An Improved Proxy Blind Signature Scheme With Forward Security

Manoj Kumar Chande
Shri Shankaracharya Institute of Professional Management & Technology
Raipur, 492015, Chhattisgarh, India

Balwant Singh Thakur
School of Studies in Mathematics, Pt. Ravishankar Shukla University
Raipur, 492010, Chhattisgarh, India

ABSTRACT

This paper presents a proxy blind signature scheme with forward security mechanism. The proposed digital signature scheme combines the two special-purpose signature schemes, blind signature and proxy signature. In this signature scheme, the original signer gives authority to another entity which is known as a proxy signer, but without having any idea about the content of the document. This paper, proposes an enhanced proxy blind signature, in which the forward security is incorporated and the security of the signature scheme relies on the discrete logarithm problem (DLP). Forward security mechanism will provide protection to the system from the key leakage or key exposure, because in this mechanism, the private key of proxy signer is updated periodically. In case if the signature key at some stage is compromised, the adversary cannot be able to forge signatures as if they had been generated before the exposure or leakage of key.

General Terms:

Public key cryptography, Digital signature

Keywords:

Discrete Logarithm Problem, Forward Security, Proxy Blind Signature

1. INTRODUCTION AND PRELIMINARIES

In the year 1983, David Chaum [1], introduced the concept of blind signature scheme and in the year 1996, the proxy signature scheme was introduced by Mambo, Usuda and Okamoto [2]. A proxy blind signature scheme is a digital signature scheme that combines the properties of proxy signature and blind signature schemes. Combining these two concepts of signature schemes a new variant of digital signature scheme, proxy blind signature scheme comes into existence.

In a proxy blind signature scheme, the proxy signer is allowed to generate a blind signature on behalf of the original signer. The proxy blind signature must satisfy the security properties of proxy signature and blind signature, and security properties for a good proxy blind signature schemes are as follows [3].

(a) **Distinguishability:** The proxy blind signature must be distinguishable from the normal signature.

(b) **Nonrepudiation:** Neither the origin nor the proxy can be able to sign in place of the other entity. In other words, they cannot deny their signatures against anyone.

(c) **Verifiability:** The receiver of the signature should be able to verify the proxy signature in a similar way to the verification of the original signature.

(d) **Unforgeability:** Only a designated proxy signer can create a valid proxy signature for the original signer (even the original signer cannot do it).

(e) **Unlinkability:** When the signature is verified, the signee knows neither the message nor the signature associated with the signature scheme.

Forward Security Mechanism

The concept of forward security means to update of signer's private key periodically. Initially at the time of system setup users will got public key $(Say\ P_k)$ and keep the initial signature key $(Say\ Sk_0)$ a secret. The total effective time of public key is distributed equally into $\{1, 2, ..., \mathrm{T}\}$ periods. During the effective signature time, the public key remains unchanged, while signature key will be updated with the different periods to provide the forward security. Sk_i means the signature key of i^{th} period obtain as $Sk_i = f(Sk_{i-1})$ where f is a one-way hash function, then Sk_{i-1} will be deleted immediately. When the attacker gets Sk_i during i^{th} period he cannot get, $Sk_{i-1}, Sk_{i-2}, ..., Sk_0$ for they all have been deleted, and Sk_i is calculated using the one-way function.

The process of signature key updating in the proposed signature scheme is as follows: The proxy signer's private key x_B is in the process of upgradation with initial private key value x_{B_0}. The upgradation of proxy private key is done in a particular time period i. Initially x_{B_i} is an empty string, but for the i^{th} period the proxy signer calculates its private key x_{B_i}, by the private key of

the $(i-1)^{th}$ period by

$$x_{B_i} = x_{B_{i-1}}^2 \, mod \, q$$

and he deletes $x_{B_{i-1}}$ immediately. So initially the public key of the proxy signer is

$$y_B = g^{x_{B_0}} \, mod \, q$$

Discrete logarithm problem

Two numbers y and g, are given then to find an integer $x \in Z_p^*$, such that $y = g^x \, mod \, q$. To find x is known as a discrete logarithm problem (DLP).

