Efficient authentication scheme based on near-ring root extraction problem

IOP Conf. Series: Materials Science and Engineering **263** (2017) 042137 doi:10.1088/1757-899X/263/4/042137

Efficient authentication scheme based on near-ring root extraction problem

V Muthukumaran and D Ezhilmaran
Department of Mathematics, School of Advanced Sciences, VIT-University, Vellore-632014, India

E-mail: muthu.v2404@gmail.com

Abstract. An authentication protocolis the type of computer communication protocol or cryptography protocol specifically designed for transfer of authentication data between two entities. We have planned a two new entity authentication scheme on the basis of root extraction problem near-ring in this article. We suggest that this problem is suitably difficult to serve as a cryptographic assumption over the platform of near-ring N. The security issues also discussed.

1. Introduction

Now a day's many cryptograph protocol proposed on the basis of non-commutative algebraic structure [1]. In 2007 M.M. Chowdhury proposed two pass authenticated scheme based on non-commutative semi-group [2]. H. Sibert et.al proposed entity authentication scheme based on braid word reduction problem and security of his scheme based on root extraction problem [3]. In 2016 Muthukumaran and Ezhilmaran proposed a symmetric decomposition problem in zero-knowledge authentication schemes using near- ring structure [8]. Lal and Chatervedi propose new two Identification scheme established on REP in non-commutative groups [4]. In 2015 Pratik Ranjan Hari Om cryptanalyze the Lal and Chaturvedi's braid group based authentication schemes insecure in the passive and active attack [5]. The root extraction problem has been widely used in cryptography protocols: see for example [6].In 2008 Vladimir Shpilrain and Alexander Ushakov introduced zero-knowledge authentication schemes established on TCSP problem in the group [7]. In this article, we introduce the Near-ring Root Extraction Problem (NREP) and propose two authentication scheme based on near-ring. First authentication scheme based on NREP and second one is a combination of conjugacy based NREP problem. The security relies on NREP. We have proven that an adversary cannot break the protocol without knowing NREP in near-ring. The security issues are also discussed.

The paper is comprises of following sections.In section 2 we recall some basic definition of near-ring, near-ring root extraction problem and twisted conjugacy search problem in near-ring. In section 3 we proposed two authentication schemes based on near-ring and security issues also discussed and section 4 conclude the article.

2. Preliminaries

Definition 1: Let $(N,+,\bullet)$ be a set with two binary operations + and $\bullet$ satisfying

i. $(N,+)$ is a group

ii. $(N,\bullet)$ is a semi-group

iii. $(n_1+n_2).n_3 = n_1.n_3 + n_2.n_3$

2.1. Cryptography assumption in near-ring

In this subsection, we introduce two cryptography assumption. In the near-ring, we define the following cryptographic problems which are related to our authentication schemes.

Near-ring Root Extraction Problem:
Instance: For given $z \in N$ and an integer $a \geq 2$.

Objective: Find $x \in N$ such that $z = x^e$ if such an x exists.

Twisted Conjugacy Search Problem (TCSP)

Instance: $\varphi, \psi \in End(N), \omega, t \in N$

Objective: Find $a \in N$ so that $t = \varphi(\mathrm{a})\omega\psi(\mathrm{a}^{-1})$.

3. Proposed authentication schemes

The role of Trusted Authority (TA):

In our proposed scheme, Alice and Bob want to communicate securely using a public channel. We introduce a trusted third party, which is the mediator in this communication channel. This is very common and practically implementable scheme. Here we assume that the TA is kept in very secret and safe place and can control the secure communication very efficiently. So, for an attacker, it is very tough to break the security of this system.

Initial setup:

Consider N be non-commutative near-rings which consists twosubnear-rings of $N_1, N_2 \in N.$ the are finitely generated and publishes the user. The element of subnear-rings satisfies the commutative axioms. We also consider H as a collision-free of near-ring.

Scheme-I

Phase I. Key generation

i. Alice choose two arbitrary integers $m \geq 2 \, and \, n \geq 2;$

ii. Alice choose $a_1 \in N_1, and \, a_2 \in N_2$ such that NREP for a_1, a_2 is hard enough;

iii. Alice computes $y = (a_1)^m (a_2)^n;$

iv. Alice P_{uk} is (y, m, n) and the secret key is the pair $(a_1, a_2).$

v. Alice sends the value of the y to the trusted authority through a secure channel.

Phase II. Entity authentication

i. Bob choose $b_1 \in N_1, b_2 \in N_2,$ and sends the challenge $f = (b_1)^m (b_2)^n$ to Alice.

ii. Alice sends the response $\omega = H((a_1)^m f (a_2)^n)$ to Bob. Bob get the value of y from trusted authority through a secure channel and checks if $\omega' = \mathrm{H}((b_1)^m y(b_2)^n)$.

If they match, authentication is successful.

