Journal of Applied Sciences

ISSN 1812-5654

science alert

ANSInet
an open access publisher
http://ansinet.com

Journal of Applied Sciences 7 (13): 1813-1817, 2007
ISSN 1812-5654

A New Multisignature Scheme Using Re-Encryption Technique

Sattar J. Aboud and Mohammed A. AL-Fayoumi
Department of Computer Information Science, Faculty of IT,
The University for Graduate Studies, Amman, Jordan

Abstract: A new multisignature scheme using re-encryption technique based on the RSA algorithm is suggested what enhance version of Okamoto scheme. The suggested scheme results bit expansion in block length of the multisignature, but the bit size of the expansion is not larger than the number of signers irrespective of their modulus. In addition, the new scheme has no limitations in signing order and in fact is more efficient than the Okamoto scheme.

Key words: RSA scheme, multisignature scheme, Okamoto scheme, bit size expansion, re-encryption technique

INTRODUCTION

In the past, we made a signature by signing a name or affixing a seal on a document to establish the corresponding rights and duties. Since we are now in the era of e-commerce and e-government, the use of digital signatures is very important. Learning the use of digital signatures is also significant. However, since the law of digital signature has been passed in October 31 2001, the security of digital signature schemes must not be ignored (Chiou, 2004). Digital signature scheme must accomplish the functions of undeniable, integrity and identification. In general, a digital signature scheme can be done by a public key cryptography. For different security hypothesis, we can divide digital signature algorithms into two types. The first one is a digital signature scheme based on the discrete logarithm problem such as Elgamal digital signature scheme. In this hypothesis the discrete logarithm problem can not be broken; this type of digital signature scheme is secure. Alternatively, if the discrete logarithm problem can be broken, this type of discrete signature scheme will become insecure. The second type is a digital signature scheme based on the factoring problem such as RSA digital signature scheme. Also, under this hypothesis the factoring problem can not be broken; this type of digital signature scheme is secure. It means that if the factoring problem can be broken, this type of digital signature scheme will also be broken. The discrete logarithm problem and the factoring problem are two hard solved mathematical problems and the two problems are believed to be unsolved in the reasonable time period (Al-Fayoumi and Aboud, 2006a,b). However, if any one of the two problems is solved in the future, the digital signature schemes based on this hard problem hypothesis will become insecure. Hence, if there is a digital signature algorithm of which the security is based on both the discrete logarithm problem and the factoring problem, the digital signature scheme will be still secure under the situation that any one of the two problems is solved.

In this study, we propose a new multisignature scheme using re-encryption technique based on the RSA scheme. The security of the RSA scheme is relied on the integer factoring problem (Rivest *et al*., 1978). The practical example of RSA scheme for multiple operations of a known message results bit expansion difficulty inherently. The early methods to solve this problem are re-blocking algorithm (Kohnfelder, 1978) and repeated square and multiply algorithm Levine and Brawley (1977). To face the problem of bit expansion in the RSA multisignature, they should permit a signer to have the RSA modulus with a different bit length corresponding to the signer place in a hierarchical structure. Thus, the signing order is limited. There are two other multisignature schemes with out bit expansion (Harn and Kiesler, 1989; Kiesler and Harn, 1990). In the first scheme the signing order is selected corresponding to the length of signers' public keys. The second scheme is relied on the re-encryption scheme with permutation polynomials technique. However, the two multisignature schemes have no bit expansion difficulty and the signing order is not limited. All signers should have a modulus with the equal length and the mathematical complexity of finding the multisignature. Alternatively, Okamoto (1998) suggested multisignature scheme without limitation of the signing order (Okamoto, 1998). In this scheme, if the size of midway signature exceeds a pre-determined threshold value, then the additional bits exceeding the threshold

Corresponding Author: Sattar J. Aboud, Department of Computer Information Science, Faculty of IT,
The University for Graduate Studies, Amman, Jordan

value are added on to the document. Thus, the size of the expanded document relies on the number of signers and the bit length of every signer's RSA modulus.

In this study, we suggested a new multisignature scheme using re-encryption technique to enhanced version of Okamoto scheme. The suggested scheme also results bit expansion in block length of the multisignature, but the bit size of the expansion is not more than the number of signers irrespective of their modulus.

HANDWRITTEN SIGNATURE

Handwritten signature has long been employed as a proof of authorship of or at least agreement with the contents of a message (Davies and Price, 1984; Yoshimura and Yoshimura, 1996). The reasons of employing signature as authorship proof (Bruce, 1996) are as follows:

- The signature is not reusable. The signature is a piece of message; the dishonest individual cannot transfer the signature to another message.
- The signature is authentic. The signature encourages the message's receiver that the signer thoroughly signed the message.
- The signature is unchangeable. Once the message is signed, it can not be changed.
- The signature is un-forgeable. The signature is evidence that the signer and there is no individual else carefully signed the message.
- The signature non-repudiation. The signature and the message are physical objects. The signer can not say that he did not sign it afterward.

