Journal of The Korea Society of Computer and Information
Vol. 18, No. 7, July 2013
www.ksci.re.kr
http://dx.doi.org/10.9708/jksci.2013.18.7.085

대리 은닉서명 에이전트의 설계를 위한 최적화 알고리즘

이 현 숙 *

An Optimal Algorithm for the Design of a Proxy Blind Signature Agent

Rhee, Hyunsook*

요 약

본 논문에서는 G. Wang의 대리 서명 방식과 Schnorr 은닉 서명 방식을 이용하여 안전한 대리 은닉 서명 방식을 제안한다. 대리 은닉 서명은 대리 서명과 은닉 서명을 결합한 전자 서명 방식이다. G. Wang은 두-참가자 Schnorr 서명 방식에 기반한 안전성 증명가능한 대리 서명 방식을 제안하였다. 이 논문에서는, G. Wang의 대리 서명 방식과 또한, 제안하는 대리 은닉 서명 방식을 이용하여 전자 투표를 위한 대리 에이전트를 고안한다. 그리고, 제안하는 서명 방식이 대리 서명과 은닉 서명의 안전성 요구사항을 모두 만족시키며 최적화된 효율적인 대리 은닉 서명 방식임을 보인다.

▸ Keywords : 전자 서명, 대리 서명, 은닉 서명, 공개 키 암호, 대리 에이전트, 최적화 알고리즘

Abstract

In this paper, on the basis of Guilin Wang's proxy signature scheme and the Schnorr blind signature, we propose a secure proxy blind signature scheme. A proxy blind signature scheme is a digital signature scheme which combines the properties of a proxy signature and a blind signature scheme. Guilin Wang proposed a provably secure proxy signature scheme, which is based on a two-party Schnorr signature scheme. Also, using the proposed proxy blind signature scheme, we propose the proxy agent system for the electronic voting. We show the proposed scheme satisfies the security properties of both the blind signature and the proxy signature scheme and is efficient and optimal proxy blind signature scheme.

▸ Keywords : digital signature, proxy signature, blind signature, public key cryptography, proxy agent, opimal algorithm

•제1저자 : 이현숙 •교신저자 : 이현숙
•투고일 : 2013. 6. 4, 심사일 : 2013. 6. 13, 게재확정일 : 2013. 7. 10.
* 동양미래대학교 전산정보학부(School of Computing & Information, Dongyang Mirae University)
"본 논문은 동양미래대학교 2011학년도 교내 학술연구과제 지원 사업에 의하여 연구되었습니다."

I. Introduction

In 1996, Mambo, Usuda, and Okamoto proposed a new concept, proxy signature [1], [2]. In a proxy signature scheme, one user Alice, called the original signer delegates her signing capability to another user Bob, called the proxy signer, and Bob can sign messages on a behalf of Alice. A verifier can validate its correctness and can distinguish between a normal signature and a proxy signature. As a result, the verifier can be convinced of the original signer's agreement on the signed message. Proxy signature schemes have been suggested for use in a number of applications, including electronic commerce, mobile agents, and distributed shared object systems, etc. In an example, the president of a company delegates a signing right to his/her secretary before a vacation. The secretary can make a signature on behavior of the president and a verifier is confident that the signature has been made by an authorized secretary, and the verifier can be convinced of the president's agreement on the signed message.

D. Chaum [3] introduced the concept of a blind signature scheme in 1982. Using this scheme a user can obtain the signature of the signer on any given message, without revealing any information about the message and

its signature. It does not only achieve the unforgeability property but also achieves the untraceability and unlinkability properties. With such properties, the blind signature scheme is useful in several applications such as e-payment and e-voting. In an e-payment system, a bank makes a blind signature for a user and the user has an untraceability and unlinkable e-coin. This is a typical untraceable scheme which allows a user to withdraw a valid e-coin from a bank and spend the e-coin anonymousely at a shop. Typically, a blind signature scheme is as follows. A user selects blinding factors randomly, makes a blinded message using blinding factors, and sends it to a signer. The signer makes the blind signature and returns it to the user. The user performs an unblinding operation and gets an original signature.

In this paper, we propose the proxy agent system for the electronic voting. We show the proposed scheme satisfies the security properties of both the blind signature and the proxy signature scheme and is efficient and optimal proxy blind signature scheme.

The rest of this paper is organized as follows. Section II introduces the computational assumptions, security requirements, and notations for a proxy blind signature scheme. Section III presents a new proxy blind signature scheme and Section IV discusses its security. The performance of the new scheme will be analyzed in section V. In Section VI, we show an instance of proxy blind signature scheme in electronic election system. And we propose the proxy agent system using the proposed scheme for electronic voting. Finally, the conclusion will be given in Section VII.

