Short Paper

A New Digital Multisignature Scheme With Distinguished Signing Authorities

SHIN-JIA HWANG, MIN-SHIANG HWANG AND SHIANG-FENG TZENG
Department of Computer Science and Information Engineering
TamKang University
Taipei Hsien, 251 Taiwan
E-mail: sjhwang@mail.tku.edu.tw
E-mail: ShiangFeng@ms67.url.com.tw

In 1999, Harn proposed a multisignature scheme with distinguished signing authorities. In Harn's scheme, a malice member easily confuses the signing authorities since individual signatures and multisignatures both generated on the whole document cannot be used as evidence to distinguish the signing authorities. Moreover, Harn's scheme is also not secure against Li et al.'s attack [4]. To provide evidence and remove Li et al.'s attack, a new multisignature scheme with distinguished signing authorities is proposed in this article.

Keywords: digital signature, multisignature, group-oriented signature scheme, cryptography, security

1. INTRODUCTION

In a multisignature scheme, a multisignature is generated only through the cooperation of all the members in the group. Then the multisignature is easily verified by using the group public-key without knowing the members' public keys. It is computationally infeasible to generate multisignatures without the knowledge of the secret keys of all the members in the group. These are three properties associated with multisignature schemes [1]. To achieve good performance, the verification cost of multisignatures should be almost the same as that of the signature. The size of a multisignature should be the same as the size of a signature in order to reduce the space needed for multisignatures. Some multisignature schemes based on the discrete logarithm problem have been proposed [2, 3].

In the multisignature scheme, all the members in the signing group have the same signing authorities for the whole message. However, there exist some applications in which each member should have his/her own distinguished signing authority. For example, the board of directors receives the annual report about a company. The report consists of many partial contents from distinct departments in the company. Due to the distinguished responsibility, each department should authorize its partial contents. Due to the need for confidentiality, the readers are only allowed to access some authorized par-

Received February 27, 2002; revised August 14, 2002; accepted January 24, 2003.
Communicated by Ja-Ling Wu.

tial contents. At the same time, they also need to validate the relationship between the whole report and the partial contents. The correctness of the partial contents should be verified, too.

Therefore, Harn [1] first proposed the multisignature scheme with distinguished signing authorities. In his scheme, each member in the signing group may be allowed to only access partial contents of the whole document. Then each member only has his distinguished singing responsibility for his partial contents. For the multisignature scheme with distinguished signing authorities, two additional properties must be satisfied. One is that each member has his distinguished signing authority. The other is that the partial contents can be easily verified without revealing the whole message.

Unfortunately, Li et al. showed that Harn's scheme is not secure against their attack [4]. To prevent their attack, the certificate authority (CA for short) should require each user to show that he/she actually knows the secret exponent of his/her public key. However, this attack still reveals a weakness of Harn's scheme. This also increases the load and causes inconvenience for CA and users.

Moreover, in Harn's scheme, no one is able to prove his/her own distinguished signing authority though he/she actually signed only for his/her partial content. No evidence can be used to distinguish the signing authorities. The reason is that, in Harn's scheme, all individual signatures and multisignatures are generated on the same hash digest of the hash digests of all the partial contents. Therefore, the individual signatures cannot be used as evidence for the partial content. Consider the following situation. A dishonest member wants to confuse the signing authority of each member. He announces that his signing authority belongs to some other member. That is, his partial content is the signing authority of another innocent member. The innocent member is falsely incriminated by the dishonest announcement. No evidence can be used to reject this dishonest announcement. The signing authorities are confused.

To guard against Li et al.'s attack without the help of CA, a new multisignature scheme with distinguished signing authorities is proposed. The new scheme also provides individual evidence to prevent confusion over authority due to malice. In the next section, Harn's scheme is reviewed. Then our new scheme is proposed in section 3. An analysis of security and discussion are given in section 4. Section 5 gives our conclusions.

