Discrete Logarithm based (t, n) Threshold Group Signature Scheme

Ganesh Mante
Computer Engineering Department
Bharati Vidyapeeth Deemed Univeristy College of Engineering, Pune 411043, Maharashtra, India

Prof.Dr.S.D.Joshi
Computer Engineering Department
Bharati Vidyapeeth Deemed Univeristy College of Engineering, Pune 411043, Maharashtra, India

ABSTRACT

Globalization of the Internet has boosted electronic information exchange on both the personal and business levels. There is a need of the authentication of messages sent by a group of individuals to another group. A (t, n) threshold group signature scheme is a method for allowing a member of a group to anonymously sign a message on behalf of the group. The idea of threshold cryptography is to protect information by distributing it among a cooperating member. Following some ideas of the classical threshold signature scheme, a (t, n) threshold group signature scheme and (k, m) threshold group signature verification scheme based on discrete logarithm problem is proposed. The group signature is generated by at least t group members and is verified by at least k members in the group. Only one group public key is required. Each group member separately signs the message. The scheme is highly secure and resists the conspiracy attack.

General Terms

Threshold Group Signatures, Security for Message

Keywords

Discrete logarithm, Group Signature, Galois Field, Polynomial, Signers, Threshold, Verifiers

1. INTRODUCTION

Traditionally to authorize the transactions done by corporation by the single person or group of persons is designed and implemented by software control defense mechanism. But considering the security threats in the highly popularized internet and mobile world above schemes are not satisfactory. Many cryptographic techniques are used to solve this problem. If the secret is kept with the single entity, it may cause the malicious damage to the system and there may also be the problem of availability. To overcome such problem the concept of threshold cryptography can be used in which the secret is distributed. Secret sharing refers to method for distributing a secret amongst a group of participants, each of which is allocated a share of the secret. The secret can be reconstructed only when a sufficient number of shares are combined together; individual shares are of no use. There are three main objects while designing a secure application:

Confidentiality: This can also be called privacy or secrecy and refers to the protection of information from unauthorized disclosure. Usually achieved either by restricting access to the information or by encrypting the information so that it is not meaningful to unauthorized individuals or entities.

Integrity: Assuring the receiver that the received message has not been altered in any way from the original. This can be thought of as accuracy. This refers to the ability to protect information, data, or transmissions from unauthorized, uncontrolled, or accidental alterations. The term integrity can also be used in reference to the functioning of a network, system, or application. Integrity is lost if unauthorized changes are made to the data by either intentional or accidental acts. To prevent the loss of integrity from happening, only authorized users should be allowed to modify data.

Authentication: Authentication serves as proof that you are who you say you are or what you claim to be. Authentication is critical if there is to be any trust between parties. Authentication is required when communicating over a network or logging onto a network. When communicating over a network you should ask yourself two questions: 1) with whom am I communicating? And 2) why do I believe this person or entity is who he, she, or it claims to be?

Nonrepudiation: The ability to prevent individuals or entities from denying that information, data, or files were sent or received or that information or files were accessed or altered, when in fact they were.

2. LITERATURE SURVEY

Threshold Cryptosystems has gradually been attractive since the proposal of the first threshold cryptosystem by Desmedt and Frankel in 1989.Numerous international studies had published research results and considerable researches were devoted to the threshold cryptography. Threshold signature cryptosystem is an important aspect of threshold cryptography, and represents almost the core of threshold cryptography research.

Li, Hwang and Lee [8] proposed the RSA based threshold signature scheme. In related research [8], it was pointed out that t+1 or t sub secret shareholders can conspire to obtain the system secret, and a conspiracy attack from the participants enables the conspirators to easily generate a group signature. The paper presents a technique where k out of l individuals is required to generate a signature for a message. This is clearly better than having each of the k individuals create k signatures which would cause an increase in bandwidth overhead. The receiver would also be required to perform more calculations and store a large key directory. No interactions between shareholders is necessary for the generation of signature and the secret key is not revealed to any individual even after signatures have been created .The scheme is based on RSA and interpolation polynomials. The scheme fails to withstand the conspiracy attack.

