INFORMATICA, 2007, Vol. 18, No. 1, 55–60

On the Proxy-Protected Property of Chen *et al.'s* Proxy Multisignature Schemes

Pei-Hui HUANG[1], Hsiang-An WEN[2], Chih-Hung WANG[3], Tzonelih HWANG[1]

[1]*Department of Computer Science and Information Engineering*
National Cheng Kung University Tainan, Taiwan, R.O.C.
e-mail: pehui@ismail.csie.ncku.edu.tw, hwangtl@ismail.csie.ncku.edu.tw
[2]*Department of Computer Science and Information Engineering*
Leader University Tainan, Taiwan, R.O.C.
e-mail: reinhard@ismail.csie.ncku.edu.tw
[3]*Department of Computer Science and Information Engineering*
National Chiayi University Chiayi, Taiwan, R.O.C.
e-mail: wangch@mail.ncyu.edu.tw

Received: March 2005

Abstract. Recently, Chen, Chung, and Huang proposed a traceable proxy multisignature scheme based on the elliptic curve cryptosystem. However, this paper shows that the original signers can produce a valid signature as the proxy signer does in the proxy protected scheme. Therefore, Chen *et al.'s* proxy-protected scheme cannot protect the proxy signer from being forged by the original signers. We further find that the early work of Chen *et al.* in 2003 suffers the same attack. To overcome this problem, an improved scheme will be presented.

Key words: proxy signature, proxy multisignature, proxy-protected, elliptic curve, digital signature.

1. Introduction

The proxy signature is a kind of signature which allows one party, named original signer, to delegate his signing capability to a designated party, named proxy signer. The proxy signer can sign messages on behalf of the original signer. The concept of proxy signature was first introduced by Mambo *et al.* (Mambo *et al.*, 1996) in 1996. In such a scheme, the original signer can delegate his/her signing capability to a proxy signer. There are three types of delegation: full delegation, partial delegation, and delegation by warrant. In full delegation, the original signer gives his/her private key to the proxy signer to sign messages. There is no difference between the signatures made by the original signer and the proxy signer. In partial delegation, although the proxy signing key is derived from the original signer's private key, it is infeasible to deduce the original signer's private key from the proxy key. In the case of delegation by warrant, the original signer signs a warrant to certify the fact of delegation. According to the original signer who can produce a valid signature or not, the proxy signature scheme can further be divided into two types.

If the original signer can generate a signature as the proxy signer signs, the scheme is called proxy-unprotected proxy signature scheme. Otherwise, it is called proxy-protected proxy signature scheme.

In contrast with the one-to-one scheme proposed by Mambo *et al.*, the concept of proxy multisignature was introduced by Yi, Bai, and Xiao (Yi *et al.*, 2000). In the Yi *et al.'s* scheme, two or more original signers can delegate a single proxy signer to sign messages. Unfortunately, Sun (Sun, 2000) showed that the scheme would suffer a public key substitution attack. That is, the original signer can forge a valid signature by using a new public key to replace the original one. Hence, Sun proposed a proxy signature scheme to avoid this attack. In order to reduce the computational overhead of Sun's scheme, Chen, Chung, and Huang (Chen *et al.*, 2003) proposed two improved schemes based on elliptic curve cryptosystem. The first is a proxy-unprotected scheme and the second is a proxy-protected scheme. Further, Chen, Chung, and Huang (Chen *et al.*, 2004) used the similar concept to design a traceable proxy multisignature scheme based on the elliptic curve cryptosystem. However, this paper shows that both schemes proposed by Chen *et al.* (Chen *et al.*, 2003; Chen *et al.*, 2004) cannot achieve the proxy-protected property. The original signers can cooperate to produce a valid proxy signature without proxy signer's assistance. An improved scheme is further proposed to solve this problem.

The rest of this paper is organized as follows. Section 2 reviews Chen *et al.'s* scheme. In Section 3, the weaknesses of Chen *et al.'s* scheme are illustrated. We give an improvement and discuss its security in Section 4. Finally, the conclusion of this paper is given in Section 5.

2. Review of Chen *et al.'s* Scheme

Chen *et al.* proposed a proxy-protected proxy multisignature scheme based on elliptic curve (Chen *et al.*, 2003) to improve the performance of Sun's scheme. Later, Chen *et al.* proposed a similar scheme with traceability (Chen *et al.*, 2004). However, both schemes do not satisfy the proxy-protected property. This section just reviews Chen *et al.'s* traceable proxy-protected scheme to explain the weakness in the proxy-protected property of both schemes.