THE PROPOSED MULTISIGNATURE SCHEME

First we present the notations used in this section:

- u_i: one of t signers $u_1,...,u_t$
- n_i: RSA modulus of u_i
- (n_i, b_i): public key of u_i
- (n_i, k_i): private key of u_i
- $\theta(n_i) = (p-1)(q-1)$
- h (m): hash function
- $|n_i|$: bit length of n_i

Also, in this section we present a new re-encryption scheme in which the length of the encrypting block differs with the length of the message block. Assume n is the RSA modulus which is the product of two large prime numbers and b is a public key with gcd (b, θ (n)) = 1. The secret key k is then computed using the multiplicative inverse (Aboud and Al-Fayoumi, 2005). Suppose an odd message m where $0 < m < 2^x*n$. Then $\theta(2^x*n) = 2^{x-1}*\theta$ and gcd (b, $2^{x-1}*\theta$ (n)) = 1. If $b*k \equiv 1 \pmod{2^{x-1}*\theta(n)}$, then $m^{b*k} \equiv m \bmod 2^x*n$. Thus, x differs with the length of a message m and k differs with x. If $c = m^b \bmod 2^x*n$ and $e*k_1 \equiv 1 \bmod 2^{x-1}$ then c mod $2^x = m^b \bmod 2^x$ and m mod $2^x = c^{k1} \bmod 2^x$. So, the suggested re-encryption technique can not be directly employed for encrypting m with large block length. However, this new re-encryption technique can be implemented in the multisignature scheme if every user calculates x^i from n^i as follows:

$$x_i = (1 \text{ If } I = 1 \text{ or } 2^{xi-1}*n_{i-1} < 2*n_i) \text{ else}$$
$$x_i = (2^{xi-1}*n_i\ 2^{xi-1}*n_{i-1} < 2^{xi}*n_i)$$

The multisignature generation is achieved as follows:

The first signer u_1 signs$_1 = (2*h(m)+1)^{k1} \bmod 2*n_1$, then the first signer u_1 sends the message m and s_i to the second signer u_2. The second signer u_i sign (i = 2,...,t)

$$s_i = s_{i-1}^{k_i}$$

$$\bmod 2^{x_i} * n_i$$

where $b_i*k_i = m \bmod 2^{xi-1}*\theta(n_i)$ and the second signer then sends m and s_i to the next signer.

The multisignature verification is done as follows:

The receiver verifies that s_t is the multisignature of m by signers $u_1, ..., u_t$

$$\begin{cases} S_{j-1} = S_j^{b_j} \pmod{2^{x_j}*n_j}, j = t, t-, ..., 2 \\ 2h(m)+1 = S_1^{b_1} \pmod{2*n_1} \end{cases}$$

But when bi+1

$$*k \equiv 1 \bmod 2^{x_i+1^{-1}}$$

and $b_i*k \equiv 1 \bmod 2^{xi}$ then

$$s_i \equiv c_i \bmod 2^{x_i+1^{-1}} \text{ and } s_i = s_{i-1} \bmod 2^{x_i}.$$

Though, we can not get the most significant $|n_{i+1}|$ bits of s_i from c_i and the most significant $|n_{i+1}|$ bits of s_i from s_{i-1}. But when $z = \max(|n_1|, |n_2|, ..., |n_t|)$, then the bit size of the multisignature .Thus the size expanded by the suggested method is not larger than the number of

signers. For instance when ($|n_1| = |n_2| = |n_t|$) = 768 and ($|n_2| = |n_4| = |n_6|$) = 512 , then $|s_t| \leq 774$. Thus, the expanded bit size is 6. But, in this example, Okamoto scheme has an expansion of 509 bits. As a result, the suggested scheme is more efficient than the Okamoto scheme. In addition, the new scheme has no limitations in signing order.

In some circumstances, the number of signers could be several. For instance, in an organization any two authorized signers may be permitted. So, according to this point the above algorithm can be extended to meet this extra work. However, when there are possible signers, then n random private keys k_1, k_2, k_n are selected. The public key b is selected so that:

$$k_1, k_2, k_n * b \equiv 1 \bmod \theta(n)$$

Every signer is then given all the secret keys unless one. For instance the jth signer is provided all k_i unless k_j. Every signer keeps all these keys and also their outcomes. Suppose $k_i = k_1, \ldots, k\ (j-1)\ k\ (j+1), \ldots k_n$ If the jth signer wants to sign a cheque, c he signs it to compute:

$$b_1 = c^{k_j} \bmod n$$

and adds his identity. The other signer can then achieve the signing by looking on the absent key, which also permits him to check the cheque and then to compute:

$$S_2 = S_1^{k_j} \bmod n$$

The receiver and any member can again check the signature by decryption with b.