2. HARN'S SCHEME

Let P be a public large prime number. Let the integer g be a public primitive element of GF(P). Let the function h be a public one-way hash function. Suppose that the signing group is $\{U_1, U_2, \ldots, U_n\}$. Each member U_i selects a random integer x_i as his/her secret key and computes his/her public key $y_i = g^{x_i} \bmod P$ for $i = 1, 2, \ldots, n$. Then the group public key $y = \prod_{j=1}^{n} y_j \bmod P$.

Suppose that the signing group wants to generate a multisignature for the message $m_1||m_2|| \ldots ||m_n$. Here, each member U_i is responsible for signing the partial message m_i. Each member U_i first selects a random integer k_i and computes $r_i = g^{k_i} \bmod P$ and $h(m_i)$ for $i = 1, 2, \ldots, n$. Then each member U_i broadcasts r_i and $h(m_i)$ to the other n-1 members and a clerk. After receiving r_j's and $h(m_j)$'s, each member U_i computes $r = \prod_{j=1}^{n} r_j \bmod P$

and finds the solution s_i satisfying the equation $s_i + k_i r \equiv x_i h(h(m_1), h(m_2), \ldots, h(m_n)) \pmod{P-1}$. Then each member transmits an individual signature (r_i, s_i) to a clerk.

The clerk computes $r = \prod_{j=1}^{n} r_j \bmod P$ and $h(h(m_1), h(m_2), \ldots, h(m_n))$. After receiving the individual signature (r_i, s_i), the clerk verifies (r_i, s_i) by means of the equation $y_i^{h(h(m_1), h(m_2), \ldots, h(m_n))} \equiv g^{s_i} \times r_i^{r} \pmod{P}$, for i = 1, 2, …, n. Then, the clerk generates the multisignature (r, s) by computing $s = s_1 + s_2 + \ldots + s_n \bmod (P-1)$. The verification equation $y^{h(h(m_1),h(m_2),\ldots,h(m_n))} \equiv g^{s} \times r^{r} \pmod{P}$ is used to verify (r, s). If the verifier is only allowed to retrieve m_i, then he/she will received $h(m_1)||h(m_2)||\ldots||h(m_{i-1})||m_i||h(m_{i+1})||\ldots||h(m_n)$ to verify the multisignature (r, s).

After generating the multisignature, a dishonest member U_j may announce that his/her partial content is m_i, and that the partial content signed by U_i is m_j. Then the individual signatures (r_i, s_i) and (r_j, s_j) cannot be used as evidence to show that his/her announcement is not correct because both (r_i, s_i) and (r_j, s_j) are generated on the same digest $h(h(m_1), h(m_2), \ldots, h(m_n))$.

3. OUR NEW SCHEME

Parameters for system and signing groups

Let P and Q be two public large primes such that Q|P-1. The integer g is a public generator with order Q in GF(P), and the function h is a public one-way hash function. Assume that the signing group is $\{U_1, U_2, \ldots, U_n\}$. Each member U_i randomly selects his/her secret key $x_i \in Z_Q^*$ and computes his/her public key $y_i = g^{x_i} \bmod P$, where Z_Q^* denotes the set $\{1, 2, \ldots, Q-1\}$. The group public key is $Y = \prod_{i=1}^{n} (y_i)^{y_i} \bmod P$.

Multisignature Generation Phase

Suppose that the signing group $\{U_1, U_2, \ldots, U_n\}$ wants to generate the multisignature for the message $M = m_1||m_2|| \ldots ||m_n$. The member U_i is only responsible for the partial content m_i, for i = 1, 2, …n.

Step 1. Each member U_i selects a random integer $k_i \in Z_Q^*$ and computes $r_i = g^{k_i} \bmod P$ and $h(m_i)$ for i = 1, 2, …, n. Then each member U_i broadcasts r_i and $h(m_i)$ to the other n-1 members and a predetermined clerk C.

Step 2. Each member U_i computes the commitment value $r = \prod_{i=1}^{n} r_i^{h(h(m_i),r_i)} \bmod P$. The clerk also computes the commitment value r.

Step 3. Each member U_i finds the solution s_i satisfying $s_i \equiv x_i y_i H + r k_i h(h(m_i),r_i) \pmod{Q}$, where $H = h(h(m_1), h(m_2), \ldots, h(m_n))$. Then each member U_i transmits his individual signature (r_i, s_i) to the clerk.

