An Improved Threshold Proxy Signature Scheme Based on RSA

Xuedong Dong[1, a] and Yuan Gao[1, b]

[1]College of Information Engineering, Dalian University, Dalian 116622, P. R. China

[a]dongxuedong@sina.com, [b]1069957580@qq.com

Keywords: Proxy signature; Threshold proxy signature; RSA cryptosystem

Abstract. This paper proposes an improved RSA-based threshold proxy signature scheme. The proposed scheme satisfies the necessary security requirements of proxy signature such as verifiability, unforgeability, threshold property and identifiability. The proposed scheme does not require any secure channel to deliver the proxy keys any more.

Introduction

A proxy signature scheme involves three entities: an original signer, a proxy signer and a verifier. 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. [1,2] first introduced the notion of proxy signature in 1996 and gave a systematic discussion of proxy signatures. They mentioned three levels of delegation:full delegation, partial delegation and delegation by warrant. In full delegation, the original signer gives its private key to the proxy signer. In partial delegation,the original signer generates a proxy signature key from its private key and gives it to the proxy signer. The proxy uses the proxy key to sign. The verification equation for proxy signature is modified, so that the proxy signature is distinguishable from the signature created by the original signer. In delegation by warrant, warrant is a certificate composed of a message part and a public signature key. The proxy signer obtains the warrant from the original signer and uses the corresponding private key to sign. The resulting signature consists of the created signature and the warrant. There are many proxy signature schemes in the literature. Kim, et al. [3] proposed a scheme by restricting proxy signer signing right using the concept of partial delegation with warrant in 1997. Okamoto et al. [4] proposed proxy signature based on RSA scheme in 1999. In 2001, Lee et al. [5, 6] proposed a proxy-protected signature scheme based on the RSA assumption. Shao [7] proposed proxy-protected signature scheme based on RSA in 2009. In 2012,Huang [8] proposed a threshold proxy signature scheme based on RSA cryptosystem. Howerer, in Huang's scheme a secure communication channel is needed among an original signer and her / his proxy signers, which is unpractical. In this paper, we propose an improved threshold proxy signature scheme based on RSA which not only keeps the original properties of the scheme in [8], but also need no any secure communication channel. The rest of the paper is organized as follows. In Section 2, we give an improved threshold proxy signature scheme based on RSA. In Section 3, we give security analysis of the scheme. Finally, a conclusion is drawn in Section 4.

Proposed Scheme

In this section, we propose an improved threshold proxy signature scheme based on RSA.

Throughout this article, we use U_O to denote the original signer and $G=\{U_1,U_2,\cdots,U_n\}$ the set of the proxy signers. The scheme is divided into four phases: *Setup Parameters, Proxy Secret Key Sharing, Proxy Signature Generation* and *Proxy Signature Verification.*

Setup Parameters:

The original signer chooses two strong primes $p_0=2p_0^{'}+1$ and $q_0=2q_0^{'}+1$, where $p_0^{'}$ and $q_0^{'}$ are also primes. Both p_0 and q_0 should be so safe that anybody can't factor $N=p_0q_0$ efficiently.

1) The original signer chooses a public key e_O, $1 < e_O < \phi(N) = (p_0 - 1)(q_0 - 1)$, such that $(e_O, \phi(N)) = 1$, and then uses extended Euclidean algorithm to compute the secret key d_O, $1 < d_O < \phi(N)$, such that $e_O d_O \equiv 1 (\mathrm{mod}\, \phi(N))$. Let (N, e_O) be public.
2) Let $h(\cdot)$ be a secure one-way hash function and m_ω a warrant which consists of the original signer and proxy signers' information, i.e., the identity of the original signer and proxy signers, the qualification of the message on which proxy signers can sign on behalf of the original signer, the validity period of delegation etc.

All proxy signers generate the following public parameters through dialogue and consultation:

1) Choose a large prime p such that $N < p$ and p has a large prime divisor q;
2) Choose a generator g with order q in the multiplicative unit group of the ring Z_p;
3) Determine the identity number ID_i for each proxy signer, where $1 \le i \le n$.
4) Each proxy signer U_i chooses her/his secret key d_i to compute proxy public key $y_i = g^{d_i} (\mathrm{mod}\, p)$ and then make it public, where $1 \le i \le n$.

Proxy Secret Key Sharing:

1) The original signer chooses a random polynomial $f(x)$ with degree $t-1$ in $Z_N[x]$ such that $f(0) = d_O m_\omega$ and then computes $k_i = f(ID_i) z_i^{-1} (\mathrm{mod}\, N)$, where $z_i = \prod_{1 \le j \le n, j \ne i} (ID_i - ID_j) (\mathrm{mod}\, N)$;
2) The original signer uses the ElGamal Cryptosystem to send $k_i (\mathrm{mod}\, N)$ to the proxy signer U_i through a public communication channel. The details are as follows. The original signer randomly selects $l_i \in Z_q^* = Z_q - \{0\}$, and computes $u_i = g^{l_i} (\mathrm{mod}\, p)$ and $v_i = k_i y_i^{l_i} \bmod p)$, where $y_i = g^{d_i} (\mathrm{mod}\, p)$ is the proxy public key of and the proxy signer U_i, $1 \le i \le n$. Then the original signer sends the pair (u_i, v_i) to the proxy signer U_i. After receiving the pair (u_i, v_i), the proxy signer U_i computes $v_i u_i^{-d_i} (\mathrm{mod}\, p)$ to recover the proxy secret key shadow k_i, where $1 \le i \le n$.

