Generation of Dynamic Group Digital Signature

Rajasree R.S.
Asst.Professor
Pimpri Chinchwad College Of Engineering
Pune-44

ABSTRACT

In todays world management of electronic documents is a very tedious job.As electronic documents are used for all the transactions the authentication of the document is very important. Digital signatures are the best methods to provide authenticity.Many existiing schemes for digital signatures are proposed..In this paper a scheme which can be used to authenticate a group of members has been proposed. The proposed scheme uses RSA algorithm. The existing scheme provides group signatures which are static. But the proposed scheme is dynamic. It allows the group members to dynamically join the group and revoke the group. The proposed work is efficient and secure for electronic transactions and even for cloud environment where authenticity is essential

Keywords

Digital signature, group signature, authentication, RSA, crypptography

1. INTRODUCTION

Organizations move away from hard-copy of documents to electronic-documents.Applications such as banking,stock exchange, online purchases increasingly emphasis on electronic transactions to minimize operation al costs. These electronic documents are generated in computers and transmitted in the network.Therefore it is necessary to protect and authenticate these document from malicious users .Traditionally paper documents are authenticated by hand-written signature.Similarly electronic documents can also be authenticated with the help of a signature called digital signature.

A digital signature is an authentication mechanism that enables the creator of the message to attach a code that acts as a signature.It can provide the function of hand-written signature and satisfies the goals of authenticity,integrity and non-repudiation.[1].For example, suppose John send an authenticated message to Mary .Consider the following disputes could arise.

1) Mary may forge a different message and claim that it came from John.

2) John can deny sending the message

Digital signatures, in particular are needed in such situations where the involved parties do not trust each other to some extent already.

A group signature is a variation of digital signature that allows any member of a group,for eg can be a group manager, 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. A group signature provides to be valid only if it provide anonymity to the user and traceability for the group manager.

A group signature should always satisfy the following properties:

- **Anonimity:**
  Any person other than the group manager should not be able to find the actual signer
- **Traceability**
  The group manager must be able to open a valid signature
- **Unforgeability**
  Any othe group member must not be able forge othe member's sign
- **Coalition resistance**
  No colluding subset of the group members should generate signature that the group manager cannot trace

2. RELATED WORKS

Digital Signature is the most ensuring technique to provide authenticity,integration and non-repudiation of the data whish is transmitted over the computer-network[1]. **Di**gital Signature was first developed by Dffie and Hellman[4] that provides authenticity of the data. 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). Chaum and van Heyst [3]introduced the concept of group signatures which are a special type of digital signatures with authentication and provides privacy of the signers gainst potential verifiers.Many Group signature schemes were proposed. Ateniese and Tsudik [5, 6] conducted some research on group digital signature. These schemes perform poorly against coalition attack. The first practical group signature was presented by Ateniese and Tsudik [5] in 1999 based on RSA strong assumption. This scheme was then bettered and proved in a formal model [11]. The weakness of this signature scheme was that revocation of members were not possible.In this paper we propose a dynamic signature generation scheme based on strong RSA algorithm[8] that allows the joining and revocation of members.The proposed scheme is secure and efficient and it can be used for all business transactions where group signatures are required. It is also well suited for cloud environment where data storage and Identity anonymization is a major issue. Threshold digital signature scheme were also proposed. These schemes are very useful for large bank transactions.The first (t,n) threshold signature scheme[11] was introduced by Desmedt and Frankel in 1991.

3. PROPOSED SYSTEM

There are situations in which a group manager must add new members to the group based on the applications.So it is necessary to generate a scheme that generates signatures dynamically.

In this paper we propose a dynamic group signature sheme that allows the joining of members to the group. The pro-

posed protocol uses RSA for preparing digital signatures. Most of the encryption techniques use mathematical operations to produce cipher text. Mathematical operations called one-way functions are well suited for this task. A one-way function is easy to do in one way direction ut harder to do the reverse operation. RSA system uses complex natured one-way functions to do this. It is unbreakable and is the most suited for digital signatures. Our proposed protocol uses the following algorithms.The manager initially shares a secret key with the receiver. This key is called as the secret group key *gpk.* The manager initially issues a registration list which is empty. All the group members should first register with the group manager by issuing their ID.

3.1 Key Generation

The key generation algorithm GKg run by the group manager generates the public key *e[i]* and private key d[i] for each member of the group.The public and private keys are calculated as follows.

(i)Select two random prime numbers p and q for each user.

(ii) calculate n=p*q and Φ(n)=(p-1)(q-1)

(iii) Select a random number e such that GCD(e,n)=1 which is the public key

(iii)Select the private key such that e*d mod Φ(n)=1

Thus the public and private key pairs(e,n)and (d,n) for each user is calculated .The private keys are given to each user for the signature generation purpose whreas the values of p and q which are used for creating the signature is kept secret.

