Volume: 09 Issue: 03 Pages: 3428-3431 (2017) ISSN: 0975-0290

# A New Key Agreement Protocol Using BDP and CSP in Non Commutative Groups

**Atul Chaturvedi**
Department of Mathematics, PSIT, Kanpur
Email: atulibs@gmail.com
**Manoj Kumar Misra**
Department of Computer Science, PSIT, Kanpur
**Varun Shukla**
Department of Electronics & Communication, PSIT, Kanpur
**Neelam Srivastava**
Department of Electronics & Communication, REC, Kannauj
**S.P.Tripathi**
Department of Computer Science, IET, Lucknow

**ABSTRACT**

**The available key agreement schemes using number theoretic, elliptic curves etc are common for cryptanalysts and associated security is vulnerable. This vulnerability further increases when we talk about modern efficient computers. So there is a need of providing new mechanism for key agreement with different properties so intruders get surprised and communication scenarios becomes stronger than before. In this paper, we propose a key agreement protocol which works in a non commutative group. We prove that our protocol meets the desired security attributes under the assumption that Conjugacy Search Problem and Decomposition Problem are hard in non commutative groups.**

Keywords **- Conjugacy Search Problem, Decomposition Problem, Key Agreement, Non Commutative Groups, Wireless Communication**

Date of Submission: Oct 25, 2017 Date of Acceptance: Nov 04, 2017

## I. INTRODUCTION

Recent years in cryptographic research have witnessed several proposals for secure cryptographic schemes using non commutative groups and braid groups [1,2,3,4,5,6,7,8]. The idea of applying non commutative groups (braid group) as a platform for cryptosystems was introduced by Anshel et al [2]. These groups are more complicated than abelian groups and not too complicated to work with. These two characteristics make these groups a convenient and useful choice to attract the attention of researchers. For new key agreement scheme we use a specific non commutative group which has special type of subgroups having the property that the elements of one subgroup are commute to other. One such example is Artin's braid group [9].In [4], Ko et al propose a braid group version of Diffie-Hellman key agreement [10] which is based on CSP. However, this protocol does not offer verification between the two parties of communication. Therefore, it is disposed to man in middle attack. We know that cryptographic protocols are based on hard problems like prime factorization problem, Diffie - Hellman like problems. The above mentioned group has two hard problems which are CSP and BDP in braid groups. We make use of Conjugacy Search Problem (CSP) and Braid Decomposition Problem (BDP) to suggest a new key agreement scheme. The CSP and BDP in braid groups are algorithmically difficult and consequently provide one-way functions. We use this characteristic of CSP and BDP to propose a key agreement protocol. The rest of the paper is organized as follows: We present the required platform for our protocol in section II. In section III, we define key agreement protocol. In section IV, we present our protocol along with the desired security consideration. The paper ends with conclusion and future scope.

## II. PLATEFORM FOR PROTOCOL

In [9] Emil Artin defined $B_n$, where $n$ is the index with following notations: Consider the *generators* $\sigma_1, \sigma_2, ..., \sigma_{n-1}$, where $\sigma_i$ represents the braid in which the $(i+1)^{st}$ string crosses over the $i^{th}$ string while all other strings remain uncrossed. The *defininin relations* are

1. $\sigma_i \sigma_j = \sigma_j \sigma_i \, for \left| i - j \right| > 1$,
2. $\sigma_i \sigma_j \sigma_i = \sigma_j \sigma_i \sigma_j \, for \left| i - j \right| = 1$.

We use geometrical interpretation of elements of the group $B_n$ by an $n$-strand braid in the usual sense [11]. The *fundamental braid* is given by $\Delta$, which commutes with any braid $b$.

