available at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

Efficient identity-based RSA multisignatures[☆]

Lein Harn[a,*], Jian Ren[b]

[a]Department of Computer Science and Electrical Engineering, University of Missouri, Kansas City, MO 64110, United States
[b]Department of Electrical and Computer Engineering, Michigan State University, East Lansing, MI 48864, United States

ARTICLE INFO

Article history:
Received 3 October 2007
Accepted 10 March 2008

Keywords:
Digital signature
Identity-based signature
Multisignature
RSA
Public-key cryptography

ABSTRACT

A digital multisignature is a digital signature of a message generated by multiple signers with knowledge of multiple private keys. In this paper, an efficient RSA multisignature scheme based on Shamir's identity-based signature (IBS) scheme is proposed. To the best of our knowledge, this is the first efficient RSA-based multisignature scheme with both fixed length and the verification time. The proposed identity-based multisignature scheme is secure against forgerability under chosen-message attack. It is also secure against multi-signer collusion attack and adaptive chosen-ID attack.

1. Introduction

Public-key cryptography is playing an increasingly popular and important role in transmitting information via the Internet and in E-commence. It has been used in web application to authenticate the web server. A public-key cryptosystem allows users to communicate securely without having prior access to a shared secret key. Public-key cryptography can be used to create digital signatures that can be used to authenticate the message and provide non-repudiation evidence.

A digital multisignature is a normal digital signature of a message generated by multiple signers with knowledge of multiple private keys. Generally speaking, the major difference between a hand-written multisignature and a digital multisignature is the length of the multisignature. In a hand-written multisignature, the length is linear in the number of signers, while in a digital multisignature, the length of the digital multisignature can be identical to a single signature. Digital multisignature is just a string of binary bits that can only be generated with the knowledge of a set of private keys. An outsider can easily verify the authenticity of a given message based on the multisignature and all signers' public keys. The verification time of multisignature can be fixed, instead of linear in the number of signers.

The concept of digital multisignature is very similar to the concept of group-oriented threshold signature. The group-oriented cryptography was first introduced by Desmedt (1987). By applying the concept of group-oriented cryptography, threshold signature scheme can be developed. Several threshold signature schemes and their modifications have been developed (Chang and Lee, 1993; Chaum and Heyst, 1991; Desmedt and Frankel, 1989; Desmedt and Frankel, 1991; Laih and Harn, 1991). In a threshold signature scheme, a group signature is generated by a number of participating members, which is larger than or equal to a predefined threshold value. For instance, in a (t, n) threshold signature scheme, any t or more than t members can represent the group to generate a group signature. Later, the verifier can use the group's public key to validate the group signature. The special case of the threshold signature called the $(1, n)$ group signature was proposed by Chaum and Heyst (1991). In a $(1, n)$ group signature, a group signature could be generated by an employee

[☆] This research was supported in part by the NSF under grant CNS-0716039.

[*] *Corresponding author.*
E-mail addresses: harnl@umkc.edu (L. Harn), renjian@egr.msu.edu (J. Ren).

0167-4048/$ – see front matter © 2008 Elsevier Ltd. All rights reserved.
doi:10.1016/j.cose.2008.03.003

(i.e. a group member) of a large company, and be verified by any outside verifier as a normal digital signature, but not be able to identify the particular employee who signed it. However, even all other group members (and the manager) collude, they cannot forge a signature for a non-participating group member. Boyd (1989) proposed the first (n, n) threshold signature based on RSA scheme in which all signers share the same modulus. The length of the group signature is fixed and the verification time of the group signature is also constant. However, it is only a (n, n) threshold signature scheme. It is not a multisignature scheme since the signer's group is predefined and cannot be changed through the application. Although multiple signers are involved in generating a digital multisignature and a threshold signature, there is a main difference between these two signatures. In a threshold signature application, the signing group is predefined and cannot be changed. However, in a multisignature application, the signing group can be dynamically formed by any set of signers.

An *efficient multisignature* scheme should possess the following two properties:

- *Fixed length*. Fixed length means that the length of the multisignature is the same as the length of the single signature.
- *Constant verification time*. Constant verification time means that to verify the multisignature, the number of modulo exponentiations required is the same as the verification of a single signature.

