A Dynamic Threshold Proxy Digital Signature Scheme by using RSA Cryptography for Multimedia Authentication

Sharavanan Thanasekkaran and Balasubramanian V
Department of Computer Science and Engineering
SSN College of Engineering,
Chennai, Tamil Nadu, India

ABSTRACT
In this paper we propose a threshold digital signature scheme by using RSA cryptography to authenticate multimedia content. Multimedia authentication deals with genuineness of the structure and content of the multimedia such as text, image, audio, video etc. The proposed scheme uses an efficient key distribution scenario where, the private key of the group is distributed as unique shares among the group members. The shares are calculated and distributed based on the ID of the group members by using efficient Shamir's secret sharing scheme. For convenience the group members can be dynamically added or deleted. The private key of the group is updated if there is any violation in the threshold limit *t* due to variation of the number of group members in the group. The signer in the group will be able to reconstruct the private key from *t* or more shares given by the group members to sign the multimedia document. In this scheme any *t* or more group members can cooperatively generate the group signature where *t-1* or fewer cannot do it. This scheme is also secure against conspiracy attack.

Keywords
Digital Signature, Threshold Signature, Multimedia Authentication, RSA, Secret Sharing.

1. INTRODUCTION
In recent times, the usage of multimedia data and its exchange have increased enormously. In order to ensure trust worthiness, multimedia authentication technique [1] is to be used. It protects multimedia data by verifying the information integrity, the alleged source of data and the reality of data. The multimedia data includes text documents, images, video, audio clips, etc. We propose a multimedia authentication technique using RSA threshold digital signature. It deals with proving the genuineness of the structure and also on the content of multimedia data.

In cryptography, a digital signature [2] or electronic signature scheme is a type of asymmetric cryptography. It will attach the attributes of the signer to the e-document. A valid digital signature gives a recipient reason to believe that the message was created by a known sender, and that it was not altered in transit. Digital signature schemes normally use two keys: private key or secret key and the public key. The private key is used to sign the multimedia document and the public key is used to verify the signature. The public key is usually exposed directly to the group members. The private key is securely shared as a secret among the group members. A digital signature scheme typically consist of three algorithms such as: (i) key generation algorithm which can be usually generated by the key distribution centre, (ii) signing algorithm used by the sender to sign the digital document and (iii) signature verification algorithm to verify the digital document send by the sender. The digital signature scheme provides authentication, integrity and confidentiality of the multimedia information.

The existing Digital Signature Scheme (DSS) [3] which is based on discrete logarithm problem can only be used for signature generation/verification and cannot be used for multimedia authentication purposes. Also the verification process is very slow. Hence, we propose a scheme based on RSA for key generation, generation/verification of signature and it can also be used for encryption.

In a *(t, n)* threshold proxy signature scheme [4] based on RSA, any *t* or more proxy signers can collectively generate a proxy signature while *t-1* or fewer of them cannot able to do it. The idea of threshold cryptography is to protect information by fault-tolerant distribution among a cluster of cooperating computers. The threshold proxy signature scheme uses the RSA cryptography to generate the group private and the public key for the group members. It gives the implementation and comparison of some threshold proxy signature schemes based on the RSA cryptography. It also specifies the proxy signature requirements such as secrecy, masquerade, non-repudiation of origin, time constraint etc [4-8].

Secret sharing scheme [9, 10] refers to the method of distributing a secret/private key among the group members. Each member will receive a unique share of a secret/private key. The secret shares are calculated based on a randomly generated polynomial. The secret can be reconstructed with a sufficient number of shares given by the group members. The shares are reconstructed by using Lagrange's polynomial. Individual shares are of no use on their own. The computed shares are given to the group member based on their ID.

The proposed technique addresses the above problems and enhances all the basic security requirements such as authentication, confidentiality, non-repudiation and message integrity with an efficient threshold digital signature scheme. The goal of multimedia authentication is to authenticate the content alone and the specific representation of the information is not taken into consideration. The secret sharing scheme used here is modified by calculating the individual shares based on unique ID given to the group members. For convenience the group members can be dynamically added and removed from the group. If a new member joins the group he will be provided

with a new share with his ID. The rest of the paper is organized as follows: Section 2 presents the proposed scheme. Section 3 analyses the security of the proposed scheme. Section 4 discusses future work and concludes the paper.

2. PROPOSED SCHEME

A threshold digital signature scheme based on RSA algorithm is presented in this section. The scheme can be used to generate the group private and public keys, signature generation and verification and for encryption and decryption process. This scheme consists of the following participants: (i) **Key Distribution Centre (KDC)** for generating the keys for the group members and distributes the keys based on the group members ID, (ii) **Signers** (group members) for creation and verification of the signature and (iii) **Signature Combiner (SC)** for receiving the signature and threshold verification. The group members have to register with the KDC in order to obtain the unique ID. The unique ID could be an IP address, system name, etc. The scheme has four phases as detailed below.

