ISSN: 0975-766X
CODEN: IJPTFI
Available through Online *Review Article*
www.ijptonline.com

A REVIEW ON CONJUGACY PROBLEMS USED IN VARIOUS SCHEMES OF CRYPTOGRAPHY

D.Ezhilmaran and V.Muthukumaran*
School of Advanced Sciences, VIT University, Tamilnadu, India-632014.
Emails:ezhil.devarasan@yahoo.com and muthu.v2404@gmail.com

Received on 05-02-2016 *Accepted on 29-02-2016*

Abstract

The conjugacy search problem in a group G is the problem of recovering an $x \in G$ from given $g \in G$ and $h = x^{-1}gx$. Ko et al. proposed a new public key cryptosystem on braid groups based on the hardness of the conjugacy problem. The foundation of this system is quite different from widely used cryptosystems on number theory, even if there are some similarities in design. Most of the authentication and signature schemes, such as digital signature scheme, blind signature scheme, proxy blind signature, Zero-knowledge Undeniable Signature Scheme which are based on conjugacy problem are computationally hard. In this article, we review the different types of conjugacy problems used in the various schemes of cryptography.

Keywords: Conjugacy problem, key exchange protocol, authentication, signature scheme.

1. Introduction

Most public-key cryptosystems that remain unbroken are based on the perceived difficulty of solving certain problems in large finite (abelian) groups. The theoretical foundations of these cryptosystems are related to the intractability of problems that are closer to number theory than to group theory [1].

In a quantum computer, most of these problems on number theory can be efficiently solved by using algorithms developed by Shor[2], Kitaev[3] and Proos-Zalka[4] .Although the quantum computation is still in its infancy, the knowledge regarding their potential will soon create distrust in the current cryptographic methods.

In order to enrich cryptography and not to put all eggs in one basket [5], many attempts have been made to develop alternative public-key cryptography (PKC) based on different kinds of problems[1,5-7].

Under this background, some noncommutative groups have been attracted considerable attentions. One of the most popular groups in this category is the braid group. In 1999, Anshel et al. [6] proposed an algebraic method for PKC. Shortly afterward, Ko et al [7]. Published a fully-fledged encryption scheme using braid groups. In these schemes, the conjugacy search problem (CSP) and its variants play a core role. Although there is no deterministic polynomial algorithms that can solve the CSP problem over braid groups [8] till now, many heuristic attacks, such as length-based attacks, linear representation attacks, have obtained remarkable success in attacking braid-based cryptosystems and lowered the initial enthusiasm on this subject.

The asymmetric cryptographic primitives remaining unbroken are based on the perceived intractability of certain mathematical problems in very large, finite, abelian groups, in particular representations. Prominent hard problems are the factorization problem and the Discrete Logarithm Problem (DLP) [9]. Unfortunately, in view of P. Shor's quantum algorithms for integer factoring, and solving the DLP, the known public-key systems will be insecure when quantum computers become practical. A recent report edited by P.Nguyen identifies these and other problems facing the field of information security in the future. It is natural to try to generalize these primitives to non-abelian groups, not only because the current systems are facing potential menace, but also there is an interesting academic adventure in trying to do so. One of the most obvious ramifications of the discrete logarithm problem in the non-commutative situation is the conjugacy search problem (CSP). Given a group G and two conjugate elements $g, h \in G,$ find a particular element $x \in G$ such that $h = x^{-1}gx.$

This problem always has a recursive solution because one can recursively enumerate all conjugates of a given element, but this kind of solution can be extremely inefficient. Specific groups may or may not admit more efficient solutions, so the choice of the platform group is of paramount importance for security of a cryptographic primitive based on the conjugacy search problem. Mahalanobis [10] studied a key exchange protocol similar to the Diffie-Hellman key exchange protocol, using abelian subgroup of the automorphism group of a non-abelian nilpotent group, and offered a signature scheme based on the conjugacy search problem.

Guangguo Han et al [11] proposed a generalization of the digital signature algorithms DSA whose security is based on the hardness of the conjugacy search problem. Girraj Kumar Verma [12] proposed two blind signature schemes over Braid groups. The foundation of construction is conjugacy search problem in braid groups. Grigoriev and Shpilrain [13]

proposed the authentication scheme from a matrix conjugation, the security of which rests on the difficulty assumption for solving the conjugacy search problem (CSP) in the noncommutative monoid of matrices of truncated polynomial over a ring. This platform seems to be the first serious candidate for the platforms that have a generically hard CSP problem.

