IOP Conf. Series: Materials Science and Engineering **263** (2017) 042131 doi:10.1088/1757-899X/263/4/042131

A new identification scheme based on near-ring root extraction problem

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

E-mail: arunmamkumaran@gmail.com

Abstract. An Identification scheme is an important and useful cryptographic tool for authentication. In this paper we propose a new Identification scheme based on near-ring root extraction problem. Given a Near polynomial ring $N(x)$ over a near-ring N, an integer $n \geq 2$ and a polynomial $f \in N(x)$, find a polynomial g∈N(x) such that $f = g^n$ (assuming one such g exists). The security of the proposed scheme is tied to the near-ring root extraction problem. We have discussed about the active attacks in this paper. The above protocol is verified with an illustration.

1. Introduction

In 1976 Diffie Hellman discovered a Public Key Cryptography (PKC)[4]. Since then there are a lot of public key schemes been designed.In that every person who wants to exchange his message to another authentically uses a pair of keys that is public key and the secret key. The secret key is known only to the sender and the public key is known to anybody, but knowing the public key one could find insufficient to retrieve the secret key in a reasonable time. As the public keys are not protected for confidentiality, it leads in many active attacks. One can replace a false public key to a true public key in a directory. Hence in order to avoid this along with both the secret and public key we can include the identification string.

The identification scheme is an important and useful cryptographic tool. This scheme enables the prover to identify himself to the verifier authentically. Typical implementations of the schemes are suited for microprocessor-based systems such as smart cards, personal computers, control systems, etc. Fiat and Shamir proposed their identification scheme using factorisation problem [7]. Guillou, Quisquater [2] and Schnorr proposed schemes are based on discrete logarithm problem. Now a days more identification protocols are developed using the root extraction problem which are crucial in maintaining the security.

The root extraction problems over Braid groups are widely used in cryptographic protocol. In [7] the identification schemes are in a non-commutative group. Many authentication schemes are based in the non-commutative rings. Here we establish a new identity scheme using a non-commutative structure, a near polynomial ring over a near-ring. The securities of the scheme rely on the near-ring root extraction problem. In Section 2 Cryptographic problem over a near-ring is presented. In Section 3, we propose a new identification scheme using near polynomial ring. In section 4 under security consideration we discuss the possible attacks in our scheme. A toy example is illustrated in section 5. We conclude the paper in section 6.

2. Preliminaries

Identification Scheme: An identification scheme is a protocol between the prover and the verifier. It consists of the following randomized algorithm.

- The polynomial time key generation algorithm: In this algorithm there is an input security parameter which returns outputs a pair of secret and public key.
- The commitment algorithm: This algorithm is run by the prover to initiate his identification.
- The challenge algorithm: In this the verifier generates a challenge.
- The response algorithm: The prover generates a response using the public key, secret key, random variable and the challenge in this algorithm.
- The verification algorithm: In this algorithm the verifier determines whether to accept or not the response.

2.1. Definition

A near-ring is a set N together with two binary operations '+' and '•' such that

a. (N, +) is a group (not necessarily abelian).
b. (N, •) is a semigroup.
c. For all $n_1, n_2, n_3 \in N$; $(n_1 + n_2)\bullet n_3 = n_1\bullet n_3 + n_2\bullet n_3$ (right distributive law).

This near-ring will be termed as right near-ring. If $n_1(n_2 + n_3) = n_1\bullet n_2 + n_1\bullet n_3$ instead of condition (c) the set N satisfies, then we call N a left near-ring.

2.2. Definition

Special form of Near-ring defined in [11]

a. (N,+) is a group with 0 as the additive identity.
b. For all $n_1, n_2 \in N$ we define $n_1, n_2 = n_1$. Hence (N, •) is a semigroup.
c. $1 \in N$ is such that 1. $n = 1$ for all $n \in N$
d. $(n_1 + n_2)n = n_1 n + n_2 n$ is the only distributive law satisfied by N for all $n_1, n_2, n \in N$.

2.3. Definition

Let (N, +, •) be a near-ring and x an indeterminate. $N(x)$ will be called near polynomial ring where

$$N(x) = \sum_{i=1}^{\alpha} n_i x^i \,/\, n_i \in N$$

Let $N(x)$ be a near polynomial ring.

For $0 \neq f(x) = a_0 + a_1 x + \ldots + a_m x^m$ where $a_m \neq 0 \in N$.