$\Delta = (\sigma_1 \sigma_2 \ldots\ldots\ldots \sigma_{n-1})(\sigma_1 \sigma_2 \ldots\ldots\ldots \sigma_{n-2}) \ldots\ldots\ldots (\sigma_1 \sigma_2)(\sigma_1)$

In fact $\Delta b = \tau(b)\Delta$, here $\tau : B_n \to B_n : \tau(\sigma_i) = \sigma_{n-i}$ is an automorphism. Since $\tau^2$ is the identity map, $\Delta^2$ truly commutes with any braid. A subword of the fundamental braid $\Delta$ is called a *permutation braid* and the set of all permutation braids is in one-to-one correspondence with the set $\sum_n$ of permutations on $\{0,1,\ldots,n-1\}$. For example, $\Delta$ is the permutation sending $i$ to $n$-$i$. The word

Volume: 09 Issue: 03 Pages: 3428-3431 (2017) ISSN: 0975-0290

length of a permutation *n*-braid is $\leq \frac{n(n-1)}{2}$. The *descant set* $D(\pi)$ of a permutation π is defined by $D(\pi) = \{i | \pi(i) > \pi(i+1)\}$. Any braid *b* can be written uniquely as $b = \Delta^u \pi_1 \pi_2 ... \pi_l$ where *u* is an integer, $\pi_i$ are permutation braids different from Δ and $D(\pi_{i+1}) \subset D(\pi_i^{-1})$. This unique decomposition of a braid *b* is called a *left canonical form*. All the braids in this paper are assumed to be in the *left-canonical form*. For example, for $a,b \in B_n$, *ab* means the left-canonical form of *ab* and so it is hard to guess its factors *a* or *b* from *ab*. In $B_n$, we say that two elements *x* and *y* are *conjugate* to each other if $y = axa^{-1}$ for some *a* in $B_n$ and we write $x \sim y$. Here *a* or $a^{-1}$ is called a *conjugator* and the pair (*x,y*) is said to be conjugate. The *Conjugacy Decision Problem* (*CDP*) asks to determine whether $x \sim y$ for a given (*x, y*). Equivalently, we can ask that given two group words *x* and *y* in $B_n$, can we decide in a finite number of steps whether or not *x* and *y* are conjugate in $B_n$? In other words, does there exist an element *a* in $B_n$ such that $y = axa^{-1}$? In [12], Garside proves that the *CDP* for braid groups is solvable, but the algorithm he proposed, as well as all improvements proposed thereafter, has a high cost that is exponential in the length of the considered words and the number of strands. The *Conjugacy Search Problem (CSP)* asks to find *a* in $B_n$ satisfying $y = ax\,a^{-1}$ for a given instance (*x, y*) in $B_n$ such that $x \sim y$. In other words, given two elements *x, y* $\in B_n$ and the information that $y = axa^{-1}$ for some *a* in $B_n$, *CSP* asks to find at least one particular element *a* like that. It is considered infeasible to solve *CSP* for sufficiently large braids. The probability for a random conjugate of *x* to be equal to *y* is negligible. For $B_n$, a pair $(x,y) \in B_n \times B_n$ is said to be *CSP-hard* if $x \sim y$ and *CSP* is infeasible for the instance (*x,y*).If (*x,y*) is *CSP-hard*, so is clearly (*y,x*). Also in braid groups, *Braid decomposition problem* (BDP) says, find the pair (*a, b*) from *asb* and *s*. In this regard this problem is similar to discrete logarithmic problem (DLP) over braid group.