Step 4. The clerk verifies each the individual signature (r_i, s_i) by means of the equation $g^{s_i} \equiv (y_i)^{y_i H} \times (r_i)^{r h(h(m_i),r_i)} \pmod{P}$ after receiving all of the individual signatures (r_i, s_i)'s. If all of the individual signatures are legal, then the clerk generates the multisignature (r, s) by computing $s = \sum_{i=1}^{n} s_i \bmod Q$.

Finally, (r, s) is the multisignature for the message $M = m_1||m_2|| \ldots ||m_n$.

Multisignature Verification Phase

The multisignature (r, s) is verified by means of the equation $g^s \equiv Y^H \times r^r \pmod P$. Why the equation $g^s \equiv Y^H \times r^r \pmod P$ can be used to verify the multisignature (r, s) is shown in the following:

$$\begin{aligned} g^s &\equiv g^{\sum_{i=1}^{n} s_i} \\ &\equiv g^{\sum_{i=1}^{n} (x_i y_i h(h(m_1),h(m_2),...,h(m_n))+rk_i h(h(m_i),r_i))} \\ &\equiv g^{\sum_{i=1}^{n} x_i y_i h(h(m_1),h(m_2),...,h(m_n))} \times (g^{\sum_{i=1}^{n} k_i h(h(m_i),r_i)})^r \\ &\equiv Y^H \times r^r \pmod P. \end{aligned}$$

The partial contents of the message $m_1||m_2||\ldots||m_n$ can be verified without revealing the whole document. If the verifier is only allowed to read the partial content m_i, then he/she will receive $h(m_1)||h(m_2)||\ldots||h(m_{i-1})||m_i||h(m_{i+1})||\ldots||h(m_n)$ to verify the multisignature (r, s).

Evidence Verification Phase

All of the individual signatures (r_i, s_i) can be used as evidence. To show that member U_i is responsible for signing only for the partial content m_i, (r, s), (r_i, s_i) and $M = m_1||m_2||\ldots||m_n$ are verified by $g^s \equiv Y^H \times r^r \pmod P$ and $g^{s_i} \equiv (y_i)^{y_i H} \times (r_i)^{rh(h(m_i),r_i)} \pmod P$. If the two equations are satisfied, member U_i is responsible for signing only for the partial content m_i because the equation $g^{s_i} \equiv (y_i)^{y_i H} \times (r_i)^{rh(h(m_i),r_i)} \pmod P$ shows the relationship between the whole document, the partial content m_i, and member U_i.

4. SECURITY ANALYSIS AND DISCUSSION

The security of the new scheme is based on the security of the underlying signature scheme. Since the underlying signature scheme is based on the discrete logarithm problem, the members' secret keys are secure.

Let us consider Li et al.'s attack [4] first. Without loss of generality, suppose that member U_n wants to execute the attack in [4] by changing his/her public key. Member U_n first selects his/her new secret key x and computes $y = g^x \bmod P$. After obtaining the other n-1 members' public keys, he/she should find the solution y'_n such that $y \equiv \prod_{i=1}^{n-1} (y_i)^{y_i} \times (y'_n)^{y'_n} \pmod P$. Because the values of y and $\prod_{i=1}^{n-1} (y_i)^{y_i} \pmod P$ are determined, he/she has to solve the equation $(y'_n)^{y'_n} \equiv y \times (\prod_{i=1}^{n-1} (y_i)^{y_i})^{-1} \pmod P$. It is an extremely difficult problem to find y'_n satisfying $(y'_n)^{y'_n} \equiv y \times (\prod_{i=1}^{n-1} (y_i)^{y_i})^{-1} \pmod P$ [2].

