An Efficient Proxy Signature Scheme Based On RSA Cryptosystem

Swati Verma and Birendra Kumar Sharma

School of Studies in Mathematics,
Pt. Ravishankar Shukla University, Raipur (C.G.), India
swativerma15@gmail.com, sharmabk07@gmail.com

Abstract

A proxy signature allows a designated person, called a proxy signer, to sign the message on behalf of the original signer. Proxy signatures are very useful tools when one needs to delegate his/her signing capability to other party. A number of proxy signature schemes have been proposed and succeeded for proxy delegations, but the schemes are in defective in proxy revocations. In this paper, we propose proxy signature scheme based on RSA cryptosystem.

Our scheme does not consider proxy revocation mechanism, but it is efficient than the existing RSA-based schemes.

Keywords: *Cryptography, Digital Signature, Proxy Signature, RSA, Security*

1. Introduction

The notion of proxy signature was first introduced by Mambo, *et al.*, in 1996 [7, 8]. A proxy signature scheme is an important investigation in the field of digital signature which involves three entities: an original signer, a proxy signer and a verifier. It provides tools to the original signer to delegate his signing right to a particular signer, known as proxy signer. Once the proxy signer signed the message on behalf of the original signer, the verifier, who knows the public keys of the original and proxy signers, verifies the validity of the proxy signature after receiving it. Mambo, *et al.*, [7, 8] classified the proxy signature on the basis of delegation, namely, full delegation, partial delegation and delegation by warrant. In full delegation, an original signer directly gives his secret key to a proxy signer and the proxy signer sign documents on behalf of the original signer with it. The main drawback of full delegation is the absence of distinguishability between the original signer and the proxy signer. In partial delegation, an original signer derives a proxy key from his secret key and hands it over to a proxy signer. In this case, the proxy signer can misuse the original signer's delegated rights because partial delegation does not restrict the proxy signer's signing capability. The weaknesses of full delegation and partial delegation are eliminated by adding an explicit warrant to the delegated rights, which is called partial delegation with warrant. A warrant consists of signer's identity, delegation period and the qualification of the message on which the proxy signer can sign. The revocation of delegated rights (*i.e.*, proxy revocation) is an important issue of proxy signatures scheme. The proxy revocation is essential for the situation where signer's key is compromised and any misuse of the delegated rights is noticed. It may also happen that the original signer wants to terminate the delegated rights before the expiry of the delegated rights.

In the literature, in 1997, Kim, *et al.*, [1] proposed a scheme by restricting proxy signer signing right using the concept of partial delegation with warrant. In 1999, Okamoto, *et al.*, [9], for the first time, proposed proxy signature based on RSA scheme, but they considered the proxy unprotected notion. In 2001, Lee, *et al.*, [2, 3] proposed a proxy-protected signature scheme based on the RSA assumption. In 2002, Shum and Wei [13] proposed another proxy

signature scheme which was proxy protected. The first proxy signature scheme based on the factoring integer problem was proposed by Shao [11] in 2003. In 2005, Zhou, *et al.*, [17] proposed two efficient proxy-protected signature schemes. Their first scheme is based on RSA assumption and the second scheme was based on the integer factorization problem. Zhou, *et al.*, [17] claimed that their schemes are more efficient than other schemes. However, Park, *et al.*, [10] pointed out the shortcoming of their schemes. In 2006, Xue, *et al.*, [14] proposed the normal proxy signature scheme and multi-proxy signature scheme based on the difficulty of factoring of large integers but without giving their formal security proofs. In 2009, Shao [12] proposed proxy-protected signature scheme based on RSA. Recently, in 2012, Yong, *et al.*, [16] proposed provably secure proxy signature scheme from factorization. Many variants of RSA-based proxy signature scheme were proposed in the sequel [4, 5, 6].

Most of the proxy signature schemes are based on discrete logarithm problems [1, 15]. A few proxy signature schemes are also constructed based on factoring problem [11, 12, 14, 17].