WANG Licheng et al.[14] the state of the art of braid cryptography is surveyed, and then a new cryptographic problem conjugate adjoining problem related to braid groups is proposed. Based on this problem, we design a new braid-based signature scheme. This scheme is efficient and provably secure in the random oracle model. Tony Thomas and Arbind Kumar Lal [15] present a zero-knowledge undeniable signature scheme based on the hardness of the conjugacy problem in non-abelian groups. Licheng Wang et al. [16] prompt a new kind of braid-based assumption one-more matching conjugate assumption; and then based on it, Authors prove that some braid based signatures are EUF-CMA secure in the random oracle model. Atul Chaturvedi and Sunder Lal [17] proposed a new authenticated key agreement protocol, called AKAP. Their protocol makes use of the fact that the CSP is hard in the braid group. Sunder Lal and Vandani Verma proposed a proxy signature scheme with delegation by warrant using conjugacy search problem over the braid groups.

The rest of the paper is organized as follows in Section 2 we recall the some basic schemes using conjugacy problem. Section 3 we recall some basic definition and types of conjugacy problem Section 4 we discuss the overall conjugacy problem in cryptography, and section 5 concludes the article.

2. Analysis of conjugacy problem in cryptography

2.1. Authentication scheme

Atul Chaturvedi and Sunder Lal [17] proposed an authenticated key agreement, which works in a braid group and authors prove that our protocol meet the security attributes under the assumption that the Conjugacy Search Problem (CSP) is hard in braid group. His scheme is secure against many well know attacks on protocols.

Vladimir Shpilrain and Alexander Ushakov [8] have introduced an authentication scheme based on the (double) twisted conjugacy problem, a new problem, which is allegedly hard in some (semi)groups. A new platform semigroup, namely the semigroup of all 2×2 matrices over truncated one-variable polynomials over F2.

Computation in this semigroup is very efficient and, at the same time, the non-commutative structure of this semigroup provides for security at least against obvious attacks. We point out here one important advantage of using the (double)

twisted conjugacy problem over using a more "traditional" conjugacy search problem as far as (semi)groups of matrices are concerned. The conjugacy search problem admits a linear algebra attack upon rewriting the equation $x^{-1}gx = h$ as $gx = hx$ the latter translates into a system of n^2 linear equations with n^2 unknowns, where n is the size of the matrices involved, and the unknowns are the entries of the matrix x. Of course, if the entries come not from a field but from a more general ring, such a system of linear equations does not necessarily admit a straightforward solution, but methods emulating standard techniques (like Gauss elimination) usually have a pretty good success rate anyway. For the twisted conjugacy problem, however, there is no reduction to a system of linear equations. Authors have considered an attack based on reducing the twisted conjugacy problem to a system of polynomial equations over F2, but this attack becomes computationally infeasible even with a much smaller crucial parameter.

Patrick Dehornoy Conjugacy is not the only possible primitive for designing braid based protocols. To illustrate this principle, we describe a Fiat–Shamir-style authentication protocol that be can be implemented using any binary operation that satisfies the left self-distributive law. Conjugation is an example of such an operation, but there are other examples, in particular the shifted conjugation on Artin's braid group B_∞ and the finite Laver tables. In both cases, the underlying structures have a high combinatorial complexity, and they lead to difficult problems. Discussed various non-classical algebraic operations that could possibly be used as cryptographical primitives, typically for a Fiat–Shamir-like authentication scheme. The most promising example seems to be the shifted conjugacy operation on braids. At the least, the existence of such an operation shows that conjugacy is not the only possible primitive for braid-based cryptography, and that further investigation in this direction is needed.

Jonathan Longrigg and Alexander Ushakov [24] modify the technique of cyclic permutations to work with the shifted conjugacy problem. We apply this technique to design a heuristic attack on the cryptographic authentication scheme based on shifted conjugacy of braids proposed by Dehornoy and report experimental results. Jonathan Longrigg and Alexander Ushakov present the first practical attack on the shifted conjugacy-based authentication protocol proposed by P. Dehornoy. Author's discussed the weaknesses of that primitive and proposes ways to improve the protocol.

M.M. Chowdhury [25] gives a new two-pass authentication scheme, which is a generalization of an authentication scheme of Sibert-Dehornoy-Girault based on the Diffie-Hellman conjugacy problem. Compared to the above scheme, for some parameters it is more efficient with respect to multiplications. Author sketch a proof that our authentication scheme is

secure. Guangguo Han and Chuangui Ma using Miller group G as the platform, authors propose a generalization of Schnorr's authentication and signature scheme whose security is based on the hardness of the conjugacy search problem. By the assumption of the hardness of CSP, the authentication and signature scheme offered by the authors is secure.

