Authentication scheme using division semi-rings

R. vijayaragavan

Department of Mathematics,

Thiruvalluvar University, Serkkadu, Vellore-632 115, India

rvijayaraagavantvu@gmail.com

---***---

Abstract - *In this article we proposed a new authentication scheme based on the division semi-rings. The security of our authenticated protocol based on conjugacy. Security issues also discussed.*

Key Words: Authentication scheme, division semi-rings, conjugacy problem

1.INTRODUCTION

Diffie and Hellman first proposed the idea of public key distribution in which two parties exchanging only public information over an insecure channel could establish a secret key for use in a conventional cryptosystem such as the data encryption standard. Many Public key cryptosystem schemes have been proposed and broken. Today most successful Public key cryptosystem schemes are based on the perceived difficult to certain problems in particular large finite commutative rings. For example, the difficulty of solving the integer factoring problem defined over the ring Z_n forms the ground of basic RSA cryptosystems [2]. In [4] 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. In [5] D. Ezhilmaran and V. Muthukumaran proposed a Diffie-Hellman and Fiat-Shamir like zero-knowledge authentication schemes based on near -rings has been proposed and also security issues have been discussed. The security of author's scheme based upon the decomposition problem in near-ring The extended multi-dimension RSA cryptosystem [3], which can efficiently resist low exponent attacks, is also defined over the commutative ring $Z_N[x]$.In this paper we described new authentication based on conjugacy problem in division semi-rings.

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 Conjugator Search Problem (CSP). Given $(x,y)\in R\times R$, the problem is to find $z\in R$ such that

$$y = z^{-1}xz.$$

3. PROPOSED AUTHENTICATION SCHEME IN CONJUGACY PROBLEM IN DIVISION SEMI-RINGS

Initial Setup: Suppose that the division semi-ring $(\mathrm{R},+,\circ)$ is the underlying work fundamental infrastructure and NPSD problem is intractable on the non-commutative group $(\mathrm{R},\circ)$. Choose two small integers $m,t\in Z$. let $H:\mathrm{R}\to\mathrm{M}$ be a cryptographic hash function which maps from R to the message space M.

Then, the public parameters of the system would be the tuple $\langle \mathrm{R}, \mathrm{M}, H \rangle$.

Key Generation: First Alice selects two random elements $x, y_1 \in R$ private key, compute $y_1 = z_1^{-1} x z_1$. and publishes her public key $(\mathrm{x}, \mathrm{y}_1, \mathrm{z}_1) \in R^3$.

Authentication: To begin authentication,

1. Bob select randomly $y_2 = z_2^{-1} x z_2$. then sends to Alice.
2. Alice sends the response $w = (z_1^{-1} x z_1)$ to Bob, and Bob checks $w = H(z_1^{-1} x z_1)$.

3.2 Security analysis

Completeness: Assume that at step (2), Alice sent $\tilde{w}$ .Then Bob accepts Alice's key if and only if $\tilde{w} = H(z_1^{-1} x z_1)$. The latter relation is equivalent to

$$\tilde{w} = H(z_1^{-1} z_2^{-1} x z_2 z_1)$$
$$= H(z_2^{-1} z_1^{-1} x z_1 z_2)$$
$$\tilde{w} = H(z_1^{-1} x z_1).$$

$$\tilde{w} = w.$$

Hence the proof

4. CONCLUSIONS

In this article we discussed authentication scheme based on the division semi-rings. Our proposed authentication secure against men-in-middle attack. The security of our protocol depending on conjugacy problem.

REFERENCES

[1] Anshel M, "Braid Group Cryptography and Quantum Cryptoanalysis" Proceedings of the 8th International Wigners Symposium,New York press, 2003.

[2] Rivest R.L, Shamir A and Adleman L, "A method for obtaining digital signatures and public key cryptosystems" Communications of the ACM, 1978, vol.21, pp.120-126,.

[3] Cao Z, "The multi-dimension RSA and its low exponent security" Science in China, 2000, vol.43, pp.349-354.

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

[5] V. Muthukumaran and D. Ezhilmaran, "Symmetric decomposition problem in zero knowledge authentication schemes using near- ring structure" *International Journal of Applied Engineering Research,*Vol-11,pp.36-40, 2016.