The algorithm for a proxy signature is as follows:

Organization: The remaining parts of this paper an organized as follows. In Section 2, we elaborate security properties of the proxy signature scheme. Next, we proposed our proxy signature scheme in Section 3. In Section 4, we analyze the security properties and performance analysis of our proposed scheme in Section 5. Finally, in Section 6, we give our concluding remarks.

2. Security Requirements of Proxy Signature Scheme

The security requirements for any proxy signature are first studied in [7, 8] and later those were improved in [2, 3]. According to them, a secure proxy signature scheme is expected to satisfy the following five requirements:

1. Verifiability: The verifier is convinced that the original signer has given consent to the proxy signer to sign a message.
2. Strong unforgeability: Nobody else other than the designated proxy signer can create a valid proxy signature on behalf of the original signer.
3. Strong identifiability: Anyone can determine the identity of the proxy signer of the corresponding proxy signature.
4. Strong undeniability: Once a proxy signer creates a valid proxy signature on behalf of an original signer, he cannot repudiate the signature creation against anyone else.
5. Prevention of misuse: The proxy signer cannot use the proxy key for the purposes other than generating a valid proxy signature. In case of misuse, the responsibility of the proxy signer should be determined explicitly.

3. Proposed Proxy Signature Scheme

The proposed scheme is divided into five phases: Initialization, Proxy key generation, Proxy key verification, Proxy signature generation and Proxy signature verification.

3.1 Initialization

For the convenience of describing our work, we define the parameters as follows:

* O: the original signer
* P: the proxy signer

* p,q : two large prime number
* $(e_o; d_o)$: secret key of original signer
* $(e_o; n_o)$: public key of original signer
* $(e_p; d_p)$: secret key of proxy signer
* $(e_p; n_p)$: public key of proxy signer
* n_o and n_p : is the product of two large safe primes
* h () : a secure one-way hash function
* m_w: a warrant.
* h $(m_{1||} m_2)$: the hash of concatenation of two messages m_1 and m_2.

3.2 Proxy Key Generation

The original signer O does the following:

1. Computes $s_o = h(m_w \| e_p)^{d_o} \bmod n_o$
2. Sends (s_o, m_w) to the proxy signer over a public channel.

3.3 Proxy Key Verification

The proxy signer P checks whether $h(m_w \| e_p)^{d_o} = s_o^{e_o} \bmod n_o$. If it holds, the proxy signer accepts it as a valid proxy key; otherwise, rejects it.

3.4 Proxy Signature Generation

To sign message m on behalf of the original signer O, the proxy signer does the following:

1. Computes $s_p = s_o \oplus h(m \| m_w \| e_p)^{d_p} \bmod n_p$ where $\oplus$ is an exclusive OR operation.
2. The proxy signature of message m is (m, m_w, s_p, e_o, e_p).

3.5 Proxy Signature Verification

The verifier verifies whether $h(m_w \| e_p) = (s_p^{e_p} \bmod n_p \oplus h(m \| m_w \| e_p))^{e_o} \bmod n_o$. If it holds, he accepts it as a valid proxy signature; otherwise, rejects it.

4. Security Analysis

In the following, we show that the proposed schemes satisfy the security features, namely, verifiability, strong unforgeability, strong undeniability, strong identifiability and prevention of misuse.

4.1 Verifiability

The verifier of proxy signature, can check whether verification equation

$$h(m_w \| e_p) = (s_p^{e_p} \bmod n_p \oplus h(m \| m_w \| e_p))^{e_o} \bmod n_o$$

holds or not. We prove this as follows.

$$(s_p^{\,e_p} \bmod n_p \oplus h(m\|m_w\|e_p))^{e_o} \bmod n_o = \{(s_o \oplus h(m\|m_w\|e_p)) \bmod n_p \oplus h(m\|m_w\|e_p)\}^{e_o} \bmod n_o$$

$$= \{h(m_w\|e_p)^{d_o} (\bmod n_o)(\bmod n_p) \oplus h(m\|m_w\|e_p) \oplus$$

$$h(m\|m_w\|e_p)\}^{e_o} (\bmod n_o)$$

$$= \{h(m_w\|e_p) \oplus h(m\|m_w\|e_p^{\,e_o})(\bmod n_p) \oplus h(m\|m_w\|e_p)^{e_o} (\bmod n_o)\}$$

