Journal of Zhejiang University-SCIENCE C (Computers & Electronics)
ISSN 1869-1951 (Print); ISSN 1869-196X (Online)
www.zju.edu.cn/jzus; www.springerlink.com
E-mail: jzus@zju.edu.cn

A novel multisignature scheme for a special verifier group against clerk and rogue-key attacks*

Jia-lun TSAI†1, Tzong-chen WU[1,2], Kuo-yu TSAI[1]

([1]*Department of Information Management, National Taiwan University of Science and Technology, Taiwan 106, Taipei*)

([2]*Taiwan Information Security Center, National Taiwan University of Science and Technology, Taiwan 106, Taipei*)

†E-mail: crousekimo@yahoo.com.tw

Received July 25, 2009; Revision accepted Nov. 23, 2009; Crosschecked Mar. 1, 2010

Abstract: The digital signature is a very important subject for network security. Considering multiple signers and multiple verifiers, Xie and Yu (2004) pointed out that the multisignature scheme of Laih and Yen (1996) is vulnerable to a harmful attack. An attack can occur when a specified group of verifiers cooperate to forge a multisignature by secret key substitution following the leak of a secret key or by group public key adjustment during the process of renewing membership. Xie and Yu proposed an improvement of Laih and Yen's multisignature scheme. In this paper, we show that Xie and Yu's scheme is vulnerable to clerk and rogue-key attacks. We propose an improved multisignature scheme to resist such attacks. In the proposed scheme, multiple signers can generate a multisignature for the message with the signers' secret keys, and the specified group of verifiers can cooperate to verify the validity of the multisignature with the signers' public keys and the verifiers' secret key. The proposed scheme for a special verifier group not only has the advantages of Xie and Yu's scheme, but also is secure against clerk and rogue-key attacks.

Key words: Multisignature, Clerk attack, Rogue-key attack, Cryptosystem
doi:10.1631/jzus.C0910457 **Document code:** A **CLC number:** TP309

1 Introduction

The digital signature is an important aspect of cryptography. It is usually used for authentication, data integrity, and non-repudiation. Digital signature schemes are generally based on complex mathematical problems, such as elliptic curve cryptography (ECC) (Miller, 1985; Koblitz, 1987), RSA (Rivest *et al.*, 1978), and ElGamal (Elgamal, 1985). Various types of signature schemes have been proposed (Mambo *et al.*, 1996; Lin *et al.*, 2002; Hsu *et al.*, 2004; Adam *et al.*, 2009; Du and Wen, 2009; Wu *et al.*, 2009).

Itakura and Nakamura (1983) first proposed a multisignature scheme. In their scheme, multiple signers can cooperate to sign the same message, which is chosen by them. Then, a verifier can verify the validity of the multisignature. The size of the multisignature is independent of the number of signers.

Laih and Yen (1996) first introduced the concept of a multisignature scheme for a specified group of verifiers. The main advantage of their scheme is that only the specified group of verifiers has the ability to verify the validity of the multisignature by using their secret keys. Later, Hwang and Yeh (1998) proposed an improved version of Laih and Yen's scheme. Unfortunately, He (2002) showed that both these schemes are vulnerable to a clerk attack. Without the help of other verifiers, the clerk of a specified group of verifiers could alone verify the validity of a multisignature. Hence, both schemes are insecure.

Xie and Yu (2004) demonstrated a new attack on Laih and Yen's multisignature scheme. In this attack, a verifier group can cooperate to forge a

* Project supported in part by the National Science Council (Nos. NSC 97-2745-P-001-001-, NSC 98-2219-E-011-001-, NSC 98-2221-E-011-073-MY3, and NSC 98-2218-E-011-018-)

multisignature by secret key substitution using a leaked secret key or by the group public key adjustment during the process of renewing membership. Xie and Yu proposed an improved scheme that could overcome the weakness of Laih and Yen's multisignature scheme. Since then, numerous extended signature schemes for specified verifier groups have been proposed (Tzeng *et al.*, 2004; Bao *et al.*, 2005; Hsu *et al.*, 2007; Lu *et al.*, 2008; Kang *et al.*, 2009).