L.Harn [7] proposed a group oriented threshold signature scheme based on Elgamal System. In this scheme any t out of n users in a group can represent this group to sign the group signature. The size of the group signature and the verification time of the group signature are equivalent to that of an individual digital signature. The signature verification process is simplified because there is only one group public key required, the group signature can be verified by any outsider. In addition the scheme proposed does not require assistance of a mutually trusted party. Each member selects its own secret key and the group public key is determined by all group members. Each group member signs a message separately and sends the individual signature to a designated clerk. The clerk validates each individual signature into a group signature.

Li, Hwang and Lee [6] proposed two (t, n) threshold signature methods for resisting the conspiracy attack. One method required a trusted distribution center, while the other did not. These two methods resisted the conspiracy attack by attaching a random number to the sub-keys of all participants, such that the signatures could be protected against tracing from the sub-key. However these schemes failed to resist forgery attack from the internal participants.

Wang, Lin and Chang proposed two new (t, n) threshold signature methods [5].The proposed methods enabled the signers traceable but do not require the attachment of random numbers to sub-keys. The scheme can withstand conspiracy attacks without attaching a secret number. The group's public key is determined by all members, each member signs a message independently and transmits the individual signature to a designated clerk who checks and integrates them into a group signature. A verifier can authenticate the group signature and track back to find the signers.

Tsen, Jan and Chien [4] forged an attack to demonstrate the insecurity in the methods by Wang [5].They summarized the concepts of the attack and created a new threshold signature system that withstands conspiracy attacks [4].The system is a signer-untraceable method against conspiracy attacks, where required two sets of keys, one depended on the discrete logarithm problem and the other on the dissolution of the large integer problem. Both of which attempted to prevent the system participants from conspiring to obtain the system signature key. In reality, the method disabled to prevent the sub-key holders from conspiring to obtain system secrets, and it thus failed to resist conspiracy attack.

Related to the research of threshold signature cryptosystem, the method of [4] by Jan is briefly described in [3].Besides the attack the way to improve the scheme is examined. Later on many threshold group signature schemes with and without trusted party [1] have been proposed. But many of them face the problems of conspiracy attack or insider forgery attack.

Based on the study of above research an attempt to implement the threshold group signature library is proposed [2].In this paper [2] we have modified the scheme at group signature generation and verification protocol. The scheme [2] is modified by using Shamir's secret sharing scheme for distributing the hash code among m members. When k or more members among m members comes together we can reconstruct the hash code. Using this hash code the group signature is verified. We are not considering the network delay so the algorithms can be executed on single machine. The scheme consists of (t, n) signing and (k, m) verifying. Till now any outsider could verify the group signature. Here in this scheme any m out of k can verify the message. If less then t and less than k members tries to sign and verify the signature signing and verifying is rejected. It can not only satisfy the properties of threshold group signatures, but also withstand the conspiracy attack. The scheme consists of six protocols:

– **KeyGen:** the group manager uses KeyGen protocol to generate system parameters and his master key.

– **Join:** a member runs join protocol, together with the group manager, to obtain a certificate as its group membership.

– **Sign:** a group member anonymously sign a message following sign protocol.

– **Verify:** a verifier uses verity protocol to check whether a signature is originated from a member in the group.

– **Open:** the group manager uses open protocol to find the original signer of a signature.

– **Revoke:** the group manager uses revoke protocol to exclude a group member.

3. PROPOSED THRESHOLD GROUP SIGNATURE SCHEME

Let p and q be two prime numbers satisfying$q|(p-1)$, and let $g = h^{(p-1)/q}\ mod\ p$, satisfying $g > 1$, where0 $< h <$ p.Suppose $U_s = \{U_{s1}, U_{s2}, \ldots U_{sn}\}$ is a set of n signers $U_v = \{U_{v1}, U_{v2}, \ldots U_{vm}\}$ is a set of m verifiers, and GM is a trusted group manager. In this scheme, GM acts to authenticate every participant's identity, including members in U_s and members inU_v. All n members in U_s share a group of secure parameters of p, q, g.Similarly all m members in U_v share a group of secure parameters of p, q, g.Let usi and uvj are the public identities of signers and verifiers. The parameters p, q, g of both groups are different.

3.1 Group Formation

This module is used to form the groups of either signer or verifier. The secure parameters p, q, g are generated after specifying the number of signers and threshold value .The public identities usi and uvj of every user is created and broadcasted for further computations. The parameters are generated by the head or authorized members of the group. And the parameters p, q, g of both the signers group and verifiers group are known to each other.

