ISSN: 0975-766X
CODEN: IJPTFI
Available Online through *Research Article*
www.ijptonline.com

A PROXY SIGNATURE SCHEME BASED ON NON-COMMUTATIVE SEMI-RINGS

R.Vijayaragavan*
Associate Professor, Department of Mathematics, Thiruvalluvar University, Serkkadu, Vellore-632 115
Email: rvijayaraagavantvu@gmail.com

Received on 24-04-2016 *Accepted on 26-05-2016*

Abstract

Proxy signatures, introduced by Mambo, Usuda and Okamoto, allow a designated person to sign on behalf of an original signer. Semi-ring has been playing an important role in the theory of cryptography as these are non-commutative semi-rings used in cryptography. Some digital signature schemes have been given but no proxy signature has been introduced over semi-rings .In this paper we have proposed proxy signature scheme using conjugacy search problem over non-commutative semi rings.

Key Words: Proxy Signature, Conjugacy Decision Problem, non-commutative semi-rings, Conjugacy.

1. Introduction

The concept of blind signatures was introduced by D. Chaum [1]. A blind signature scheme is a cryptographic primitive in which two entities a user and a signer are involved. It allows the user to have a given message signed by the signer, without revealing any information about the message or its signature. Blind signatures are the basic tools of digital cash payment systems, electronic voting systems etc.

Proxy signatures as mentioned in [2] allow a designated person called proxy signer, to sign a message on behalf of an original signer. According to the delegation type, the proxy signatures are classified as full delegation, partial delegation and delegation by warrant. In this paper we are introducing a proxy signature scheme over non-commutative semi-rings.

The base for our construction is conjugacy search problem in non-commutative semi-rings. In conjugacy decision problem is easy to compute and conjugacy search problem is computationally hard. In thisarticle we propose a first proxy signature scheme over non-commutative semi-rings. This demonstrates the usefulness of semi-rings in cryptography as implementation over a computer system.

2. Preliminaries

Definition

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

i. $(R,+)$ is a commutative monoid with identity element 0

ii. $(R,\bullet)$ 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

2.1 Further cryptographic assumptions on Non-commutative semi-rings

We consider some mathematically hard problem in near-rings. We say that x and y are conjugate if there is an element a such that $y = axa^{-1}$.

Conjugacy Decision Problem (CDP)

Instance: $(x, y) \in R \times R$ such that $y = axa^{-1}$ for some $a \in R$.

Objective: Determine whether x and y are conjugate or not

Conjugacy Search Problem (CSP)

Instance: $(x, y) \in R \times R$ such that $y = axa^{-1}$ for some $a \in N$.

Objective: Find $b \in R$ such that $y = bxb^{-1}$.

3. Proposed Proxy Signature Scheme

In this section we analysis proposed scheme. Let the message to be signed be $m \in \{0,1\}^*$, *and* $H : \{0,1\}^* \to R$ *and* $H_1 : R \to \{0,1\}^*$ be one way hash functions.

3.1 Key generations using non-commutative semi-ring in conjugacy problem

Generation of secret and public keys:

Select a $y \in R$ and compute $y' = byb^{-1}$ such that b is secret key and public key is (y, y').

Temporary key generation by the user: Alice choose a random $b_1, \beta_1 \in R$ such that $y_1' = b_1 y_1 b_1^{-1}$ and compute $b_1\beta_1 = T_p$ as the self-proxy and $z = b_1\beta_1 y_1 b^{-1}{}_1\beta_1^{-1}$ as the proxy public key.

Generation of Self proxy warrant: Alice user her proxy key to generate the self- proxy warrant as follows:

$$\sigma = T_p y_1 T_p^{-1}, h = H_1\left[H_2(\sigma) \square m_w\right], \alpha = \beta_1 h \beta_1^{-1}$$

$$\theta_1 = (m_w, \sigma, \alpha)$$

is considered as the warrant on message 'm'.

Anyone can verify the warrant as $\alpha\sigma \sim hy_1^{'}$:

$$\begin{aligned}\alpha\sigma &= \beta_1 h \beta_1^{-1} T_p y_1 T_p^{-1} \\ &= \beta_1 h \beta_1^{-1} b_1 \beta_1 y_1 (b_1\beta_1)^{-1} \\ &= \beta_1 h \beta_1^{-1} b_1 \beta_1 y_1 \beta_1^{-1} b_1^{-1} \\ &= \beta_1 h (b_1 y_1 b_1^{-1}) \beta_1^{-1} \\ &= \beta_1 (h y_1^{'}) \beta_1^{-1} \\ \alpha\sigma &\sim h y_1^{'}\end{aligned}$$