2.1 System Initialization phase

In this phase U_i stands for the original signer and U_1, U_2...U_t ...U_n stands for the n group members. N_i represents the public RSA modulus value for the group member U_i, such that $N_i = p_i \times q_i$, where p_i and q_i represents two large primes. Let d_i is the private key and e_i is the public key for the member U_i, such that

$$d_i \equiv e_i^{-1} \bmod \phi(N_i),\ \phi(N_i) = (p_i - 1) \times (q_i - 1)$$

Where $\phi(N_i)$ represents Euler's totient function, which is the number of positive integers less than N_i and relatively prime to N_i. The parameters e_i and N_i can be public. Let $H()$ represents a one way hash function and HI is the header information of the multimedia message, such as length, number of frames, pixel rate etc.

2.2 Key Generation Phase

Key generation is the process of generating the keys for cryptography. A key is used to encrypt/decrypt the information to be exchanged. Key Distribution Centre (KDC) is a part of cryptosystem intended to securely exchange the keys. The complementary keys for asymmetric cryptography for digital signatures are group private and public keys. KDC will generate the public and private key pairs based on RSA cryptography. The group private key $\{d_i, N_i\}$, which is known only to the signer used to create the digital signature. The group public key $\{e_i, N_i\}$, which ordinarily known and used by the party to verify the signature. The generated keys are distributed among the group members in a fault tolerant way. The public key is available to all the group members, whereas the private key is distributed as a secret among the group members.

2.2.1 Proxy Key Generation

U_i calculates the group proxy signing key D and the verification key E, where

$$D = d_i^{m_w} \bmod \phi(N_i) \ \text{ And } \ E = e_i^{m_w} \bmod \phi(N_i) \qquad (1)$$

Where,

$$m_w = (V + ID + r) \bmod \phi(N) \qquad (2)$$

V is the validity period of proxy signatures; ID is the identities of U_1, U_2... U_n and r is a random number. Finally U_i publishes the individual sub signature ($m_w, E, [m_w, E]^{d_i} \bmod N_i$).

2.2.2 Proxy Secret Sharing

The group private key D has to be shared as a secret among the group members. Shamir's Secret sharing scheme is used to share the secret among the group members. U_i selects a *t-1* degree polynomial,

$$f(x) = a_{t-1}x^{t-1} + \ldots + a_2x^2 + a_1x + a_0 \qquad (3)$$

Where a_0, a_1... a_{t-1} are random numbers. Calculate the signer's partial proxy signing key $k_i = f(ID_i)$ and send $[[k_i]^{d_i} \bmod N_i, k_i]^{e_i} \bmod N_i$ to the sender U_i.

2.2.3 Signature Generation Phase

2.2.3.1 Partial Signature Generation

Anyone in the group G intends to send the multimedia message M will send the message on behalf of U_i. Each signer uses the key k_i to generate the partial signature

$$s = H(M \,||\, HI)^{k_i} \bmod N_i \qquad (4)$$

Then U_i sends $\{[s_i, i]^{d_i} \bmod N_i, s_i\}$ to the signature combiner (SC).

2.2.3.2 Group Signature Generation

The SC will generate the proxy signature s_i from P_i and verifies the validity of the proxy signature by checking if $[s_i, i]^{d_i} \bmod N_i = (s_i, i)$ or not. If all proxy signatures are valid, then the signature combiner will construct the signature S as follows

$$S = \prod_{i \in G} [s_i]^{vG_i} \bmod N_i \qquad (5)$$

Where,

$$v = \prod_{ID_g, ID_h \in G, g > h} ID_g - ID_h \qquad (6)$$

And

$$G_i = \prod_{j=1, j \neq i}^{t} (-ID_j / (ID_i - ID_j)) \qquad (7)$$

Here, G_i is a factor of v. It is obvious that vG_i is an integer and the sender need not compute the inverse of

$$\prod_{ID_g, ID_h \in G, g > h} (ID_g - ID_h) \qquad (8)$$

The generated proxy signature is $\{v, s\}$.

2.2.4 Signature Verification Phase

Anyone in the group can verify the signature on behalf of the original signer U_i by the equation

$$S^E \bmod N_i = H(M \,||\, HI)^v \bmod N_i \qquad (9)$$

$$S = \prod_{i \in G} [s_i]^{vG_i} \bmod N_i$$

$$S = (\prod_{i \in G} [s_i]^{vG_i})^{e_i} \bmod N_i$$

$$S = (\prod_{i \in G} [H(M||HI)]^{d_i vG_i})^{e_i} \bmod N_i$$

$$S = ([H(M||HI)]^{v\sum_{i=1}^{t} d_i G_i})^{e_i} \bmod N_i$$

$$s = [H(M||HI)]^{vd_i e_i} \bmod N_i$$

$$S = [H(M||HI)]^{v} \bmod N_i$$

Thus, if equation (9) satisfies the condition then the signature is valid otherwise the multimedia message will be discarded.

