International Journal of Information & Network Security (IJINS)
Vol.1, No.2, June 2012, pp. 60~66
ISSN: 2089-3299

A New Proxy Blind Signature Scheme Based on DLP

Swati Verma*, Birendra Kumar Sharma**
*School of Studies in Mathematics, Pt.Ravishankar Shukla University Raipur(C.G.), India.
** School of Studies in Mathematics, Pt.Ravishankar Shukla University Raipur(C.G.), India.

Article Info

Article history:

Received May 10th, 2012
Revised May 30th, 2012
Accepted June 4th, 2012

Keyword:

Blind Signature
Cryptography
Discrete Logarithm Problem
Proxy Signature
Proxy Blind Signature

ABSTRACT

A proxy blind signature scheme is a special form of blind signature which allows a designated person called proxy signer to sign on behalf of two or more original signers without knowing the content of the message or document. It combines the advantages of proxy signature and blind signature and satisfies the security properties of both proxy and blind signature scheme. In this paper, a new proxy blind signature scheme based on discrete logarithm problem (DLP) has been proposed, which satisfies the security properties of both the blind signature and proxy signature. Security analysis also given which shows that our scheme is secure and efficient.

Corresponding Author:

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

1. INTRODUCTION

Proxy signature is a special form of digital signature. In 1996, Mambo et al. [10, 11]. Firstly introduced the concept of the proxy signature, which allows an original signer delegates his signing capacity to a proxy signer who can sign a message submitted on behalf of the original signer. A verifier can validate its correctness and can distinguish between a normal signature and a proxy signature. Many proxy signature schemes have been proposed [6, 7, 13, 16, 17].

In 1983, David Chaum [2] proposed the concept of bind signature, which allows the sender to have a given message signed by the signers without revealing any information about the message or its signature. The most distinguishing properties of a blind signature scheme are: untraceability and unlinkability, which may ensure that requesters can prevent the signer from deriving the exact correspondence between the actual signing process performed by the signer and the signature opened later. Therefore, the blind signature largely protects the privacy of participants and can be applied in secure electronic payment systems [4] and secure voting systems [15]. Blind signature also has received significant attention and lot of research work has been done in this field [1, 3, 5].

A proxy blind signature scheme is a digital signature scheme that ensures the properties of both proxy signature and blind signature. In a proxy blind signature, an original signer delegates his signing capacity to proxy signer. The proxy signature plays an important role in many applications too. On the combination of the proxy signature and blind signature.

In 2000, The first proxy blind signature was proposed by Lin and Jan [9]. Later, Tan et al. [14] proposed a proxy blind signature scheme. In 2003, Lal et al. [8] pointed out that Tan et al.s scheme was insecure and proposed a new proxy blind signature scheme based on Mambo et al.s scheme [10]. In 2002, Tan et al. [14] presented a proxy blind signature based on Schnorr blind signature scheme [3]. Later, Lal and Awasthi [8] pointed out that Tan et al.'s proxy blind signature schemes suffer from a kind of forgery attack

due to the signature receiver. Compared with Tan et al.'s schemes, Lal and Awasthi further proposed a more efficient and secure proxy blind signature scheme. Tan et al.s schemes do not satisfy the unforgeability and unlinkability properties. In this paper, we propose a new proxy blind signature scheme based on discrete logarithm problem (DLP), which satisfied all the security requirements of both the blind signature scheme and the proxy signature scheme. The analysis of security shows that our scheme is more efficient and low computation.

The rest of this paper is organized as follows. In Section 2, we briey list some security properties of the scheme. And then, our proposed proxy blind signature scheme is presented in Section 3. In Section 4, we analyze the efficiency and the security properties of the proposed scheme in section 5. Finally Section 6, describes the concluding remarks.