An efficient digital multisignature scheme (Harn, 1994) based on discrete logarithm problem has been proposed in 1994. In this scheme, the length and the verification time of the multisignature are both fixed. For RSA (Rivest et al., 1978) based multisignature scheme, the moduli clashing problem has to be overcome first so that all signing process can operate in the same domain (Kohnfelder, 1978; Kiesler and Harn, 1990). Some proposals have been proposed to solve the moduli clashing problem (Harn and Kiesler, 1989; Pon et al., 2002). However, in these schemes, the verification time of each multisignature is still a linear function in the number of signers involved. There is no efficient RSA-based multisignature scheme exists in the literature. To address this problem, all signers need to share the same modulus, which is impossible in traditional RSA public-key system.

In 1985, Shamir introduced the concept of an identity-based (ID-based) cryptosystem to simplify the public-key authentication problem. In this system, each signer needs to register at a private key generator (PKG) and identify himself before joining the network. Once a signer is accepted, the PKG will generate a secret key for that signer based on the signer's identity, which may include the signer's name, email address, etc. The signer's identity will be the signer's public key. In this way, a signer only needs to know the "identity" of his communication partner and the public key of the PKG, to verify a digital signature or to send an encrypted message. There is no public-key directory needed in this system. Shamir proposed an identity-based signature (IBS) scheme (Shamir, 1985) based on integer factorization problem (IFP) in 1984. Bellare et al. (2004) proved that the scheme is secure against forgerability under chosen-message attack. In an IBS scheme, all signers can share the same modulus in generating their individual signatures.

In this paper, we propose an efficient multisignature scheme based on Shamir's IBS scheme. To the best of our knowledge, this is the first efficient RSA-based multisignature scheme. In our scheme, the length of the multisignature is fixed. The verification time of the multisignature is also fixed since the modulo multiplications in signature verification are much more efficient comparing to the modulo exponentiations and can be ignored.

The paper is organized as follows. In Section 2, we review of Shamir's IBS scheme. Our proposed multisignature scheme is in Section 3. Security analysis of the proposed scheme is discussed in Section 4. We conclude in Section 5.

2. Review of Shamir's identity-based signature scheme

2.1. *PKG keys*

The PKG chooses its public and private key pairs as follows:

1. Runs the probabilistic polynomial algorithm to generate two random large primes, p and q.
2. Chooses a random public key e such that $\gcd(e, \phi(n)) = 1$ and computes the private key $d = e^{-1} \bmod \phi(n)$.

2.2. *Signer secret key generation*

In this algorithm, the signer gets a copy of his secret key from the PKG through a two-step process:

1. A signer submits his identity i to the PKG.
2. The PKG, with its private key d and the corresponding public key e, signs i by generating a secret key g, such that $g = i^d \bmod n$, where g is the secret key of the signer.

2.3. *Message signing*

To sign a message m, the signer with the secret key g and the corresponding public key e of the PKG signs a message m by generating a signature pair $\sigma = (t, s)$ as follows:

1. Selects a random number r and computes

   $t = r^e \bmod n\,.$

2. For the same random number r, computes

   $s = g \cdot r^{H(t,m)} \bmod n\,,$

   $\sigma = (t, s)$ is the complete signature of the message m.

2.4. *Message verification*

The identity-based signature $\sigma = (t, s)$ of a signer with identity i is valid if and only if the following equality holds

$$s^e = i \cdot t^{H(t,m)} \bmod n\,. \qquad (1)$$

3. Proposed identity-based multisignature

In this section, we will propose an identity-based multisignature scheme. Our description follows the model proposed in Micali et al. (2001).

3.1. PKG keys

The PKG chooses its public and private key pairs as follows:

1. Runs the probabilistic polynomial algorithm K_{rsa} to generate two random large primes, p and q.
2. Chooses a random public key e such that $\gcd(e, \phi(n)) = 1$ and computes the private key $d = e^{-1} \bmod \phi(n)$.

3.2. Multisignature generation

3.2.1. Signer secret key generation

In this algorithm, the signer gets a copy of his secret key from the PKG through a two-step process:

1. A signer submits his identity to the PKG.
2. The PKG, with its private key d and the corresponding public key e, signs the *message digest* of the identity, denoted as i_j, by generating a secret key g_j, such that $g_j = i_j^d \bmod n$. g_j is the signer i_j's secret key. We will not distinguish between the identity and its message digest.