Consider the security of the individual signatures (r_i, s_i). Suppose that some dishonest attacker wants to forge (r_i, s_i) on some message $M = m_1||m_2|| \ldots ||m_n$. Due to the secure one-way hash function, he/she has to compute $r_i = g^{k_i} \bmod P$, H and $h(h(m_i), r_i)$ first. Then he/she has to solve the discrete logarithm problem $g^{s_i} \equiv (y_i)^{y_i H} \times (r_i)^{rh(h(m_i),r_i)} \pmod P$ to find the value of s_i. If he/she determines the value of s_i first, then he/she has to overcome the challenges of the discrete logarithm problem and one-way hash functions.

Consider the security of the multisignature (r, s). Suppose that someone wants to forge (r, s) on a given digest H; he/she may determine r first and then find s, or he/she may determine s first and then find r. According to the equation $g^s \equiv Y^H \times r^r \pmod P$, he/she has to either solve the discrete logarithm problem $g^s \equiv Y^H \times r^r \pmod P$ to obtain s or solve another hard problem $r^r \equiv g^s \times Y^{-H} \pmod P$ [2] to obtain r. Therefore, it is hard to forge the multisignature (r, s). Since the group secret key is the sum $\sum_{i=1}^{n} x_i y_i \bmod Q$, the multisignature (r, s) is generated by all of the secret keys of the members. Therefore, the multisignature (r, s) has to be generated through the cooperation of all the members.

Now consider the security of the evidence (r, s) and (r_i, s_i). The individual signature (r_i, s_i) is also a signature generated by U_i on the partial content m_i. At the same time, (r_i, s_i) could be used to show the relation between member U_i, M and m_i for $s_i \equiv x_i y_i H + rk_i h(h(m_i), r_i) \pmod Q$. Therefore, (r, s) and (r_i, s_i) can be used as evidence to show that member U_i only signs the partial content m_i belonging to the whole message M.

The new scheme is secure against Li et al.'s attack. In the new scheme, someone can discriminate each member's distinguished signing authority by using the evidence (r, s) and (r_i, s_i). However, compared with Harn's scheme, an additional computation cost should be paid. In the following, the notation ME_P denotes one modular exponentiation operation modular p, and the notation MM_Q denotes one modular multiplication operation modular Q. The notation T_H denotes the computation cost of the hash function H. Compared with the group public key $y = \prod_{i=1}^{n} y_i \bmod P$ in Harn's scheme, the additional cost n ME_P for the group public key is $Y = \prod_{i=1}^{n} (y_i)^{y_i} \bmod P$. Usually, the group key is computed once and then used. Thus, this cost can be ignored. In the multisignature generation phase, the totally additional computation cost for the commitment value r is n^2 ME_P and $2n^2$ T_H because the $r = \prod_{i=1}^{n} r_i^{h(h(m_i),r_i)} \bmod P$ is computed by the n members. For each member, since the equation $s_i \equiv x_i y_i H + rk_i h(h(m_i),r_i) \pmod Q$, the additional cost of finding s_i is $2MM_Q + 2T_H$. Due to the verification equation $g^{s_i} \equiv (y_i)^{y_i H} \times (r_i)^{rh(h(m_i), r_i)} \pmod P$, the additional cost of verifying all of the n individual signatures is $2n\ MM_Q + 2n\ T_H$. Therefore, in the multisignature generation phase, the total additional cost is $n^2\ ME_P + (2n^2 + 2n)\ T_H + 2n\ MM_Q$. Here the clerk is assumed to be some member of the group. Due to the equation $g^s \equiv Y^H \times r^r \pmod P$, there is no additional computational cost for multisignature verification. Moreover, the verification cost is almost the same as the cost of verifying the signature generated by a single signer. To provide evidence and to guard against Li et al.'s attack, the major additional cost is caused by multisignature generation. The major additional computation cost is bearable because each multisignature is generated once and will be verified many times. This is another advantage of our new scheme.

Finally, let us consider the size of the individual signatures and the multisignature. It is easy to see that the size of an individual signature or the multisignature is $|P| + |Q|$. This

size is the same as the size of a signature generated by a single signer. This size is also the same as the size of an individual signature or the multisignature in Harn's scheme. Although our new scheme provides evidence for distinguishing authority and is secure against Li et al.'s attack, the sizes of individual signatures or multisignatures are still the same those of individual signatures or multisignatures in Harn's scheme.