3.2 Key Generation Phase I

All members in $U_s$negotiate their communication keys as below:

According to the given threshold value$t$, every member of signer group secretly constructs a $t-1$ rank polynomial:

$$f_{si}(x) = f_{si,0} + f_{si,1}x + \cdots + f_{si,t-1}x^{t-1}\ \ mod\ q$$

where x is a randomly generated integer in range of q and $f_{si,t-1} \neq$ 0.Simultaneously, he randomly selects a secret nonzero integer d in $GF(p)$ .Then he computes $D = g^{d}\, mod\, p$ and $g^{a}\, mod\, p$ where $a = f_{si,l}\ mod\ p,\ (l = 0,1,..t-1)$. Then U_{si} computes $f(u)$ where $f(u) = f_{si}(u_{sj})$ and sends it toU_{sj} $(j = 1,2, \dots n)$. Every member computes $f(u)$ by putting public identity of other members in their polynomial .At last U_{si} broadcasts D and g^{a} in the set of U_{s}. When every member receives$f(u)$, they can verify its validity via the equation

$$g^{a}\, mod\, p = \prod_{l=0}^{t-1} (g^{\ fsi,l})^{\ usj}\ mod\, p$$

If the equation is true, then $f(u)$ is valid, otherwise invalid.

3.3 Key Generation Phase II

When all participants complete the Key Generation Phase I step every U_{si} computes his Private Key $X = \left(d + \sum_{j=1}^{n}(f(u)\, mod\, p)\right) mod\, p$,Public key $Y = gX\, mod\, p$, the group public key $YU=i=1nDi=1nga,0\ mod\, p$ and additional data $Y^{d}\, mod\, p$ and $D_{S}N = \prod_{i=1}^{n} D^{-1}\, mod\, p$where D^{-1} is the reverse of D in $GF(p)$. U_{si} then broadcasts his public key Y .With the same procedure as above, according to the given threshold k , all m verifiers in U_{v} could negotiate their own keys. Every U_{vi} $(i = 1,2 \dots, m)$ gets his own private key X , public key Y and their group public key Y_{U} .

3.4 Join

When all members in a group have negotiated their communication keys, they can subscribe their public keys and identity information to GM for register. After communication keys have been negotiated every $U_{s} = \{U_{s1}, U_{s2}, \dots U_{sn}\}$ sends (i, usi, D, Y) to GM to register via a secure channel. After GM has authenticated his identity, GM adds his public information into public key status list ofU_{s}. The structure of public key status list for U_{s} is as below:

Table 1: Public Key Status List of Signers Group

Serial number	Identity	Public data	Public key	Time-start	Time-end
i	usi	D	Y	Ti-start	Ti-end

Similarly, when all verifiers in U_{v} have negotiated their own keys, every $U_{v} = \{U_{v1}, U_{v2}, \dots U_{vm}\}$ sends (i, uvi, D, Y) to GM to register via a secure channel. After GM authenticates his identity, GM adds his public information into public key status list ofU_{v}. The structure of public key status list for U_{v} is as below:

Table 2: Public Key Status List of Verifiers Group

Serial number	Identity	Public data	Public key	Time-start	Time-end
i	uvi	D	Y	Ti-start	Ti-end

3.5 Individual Signature Generation

Among the n members in U_{s}, any t participants could sign a message M on behalf of the group U_{s}.Every $U_{s} = \{U_{s1}, U_{s2}, \dots U_{sn}\}$could generate his own individual signature as below:

Firstly, U_{si} randomly selects a secret integer w from$[1, q-1]$, and then he computes and broadcasts $W = g^{w}\, mod\, p$ and $z = g^{wd\sim}\ mod\ p$ where d isU_{si}'s secret random integer brought during the key generation and $d\sim$ is d 's reverse in $GF(p)$.After every U_{si} have received other participants' information through broadcast, he opens the document to be signed ,get the hash code of document and computes $r = \sum_{i=1}^{t} z\, mod\, p$and $s = Xah(M) - rwd^{\sim}\ mod\, q$, where $a = \prod_{j=1, j\neq i}^{n}\left(\frac{usj}{usj-usi}\right)$.At last U_{si} sends (usi, r, si) as his own individual signature on the message M, to the appointed group signature generator, for example,U_{s1}.

