Digital signature

I. Introduction

The main role of digital signature primitive is to preserve the data integrity of electronic document and to accomplish the requirement of authentication and verification. Only one signer using his/her private key generates an ordinary digital signature scheme. However, in some practical application, a document requires all group members to generate a signature together. These schemes are called digital multisignature schemes [2], in which all group members sign the same document by using their private keys. The multisignature scheme has three characteristics, refer to [2, 4]. For generating an efficient multisignature, the verification cost and the size of a multisignature might be almost as same as that of an ordinary signature.

In the past decade, several multisignture schemes were proposed based on the factorization, discrete logarithm problems or a combination of both. Moreover, there are a few schemes proposed based on the identity-based cryptosystem. A normal

multisignature scheme is called a multisignature with undistinguished signing authorities, as each group member has the same responsibility for signing the document. However, there are some situations when each member should have his/her own distinguished signing authority [4, 5, 7, and 15]. In this case, the multisignature scheme is called a multisignature scheme with distinguished signing authorities

For constructing a multisignture scheme with distinguished signing authorities, Harn [4] proposed the first scheme come out with this characteristic. In this scheme, each member only has his/her distinguished

signing responsible for his/her subdocument. The partial contents can be easily verified without revealing the whole message. However, Li et al. [9] claimed that Harn's scheme is not secure against insider attack. Moreover, Hwang et al. [7] pointed out that, in the Harn scheme, no evidence could be used to distinguish the signing authorities; this is due to the fact that all individual signatures and multisignatures are produced on the same hash digest of all the partial subdocuments. In the same paper, Hwang et al. [7] proposed a scheme based on the Harn scheme. In the expose, they claimed that their scheme overcomes the weaknesses of the Harn scheme. However, this is increasing the cost of generating multisignature. Huang et al. [6] proposed two multisignatures with distinguished signing authorities for sequential and broadcasting architectures. One year later, Yoon et al. [15] showed that Huang's scheme is unsecure since an attacker can derive a user's secret key and forge the multisignature of the scheme on arbitrary message. All of those schemes are based on the factorization or discrete logarithm problems or a combination of both.

In 1998, Shamir [12] introduced the concept of an identity-based (ID-based) cryptosystem to simplify the key management problem. In general, the main idea of identity-based cryptosystem is that the public key of a user is inferred from his/her identity. Each user needs to register at a private key generator (PKG) by identifying his/herself before joining the network. Later, the PKG will generate a secret key for that signer which is related to his/her identity. The secret key is sent to the user via a secure channel. Shamir proposed an ID-based signature (IBS) scheme from RSA primitive [11]. The

security of IBS was not proved or argued until Bellare et al. [1] proved that the IBS is secure against forgeability under chosen-message attack.

In the literature, there is only one ID multisignature with distinguished signing authorities for sequential and broadcasting architectures based on the identity-based cryptosystem. Wu et al. [14] proposed two ID-based multisigntures with distinguished signing authorities, relying on the Wu's [13] ID-based multisignature scheme, which however is shown to be unsecure [8]. Chien [3] showed that Wu et al. [14] two ID-based multisignatures have the security weakness by two attacks; insider attack and partial document substitution attack. More recently, Harn [5] proposed a new efficient ID-based RSA multisignature relying on IBS. Their scheme has constant signature length and verification time independent of the number of signers. They proved that their scheme is secure against multisignature collusion attack, adaptive chosen-ID attack and forgeability under chosen-message attack.

In this paper, we propose an efficient ID-based multisignature with distinguished signing authorities based Harn's multisignature [5]. We modify the Harn's scheme to be suitable as a mutlisignature with distinguished signing authorities for broadcasting architecture. We use Wu's mechanism of generating a multisignature with distinguished signing authorities only for broadcasting architecture. We suppose that the signing group U1, U2,..., Ul , to l the number of signers, want to generate the multisignature for the document D which can be divided to meaningful subdocuments d1, d2,..., dl . The member Uj is only responsible for signing partial subdocumentdj, forj= 1, 2,..., l.

The rest of this paper organized as follows. In section 2, we review of Harn's multisignature scheme. Section 3, we describe our proposed scheme. The security analysis of the proposed scheme is discussed in section 4. The paper is concluded in section 5.

II. Review of Harn's efficient identity-based RSA multisignature

A. PKG keys

The PKG picks two random large primes, p and q by run probabilistic polynomial algorithm Krsa, then calculates n= p. q, after that chooses a random public key e such that gcde,∅n= 1 and computes the private key d= e-1 mod∅n.