2.2. Signature scheme

Girraj Kumar Verma [29] proposed a proxy blind signature scheme using conjugacy search problem over braid groups. His proxy blind signature scheme is partial delegated protected proxy signature. Although we have not discussed the efficiency of our schemes none the less our schemes proposed a new setting for constructing protocols for delegating signing rights. Tony Thomas and Arbind Kumar Lal [15] use the conjugacy problem in non-abelian groups to construct a zero-knowledge undeniable signature scheme. They Suggested some potential non-abelian groups in which the above digital signature scheme can be implemented. The security of author's scheme is depending upon the conjugacy problem in non-abelian groups. It is worth reformulating these protocols by employing other hard problems in non-abelian groups like the decomposition problem. There are many desirable features for good undeniable signatures like convertibility, delegation. We have not considered these problems in this paper. It is worth constructing protocols for these cases in the non-abelian group settings.

Wang Licheng, et al. [14] the state of the art of braid cryptography is surveyed, and then a new cryptographic problem conjugate adjoining problem related to braid groups is proposed. Based on this problem, we design a new braid-based signature scheme. This scheme is efficient and provably secure in the random oracle model. Further, we present the comparison between braid-based signatures and RSA-based ones. The signing process of the braid-based schemes is more efficient than that of RSA-based ones, while the verifying process of the braid-based ones is observably slow. Hence, braid-based signatures are suitable for scenarios where the signing process has to be as quick as possible but delays are permitted in the verifying process, for example, in off-line e-cash systems.

The key sizes in braid-based schemes are considerably large about 2K bits in the case of secret keys and 12K bits in the case of public keys. However, braid operations are much simpler and more efficient than modular exponential operations. Therefore, braid-based schemes can be embedded into devices with low computational ability and large memory space. The capability of braid cryptosystems to resist currently known quantum attacks is also discussed from the perspective of hidden subgroup problems.

Licheng Wang, et al. [31] purpose to enhance the security of the braid based signatures; we have proposed a new type of braid based assumption, i.e., one-more matching conjugate assumption. Based on this new assumption, we have proved that both Ko et al.' simple conjugacy signature scheme and Ding et al.'s enhanced scheme can reach the highest security, i.e., existential unforeability against adaptively chosen message attack (EUF-CMA) in the random oracle model. As far as we know, it is the first time to conclude the security of some braid-based signatures to EUF-CMA level.

Ki Hyoung Ko, et al. [19] proposed a new digital signature scheme based on a non-commutative group where the conjugacy search problem is hard and the conjugacy decision problem is feasible. Authors implement our signature scheme in the braid groups and prove that an existential forgery of the implementation under no message attack gives a solution to a variation of conjugacy search problem and discuss performance of our scheme under suggested parameters.

Sunder Lal and Vandani Verma [32] have proposed a proxy signature scheme with delegation by warrant using conjugacy search problem over the braid groups. Firstly, authors proposed our proxy signature scheme that includes the warrant with the signatures that restricts the proxy signer to create the valid proxy signatures for a certain period of time and he discuss designated verifier and bi-designated verifier signature schemes. Finally, authors added these two concepts of proxy signatures and designated verifier signatures and bi-designated verifier signatures. The security of our schemes is based on the conjugacy problem of braid groups. To the best of our knowledge these are first signature schemes of this type defined over braid groups.

2.3. Conjugacy problem in key exchange protocol

Jung Hee Cheon and Byungheup Jun [27] propose the first polynomial time algorithm for the braid Diffie-Hellman conjugacy problem (DHCP) on which the braid key exchange scheme and the braid encryption scheme. a polynomial time algorithm to solve the DHCP in braid groups. Though the complexity is too large to break the encryption scheme with the proposed parameters in real time, the braid encryption scheme is considered to be insecure since increasing the key size increase the attack complexity only a little.

Ko-Kyu Lee1etal [23] extend the 2-party key exchange protocol on braid groups to the group key agreement protocol based on the hardness of Ko-Lee problem. Authors also provide authenticity to the group key agreement protocol.

