Comput Syst Sci & Eng (1998) 2: 109–112
© 1998 CRL Publishing Ltd

Computer Systems
Science & Engineering

An encryption/multisignature scheme with specified receiving groups

Shin-Jia Hwang*, Chien-Yuang Chen*, and Chin-Chen Chang†

**Institute of Computer and Information Science, National Chiao Tung University, Hsinchu, Taiwan 300, ROC. Email: hwangsj@winston.cis.nctu.edu.tw*
†Institute of Computer Science and Information Engineering, National Chung Cheng University, Chiayi, Taiwan 621, ROC. Email: ccc@cs.ccu.edu.tw

In this paper, we propose a new multisignature scheme that allows all of the signers to specify the recipients. The encryption function is also integrated into our multisignature scheme, thus the new soheme can provide secrecy, authenticity, and integrity services. Moreover, the message expansion is also reduced. Comparing to the proposed multisignature scheme, the new scheme is the first one which allows the singers to specify the recipients.

Keywords: data security, office automation, multisignature, public key cryptography

1. INTRODUCTION

Secrecy, authenticity, and integrity are the three major services provided by the public key cryptography. These services are important for the office automation. By the secrecy service, the digital documents are protected from unauthorized accesses. By the authenticity and integrity services, the electronic analogues of handwritten signatures are generated for the sensitive digital documents to point the ones with responsibility out. In addition, the authenticity and integrity services are important because the digital documents can be easily modified. The secrecy service is provided by public key cryptosystems while the other services are provided by digital signature schemes.

Since Diffie and Hellman[1] proposed the concepts of the public key cryptosystem and the digital signature scheme, many digital signature schemes were proposed[2-13]. In offices, though the digital signature schemes provide the authenticity and integrity services, there still exist some situations that the digital signature scheme cannot deal with.

Consider the situation that an office member always takes partial responsibility for a document. Thus, a document should sometime be signed cooperatively by several members in the office. If each member signs the document by a digital signature scheme, the number of signatures is equal to the number of signers. Then these signatures will waste a lot of computer storage. This is an inefficient way.

To overcome the above problem, Itakura and Nakamura[14] proposed the first digital multisignature scheme. In the multisignature scheme, the documents can be signed by many users and the size of the multisignature is fully independent on the number of the signers. However, the signing order is fixed in Itakura and Nakamura's scheme. In 1988, Okamoto proposed another multisignature scheme such that the signing order is not fixed; but the size of the multisignature may be enlarged for some signing orders.

Based on the RSA public key cryptosystem and the digital signature scheme, Harn and Kiesler[15] proposed the first multisignature scheme that also provides secrecy service. However, the order of the signer must be fixed in Harn and Kiesler's scheme. To remove the restriction of the fixed signing order, Kiesler and Harn[16] utilized the repeated exponentiation method to improve Harn and Kiesler's scheme. The above three multisignature schemes adopted the message recovery mode to design their schemes. By the message recovery mode, we mean the signed message can be recovered from the multisignature.

In addition, based on Fiat and Shamir's digital signature scheme[4], Ohta and Okamoto[17] and Boyd[18] proposed their multisignature schemes, respectively. Ohta and Okamoto's and Boyd's schemes adopted the comparison mode to design their multisignature schemes. The secrecy service is not token into consideration in both Ohta and Okamoto's and Boyd's schemes.

In 1994, Harn proposed the first multisignature scheme based on the discrete logarithm problem. In Harn's scheme, the multisignature can be easily generated by the cooperation of all signers. Therefore, Harn's scheme is efficient because the scheme provides an easy way to integrate all partial signatures into the multisignature. Although the signer needs the help of a clerk, the clerk may be untrusted. Thus any signer can be the clerk.

The common disadvantage of the proposed multisignature schemes is that the multisignature is easily transmitted from the original recipient to another one. The transmission among recipients is unreasonable, because the transmission may cause the damage on the benefit of the signers. For example, let us suppose the users A and B have their deposit accounts in a bank. The bank should give certificates to the users A and B, respectively. The certificates of the deposit should be signed by some clerks in the bank. If the user A finds that M is the individual message block representing the amount of money, then he can give the multisignature of M signed by clerks to the user B. Now the user B has a new certificate by replacing the old multisignature of the new multisignature. Then he has two deposit accounts in the same bank. In addition, it is also necessary to provide the secrecy service against unauthorized accesses. Therefore, a new encryption/multisignature scheme will be proposed to provide the secrecy service and the function to specify the recipient.