3.6 Group Signature Generation

After the appointed group signature generator, U_{si} , have received the individual signature (usi, r, si) of $U_{s} = \{U_{s1}, U_{s2}, \dots U_{sn}\}$ he firstly verifyU_{si}'s identity according to the public key status list of U_{S} .Then he verifies the received signature of members using the equation $D^{s} mod\, p\, W^{r} mod\, p = ((Y^{d}\, mod\, p)^{\ (h(M)a) mod\, q})mod\, p)$.

If the equation is true, U_{si} 's individual signature is valid, otherwise invalid. After the appointed group signature generator have received t valid individual signatures $(r, si)(i = 1,2, .. t)$ he computes $D_{SA} = \prod_{j=1, j\neq i}^{t} Yi^{\ ai}$ and $s = \sum_{i=1}^{t} s\ mod\ q$.

The group signature generator randomly selects a secret integer w from $[1, q-1]$ where q is parameter of verifier group and computes:
$B = g^{w}\ mop\, p$, $Wvi = D^{-w}\ mop\, p$, $Rvi = g^{Y**w}\, mod\, p\ (i = 1,2, .. m)$ .Instead of sending the

plain message the group signature generator generates a $k-1$ rank polynomial:

$$f(Wvi) = M' + c1\,x + \cdots + cn\,x^{k-1} \quad mod\ q$$

and send $f(Wvi)$ to all the m verifiers. The first constant of the polynomial contains the hash code. We have used here the Shamir's secret sharing scheme..At last he broadcasts the computing value $(B,\ (Wvi, Rvi)(i = 1,2, \dots m))$ the attachment information $(s1, s2, \dots st, us1)$ and the group signature on the message $M{:}\,\{Y_{U,}, r, s, D_{SA,}D_{SN}\}$.

3.7 Group Signature Verification

Among the m members in U_v, any k participants could verify a group signature on a message M on behalf of the group U_v. Suppose that the k verifying participants are $U_{v1}, U_{v2,\dots..}U_{vk}$. Firstly, with his own private key, every $U_{v1}, U_{v2,\dots..}U_{vk}$ computes $Evi = B^X\ mod\ p$ and submits $(uvi, Evi, f(Wvi))$to the appointed group signature verifier, for exampleU_{v1}.When the appointed group signature verifier, U_{v1} have received all $(uvi, Evi, f(Wvi))$ from k members he firstly verify U_{vi} 's identity.He verifies their Signatures using $g^{Evi} mod\ p = Rvi\ mod\ p$. And only when the equation is true, the Evi could be accepted as valid information. Then using LaGrange's interpolation he calculates the $M^{'}$.

$$M^{'} = \sum_{i=1}^{k} f(Wvi) \prod_{j=1, j\neq i}^{k} Wvj/(Wvj - Wvi)$$

And when $M{=}M^{'}$, he verify the equation $g^s r^r = (Y_{U,}\ D_{SA,} D\ _{SN}\ )^{\ h(M^{'})}$.Only when the equation is true, the group signature $M{:}\,\{Y_{U,}, r, s, D_{SA,}D_{SN}\}$ could be accepted as a valid group signature on the message$M$. After the group signature has been accepted as a valid group signature.

3.8 Open

According to the attachment information $(s1, s2, \dots st, us1)$of a group signature on the message$M{:}\,\{Y_{U,}, r, s, D_{SA,}D_{SN}\}$, GM could find the group signature generator U_{v1} .And then U_{v1} could find the t original signers according to the attachment information if necessary. And so every signer of a group can not cheat others successfully.

3.9 Revoke

To revoke one member from a group, the group manager modifies the end time of the member in public key status list and broadcasts the current public key status list. From then on the member could not participate in the group signing phase, but the former signature he has signed is still valid. The group needs to be reestablish again otherwise the group signature cannot be validated.

4. SECURITY ANALYSIS

The security of the proposed scheme is based on the difficulty to solve the discrete logarithm problem and difficulty to break Shamir's secret sharing scheme.