2. CHARACTERISTICS OF PROXY BLIND SIGNATURE SCHEME

The proxy blind signature should satisfy the following properties:

1. **Distinguishability:** The proxy signature must be distinguishable from the original signature.
2. **Unforgeability:** Only the designated proxy signer can generate a valid proxy signature.
3. **Non-repudiation**: The original and proxy signer cant deny their signatures against any one.
4. **Verifiability**: The receiver should be able to verify the proxy signature.
5. **Identifiability**: Anyone can determine the identity of the corresponding proxy signer and original signer from the signature.
6. **Unlinkability**: When the signature is revealed the proxy signer cannot identify the association between the message and the blind signature he generated.
7. **Prevention of misuse**: The proxy key pair should be used only for creating proxy signature.

3. THE NEW PROXY BLIND SIGNATURE SCHEME

In this section, we propose an efficient proxy blind signature scheme based on DLP. The proposed scheme is divided into four phases: Notations, Proxy delegation phase, Blind signing phase, and Signature verification phase.

3.1. Notations

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

* O: the original signer
* P: the proxy signer
* A: the Signature Verifier
* p,q: two large prime number with $q/(p-1)$
* g: an element of order q in Z_q^*
* h () : a secure one-way hash function
* x_o : the secret key of original signer
* y_o : the public key of original signer, , $y_o = g^{x_o} \bmod p$
* x_p : the secret key of proxy signer,
* y_p : the public key of proxy signer, $y_p = g^{x_p} \bmod p$
* O sends message to P
* ‖: denotes the concatenation of strings.

3.2. Proxy Delegation Phase

The original signer O randomly select $v_o \in Z_q^*$ on the condition and computes:

$$r_o = g^{v_o} \bmod p \quad (1)$$

$$s_o = x_0 + v_o \bmod q \quad (2)$$

Original signer O sends (r_o, s_o) to the proxy signer P in a secure manner..

P accept (r_o, s_o) if the equation

$$g^{s_o} = (r_o y_o) \bmod q \quad (3)$$

does hold. The proxy signer P computes the proxy private key

$$s_p = s_o + x_p \bmod q \quad (4)$$

3.3. Blind Signing Phase

The proxy signer P selects random number $k \in Z_q^*$ and computes:

$$t = g^k \bmod p \quad (5)$$

and sends $(t; r_o)$ to the signature verifier A.
To obtain the blind signature of message m, original signer O randomly choose two random numbers $\alpha, \beta \in Z_q^*$ and computes:

$$r = tg^{\alpha}(y_o y_p) \bmod p \quad (6)$$

$$e = h(r \| m) \bmod q \quad (7)$$

$$e' = e - \beta \bmod q \quad (8)$$

A sends e_0 to proxy signer P, after receiving e', Proxy signer P computes:

$$s' = e's_p + k \bmod q \quad (9)$$

and sends the sign message s' to A, after receiving s', A computes:

$$s = g^{s'+\alpha} r_o^{-\beta} \bmod q \quad (10)$$

The proxy blind signature of message m is $(m; s; e; r_o)$

3.4 Signature Verification Phase

The verifier can verify the proxy blind signature by checking whether

$$e = h(sy_{pr}^{-e} \bmod p \| m) \bmod q \quad (11)$$

holds. Where $y_{pr} = (y_o y_p)$ or $g^{sp} \bmod p$.

If it is true, the verifier accepts it as a valid proxy blind signature, otherwise rejects.

Theorem 3.1 Suppose all the entities involved in the protocol follow the protocol, then equation(12) holds.

Proof : As per equation (7) and (11) follows from the equation:

$$r = s\, y_{pr}^{-e} \bmod p \tag{12}$$

By computing using the equation (1) to (11), we have

$$\begin{aligned} sy_{pr}^{-e} &= g^{s'+\alpha} r_o^{-\beta} r_o^{-\beta} y_p^{-e} \bmod p \\ &= g^{e's_p + k + \alpha} r_o^{-\beta} y_p^{-e} \bmod p \\ &= g^{k+\alpha+(e-\beta)s_p} r_o^{-\beta} y_p^{-e} \bmod p \\ &= tg^{\alpha} g^{es_p} g^{-\beta s_p} r_o^{-\beta} y_p^{-e} \bmod p \\ &= tg^{\alpha} g^{es_p} g^{-\beta(s_o + x_p)} r_o^{-\beta} y_p^{-e} \bmod p \\ &= tg^{\alpha} g^{es_p} g^{-\beta(x_o - v_o + x_p)} r_o^{-\beta} y_p^{-e} \bmod p \\ &= tg^{\alpha} g^{es_p} (y_o y_p)^{-\beta} r_o^{\beta} r_o^{-\beta} y_p^{-e} \bmod p \\ &= tg^{\alpha} (y_o y_p)^{-\beta} \bmod p \\ &= r. \end{aligned}$$

The message flows of the proxy blind signature scheme is described in following Figure 1.