2. RELATED WORK

The first proxy blind signature scheme was introduced by Lin and Jan [4], in the year 2000. In 2002, Tan et al. [3], presented two proxy blind signature schemes by applying schnorr blind signature, the security of the schemes were based on discrete logarithm problem (DLP) and elliptic curve discrete logarithm problem (ECDLP) respectively. This signature scheme attracts focus of many researchers. In 2003, Lal et al. [5], pointed out that Tan et al. [3], scheme was insecure and proposed a new proxy blind signature scheme based on Mambo et al. [2] scheme. Wang et al. [6], in the year 2004, demonstrated that Tan's scheme was insecure and proposed two effective attacks. In 2004, Xue and Cao [7], showed that there exists one weakness in Tan's scheme [3], and Lal et al. scheme [5], since the proxy signer can get the link between the blind message and the signature or plaintext with great probability. Xue and Cao [7], introduced the concept of strong unlinkability and they also proposed a proxy blind signature scheme, in comparison with Tan's and Lal's scheme; their scheme is more efficient. However, Li, Zhang and Yang et al. [8], showed that the scheme of Xue and Cao [7], can't satisfy unforgeability and strong unlinkability properties. In 2005, Sun et al. [9], showed that Tan's schemes didn't satisfy the unforgeability and unlinkability properties, and they also pointed out that Lal's scheme [5], didn't possess the unlinkability property. But Wu, Yeh and Liu [10], shows that Sun's [9], attack failed and the schemes of Tan's and Lal's still satisfy the unlinkability property. In the same year 2005, Wang, Fan and Cui [11], analyzed the security shortcoming of Tan [3], and presented a new proxy blind signature based on DLP. They also described application of the proposed scheme as an instance, in electronic voting. Recently, Li and wang et al. [12] proposed a proxy blind signature scheme using verifiable self-certified public key, and they claim that their scheme is more efficient than the schemes published in the open literature.

The scope of proxy blind signature is really very wide in the field of e-commerce, e-voting, e-payment, mobile communication etc. unfortunately there is no forward security [13], in any proxy blind signature schemes [2, 3, 4, 5, 6, 7, 8, 9, 11, 12], so it will impact the system security tremendously that the key is stolen or leaked. In this condition, after the attacker gets the proxy signature key, he/she can forge the proxy signature which cannot be distinguished by people. It has been a matter of great concern how to minimize the key leakage impact on system security. The forward security theory [14, 15, 16], is an effective means to solve that problem.

3. REVIEW OF TAN'S PROXY BLIND SIGNATURE

3.1 System Parameters and Notation

Throughout this paper, the following notations are used to explain and analyze the scheme.

p, q – Large Primes Such That $q|p-1$.
g – An Element of Z_p^* of Order q.
x_A – Secret Key of Original Signer A.
x_B – Secret Key of Proxy Signer B.
y_A – $y_A = g^{x_A} \, mod \, p$, Public Key of Original Signer A.
y_B – $y_B = g^{x_B} \, mod \, p$, Public Key of Proxy Signer B.
$H()$ – A Collision Free Hash Function.
$\|$ – Concatenation of Strings.

3.2 Proxy Phase

(i) **Commission Generation:** The original signer A select randomly $\bar{k} \in Z_q^*$, with the condition that $\exists$ inverse of $\bar{r}\bar{y_A} \, mod \, q$, where $\bar{r} = g^{\bar{k}} \, mod \, p$ and compute

$$\bar{s} = x_A \bar{r} + \bar{k} \, mod \, q \quad (1)$$

(ii) **Proxy Delegation:** The original signer A sends the pair $(\bar{r}, \bar{s})$ to the proxy signer secretly.

(iii) **Proxy Verification:** Proxy signer checks whether

$$g^s = \bar{r} y_A^{\bar{r}} \, mod \, p \quad (2)$$

is true or not, if true then B accepts else reject. Then computes

$$s' = \bar{s} + x_B \, mod \, q \quad (3)$$

as his secret proxy signature key.

3.3 Signature Generation Phase

(i) Proxy signer B randomly select a number $k \in Z_q^*$, and computes

$$t = g^k \, mod \, p \quad (4)$$

and send $(\bar{r}, t)$ to receiver R.