Digital multisignature scheme which requires the knowledge of the message as on input to the verification algorithm is called digital signature scheme with appendix. Digital signatures schemes with appendix are the most commonly employed in practice (Menezes, 1997). They based on cryptography hash function rather than redundancy function and are less prone to existential forgery attacks. The proposed scheme is designed to use a combination of an appropriate one way hash function h with which m shell be hashed before signing in order to bound the size of the key in verification. To avoids the potentiality of message collisions. It is preferable that the hash function employed must have a 160 bits product and secure hash algorithm (FIPA 180-1; 1995) which seems to be appropriate choice.

The multiplicative ability used in this algorithm can also be employed to attack RSA signature in some situation (Aboud, 2004). For instance, since ($m_1 * m_2$) ≡ m_1, m_2) the signature of m_1, m_2 can be gathered from those of m_1 and m_2. Various tools are available to exclude these attacks and they are also usable in this algorithm. One technique is to employ a one way hash function h with which the message should be hashed pre-signing to bind the size of the key in verification. To avoid the potentially of collision of messages, it is preferable that the hash function employed must have a 160 bits outcome and secure hash algorithm (FIPA 180-1, 1994; FIPA 180-1, 1995). So we have h (m_1, m_2) = h (m_1) *h (m_2). This also has the benefit that just single block requires to be signed.

SECURITY OF THE SCHEME

Many useful multisignature schemes do not bear any proof of security; it is known that breaking RSA multisignature is based on the factorization difficulty. The only visible attacks on the suggested schemes are as difficult as factoring the modulus n (Aboud and Abu-Taieh 2006) but it is not shown if there is any certain efficient attack. For the security examination, we gain from the modular design of the proposed system employing well known cryptography scheme. Though all known attacks are verified to be prevented (Rivest, 1978). The security analysis is obviously constructive as we stay away from interaction among the scheme as can as possible. However, we will set out the security of the scheme we proposed. Assume that n is the RSA modulus for the suggested algorithm. As n had large prime factors p and q, then no one can factor n through any integer factoring technique. Furthermore, p-1 and q-1 have large prime factors p and q. Though each user has n_i s, the most significant bits of which are of the same value, the prime factors p_i and q_i of n_i are arbitrary. As a result, u_i can not deduce the prime factors p_i and q_i of the other user u_t. The following theorems are simply verified:

Theorem 1: If we able to calculate the private key k by $b*k \equiv 1 \bmod 2^{x-1} * \theta(n)$, then the signature of random message m can be found.

Proof 1: If $k \equiv k \bmod \theta(n)$, then $c \equiv m^k \equiv m^k \bmod n$ and $e*k \equiv b*k \equiv 1 \bmod \theta(n)$. Thus c is the signature of the message m

Theorem 2: For any odd m where $0<m<2^x * n$, we can calculate c by $c\ c \equiv m^b \bmod 2^x * n$ so the signature of the message m can be found.

Proof 2: If

$$c^{-} = c \bmod n \cdot$$

So

$$c^{-} = m^{b} \bmod n$$

then c is the signature of the message m.

Through theorems 1 and 2, the security of the scheme relied on the novel re-blocking method based on the security of RSA signature algorithm.

Many practical multisignature schemes including the RSA are liable to existential forgery attacks if a hash function is not employed pre-signing. In such attacks, there are unrestricted numbers of multi-signatures for random messages may be created. For the suggested algorithm, a simple existential forgery is that the value s = 1 is the multisignature for the message m = c. Additional random multi-signatures appear difficult to perform.

Choosing forgery relates to the complexity of forging a multisignature of a message selected in advance by the opponent. With the employment of one technique hash function, this seems the only way to compute any valid multisignature (Stinson, 2006). The opponent selects a message m and is needed to compute a signature S with s^{m} mod n = c. The possibility to calculate the multisignature s from knowledge of the public key is identical to breaking the RSA encryption algorithm for an existing cipher text c and public key b, with the part data there is a factor of θ (n) of size 160 bits. It is unobvious if the part data is an aid in factoring n. The likeness to the security of identification protocol (Brickel and McCurle, 1992; Aqel and Ammar, 2005) may again be explored.