In the next section, the review of the encryption/signature scheme will be given. Then the new multisignature scheme will be presented in Section 3. The security analysis and some discussions are given in Section 4. Finally, the conclusions are given in Section 5.

2. REVIEW OF THE ENCRYPTION/ SIGNATURE SCHEME

Here we describe Hwang *et al.*'s encryption/signature scheme[13]. In the encryption/signature scheme, the trusted center publishes the following two system parameters:

P: A large prime such that P – 1 contains at least one large prime factor.
α: A primitive element of GF(P).

Then each legal user U_i randomly chooses his secret key x_i from $[1, P - 1]$ and sends his public key $y_i = \alpha^{x_i} \bmod P$ to the trusted center. The trusted center publishes the public keys to all of the legal users.

Suppose that a legal user U_i signs the message M and then only sends the signature to the user U_j, where $1 \leq M < P - 1$. First, User U_i randomly selects an integer k from $[1, P - 1]$ and computes $t'_1 = \alpha^{-k} \bmod P$ and $t_2 = (y_j)^k \bmod P$. Next, User U_i computes $r = M \times t'_1 \times (\alpha^{-t_2}) \bmod P$ and constructs the integer s such that $rx_i + s \equiv k \pmod{P - 1}$. Finally, the signature is the pair (r, s). Consequently, the signature (r, s) is also the ciphertext of the signed message M because the message M is hidden in r.

After receiving the signature pair (r, s), User U_j first computes $t_1 \equiv \alpha^s \times y_i^r \equiv \alpha^{rx_i+s} \equiv \alpha^k \pmod P$ and $t_2 \equiv (y_j)^k \equiv (t_1)^{x_j} \pmod P$. Then User U_j caiculates $M = r \times t_1 \times \alpha^{t_2} \bmod P$ to obtain the signed message M. If the message is meaningful, then User U_j is sure that M is signed and sent by the signer.

In the encryption/signature scheme, the recipient of the digital signature first uses the signer's public key to generate $t_1 = \alpha^k \bmod P$, and then the recipient uses his secret key to recover $t_2 \equiv (y_j)^k \equiv (t_1)^{x_j} \bmod P$; otherwise, the recipient cannot derive the signed message from the digital signature (or ciphertext). Because only the signer can use his secret key to generate the signature, he cannot deny that he had signed this message. On the other hand, the recipient should use his secret key to recover the message from the signature, so the signature is also the ciphertext of the signed message.

In the encryption/signature scheme, the recipient of the signature/ciphertext is specified by the signer. In the verification process, the signer can specify the qualified recipients of the signature. And each qualified recipient will use his secret key and the signer.s public key to recover the message from the signature. If the specified recipient transmits the signature to someone, say User A, then User A cannot show that this signature is generated for him since the secret key of User A is different from that of the specified recipient.

3. ENCRYPTION/MULTISIGNATURE SCHEME WITH SPECIFYING RECIPIENTS

In the new multisignature scheme, a trusted center publishes the following system parameters:

P: A large prime such that $P - 1$ contains at least one large prime factor.
Q: The largest prime factor of $P - 1$.
α: A generator of order Q in $GF(P)$.

The legal users are divided into many groups. In each group, there is a special user, clerk. The clerk of each group is responsible for generating the multisignature by merging the partial signatures from all the members of the same group, and for sending and receiving the multisignatures. The clerk should be trustworthy. The new scheme is divided into three phases: key generation phase, multisignature generation phase, and multisignature verification phase.

3.1 Key generation phase

In each group G_i, each member U_{ij} selects his own secret key x_{ij} from $[1, Q - 1]$ and all members of the same group share a common secret key X_i from $[1, Q - 1]$. Each member U_{ij} publishes his public keys $y_{ij} = \alpha^{x_{ij}} \bmod P$ and $Y_{ij} = \alpha^{X_i x_{ij}} \bmod P$. Then, there are three public keys of the groupG_i. One is $Y_i = \alpha^{X_i} \bmod P$, another is Y'_i, which is the product of all legal y_{ij}'s, and the other is Y''_i which is the product of all legal Y_{ij}'s.