Ping Pan et al. [33] propose a new public-key cryptosystem named conjugacy search problem-based Diffie–Hellman integrated encryption scheme (CSP-DHIES), by using conjugation-related assumptions for a special monoid of matrices

of truncated multi-variable polynomials over the ring Z_{12} where the CSP is assumed to be intractable. Our construction can be viewed as the first noncommunicative variant of the well-known DHIES cryptosystem. Under the assumptions of the intractability of the CSP-based hash Diffie–Hellman problem and the CSP-based oracle Diffie–Hellman problem, our scheme is provably secure against both chosen-plaintext attacks and secure against chosen-ciphertext attacks. Our proofs are constructed in the standard model. We also discuss the possibility of implementing our proposal using braid groups. Authors reviewed the well-known Diffie–Hellman integrated encryption scheme (DHIES) defined over cyclic groups. Under the intractability assumption of the CSP for a special monoid of matrices over truncated multi-variable polynomials over the ring Z12, we developed some related cryptographic assumptions, including the CSP-based HDH assumption and the CSP-based ODH assumption. We then constructed a CSP-based DHIES variant that is proven to be secure in the standard model. As far as we know, this is the first noncommutative variant of DHIES. Considering that the DLP is vulnerable to existing quantum attacks and there is no known quantum algorithm for solving the CSP problem over the suggested platform, our proposal may be an effective alternative in the post-quantum era.

Volker Gebhardt[35] demonstrate that recent advances in the theory of braid groups, in particular a new invariant of conjugacy classes of braids, the ultra-summit set, make some braid-based cryptographic protocols insecure for almost all randomly chosen keys. As part of this we present an overview of the known algorithms for solving the conjugacy decision and search problems in braid groups and an assessment of their practical performance from the point of view of braid-based cryptography. Licheng Wang, et al. [34] proposed new cryptosystems based on self-distributive systems that are defined by Conjugator searching problems (CSP) in noncommutative groups. Under certain assumptions, the Ciphertext of our basic construction are proven indistinguishable against chosen plaintext attacks (IND-CPA) in the standard model, and two extended schemes achieve the IND-CCA security in the random oracle model. Then, our proposal is instantiated with braid groups, and leads to a new braid-based encryption scheme that is directly based on the intractability assumption of CSP in braid groups. Furthermore, authors quote an analysis to manifest that our newly derived braid-based cryptosystem has the potential to resist currently known quantum attacks. Juha Partala and Tapio Seppanen give a formulation of the CSP for left conjugacy closed loops. In order to construct a generalization of the Anshel-Anshel-Goldfeld key establishment method, we also define a partial conjugacy search problem PCSP and show it to be equivalent to the CSP, if the underlying structure is a group. We also study closer the PCSP in a class of conjugacy closed loops of

order P^2, where P is a prime. D.B.Ojha, et al.[35] elaborated the process for well secured and assured for sanctity of correctness about the sender's and receiver's identity , as non- repudiable biased bitstring key agreement protocol (NBBKAP) using conjugacy problem in non-abelian group. Non-repudiable key agreement protocols are an essential part of secure e-gaming and e-gambling protocols. In fact, such protocols are a guarantee that player misbehaviours or deviations from the protocols will be detected. Using the new primitive, one party is allowed to agree on the same value to both party with a given, fixed bias while the basic bitstring can be viewed as special case when the bias value is set to 1/ 2. Using a public key cryptosystem to construct a shared key is away of achieving non-repudiability, a property which cannot be offered by hash functions alone. The author presented a non-repudiable biased bitstring key agreement protocol that allows both players to share a bitstring in a non-repudiable way based on the braid conjugator search problems with 1/ *k* –biased bitstring. Hence, our proposed scheme is well secured and assured for sanctity of correctness about the sender's and receiver's identity.

3. Preliminaries

In this section we discuss the basic definition of the conjugacy problem and types of conjugacy problem in the various schemes.

3.1. Conjugacy problem

In a non-commutative group $G,$ two elements x, y are conjugate, written x~y if $y = zx^{-1}z$ for some $z \in G$. Here z or z^{-1} is called a conjugator. Over a non-commutative group $G,$ we can define the following cryptographic problems which are related to conjugacy.

Conjugacy search problem (CSP): Given $(x, y) \in G \times G,$ $_{\text{find}}$ $z \in G$ such that $y = zx^{-1}z$.

