IJCSE International Journal of Computer Sciences and Engineering Open Access
Review Paper Volume-5, Issue-12 E-ISSN: 2347-2693

An Authenticated Key Agreement Protocol Using Artin's Braid Group

Atul Chaturvedi[1*], Manoj Kumar Misra[2], S.P. Tripathi[3] Varun Shukla[4]

[1*]Dept. of Mathematics, PSIT, Kanpur, India|
[2] Dept. of Computer Science, PSIT, Kanpur, India
[3] Dept. of Computer Science, IET, Lucknow, India
[4] Dept. of Electronics & Communication, PSIT, Kanpur, India

[*]*Corresponding Author: atulibs@gmail.com,*

Available online at: www.ijcseonline.org

Received: 28/Nov/2017, Revised: 10/Dec/2017, Accepted: 20/Dec/2017, Published: 31/Dec/2017

Abstract— This paper proposes a new and efficient key agreement protocol where trusted third party (TTP) is involved. There are various available schemes which are based on number theoretic, elliptic curves etc. Due to the availability of modern computers, these schemes are vulnerable to man in the middle attack (MITM). So there is a requirement of new technique for key agreement which surprises the intruders and enhances the security of communication system. Our proposed protocol utilizes the property of a non commutative group. We have given the security proof of our protocol keeping the fact in mind that decomposition and conjugacy search problem are hard in a group which is non commutative.

Keywords— Braid Decomposition Problem(BDP), Conjugacy Search Problem(CSP), Key Agreement, Non Commutative Groups, Trusted Third Party (TTP), Wireless Communication

I. INTRODUCTION

Many cryptographic schemes [1-8] were proposed after the seminal work of Anshel et al [2] over non commutative groups (braid group). These schemes have utilized the fact that non commutative groups are complicated than abelian groups and at the same time too complicated for protocol development. Due to these properties, braid group became a popular choice among researchers. Our new scheme utilizes the fact that in a subgroup, elements are commutative with each other. To make new agreement scheme between TTP, sender and receiver we use a specific property that the element of a group are commutative to each other. This property is already utilized in Artin's braid group [9].Another utilization is done by Ko et al [4],which is a braid group version of DH key agreement [10]. However this protocol faces a problem of verification between sender and receiver since any of the cryptographic protocol is based on hard problem, whether it is prime factorization or DH like problems. We use two hard problems of braid groups CSP and BDP. These problems provide one way function and at the same time algorithmically difficult for the purpose of verification we have used trusted third party (TTP) which will be an intermediary between the sender and receiver to generate the key for secure communication. Our proposed protocol is secure enough for the attacks like man in the middle attack due to the TTP involvement between the communicating parties.

The rest of this paper is organized as follows. Section 2 introduces mathematical foundation of our protocol. In Section 3, we described authenticated key agreement protocol (AKAP). In Section 4, we have proposed our protocol. Finally, some conclusions are drawn in Section 5.

II. PLATEFORM FOR PROTOCOL

Any Braid group B_n is the set of n braids. It was defined by Emil Artin [9], where it is defined in terms of generators.

Suppose we have generators $\sigma_1, \sigma_2, ..., \sigma_{n-1}$ where σ_j is used to denote the braid in which string $(j + 1)$ crosses j^{th} string, but other strings remain uncrossed. Relations can be defined as follows.

1- $\sigma_j \sigma_k = \sigma_k \sigma_j \; for \left| j-k \right| > 1$,

2- $\sigma_j \sigma_k \sigma_j = \sigma_k \sigma_j \sigma_k \; for \left| j-k \right| = 1$.

Every element of the group B_n is geometrically interpreted by an n-strand braid in the normal sense [11]. Δ represents the fundamental braid, which is commutative with any braid b. For further details of braid groups, readers can see suitable references [12-14].

III. AUTHENTICATED KEY AGREEMENT PROTOCOL (AKAP)

Key agreement is the process by which participating entities maintain a secret key [15-16]. Formally, purpose of key agreement protocol is to provide key confirmation. In better way it can be divided into key transport and mutual key agreement. Most important thing is to make involvement of both parties, in a shared key calculation. If multiple (more than two) parties are involved then there is a need of common shared key called a session key. Various protocols [4,15,17-20] have been proposed after the seminal work of Diffie-Hellman[10] but their protocol faces a problem against MITM. Key attributes [19] required in a key agreement protocol can be tested under the following parameters.

- Known-key security: It recommends that, in point to point correspondence, the private key is different in every execution of protocol. So regardless of whether intruder adapts some session keys, it is of no significance.
- Perfect forward secrecy: It tells that if long haul private keys of participants are known to intruder, at that point the secrecy of old session keys stay safe.
- Key-trade off impersonation: It is essential for the circumstances which utilizes uncertain remote channels. Assume sender's (or A's) long haul private key is disclosed. That is to say, intruder can mimic sender yet here it is alluring that this loss can't offer flexibility to mimic sender.
- Unknown key-share: The receiver (or B) can't be revealed into key sharing without his insight. It implies when beneficiary trusts that the key is imparted to some element (say C and C≠A), it is really imparted to that one.
- Key control: No communicating party can have the capacity to force the session key to a pre decided value.