3.2 Multisignature generation phase

Suppose that all of the members of the group G_i want to sign a message M and'send the multisignature to a special recipient. Assume that the public key of the recipient is Y and the secret key of the recipient is x, where $Y = \alpha^x \bmod P$. All the members of the group G_i execute the following steps to generate the multisignature for the recipient.

Step 1: The member U_{ij} of the group G_i selects a random integer r_j and then computes $\alpha^{r_j} \bmod P$ and $(Y)^{-r_j} \bmod P$. Then the member U_{ij} sends his package $\{\alpha^{r_j} \bmod P, (Y)^{-r_j} \bmod P\}$ to the clerk of G_i.

Step 2: The clerk verifies whether any two members. U_{ig} and U_{ih}, select the same random integer by checking $(Y)^{-r_h} \equiv (Y)^{-r_g} \pmod P$. If any two members select the same random integer, the clerk informs them to resend their new packages; otherwise, he broadcasts $\{(Y)^{-r_1} \bmod P, (Y)^{-r_2} \bmod P, \ldots, (Y)^{-r_n} \bmod P\}$ to the members in G_i, where n is the number of the members in G_i.

Step 3: The member U_{ij} of the group G_i computes $t_1 = (\prod_{j=1}^{n} (Y)^{-r_j}) \bmod P$ and $t_2 = (t_1^{-1})^{X_i} \bmod P$.

Step 4: The member U_{ij} computes $R = M \times t_1 \times (Y)^{(-t_2 \bmod Q)} \bmod P$ and $s_j = r_j - R \times x_{ij} \bmod Q$ for $j = 1, 2, \ldots, n$. Finally, the member U_{ij} sends s_j to the clerk.

Step 5: After receiving all partial signatures s_j's, the clerk verifies the correctness of s_j by $(y_{ij})^R \times \alpha^{s_j} \times \alpha^{r_j}$ mod P for $j = 1, 2, \ldots, n$. If all partial signatures are correct, then the clerk computes $S = s_1 + s_2 + \ldots + s_n \bmod Q$. and sends the signature pair (R, S) to the recipient.

3.3 Multisignature verification phase

The recipient executes the following steps to recover the message M and verifies the signature (R, S).

Step 1: The recipient first computes $(t_1^{-1}) = Y^S \times (Y'^R_i)^x \bmod P$ and $t_2 = (Y_i^S \times Y''^R_i)^x \bmod P$.

Step 2: The recipient obtains $M = R \times (t_1^{-1}) \times Y^{t_2} \bmod P$. If the recovered message is meaningful, then the recipient is sure that the message M is indeed sent and signed by the group G_i.

In the following theorem, we show why the recipient can recover the original message M and verify the multisignature pair (R, S).

Theorem 1

If the signing group follows the steps in multisignature generation phase, then the recipient can recover the signed message M correctly.

Proof

If the recipient has the ability to obtain (t_1^{-1}) and t_2, then he can reveal the original message M. The following shows that (t_1^{-1}) can be computed by the recipient.

$$(t_1^{-1}) \equiv Y^S \times (Y'^R_i)^x \equiv (\prod_{j=1}^{n} \alpha^{S_j})^x \times (\prod_{j=1}^{n} y_{ij}^R)^x$$
$$\equiv (\prod_{j=1}^{n} \alpha^{S_j} \times \alpha^{Rx_{ij}})^x \equiv (\prod_{j=1}^{n} Y^{r_j}) \equiv (\prod_{j=1}^{n} Y^{-r_j})^{-1} \pmod P$$

The following shows that t_2 can be obtained by the recipient:

$$(t_2) \equiv (Y_i^S \times Y''^R_i)^x \equiv (\prod_{j=1}^{n} \alpha^{X_i s_j})^x \times (\prod_{j=1}^{n} \alpha^{X_i x_{ij} R})^x$$
$$\equiv (\prod_{j=1}^{n} Y^{S_j} \times Y^{x_{ij} R})^x \equiv (\prod_{j=1}^{n} Y^{r_j})^{X_i}$$
$$\equiv ((\prod_{j=1}^{n} Y^{-r_j})^{-1})^{X_i} \equiv (t_1^{-1})^{X_i} \pmod P$$

Since both (t_1^{-1}) and t_2 are correct. then the recipient can derive the message M as follows:

$$M \equiv R \times (t_1^{-1}) \times Y^{t_2}$$
$$\equiv M \times t_1 \times (t_1^{-1}) \times (Y)^{(t_2 - t_2 \bmod Q)} \pmod P \qquad \square$$