2.1. *System Initialization and Key Generation Phase*

The used notation will be listed below.

1. F_p: a finite field, where p is a prime.
2. E: an elliptic curve $y = x^3 + ax + b$ over F_p, where $a, b \in F_p$ and $4a^3 + 27b^2 \neq 0$.
3. G: a finite point on $E(F_p)$ with prime order t.
4. h: $\{0,1\}^* \times F_p \times F_p \times F_p \rightarrow Z_t^*$, a public collision-resistant hash function.

For each $i \in [1, n]$, the original signer A_i has a private/public key pair d_{o_i}/Q_{o_i} certified by a trust authority, where $d_{o_i} \in Z_t^*$ and $Q_{o_i} = d_{o_i}G = (x_{o_i}, y_{o_i})$. The proxy signer also has the private/public key pair d_p/Q_p and $Q_p = d_pG = (x_p, y_p)$.

2.2. *Proxy Multisignature Generation and Verification Phase*

1. *Subproxy key generation:* For $i = 1, 2, \cdots, n$, each original signer A_i selects a random number $k_i \in Z_t^*$ and computes $R_i = k_i G = (x_{R_i}, y_{R_i})$. If $x_{R_i} = 0$, then he/she selects another k_i, otherwise broadcasts R_i to other original signers. After receiving all R_j, $1 \leqslant j \leqslant n$, $j \neq i$, from the other original signers, A_i computes $R = \sum_{i=1}^{n} R_i = (x_R, y_R)$ and $s_i = d_{o_i} \cdot h(M_w, x_{o_i}, x_p, x_R) - k_i \bmod t$, where M_w is a warrant that specifies the fact of delegation, the delegation period, and other information.
2. *Subproxy key delivery:* For $i = 1, 2, \cdots, n$, each original signer A_i sends (M_w, s_i) to the proxy signer via a public channel.
3. *Subproxy key verification:* The proxy signer computes $U_i = h(M_w, x_{o_i}, x_p, x_R) \cdot Q_{o_i} - s_i G = (x_{U_i}, y_{U_i})$, for $i = 1, 2, \cdots n$. If $x_{U_i} = x_{R_i}$, the proxy signer accepts s_i as a valid subproxy key, otherwise, he/she rejects it.
4. *Proxy key generation:* The proxy signer computes $d = d_p + \sum_{i=1}^{n} s_i$ as a valid proxy key.
5. *Signing by the proxy signer:* The proxy signer uses the signing function $Sign_d()$ with the proxy key d to generate a signature on the message m. Note that $Sign_d()$ can be any secure signature scheme based on elliptic curve such as (Pohlig and Hellman, 1978). The result of whole signature is $(m, Sign_d(m), R, M_w)$.
6. *Proxy multisignature verification:* The verifier computes the corresponding proxy public key $Q = Q_p + h(M_w, x_{o_1}, x_p, x_R) \cdot Q_{o_1} + \cdots + h(M_w, x_{o_n}, x_p, x_R) \cdot Q_{o_n} - R$ to verify the signature. The equation $Q_p + h(M_w, x_{o_1}, x_p, x_R) \cdot Q_{o_1} + \cdots + h(M_w, x_{o_n}, x_p, x_R) \cdot Q_{o_n} - R = dG$ holds if the signature $(m, Sign_d(m), R, M_w)$ is valid.

3. The Weakness of Chen *et al.'s* Proxy-Protected Scheme

In this section, we show that Chen *et al.'s* traceable proxy-protected scheme (Chen *et al.*, 2004) cannot resist the original signers' forgery attack. The original signers can cooperate to impersonate the proxy signer to sign a valid proxy signature. We can also apply the same attack to Chen *et al.'s* proxy-protected proxy multisignature proposed in (Chen *et al.*, 2003). The original signers perform this attack as follows:

1. Each original signer except a special one named A_ℓ follows the scheme mentioned above. A_ℓ randomly chooses k_ℓ and computes $R_\ell = k_\ell G + Q_p$, and then broadcasts R_ℓ. After receiving all R_j, $1 \leqslant j \leqslant n$, $j \neq \ell$, from the other original signers, A_ℓ computes $R = \sum_{i=1}^{n} R_i = (x_R, y_R)$ and $s_\ell = d_{o\ell} \cdot h(M_w, x_{o\ell}, x_p, x_R) - k_\ell \bmod t$. The other original signers A_i, for $1 \leqslant i \leqslant n$ and $i \neq \ell$ follow the scheme to compute $R = \sum_{i=1}^{n} R_i = (x_R, y_R)$ and $s_i = d_{o_i} \cdot h(M_w, x_{o_i}, x_p, x_R) - k_i \bmod t$.
2. The original signers can compute a signing key $d' = \sum_{i=1}^{n} s_i$ to generate a proxy signature $Sign_{d'}(m')$ on a forged message m'.

