Generating A New Group Digital Signatures
Dr. Abdulameer Khalaf Hussein
Middle East University
abdulameer.hussain@yahoo.com

ABSTRACT

This paper presents a new method for generating group digital signatures. Because of the importance of digital signatures in electronic management of business’s documents, it is important to develop strong methods to enhance and authenticate business’s documents in electronic environment, especially in sensitive applications. Existing methods normally implement asynchronous encryption algorithms like RSA for producing such digital signatures but we extend the approach by introducing the concept of document’s context in order to group selected authenticated users to each context type. This scheme uses alternative steps for signing sensitive documents by classifying data according to their sensitivity such as classified, secret, or top secret data. The main property of this scheme is that the group signature is a combination of message group and context group signatures. Finally, this scheme generates group signatures with multiple public keys corresponding to group members instead of one public key for each group implemented in most other group signatures schemes.

Keywords: Digital signatures, Cryptography, Group Signature, Authentication.

1. INTRODUCTION

Digital signatures play an important role in recent technology for providing essential properties such as integrity, authentication and undeniability. In conventional digital signatures, such as RSA and DSA, the existence of a single signer is enough to produce a valid signature, and anyone can verify the validity of any given signature. Many alternative schemes to digital signature were proposed because of its importance. These variations of digital signature include blind signature group signature, undeniable signature etc and can be used in different types of applications. Chaum and van Heyst introduced the concept of group signatures which are a special type of digital signatures [1]. One of the most important properties of digital signature is its ability to sign people’s documents in a secure and efficient manner. In digital signature, it is very difficult to forge the signatures in spite of the ease of verifying the validity of the digital signature. Rivest was the first who constructed a digital signature based on anumber-theoretic assumption [2].

It is important to provide evidence of possession of documents especially in electronic political and commercial applications. A digital signature is analogous to an ordinary hand-written signature and establishes both of sender authenticity and data integrity assurance. There are two most popular public-key algorithms which can provide digital signatures: one is the RSA-type signature scheme [3], the security of which is based on factoring; the other is the ElGamal-type signature scheme [4], the security of which is based on the discrete logarithm problem over the finite field GF (p).

A group signature allows any member of a group to anonymously sign a document on behalf of the group. A user can verify a signature with the group public key that is usually constant and unique for the whole group. However, he/she cannot know which individual of the group signs the document. Many group signature schemes had been proposed [5, 6]. All of them are much less efficient than regular signature schemes. Designing an efficient group signature scheme is still an open problem. The recent scheme proposed by Ateniese et al. is particularly efficient and provably secure [7].

From the viewpoints of verifiers, only a single group public key is needed to verify group signatures. On the other hand, from the viewpoint of the signing group, its internal structure is hidden from verifiers while the signer’s identities can be revealed, if necessary. In virtue of these advantages, group signatures have many potentially practical applications, such as e-voting, e-bidding and e-cash etc. Group signatures have many potentially practical applications, such as e-voting, e-bidding and e-cash etc [8, 9].

After the construction of the first scheme, many group signature schemes had been proposed such as [10, 11, 12, 13]. Chen and Pedersen constructed the first scheme which allows new members to join the group dynamically, and suggested to use group signatures in e-bidding. Camenisch and Stadler proposed the first group signature scheme. This scheme can be used for large groups, independent of the group size [10].

Some general properties of group signatures are briefly introduced as follows [14]:

1. Anonymity: This property states that for any given signature it is more difficult to discover the identity of the actual signer except the designated group manager.
ii. Un-linkability: If there are two signatures, it is computationally difficult to determine whether the signatures generated by the same member or not.

iii. Unforgeability: Only registered members can sign messages on behalf of their group.

iv. Traceability: To identify the actual signer, the group manager or the authority institution is always able to open a valid signature.

v. Coalition-resistance: There is no colluding subset of group members can generate a valid signature that the group manager cannot trace.

Camenisch [15] introduced the presented the first efficient group signature schemes for large groups. The property of these schemes is the group public key and the length of signature is both of constant size. But, Mao and Lim [16] showed that the anonymity of the scheme was not guaranteed. Miyaji et al. proposed a fully functional over only known-order groups that are based only on discrete logarithm related assumptions. This group signature satisfied unforgeability, exclaudability, anonymity, traceability, unlinkability, and revocability. [17]