Decomposition problem (DP): Given $(x, y) \in G \times G,$ $_{\text{and}}$ $S \subseteq G$ find $z_1, z_2 \in S$ such that $y = z_1 x z_2$

At present, author believes that for general non-commutative group G, both of the above problems are difficult enough to be cryptographic assumptions. That is, the CSP (DP, respectively) assumption says that CSP (DP, respectively) is intractable. More precisely, the CSP (DP, respectively) assumption states that there does not exist probabilistic polynomial time algorithm which can solve CSP (DP, respectively) with non-negligible accuracy with respect to problem scale, i.e., the number of input bits of the problem

3.2. Conjugacy problem in braid groups

Conjugacy search problem (CSP)

Instance: $(x, y) \in B_n \times B_n$ such that $y = a^{-1}xa$ for some $a \in B_n$.

Objective: Find $b \in B_n$ such that $y = b^{-1}xb$.

Conjugacy Decision Problem (CDP)

Instance: $(x, y) \in B_n \times B_n$ such that $y = a^{-1}xa$ for some $a \in B_n$.

Objective: Determine whether *x* and *y* are conjugate or not.

Generalized Conjugacy search problem (GCSP)

Given $(x, y) \in B_n \times B_n$ such that $y = a^{-1}xa$ for some $a \in B_n$; $m \le n$ .find $b \in B_n$ such that $y = b^{-1}xb$

Conjugacy Decomposition Problem (CDP)

Given $(x, y) \in B_n \times B_n$ such that $y = a^{-1}xa$ for some $a \in B_w$. Find $b_1, b_2 \in B_n$ such that $y = b_1 x b_2$

Shifted Conjugacy Search Problem

Assuming that s, p are braids in B_∞ and $p' = s * p$ holds, find a braid $\tilde{s}$ satisfying $p' = \tilde{s} * p$.

Twisted conjugacy problem

Given a pair of endomorphism's, φ, ψ of a group G and a pair of elements $\omega, t \in G,$ find an element $s \in G$ such that $t = \varphi(s^{-1})\omega\varphi(s)$ provided at least one such s exists.

Conjugate adjoining problem in braid groups

Given a triple $(p, q, c) \in B_n^3$ under the condition that $q = \omega^{-1}p\omega$ and $c \neq \langle p \rangle$ hold for some unknown braid $\omega \in B_n$, find some braid $r \in B_n$ such that $r = \omega^{-1}pc\omega$ holds. The geometric meaning of CAP is to adjoin p and c under certain conjugate condition.

Multiple conjugacy search problem

Given words $a_1, \ldots, a_m, b_1, \ldots, b_m \in V_n$ such that $b_i = x^{-1}a_i x$ for some $x \in V_n$ and all $i = 1, 2, \ldots, m,$ find $x' \in V_n$ such that $b_i = x'^{-1} a_i x'$ for all i .

Multiple Simultaneous Conjugacy Problems

Given the r-tuples $(a_1,\ldots,a_r)$ and $(x^{-1}a_1x,\ldots,x^{-1}a_rx)$ in B_n, find the conjugator x.

3.3. Braid Diffie-Hellman Conjugacy Problem

Let *G* be a non-abelian group and $u,a,b,c \in G$. In order to perform the Diffie-Hellman key agreement on *G* we need to choose a,b in *G* satisfying $ab=ba$ in the DHCP. Hence we introduce two commuting subgroups $G_1,G_2 \subset G$ satisfying $ab=ba$ for any $b \in G_1$ and $b \in G_2$. More precisely, the problems the braid cryptography is based on are as follows:

Input: A non-abelian group *G*, two commuting subgroups $G_1,G_2 \subset G$

Conjugacy Problem (CP)

Given (u,aua^{-1}) with $u,a \in G$, compute *a*.

Diffie-Hellman Conjugacy Problem (DHCP)

Given (u,aua^{-1},bub^{-1}) with $u \in G$, $a \in G_1$ and $b \in G_2$, compute $baub^{-1}a^{-1}$.

Decisional Diffie-Hellman Conjugacy Problem (DDHCP)

Given (u,aua^{-1},bub^{-1}) with $u,c \in G$, $a \in G_1$ and $b \in G_2$, decide whether $c=ba$.

3.4. Matching conjugacy problems in non-commutative groups

For a non-commutative group G, a pair $(x,x') \in G \times G$ is said to be CSP-hard if $x \sim x'$ and CSP is infeasible for the instance (x,x'). If (x,x') is CSP-hard, so is clearly (x',x).

The matching conjugate search problem (MCSP)

Instance: A CSP hard pairs (x,x') in G and $y \in G$

Objective: Find $y' \in G$ such that $y \sim y'$ and $xy \sim x'y'$

Matching Triple Search Problem (MTSP)

Instance: A CSP-hard pair (x,x') in G and $y \in G$.