3. SECURITY ANALYSIS

In the proposed scheme the private key *D* of the group is shared as a secret by using the Shamir's secret sharing scheme. According to this scheme no group of faulty servers (smaller than a given threshold) can reconstruct the secret information individually and the attacker will not be able to reconstruct the private key *D* until he breaks the RSA. Only *t* or more group members can reconstruct. Hence if there is any violation in the threshold limit then KDC will update the group private key *D*.

If the member newly joins the group he will get a new share of the secret based on the ID of the group member. If the member quits the group and also any violation in the threshold limit, the group private key *D* is updated. When the group member is removed from the group, the deleted information is informed to all the group members, so that he will not forge the group signature with his old private key share.

Without the individual secret key information k_i, no one in the group can create a valid individual signature on behalf of the original signer U_i. The invalid signer can be distinguished by verifying the equation (9). If the condition in this equation is true then the sender is authentic.

If a person not in the group masquerades the attack by generating partial signature, the SC can differentiate the actual signer using the equation (9). Then the SC can trace the actual signer from e_i.

An adversary may try to forge the group secret key *D*, if the partial signature in equation (4) is known. Based on the security of the RSA cryptography the adversary will not succeed, because it is computationally infeasible to obtain d_i from equation (4) and k_i to reconstruct the group secret key.

If the sender U_i intends to send a multimedia message to a single person, say U_n, he can sign the message with his secret key d_i and encrypt the message with e_n. So only U_n can decrypt the message with his secret key d_n and he only will be able to verify the message. The individual signature of the valid member U_i is undeniable where the public key of the group is unique.

Since the signer can check the validity of the multimedia message by verifying his identities included in the message, the SC cannot forge the *HI*, even though he could generate *HI* from a different multimedia message or a different multimedia message with different *HI*. It can be easily distinguished by computing *H (M||HI)* which will give different value at the verification side. Hence the *ID, M, HI* can trace back to find the identities of signers without revealing the secret values. Hence the authenticity of the sender, integrity of the multimedia message, and the security of the message from masquerader is assured.

4. CONCLUSION AND FUTURE WORK

In this paper, we introduce a threshold digital signature scheme which can be used for authenticating the sender and also the multimedia message. The scheme enjoys the dynamic property where the group members can dynamically join or remove from the group. The private key of the group is shared as a secret among the group. The person acting as a sender can reconstruct the private key and share the multimedia message by signing the document with the group private key. The group private key is updated when the threshold property violates. Each unique key shares and public key of the group members are distributed based on their ID. Thus the proposed scheme ensures the authenticity, integrity, non-repudiation and secret sharing for multimedia message.

Ongoing work focuses on testing the suitability of the proposed scheme in one of the following application scenarios: medical image archiving, imaging or sound recording of criminal events, accident scene capturing for insurance and forensic purposes, military intelligence.

5. REFERENCES

[1] Ching-Yung Lin and Shih-Fu Chang. 2003 Robust Digital Signature for Multimedia Authentication: A Summary in Info lab Technical Report Series, no. 17.

[2] N. Gupta Kailash, N. Agarwala Kamlesh, and A. Agarwala Prateek Digital Signature: Network Security Practices. ISBN 81-203-2599-0.

[3] Danni Liu, XingweiWang, Lei Guo, and Min Huang. 2007 A Dynamic (t, n) Threshold Signature Scheme with Provable Security in IEEE International conference on Future Computer and Communication, pages V3–322–V3–325.

[4] Raman Kumar and Harsh Kumar Verma.2010 An Advanced Secure (t, n) Threshold Proxy Signature Scheme Based on RSA Cryptosystem for Known Signers in IEEE 2nd International Conference on Advance Computing Conference (IACC), pages 293–298, 2010.

[5] W. Xiaoming, Z. Zhen, and F. Fangwei. 2006 A Secure Threshold Proxy Signature Scheme in Journal of Electronics and Information Technology, 28:1308–1311.

[6] C. Wang, C. Chang, and C. Lin. 2000 Generalization of threshold signature and authenticated encryption for group communications in IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 83:1228–1237.

[7] G. Li, X. Xin, and W. Li. 2008 Digital Signature Scheme with a (t, l) Threshold Subliminal Channel Based on RSA Signature Scheme in proceedings on International Conference on Computational Intelligence and Security, 2:342–346.

[8] J. Lee. Threshold signature scheme with multiple signing policies in Proceedings-Computers and Digital Techniques, 148:95– 99.

[9] Adi Shamir. 1979 How to Share a Secret in Communications of the ACM, 22:612–613.

[10] Feng Shen, Chonglei Mei, and Hai Jiang. Secret Sharing with Extended Coefficient Use for Improved Data Capacity in IEEE SoutheastCon 2010, pages 119–122.