanghi, "Public key cryptosystem and a key exchange protocol using tools of non-abelian group," IJCSE Int. J. Comput. Sci. Eng., vol. 2, no. 04, pp. 1029–1033, 2010.
[36] A. J. Menezes and Y. H. Wu, "The discrete logarithm problem in GL (n, q)," Ars Comb., vol. 47, pp. 23–32, 1997.
[37] E. Stickel, "A new public-key cryptosystem in non abelian groups," 2004, pp. 70–80.
[38] V. Shpilrain, "Cryptanalysis of Stickel's key exchange scheme," in Computer Science - Theory and Applications, 2008, pp. 283–288, doi: 10.1007/978-3-540-79709-8_29.
[39] L. Wang, L. Wang, Z. Cao, E. Okamoto, and J. Shao, "New constructions of public-key encryption schemes from conjugacy search problems," in Information Security and Cryptology, 2010, pp. 1–17, doi: 10.1007/978-3-642-21518-6_1.
[40] S. Baba, S. Kotyad, and R. Teja, "A non-Abelian factorization problem and an associated cryptosystem.," IACR Cryptol EPrint Arch, vol. 2011, p. 48, 2011.
[41] L. Gu, L. Wang, K. Ota, M. Dong, Z. Cao, and Y. Yang, "New public key cryptosystems based on non-Abelian factorization problems," Secur. Commun. Netw., vol. 6, no. 7, pp. 912–922, 2013, doi: 10.1002/sec.710.
[42] L. Gu and S. Zheng, "Conjugacy systems based on nonabelian factorization problems and their applications in cryptography," J. Appl. Math., vol. 2014, 2014, doi: 10.1155/2014/630607.
[43] V. Roman'kov, "Two general schemes of algebraic cryptography," Groups Complex. Cryptol., vol. 10, no. 2, pp. 83–98, 2018, doi: 10.1515/gcc-2018-0009.
[44] V. Shpilrain and G. Zapata, "Using the subgroup membership search problem in public key cryptography," Contemp. Math., vol. 418, p. 169, 2006, doi: 10.1090/conm/418/07955.
[45] N. R. Wagner and M. R. Magyarik, "A public-key cryptosystem based on the word problem," 1984, pp. 19–36, doi: 10.1007/3-540-39568-7_3.
[46] M. Dehn, "Over infinite discontinuous groups," Math. Ann., vol. 71, no. 1, pp. 116–144, 1911.
[47] M. Garzon and Y. Zalcstein, "The complexity of Grigorchuk groups with application to cryptography," Theor. Comput. Sci., vol. 88, no. 1, pp. 83–98, 1991, doi: 10.1016/0304-3975(91)90074-c.
[48] M. I. G. Vasco, D. Hofheinz, C. Martínez, and R. Steinwandt, "On the security of two public key cryptosystems using non-abelian groups," Des. Codes Cryptogr., vol. 32, no. 1, pp. 207–216, 2004, doi: 10.1023/b:desi.0000029223.76665.7e.
[49] J. C. Birget, S. S. Magliveras, and W. Wei, "Trap doors from subgroup chains and recombinant bilateral transversals," Proc. RECSI, vol. 7, pp. 31–48, 2002.
[50] R. I. Grigorchuk, "Degrees of growth of finitely generated groups, and the theory of invariant means," Izv. Ross. Akad. Nauk Seriya Mat., vol. 48, no. 5, pp. 939–985, 1984, doi: 10.1070/im1985v025n02abeh001281.
[51] T. Van Trung, Magliveras, and Stinson, "New approaches to designing public key cryptosystems using one-way functions and trapdoors in finite groups," J. Cryptol., vol. 15, no. 4, pp. 285–297, 2002, doi: 10.1007/s00145-001-0018-3.
[52] W. Lempken, T. Van Tran, S. S. Magliveras, and W. Wei, "A public key cryptosystem based on non-abelian finite groups," J. Cryptol., vol. 22, no. 1, pp. 62–74, 2009, doi: 10.1007/s00145-008-9033-y.
[53] D. Kahrobaei and M. Anshel, "Decision and search in non-abelian Cramer-Shoup public key cryptosystem," Groups Complex. Cryptol., vol. 1, no. 2, pp. 217–225, 2009, doi: 10.1515/gcc.2009.217.

Dr. G. H. J. Lanel
(******corresponding author*) is a Senior Lecturer at the Department of Mathematics, University of Sri Jayewardenepura, Sri Lanka. He has received B. Sc. (Special) degree in Mathematics from the Open University, Sri Lanka. Furthermore, he has received M. Sc. in Industrial Mathematics and Ph. D. in Mathematics degrees from the University of Sri Jayewardenepura, Sri Lanka and the Oakland University, Rochester, Michigan, respectively. His research interests lie in Computer Algebra/Symbolic Mathematics, Graph Theory/Computational Discrete Mathematics, Queuing Theory, and Operational Research. His mathematical expertised areas are Computer Algebra, Graph Theory, Algorithmic Analysis, Engineering Mathematics, and Numerical Analysis.

Dr. T. M. K. K. Jinasena
(*author*) is a Senior Lecturer at the Department of Computer Science, University of Sri Jayewardenepura, Sri Lanka. He has received the B. Sc. (Special) degree in Computer Science from the same university and Bachelor of Information Technology, M. Sc. in Computer Science degrees from the University of Colombo, Sri Lanka. He has completed the Ph. D. degree in Computer Science at the University of Sri Jayewardenepura. His research interests include Robotics, Embeded Systems, Artificial Inteligence, Image Processing, Datamining, Mobile Computing and Computer Security.

Miss. B. A. K. Welihinda
(*author*) received the B. Sc. (Special) degree in Mathematics from the university of Sri Jayewardenepura, Sri Lanka. After working as a Mathematics Instructor/Demonstrator, Research Assistant and a Lecturer (Probationary), she is currently following the Ph. D. degree in Mathematics at the Department of Mathematics in the same university. Her research interests include Algebraic Graph Theory, Group Theory and Cryptography.