International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 06 | June-2016 www.irjet.net p-ISSN: 2395-0072

Authenticated key agreement in division semi-rings

R. vijayaragavan

Department of Mathematics,

Thiruvalluvar University, Serkkadu, Vellore-632 115, India

rvijayaraagavantvu@gmail.com

Abstract – In this article we proposed authenticated key agreement protocol based on division semi-rings .The security of our protocol based on decomposition problem in division semi-rings.

Key Words: Authenticated key agreement protocol, Division semi-rings, decomposition problem

1.INTRODUCTION

Recent years in crypto logical research have witnessed several proposals for secure cryptographic schemes using noncommutative groups; in particular Artin's braid groups [1, 2, 3, 4, 5]. The idea of applying braid group as a platform for cryptosystems was introduced by Anshel et al [2]. Braid groups, on the one hand, are more complicated than Abelian groups and, on the other hand, are not too complicated to work with. These two characteristics make braid group a convenient and useful choice to attract the attention of researchers. In [3], Ko et al. proposed a braid group version of Diffie-Hellman key agreement [6]. Man-in-the-middle attack works on this protocol, which sets ground for our work, presented in this paper. We improve the above scheme by proposing a new authenticated key agreement protocol based on CSP in braid groups. We make use of Conjugacy Search Problem (CSP) to suggest a new key agreement scheme. The CSP in braid groups is algorithmically difficult and consequently provides one-way functions. We use this characteristic of CSP to propose a key agreement protocol which is resistant to Man-in-the middle attack. In [7] D. Ezhilmaran and V. Muthukumaran proposed new key exchange protocol based on decomposition problem in centralizer near-rings and secure the men-in-middle attacks. The security of author's scheme based upon the decomposition problem in near-ring. In this article we proposed new authenticated key agreement protocol based on division semi-ring.

The rest of the paper is organized as follows: We present a brief introduction of division semi-rings in Section 2. In Section 3, we give authenticated key agreement protocol. Section 4, we conclude the paper.

2. PRELIMINARIES

Definition 1

A semi-ring R is a non-empty set, on which operations of addition and multiplication have been defined as follows

i. $(\mathrm{R},+)$ is a commutative monoid with identity element 0
ii. $(\mathrm{R},\bullet)$ is a monoid with identity element 1
iii. Multiplication distributes over addition from either side
iv. $0\bullet r = r\bullet 0$ for all r in R

Definition 2

An element r of a semi-ring R, is a "unit" if and only if there exists an element r^1 of R satisfying $r\bullet r^1 = r^1\bullet r = 1$The element r^1 is called the inverse of r in R. If such an inverse r^1 exists for a unit r, it must be unique. We will normally denote the inverse of r by r^{-1}. It is straightforward to see that, if r & r^1 units of R, then $r\bullet r^{-1} = r^{-1}\bullet r = 1$ & In particular $(r^{-1})^{-1} = r$. We will denote the set of all units of R, by $U(R)$.This set is non-empty, since it contains "1" & is not all of R, since it does not contain "0". we have just noted that $U(R)$ is a sub-monoid of $(R,\bullet)$, which is in fact a group. If $U(R) = \mathrm{R}/\{0\}$, Then R, is a *division semi-ring.*

The Decomposition Problem (DP). Given $(x, y) \in R\times R$ and $S \subseteq R,$ the problem is to find $z_1, z_2 \in S$ such that $y = z_1 x z_2$.

3. PROPOSED SCHEME

3.1 Key Agreement protocol in Decomposition Problem in Division semi-rings

Step 1: One of the parties Alice publishes a random element $\beta \in R$

Step 2: Alice chooses $a_1, a_2 \in R$ and sends $a_1 \beta a_2$ to Bob

Step 3: Bob chooses $b_1, b_2 \in R$ and sends $b_1 \beta b_2$ to Alice

Step 4: Alice computes $K_A = a_1 b_1 \alpha a_2 b_2$ and Bob computes $K_B = a_1 b_1 \alpha a_2 b_2$

If $a_i b_i = b_i a_i$ then $K_A = K_B$ in R .Thus Alice and Bob have a shared secret key

3.2 Authenticated Key Agreement Protocol

Known-key security: A protocol is considered to be known session key secure if it remains unaffected achieving its goal in the face of an adversary who has learned some previous session keys.

Forward secrecy: A protocol enjoys forward secrecy if the secrecy of the previous session keys is not affected when the long term private keys of one or more entities are compromised. Perfect forward secrecy refers to the scenario when the long term private keys of all the participating entities are compromised.

Key-compromise impersonation resistance: Suppose Alice long term private key is disclosed. Then an adversary who knows this value can now impersonate A since it is precisely the value which identifies Alice. We can say that a protocol is *key compromise impersonation resistant* if this loss will not enable an adversary to masquerade as other legitimate entities to A as well or obtain other parties secret key.

Unknown key share resistance: In an *unknown-key share attack* an adversary convinces a group of entities that they share a key with the adversary whereas in fact, the key is shared between the group and another party. This situation can be exploited in a number of ways by the adversary when the key is subsequently used to provide encryption of integrity.

Key control resistance: It should not be possible for any of the participants (or an adversary) to force the session key to a presume value or predict the value of the session key.

4. CONCLUSIONS

In this article we discussed authenticate key agreement protocol base in division semi-rings and security of our protocol depending on decomposition problem in division semi-rings.

REFERENCES

[1] I. Anshel, M. Anshel, B. Fisher, and D. Goldfeld, "New key agreement protocols in braid group cryptography," in Proceedings of the CT-RSA 2001, LNCS 2020, pp. 1-15, Springer-Verlag, 2001.

[2] I. Anshel, M. Anshel, and D. Goldfeld, "An algebraic method of public-key cryptography," Mathmetics Research Letters, vol. 6, pp. 287-291, 1999.

[3] 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," in Advances in Cryptology (Crypto'00), LNCS 1880, pp. 166-183, SpringerVerlag, 2000.

[4] K. H. Ko, D. H. Choi, M. S. Cho, and J. W. Lee, "New signature scheme using conjugacy problem." (http://eprint.iacr.org/2002/168)

[5] H. Sibert, P. Dehornoy, and M. Girault, "Entity authentication schemes using braid word reduction," in Discrete Applied Mathematics, vol. 154, no. 2, pp. 420-436, 2006.

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

[7] D. Ezhilmaran and V. Muthukumaran, "Key Exchange Protocol Using Decomposition Problem In Near-Ring," *Gazi University Journal of Science*, *29*(1), 123-127, 2016.