In this paper, we present a clerk attack and a rogue-key attack (Boldyreva, 2003; Lu *et al.*, 2006; Ristenpart and Yilek, 2007; Shim, 2008; Wang *et al.*, 2008) on Xie and Yu's scheme. In the clerk attack, the clerk of the signers can cheat other partners to generate the multisignature for any message chosen by the clerk, instead of the original message to be signed. The signers and the verifiers cannot discover that the generated multisignature is a fake multisignature. In the rogue-key attack, a malicious signer in the signer group chooses a public key arbitrarily and attempts to forge the multisignature for his chosen message without knowledge of other signers' secret keys. To overcome these weaknesses, we propose an improvement to Xie and Yu's scheme. We show that the proposed multisignature scheme for a special group verifiers is secure against clerk and rogue-key attacks.

2 Review of Xie and Yu's multisignature scheme

Xie and Yu's multisignature scheme consists of three phases: system initialization, multisignature generation, and multisignature verification. Details of each phase are described as follows.

2.1 System initialization phase

Initially, a trusted center chooses a large prime p, a large prime divisor q of $p-1$, an element g in Z_p of order q, and a one-way hash function $H(\cdot)$. These are then published as the public parameters.

Let $G_s=\{U_{s_1}, U_{s_2}, \cdots, U_{s_n}\}$ be the signer group of n signers and $G_v=\{U_{v_1}, U_{v_2}, \cdots, U_{v_m}\}$ be the verifier group of m verifiers. In G_s and G_v, each of them has a special user, called the 'clerk'. Each $U_{s_i}\in G_s$ chooses his secret key $s_i\in Z_q^*$ and computes his public key $Y_{s_i}=g^{-s_i} \bmod p$. In the same way, each $U_{v_j}\in G_v$ chooses $v_j\in Z_q^*$ as his secret key and then computes $Y_{v_j}=g^{-v_j} \bmod p$ as his public key. G_s's public key $Y_s=\prod_{i=1}^{n} g^{-s_i} \bmod p$ and G_v's public key $Y_v=\prod_{j=1}^{m} g^{-v_j} \bmod p$ are then published.

2.2 Multisignature generation phase

Assume that a message M is the intended context to be signed. All signers in G_s cooperate to generate the multisignature (r, w) of message M for the specified group G_v of verifiers as follows:

Step 1: Each U_{s_i} chooses a random number $k_i\in_R Z_q$, and then computes $r_i=g^{k_i} \bmod p$ and $r_i'=Y_v^{k_i} \bmod p$. Finally, (r_i, r_i') is sent to a clerk of the signer's group U_{s_c}.

Step 2: The clerk U_{s_c} computes $r=\prod_{i=1}^{n} r_i \bmod p$, and $r'=\prod_{i=1}^{n} r_i' \bmod p$. Then, U_{s_c} broadcasts (r, r') to all signers.

Step 3: Each signer $U_{s_i}\in U_s$ computes $w_i=\left(r+h(r', M)\right)k_i+s_i \bmod q$. Next, $U_{s_i}\in U_s$ sends w_i to the clerk U_{s_c}.

Step 4: Upon receiving w_i from $U_{s_i}\in U_s$ the clerk U_{s_c} verifies the validity of each signer's partial signature: $Y_{s_i} g^{w_i}=r_i^{r+h(r', M)} (\bmod p)$, where $i=1, 2, \ldots, n$.

If all the partial signatures are valid, U_{s_c} computes part of the multisignature $w=\sum_{i=1}^{n} w_i \bmod q$. Finally, U_{s_c} sends the multisignature (r, w) to G_v.