The addition of polynomials

$$f(x) + g(x) = \sum_{i=0}^{n} a_i x^i + \sum_{i=0}^{m} b_i x^i = \sum_{i=0}^{m} (a_i + b_i) x^i + \sum_{i=m+1}^{n} a_i x^i \text{ if } n \geq m.$$

$0 = 0 + 0x + .. + 0x^n + \ldots$ is the zero polynomial. clearly $(N(x), +)$ is a group.

for $f(x), g(x) \in N(x)$ define '$\circ$' as $f(x) \circ g(x) = f(x)$.

Clearly $(N(x), \circ)$ is a semi group.

for $f(x), g(x), h(x) \in N(x)$.

$[f(x) + g(x)]h(x) = f(x) \circ h(x) + g(x) \circ h(x)$ satisfying the near ring distributivity.

Hence $(N(x), +, \circ)$ is a near ring called the near polynomial ring.

Example:
Let $Z_2 = \{0,1\}$ be the near-ring. $Z_2[x]$ is near polynomial ring.
Let $Z_3 = \{0,1,2\}$ be the near-ring. $Z_3[x]$ is near polynomial ring.

2.4. Cryptographic problems over a near-ring

2.4.1. Near polynomial ring over a near-ring:
Let $N(x)$ be a near polynomial ring over a near-ring N. We define $P_x = \{f(x) \in N(x) / f(0) \neq 0\}$ the set of all polynomial in $N(x)$ with non zero constant term and all the polynomials are irreducible.

2.4.2. Cryptographic problem:
Near ring-root extraction problem: Given a polynomial $f \in N(x)$ and an integer $n \geq 2$, find $g \in N(x) \ni f = g^n$ if such 'g' exists.

3. Proposed identification scheme
The new identification scheme is based on zero knowledge interactive proof and the identity-based scheme. The security of this scheme works on the difficulty of extracting the near ring-root problem. In this scheme we assume the trusted centre or trusted authority issue the randomly chosen secret key P_s to the prover/user. Now the prover demonstrate his/her identity to the verifier using the properties of the secret key P_s. The public key which is computed using the secret key becomes the function of provers identity. Let C be the challenge space for $t \in N$ times we repeat the protocol in order to make the brute force attack less than $\frac{1}{|c|^t}$ is the probability of this attack is nearer to '0'.

3.1. Key generation
Let P be the prover/user, V be the verifier and T be the Trusted Authority/Trusted Centre. Initially the Trusted Authority T selects an integer $e \geq 2$. Now the Trusted Authority T computes the public key Y using the secret key $X \in P_x$ follows $Y = X^e$. T publishes the public key Y and sends the secret key X to the prover P.

3.2. Identification Scheme based on the following protocol
Prover P has to prove his/her identity to the verifier V using the algorithm $t \in N$ iterations. V accepts P's identification if and only if all 't' iterations are completed successfully.
Step 1 P selects a random secret polynomial $P_1(x) \in P_x$ and then computes $r(x) = [P_1(x)]^e$.
Step 2 P sends $r(x)$ to V.
Step 3 Now V selects a random integer ν (the challenge), $\nu \in C \subseteq [0, e-1]$ and sends to P.
Step 4 P computes $U(x) = P_1(x)\, X^{\nu}$ and sends to V.
Step 5 V accepts the protocol execution if and only if $U(x) \neq 0$ and $U(x)^e = r(x)Y^{\nu}$.
Verification of the protocol works as follows.

$$\begin{aligned} r(x)Y^{\nu} &= (P_1(x))^e Y^{\nu} \\ &= (P_1(x))^e (X^e)^{\nu} \\ &= (P_1(x) X^{\nu})^e \\ &= [U(x)]^e \end{aligned}$$

4. Security considerations of our scheme

4.1. Trusted authority in security consideration

The Trusted Authority chooses a secret key X and send to the prover P. Assume that A the adversary for P does not know X, He can guess and find out the secret key X taking the e^{th} root of Y however the probability for this event to happen is only $\frac{1}{2^e}$ iteration and for the whole protocol it takes the probability $\frac{1}{2^{et}}$ that is 2^{-et}. As we select $e \geq 2$ to be a large integer the probability for an adversary A to find the secret key X is negligible. Hence we assume that the trusted party can control the secure communication very efficiently as it is very tough for the attacker to break the security system which is built under hardness of near ring-root problem.