B. Multisignature generation

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 ij, by generating a secret key gj, such that gj= ijdmod n.

2) Message signing

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

1. Chooses a random integer rj and computes

tj= rje mod n

2. Broadcasts tj to all the signers.

3. Upon receiving of tj, j= 1, 2,..., l, each signer computes

t= j= 1ltj mod n

and

sj= gj. rjh(t, D) mod n

4. Broadcasts sj to all the signers.

5. After receiving of sj, j= 1, 2,..., l the multisignature component s can be computed as

s= j= 1lsj mod n

The multisignature for a document D is σ= t, s.

C. Multisignature verification

To verify a multisignature σ= t, s of a document D of signers whose identities are i1, i2, ..., il one verifies the following:

se= i1. i2.... il . th(t, D) mod n (1)

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

III. Our proposed scheme

Our proposed scheme as same is the same as Harn's scheme in the model description which follows the model proposed in Micali et al. [10].

In our modification, there are two new players; a document issuer (DI) and a document collector (DC). The DI is responsible of dividing the document into l smaller subdocuments such that D= d1‖d2‖…‖dl and the DC is responsible of collecting the partial signature and issue the multisignature.

A. PKG Keys

The PKG picks two random large primes, p and q by run probabilistic polynomial algorithm Krsa, then calculates n= p. q, after that chooses a random public key e such that gcde,∅n= 1 and computes the private key d= e-1 mod∅n.

B. Extract Signer key generation

Through this algorithm, a signer collects his private key by dealing with PKG in two steps:

1. A signer submits his identity to ij 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 ij, by generating a secret key gj, such tha gj= ijdmod n.

C. Message signing

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

1. Chooses a random integer rj and computes

tj= rjemod n

2. Broadcasts tj, htj, djto all the signers and DC.

3. Upon receiving of tj, j= 1, 2,..., l, each signer computes

t= j= 1ltjhtj, dj mod n

H= h(t, D)

And generats hisher partial signature

sj= gj. rjH. h(tj, dj) mod n

4. Broadcasts sj to all the signers and DC.

5. DC verifies all partial signatures by holding the following :

sje= ij . tjH. h(tj, dj) (2)

5. After that for all sj, j= 1, 2,..., l the multisignature component s can be computed as

s= j= 1lsj mod n

The multisignature for a document D is σ= t, s

D. Multisignature verification

To verify a multisignature σ= t, s of a document D of signers whose identities are i1, i2, ..., il one verifies the following:

se= i1. i2.... il . tH mod n (3)

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

E. Correctness

s= j= 1lsj= j= ilgj. rjH. h(tj, dj) mod n

s= g1. g2…. gl . j= 1lrjH. h(tj, dj) mod n

se= g1e. g2e….. gle. j= 1l. rjH. e. h(tj, dj) mod n

se= g1e. g2e….. gle.[j= 1ltjhtj, dj]Hmod n

se= i1. i2…. in. tHmod n

IV. Security Analysis

Our proposed scheme is an efficient improvement on Hern's multisignature (IBMS), which is suitable to meet the property of distinguishing signing authorities. Therefore, the proposed scheme construct based on Shamir identity based signature (IBS) scheme. Without lost generality, both scheme are proved secure based on RSA cryptosystem, refer to [5], [12]. Our proposed scheme inherits the security aspects from its root schemes; therefore, those aspects are still applicable and approvable to our scheme.

Next, we will discuss some potential and essential attacks against our scheme.

Attack 1. An existential forgery under adaptive chosen-message attack, which an adversary attempts to forge a multisignature or a partial signature for a chosen document or subdocument adaptively without knowing any private key.

Essentially, the standard Shamir IBS scheme is secure against forgery under adaptive chosen-message attack, according to Berllare et al. [1]. Thus, it is easy to get the proposed scheme secure against this type of attack, due to both schemes having the same identical forms and assuming one-wayness of the underlying RSA crypotsystem.

Attack 2. The adaptive chosen-ID attack, which an adversary (adversaries) tries to adaptively choose identity (identities) and forge private key from the PKG, therefore, it can forge a multisignature or partial signature.

Harn et al. [5] introduced the concept of the adaptive chosen-ID attack and proved that their IBMS scheme is secure against this attack. Our scheme resembles Harn’s scheme, this result in our scheme also secure against adaptive chosen-ID attack.

V. Conclusion

We have proposed an efficient ID-based RSA multisignatures with distinguished signing authorities for broadcasting architecture based on Shamir’s IBS scheme and Hern et al. IBMS scheme. The proposed scheme is secure against forgeability under adaptive chosen-message attack and adaptive chosen-identity attack.