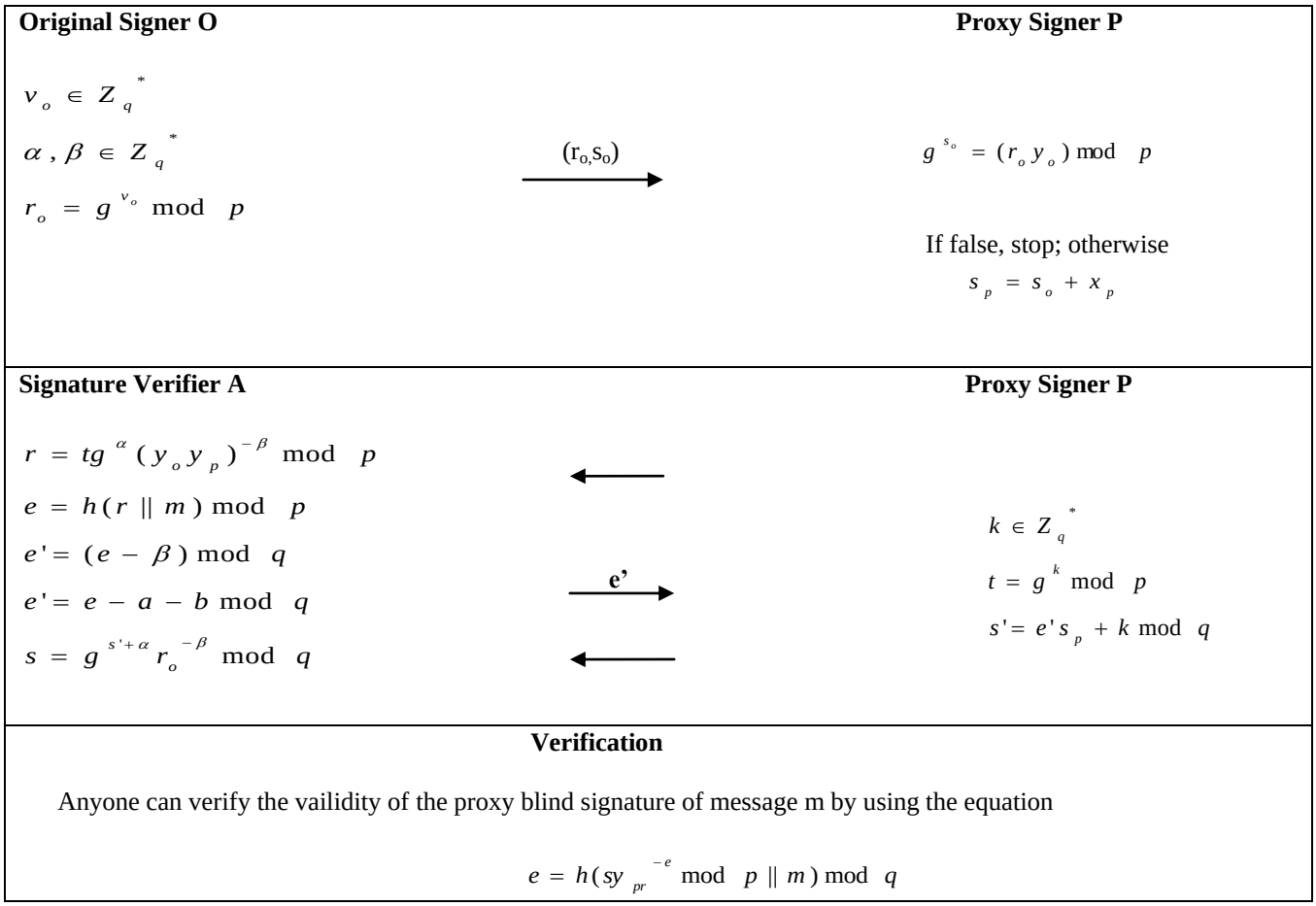

Figure 1. The message flows of the proxy blind signature scheme.

4. EFFICIENCY OF PROPOSED SCHEME

In this section, we can show that our scheme is more efficient and low computation cost than previous scheme [8, 14]. Let E, M and I respectively denote the computational load for exponentiation, multiplication and inversion. Then following table shows the comparison of computational cost with previous schemes.

Table 1: Comparison of computational cost with previous schemes [8, 14].

Schemes	Delegation Phase	BlindSigning Phase	Verification	Total Costs
Tan et.al.	3E+2M	8E+7M+4I	3E+3M+I	14E+12M+5I
Lal and Awasthi	4E+2M	3E+3M+2I	2E+M	9E+6M+2I
Our Scheme	3E+1M	3E+4M+2I	2E+2M+1I	8E+7M+3I

5. SECURITY ANALYSIS OF THE PROPOSED SCHEME

In this section we discuss the some of the properties of our proposed proxy blind signature scheme, described in section 2.

5.1 Unforgeability :

In the signing agreement, P wants to compute x_o, through (r_o; s_o) , which is the process of computing a discrete logarithm. We can confirm that the common signature of original signer O can not be forged by proxy signer P. Because the information owned by other attackers is less than P's, original signer O others can not forge the common signature of, either.

5.2 Distinguished :

Proxy signature is distinguishable from original signer's to normal signature. Since proxy key is different from original signer's private key and proxy keys created by different proxy signers are different from each other, any proxy signature is distinguishable from original signer's signature and different proxy signer's signature. We can distinguish the proxy signature with normal signature due to the extra part which is included in the proxy signature but not normal signature.

5.3. Unlinkability:

Message m is blinded before it is signed by proxy signer P. Because blinded element is known only by message owner, if only it is chosen randomly, message m extracted from message M is the factorization of large number. In addition, in the process of extraction, blinded element will be used, so the proxy signer cannot associate his precious signing transcripts with any message received in the process of signing. In verification stage, the signer checks only whether

$$r = tg^{\alpha}(y_o y_p)^{-\beta} \bmod p$$

He does not know the original signer's private key and proxy signer's private key. Thus the signer knows neither the message nor the signature associated with the signature scheme.

5.4. Undeniability:

Because no matter who cannot forge the common signature of O and proxy signature of P, O can not repudiate its valid strong delegation signature and P can not repudiate its valid proxy signature.

5.5. Identifiability :

In the verification equation $y_{pr} = y_o\ y_p$ which includes the original signer O's public key y_o and the proxy signer P's public key y_p. Hence, anyone can determine the identity of the corresponding proxy signer from a proxy signature.

5.6. Non-repudiation :

The original signer does not obtain the proxy signer's secret key x_p and proxy signer doesnot obtain original signer's secret key x_o. Thus, neither the original signer nor the proxy signer can sign in place of the other party. At the same time, through the valid proxy blind signature, the verifier can confirm that the

signature of the message has been entitled by the original signer, because the verifier must use the original signer's public key during the verification. Likewise, the proxy signer cannot repudiate the signature. The scheme offers non- repudiation property.