In the above multisignature scheme, the recipient can be a single user or a whole group. If the recipient is a single user, then the public key Y is the public key of some single user. If the recipient is a legal member of the group G_k, then the public key Y is means the group,s public key Y_k of some group G_k. This is suitable for sending an urgent message to a group. Finally, if the public key Y is G_k's public key Y'_k, then this multisignature (R, S) can be decrypted and verified by the cooperation of all the members in G_k. The clerk in the group G_k is responsible for executing all the steps of the multisignature verification phase. The clerk first computes $Y'^R_i \bmod P$ and $(Y_i^S \times Y''^R_i) \bmod P$, and then sends the results to all members. Each member of G_k computes $(Y'^R_i)^{x_{kj}} \bmod P$ and $(Y_i^S \times Y''^R_i)^{x_{kj}} \bmod P$, and sends $(Y''^R_i)^{x_{kj}} \bmod P$ and $(Y_i^S \times Y''^R_i)^{x_{kj}} \bmod P$ back to the clerk. The clerk then computes $(t_1^{-1}) = \mathrm{Y}^{\mathrm{S}} \times \prod_{j=1}^{m} (Y'^R_i)^{x_{kj}} \bmod P$ and $t_2 = \prod_{j=1}^{m} (Y_i^S \times Y''^R_i)^{x_{kj}} \bmod P$, where m is the number of the members in G_k. Finally, the clerk can execute Step 2 in the multisignature verification phase to obtain the message and verify the multisiganture (R, S).

4. SECURITY ANALYSIS AND DISCUSSION

First, we analyse the security of the secret keys. To derive any secret key from the corresponding public key is equivalent to solving the discrete logarithm problem. A possible attack to derive the secret key is solving the equation $R \times x_{ij} + s_j \equiv r_j \pmod Q$. To derive the random integer r_j from $\alpha^{r_j} \bmod P$ or $(Y)^{-r_j} \bmod P$ is also equivalent to solving the discrete logarithm problem. Consequently, the number of unknown variables is greater than the number of equations $R \times x_{ij} + s_j \equiv r_j \pmod Q$ collected by the intruder. So this attack is not successful.

Next, we analyse the security of the multisignature. The first possible attack is whether the recipient forges the multisignature for some message M'. The recipient can compute R' when all random integers r'_j are selected by himself; however, he cannot construct each partial signature s'_j such that $R' \times x_{ij} + s'_j \equiv r'_j \pmod Q$, since he does not know the secret key x_{ij}. So, the recipient must solve the discrete logarithm problem to obtain s'_j from $\alpha^{s'_j} = \alpha^{r'_j} \times (y_{ij})^{-R'} \bmod P$. Similarly, if the clerk wants to forge the multisignature (R', S'), he also must to derive s'_j from $\alpha^{s'_j} = \alpha^{r'_j} \times (y_{ij})^{-R} \bmod P$. Therefore, it is hard to forge the multisignature (R', S') for some meaningful message M'.

Consider whether an intruder has the ability to derive the multisignature (R', S') for some known multisignature (R, S) for the message M. Because the relation among R and all r_j's are not linear, the intruder cannot construct (R', S') for M' by computing (M/M') or $(M - M')$. So this attack fails.

This multisignature scheme provides a special advantage that the multisignature (R, S) cannot be transferred from the original recipient to another. Because the public key of the recipient is used to compute R, only the recipient can decrypt and verify the multisignature (R, S). If the recipient wants to replace his public key by the public keys of the others, then the value of R should be changed. The recipient must construct S' for the new R'. Due to the above security analysis, it is hard for him to do this. Therefore, the multisignature (R, S) cannot be transferred to another.

Now we consider the security of the encryption function. To recover the original message, an intruder must remove t_1 and $(Y)^{(-t_2 \bmod Q)} \bmod P$ from R. Though anyone can compute t_1, the intruder cannot compute t_2 because he does not have the secret key of the recipient.

Finally, we consider the ratio of message expansion. The ratio of messages expansion is $(|R| + |S|)/|M| = (|P| + |Q|)/|P| \leq 2$, where $|W| = \log_2 W$ denotes the bit length of the integer W. According to the Digital Signature Algorithm (DSA) proposed by the National Institute of Standards and Technology (NIST), $511 < |P| < 512$ and $159 < |Q| < 160$. Thus, the ratio of messages expansion is $1 + (160/512) = 1.3125$, which is less than two. We see that the newly proposed scheme can reduce the communication cost and save storage used.