Proxy Signature Generation:

Without loss of generality, assume that $U_1, U_2, \cdots, U_t$ are practical proxy signers who creates a signature for a message m on behalf of the original signer. Signature generation is as follows.

1) Each proxy signer U_i randomly chooses a $t_i \in Z_q^* = Z_q - \{0\}$, where $1 \le i \le t$, then computes $r_i = g^{t_i} (\mathrm{mod}\, p)$ and broadcasts it in the proxy group;
2) Each proxy signer U_i computes $R = \prod_{i=1}^{t} r_i (\mathrm{mod}\, p), s_i = d_i h(R, m, A) + t_i R (\mathrm{mod}\, p)$, $y_i = g^{d_i} (\mathrm{mod}\, p)$, and then sends the triple (R, s_i, y_i) to the designated combiner (DC), where A is the set consisting of identities of practical proxy signers;
3) After receiving (R, s_i, y_i), DC verifies whether $g^{s_i} \equiv r_i^R y_i^{h(R,m,A)} (\mathrm{mod}\, p)$. If the equality holds, DC computes $S = \sum_{i=1}^{t} s_i (\mathrm{mod}\, p)$ and broadcasts it in the proxy group;
4) Each proxy signer U_i uses her/his secret key shadow k_i to compute $C^i \equiv S^{k_i \delta_i} (\mathrm{mod}\, N)$, and then sends it to DC again, where $\delta_i = \prod_{1 \le j \le t, j \ne i} (-ID_j) (\prod_{t < j \le n, j \ne i} (ID_i - ID_j) (\mathrm{mod}\, N)$. DC computes $C = \prod_{i=1}^{t} C_i (\mathrm{mod}\, N)$. The final proxy signature for the message m is (R, S, C, A, m_ω).

Proxy Signature Verification:

After receiving proxy signature (R, S, C, A, m_ω) for the message m, the verifier verifies whether equations $g^s \equiv R^R \prod_{i=1}^{t} y_i^{h(R,m,A)} (\text{mod } p)$ and $C^{e_O} \equiv S^{m_\omega} (\text{mod } N)$ hold or not. If both equations hold, she/he accepts it as a valid proxy signature; otherwise, rejects it.

Security Analysis

We now show that the proposed scheme satisfies the security features, namely, verifiability, unforgeability, threshold property, identifiability as follows.

1) *Verifiability*

It is clear that $g^s \equiv g^{\sum_{i=1}^{t} s_i} \equiv \prod_{i=1}^{t} r_i^R y_i^{h(R,m,A)} \equiv R^R \prod_{i=1}^{t} y_i^{h(R,m,A)} (\text{mod } p)$. By Lagrange interpolation formula we have $f(x) = \sum_{i=1}^{t} f(ID_i) \prod_{1 \le j \le t, j \ne i} (x - ID_j) / (\prod_{1 \le j \le t, j \ne i} (ID_i - ID_j)$ and therefore $\sum_{i=1}^{t} k_i \delta_i e_O \equiv \sum_{i=1}^{t} e_O f(ID_i) z_i^{-1} \prod_{1 \le j \le t, j \ne i} (-ID_j)(\prod_{t < j \le n, j \ne i} (ID_i - ID_j) \equiv e_O f(0) = e_O d_O m_\omega (\text{mod } N)$. Thus we get $C^{e_O} \equiv \prod_{i=1}^{t} C_i^{e_O} \equiv \prod_{i=1}^{t} S^{k_i \delta_i e_O} \equiv S^{\sum_{i=1}^{t} k_i \delta_i e_O} \equiv S^{m_\omega} (\text{mod } N)$. This show that the verifier of proxy signature can check whether above two verification equations hold or not.

2) *Unforgeability*

The original signer cannot construct the proxy signature assuming the hardness of breaking RSA. Besides, the proxy signature is created with the proxy signer's secret key d_i and secret key shadow k_i. Obtaining these secret keys by any other party is as difficult as breaking RSA and Discrete Logarithm problem. Therefore, the proposed scheme satisfies the unforgeability property.

3) Threshold property

If the number of proxy signers is less than the threshold t, then by Shamir's secret sharing scheme They cannot recover the proxy secret key $f(0) = d_O m_\omega$ and therefore they cannot create the proxy signature. Whereas, if the number of proxy signers is larger than or equal to the threshold t, then they can recover the proxy secret key $f(0) = d_O m_\omega$ and therefore they can create the proxy signature.

4) *Identifiability*

The verification process of the proposed scheme requires proxy signer's proxy public key $y_i = g^{d_i} (\text{mod } p)$ and warrant m_ω. Thus, in the verification process any verifier can determine the identity of the proxy signer.

Summary

In this paper, we have proposed an improved threshold proxy signature scheme based on RSA. The proposed scheme satisfies the necessary security requirements of proxy signature and does not require any secure channel to deliver the proxy keys unlike the scheme of [8].

Acknowledgements

This research was financially supported by the Research Project of Liaoning Education Bureau under Project Code L2014490.

References

[1] 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.

[2] M. Mambo, K. Usuda and E. Okamoto, Proxy signatures: delegation of the power to sign messages, IEICE Trans Fundam, E79-A (1996) 1338-1354.

[3] S. Kim, S. Park and D. Won, Proxy signatures, In: ICICS97, LNCS 1334, Springer-Verlag, 1997, pp. 223-232.

[4] 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.

[5] 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.

[6] 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.

[7] Z. Shao, Provably secure proxy-protected signature schemes based on RSA, Comput. Electr. Eng., 35 (2009) 497-505.

[8] M.J.Huang,Threshold proxy signature scheme based on RSA cryptosystem, Computer Engineering, 38(2012)105-106.