II. Preliminaries

2.1 Definitions

Definition 1. A proxy blind signature scheme is usually comprised of the following procedures:

-Setup: The original signer Alice and the proxy signer Bob generate their private, public key pairs, respectively. These key pairs are used in a normal signature scheme.

-Proxy delegation: The original signer Alice and the proxy signer Bob perform an interactive protocol to generate a proxy private, public key pair (x_p, y_p). x_p is known only to the proxy signer Bob and y_p is public or revocable publicly.

-Proxy blind signature generation: A user(verifier) Cindy blinds the message m and sends it to Bob. The proxy signer Bob signs on a blinded message using proxy private key x_p and sends the

blinded signature to Cindy. In this protocol, Bob cannot know the original message m.

-Unblinding & verification: Cindy performs an unblinding operation and derives an unblinded signature σ from the information that is sent by Bob, and Cindy verifies m and σ using usual verification equation.

The security requirements for proxy blind signature are first specified in [4].

Definition 2. A secure proxy blind signature scheme should satisfy the following requirements:

-Distinguishability: The proxy blind signature must be distinguishable from the normal signature.

-Non-repudiation: Neither the original signer nor the proxy signer can sign the message instead of the other party. Both the original signer and the proxy signer cannot deny their signatures against anyone.

-Verifiability: The proxy blind signature can be verified by everyone.

-Unforgeability: Only the designated proxy signer can create the proxy blind signature(even the original signer cannot do it).

-Unlinkability: When the signature is verified, the signee knows neither the message nor the signature associated with the signature scheme.

2.2 Notations

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

-p, q: two large prime numbers, $q \mid p-1$

-g: an element of Z_p^*, its order is q

-x_u, y_u: participant U's private key and public key respectively, $y_u = g^{x_u}$

-H(): a public cryptographically strong hash function

-||: which denotes the concatenation of strings

-m_w: the warrant which specifies the delegation period for the kind of message m is delegated, and identities of the original signer and the proxy signer, etc.

III. A Secure proxy blind signature algorithm

We now present a new secure proxy blind signature scheme. Our new scheme is constructed in two parts. One is the proxy delegation part, using Wang's proxy siganture scheme [5] that is based on the two-party Schnorr signature. Another is the blind signature part using the Schnorr blind signature scheme [6].

In the following description, it is supposed that the original signer Alice and the proxy signer Bob have agreed on a warrant m_w before generating a proxy key pair. Other system parameters are the same as Tan et al.'s [4] and Lal and Awasthi's [7] proxy blind signature schemes. We skip the setup phase

The original signer Alice and the proxy signer Bob jointly generate a proxy key pair (x_p, y_p) for Bob, and the asker(verifier) Cindy can recover the proxy public key y_p for verification.

3.1 Proxy Delegation Phase

To generate a proxy key pair x_p, y_p for the proxy signer Bob, Alice and Bob execute the following interactive protocol jointly.

(1) Alice picks a random number $k_A \in_R Z_q^*$, computes $r_A = g^{k_A} \bmod p$ and $c = H(r_A)$, and then sends c to Bob.

(2) Similarly, Bob chooses a random number $k_B \in_R Z_q^*$, computes $r_B = g^{k_B} \bmod p$, and replies to Alice with (c, r_B).

(3) When (c, r_B) is received, Alice checks whether $r_B^q \equiv 1 \bmod p$. If the validation goes through, she computes $r_P = r_A r_B \bmod p$, $s_A = k_A + x_A H(m_w, r_P) \bmod q$, and sends the pair (r_A, s_A) to Bob.

(4) Upon receiving (r_A, s_A), Bob first computes $r_P = r_A r_B \bmod p$, and then checks whether $r_A^q \equiv 1 \bmod p$, $c \equiv H(r_A)$, and $g^{s_A} \equiv y_A^{H(m_w, r_P)} r_A \bmod p$. If all validations are passed, he calculates $s_B = k_B + x_B H(m_w, r_P) \bmod q$, and finally sets his proxy key pair (x_P, y_P) by $x_P = s_A + s_B \bmod q$, and $y_P = g^{x_P} \bmod p$.

3.2 Signing Phase

To generate a proxy blind signature for the asker(verifier) Cindy, the proxy signer Bob and Cindy execute the following interactive protocol jointly.

(1) Bob picks a random number $\bar{k} \in_R Z_q^*$, computes $\bar{r} = g^{\bar{k}} \bmod p$, and then sends $(\bar{r}, r_P, m_w)$ to Cindy.