2.3 Multisignature verification phase

Upon receiving the multisignature (r, w), each $U_{v_i}\in U_v$ computes $X_j=r^{-v_j} \bmod p$, and sends X_j to the clerk U_{v_c} of the verifier group. The clerk U_{v_c} computes $X=\prod_{j=1}^{m} X_j$, and then broadcasts X to other verifiers. Finally, each $U_{v_j}\in U_v$ verifies the validity of the multisignature (r, w) for message M by the following equality:

$$Y_s g^w = r^{r+h(X, M)} \bmod p.$$

3 Cryptanalysis of Xie and Yu's scheme

In this section, we show that Xie and Yu's scheme is vulnerable to clerk and rogue-key attacks.

3.1 A clerk attack on Xie and Yu's scheme

Suppose that a malicious clerk attempts to cheat other partners to sign a message M' chosen by the malicious clerk, instead of the original message M. In the multisignature generation phase, the malicious clerk takes the following steps:

Step 1: When the clerk U_{s_c} receives all the r_i and r_i', the clerk U_{s_c} computes $r=\prod_{i=1}^{n} r_i \bmod p$, $r'=\prod_{i=1}^{n} r_i' \bmod p$, and $\bar{r}=r+h(r',M')-h(r',M) \bmod p$. Finally, $\bar{r}$ and r' are broadcasted to all signers.

Step 2: Each signer $U_{s_i} \in U_s$ computes

$$\bar{w}_i=(\bar{r}+h(r',M))k_i+s_i(\bmod q). \tag{1}$$

Finally, $\bar{w}_i$ is sent to U_{s_c}.

Analysis According to Eq. (1), we can obtain

$$\begin{aligned}\bar{w}_i&=(\bar{r}+h(r',M))k_i+s_i(\bmod q)\\&=(r+h(r',M')-h(r',M)+h(r',M))k_i+s_i(\bmod q)\\&=(r+h(r',M'))k_i+s_i(\bmod q).\end{aligned}$$

Signers in G_s are unaware that the message M has been replaced with the message M'.

The malicious clerk can obtain a valid part of the multisignature $\bar{w}=\sum_{i=1}^{n}\bar{w}_i \bmod q$, and sends the multisignature $(r,\bar{w})$ of the message M' to G_v.

Upon receiving the multisignature $(r,\bar{w})$, each $U_{v_j} \in U_v$ computes $X_j=r^{-v_j} \bmod p$, and sends X_j to the clerk U_{v_c}. The clerk U_{v_c} computes $X=\prod_{j=1}^{m} X_j$, and then sends X to all verifiers. Each $U_{v_j} \in U_v$ verifies the validity of the multisignature $(r,\bar{w})$ by checking $Y_s g^{\bar{w}}=r^{r+h(X,M')} \bmod p$.

Clearly, the verifiers in G_v cannot find out that the multisignature (r, w) of the message M has been replaced with the multisignature $(r, \bar{w})$ of the message M'.

3.2 A rogue-key attack on Xie and Yu's scheme

Suppose that an adversary E wants to forge a multisignature for his chosen message M'. The rogue-key attack is performed as follows:

Step 1: E chooses a random integer $t \in Z_q^*$ as his secret key and computes $Y_{s_E}=g^{-t}-\prod_{i=1}^{n} g^{-s_i} \bmod p$ as his public key. Then, E joins the G_s, so the G_s's public key $Y_s=\prod_{i=1}^{n} g^{-s_i} \bmod p$ is turned into $\overline{Y_s}=g^{-t} \bmod p$.

Step 2: To forge G_s's multisignature for the verifier group, E chooses a random integer k and computes $\bar{r}=g^k \bmod p$, $\bar{r}'=Y_v{}^k \bmod p$, and $\bar{w}=(\bar{r}+h(\bar{r}',M'))k+t \bmod q$, where M' is chosen by E. Then, the forged multisignature $(\bar{r},\bar{w})$ of the message M' is sent to G_v.