3.2 Signature Generation

The signature generation algorithm takes as input the secret key d[i], generated as a result of key generation protocol and a message m and outputs a signature σ.

In our proposed protocol we employ RSA algorithm for signature generation**.** The signature σ is generated by

$$\sigma\,[i] = M^{d[i]} \bmod n \qquad (1)$$

Thus the signature generated for each user in the group.

3.3 Signature Verification

The validity of the created signature by each user is verified using the verification algorithm**.**The signature verification algorithm takes as input the public key e[i] message m and the signature σ.

$$\textbf{If} \quad \sigma^{d[i]} \bmod \Phi(n) \qquad (2)$$

when calculated for each user gives the same result as that of the message then the users are valid.

The strongest point of this algorithm is that any other user who has the knowledge of the public key as well as the value of Φ(n) cannot sign the message .Because the strong factorization property of RSA algorithm it is not possible for him to calculate the value of p and q even if the value of Φ(n) is known.

After the verification of the signatures of group members ,the group manager removes the signatures from the message and attaches his own signature.Now the original message is send along with the signature of the group manager. This protocol also provides tracability of the group members by the group manager.

At the receiving end the signature of the group manager is verified by the receiver with the help of the key gp_k that is shared between the group manager and the receiver.

In addition to this algorithms, dynamic group signatures offer a protocol called **Join.**This protocol is executed between the group manager and the member of the group

3.3.1 Join Protocol

The group mansger maintains a registration list which is initially empty.The join protocol is executed for each memember of the group who wishes to join the group.It takes as input the identity of the user. After execution of this protocol,the group member receives the secret key for signing and the group manager receives some secret information that is needed to open the signature.A trapdoor commitment scheme as explained in [7][8]enhances the strength of the join protocol wherein the user is registerd by the manager but he himself does not know the private key of the user. The upper bound for the number of users is also defined by the .group manager

3.3.2 Revoke Protocol

If any member wants to withdraw from the group,group manager executes the REVOKE procedure and updates the information in the information table.The revoked member can no longer use the signature to sign the documents.Every time whenever the group manager recives the signed message from the group members the group manager first verifies the identitiy of the user by checking in the registration list.If the identity of the user proves to be valid then he considers the signature as valid. A user who is revoked from the group cannot use his old identity to validate himself.

4. CONCLUSION AND FUTURE WORK

In this paper we have proposed a dynamic digital signature scheme that allows the members to join and revoke the group.In this method a message cannot be send to the receiver directly by the group member.Thus it ensures security. Moreover it maintains the traceability of the members by the group manager.The security of the scheme is enhanced by providing different private keys for different users and is difficult to break because of the strong factorization problem.Thus the scheme provide to be more secure and efficient one.

5. REFERENCES

[1] H. Zhu, D. Li, "Reseach on Digital Signature in Electronic Commerce," The 2008 IAENG International Conference on Internet Computing and Web Services, HongKong,2008,pp. 8

[2] N. Asokan, V. Shoup, and M. Waidner, "Optimistic fair exange of digital signatures," in Proc. EUROCRYPT'98, 1998, vol. 1403, LNCS, pp. 591–606, Springer-Verlag

[3] D. Chaum and E. van Heyst. Group signatures. In:Advances in Cryptology - EUROCRYPT' 91, LNCS 950, pages 257-265. Springer-Verlag, 1992

[4] W. Diffie, M. Hellman, "New Directions in Cryptography," IEEE Transactions in Information Theory, vol. It-22, no. 6, 1976.

[5] G. Ateniese and G. Tsudik,."A coalition resistant group signature scheme" Technical Report, in Submission, 1998.

[6] G. Ateniese and G. Tsudik, "Group signatures á la carte," in Proceedings of the ten-th annual ACM-SIAM symposium on Discrete algorithms, pp. 848–849, 1999.

[7] Kiayias and M. Yung, "Group signatures: Provable security, efficient constructions and anonymity from trapdoor-holders," IACR

[8] Using the RSA Algorithm for Encryption and DigitaSignatures:Can You Encrypt, Decrypt, Sign and Verify without Infringing the RSA Patent? Patrick J. Flinn and James M. Jordan III (c) 1997 Alston & Bird LLP July 9, 1997 anonymity from trapdoor-holders," IACR

[9] "Generating A New Group Digital Signatures",Dr. Abdulameer Khalaf Hussein ,Journal of Emerging Trends in Computing and Information Sciences

[10] Rajasree R.S. , "RSA Based Solution For fair Contract Signing"International Journal of Engineering Research and Technology, Vol. 1, Issue 8.

[11] Desmedt, Y. and Frankel Y.(1991).Shared Generation of Authenticators and Signatures. In
Advances in Cryptology –Crypto -91, Proceedings. p.p. 457-469. New York: Springer Verlag