(ii) Receiver R chooses randomly two numbers $a, b \in Z_q^*$ and computes

$$r = t \, g^b y_B^{-a-b} (\bar{r} y_A^{\bar{r}})^{-a} \, mod \, p \quad (5)$$

$$e = H(r \| m) \, mod \, q \quad (6)$$

$$u = (\bar{r} y_A^{\bar{r}})^{-e+b} y_A^{-e} \, mod \, q \quad (7)$$

$$e^* = e - a - b \, mod \, q \quad (8)$$

provided $r \neq 0$, otherwise select new a, b. then send r to proxy signer B.

(iii) As proxy signer received e^*, he computes

$$s'' = e^* s' + k \, mod \, q \quad (9)$$

using the same k as in (4). Then proxy signer B sends s'' to R.

3.4 The Signature Extraction Phase

While receiving s'', receiver R computes

$$s = b + s'' \, mod \, q \quad (10)$$

(m, u, s, e) is the proxy blind signature.

3.5 Signature Verification

The recipient of a proxy blind signature can verify its validity by checking

$$e = H(g^s y_B^{-e} y_A^e u \| m) \bmod q \tag{11}$$

THEOREM 1. *Suppose all the entities involved in the protocol follow the protocol, then equation (11) holds.*

PROOF. In signature generation phase from equation (6) and By equation (11)

$$r = g^s y_B^{-e} y_A^e u \bmod p \tag{12}$$

using equations (1) to (10), gives

RHS = $g^s y_B^{-e} y_A^e u$
$= g^{s"+b} y_B^{-e} y_A^e u$
$= g^{k+b} g^{s'e^*} y_B^{-e} y_A^e u$
$= t g^b g^{\bar{s} e^*} y_B^{e^*-e} y_A^e u$
$= t g^b (\bar{r} y_A^{\bar{r}})^{e-b} (\bar{r} y_A^{\bar{r}})^{-a} y_B^{-a-b} y_A^e u$
$= r$
$= LHS.$

□

4. PROPOSED PROXY BLIND SIGNATURE SCHEME WITH FORWARD SECURITY

4.1 System Parameters and Notation

The system parameters and notations for the proposed signature scheme are same as in Tan's scheme [3]. In this proposed scheme, private and public keys of the receiver are also used, and the notations for them are mentioned below:

x_R – Secret Key of Proxy Signature Receiver.
y_R – $y_R = g^{x_R} \bmod p$, Public Key of Proxy Signature of receiver R.

4.2 The Proxy Delegation Phase

(i) **Proxy Key Generation:**
Original signer O select a random number, $k_o \in Z_p^*$ and compute $r_o = g^{k_o} \bmod p$, then calculate $s_o = x_A + k_o y_B \bmod q$ and send (s_o, r_o) to proxy signer B.

(ii) **Proxy Verification:**
Proxy signer B checks, whether $g^{s_o} = y_A r_o^{y_B} \bmod q$, if it's true, then compute the proxy private key $x_{\mathrm{p}} = s_o + x_{B_0} y_A \bmod q$ and proxy public key $y_{\mathrm{p}} = g^{x_{\mathrm{p}}} \bmod p$.

4.3 Proxy Private Key Updatation

For the i^{th} period to sign the message, the proxy signer B calculates the private key of the i^{th} period

$$x_{B_i} = x_{B_{i-1}}^2 \bmod q \tag{13}$$

using the private key $x_{B_{i-1}}$ of the $(i-1)^{th}$ period, and he deletes $x_{B_{i-1}}$ immediately. After this, he calculates the proxy private and public key respectively as

$$x'_{\mathrm{p}} = s_o + x_{B_i} y_A \bmod q \tag{14}$$

$$y'_{\mathrm{p}} = g^{x'_{\mathrm{p}}} \bmod p \tag{15}$$

4.4 Proxy Blind Signature Generation

(i) Proxy signer select randomly $k_{\mathrm{p}} \in Z_p^*$ and compute $r_{\mathrm{p}} = g^{k_{\mathrm{p}}} \bmod p$ and send r_{p} to the signature receiver.

