Information Processing Letters 114 (2014) 5–8

Contents lists available at ScienceDirect

Information Processing Letters

www.elsevier.com/locate/ipl

Security pitfalls of an efficient threshold proxy signature scheme for mobile agents

Yong Yu [a,b,*], Yi Mu [b], Willy Susilo [b], Man Ho Au [b]

[a] School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu, 610054, PR China
[b] School of Computer Science and Software Engineering, University of Wollongong, Wollongong, NSW 2522, Australia

ARTICLE INFO

Article history:
Received 22 April 2013
Accepted 17 October 2013
Available online 25 October 2013
Communicated by S.M. Yiu

Keywords:
Cryptography
Digital signature
Proxy signature
RSA cryptosystem
Security analysis

ABSTRACT

A (t, n) threshold proxy signature scheme enables an original signer to delegate his/her signing power to n proxy signers such that any t or more proxy signers can sign messages on behalf of the original signer, but $t-1$ or less of them cannot produce a valid proxy signature. Based on the RSA cryptosystem, Hong proposed an efficient (t, n) threshold proxy signature for mobile agents. Cai et al. found that the scheme due to Hong is proxy-unprotected, meaning that the original signer can generate a valid proxy signature by himself. However, it is unclear whether the scheme can be used in reality after fixing the security problem discovered by Cai et al. In this letter, we provide a detailed analysis on Hong's scheme and show that the scheme fails to achieve the properties of secrecy, proxy protected, undeniability, identifiability and even time constraint and thus adopted of this efficient construction in practice is not recommended.

1. Introduction

The notion of proxy signature [1] was invented by Mambo et al., which enables a proxy signer to sign messages on behalf of an original signer in case of say, temporal absence, lack of computational power, etc. After validating the correctness of a proxy signature following a given verification algorithm, a verifier can be convinced of the original signer's agreement on the signed message. In the last years, fruitful achievements [2–9] of proxy signatures have been seen, including novel constructions, analysis, improvements and applications. Proxy signatures have found extensive uses in numerous practical applications such as in distributed computing, e-commerce, e-cash, and grid computing where delegation of rights is quite common [2,3]. Mambo et al. [1] classified this kind of cryptographic primitive into two categories, namely, proxy-unprotected and proxy-protected. A proxy-protected scheme, where only the proxy signer is able to generate valid proxy signatures, is more practical since it accommodates some highly desirable properties such as fairness and signature ownership. In the latest research, delegation with warrant is popular because of its high security and flexible delegation policy for a proxy signature scheme.

Among all the variants of proxy signature schemes, threshold proxy signature is one of the useful cryptographic primitives. In a (t, n) threshold proxy signature scheme, the original signer delegates and distributes the signing power to n proxy signers such that collaborative effort of at least t proxies is required to the creation of a valid proxy signature, while $t-1$ or less of them cannot complete a signing operation. Threshold proxy signature is a promising primitive for it allows the original signer to control the delegation of his signing capability. Not only does it allow the original signer to choose the group of proxies, but also the selection of the threshold value. Thus, to some extent, threshold proxy signatures are more flexible and practical than traditional proxy signature schemes. Based on the tricks of secret sharing and threshold cryptography, Zhang [10] and Kim [11] proposed threshold proxy signature schemes for the first time independently. Subsequently, Sun et al. [12] extended

* Corresponding author.
E-mail address: yyucd2012@gmail.com (Y. Yu).

0020-0190/$ – see front matter
http://dx.doi.org/10.1016/j.ipl.2013.10.006

the construction due to Kim et al. and presented a non-repudiable threshold proxy signature scheme with known signers. Unfortunately, Hsu et al. [13] found the scheme in [12] suffers from the conspiracy attack, namely, any t or more proxy signers can get the secret keys of other proxy signers. Hwang et al. [14] proposed a new threshold proxy signature scheme with known signers and claimed their construction can achieve all the desirable security properties of a proxy signature scheme. However, Wang et al. [15] identified several security weaknesses in the scheme and concluded that the scheme is not secure. Observing there are few secure (t, n) threshold proxy signature schemes based on the RSA cryptosystem, Hong [16] proposed a novel and practical (t, n) threshold proxy signature from RSA mechanism by applying the traditional RSA cryptosystem without using additional cryptographic techniques, and suggested to apply the proposal to mobile agent systems. They claimed that the scheme satisfies all the desirable security requirements. Unfortunately, Cai et al. [17] demonstrated an concrete attack against Hong's construction in which a malicious original signer can forge a valid threshold proxy signature.

Our contributions: It is not an easy task to construct a secure threshold proxy signature scheme from the well-studied RSA problem since sharing the private key of the RSA system [20] among multiple members is difficult and the Euler phi function of the modulus cannot be leaked to any proxy signer. Hong's scheme [16] has many advantages over other schemes in the same style such as it shares the proxy signing key using the simple Lagrange formula; the proxy signature generation and combination are completely non-interactive; the sizes of both the partial proxy signing key and partial proxy signature are independent of the number of the proxy signers. It is interesting to find out whether we can use Hong's scheme in reality after fixing the security problem identified by Cai et al. [17]. Unfortunately, in this letter, after giving a detailed analysis of Hong's scheme, we find that the construction fails to achieve all the security properties of a secure proxy signature scheme, including secrecy, proxy protected, undeniability, identifiability and even time constraint (prevention of misuse).