5. CONCLUSIONS

In this paper, we have proposed a new multisignature scheme by which the signers can specify the recipient or the receiving group. By our multisignature scheme, only the specified recipient has the ability to verify the multisignature. In the new scheme, the encryption is integrated into the multisignature scheme to provide the secrecy service, so the new scheme can provide the three major services of cryptography: secrecy, authenticity and integrity. Furthermore, the new scheme allows the multisignature to be verified by not only a single recipient, but also by a group of recipients.

ACKNOWLEDGEMENT

This research was partially supported by the Chung Shan Institute of Science and Technology under contract CS84-0210-D-194-001.

REFERENCES

1 **Diffie, W. and Hellman, M. E.** 'New directions in cryptography', *IEEE Trans. Infor. Theory*, Vol. IT-22 (1976) pp. 644--654.

2 **Rivest, R. L., Shamir, A. and Adleman, L.** 'A method for obtaining digital signatures and public key cryptosystems', *Comm. ACM*, Vol. 21 No. 2 (1978) pp. 120–126.

3 **ElGamal, T.** 'A public key cryptosystem and a signature scheme based on discrete logarithms', *IEEE Trans. Infor. Theory*, Vol. IT-31 No. 4 (July 1985) pp. 469–472.

4 **Fiat, A. and Shamir, A.** 'How to prove yourself: Practical solutions to identification and signature schemes', *Advances in Cryptology: Crypto 86*, Springer-Verlag (1987) pp. 186–199.

5 **Schnorr, C. P.** 'Efficient identification and sgnatures for smart cards', *Advances in Cryptology: Crypto ,89*, Springer-Verlag, New York (1990) pp. 239–252.

6 **National Institute of Standards and Technology** 'A Proposal Federal Information Processing Standard for Digital Signature Standard (DSS)', *Federal Register*, Vol. 56 No. 169 (August 1991) pp. 42980–42982.

7 **Yen, S. M. and Laih, C. S.** 'New digital signature scheme based on discrete logarithm', *Electronics Letters*, Vol. 29 No. 12 (1993) pp. 1120–1121.

8 **Piveteau, J. M.** 'New signature scheme with message recovery', *Electronics Letters*, Vol. 29 No. 25 (1993) pp. 2185–2185.

9 **Harn, L.** 'New digital signature scheme based on discrete logarithm', *Electronics Letters*, Vol. 30 No. 5 (1994) pp. 396–398.

10 **Harn, L. and Xu, Y.** 'Design of generalized ElGamal type digital signature schemes based on discrete logarithm', *Electronics Letters*, Vol. 30 No. 24 (1994) pp. 2025–2026.

11 **Horster, P., Michels, M. and Petersen, H.** 'Authenticated encryption schemes with low communication costs', *Electronics Letters*, Vol. 30 No. 15 (1994) pp. 1212–1212.

12 **Horster, P., Michels, M. and Petersen, H.** 'Meta-ElGamal signature scheme', *Proc. 2nd ACM Conf. on Computer and Comm. Security*, Fairfax, VA (May 1994).

13 **Hwang, S. J., Chang, C. C. and Yang, W. P.** 'An encryption/signature scheme with low message expansion', *J. Chinese Institute of Engineers* (to appear).

14 **Itakura, K. and Nakamura, K.** 'A Public-Key Cryptosystem Suitable for Digital Multisignatures', *NEC Research and Development*, Vol. 71 (1983) pp. 1–8.

15 **Harn, L. and Kiesler, T.** 'New scheme for digital multisignature', *Electronics Letters*, Vol. 25 No. 15 (1989) pp. 1002–1003.

16 **Kiesler, T. and Harn, L.** 'RSA blocking and multisignature schemes with no bit expansion', *Electronics Letters*, Vol. 26 No. 18 (1990) pp. 1490–1491

17 **Ohta, K. and Okamoto, T.** 'A digital multisignature scheme based on the Fiat-Shamir scheme', *Advances in Cryptology-ASISCRTPT ,91*, Springer-Verlag, New York (1991) pp. 75–79.

18 **Boyd, C.** 'Multisignatures based on zero knowledge schemes', *Electronics Letters*, Vol. 27 No. 22 (1991) pp. 2002–2004.