Generation of self-proxy signature: Alice chooses a random $c \in R$ and computes

$$s_1 = c^{-1} y_1 c, H = H_1\left[H_2(\alpha) \square m_w\right],$$

$$s_2 = s_1 c T_p s_1^{-1} H s_1 T_p^{-1} c^{-1} s_1^{-1}$$

$$s_3 = s_1 c y_1 c^{-1} s_1^{-1}, s_4 = T_p s_1^{-1} H s_1 T_p^{-1}, s_5 = s_1 H s_1^{-1}$$

$$\theta_1 = (m_w, s_1, s_2, s_3, s_4, s_5)$$

Is signature generated by Alice on message 'm'

Verification of Self proxy signature: One can compute $H = H_1\left[H_2(\alpha) \square m_w\right]$ and accepts iff the conjugacy of the following can proven:

$$s_2 \sim H, s_1 \sim y_1, s_2 s_3 \sim s_4 s_1, s_4 z \sim s_5 y_1$$

4. Analysis of Proposed Schemes:

The security of the proposed scheme depends on conjugacy search problem as finding c from $s_1 \sim y_1$ is conjugacy search problem. Also find $b_1\beta_1$ from $s_4 z \sim s_5 y_1$ is a base problem 1.

Verifiability: Alice public key (y_1), self-proxy public key (z) and message warrant (m_w) appears in the verification process $s_4 z \sim s_5 y_1$ which is sufficient for the verifier to get convinced that the signatures are generated by Alice using the self- proxy concept.

Strong Identifiability: Warrant (m_w) used in the verification of the signatures includes original signer and self-proxy signer's identity and moreover, their public keys are used in the signature verification $(s_4 z \sim s_5 y_1, s_1 \sim y_1)$. so, it is easy to identify the original and the proxy signer.

Strong undeniability: $H = H_1\left[H_2(\alpha) \square m_w\right]$ is used in the verification that indirectly involves $\alpha = \beta_1 h \beta_1^{-1}$ *and* $h = H_1\left[H_2(\alpha) \square m_w\right]$ So, Alice cannot deny having being signed the message due to the contents from the warrant θ_1.

Strong unforgeability: Alice used her secret key b_1 and random number β_1 to create the self- proxy key as $b_1\beta_1$ and proxy public key as $z = b_1\beta_1 y_1 b^{-1}{}_1\beta_1^{-1}$.Now finding $b_1\beta_1$ from z is a base problem 1. So, no one can derive her secret key from the proxy public key.

5. Conclusion

In this article we proposed proxy signature scheme based on non-commutative semi-rings. Our protocol meets security attributed based conjugacy problem and we analysed the security aspects. Conjugacy search problem and base problem 1 forms the building blocks for the security in terms of verifiability, strong Identifiability, strong undeniability and strong unforgeability.

References

1. D. Chaum, Blind signature systems, Proceedings of Crypto 83, Springer Verlag, pp. 153- 158, 1984.
2. M. Mambo, K. Usuda and E. Okamoto, Proxy signatures for delegating signing operation, in proceedings of the 3rd ACM conference on Computer and Communication Security (CCS), pp 48-57, 1996.
3. S. Kim, S. Park and D. Won, Proxy signatures: Revisited, in Y. Han, T. Okamoto, S. Quing, editors, Proceedings in International Conference on Information and Communications Security (ICICS), of LNCS#1334, pp 223-232, 1993.
4. W. Diffie and M. E. Hellman. New directions in cryptography, IEEE transaction on Information Theory, 22(6),pp. 74-84, 1977.
5. D. Pointcheval and J. Stern, Probably secure blind signature schemes, Proc. Asiacrypt-96, LNCS#1163, pp. 252-265, 1996.
6. A. Boldyreva, Efficient threshold signature, multisignature and blind signature schemes based on the Gap-Diffie Hellman group signature schemes, available at http://eprint.iacr.org/2002/118.

7. I. Anshel, M. Anshel, and D. Goldfeld, An algebraic method for public key cryptography, Math. Research Letter (6), pp. 287-291, 1999.
8. D. Chaum, A. Fiat, M. Naor, Untraceable electronic cash, Proceedings of Crypto 88, LNCS#403, pp. 319-327, Springer Verlag, 1988.
9. G. K. Verma, Blind signature schemes over Braid groups, 2008, available at http://eprint.iacr.org/2008/027.
10. A. Boldyreva, A. Palacio and B. Warinschi, Secure proxy signature schemes for delegation of signing rights, available at http://eprint.iacr.org/2003/096.

Corresponding Author:

R.Vijayaragavan*,

Email: *rvijayaraagavantvu@gmail.com*