## III. AUTHENTICATED KEY AGREEMENT PROTOCOL (AKAP)

It is always desired to have key agreement after the authentication phase of a protocol gets over. Key agreement is a dedicated process where a common shared key becomes available to participating entities [13,14]. For better sense of understanding, key agreement process can be separately bifurcated into key transport and mutual key agreement. In key transport process, one participating entity (considering peer to peer protocol in mind) develops a secret value as a key and transfers it to the other entity in a secure fashion. In mutual key agreement, it is expected that shared secret key (session key) is calculated by two entities in such a way that the involvement of both the entities is desired. That means no entity can predict the resultant value of the secret key. So authenticated key agreement protocols are very dominating for the development of secure data communication systems keeping the facts in mind that communication channels are always insecure and intruders have full access to communication channels. In a key agreement protocol two or more distributed entities need to share some key in secret, called session key. This secret key can then be used to create a confidential communication channel amongst the entities. Since the path breaking work of Diffie-Hellman [10] in 1976, several key agreement protocols have been proposed over the years [4, 13,15,16,17]. However, the protocol of [10] does not provide verification for peer to peer communication. So it is not secure against man in middle attack. A number of desirable attributes of such key agreement protocols have been identified in [17]. Nowadays most protocols are analyzed with such attributes. These are listed as under:

- **Known-key security**: It suggests that, in point to point communication, the secret key is unique in every run of key agreement protocol. So even if intruder learns some session keys, it is of no meaning.
- **Perfect forward secrecy**: It tells that if long-term private keys of participating entities are known to hacker, then the confidentiality of old session keys remain safe.
- **Key-compromise impersonation**: It is important for the situations which uses insecure wireless channels. Suppose sender's (or A's) long term private key is disclosed. It means, intruder can impersonate sender but here it is desirable that this loss can't give freedom to intruder to impersonate sender.
- **Unknown key-share**: The receiver (or B) can't be indulged into key sharing without his knowledge. It means when receiver believes that the key is shared with some entity (say C and C≠A), it is actually shared with that one.
- **Key control**: No participating entity can be able to compel the session key to a pre determined value.

## IV. OUR PROPOSED PROTOCOL

**4.1 Initial set up:** Suppose two users *A* and *B* want to share a secret key *K*. A sufficiently complicated *n* - braid *s* from the braid group $B_n$ is selected and published. We consider two subgroups $LB_n$ and $UB_n$ of $B_n$ where $LB_n$ is generated by $\sigma_1, \sigma_2, .... \sigma_{\frac{n}{2}-1}$ and $UB_n$ is generated by $\sigma_{\frac{n}{2}+1}, ...., \sigma_{n-1}$, This $B_n$ is non – commutative but every element of $LB_n$ commutes with every element of $UB_n$. Choose $x_1 \in LB_n, x_2 \in UB_n$ ,computes $x_A = x_1 s x_1^{-1}$, $x_B = x_2 s x_2^{-1}$. These, $(x_1, x_A)$ and $(x_2, x_B)$ are long term private and public key pairs of users *A* and *B* respectively.

Volume: 09 Issue: 03 Pages: 3428-3431 (2017) ISSN: 0975-0290

**4.2 Protocol run:**

- **Step1:** *A* randomly chooses two braids *a* and *b* from $LB_n$, compute $X_A = asb$ and sends it to *B*.
- **Step 2:** After receiving $X_A$ from *A* , *B* randomly chooses two braids *c* and *d* from $UB_n$, computes $k_B = x_2 x_A x_2^{-1}$ , $K_B = k_B csd k_B^{-1}$ and sends $K_B$ to *A*.
- **Step 3:** Upon receiving $K_B$ from *B*. Entity *A* computes $k_A = x_1 x_B x_1^{-1}$ and the shared key $key(A) = a(k_A^{-1} K_B k_A)b$.
- **Step 4:** Receiver, *B* also computes the shared key $key(B) = cX_A d$ .

**4.3 Correctness:** Since each element of $LB_n$ commutes with each element of $UB_n$, therefore $k_A = x_1 x_B x_1^{-1} = x_1 (x_2 s x_2^{-1}) x_1^{-1} = x_1 x_2 s x_2^{-1} x_1^{-1}$ and $k_B = x_2 x_A x_2^{-1} = x_2 (x_1 s x_1^{-1}) x_2^{-1} = x_1 x_2 s x_1^{-1} x_2^{-1}$. Also $key(A) = a(k_A^{-1} K_B k_A)b = a(k_A^{-1} k_B csd k_B^{-1} k_A)b = acsdb$ and and $key(B) = cX_A d = c(asb)d = casbd$. Thus $key(A) = key(B)$ because *ac* = *ca* and *bd* = *db*.