Upon receiving the forged multisignature $(\bar{r},\bar{w})$, each $U_{v_j} \in U_v$ computes $X_j=r^{-v_j} \bmod p$, and sends X_j to the clerk U_{v_c}. The clerk U_{v_c} computes $X=\prod_{j=1}^{m} X_j$, and then sends X to all verifiers. Each $U_{v_j} \in U_v$ verifies the validity of the multisignature $(\bar{r},\bar{w})$ by checking $\overline{Y_s} g^{\bar{w}}=\bar{r}^{\bar{r}+h(X,M')} \bmod p$.

Clearly, all verifiers in G_v cannot be aware that the multisignature $(\bar{r},\bar{w})$ of the message M' is forged by E.

4 Our proposed scheme

Our proposed scheme also consists of three phases: system initialization, multisignature generation, and multisignature verification. The difference between the system initialization phase of our proposed scheme and that of Xie and Yi's scheme is that we adopt the proofs of possession (POP) key registration protocol (Boldyreva, 2003; Lu *et al.*, 2006; Ristenpart and Yilek, 2007; Shim, 2008; Wang *et al.*, 2008) to resist the rogue-key attack. In this protocol, each signer (or verifier) has to prove possession of the secret key before computing the signer (or verifier) group key. Details of each phase are described as follows.

4.1 System initialization phase

All of the signers/verifiers have to prove possession of the secret key to a trusted center to join the signer group/verifier group. The processes for the signers and verifiers are the same, and hence we just describe the process for the signer.

Step 1: When each signer wants to join the G_s, $U_{s_i} \in G_s$ first chooses his secret key $s_i \in Z_q^*$ and corresponding public key $Y_{s_i} = g^{-s_i} \bmod p$.

Step 2: $U_{s_i} \in G_s$ chooses a random integer k_i, and computes $r_i = g^{k_i} \bmod p$, $c_i = h(r_i, m_{U_i}) \bmod p$, $w_i = k_i + c_i s_i$, where m_{U_i} is the message consisting of some personal information and Y_{s_i}.

Step 3: $(Y_{s_i}, c_i, w_i, m_{U_i})$ is sent to the trusted center. Upon receiving $(Y_{s_i}, c_i, w_i, m_{U_i})$, the trusted center computes $r_i = g^{w_i} Y_{s_i}^{c_i} \bmod p$, and then checks whether c_i is the same as $h(r_i, m_{U_i})$. If it holds, the trusted center computes and publishes G_s's public key $Y_s = \prod_{i=1}^{n} g^{-s_i} \bmod p$.

4.2 Multisignature generation phase

Assume that M is the message to be signed. All signers in G_s cooperate to generate the multisignature for a specified group G_v of verifiers. They perform the following steps:

Step 1: Each $U_{s_i} \in U_s$ randomly chooses $k_i \in_R Z_q$ and computes $r_i = g^{k_i} \bmod p$ and $r_i' = Y_v^{k_i} \bmod p$. Finally, $U_{s_i} \in U_s$ sends (r_i, r_i') to the clerk of the signer group U_{s_c}.

Step 2: The clerk U_{s_c} computes $r = \prod_{i=1}^{n} r_i \bmod p$ and $r' = \prod_{i=1}^{n} r_i' \bmod p$, and broadcasts (r, r') to all signers in G_s.

Step 3: Each $U_{s_i} \in U_s$ computes

$$w_i = h(r, M) k_i - h(r', M) s_i \pmod q, \tag{2}$$

and then sends w_i to the clerk U_{s_c}.

Step 4: Upon receiving w_i from $U_{s_i} \in U_s$, the clerk U_{s_c} verifies each signer's individual signature (r_i, r, r', w_i) by computing

$$g^{w_i} = Y_{s_i}^{h(r', M)} r_i^{h(r, M)} \pmod p, \tag{3}$$

where i=1, 2, …., n.