2. RELATED WORKS

In [18], a group digital signature technique using a digital signature algorithm and a challenge-response identification protocol was proposed to provide effective authentication. This algorithm is based on solving quadratic congruence, factorization, and discrete logarithm problems. Also, this proposed method is suitable for to microprocessor-based devices such as smart cards, computer systems, networks and control systems because of its simplicity, confidentiality, and fast processing speed. To enhance the efficiency of group signature schemes, a proposed efficient group signature scheme which adds some redundant bits to each divided message block. This procedure will lead to avoiding the conspiracy attack. The security of the proposed scheme is based on the difficulty of computing the discrete logarithm modulo for a composite number [19]. Anovel model of group signature scheme was proposed and introduced a new entity called User-Revocation manager. User-Revocation manager plays an independent role regarding user revocation which was previously covered by either Group manager or Issuing manager. This method extends the idea of the Camenisch-Groth scheme and presents an efficient revocation scheme where the cost of user revocation is smaller than that of the Camenisch-Groth scheme. We also discuss the details of our implementation [20]. In [21], a short group signature scheme was proposed in which signatures are approximately the size of a standard RSA signature with the same security. Security of this group signature is based on the Strong Diffie-Hellman assumption and a new assumption in bilinear groups called the Decision Linear assumption. Finally, another short group signature scheme for dynamic membership with controllable link ability had been proposed. This scheme can be used for various anonymity-based applications that require necessarily the link ability such as vehicular adhoc network, and privacy-preserving data mining. Furthermore, this scheme supports controllable link ability that yields a signature which is shorter than the best-known normal group signature [22].

3. PROPOSED DIGITAL SIGNATURES

The scheme in this paper uses RSA method to generate the proposed group digital signatures. First, the documents are classified according to their context type and document’s classification. Suppose that the set of context type is CX= {CX1, CX2, ..., CXn}, the set of users is u={CX1u1, CX1u2, ..., CX1un}. These context types and related information are explained in table1:

| Table1: Context Information Sample Table |
|-----------------|-----------------|-----------------|-----------------|
| Context type   | Users           | Private Keys    | Public Keys     |
|                |                 | Digital         |                 |
|                |                 | Representation  |                 |
| CX1            | CX1u1, CX1u2,   | DC11, DC12,     | EC11, EC12,     | DG1  |
|                | CX1u3           | DC13            | EC13            |      |
| CX2            | CX2u1, CX2u2,   | DC21, DC22      | EC21, EC22      | DG2  |
|                | CX2u3           |                 |                 |      |
| CXn            | CXnu1, CXnu2,...| DCnk            | ECnk            | DGn  |

Assume M denotes any message in each context type, e for public keys and d for private key. Therefore: Cn=CXMn^dk

The following steps are used to explain the digital signature generation:

i. Choose the context type and let it XC1.

ii. Select the proper key prime numbers assigned to XC1 and let them p1 and q1. Then the member of that generate n1 as follows:

n1=p1*q1. Then they must calculate θ (n1) as follows: θ = (p1-1) (q1-1).

iii. Generate the group digital signatures for each element in the set of authenticated users using the private key for each member as follows (which constitute the digital signatures group set SG):

C1 = M1^d mod n, C2 = M2^d mod n and C3 = M3^d mod n.

Therefore the group signature of the message is: SG = {C1, C2, C3}. 
iv. Generate the signatures of digital representation of context type DG1 as explained below:

\[ C_1' = DG_1^{d_1} \mod n \], \[ C_2' = DG_1^{d_2} \mod n \] and \[ C_3' = DG_1^{d_3} \mod n \].

The above formulas represent the group signature of the message context DG1 and can be represented as follows:

\[ SG' = \{C_1', C_2', C_3'\} \].

So, the resultant group signature is a combination of both message group signatures and the group context signatures.

v. These signatures sets are sent to the signature manager with the context type of that group. So the group signature appears as a block in the following form:

\[ SGF = [SG, SG', CX_1] \]. The signature manager sends this block to the receiver.

vi. At the recipient end, the receiver extracts the context type CX1 from table1 to find the corresponding users of this type in order to obtain their public keys. The receiver can examine each signature element and decrypts it by using the following procedures:

\[ M_1 = C_1^{e_1} \mod 77 = 18, \] \[ M_2 = C_2^{e_2} \mod 77 = 18, \] \[ M_3 = C_3^{e_3} \mod 77 = 18, \]

\[ DG_1 = C_1^{e_1} \mod 77 = 20, \] \[ DG_1 = C_2^{e_2} \mod 77 = 20, \] \[ DG_1 = C_3^{e_3} \mod 77 = 20. \]

vi. If the message \( M_1 \) matches the corresponding message and \( DG_1 \) is the same as the original \( DG_1 \) value stored in table1, then the group signature (SGF) is authenticated. If one or more signatures do not match the stored \( DG_1 \), then the group signature is rejected and considered unauthenticated. For example, if one user from another context type generates its own signature and considered it belongs to context CX1, and this signature will not match the corresponding DG corresponding to CX1, then the group signature is rejected. On the other hand, this user can generate an authenticated signature inside his/her context type. Note that table1 must be maintained at a sender side and receiver side in a secure form.