Organization: Section 2 reviews Hong's threshold proxy scheme. Section 3 describes our security analysis of the scheme. Section 4 concludes the paper.

2. Review of Hong's scheme

The following notations are used in Hong's scheme [16]. The original signer is denoted by U_0, the n proxy signers are denoted by $U_1, \ldots, U_n$, and a combiner is denoted by C. H is a secure hash function; m_w denotes a warrant, which specifies the identities of the original signer and the proxy signers, the parameters (t, n), the valid delegation period and the kind of messages being delegated, etc. Q_N denotes the subgroup of squares in Z_N^*. The following five phases are involved in the scheme.

Setup: The original signer U_0 picks two large secure primes of equal length p_0, q_0 and computes $N_0 = p_0 q_0$, where $p_0 = 2p_0' + 1, q_0 = 2q_0' + 1$ with p_0', q_0' themselves prime. Let $M_0 = p_0' q_0'$, which is the order of the group Q_{N_0}. U_0 computes her RSA exponents e_0 and d_0 such that $e_0 d_0 \equiv 1 \pmod{M_0}$. The private key of U_0 is (d_0, M_0) and the public key is (e_0, N_0). Each proxy signer U_i $(i = 1, 2, \ldots, n)$ chooses two random large secure primes of equal length p_i and q_i, and computes $N_i = p_i q_i$, $\phi(N_i) = (p_i - 1)(q_i - 1)$, e_i and d_i where $e_i d_i \equiv 1 \pmod{\phi(N_i)}$. The private key and the public key of U_i are d_i and (e_i, N_i) respectively.

Proxy sharing: U_0 firstly generates the threshold proxy signing key $D \equiv d_0 \cdot H(m_w) \pmod{M_0}$, and shares the signing key among the proxy signer group as follows.

(1) Set $a_0 = D$ and for $1 \leqslant i < t$, pick at random a_i from $\{0, \ldots, M_0 - 1\}$, and define a $t - 1$ degree polynomial

$$f(x) \equiv a_0 + a_1 x + \cdots + a_{t-1} x^{t-1} \pmod{M_0}.$$

(2) Compute partial proxy signing key $k_i \equiv f(i) \pmod{M_0}$ for each proxy singer U_i.

(3) For the purpose of share validation, U_0 picks a random element $v \in Q_{N_0}$ and computes $v_i = v^{k_i}$ for $1 \leqslant i \leqslant n$. U_0 makes $(v, v_1, \ldots, v_n)$ public and sends k_i to U_i in a secure manner.

Proxy signature generation: Assume t different proxy signers U_i $(i = 1, \ldots, t)$ would like to generate a proxy signature of message m on behalf of U_0 cooperatively. Let $x = H(m, m_w)$ and $\Delta = n!$. Each proxy signer computes the partial proxy signature $x_i = x^{2\Delta \cdot k_i} \in Q_{N_0}$. Then, U_i computes $\Delta\sigma_i = \lfloor x_i / N_i \rfloor$, $\sigma_i \equiv x_i^{d_i} \pmod{N_i}$. To guarantee soundness, U_i produces a proof that the discrete log of x_i^2 to the base $\hat{x} = x^{4\Delta}$ equals to the discrete log of v_i to base v. Specifically, U_i chooses a random $r \in \{0, \ldots, 2^{|N_0|+2L_1} - 1\}$, where L_1 is a secondary security parameter, and a secure hash function $H'(\cdot)$, then computes $v' = v^r, x' = \hat{x}^r, c_i = H'(v, \hat{x}, v_i, x_i^2, v', x'), z_i = k_i c + r$. The final partial proxy signature due to U_i is $(i, \Delta\sigma_i, \sigma_i, c_i, z_i)$.

Proxy signature combining: The combiner C can be one of the proxy signers or a secretary who does not possess any secret parameter. Upon receiving the partial proxy signature $(i, \Delta\sigma_i, \sigma_i, c_i, z_i)$ from U_i, C computes $x_i = \Delta\sigma_i \times N_i + (\sigma_i^{e_i} \pmod{N_i})$ and then checks if

$$c = H'\left(v, \hat{x}, v_i, x_i^2, v^z v_i^{-c}, \hat{x}^z x_i^{-2c}\right).$$

If the equation holds, the partial proxy signature is valid; Otherwise, invalid.

Assume t partial proxy signatures are valid and without losing generality, the corresponding proxy signers set is $s = \{1, \ldots, t\} \subset \{1, \ldots, n\}$. The proxy signature w of the message m under the warrant m_w is $w = x_1^{2\lambda_{0,1}^S} \cdots x_t^{2\lambda_{0,t}^S} \pmod{N_0}$, where $\lambda_{i,j}^S = \Delta \frac{\prod_{j' \in Sj}(i - j')}{\prod_{j' \in Sj}(j - j')}$.

Since $w^{e_0} \equiv x^{4\Delta^2 \cdot H(m_w)} \pmod{N_0}$ and $\gcd(4\Delta^2, e_0) = 1$, it is easy to find out the final proxy signature y such that $y^{e_0} \equiv x^{H(m_w)} \pmod{N_0}$ by using a standard algorithm $y = w^a x^b$,[1] where a, b are integers such that $4\Delta^2 a + e_0 b = 1$.

[1] This is a typo in [16], and the correct one is $y = w^a x^{bH(m_w)}$.