If it holds, the clerk U_{s_c} computes $w = \sum_{i=1}^{n} w_i \bmod q$. Finally, U_{s_c} sends the multisignature (r, w) to all the verifiers.

The correctness of Eq. (3) is shown as follows:

$$g^{w_i} = \begin{cases} g^{h(r,M)k_i - h(r',M)s_i}, & \text{according to Eq. (2),} \\ Y_{s_i}^{h(r',M)} r_i^{h(r,M)}, & \text{according to } (Y_{s_i}, r_i'). \end{cases}$$

4.3 Multisignature verification phase

Upon receiving the multisignature (r, w), each $U_{v_j} \in U_v$ computes $X_j = r^{-v_j} \bmod p$ and then sends X_j to the clerk U_{v_c}. The clerk U_{v_c} computes $X = \prod_{j=1}^{m} X_j$ and then sends the computed X to all verifiers. Then, each $U_{v_j} \in U_v$ verifies the validity of the multisignature by checking

$$g^{w} = Y_s^{h(X,M)} r^{h(r,M)} \bmod p. \tag{4}$$

We show the correctness of Eq. (4) as follows:

$$g^{w} = \begin{cases} g^{\sum h(r,M)k_i} g^{-\sum h(r',M)s_i}, & \text{according to} \\ \quad w = \sum h(r, M) k_i - h(r', M) s_i, & \\ Y_s^{h(X,M)} r^{h(r,M)} \bmod p, & \text{according to} \\ \quad r = \prod g^{k_i}, Y_s = \prod g^{s_i}, \text{and } r' = \prod Y_v^{k_i} = X. & \end{cases}$$

5 Security analysis of the proposed scheme

A multisignature scheme for a specified group should be unforgeable and withstand the clerk and rogue-key attacks. The security of the proposed scheme is based on the one-way hash function and solving the discrete logarithm problem, described as follows:

Assumption 1 One-way hash function (OWHF): (1) Given $y=h(x)$, it is computationally infeasible to derive x from $h(x)$. (2) It is difficult to find two x and x' such that $h(x)=h(x')$.

Assumption 2 Discrete logarithms problem (DLP): Given $y=g^x \bmod p$, it is computationally infeasible to derive x from y.

Under the DLP and OWHF assumptions, we discuss the security considerations of the multisignature scheme for a special verifier group.

Theorem 1 In the proposed multisignature scheme for a specified group, any adversary cannot reveal the signer's (or verifier's) secret key from the signer's (or verifier's) public key.

Proof In the proposed multisignature scheme for a specified group, any adversary cannot know the secret key $s_i \in Z_q^*$ (or $v_j \in Z_q^*$) of any signer U_{s_i} or verifier U_{v_j} from its corresponding public key $Y_{s_i} = g^{-s_i} \bmod p$ (or $Y_{v_j} = g^{-v_j} \bmod p$). It is computationally infeasible for the adversary under the DLP.

Theorem 2 The proposed multisignature scheme for a specified group achieves rogue-key attack.

Proof The proposed multisignature scheme for a specified group takes the POP assumption. Each signer (or verifier) is required to prove possession of the secret key before the signer's (or verifier's) public key and group key are computed. Hence, the proposed scheme is secure against the rogue-key attack.

Theorem 3 The proposed multisignature scheme for a specified group can resist the clerk attack.

Proof The clerk attack is workable in Xie and Yu's scheme, since the malicious clerk U_{s_c} replaces the r with $\overline{r}$ and broadcasts $\overline{r}$ to each signer. The replaced $\overline{r}$ then modifies each signer's partial signature w_i, so the malicious clerk can obtain the multisignature $(\overline{r}, \overline{w})$ for his chosen message M'. However, it cannot work successfully in our proposed scheme. Checking Eq. (2):

$$w_i = h(r, M)k_i - h(r', M)s_i \pmod q.$$

Under the OWHF assumption, it is computationally unfeasible for any adversary to compute r to replace the message M with the message M', because r, r', and the message M are protected by the one-way hash function.