IV. OUR PROPOSED PROTOCOL

4.1 Initial set up: Suppose two users *A* and *B* want to share a secret key *K* with the help of a trusted third party (TTP). TTP randomly chooses two sufficiently complicated *n* - braid *s* and *t* from the braid group B_n , two subgroups LB_n and UB_n of B_n where LB_n is generated by $\sigma_1, \sigma_2, \ldots \sigma_{\frac{n}{2}-1}$ and UB_n is generated by $\sigma_{\frac{n}{2}+1}, \ldots\ldots, \sigma_{n-1}$, This B_n is non – commutative but every element of LB_n commutes with every element of UB_n. TTP has published s, LB_n, UB_n and *t* kept as a secret.

4.2 Protocol run:

- A chooses $x \in LB_n$, and through a secure channel submit it to TTP.
- B chooses $y \in UB_n$, and through a secure channel submit it to TTP.
- TTP computes $x_A = xtx^{-1}$ and $x_B = yty^{-1}$.
- *A* randomly chooses two braids *u* and *v* from LB_n, compute $X_A = usv$ and sends it to *B.*
- After receiving X_A from *A* , *B* randomly chooses two braids *p* and *q* from UB_n, then ask x_A from TTP through secure channel, computes , $k_B = yx_Ay^{-1}$, $X_B = k_B pX_A qk_B^{-1}$ and sends X_B to *A.*
- Upon receiving X_B from *B.* Entity *A* asks x_B from TTP, computes $k_A = xx_Bx^{-1}$ and then the shared $key(A) = k_A^{-1} X_B k_A$.
- Receiver, *B* also computes the shared key $key(B) = pX_Aq$.

4.3 Correctness: Since each element of LB_n commutes with each element of UB_n, therefore $k_A = xx_Bx^{-1} = x(ysy^{-1})x^{-1} = xysy^{-1}x^{-1}$ and $k_B = yx_Ay^{-1} = y(xsx^{-1})y^{-1} = xysx^{-1}y^{-1}$. Also $key(A) = k_A^{-1}X_Bk_A = k_A^{-1}(k_B pX_A qk_B^{-1})k_A = pX_Aq = p(usv)q$ and $key(B) = pX_Aq = p(usv)q = pusvq$. Thus $key(A) = key(B)$ because *up* = *pu* and *vq* = *qv*.

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: Since every run of protocol generates a unique key so it is quite obvious as calculated in section 4.2.
- (Perfect) Forward Secrecy: For calculation of session key, most important role is played by the group element pair (u,v) and (p,q).If any intruder tries to find secret key x or y from k_A or k_B.It is not possible because these values are submitted through a secure channel to TTP. Since CSP and BDP are hard problems so it is also not possible to find x or y from k_A or k_B.
- Key-Compromise Impersonation: Suppose the sender's key x is disclosed to intruder and he can

impersonate the sender. Here the point of discussion is that whether the intruder can impersonate the receiver without having information of y. For this, the intruder must know the sender's key pair (u, v). For this purpose the intruder is supposed to retrieve p from sender's public value $X_A = usv$ which is not possible under the assumption that BDP is hard.

- Unknown Key-share: Suppose an intruder tries to convince the sender that he has key sharing with receiver but receiver knows that he shares key with intruder. For this, the intruder has to publish the correct public key without having the information of private key which is impossible.

- Key Control: For a intruder it is not possible to control the key. There is only one possibility which moves around with receiver B but receiver B is bounded by the sender A as the session key involves pre-selected value by sender A. So receiver B has to solve *psq* which is not possible due to the hardness of BDP.

V. CONCLUSION & FUTURE SCOPE

Secure key distribution is the basic need of a key agreement protocol. Available schemes are not involving any third party. In this paper we have involved TTP, which enhances the security level. This protocol is secure against all the possible attacks. Masquerade kind of attack is not possible due to the presence of TTP. Its security and ease of implementation makes it useful for banking or any financial transaction, where security is of paramount importance. It can also be extended to secure communication among multiple parties.

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.

[6] Y. K. Peker, A new key agreement scheme based on the triple decomposition problem, International journal of network security (6), 2014, 426 – 436.

[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] A.Chaturvedi, M.K.Misra,S.P.Tripathi,V.Shukla,N. Srivastava A New Key Agreement Protocol Using BDP and CSP in Non Commutative Groups, Int. J. Advanced Networking and Applications. 9(3) ,2017,3428-3431.

[14] A.Chaturvedi,V.Shukla,N.Srivastava A secure wireless peer to peer authentication protocol using triple decomposition problem, Asian journal of mathematics and computer research.22(2) 2017,63-69.

[15] 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.

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

[17] 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.

[18] A.Menezes, M.Qu, S.Vanstone, Key agreement and the need for authentication, in proceedings of PKS'95, 1995, 34 – 42.

[19] 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.

[20] M.V.Bhaskar,G.A.Ramchandra,Y.Deepika,Multipath optimized link state protocol(OLSR) with security for moblle ad-hoc networks .International journal of computer science and engineering,5(11),2017,182-186.

Authors Profile

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.

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.

Varun Shukla received his B.Tech from JUIT, M.Tech(Hons) from RGTU. He is a state topper in M.Tech and awarded by Honourable 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.