(2) Cindy checks Alice′s and Bob′s identities and delegation lifetime of the warrant m_w. If the above checking is passed, Cindy follows the next operations for blinding the message. Cindy recovers y_P by $y_P = y_A y_B^{H(m_w, r_P)} r_P \bmod p$ and chooses random numbers $\alpha, \beta \in_R Z_q^*$. Next Cindy computes $r = \bar{r} g^{\alpha} y_P^{\beta} \bmod p$, $\bar{c} = H(r, m, m_w) + \beta \bmod q$, and replies to Bob with $\bar{c}$.

(3) Upon receiving $\bar{c}$, Bob computes $\bar{s} = \bar{k} + x_P \bar{c} \bmod q$ and sends $\bar{s}$ to Cindy.

(4) Upon receiving $\bar{s}$, Cindy first computes $s = \bar{s} + \alpha \bmod q$, $c = \bar{c} - \beta \bmod q$. The proxy blind signature on message m is (s, c).

3.3 Verification Phase

The verifier Cindy can verify the proxy blind signature by checking whether

$$c \equiv \mathrm{H}(g^{\mathrm{s}} y_{\mathrm{P}}^{-\mathrm{c}}, \mathrm{m}, \mathrm{m_w}) \bmod q$$

holds. This is because:

$$\begin{aligned} H(g^s y_P^{-c}, m, m_w) &= H(g^{\bar{s}+\alpha} y_P^{-\bar{c}+\beta}, m, m_w) \\ &= H(g^{\bar{k}+x_P\bar{c}+\alpha} g^{-x_P\bar{c}+x_P\beta}, m, m_w) \\ &= H(g^{\bar{k}+\alpha+x_P\beta}, m, m_w) \\ &= H(\bar{r} g^{\alpha} y_P^{\beta}, m, m_w) \\ &= H(r, m, m_w) \\ &= \bar{c} - \beta \\ &= c \end{aligned}$$

IV. Analysis of the proposed algorithm

Theorem 1. The proposed scheme satisfies the unforgeability property.

Proof. Firstly, we show that the original signer cannot forge the proxy signature without the proxy signer′s help. Assume that the original signer Alice can forge proxy signature $(m, (s, c), m_w, r_P)$. Then,

$$\begin{aligned} \bar{c} &= H(r, m, m_w) + \beta \bmod q \\ c &= \bar{c} - \beta \bmod q \end{aligned}$$

Because $\bar{c} = c + \beta \bmod q$, it is clear that

$$c = H(r, m, m_w) \bmod q.$$

By the way, we can get c′, another result using the same input (r, m, m_w) and the other hash function H′. In other words,

$$c' = H'(r, m, m_w) \bmod q.$$

Therefore, the original signer Alice can forge another signature $(m, (s', c'), m_w, r_P)$ for message m. And, because $r = \bar{r} g^{\alpha} y_P^{\beta} = g^s y_P^{-c} \bmod p$, then

$$g^s y_P^{-c} = r = g^{s'} y_P^{-c'} \bmod p.$$

And,

$$g^{(s-s')} = y_P^{(c-c')} = g^{x_P(c-c')}.$$

Consequently,

$$g^{x_P} = g^{\frac{s-s'}{c-c'}} \bmod p,$$
$$x_P = \frac{s-s'}{c-c'} \bmod q.$$

That is to say, the original signer Alice can compute x_P, the discrete log of y_P. However, we already know that this is infeasible as previously stated in Assumption 1. Therefore, the original signer Alice cannot forge the proxy signature without the proxy signer's help. Also, in case Alice tries to generate $(m,(s',c'),m_w{}',r_P{}')$ by replacing proxy secret key, x_P, this is also infeasible. When the proxy signature is verified, not only the proxy signer's but also the original signer's public keys are used in the verification equation. Thus the forged proxy signature that is generated without valid proxy secret key x_P cannot pass the verification. Also, in this case, the original signer Alice cannot forge the proxy signature.

Secondly, the third party cannot forge the valid proxy signatures as the third party knows less than the original signer Alice. Now that the original signer Alice is unable to generate valid proxy blind signatures, the third party cannot generate valid proxy blind signatures either.

Consequently, our proxy blind signature scheme satisfies the unforgeability property.

Theorem 2. The proposed scheme satisfies the unlinkability property.

Proof. In order to prove the blindness of the protocol, we show that given any view ν and any valid message and signature $(m,(s,c),m_w,r_P)$, there exists a unique pair of blinding factors α,β. If that is true, the proxy signer's view ν and message-signature pair are statistically independent. Then the signature scheme is called blind.