A suitable selected message attack that employs multi-signatures on selected messages is difficult to hinder the attack of employing just the public key. Such an attack is no longer identical to an attack of RSA but could accord to a case where an opponent could select the public key of the RSA and get the original message according to the cipher text c (Aboud and El Sheikh, 2004; Trappe and Washington, 2006). It does not seem to be a clear manner that aids an opponent.

CONCLUSIONS

We have suggested a multisignature algorithm and also a novel re-blocking technique in which the length of the encryption block differs by the length of a message block and have employed the novel re-blocking technique to a multisignature scheme. Every signer is allowed to have the RSA modulus with different bit length. It results bit expansion which relies only on the number of signers despite of the bit size of RSA modulus. The size of the expansion is less than or equal to the number of signers. But when every signer has the RSA modulus and the same length, then our algorithm and Okamoto one have an equal expansion. But the proposed scheme has lesser bit expansion than Okamoto's algorithm. So the suggested scheme is claimed to be more efficient than Okamoto scheme.

REFERENCES

Aboud, S.J., 2004. Baghdad method for calculating multiplicative inverse. International Conference on Information Technology, Las Vegas, Nevada, USA., pp: 816-819.

Aboud, S.J. and A. El Sheikh, 2004. A New method for public key cryptosystem and digital signature scheme based on both integer factorizations and discrete logarithms. Asian J. Inform. Technol., 3: 284-289.

Aboud, S.J. and M.A. Al-Fayoumi, 2005. Two Efficient Digital and Multisignature Schemes, Proceeding of the IASTED. International Conferance Computational Intelligence, Calgary, Canada, pp: 457-362.

Aboud, S.J. and E.M. Abu-Taieh, 2006. A new deterministic rsa factoring algorithm, Jordan. J. Applied Sci., 8: 54-66.

Al-Fayoumi, M.A. and S.J. Aboud, 2006a. An efficient concept in digital signature schemes using computational delegation. Int. J. Wseas Trans. Computer Res., 1: 25-30.

Al-Fayoumi, M.A. and S.J. Aboud, 2006b. A new idea on Digital Signature Schemes, the Wseas Multi-Conference in Venice, the 5th Wseas. International Conferance Information Security Privacy (ISP '06), November 20-22 October.

Aqel, M. and M. Ammar, 2005. Function structure and operation of a modern system for authentication of signature scheme. Pak. Inform. Technol. J., 4: 96-105.

Bruce, S., 1996. Applied Cryptography. 2nd Edn, John Wiley and Son, Ltd.

Brickel, E.F and K.S. McCurle, 1992. An interactive identification scheme based on discrete logarithms and factoring. J. Cryptol., 5: 29-39.

Chiou, S.Y., 2004. The design and analysis of digital signature based on factoring and discrete logarithm problems. Ph.D. Thesis, National Cheng Kung University China, pp: 1-10.

Davies and W.L. Price, 1984. Security for Computer Network. John Wiley and Son, Ltd.

FIPA 180-1, Secure Hash Standard, US Department of Commerce/NIST.

FIPA 180-1, 1994. Secure Hash Standard, US Department of Commerce/NIST, 1995.

Harn, L. and T. Kiesler, 1989. New scheme for digital signatures. Electron. Lett., 25: 1527-1528.

Kiesler, T. and L. Harn, 1990. RSA blocking and multisignature schemes with no bit expansion. Electron. Lett., 26: 1490-1491.

Kohnfelder, L.M., 1978. On the signature re-blocking problem in public key cryptography. Communication of ACM, 21: 179.

Levine, J. and J.V. Brawley, 1977. Some cryptographic applications of permutation polynomials. Cryptologia, 1: 76-92.

Menezes, A., 1997. Oorschot P. van and S. Vanstone, Handbook of Applied Cryptography, ARC Press.

Okamoto, T., 1998. A digital multisignature scheme using bijective public key cryptosystems. ACM Trans. Comput. Sys., 6: 432-441.

Rivest, R.L., A. Shamir and L. Adleman, 1978. A method for obtaining digital signatures and public key cryptosystem. Communications of ACM., 21: 120-126.

Rivest, R.L., 1978. Remarks on a proposed cryptanalytic attack on the M.I.T, Public key cryptosystem. Cryptologia, 2: 62-65.

Stinson, D.R., 2006. Cryptography. Theory and Practice. CRC 2nd Edn., pp: 117-149.

Trappe, W. and L. Washington, 2006. Introduction to Cryptography with Coding Theory. 2nd Edn., Pearson Education International, pp: 245-255.

Yoshimura, M. and I. Yoshimura, 1996. Recent trends in writer recognition technology. J. Inst. Electro. Inform. Commun. Eng., PRM, U96-48, pp: 81-90.