(ii) Updated proxy public key y'_{p} is available but receiver verify it as

$$y'_{\mathrm{p}} = y_A r^{y_B} y_B^{y_A} \bmod p \tag{16}$$

if it's true, then he moves to next step else stop.

(iii) Signature receiver R select $\alpha, \beta, \gamma \in Z_p^*$ and compute

$$r^* = (r_{\mathrm{p}})^{\alpha} g^{\beta + x_R} (y'_{\mathrm{p}})^{-\gamma} \bmod p \tag{17}$$

$$e^* = h(r^* \| m) \bmod q \tag{18}$$

$$e = \alpha^{-1}(e^* + \gamma) \bmod q \tag{19}$$

send e to proxy signer B.

(iv) Proxy signer B computes

$$s = k_{\mathrm{p}} - e x'_{\mathrm{p}} \bmod q \tag{20}$$

and computes $y'_{\mathrm{p}} = g^{x'_{\mathrm{p}}} \bmod p$ then sends s to the signature receiver R. y'_{p} is used only to verify proxy blind signature by receiver R.

(v) Upon receiving s signature receiver R computes

$$s^* = \alpha s + \beta \bmod q \tag{21}$$

(r^*, s^*, e^*) is the proxy blind signature.

4.5 Signature Verification

THEOREM 2. *Suppose all the entities involved in the protocol follow the protocol. Then the verifier verify the signature with the help of equation*

$$e^* = h(g^{s^*} (y'_{\mathrm{p}})^{e^*} y_R \bmod p \| m) \tag{22}$$

PROOF. It equation (22) holds if $r^* = g^{s^*} (y'_{\mathrm{p}})^{e^*} y_R \bmod p$, so

RHS
$= g^{s^*} (y'_{\mathrm{p}})^{e^*} y_R \bmod p$
$= g^{\alpha s + \beta} (y'_{\mathrm{p}})^{\alpha e - \gamma} g^{x_R} \bmod p$
$= g^{\alpha k_{\mathrm{p}} - e\alpha x'_{\mathrm{p}} + \beta} g^{e\alpha x'_{\mathrm{p}} - \gamma x'_{\mathrm{p}}} g^{x_R} \bmod p$
$= (r_{\mathrm{p}})^{\alpha} g^{\beta + x_R} (y'_{\mathrm{p}})^{-\gamma} \bmod p$
$= r^* \bmod p$
$= LHS.$

□

5. SECURITY ANALYSIS

The proposed proxy blind signature scheme in this paper is based on the signature scheme of Tan [3]. In this improved signature forward security mechanism is incorporated and some improvement regarding computations also has been done in such a way the scheme presented in this paper fulfil all the desired security properties.

(I) **Distinguishability:** The proposed proxy blind signature is composed of (r^*, s^*, e^*) in which there are normal signatures (r^*, s^*) and another e^*. Anyone can distinguish the proxy signature with normal signature due to the additional e^*, which is included in the proxy signature but not a part of normal signature.

(II) **Nonrepudiation:** Secret key's of the original signer A and proxy signer B, are not accessible to each other or anyone except themselves, thus they were not able to sign in place of each other. Only the proxy signer B himself can generate his effective proxy signature, and any other cannot forge his proxy signature, so B cannot deny his proxy signature. In the verification process, through the valid proxy blind signature, the verifier can confirm that the signature on the message is of original signer, because the verifier must use the original signer's public key during the verification. Thus, the proposed scheme holds the non-repudiation property.

(III) **Verifiability:** The proposed proxy blind signature is verifiable, which is shown in the verification phase.

(IV) **Unforgeability:** The private key for i^{th} time period, x_{B_i} of proxy signer B is included in x'_{p}, which is the private key of proxy signer. Only B can generate a proxy signature. Anyone, including A, cannot forge a valid proxy signature.

(V) **Unlinkability:** The adversary cannot forge or attack the scheme because it is not feasible for him to find α, β or γ from the equations (16) to (21). One more difficulty is because of, he/she cannot find a corresponding r_{p} by checking $r^* = (r_{\mathrm{p}})^{\alpha}\, g^{\beta + x_R} (y_{\mathrm{p}})^{-\gamma}\, mod\, p$, without x_R. So, the proxy signer cannot know which (r^*, s^*, e^*) is the related blind information corresponding to the revealed message m.