**4.4 Security Consideration:** Here we show that our protocol fulfils the recurred security aspects keeping the fact in mind that above discussed problems are secure.

- **Known-Key Security:** This is quite obvious as sender A, and receiver B execute the protocol and they will get unique session key as calculated in section 4.2.
- **(Perfect) Forward Secrecy:** When the calculation phase of session key by each entity is going on, the random group element pairs (*a, b*) and (*c, d*) play an important role. Assume that an intruder has private keys $x_1$ or $x_2$ can extract $k_A$ or $k_B$ from the information to know the session keys. It creates a contradiction because that *CSP* and *BDP* are hard which is our assumption.
- **Key-Compromise Impersonation:** Let us assume that the sender's long term private key $x_1$ is disclosed to intruder and he can impersonate the sender. Here the important question is that whether the intruder can impersonate the receiver without knowing $x_2$. For this, the intruder must know the sender's ephemeral key pair (*a, b*). For this purpose the intruder is supposed to retrieve *c* from sender's ephemeral public value $x_A = asb$ which is not possible under the assumption that BDP is hard.
- **Unknown Key-share:** Assume an intruder tries to convince the sender that sender has key sharing with receiver but receiver knows that he shares key with intruder. To launch this, the intruder has to publish the correct public key without knowing the private key which is impossible.
- **Key Control:** In our case key control is not possible for intruder. The only possibility moves around with receiver B but receiver B is bounded by the sender A as the session key involves preselected value by sender A. So receiver B need to solve *csd* which is not possible as BDP is hard.

## V. CONCLUSION & FUTURE SCOPE

In this paper we have proposed a new key agreement protocol along with the security analysis. Our protocol makes use of hard problems in non commutative groups. The protocol is secure against all the five possible attacks. Entity impersonation by an intruder is not possible which enhances the utility of the protocol.

We have proposed peer to peer protocol which can be extended to multiparty. The protocol is easy to implement and it can be very useful in data communication scenarios where the wireless communication channel is not secure. The hard problems we used belong to non commutative group and they are comparatively new to intruders.

## REFERENCES


[1] I.Anshel, M.Anshel, B.Fisher, D.Goldfeld, New key agreement protocols in braid group cryptography, *Proc.of CT-RSA , LNCS (2020)*, Springer-Verlag, 2001, 1-15.

[2] I. Anshel, M. Anshel , D. Goldfeld, An algebraic method of public-key cryptography, *Math. Research Letters, 6* ,1999, 287-291.

[3] K.H.Ko, D.H.Choi, M.S.Cho, J.W.Lee, New signature scheme using conjugacy problem, *e print archive*, http://eprint.iacr.org/2002/168.

[4] K.H. Ko, S.J. Lee, J.H. Cheon, J.W. Han, J.S. Kang, C Park, New public-key cryptosystem using braid groups, *Advances in Cryptology*, *Proceeding of Crypto - 2000, LNCS (1880)* , Springer Verlag ,2000, 166-183.

[5] G. Kumar , H. Saini , Novel non commutative cryptography scheme using extra special group, *Security and communication networks*, 2017. https://www.hindawi.com/journals/scn/2017/9036382,

[6] Y. K. Peker, A new key agreement scheme based on the triple decomposition problem, *International Journal of Network Security (6)*, 2014, 426 – 436.

Volume: 09 Issue: 03 Pages: 3428-3431 (2017) ISSN: 0975-0290

[7] H.Sibert, P.Dehornoy, M.Girault, Entity authentication schemes using braid word reduction, in *International workshop on coding and cryptography (WCC) 2003, Discrete Applied Mathematics, 154-2*, Elsevier, 2006, 420 – 436. (http://eprint.iacr.org/2002/187).