3.2.2. Message signing

To generate an identity-based multisignature, each signer carries out the followings steps:

1. Chooses a random integer r_j and computes

   $$t_j = r_j^e \bmod n.$$

2. Broadcasts r_j to all the signers.
3. Upon receiving of r_j, $j = 1, 2, \ldots, l$, each signer computes

   $$t = \prod_{j=1}^{l} r_j \bmod n$$

   and

   $$s_j = g_j \cdot r_j^{H(t,m)} \bmod n.$$

4. Broadcasts s_j to all the signers.
5. After receiving of s_j, $j = 1, 2, \ldots, l$, the multisignature component s can be computed as

   $$s = \prod_{j=1}^{l} s_j \bmod n.$$

The multisignature for message m is $\sigma = (t, s)$.

From the above algorithm, it is clear that the signing phase of each individual signature is identical to the original IBS scheme. It is also clear that the length of each multisignature is the same as the individual IBS.

3.3. Multisignature verification

To verify a multisignature $\sigma = (t, s)$ of a message m of signers whose identities are $i_1, i_2, \ldots, i_l$, one verifies the following:

$$s^e = (i_1 \cdot i_2 \cdot \cdots \cdot i_l) \cdot t^{H(t,m)} \bmod n. \tag{2}$$

If it holds, the identity-based multisignature is valid, otherwise it is invalid.

From the above verification algorithm, we can see that for the proposed identity-based multisignature scheme, the number of modulo exponentiations is identical to Eq. (1), which is the same as the verification of the individual IBS. However, it does require $l - 1$ extra modulo multiplications. Since modulo multiplications are much more efficient than modulo exponentiations, they can simply be ignored. Therefore, the verification time of each multisignature is fixed.

4. Security analysis

In this section, we will analyze the security of our proposed identity-based RSA multisignatures from two aspects: multisignature forgery and multisignature specific collusion attack.

To prove that the proposed identity-based RSA multisignature scheme is secure against forgeability under chosen-message attack, we need to introduce a preliminary result from Bellare et al. (2004) and Fiat and Shamir (1986).

Lemma 1. *Shamir's identity-based signature scheme is secure against forgeability under chosen-message attack.*

Now we can present our main theorem below.

Theorem 1. *The proposed identity-based multisignature is secure against forgeability under chosen-message attack assuming one-wayness of the underlying RSA key generator K_{rsa}.*

Proof. To prove that for a chosen message m, it is computationally infeasible for the attacker to forger a multisignature for a set of signers $i_1, \ldots, i_n$, let $i = i_1 i_2 \ldots i_l$, then the multisignature verification Eq. (2) becomes

$$s^e = i \cdot t^{H(t,m)} \bmod n, \tag{3}$$

which is identical to Eq. (1). In other words, the proposed identity-based multisignature and the standard Shamir's identity-based signature scheme have identical forms. Therefore, according to Bellare et al. (2004), the proposed identity-based multisignature scheme is secure against forgeability under chosen-message attack assuming one-wayness of the underlying RSA key generator K_{rsa}. □

Now we will consider two multisignature specific security attacks. First, we need to introduce some new concepts. The *multi-signer collusion attack* refers to the attack that a legitimate group of message signers is trying to conspire and forge the multisignature of another group.

The *adaptive chosen-ID attack* is defined as the attack that a legitimate group of message signers is trying to adaptively choose their identities and obtain private keys from the PKG so that they can forger a multisignature for another group.

Theorem 2. *The proposed identity-based RSA multisignature scheme is secure against multi-signer collusion attack.*

Proof. For a group of signers, say $i_1, i_2, \ldots, i_l$, to generate a multisignature for another group, say $i'_1, i'_2, \ldots, i'_l$ in collusion, it requires that $i_1 i_2 \ldots i_l = i'_1 i'_2 \ldots i'_l \bmod n$. The probability for this identity collision is negligible. □

Theorem 3. *The proposed identity-based RSA multisignature scheme is secure against adaptive chosen-ID attack.*

Proof. For a group of attackers to forge a multisignature of another group of signers, say $i_1, i_2, \ldots, i_l$, the attackers can adaptively create a set of signers, say $i'_1, i'_2, \ldots, i'_l$, such that $i'_1 i'_2 \ldots i'_l = i_1 i_2 \ldots i_l \bmod n$ and obtain their private keys from the PKG. Then the group of attackers can forger a multisign nature of the group $i_1, i_2, \ldots, i_l$. Since the i_j, $j = 1, 2, \ldots, l$ are the message digest of the identities of the message signers, due to the one-wayness of the hash function, it is computationally infeasible for the attackers to derive the real identities for registration. □

5. Conclusion

We have proposed an efficient multisignature scheme based on Shamir's IBS scheme. Our scheme has constant signature length and verification time independent of the number of signers involved. The proposed scheme is secure against multisignature collusion attack, adaptive chosen-ID attack and forgeability under chosen-message attack.