Because the verifier Cindy chooses the blinding factor α,β at random, the blindness of the signature scheme follows. If the signature $((s,c),m_w,r_P)$ of m has been generated during an execution of the protocol with view ν consisting of $\bar{k},\bar{r}=g^{\bar{k}} \bmod p,\bar{c},\bar{s}=\bar{k}+\bar{c}x_P \bmod q$, then the following equations must hold for α,β.

$$\bar{c} = H(\bar{r}g^{\alpha}y_p^{\beta},m,m_w) + \beta \bmod q,$$
$$s = \bar{s}+\alpha \bmod q,$$
$$c = \bar{c}-\beta \bmod q$$

The blinding factors α,β are uniquely determined by the following two equations:

$$\alpha = s-\bar{s} \bmod q,$$
$$\beta = \bar{c}-c \bmod q$$

By substituting the above equations, we obtain:

$$\bar{c} = H(\bar{r}g^{s-\bar{s}}y_P^{\bar{c}-c},m,m_w) + \bar{c}-c \bmod q$$

Because

$$H(\bar{r}g^{s-\bar{s}}y_P^{\bar{c}-c},m,m_w)$$
$$= H(g^{\bar{k}}g^{s-\bar{k}-x_P\bar{c}}g^{x_P\bar{c}-x_Pc},m,m_w)$$
$$= H(g^{s}y_P^{-c},m,m_w)$$
$$= c \quad (by\ verification\ equation)$$

Therefore, given any view ν and any valid message signature pair, there exists a unique pair of blinding factors α,β. Consequently, our proxy blind signature scheme satisfies the unlinkability property.

Theorem 3. The proposed scheme satisfies the non-repudiation property.

Proof. As to the property of non-repudiation, it implies that proxy signers cannot deny having signed the message on behalf of the original signer to any person. In the proposed scheme, when the

proxy blind signature $(m,(s,c),m_w,r_P)$ is verified, the warrant m_w is checked and the public keys y_A and y_B of the original signer and the proxy signer are used in the verification equation. So the original signer and proxy signer cannot deny having signed the message m on behalf of the original signer to any person.

Theorem 4. The proposed scheme) satisfies the distinguishability property.

Proof. In the proposed scheme, when the proxy blind signature $(m,(s,c),m_w,r_P)$ is verified, not only the proxy signer's but also the original signer's public keys and identities are used in the verification equation, so we can regard it as a proxy signature and not a normal signature. Thus, anyone can distinguish the proxy blind signature from normal signatures.

Theorem 5. The proposed scheme satisfies verifiability property.

Proof. The security property implies that from the proxy signature a verifier can be convinced of the original signer's agreement on the signed message. In the proposed scheme, on the one hand, from the warrant m_w, the verifier can know who the original signer and the proxy signer are. On the other hand, when the proxy signature is verified, the original signer's and the proxy signer's public keys and identities are used in the verification equation. Thus the original signer cannot deny having delegated his signing capability to the designated proxy signer. That is to say, any verifier can be convinced of the original signer's agreement on the signed message. Therefore, the proposed scheme can fulfill the verifiability property.

V. Performance analysis of the proposed algorithm

In this section, Tan et al's scheme [4], Lal et al's scheme [7] and the proposed scheme are compared in terms of computational complexities. We denote the following notations to facilitate the performance evaluation:

E: The time for performing a modular exponentiation computation

M: The time for performing a modular multiplication computation

I: The time for performing a modular inverse computation

The comparison of computational complexities among Tan et al's scheme, Lal et al's scheme and the proposed scheme is described in Table 1.

Table 1. Comparison of computational complexity

Phase	Tan et al's Scheme	Lal et al's Scheme	The Proposed Scheme
Proxy Delegation Phase	3E + 2M	4E + 2M	6E + 5M
Signing Phase	8E + 7M + 4I	3E + 3M + 2I	4E + 5M
Verification Phase	3E + 3M + I	2E + M	2E + M + I
Total	14E + 12M + 5I	9E + 6M + 2I	12E + 11M + I

From Table 1, it can be seen that the computation cost of our scheme is more efficient and optimal proxy blind signature scheme than Tan et al's scheme but has some overhead comparing with Lal et al's scheme.