(VI) **Forward Security:**
If the adversary any how manage to find proxy signer's private key x_{B_i} for the i^{th} period he must get private key $x_{B_{i-1}}$ of the $(i-1)^{th}$ period, but again by strong RSA assumption of equation (13) it is not feasible for him/her. So he is unable to find proxy private x'_{p} either. That is why there is forward security in the proposed scheme.

6. CONCLUSION

This paper proposes an improved proxy blind signature scheme based on Tan et al.'s, by incorporating forward security mechanism. This forward security mechanism reduces the key leakage impact on system security, due to this even if the present signature key has been compromised, the adversary cannot forge signatures that have been signed earlier or in the past. So signatures that have been signed earlier are still valid. In this manner, the proposed proxy blind signature scheme provides a higher level security to the signature key.

7. REFERENCES

[1] D. Chaum. Blind signatures for untraceable payments. In CRYPTO'82, pages 199–203. Plenum Press, 1983.

[2] E. Okmamoto M. Mambo K. Usuda. Proxy signatures: delegation of the power to sign message. IEICE Transaction Functional, E-79(A-9):1338–1354, 1996.

[3] Z. Liu Z. Tan and C. Tang. Digital proxy blind signature schemes based on dlp and ecdlp. MM Research Preprints, MMRC, AMSS, Academia, Sinica, Beijing, 21:212–217, 2002.

[4] J. K. Jan and W. D. Lin. A security personal learning tools using a proxy blind signature scheme. In Proccedings of International Conference on Chinese Language Computing, pages 273–277, 2000.

[5] A. K. Awasthi and S. Lal. Proxy blind signature scheme. Journal of Information Science and Engineering. 2003. Cryptology ePrint Archive, Report 2003/072, Available at $< http://eprint.iacr.org/ >$.

[6] S. H. Wang F. Bao G. L. Wang and J. Wang. Cryptanalysis of a proxy blind signature scheme based on DLP. Journal of Software. 16(5):911–915, 2005.

[7] Q. Xue and C. Cao. A new proxy blind signature scheme with warrant. In Proceedings of the 2004 IEEE Conference on Cybernetics and Intelligent Systems, pages 1386–1391, 2004.

[8] J. G. Li Y.C. Zhang and S.T. Yang. Cryptanalysis of new proxy blind signature scheme with warrant. In ICCMSE'05, 2005.

[9] H. M. Sun B. T. Hsieh and S. M. Tseng. On the security of some proxy signature schemes. Journal of System and Software, 74:297–302, 2005.

[10] Lin-Chuan Wu Yi-Shiung Yeh and Tsann-Shyong Liu. Analysis of sun et al.'s linkability attack on some proxy blind signature schemes. The Journal of Systems and Software, 79:212–217, 2006.

[11] Shaobin Wang Hong Fan and Guohua Cui. A proxy blind signature schemes based dlp and applying in e-voting. In ICEC'05, pages 641–645, 2005.

[12] J. G. Li and S. H. Wang. New efficient proxy blind signature scheme using verifiable self-certified public key. International Journal of Network Security, 4(2):193–200, 2007.

[13] Mihir Bellare and Sara K. Miner. A forward-secure digital signature scheme. In CRYPTO'99, Lecture Notes in Computer Science, volume 1666, pages 431–448. Springer Verlag, 1999.

[14] R. Anderson. Invited lecture. In Proceedings of 4^{th} ACM Conference on Computer and Communications Security, pages 1–7. ACM Press, 1997.

[15] G. Itkis and L. Reyzin. Forward–secure signature scheme with optimal signing and verifying. In Proceedings of 21^{st} Annual International Cryptology Conference, Lecture Notes in Computer Science, volume 2139, pages 332–354. Berlin: Springer Verlag, 2001.

[16] A. Kozlov and L. Reyzin. Forward-secure digital signature scheme with fast key update. In Proceedings of Security in Communication Network, Lecture Notes in Computer Science, volume 2576, pages 247–262. Berlin: Springer Verlag, 2002.