Objective: Find a triple $(\alpha,\beta,\gamma) \in G \times G \times G$ such that $\alpha \sim x, \beta \sim \gamma \sim y, \alpha\beta \sim xy,$ and

$\alpha\gamma \sim x'y$

k-simultaneous conjugator search problem (k-SCSP)

Instance: Given k pairs $\left(x, x', y\right) \in G \times G \times G$ with $x_i' = s x_i s^{-1}$ for all i,

Object: find $b \in G$ such that $x_i' = b x_i b^{-1}$ for all i.

3.5. Conjugacy Systems Based on Non-abelian Factorization Problems

Subgroup conjugator searching problem (SCSP): Let G be any non-abelian finite group with identity e .Let $g, h \in G$ be two random elements so that $\langle g \rangle \cap \langle h \rangle = \{e\}$. The subgroup conjugator searching problem (SCSP) with respect to, G, g, h denoted by $SCSP_{g,h}{}^{G}$, is to recover g^x from the given pair $\left(h^y, g^x h^y g^{-x}\right) \in G^2$,where x, y are arbitrary integers picked at random.

Subgroup conjugacy deciding problem (SCDP)

Let G be any non-abelian finite group with identity e .Let $g, h \in G$ be two random elements so that $\langle g \rangle \cap \langle h \rangle = \{e\}$. The subgroup conjugator deciding problem (SCDP) with respect to, G, g, h denoted by $SCDP_{g,h}{}^{G}$, is to distinguish the distribution.

$$D_2 = \left\{ \left(h^b, g^a h^a g^c\right) : a, b, c \in_R Z \right\}$$

And the distribution

$$D_3 = \left\{ \left(h^b, g^a h^a g^{-a}\right) : a, b \in_R Z \right\}.$$

Conjugated computational Diffie-Hellman problem (CCDH)

Let G be any non-abelian finite group with identity e .Let $g, h \in G$ be two random elements so that $\langle g \rangle \cap \langle h \rangle = \{e\}$. The conjugator computational Diffie-Hellman (CCDH) with respect to, G, g, h denoted by $CCDH_{g,h}{}^{G}$, is to recover $g^{a+c} h^b g^{-a-c}$ from given triple.

$$\left(h^a, g^a h^b g^{-a}, g^c h^b g^{-c}\right) \in G^3,$$

where a, b, c, d are arbitrary integers picked at random.

Conjugated decisional Diffie-Hellman problem (CDDH)

Let G be any non-abelian finite group with identity e .Let $g,h \in G$ be two random elements so that $\langle g \rangle \cap \langle h \rangle = \{e\}$. The conjugated decisional Diffie-Hellman problem (CDDH) with respect to, G, g, h denoted by $CDDH_{g,h}{}^{G}$, is to distinguish the distribution.

$$D_4 = \left\{ \left(h^b, g^a h^a g^{-a}, g^c h^b g^{-c}, g^d h^b g^{-d} \right) : a,b,c,d \in_R Z \right\},$$

$$D_5 = \left\{ \left(h^b, g^a h^a g^{-a}, g^c h^b g^{-c}, g^{a+c} h^b g^{-a-c} \right) : a,b,c \in_R Z \right\},$$

Gap conjugated computational Diffie-Hellman problem (Gap-CCDH): Let G be any non-abelian finite group with identity e .Let $g,h \in G$ be two random elements so that $\langle g \rangle \cap \langle h \rangle = \{e\}$. The conjugated computational decisional Diffie-Hellman problem (Gap-CDDH) with respect to, G, g, h denoted by $Gap - CDDH_{g,h}{}^{G}$, is to solve the $CDDH_{g,h}{}^{G}$, give access to an oracle that solves the $CDDH_{g,h}{}^{G}$ problem.