[8] V.Halava, T.Harju, R.Niskanen, I.Potapov, Weighted automata on infinite words in the context of Attacker – Defender games, *Information and Computation* , Elsevier, 255 (1), 2017, 27 – 44.

[9] E. Artin, Theory of braids, *Annals of Math.48* (1947),101-126.

[10] W. Diffie, & M.Hellman, New directions in cryptography, *IEEE Trans. Inform. Theory,22 (6)*,1976,644-654.

[11] J.Birman, Braids, links, and mapping class groups, *Annals of Math*. Studies, Princeton Univ. Press ,1975.

[12] F.A. Garside, The braid group and other groups, *Quart. J. Math. Oxford 20-78* ,1969, 235-254.

[13] L.Law, A.Menezes, M.Qu, J.Solinas, S.Vanstone, An efficient protocol for authenticated key agreement, *Design, codes and cryptography, 28 (2)*, 2003, 119-134.

[14] M.Bellare, P.Rogaway, Entity Authentication and key distribution, *Proceeding of CRYPTO'93*, Santa Barbara, USA,1994, 341-358.

[15] A.O. Baalghusun, O.F. Abusalem, Z. A. A. Abbas, J. P. Kar, Authenticated key agreement protocols: A comparative study, *Journal of information security, (6)*, 2015, 51 – 58.

[16] A.Menezes, M.Qu, S.Vanstone, Key Agreement and the need for authentication, in *Proceedings of PKS'95*, 1995, 34 – 42.

[17] S. B. Wilson, D.Johnson, A.Menezes, Key agreement protocol and their security analysis, *Proceedings of sixth IMA International conference on cryptography and coding*, Cirencester, UK,1997,30-45.

**Biographies and Photographs**

**Atul Chaturvedi** received his M.Sc., M.Phil. and Ph.D from Dr.B.R.A University, Agra. His research interests include Cryptography and Networks Security. He is a life member of Cryptology Research Society of India (CRSI) and Indian Society for Technical Education (ISTE). He has published various books, research papers in various journals and reviewer of many International journals. He has been convener of many national and international conferences. He is currently Professor and Head department of Mathematics at PSIT, Kanpur. He is guiding many research fellows in the area of Cryptography and Network Security.

**Varun Shukla** received his B.Tech from JUIT, M.Tech(Hons) from RGTU. He is a state topper in M.Tech and honored by Honorable President of India. He has done Post Graduate Diploma in Business Administration. He is a life member of Cryptology Research Society of India (CRSI), ISTE and Indian Science Congress. His research interests include Cryptography and Network Security. He has many publications in International journals and conferences. Presently, he is an Assistant Professor, department of Electronics & Communication at PSIT, Kanpur.

**Neelam Srivastava** received her B.Tech from MMMEC, Gorakhpur, M.Tech from IIT-BHU and Ph.d From Lucknow University. She has published many research papers in reputed journals. She has delivered invited talks in many government and non government organizations, authored many books in Electronics and Communication. She has supervised many master and doctoral candidates. She is a fellow member of IETE and chief project coordinator (CPC) of the TEQIP (Technical education quality improvement program) of World Bank for Uttar Pradesh. Presently, she is Director at Rajkiya Engineering College, Kannauj, Uttar Pradesh.

**Manoj Kumar Misra** has received his M.Tech from HBTU, Kanpur. He is Assistant Professor in the department of Computer science at PSIT, Kanpur. He is a member of Computer Society of India. He has published many papers in various international journals. He has presented many papers in reputed conferences and organized many workshops.

**S.P.Tripathi** is Professor at IET, Lucknow. He received Ph.D from Lucknow University. He has published many papers in various international journals and delivered invited talks in reputed conferences. He is Life Member of Indian Science Congress, Computer Society of India etc. He is associated as an expert member of various universities. He is a member of various regulatory bodies and panel member of various RDC committees.