Volume 1, No. 4, November 2010
Journal of Global Research in Computer Science
ISSN-2229-371X
RESEARCH PAPER
Available Online at www.jgrcs.info

A NON-REPUDIABLE BIASED BITSTRING KEY-AGREEMENT PROTOCOL WITH ROOT PROBLEM IN NON-ABELIAN GROUP

Abhishek Dwivedi*[1] and D.B.Ojha[2]

[1]Research Scholar Singhania University, Jhunjhunu, Rajsthan
& Department of M.C.A, Raj Kumar Goel Engineering College, Ghaziabad, U.P., India
dwivediabhi@gmail.com
[2]Department of Mathematics, R. K. G. Institute of Technology, Ghaziabad, U.P., India
ojhdb@yahoo.co.in

Abstract: The Key exchange problems are of central interest in security world. The basic aim is that two people who can only communicate via an insecure channel want to find a common secret key without any attack. In this paper, we 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 using root problem in non-abelian group (NKR-NAG).

Keywords: Diffie-Hellman key Agreement, Root Problem, Braid Groups, Protocol Crypto--graphy, Key Distribution Center (KDC), Non-Abelian Group.

INTRODUCTION

A common cryptographic technique to encrypt each individual conversation with a separate key. This is called a session key, because it is used for only one particular communication session,[3].In this protocol we assume Alice & bob are users of network ,each share secret key with the KDC(Trent).This protocol relies on the absolute security of Trent. Here we also assume Mallory is a lot more powerful than Eve if Mallory corrupt Trent, the whole network is compromised. This is known as man –in-the-middle attack and Alice & Bob have no way to verify that they are talking to each other. The problem in [12] sets around for our work, in Ko et al [6] proposed a braid group version of Diffie-Hellman key agreement, Man-in- the- middle attack works on this protocol. Since the path breaking work of Diffie -Hellman in 1976, several key agreement protocols have been proposed over the years [7, 8, 1, 11, 2, 9, and 10]. We improve the above scheme by proposing a biased key agreement protocol based on RP in non-abelian groups (NKR-NAG). We make use of Root Problem (RP) to suggest a new key agreement scheme. The RP in braid groups is algorithmically difficult and consequently provides one-way functions. In proposed scheme, we establish a new security pole for improve man- in-the-middle attack. So that Mallory can't impersonation between communicate parties. Braid Group has good enough candidature for choosing it as a non abelian group.

PRELIMINARIES

BRAID GROUPS:

Emil Artin [5] in 1925 defined B_n, the braid group of index n, using following generators and relations: Consider the generators $\sigma_1, \sigma_2, \dots, \sigma_n$, where σ_i represents the braid in which the $(i+1)^{st}$ string crosses over the i^{th} string while all other strings remain uncrossed. The defining relations are

1. $\sigma_i\sigma_j = \sigma_j\sigma_i \; for \; |i-j| \geq 2,$
2. $\sigma_i\sigma_j\sigma_i = \sigma_j\sigma_i\sigma_j \; for \; |i-j| = 1,$

An n-braid has the following geometric interpretation: It is a set of disjoint n-strands all of which are attached to two horizontal bars at the top and at the bottom such that each strands always heads downward as one walks along the strand from the top to the bottom. In this geometric interpretation, each generator σ_i represents the process of swapping the i^{th} strand with the next one (with i^{th} strand going under the $(i+1)^{th}$ one). Two braids are equivalent if one can be deformed to the other continuously in the set of braids. B_n is the set of all equivalence classes of geometric n-braids with a natural group structure. The multiplication *ab* of two braids *a* and *b* is the braid obtained by positioning *a* on the top of *b*. The identity *e* is the braid consisting of *n* straight vertical strands and the inverse of *a* is the reflection of a with respect to a horizontal line. So σ^{-1} can be obtained from σ by switching the over-strand and under-strand. $\Delta = (\sigma_1, \sigma_2, \dots \sigma_{n-1})(\sigma_1, \sigma_2, \dots, \sigma_{n-2}) \dots (\sigma_1, \sigma_2)(\sigma_1)$ is called the fundamental braid.