4. An overview of conjugacy problems in cryptography.

Conjugacy problems	**Authentication**	**Signature schemes**	**Key exchange**
Conjugacy search problem	Guangguo Han [28]Chuangui Ma propose a generalization of Schnorr's authentication and signature scheme whose security is based on the hardness of the conjugacy search problem	Sunder Lal and Vandani Verma[29] using proxy signature scheme	Ki Hyoung Ko et al [30]. Proposed and implement a new key agreement scheme and public key cryptosystem based on these primitives in the braid groups.
Diffie-Hellman Conjugacy Problem	M. Chowdhury [25]presented a new two pass authentication scheme	Manoj Kumar[26] presents the security analysis of a proxy signature scheme over braid groups	Jung Hee Cheon1 and Byungheup Jun[27] define a polynomial time algorithm for the braid Diffie-Hellman conjugacy problem (DHCP) on which the braid key exchange scheme
Shifted Conjugacy problem	Jonathan Longrigg and Alexander Ushakov[24] design a heuristic attack on the cryptographic authentication scheme	-	-

Braid Conjugacy problem	Atul Chaturvedi and Sunder Lal propose[17] an authenticated key agreement protocol based on braid conjugacy problem	Tony Thomas and Arbind Kumar Lal[15] construct a zero-knowledge undeniable signature scheme	Ho-Kyu Lee1, et al.[23] extend the 2-party key exchange protocol on braid groups and also provide authenticity to the group key agreement protocol
Twisted conjugacy problem	Vladimir Shpilrain and Alexander Ushakov[8] proposed authentication scheme and reduce linear algebraic attack	-	-
Conjugate adjoining problem	-	Wang Licheng, et al.[14] design a braid-based signature scheme and This scheme is efficient and provably secure in the random oracle model.	-
Multiple Simultaneous Conjugacy Problems	-	Tony Thomas and Arbind Kumar Lal[21]. propose the first undeniable signature schemes based on braid groups .The security of our scheme are based on the hardness of multiple simultaneous conjugacy problem	Milton M. Chowdhury[22] solve the decomposition problem using the Multiple Simultaneous Conjugacy Problems
conjugacy search problem of left conjugacy closed loops	-	-	Juha Partala and Tapio Seppanen[20] give a formulation of the CSP for left conjugacy closed loops to construct a generalization of the Anshel-Anshel-Goldfeld key establishment method
Matching conjugacy problems	-	Ki Hyoung Ko et al.[19] propose a new digital signature scheme based on a non-commutative group and implement our signature scheme in the braid groups	-
Conjugacy Systems Based on Non-abelian		Lize Gu et al.[18] present new construction of encryption, signature, and	

Factorization Problems	--	signcryption based on the newly introduced cryptographic intractable assumptions	-

5. Conclusions

Recently non-abelian groups have attracted the attention of cryptographers for constructing public-key cryptographic protocols. In this article we have discussed about the different types of conjugacy problems in different algebraic structures. From our survey, we find that the conjugacy problem works on the various structures to build public-key cryptosystems and in most of the cases it is found that conjugacy problems used in the braid group are computationally hard.

Reference

1. Magliveras S S, Stinson D R, Trung T V. New approaches to designing public key cryptosystems using one-way functions and trapdoors in finite groups. J Cryptogr, 2002, 15: 285–297.
2. Shor P. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM J Comput, 1997, 26: 1484–1509.
3. Proos J, Zalka C. Shor's discrete logarithm quantum algorithm for elliptic curves. Quant Inf Comput, 2003, 3: 317–344.
4. Lee E. Braid groups in cryptography. IEICE Trans Fund Electr, 2004, E87-A: 986–992.
5. Anshel I, Anshel M, Goldfeld D. An algebraic method for public-key cryptography. Math Res Lett, 1999, 6: 287–291.
6. Ko, K. H., Lee, S. J., Cheon, J. H., Han, J. W., Kang, J. S., & Park, C. (2000, January). New public-key cryptosystem using braid groups. InAdvances in cryptology—CRYPTO 2000 (pp. 166-183). Springer Berlin Heidelberg.
7. Shpilrain, V., & Ushakov, A. (2008, January). An authentication scheme based on the twisted conjugacy problem. In Applied Cryptography and Network Security (pp. 366-372). Springer Berlin Heidelberg.
8. Shor, P. W. (1997). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM journal on computing,26(5), 1484-1509.
9. Han, G., Ma, C., & Cheng, Q. (2010, March). A generalization of DSA based on the conjugacy search problem. In Education Technology and Computer Science (ETCS), 2010 Second International Workshop on (Vol. 3, pp. 348-351). IEEE.