REFERENCES

Bellare M, Namprempre C, Neven G. Security proofs for identity-based identification and signature schemes. In: Koblitz N, editor. Advances in cryptology – EurcoCrypt '04. Lecture Notes in Computer Science, vol. 3027. Berlin: Springer-Verlag; 2004. p. 268–86.

Boyd C. Digital multisignatures. Cryptography and Coding 1989: 241–6.

Chang C, Lee H. A new generalized group oriented cryposcheme without trusted centers. IEEE Journal on Selected Areas in Communications 1993;11(5):725–9.

Chaum D, Heyst Ev. Group signatures. In: Davies DW, editor. Advances in cryptology – EuroCrypt'91. Lecture Notes in Computer Science, vol. 547. Berlin: Springer-Verlag; 1991. p. 257–65.

Desmedt Y. Society and group oriented cryptography: a new concept. In: Pomerance C, editor. Advances in cryptology – Crypto'87. Lecture Notes in Computer Science, vol. 293. Berlin: Springer-Verlag; 1987. p. 120–7.

Desmedt Y, Frankel Y. Threshold cryptosystems. In: Brassard G, editor. Advances in cryptology – Crypto '89. Lecture Notes in Computer Science, vol. 435. Berlin: Springer-Verlag; 1989. p. 307–15.

Desmedt Y, Frankel Y. Shared generation of authenticators and signatures. In: Feigenbaum J, editor. Advances in cryptology – Crypto'91. Lecture Notes in Computer Science, vol. 576. Berlin: Springer-Verlag; 1991. p. 457–69.

Fiat A, Shamir A. How to prove yourself: practical solutions to identification and signature problems. In: Odlyzko AM, editor. Advances in cryptology – Crypto'86. Lecture Notes in Computer Science, vol. 263. Berlin: Springer-Verlag; 1986. p. 186–94.

Harn L. Group-oriented (*t*, *n*) threshold digital signature scheme and digital multisignature. IEE Proceedings – Computers and Digital Techniques Sept. 1994;141(5):307–13.

Harn L, Kiesler T. New scheme for digital multisignature. Electronics Letters 1989;25(15):1002–3.

Kohnfelder LM. On the signature reblocking problem in public-key cryptography. Communications of the ACM 1978;21(2): 179.

Kiesler T, Harn L. RSA blocking and multisignature schemes with no bit expansion. Electronics Letters 1990;26(18):1490–1.

Laih C, Harn L. Generalized threshold cryposystem. Advances in cryptology – ASIACRYPT 1991:159–69.

Micali S, Ohta K, Reyzin L. Accountable-subgroup multisignatures. In: ACM conference on computer and communications security; 2001. Available from: <citeseer.ist.psu.edu>, <ohta00accountablesubgroup.html>.

Pon S-F, Lu E-H, Lee J-Y. Dynamic reblocking RSA-based multisignatures scheme for computer and communication. IEEE Communications Letters 2002;6(1):43–4.

Rivest R, Shamir A, Adleman L. A method for obtaining digital signatures and public-key cryptosystems. Communications of the Association for Computing Machinery 1978;21(2):120–6.

Shamir A. Identity-based cryptosystems and signature schemes. In: Blakley GR, Chaum D, editors. Advances in cryptology: proceedings of crypto '84. Lecture Notes in Computer Science, vol. 196. Berlin: Springer-Verlag; 1985. p. 47–53.

Lein Harn is with the Department of Computer Science and Electrical Engineering, University of Missouri-Kansas City, MO 64110, USA. Email: harnl@umkc.edu.

Jian Ren is with the Department of Electrical and Computer Engineering, Michigan State University, East Lansing, MI 48824, USA. Email: renjian@egr.msu.edu.