DIFFIE-HELLMAN KEY AGREEMENT (DHKA)

Suppose that A and B want to agree on a shared secret key using the Diffie-Hellman key agreement protocol [12]. They proceed as follows: First, A generates a random private value a_1, a_2 and B generates a random private value b_1, b_2. Then they derive their public values using parameters p and g and their private values. A's public value is $g(a_1, a_2)$ mod p and B's public value is $g(b_1, b_2)$ mod p. They then exchange their public values. Finally, A computes $ka_1, a_2(b_1, b_2) = (g(b_1, b_2))a_1, a_2$ mod , and B computes

BRAID GROUP VERSION OF DHKA USING ROOT PROBLEM

Ko et al. [6] proposed a braid group version of Diffie-Hellman key agreement protocol. Let B_n be a braid group where RP is infeasible. As mentioned earlier, all the braids in B_n are assumed to be in the left canonical form. Thus for $(a_1, a_2), (b_1, b_2)$ in B_n , it is hard to guess (a_1, a_2) or (b_1, b_2) from $(a_1, a_2), (b_1, b_2)$.

Initial set up:

A sufficiently complicated n-braid $x_1, x_2 \in B_n$ for a large n is selected and is known to both the parties A and B.

Key agreement:

(a) A chooses a random secret braid $a_1, a_2 \in LB_n$ computes $a_1^e x a_2^e$ and sends it to B.

(b) B chooses $b_1, b_2 \in UB_n$ computes $b_1^e x b_2^e$ and sends to A.

(c) A receives $b_1^e x b_2^e$ and computes $a_1^e(b_1^e x b_2^e)a_2^e$.

(d) B receives $a_1^e x a_2^e$ and computes $b_1^e(a_1^e x a_2^e)b_2^e$.

2.4 Man-in-the Middle Attack

Above protocol is vulnerable to a middle-person attack. In this attack, an opponent, C, does the following

1) C intercepts A's public value $a_1^e x a_2^e$ and sends $c_1^e x c_2^e$ to B.

$kb_1, b_2(a_1, a_2) = (g(a_1, a_2))b_1, b_2$ mod p . Since $k(a_1, a_2)(b_1, b_2) = k(b_1, b_2)(a_1, a_2) = k$, A and B now have a shared secret key k.

2) When B transmits his public value $b_1^e x b_2^e$, C substitutes it with $c_1^e x c_2^e$ and sends it to A.

3) C and A thus agree on one shared key KAC $= a_1^e(c_1^e x c_2^e)a_2^e$ and C and B agree on another shared key KBC $= b_1^e(c_1^e x c_2^e)b_2^e$ A.

4) After this exchange, C simply decrypts any messages sent out by A or B, and then reads and possibly modifies them before re-encrypting with the appropriate key and transmitting them to the correct party. This vulnerability is due to the fact that Diffie-Hellman key agreement does not authenticate the participants.

OUR APPROACH

In this section we describe our two-pass biased key agreement protocol between entities. Our protocol works in the following steps.

Initial set up

Both Alice and Bob share a secret key k_s without sharing Trent (KDC). Firstly Alice chooses a probability set as $P_0, P_1, \dots \dots P_{k-1} \in B_n^k$ and send to Bob after encrypt it with his secret key. Assume, Mollary corrupt after completion of setup phase.

After That,

Alice

$E_k(P_0, P_1, \dots \dots P_{k-1})$ sends

P_b : Sufficiently complicated n-Braid

$p \in LB_n$ Known as Alice private key.

$Id_A =$ Alice's Identity.

$q \in UB_n$ Known as Bob private key, and

$Id_B -$ Bob's Identity.