3. To verify the validity of a proxy signature, the verifier computes the proxy public key $Q' = Q_p + h(M_w, x_{o_1}, x_p, x_R) \cdot Q_{o_1} + \cdots + h(M_w, x_{o_n}, x_p, x_R) \cdot Q_{o_n} - R$. However,

$$\begin{aligned} Q' &= Q_p + h(M_w, x_{o_1}, x_p, x_R) \cdot Q_{o_1} + \cdots + h(M_w, x_{o_\ell}, x_p, x_R) \cdot Q_{o_\ell} \\ &\quad + \cdots + h(M_w, x_{o_n}, x_p, x_R) \cdot Q_{o_n} - R \\ &= Q_p + h(M_w, x_{o_1}, x_p, x_R) \cdot Q_{o_1} + \cdots + h(M_w, x_{o_\ell}, x_p, x_R) \cdot Q_{o_\ell} + \cdots \\ &\quad + h(M_w, x_{o_n}, x_p, x_R) \cdot Q_{o_n} - (R_1 + \cdots + k_\ell G + Q_p + \cdots + R_n) \\ &= h(M_w, x_{o_1}, x_p, x_R) \cdot Q_{o_1} + \cdots + h(M_w, x_{o_\ell}, x_p, x_R) \cdot Q_{o_\ell} \\ &\quad + \cdots + h(M_w, x_{o_n}, x_p, x_R) \cdot Q_{o_n} - (R_1 + \cdots + k_\ell G + \cdots + R_n) \\ &= \sum_{i=1}^{n} s_i G \\ &= d' G \end{aligned}$$

and the original signers know how to compute d'. Therefore, the signature $(m', Sign_{d'}(m'), R, M_w)$ is a valid signature.

4. The Modified Scheme and Security Analysis

In this section, we propose an improvement to the above mentioned Chen *et al.'s* scheme and show that the improvement achieves the proxy-protected property. The same idea can also be applied to remedying their another scheme in (Chen *et al.*, 2003).

4.1. *The Proposed Scheme*

All the steps are the same as the original scheme except the proxy key generation step and the proxy multisignature verification step. In the proxy key generation step, the proxy key is replaced by $d = d_p \cdot h_1(M_w, x_R) + \sum_{i=1}^{n} s_i$, where $h_1 : \{0,1\}^* \times F_p \rightarrow Z_t^*$ is a public collision-resistant hash function. In the proxy multisignature verification step, the verifier uses $Q = Q_p \cdot h_1(M_w, x_R) + h(M_w, x_{o_1}, x_p, x_R) \cdot Q_{o_1} + \cdots + h(M_w, x_{o_n}, x_p, x_R) \cdot Q_{o_n} - R$ to verify the signature.

4.2. *Security Analysis*

Chen *et al.* have shown that their scheme can prevent the substitution attack and satisfy all security requirements (Chen *et al.*, 2004). Our improvement is similar to Chen *et al.'s* scheme. The improvement does not change the basic operations made by the original signer's private key and the proxy signer's private key. Thus, the improved scheme can resist the substitution attack according to the proof in Chen *et al.'s* scheme.

In Section 3, we show that the original signers can cooperate to create a valid proxy signature without the proxy signer's authorization. It is because that the original signers choose a specific random number R_ℓ to eliminate Q_p. Our improvement replaces Q_p

with $Q_p \cdot h_1(M_w, x_R)$ to avoid the attack. Suppose that the original signer A_ℓ wants to use R_ℓ to eliminate $Q_p \cdot h_1(M_w, x_R)$, he/she must compute R_ℓ to get x_R before deciding $h_1(M_w, x_R)$. However, $h_1(M_w, x_R)$ cannot be decided in the first priority than R_ℓ. Since x_R is the x-coordinate, R_ℓ must be decided coinciding with x_R. Therefore, it is infeasible for original signers to create a valid proxy signature by the method that we mentioned above.