Theorem 4 In the proposed multisignature scheme for a specified group, the clerk of the verifier group cannot verify the validity of the multisignature without other verifiers.

Proof According to Eq. (3), we find that the clerk U_{v_c} needs to have each signer's secret key v_j to compute X_i, if the clerk U_{v_c} wants to verify the validity of the multisignature (r, w) alone. However, we have shown that it is computationally infeasible to solve the discrete logarithm to obtain the verifier's secret key v_j. Hence, in the proposed scheme, the clerk U_{v_c} alone cannot verify the validity of the multisignature (r, w).

Theorem 5 In the proposed multisignature scheme for a specified group, even though verifiers in the verifier group obtain a multisignature, they still cannot forge the multisignature for any message chosen by themselves.

Proof In the proposed multisignature scheme for a specified group, the multisignature $\sum_{i=1}^{n} w_i = \sum_{i=1}^{n} h(r, M)k_i - h(r', M)s_i \pmod q$ consists of r, r', the random numbers k_i and the signers' secret key s_i. k_i and s_i are held only by the signers. We have also shown in Theorem 1 that it is infeasible for any adversary to reveal s_i from the signer's public key $Y_{s_i} = g^{-s_i} \bmod p$. The verifier group, without knowing the signers' secret key s_i, can first try to determine $(r, Y_s = \prod_{i=1}^{n} g^{-s_i} \bmod p)$ and attempt to obtain w from $g^w = Y_s^{h(X, M)} r^{h(r, M)} \bmod p$. They cannot carry out the attack successfully, since it is infeasible to solve DLP. Hence, the proposed scheme can withstand the forgery attack.

6 Conclusion

This paper shows that Xie and Yu's scheme is vulnerable to clerk and rogue-key attacks. To overcome this weakness, we propose an improved multisignature scheme for a special verifier group. The proposed scheme has all the advantages of Xie and Yu's scheme and can withstand the clerk and rogue-key attacks. Further work is needed to apply

multiparty computation to substitute the functionality of the clerk.

References

Adam, B., Jonathan, K., Ruggero, M., 2009. Ring signatures: stronger definitions, and constructions without random oracles. *J. Cryptol.*, **22**(1):114-138. [doi:10.1007/s00145-007-9011-9]

Bao, H.Y., Cao, Z.F., Wang, S.B., 2005. Improvement on Tzeng *et al.*'s nonrepudiable threshold multi-proxy multi-signature scheme with shared verification. *Appl. Math. Comput.*, **169**(2):1419-1430. [doi:10.1016/j.amc.2004.10.075]

Boldyreva, A., 2003. Threshold Signatures, Multisignatures and Blind Signatures Based on the Gap-Diffie-Hellman-Group Signature Scheme. Public Key Cryptography, p.31-46.

Du, H., Wen, Q., 2009. Efficient and provably-secure certificateless short signature scheme from bilinear pairings. *Comput. Stand. Interfaces*, **31**(2):390-394. [doi:10.1016/j.csi.2008.05.013]

Elgamal, T., 1985. A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Trans. Inform. Theory*, **31**(4):469-472. [doi:10.1109/TIT.1985.1057074]

He, W.H., 2002. Weakness in some multisignature for specified group of verifiers. *Inform. Process. Lett.*, **83**(2):95-99. [doi:10.1016/S0020-0190(01)00317-9]

Hsu, C.L., Wu, T.S., Wu, T.C., 2004. Group-oriented signature scheme with distinguished signing authorities. *Future Gener. Comput. Syst.*, **20**(5):865-873. [doi:10.1016/j.future.2003.11.013]

Hsu, C.L., Tsai, K.Y., Tsai, P.L., 2007. Cryptanalysis and improvement of nonrepudiable threshold multi-proxy multi-signature scheme with shared verification. *Inform. Sci.*, **177**(2):543-549. [doi:10.1016/j.ins.2006.04.004]

Hwang, S.J., Yeh, S.M., 1998. An encryption/multisignature scheme with specified receiving groups. *Comput. Syst. Sci. Eng.*, **13**(2):109-112.