$$= h(m_w\|e_p).$$

4.2 Strong Unforgeability

In this scheme, the proxy signature is created with the proxy signer's secret key d_p and delegated proxy key s_o. The proxy key is binding with the original signer's secret key d_o. No one (including the original signer) can construct the proxy signature without having the knowledge of the secret keys d_p and d_o. Obtaining these secret keys by any other party is as difficult as breaking RSA. Moreover, the verification of $h(m_w\|e_p)$ with the signed message prevents the dishonest party from the creation of forged proxy signatures. Therefore, any party including the original signer cannot forge a valid proxy signature and thus the proposed scheme satisfies the unforgeability property.

4.3 Strong Identifiability

The verification process of the proposed scheme requires proxy signer's public key e_p and warrant m_w. Any verifier can determine the identity of the proxy signer from the signed message, because the signed message is computed as $s_p = s_o \oplus h(m\|m_w\|e_p)^{d_p} \bmod n_p$, where so is a signed warrant by the original signer. Therefore, in the verification process any verifier can determine the identity of the proxy signer from m_w.

4.4 Strong Undeniability:

From a proxy signature of the proposed scheme, the involvements of both original signer and proxy signer are determined by the warrant m_w and the connection of the public keys e_p and e_o in the verification process. Thus the proxy signer and the original signer cannot deny their involvement in a valid proxy signature. So the scheme satisfy the undeniability property.

4.5 Prevention of Misuse

Both the proxy signer and the original signer's misuse are prevented in our scheme. The proxy signer cannot forge the delegated rights. In case of the proxy signer's misuse, the responsibility of the proxy signer is determined from the warrant m_w. The original signer's misuse is also prevented because he cannot compute a valid proxy signature against the proxy signer, which is the unforgeability property of our scheme.

5. Performance Analysis

In order to analyze the performance of our scheme, we compare the computational complexity of our scheme with the existing RSA-based proxy signature schemes Lee, *et al.*, [2] and Shao [11].

Table 1. Comparison of Computational Time with Previous Schemes

Phases	LKK Scheme (2001)	Shao's Scheme (2003)	Our Scheme
Setup parameter	2Te + 2Tm + 2To	Te + Tm + To	2Te + 2Tm + 2To
Proxy Key Generation	Te + To + H	Te + To + H	Te + To + H
Proxy Key Verification	Te + To + H	Te + Tm + To + H	Te + To + H
Signature Generation	3Te + 3To + 2H	2Te + 2Tm + 2To + H	Te + To + H
Signature Verification	3Te + 3To + 2H	2Te + Tm + To + 2H	2Te + 2To + 2H

It is noted that the existing schemes and our scheme do not provide the proxy revocation mechanism, but, in this comparison, we show that our scheme is efficient than the existing schemes. For simplicity, we neglect exclusive-OR operation (⊕) time of the scheme.

The notations used in the Table 1 are as follows:

Te: computation time for an exponentiation operation;

Tm: computation time for a multiplication operation;

To: computation time for a modular operation;

H: computation time for a hash operation.

The computation time of different phases of the schemes is given in Table 1. It is important to note that the computation time for a valid proxy signature falls into two parts. The first part consists of the time taken for the setup parameters, proxy key generation and proxy key verification process, which are a one-time computation and remain fixed for the entire delegation period. It is observed from Table 1 that for a proxy signature without revocation our scheme saves at least **Te** or **To** time unit in comparisons to others.

6. Conclusion

In this paper, we have proposed proxy signature scheme based on RSA cryptosystem. Our scheme does not consider proxy revocation mechanism, but it is efficient than the existing RSA-based schemes, *i.e.*, Lee, *et al.*, [2] and Shao's [11] scheme. The proposed scheme satisfies the necessary security requirements of proxy signature and do not require any secure channel to deliver the proxy key, whereas, a secure channel is must for the existing scheme.

Acknowledgements

The author wishes to thank the anonymous referees for their very useful comments and suggestions.