4. RESULTS

Suppose that the context is CX1, \( p1=7 \) and \( q1=11 \). \( n_1=p1*q1=7*11=77 \). \( \Omega(n_1)=(p1-1)(q1-1)=60 \). Select public keys for CX1. These public keys are:

\[ e_1=13, e_2=7, \text{ and } e_3=11. \]

Let the stored message \( M=18 \). Calculate private keys by using the equation (1):

\[ d_1=\text{inv}(13) \mod 60 = 37, \] \[ d_2=\text{inv}(7) \mod 60 = 43 \] and \[ d_3=\text{inv}(11) \mod 60 = 11. \]

To generate message signatures group, apply equation (2):

\[ C_1 = 18^{37} \mod 77 = 39, \] \[ C_2 = 18^{13} \mod 77 = 46, \] \[ C_3 = 18^{11} \mod 77 = 51. \]

Now, suppose that \( DG_1=20 \), then context group signature is:

\[ C_1' = 20^{37} \mod 77 = 48, C_2' = 20^{13} \mod 77 = 69 \] and \[ C_3' = 20^{11} \mod 77 = 20. \]

The signature group (SGF) is sent to signature manager with context \( C_1 \) as follows:

\[ 394651486920CX1. \]

The signature manager sends SGF to the receiver who recovers signatures groups to the stored message \( M \) by using equation (3) as explained below:

\[ M_1 = 39^{13} \mod 77 = 18, \] \[ M_2 = 46^{7} \mod 77 = 18, \] \[ M_3 = 51^{11} \mod 77 = 18, \]

\[ DG_1 = 48^{13} \mod 77 = 20, \] \[ DG_1 = 69^{7} \mod 77 = 20, \] \[ DG_1 = 20^{11} \mod 77 = 20. \]

The generated messages match the original \( DG_1 \), so the signature group (SGF) is authenticated. If one user from another context type performs the above steps, then the recovered digital representation of his/her own context type will not match the original \( DG_1 \) of CX1. For example, suppose that this user selects \( p_2=29 \) and \( q_2=61 \), then \( n = 29*61=1769 \). \( \Omega(n)=(29-1)(61-1)=1680 \) and select \( e=13 \). Let \( M=88 \) and \( DG_2=15 \).

In this case, the group digital signatures are generated as follows:

\[ C=88^{517} \mod 1769 = 552 \] and \( C'= 15^{517} \mod 1769 = 1303 \)

\[ M= 552^{13} \mod 1769 = 88 \]

\[ DG_1 = 1303^{13} \mod 1769 = 15. \]

In his example the \( DG_1 \) do not match the original \( DG_1 \) which equals to 20, so this signature is rejected and this user is considered unauthenticated one.

5. ANALYSIS

This scheme provides two important properties of the group digital signatures. First, the digital signature is only generated by the authenticated group. This selection is dependent on message classification secret, in other words, each group are only the parties who recover that message’s class. To provide the unforgeability property of digital signature, any member of each group cannot forge his/her
signature because the signature depends on context of the message which is agreed by all members and the final signature block $SGF = [SG, SG', CX_1]$ limits the forgeability of any member. The proposed group signature also leads to infeasible task of denial because each piece of member’s signature is stamped by a trusted signature manager before the next piece of signature is attached to the group signature block. The proposed group signature provides a highly coalition-resistance property in that there is no subset of groups can generate any valid signature without cooperation among other subsets and this signature is controlled and managed by the signature manager.

6. CONCLUSION

In this paper, the digital signature generated is different from the traditional RSA digital signatures. First, this method considers the context type of each document in order to classify them according to their sensitivity. So, this sensitive document is signed by a group of users designated for that context type. The benefit of this procedure is to sign this document by more than one user to prevent denial action of user’s signature which is a major problem in most digital signatures schemes. Second, in this method, we proposed an alternative procedure to solve this problem by first, the message is signed by a group of users and this set of digital signature is sent to signature manager who can be used to solve any disputes may be occurred. Another point in this method is using different public keys, private keys, and related digital representation for each context type, so this piece of information can be used by the receiver to compare the original digital representation which ultimately provides the validate decision of the signatures group. By using these additional parameters, the signature generation becomes more secure and strong authenticated signature. The security of digital signature is enhanced by using multiple private keys instead of one, so the signature includes more secure information depending on strong factorization problem. This may lead to deceiving any attack because of his/her trial will be tested among confused large area of information of private keys. Another important property of this group signature is the block signature contains signatures of both the message and the related context of that message. In this case, this system is the first that includes the context’s signature and that procedure leads to difficulty faced any opponent to discover the signature whether it is belong to the message or to the context.

REFERENCES