VI. The Proxy Agent System of in the Mobile Environment

Recently, many applications of the proxy blind signture scheme are proposed in the domain of

electronic cash, electronic voting, and etc [8-11]. J. Liu et al. proposed a new proxy blind signature scheme and it application for electronic cash [8]. X Wen et al. proposed a proxy blind signature scheme for electronic payment [9]. S. Panda et al. proposed stamped proxy blind signature scheme [10] and J. shi et al. proposed proxy signature and two-paricle entangled system [11]. As an instance of the proposed proxy blind signature agent scheme an electronic election system is described. In an electronic election system, a vote managing center delegates the right of vote managing to the vote branches(proxy blind agent). A voter can log a vote branch and vote. In this process, a voter's voting information cannot be revealed. In other words, a vote branch cannot know for whom a voter voted. The proposed proxy blind signature scheme can be used in a secure electronic election system. The original signer Alice as a vote managing center delegates signing right to the proxy signer Bob - proxy blind agent - as a vote branch. The proxy signer is proxy blind agent system. A user(the verifier), as a voter, can vote and the voting message is not known to the vote branch. In addition, a vote branch cannot trace the message and the signature. Our proxy blind signature scheme can be used in a secure electronic election system and can protect the voter.

VII. Conclusion

In this paper, we propose a new secure proxy blind signature scheme. Our new proxy blind signature scheme is secure because of the removal of some of the previous scheme's shortcomings. To remove the weaknesses, we have proposed a proxy blind signature scheme with warrant and used the two-party Schnorr signature scheme and the Schnorr blind signature scheme. We have shown that our scheme satisfies all security properties of the proxy blind signature scheme: Distinguishability, Non-repudiation, Verifiability, Unforgeability, and Unlinkability. Our scheme is more secure than the existing proxy blind signature schemes. And, we propose the proxy agent system for the electronic voting. We show the proposed scheme is efficient and optimal proxy blind signature scheme.

References

[1] M. Mambo, K. Usuda, and E. Okamoto. "Proxy signatures: Delegation of the power to sign messages", IEICE Trans. Fundamentals, Vol. E79-A, No. 9, pp. 1338-1353, Sep 1996.

[2] M. Mambo, K. Usuda, and E. Okamoto. "Proxy signatures for delegating signing operation", 3rd ACM Conference on Computer and Communications Security (CCS'96), New York: ACM Press, pp. 48-57, 1996.

[3] D. Chaum. Blind signatures for untraceable payments. In Crypto'82, New York: Plenum Press, pp. 199-203, 1983.

[4] Z. Tan, Z. Liu, C. Tang. Digital Proxy Blind Signature Schemes Based on DLP and ECDLP. In: MM Research Preprints, No. 21, MMRC, AMMS, Academia Sinica, Beijing, pp. 212-217, 2002.

[5] G. Wang. Designated-Verifier Proxy Signature Schemes. In: Security and Privacy in the Age of Ubiquitous Computing (IFIP/ SEC 2005), Springer, pp. 409-423, 2005.

[6] C.P. Schnorr. Security of blind discrete log signatures against interactive attacks. In: Information and Communications Security (ICICS 2001), LNCS 2229, Springer-Verlag, pp. 1-12, 2001.

[7] S. Lal, A. K. Awasthi. Proxy Blind Signature Scheme. In: Journal of Information Science and Engineering. Cryptology ePrint Archive, Report 2003/072, http://eprint.iacr.org/

[8] J Liu, J Liu, X Qiu, A proxy blind signature scheme and an off-line electronic cash scheme. Wuhan University Journal of Natural Sciences. Vol. 18. No. 2, pp. 109-116. 2013.

〔9〕 X Wen, Y Chen, J Fang, An inter-bank E-payment protocol based on quantum proxy blind signature. Quantum information processing, pp. 549-558, 2013.
〔10〕 S Panda, R Kumar Mohapatra, Stamped Proxy Blind Signature Scheme, International Journal of Computer Applications, vol. 64, issue 15, pp. 38-41, 2013.
〔11〕 J Shi, R Shi, X Peng, MH Lee, Quantum communication scheme for blind signature with arbitrary two-particle entangled system, Advanced Communication Technology (ICACT), 2013 15th International Conference, pp. 58-62, Jan. 2013.

저 자 소 개

이 현 숙
1989년 : 서강대학교 전자계산학과(학사)
1991년 : 포항공과대학교 컴퓨터공학과(석사)
1997년 : 서강대학교 컴퓨터학과(박사)
1991년~1997년 : 한국전자통신연구소(ETRI) 연구원
2006-2007년 : University of Central Florida 방문교수
1997년~현재 : 동양미래대학교 전산정보학부 교수
관심분야 : 지능형정보처리, 소프트웨어개발방법론, 알고리즘
Email : hsrhee@dongyang.ac.kr