5. Conclusions

This paper pointed out that both of Chen *et al.'s* proxy-protected schemes (Chen *et al.*, 2003; Chen *et al.*, 2004) do not achieve the proxy-protected property. That is, the original signers can cooperate to generate a valid proxy signature. Essentially, it is unfair for the proxy signer to take the responsibility on the malicious behavior of the original signers. To overcome this weakness, we have proposed an improved scheme and shown that it satisfies the proxy-protected property.

Acknowledgement

This research was partially supported by the National Science Council of Republic of China (R.O.C.), under contract No.: NSC 93-2213-E-006-104.

References

Chen, T.S., Y.F. Chung and K.H. Huang (2004). A traceable proxy multisignature scheme based on the elliptic curve cryptosystem. *Applied Mathematics and Computation*, **159**(1), 137–145.

Chen, T.S., Y.F. Chung and G.S. Huang (2003). Efficient proxy multisignature schemes based on the elliptic curve cryptosystem. *Computer & Security*, **22**(6), 527–534.

Mambo, M., K. Usuda and E. Okamoto (1996). Proxy signature: delegation of the power to sign messages. *ICICE Trans. Fundamentals*, **E79-A**(9), pp. 1338–1353.

Pohlig, S., and M. Hellman (1978). An improved algorithm for computing logarithms over GF(p) and its cryptographic significance. *IEEE Trans. on Information Theory*, **24**(1), 106–110.

Sun, H.M. (2000). On proxy multisignature scheme. *Proceedings of the International Computer Symposium*, 65–72.

Yi, L., G. Bai and G. Xiao (2000). Proxy multisignature scheme: A new type of proxy signature signature scheme. *Electronics Letters*, **36**(6), 527–528.

P.-H. Huang was born in Taipei Taiwan, in 1980. He received his BS degree in applied mathematics from Fu Jen Catholic University in 2003. He is currently pursuing his MS degree in Department of Computer Science and Information Engineering, National Cheng Kung University. His research interests include cryptography and information security.

H.-A. Wen was born in Taipei Taiwan, in 1976. He received his BE degree in Department of Mathematics from National Cheng Kung University in 1998, and PhD degree in Department of Computer Science and Information Engineering from National Cheng Kung University in 2005. He is presently an assistant professor of Department of Computer Science and Information Engineering, Leader University. His research interests include cryptography and information security.

C.-H. Wang was born in Kaohsiung Taiwan, in 1968. He received his BS degree in information science from Tunghi University and MS degree in information engineering from National Chung-Cheng University, Taiwan, R.O.C., in 1991 and 1993, respectively. He received the PhD degree in information engineering from National Cheng Kung University, Taiwan, R.O.C. in 1998. He is presently an assistant professor of Department of Computer and Information Engineering, Nation Chiayi University, Taiwan, R.O.C. His research interests include cryptography, information security and data compression.

T. Hwang was born in Tainan Taiwan, in 1958. He received his undergraduate degree in National Cheng Kung University in 1980, and the MS and PhD degrees in computer science from the University of Southwestern, Louisiana, USA, in 1988. He is presently a professor of Department of Computer and Information Engineering, Nation Cheng Kung University. His research interests include cryptology, network security and coding theory. Dr. Hwang is a member of IEEE and of the International Association for Cryptographic Research.

Apie pavaduojančiojo-apsaugotumą Chen ir kitų pavaduojančiojo daugiaparašinėse schemose

Pei-Hui HUANG, Hsiang-An WEN, Chih-Hung WANG, Tzonelih HWANG

Neseniai Chen, Chung ir Huang pasiūlė susekamą pavaduojančiojo daugiaparašinę schemą, pagrįstą elipsinės kreivės kriptosistema. Tačiau šis straipsnis parodo, kad originalūs pasirašantys asmenys gali pateikti galiojantį parašą kaip pavaduojantysis pasirašantis asmuo pateikia pavaduojančiojo apsaugotoje schemoje. Dėl to Chen ir kitų pavaduojančiojo-apsaugota schema negali apsaugoti pavaduojančiojo pasirašančio asmens nuo originalių pasirašančių asmenų falsifikavimo. Ankstesnis Chen ir kitų darbas, skelbtas 2003, taip pat neatsparus šiai atakai. Straipsnyje pristatoma pagerinta schema šios problemos išvengimui.