10. Verma, G. K. (2008). Blind Signature Scheme over Braid Groups. IACR Cryptology ePrint Archive, 2008, 27.
11. Grigoriev, D., & Shpilrain, V. (2010). Authentication from matrix conjugation. arXiv preprint arXiv:1010.5034.
12. Wang, L., Wang, L., Cao, Z., Yang, Y., & Niu, X. (2010). Conjugate adjoining problem in braid groups and new design of braid-based signatures. Science China Information Sciences, 53(3), 524-536.
13. Thomas, T., & Lal, A. K. (2008). A Zero-knowledge Undeniable Signature Scheme in Non-abelian Group Setting. IJ Network Security, 6(3), 265-269.
14. Wang, L., Cao, Z., Zeng, P., & Li, X. (2007, March). One-more matching conjugate problem and security of braid-based signatures. In Proceedings of the 2nd ACM symposium on Information, computer and communications security (pp. 295-301). ACM.
15. Mahalanobis, A. (2008). The Diffie-Hellman key exchange protocol and non-abelian nilpotent groups. Israel Journal of Mathematics, 165(1), 161-187.
16. Chaturvedi, A., & Lal, S. (2008). An Authenticated Key Agreement Protocol Using Conjugacy Problem in Braid Groups. IJ Network Security, 6(2), 181-184.
17. Gu, L., & Zheng, S. (2014). Conjugacy systems based on nonabelian factorization problems and their applications in cryptography. Journal of Applied Mathematics, 2014.
18. Ko, K. H., Choi, D. H., Cho, M. S., & Lee, J. W. (2002). New Signature Scheme Using Conjugacy Problem. IACR Cryptology ePrint Archive, 2002, 168.
19. Kitaev A. Quantum measurements and the abelian stabilizer problem. Report arXiv:quant-ph/9511026, 1995.
20. Partala, J., & Seppänen, T. (2008). On the conjugacy search problem and left conjugacy closed loops. Applicable Algebra in Engineering, Communication and Computing, 19(4), 311-322.
21. Thomas, T., & Lal, A. K. (2006). Undeniable signature schemes using braid groups. arXiv preprint cs/0601049.
22. Chowdhury, M. M. (2007). On the Security of the Cha-Ko-Lee-Han-Cheon Braid Group Public Key Cryptosystem. arXiv preprint arXiv:0708.2571.
23. Lee, H. K., Lee, H. S., & Lee, Y. R. (2003). An Authenticated Group Key Agreement Protocol on Braid groups. IACR Cryptology ePrint Archive, 2003, 18.

24. Longrigg, J., & Ushakov, A. (2008). Cryptanalysis of the shifted conjugacy authentication protocol. Journal of Mathematical Cryptology, 2(2), 109-116.
25. Chowdhury, M. M. (2007, August). An authentication scheme using non-commutative semigroups. In null (pp. 115-118). IEEE.
26. Kumar, M. (2009). On the Security of a Proxy Blind Signature Scheme over Braid Groups. IACR Cryptology ePrint Archive, 2009, 361.
27. Cheon, J. H., & Jun, B. (2003). A polynomial time algorithm for the braid Diffie-Hellman conjugacy problem. In Advances in Cryptology-CRYPTO 2003(pp. 212-225). Springer Berlin Heidelberg.
28. Han, G., & Ma, C. (2010, April). A new authentication and signature scheme based on the conjugacy search problem. In Networks Security Wireless Communications and Trusted Computing (NSWCTC), 2010 Second International Conference on (Vol. 2, pp. 317-320). IEEE.
29. Verma, G. K. (2009). A Proxy Blind Signature Scheme over Braid Groups. IJ Network Security, 9(3), 214-217.
30. Ko, K. H., Lee, S. J., Cheon, J. H., Han, J. W., Kang, J. S., & Park, C. (2000, January). New public-key cryptosystem using braid groups. In Advances in cryptology—CRYPTO 2000 (pp. 166-183). Springer Berlin Heidelberg.
31. Wang, L., Cao, Z., Zeng, P., & Li, X. (2007, March). One-more matching conjugate problem and security of braid-based signatures. In Proceedings of the 2nd ACM symposium on Information, computer and communications security (pp. 295-301). ACM.
32. Lal, S., & Verma, V. (2009). Some proxy signature and designated verifier signature schemes over braid groups. arXiv preprint arXiv:0904.3422.
33. Gebhardt, V. (2006). Conjugacy search in braid groups. Applicable Algebra in Engineering, Communication and Computing, 17(3-4), 219-238.
34. Ojha, D. B., Dwivedi, A., Sharma, A., & Singh, R. (2010). A Non-Repudiable Biased Bitstring Key Agreement protocol (NBBKAP) Using Conjugacy Problem in Non-abelian Group. International Journal of engineering Science and technology, 2(9), 4162-4166.

Corresponding Author:

V.Muthukumaran*,

Email: *muthu.v2404@gmail.com*