4.2. Insider Attack

If any manager of the system purposely leaks the secret information which leads to serious security flows of authentication scheme, the intruder finds difficult to extract the secret key from the message because of the near ring-root problem of the near polynomial ring where all the polynomials are with non-zero constant terms and are irreducible.

4.3. Active Attack

The adversary A tries to prove himself as a prover to the verifier, before the impersonation he interacts with the prover P numerous time. If the adversary A proves his identity by impersonating P to the verifier, the protocol will not be executed successfully, as the prover and verifier only knows $r(x)$ and ν. To find $r(x)$ the adversary has to find the polynomial $P_1(x) \in P(x)$ which is difficult by our cryptographic problem near ring-root problem. Similarly he has to try $e-1$ times to find ν (the challenge) which has time complexity as they select e as a larger integer. Hence our Identification Scheme is secured against impersonation.

5. Illustration

Let $N = \{0,1,2\}$

$N[x] = \{0,1,2,x,2x,x+1,x+2,2x+1,2x+2,x^2,2x^2,x^2+1,x^2+2,2x^2+1,2x^2+2,x^2+x,x^2+2x,$
$x^2+x+1,x^2+x+2,x^2+2x+1,x^2+2x+2,2x^2+x+1,2x^2+x+2,2x^2+2x+1,2x^2+2x+2,2x^2+x,\ 2x^2+2x\}$

Consider $P_x = \{1,2,x+1,x+2,2x+1,2x+2,x^2+1,x^2+2,2x^2+1,2x^2+2,x^2+x+1,x^2+x+2,$
$x^2+2x+1,\ x^2+2x+2,2x^2+x+1,2x^2+x+2,2x^2+2x+1,2x^2+2x+2\}$

Let $X = 2x^2+1 \in P_x, e = 7 \geq 2$.

Now T publishes the public key $Y = X^e = (2x^2+1)^7 = 2x^{14}+x^{12}+\ 2x^8+x^6+2x^2+1$ and sends the private key $X = 2x^2+1$ to P.

P selects $P_1(x) = x^2+1$ and computes $r(x) = P_1(x)^e = (x^2+1)^7 = x^{14}+x^{12}+2x^8+2x^6+x^2+1$ and send to V.

Now V selects $v = 1$ where $1 \in [0,6]$ and sends to P.

P computes $U(x) = P_1(x)X^v = (x^2+1)(2x^2+1) = 2x^4+1$ and sends to V.

Now the verifier V verifies the algorithm as follows.

$r(x)Y^v = (x^{14}+x^{12}+2x^8+2x^6+x^2+1)(2x^{14}+x^{12}+2x^8+x^6+2x^2+1)$

$= 2x^{28}+x^{24}+2x^{16}+x^{12}+2x^4+1.$

$[U(x)]^e = (2x^4+1)^7$

$= 2x^{28} + x^{24} + 2x^{16} + x^{12} + 2x^4 + 1$.

Hence V accepts the protocol as $U(x)^e = r(x)Y^v$ and $U(x) = 2x^4 + 1 \neq 0$.

6. Conclusion

Our proposed identification scheme using Near polynomial ring over the near-ring meets all the security considerations. We have proved that our scheme is secured against active attack, insider attack etc. The security of this scheme depends on the difficulty of near ring-root extraction problem. In future we want to develop the multi-server identification scheme using near ring-root extraction problem over the Near polynomial ring, also would discuss about the concurrent active attack in it.

References

[1] Wang B C and Hu Y P 2009 *IET Information Security* **3**(2) 53-59

[2] Guillou L C and Quisquater J J 1988 *Advances in Cryptology-Encrypt'88* Proceeding: Springer Verlag 123-128

[3] Pratik Ranjan and Hari Om 2015 *NGCT*

[4] Diffie W and Hellman ME 1976 *Transactions on Information Theory* IEEE **22(**5) 644-654

[5] Ferrero and Giovanni 2013 Springer Science & Business Media

[6] Gentry C, Szydio M and Knudsen In L (editor) 2002 *Advances in Cryptology* EUROCRYPT **2332** of Lecture Notes in Computer Science Springer-Verlag 299-320

[7] Fiat A and Shamir A 1987 *In Advances in Cryptology* Springer-Verlag 186-194

[8] Arunma M, Ezhilmaran D 2016 *Int. J. Applied Engineering Research* ISSN 0973-4562 **11**(1)

[9] Pils G 1983 North Holland American Elsevier

[10] Clay J R 1992 Oxford Science Publication New York

[11] Kandasamy W V 2002 Infinite Study