5.7. Prevention of misuse:

The proposed proxy signature can avoid any misuse of the proxy private key, which includes the information about the type of message can be signed by the proxy signer. Hence, the responsibility of proxy signers is determined explicitly. Therefore, the proxy signer cannot sign any message that has not been authorized by the original signer and this prevents abuse of the proxy key.

CONCLUSION

In this paper, we proposed a new proxy blind signature scheme based on discrete logarithm problem (DLP). The proposed scheme satisfies the given security requirements and has minimum computational cost when comparing with previous schemes. The future work is to design more effective proxy blind signature schemes which provably secure with lower computational cost.

ACKNOWLEDGEMENTS

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

REFERENCES

[1] Abe M., Fujisaki E., "How to date blind signatures", *in: Advances in Cryptology AisaCrypt96 LNCS 1163, Springer-Verlag*, pp. 244-251, (1996).
[2] Chaum D., "Blind signatures for untraceable payments", *Advances in Cryptology Crypto82*, pp. 199-203, (1983).
[3] Chaum D, *et al*, "Untraceable electronic cash", in: *Proceedings of Crypto88, LNCS 403, Springer-Verlag*, pp. 319-327, (1988).
[4] Dai J.Z., *et al*, "Designated-Receiver Proxy Signature Scheme for Electronic Commerce"; In: *Proc. of IEEE International Conference on Systems, Man and Cybernetics*, Vol. 1, pp. 384-389, Oct 5-8, (2003).
[5] Fan C.I., *et al*, "Randomization enhanced Chaums blind signature scheme", *Computer Communication*, vol. 23, pp. 1677-1680, (2000).
[6] Hwang S.J., and Shi C.H., "A simple multi-proxy signature scheme", in: *Proceedings of the Tenth National Conference on Information Security, Taiwan*, pp. 134-138, (2000).
[7] Kim S., *et al* , "Proxy Signatures". revisited. In: *ICICS97. LNCS 1334. Springer-Verlag*, 223-232, (1997).
[8] Lal S., and Awasthi A.K., "Proxy Blind Signature Scheme"; *to appear in Journal of Information Science and Engineering.* 2003, Cryptology ePrint Archive, Report2003/072.Available at: http://eprint.iacr.org/.
[9] Lin W.D., and J.K. Jan, "A security personal learning tools using a proxy blind signature scheme", *Proc. of Intl Conference on Chinese Language Computing*, pp.273-277, (2000).
[10] Mambo M, *et al*, "Proxy signatures for delegating sign operation". In: *Proceeding of the 3rd ACM conference on computer and communications security (CCS96), ACM press*, 48-57, (1996).
[11] Mambo M, *et al*, "Proxy signatures: delegation of the power to sign messages". *IEICE Trans Fundam, E79* A(9):1338-1354, (1996).
[12] Shao Z., "Provably secure proxy-protected signature schemes based on RSA". *Comput. Electr. Eng.*, 35, 497-505, (2009).
[13] Shao Z., "Proxy signature schemes based on factoring". *Inform Process Lett* (85), 137-143, (2003).
[14] Tan Z., *et al* ., "Digital proxy blind signature schemes based on DLP and ECDLP*", MM Research Preprints, No. 21, MMRC, AMSS, Academia, Sinica, Beijing* pp 212-217, (2002).
[15] Wang S., *et al* , "A Proxy Blind Signature Schemes Based DLP and Applying in e-Voting", *Proceedings of the 7th international conference on Electronic commerce, Xi'an, China, SESSION: Innovative technologies of e-commerce*, Vol. 113, pp. 641-645, (2005).
[16] Yi L., *et al*, "Proxy multi-signature scheme", *Electronics Letters*, vol. 36, pp. 527-528, (2000).
[17] Zhou Y, *et al*, "Provably secure proxy-protected signature schemes based on factoring". *Appl Math Comput*, 164(1), 83-98, (2005).

BIBLIOGRAPHY OF AUTHORS

Swati Verma received the B.Sc. and M.Sc. degree in Mathematics form 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.