$X_A = p_1^e P_b p_2^e$ Known as Alice public key

$X_B = q_1^e P_b q_2^e$ Known as Bob public key

Bob

$E_k(P_0, P_1, \dots \dots P_{k-1})$ receive and decrypt it $D_k(E_k(P_0, P_1, \dots \dots P_{k-1}))$ and retrieve $(P_0, P_1, \dots \dots P_{k-1})$ braids

Key Agreement

<table>
<tr>
<td>Alice
Choose $x_1, x_2 \in LB_n$
And $r' \in LB_n$
Calculate $X = x_1^e r' x_2^e \| Id_A$
And $R = r' \| Id_A$
And $C_A = p(X) \ominus X_B(R) \quad ----(1)$
And also Calculate $x_1^e P_b x_2^e$

Alice decrypt $X_A(R')$ with its private key p.
Then,
i.g. $C_B \ominus X_A(R') = q(Y) \quad -----(3)$
and Alice encrypt $q(Y)$ with its public key $X_B(q(Y))$ and find Y and Alice verify that Y contain Id_B as suffix, Alice know the identity of bob.</td>
<td>C_A →

C_B ←</td>
<td>Bob
Choose $y_1, y_2 \in UB_n$
And $r'' \in UB_n$
And $Y = y_1^e r'' y_2^e \| Id_B$
And $R' = r'' \| Id_B$
And $C_B = q(Y) \oplus X_A(R') \quad ----(2)$

Bob decrypt $X_B(R)$ with its private key q.
Then,
i.g $C_A \ominus X_B(R) = p(X) \quad ----(4)$
and bob encrypt $p(X)$ with its public key $X_A(p(X))$ and find Y and bob verify that X contain Id_A as suffix, bob know the identity of Alice.</td>
</tr>
<tr>
<td colspan="3">Firstly, to find out the identity of each other, both make some calculation as</td>
</tr>
<tr>
<td>Calculate $k_A (= k_B) = p_1^e X_B p_2^e$
And $key_A = x_1^e k_{A_2}^e M_B k_{A_1}^e x_2^e$</td>
<td>M_A →
M_B ←</td>
<td>Calculate $k_B = q_1^e X_A q_2^e$
And $M_B = k_B^e y_1^e M_A y_2^e k_B^e$

Calculate $key_B = y_1^e M_A y_2^e$</td>
</tr>
<tr>
<td colspan="3">• In each above step, if key_A or key_B is I, then the protocol run is terminated with failure.
• So both Alice and Bob have secret key $K = key_A = key_B$ and both can communicate secretly for that session.</td>
</tr>
</table>

SECURITY ANALYSIS

Here we prove our protocol meets the following desirable attributes for essential security analysis.

Known-Key: If Alice and Bob execute the regular protocol run, both share unique session key K as shown in step 3.

Perfectness for Forward Secrecy: During the computation of the session key K for each entity, the random braids x_1, x_2 and y_1, y_2 still act on it. An adversary who may have captured their private keys p_1, p_2 or q_1, q_2 should extract k_A or k_B from the information M_A and M_B to know the previous or next session keys between them. However, this contradicts that RP is hard. Hence, under the assumption that the RP is secure, NKR-NAG meets the forward secrecy.

Key-Compromise Impersonation: Suppose Alice's long-term private key, p_1 and p_2 is disclosed. Now an adversary who knows this value can clearly impersonate Alice. Is it possible for the adversary to impersonate Bob to Alice without knowing Bob's long-term private key, q_1 and q_2. For the success of the impersonation, the adversary must know Alice's ephemeral key x_1 and x_2 at least. So, also in this case, the adversary should extract x_1, x_2 from Alice's ephemeral public value $M_A = x_1^e P_b x_2^e$. This also contradicts that RP is hard.

Unknown Key-share: Suppose an adversary Mallory now try to make Alice believe that the session key is shared with Bob, while Bob believes that the session key is shared with Mallory. To launch the unknown key-share attack, the adversary Mallory should set his public key to be certified even though he does not know his correct private key. For this, Mallory makes it by utility the public values X_A, X_B and P_b. With some simple calculations, we see that the unknown key-share attack fails.

Key Control: As the same argument in the above, the key-control is clearly impossible for the third party. The only possibility of key-control attack may be brought out by the participant of the protocol, Bob. But for participant Bob, in order to make him a party, Alice generate the session key $K(key_A)$ which is pre-selected value by Bob. For example Bob should solve the following $key_B = y_1^e M_A y_2^e$. But this again falls into the problem of RP.