References

[1] S. Kim, S. Park and D. Won, "Proxy signatures", In: ICICS97, LNCS 1334, Springer-Verlag, **(1997)**, pp. 223-232.
[2] B. Lee, H. Kim and K. Kim, "Secure mobile agent using strong non-designated proxy signature", In: Information security and private (ACISP01), LNCS 2119, Springer-Verlag, **(2001)**, pp. 474-486.
[3] B. Lee, H. Kim and K. Kim, "Strong proxy signature and its applications", In: Proceeding of the 2001 symposium on cryptography and information security (SCIS01), vol. 2, no. 2, **(2001)**, pp. 603-608.

[4] Y. Liu, H. Wen and C. Lin, "Proxy-protected signature secure against the un-delegated proxy signature attack", Comput Electron Eng., vol. 33, no. 3, **(2007)**, pp. 177-185.
[5] R. Lu and Z. Cao, "Designated veri_er proxy signature scheme with message recovery", Appl Math Comput., vol. 169, no. 2, **(2005)**, pp. 1237-1246.
[6] R. Lu, X. Dong and Z. Cao, "Designing e_cient proxy signature schemes for mobile communication", In: Science in China, vol. 51, no. 2, **(2008)**, pp. 183-195.
[7] M. Mambo, K. Usuda and E. Okamoto, "Proxy signatures for delegating sign operation", In: Proceeding of the 3rd ACM conference on computer and communications security (CCS96), ACM press, **(1996)**, pp. 48-57.
[8] M. Mambo, K. Usuda and E. Okamoto, "Proxy signatures: delegation of the power to sign messages", IEICE Trans Fundam, vol. E79-A, no. 9, **(1996)**, pp. 1338-1354.
[9] T. Okamoto, M. Tada and E. Okamoto, "Extended proxy signaures for smart card", In: Proceedings of Information Security Workshop 99, LNCS 1729, Springer-Verlag, **(1999)**, pp. 247-258.
[10] J. H. Park, B. G. Kang and J. W. Han, "Cryptanalysis of Zhou, *et al.*, proxy-protected signature schemes", Appl. Math Comput., vol. 169, no. 1, **(2005)**, pp. 192-197.
[11] Z. Shao, "Proxy signature schemes based on factoring", Inform Process Lett., no. 85, **(2003)**, pp. 137-143.
[12] Z. Shao, "Provably secure proxy-protected signature schemes based on RSA", Comput. Electr. Eng., vol. 35, **(2009)**, pp. 497-505.
[13] K. Shum and V. K. Wei, "A strong proxy signature scheme with proxy signer privacy protection", In: Proceedings of IEEE International Workshop on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE02), **(2002)**.
[14] Q. Xue and Z. Cao, "Factoring based proxy signature schemes", Journal of Comput Appl Math, vol. 195, **(2006)**, pp. 229-241.
[15] L. Yi, G. Bai and G. Xiao, "A new type of proxy signature scheme", Electron. Lett., vol. 36, no. 6, **(2000)**, pp. 527-528.
[16] Y. Yong, M. Yi, W. Susilo, Y. Sun and Y. Ji, "Provably secure proxy signature scheme from factorization", Mathematical and Computer Modelling, vol. 55, **(2012)**, pp. 1160-1168.
[17] Y. Zhou, Z. Cao and R. Lu, "Provably secure proxy-protected signature schemes based on factoring", Appl Math Comput., vol. 164, no. 1, **(2005)**, pp. 83-98.

Authors

Swati Verma received the B.Sc. and M.Sc. degree in Mathematics from Pt. Ravishankar Shukla University, Raipur. Chhattisgarh, India in 2005 and 2007. She joined School of Studies in Mathematics, Pt. Ravishankar Shukla University, Raipur, India for her research work. She is a life member of Cryptology Research Society of India (CRSI). Her area of interest is Public Key Cryptography and Digital Signature.

Birendra Kumar Sharma Professor, School of Studies in Mathematics, Pt. Ravishankar Shukla University Raipur (C. G.) India. He has been working for long time in the field of Non Linear Operator Theory and currently in Cryptography. He and his research scholars work on many branches of public key cryptography. He is a life member of Indian Mathematical Society and the Ramanujan Mathematical Society.