Itakura, K., Nakamura, K., 1983. A public-key cryptosystem suitable for digital multisignatures. *NEC Res. Dev.*, **71**:1-8.

Kang, B., Boyd, C., Dawson, E., 2009. A novel nonrepudiable threshold multi-proxy multi-signature scheme with shared verification. *Comput. Electr. Eng.*, **35**(1):9-17. [doi:10.1016/j.compeleceng.2008.04.001]

Koblitz, N., 1987. Elliptic curve cryptosystems. *Math. Comput.*, **48**(177):203-209. [doi:10.2307/2007884]

Laih, C.S., Yen, S.M., 1996. Multisignature for specified group of verifiers. *J. Inform. Sci. Eng.*, **12**(1):143-152.

Lin, C.Y., Wu, T.C., Hwang, J.J., 2002. Multi-Proxy Signature Schemes for Partial Delegation with Cheater Identification. 2nd Int. Workshop for Asia Public Key Infrastructure, p.147-152.

Lu, R., He, D., Wang, C., 2008. Security analysis and improvement of new threshold multi-proxy multi-signature scheme. *J. Electron. (China)*, **25**(3):372-377. [doi:10.1007/s11767-006-0186-2]

Lu, S., Ostrovsky, R., Sahai, A., Shacham, H., Waters, B., 2006. Sequential aggregate signatures and multisignatures without random oracles. *LNCS*, **4004**:465-485. [doi:10.1007/11761679]

Mambo, M., Usuda, K., Okamoto, E., 1996. Proxy Signature for Delegating Signing Operation. Proc. 3rd ACM Conf. on Computer and Communications Security, p.48-57. [doi:10.1145/238168.238185]

Miller, V., 1985. Use of Elliptic Curves in Cryptography. Advances in Cryptology, Springer-Verlag, Santa Barbara, California, USA, **218**:417-426.

Ristenpart, T., Yilek, S., 2007. The power of proofs-of-possession: security multiparty signature against rogue-key attacks. *LNCS*, **4515**:228-245. [doi:10.1007/978-3-540-72540-4]

Rivest, R.L., Shamir, A., Adelman, L., 1978. A method for obtaining digital signature and public key cryptosystem. *Commun. ACM*, **21**(2):120-126. [doi:10.1145/359340.359342]

Shim, K.A., 2008. Rogue-key attacks on the multi-designated verifiers signature scheme. *Inform. Process. Lett.*, **107**(2):83-86. [doi:10.1016/j.ipl.2007.11.021]

Tzeng, S.F., Yang, C.Y., Hwang, M.S., 2004. A nonrepudiable threshold multi-proxy multi-signature scheme with shared verification. *Future Gener. Comput. Syst.*, **20**(5):887-893. [doi:10.1016/j.future.2004.01.002]

Xie, Q., Yu, X.Y., 2004. Improvement of Laih and Yen's multisignature scheme. *J. Zhejiang Univ.-Sci.*, **5**(9):1155-1159. [doi:10.1631/jzus.2004.1155]

Wang, Z., Si, T., Qian, H., Li, Z., 2008. A CDH-Based Multi-Signature Scheme with Tight Security Reduction. 9th Int. Conf. for Yong Computer Scientists, p.2096-2101.

Wu, T.S., Hsu, C.L., Lin, H.Y., 2009. Self-certified multi-proxy signature schemes with message recovery. *J. Zhejiang Univ.-Sci. A*, **10**(2):290-300. [doi:10.1631/jzus.A0820202]