Let us first check the properties that C_A and C_B do not reveal x_1, x_2 and y_1, y_2 respectively. From equation (1) and equation (2) can actually be viewed as result of encrypting $p_1^e(X), p_2^e(X)$ and $q_1^e(Y), q_2^e(Y)$ respectively using a string cipher with braid key $X_A(R')$ and $X_B(R')$ respectively; thus, the secrecy of $p_1^e(X), p_2^e(X)$ and $q_1^e(Y), q_2^e(Y)$ respectively depends on the r' and r'' in R and R' respectively.

Finally, non-repudiability of C_A and C_B follows from the fact that the value x_1, x_2 and y_1, y_2 respectively agreed to are concatenated to Alice and Bob identifier Id_A and Id_B.

CONCLUSION

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. In this paper, we have 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 root problems with 1/ *k* – biased bitstring.

In this paper, specially, the key sharing process will be start after being assured about the perfectness of sender's and receiver's identity. Hence, our proposed scheme is well secured and assured for sanctity of correctness about the sender's and receiver's identity.

REFERENCES

[1] Menezes, M. Qu, and S. Vanstone, "Key agree-ment and the need for authentication," in Proceedings of PKS'95, pp. 34-42, 1995.

[2] Atul Chaturvedi, Sunderlal" An Authenticated Key Agreement Protocol Using Conjugacy Problem in Braid Groups" in International Journal of Network Security Vol.6 No.2 p.p. 181-184, March, 2008.

[3] Bruce Schneier "applied cryptography, second edition" John wiley &sons, Inc.

[4] D.B.Ojha, J.P.Pandey, Ajay Sharma, and Abhishek Dwivedi, "A non-repudiable biased bitstring commitment scheme on a post quantum cryptosystem" Journal of Theoretical and Applied Information Technology, Vol. 12, No.1, 2010.

[5] E. Artin, "Theory of braids," Annals of Mathematics, vol. 48, pp. 101-126, 1947.

[6] K. Ko, S. Lee, J. Cheon, J. Han, J. kang C. Park. New public key cryptosystem using braid groups, Crypto'2000, LNCS 1880, pp.166-183, Springer 2000.

[7] L. Law, A. Menezes, M. Qu, J. Solinas, and S. Van-stone, An Efficient Protocol for Authenticated Key Agreement, Technical Report CORR98-05, Department of CO, University of Waterloo, 1998.

[8] L. Law, A. Menezes, M. Qu, J. Solinas, and S. Van-stone, "An efficient protocol for authenticated key agreement," Design, Codes and Cryptography, Vol.28, no. 2, pp. 119-134, 2003.

[9] M. Bellare, A. Desai, D. Pointcheval and P. Rogaway, Relations among notions of security for public-key encryption schemes, Advances in Cryptology | CRYPTO '98, Lecture Notes in Computer Science, 1462 (1998), Springer-Verlag, pp. 26-45.

[10] R.Dutta, R. Barua and P. Sarkar,"Pairing Based Cryptography: A Survey Cryptology e-print Archive", Report 2004/064, 2004.

[11] S. B. Wilson, D.Johnson, and A. Menezes,"Key agreement protocol and their security analysis," in Proceedings of Sixth IMA International Conference on Cryptography and Coding, pp. 30-45, 1997.

[12] W. Diffie and M.Hellman, "New directions in cryptography," IEEE Transactions on Information Theory, Vol. 22, no. 6, pp. 644-654, 1976.

AUTHORS

Abhishek Dwivedi, Master of Computer Application from Uttar Pradesh Technical University, Lucknow (U.P.), India in 2007. Pursuing Ph.D from Singhania University, Jhunjhunu, Rajsthan, India. He has more than four year experience in teaching and research as Assistant Professor. He is working at Raj Kumar Goel Engineering College, Ghaziabad (U.P.), India. His main research interests are in Public Key Cryptography and its applications.

Dr. Deo Brat Ojha, Ph.D from Department of Applied Mathematics, Institute of Technology, Banaras Hindu University, Varanasi (U.P.), India in 2004. His research field is Optimization Techniques, Functional Analysis & Cryptography. He has more than Six year teaching & more than eight year research experience. . He is working as a Professor at Raj Kumar Goel Institute of Technology, Ghaziabad (U.P.), India. He is the author/co-author of more than 50 publications in International/National journals and conferences.