Proof

$$\begin{aligned}\omega' &= H((b_1)^m((a_1)^m(a_1)^n)(b_1)^n) \\ &= H((a_1)^m((b_1)^m(b_1)^n)(a_1)^n \\ &= H((a_1)^m f(a_1)^n) \\ &= \omega\end{aligned}$$

Proposition 3.1

Our entity authentication scheme-I is a completely Zk-nesscollective proof of knowledge of $a_1 \, and \, a_2.$

Completeness:

Phase II (ii), Alice sent ω' through trusted authority. The Bob accept's Alice's key iff we have $\omega' = H(b_1)^m y(b_2)^n)$ is equal to

$$\omega' = H(b_1)^m((a_1)^m(a_2)^n)(b_2)^n) \qquad (3.1.1)$$

By hypothesis, $a_1, b_1 \in N_1$ while $a_2, b_2 \in N_2,$ so that $a_1 a_2 = a_2 a_1 \, and \, b_1 b_2 = b_2 b_1.$ Therefore Equation 1 is equivalent to $\omega' = \omega$

Soundness:

Attacker(C) is recognized with non-negligible and C calculate $H(b_1)^m y(b_2)^n)$ with non-negligible probability. Then H is ideal hash functionof C then calculates ω and verifying $H(\omega) = H((b_1)^m y(b_2)^n)$ with non-negligible probability. We have two options $\omega = (b_1)^m y(b_2)^n,$ which challengesto find $b_1 \, and \, b_2$ is hard, or $\omega \neq (b_1)^m y(b_2)^n.$

Honest-verifier zero-knowledge:

Take the probabilistic Turing machine defined as follows: selectingasubnear-rings b_1 *and* b_2 *the* outputs the instance $(b_1, b_2, H(b_1)^m y(b_2)^n))$. Then they getting same probability function (A, B).

Scheme-II

Phase I.Key generation:

Alice select a secret element a in N and compute $b = a^2$, such that the TCSP for a and b, the NREP for b are hard; Pu_k is b, Pv_k is a.

Phase II.Authentication:

i. Alice selects element random element x, and sends $y = \varphi(x)b\psi(x^{-1})$ to Bob (B).

ii. Bob sends a random bit δ to Alice.

iii. For $\delta = 0$, Alice sends $z = x$ to Bob; then Bob check $y = \varphi(z)b\psi(z^{-1})$.

iv. For $\delta = 1$, Alice sends $z = \varphi(x)a\psi(x^{-1})$ to Bob; then Bob check $y = z^2$.

Proposition 3.2

Our entity authentication scheme-II is a ZK-ness interactive proof of knowledge of z.

Completeness:

In Phase II (ii), we have $y = \varphi(x)b\psi(x^{-1})$ i.e. $y = \varphi(z)a\psi(z^{-1})$. in step (iv) and we find $y = z^2$.

$$y = \varphi(x)b\psi(x^{-1}) \text{ and } z = \varphi(x)\,a\,\psi(x^{-1})$$
$$z^2 = \varphi(x)a^2\psi(x^{-1})$$
$$= \varphi(x)b\psi(x^{-1})$$
$$z^2 = y \text{ or } y = z^2$$

Hence Bob accepts a correct answer at each round therefore Bob agree Alice proof of identity with probability 1.

Soundness:

Attacker A' is implementation tree of (A', B). Every vertex A' has computed z and z' satisfying $\varphi(z)b\psi(z^{-1})$ and $y = z^2$. This implies $\varphi(z)\varphi(z')b\psi(z^{-1})\psi(z'^{-1})$ are equal to $y = z^2$, using TCSP with NREP for y and z. Indeed, the $\varphi(z')^{-1}\psi(z)$ enable to the z.

Honest-verifier zero-knowledge:

ZK-ness accepting inputs are of the type $(y, 0, z)$ and $(y, 1, z)$ to generate the instances $(y, 0, z)$, we choose a near-ring specifies z at random we take $y = \varphi(x)b\psi(x^{-1})$.

Assume that $(y, 1, z)$ a twisted conjugate of a will be revealed in any case, we can accept, without cost of simplification, in near-ring $a' = \varphi(q)\,a\,\psi(q^{-1})$ of the twisted conjugate class of a is distributed at key generation. Choose a specifies x at random, and take $z = \varphi(x)a'\psi(x^{-1})$ and $y = z^2$. Then we have $z = \varphi(xq)b\psi(xq)^{-1}$ and $y = (xq)a^2\psi(xq)^{-1} = (xq)b\psi(xq)^{-1}$, so, as $x \to xq^{-1}$ is a one to one of N and probability distribution is consider to the right invariant and getting same probability function.

4. Conclusions

In this article, we presented a two authentication scheme based near-ring. The first authentication scheme is two pass protocols depending on a NREP and second authentication scheme based on a combination of NREP with TCSP. The proposed authentication scheme is proved to be secure against passive and active attacks.

References

[1] Anshel I, Anshel M and Goldfeld D 1999 *Mathematical ResearchLetters,* **6** 287-292
[2] Chowdhury M 2007 *arXivpreprint arXiv:*0708.2395
[3] Sibert H, Dehornoy P and Girault M 2006 *Discrete Applied Mathematics*, **154**(2) 420-436
[4] Lal S and Chaturvedi A 2005 *arXivpreprintcs/0507066*.
[5] Ranjan P and Om H 2015 *In Next Generation Computing Technologies,IEEE*, 432-436
[6] Wang B C and Hu Y P 2009 *IET Information security*, **3**(2) 53-59
[7] Shpilrain V and Ushakov A 2008 *In Applied Cryptography and Network Security. Springer Berlin/Heidelberg,* 366-372
[8] Muthukumaran V and Ezhilmaran D 2016 *Int. J. App. Eng. Res.* 0973-4562