5. CONCLUSIONS

The new multisignature scheme satisfies the five properties of multisignature schemes with distinguished signing authorities in [1]. Compared with Harn's scheme, our new scheme provides additional evidence members can use to prove their distinguished signing responsibility. In the new scheme, an individual signature (r_i, s_i) and the multisignature (r, s) can show the relationship between the whole document, the partial content, and the signing member. Therefore, each member is able to show that he/she only has signing responsibility for the partial content for which he/she has signed.

Moreover, a new way for generating group public keys has been proposed to guard against Li et al.'s attack in [4]. On the other hand, Harn's scheme is not secure against Li et al.'s attack. The verification cost of the multisignature is almost the same as the cost of a signature generated by a single singer. The major additional computation cost is paid to generate the multisignature. This additional cost is bearable because the multisignature is usually generated once and verified many times. Although the new scheme is more secure than Harn's scheme, the size of the multisignature is still the same as the size of a signature generated by a single singer.

REFERENCES

1. L. Harn, "Digital multisignature with distinguished signing authorities," *Electronics Letters*, Vol. 35, 1999, pp. 294-295.
2. L. Harn, "Group-oriented (t, n) threshold digital signature scheme and digital multisignature," *IEE Proceedings: Computers and Digital Techniques*, Vol. 141, 1994, pp. 307-313.
3. L. Harn and Y. Xu, "Design of generalised ElGamal type digital signature schemes based on discrete logarithm," *Electronics Letters*, Vol. 30, 1994, pp. 2025- 2026.
4. Z. C. Li, L. C. K. Hui, K. P. Chow, C. F. Chong, H. H .Tsang, and H. W. Chan, "Cryptanalysis of Harn digital multisignature scheme with distinguished signing authorities," *Electronics Letters*, Vol. 36, 2000, pp. 314- 315.

Shin-Jia Hwang (黃心嘉) is the associate professor of Department of Computer Science and Information Engineering, Tamkang University, Tamsui, Taipei, Taiwan. During the academic years of 1996-2001, he was on the faculty of the Department of Information Management at Chaoyang University of Technology, Wufeng, Taichung Hsien, Taiwan. He received his B.S. degree in information and computer engineering from Chung-Yuan Christian University, Chungli, Taiwan in 1987 and his MS degree in computer science and information engineering from National Chung Cheng University,

Chiayi, Taiwan in 1992. He received his Ph.D. degree in computer and information science form National Chaio Tung University, Hsinchu, Taiwan. His research interests include cryptography and computer security.

Min-Shiang Hwang (黃明祥) received the B.S. in Electronic Engineering from National Taipei Institute of Technology, Taipei, Taiwan, Republic of China (ROC), in 1980; the M.S. in Industrial Engineering from National Tsing Hua University, Taiwan, in 1988; the Ph.D. in Computer and Information Science from National Chiao Tung University, Taiwan, in 1995. He also studied Applied Mathematics at National Cheng Kung University, Taiwan, from 1984 to 1986. Dr. Hwang passed the National Higher Examination in field "Electronic Engineer" in 1988. He also passed the National Telecommunication Special Examination in field "Information Engineering", qualified as advanced technician the first class in 1990. From 1988 to 1991, he was the leader of the Computer Center at Telecommunication Laboratories (TL), Ministry of Transportation and Communications, ROC. He was also a project leader for research in computer security at TL in July 1990. He obtained the 1997, 1998, 1999, 2000, 2001 Distinguished Research Awards of the National Science Council of the Republic of China. He is currently a professor and chairman of the Department of Information Management, Chaoyang University of Technology, Taiwan, R.O.C. He is a member of IEEE, ACM, IEICE, and Chinese Information Security Association. His current research interests include database and data security, cryptography, image compression, and mobile communications.

Shiang-Feng Tzeng (曾祥峰) received the B.S. degree in Information Management from Chaoyang University of Technology (CYUT), Taichung, Taiwan, Republic of China, in 2001. He is currently pursuing his M.S. degree in Information Management from CYUT. His current research interests include applied cryptography and data security.