1. In key generation Phase I the members cannot send false $f(u)$ to other members within the group. This can be verified using the equation

$$g^a\ mod\ p = \prod_{l=0}^{t-1} (g^{\ fsi,l})^{\ usj}\ mod\ p$$

2. In threshold group signature generation the individual member cannot send false signature (usi, r, si) to the group signature generator. This can be verified using the equation

$$D^s mod\ p\ W^r mod\ p = ((Y^d\ mod\ p)^{\ (h(M)a) mod\ q}\ ) mod\ p)$$

3. If $t-1$ or less signers try to sign the message the group signature cannot be generated.

4. If $k-1$ or less verifiers try to verify the message the group signature cannot be verified.

5. COCLUSIONS

The security of the proposed scheme is based on the difficulty to solve the discrete logarithm problem and difficulty to break Shamir's secret sharing scheme which we have used in threshold group signature generation and verification. Instead of sending the plain message with group signature we have encrypted the message using AES which maintains the integrity property. We have taken the double hash code of message to be signed so there are no limitations for message size. When k or more members come together the hash code can be reconstructed using Lagrange's interpolation and then only the threshold group signature can be verified. We have introduced a scheme where at least t of n signers could cooperate to create a valid group signature on behalf of the group of signers. Similarly at least k of m verifiers could cooperate to verify a group signature on behalf of the group of verifiers.

6. FUTURE SCOPE

The scheme can be modified by using algorithms for generating the large prime numbers. We can also enhance the scheme without using the group manager as third trusted party. In this scheme the size of individual signature and group signature varies that can be modified by making the size of individual signature and threshold group signature same. The proposed scheme requires more additions, multiplications, exponentiations and division operations as no standard algorithms are used .The computation cost can be reduced by using standard algorithms.

7. ACKNOWLEDGEMENTS

I wish to thank all the people who gave me an unending support right from the stage the idea was conceived. I am also grateful to BVDU team for providing us with the setup for work, without which implementation was just impossible. I express my profound thanks to Prof.Dr.S.D.Joshi and Dr.S.H.Patil,Head of Department, BVDU College of Engineering,Pune who have guided and helped me in preparation of this paper .

8. REFERENCES

[1] J.V.Merve, D.S.Dawoud and S.McDonald,"A fully Distributed Proactively Secure Threshold –MultiSignature Scheme", *IEEE Transactions on Parallel and Distributed Systems*, Vol.18, No.4, 2007

[2] F.Li,J.Yu and H.Ju, "A new threshold Group Signature scheme based on discrete logarithm problem", *IEEE Eight ACIS International conference on software engineering, artificial intelligence ,Networking and Parallel Distributed computing*, 2007.

[3] Y.F.Chung.C.H.Liu, F.Lai and T.S.Chen, "Threshold signature scheme resistible for conspiracy attack", *IEEE Proceedings of the Seventh International Conference on Parallel and distributed Computing, Applications and Technologies*, 2006.

[4] J.Camenisch and A.Lysyanskaya, A signature scheme with efficient protocols, In SCN'02, LNCS 2576, 2002, pp. 268-289.

[5] D.Boneh, X.Boyen, and H.Shacham, Short group signatures, In Advances in Cryptology-Crypto'04, LNCS 3152, 2004, pp. 41-55.

[6] D.Boneh and H.Shacham, Group signatures with verifier-local revocation, In Proc. of the 11th ACM Conference on Computer and Communications Security (CCS 2004) , 2004, pp. 168-177.

[7] J.Camenisch and J.Groth, Group signatures: Better efficiency and new theoretical aspects, In Security in Communication Networks (SCN 2004), LNCS 3352, 2005, pp. 120-133.

[8] J.K.Jan, Y.M.Tseng, and H.Y.Chien, "A threshold signature scheme withstanding the conspiracy attack", *Communications of Institute of Information and Computing Machinery*, Vol.2, No.3, 1999.

[9] C.T.Wang, C.H.Lin and C.C.Chang, "Threshold signature schemes with traceable signers in group communications", Elsevier ,*Computer Communications,Vol 21, No.8*, 1998.

[10] C.M.Li, T.Hwang and N.Y.Lee,"Threshold multisignature schemes where suspected forgery implies traceability of adversarial shareholders", *Advances in Cryptology-Proceedings of EUROCRYPT '*94, LNCS, Vol.950, Springer –Verlag, 1995.

[11] L.Harn,"Group-oriented (t,n) threshold digital signature scheme and digital Multisignature", *IEEE Proceedings-Computers and Digital Techniques, Vol.141, No.5, 1994*.

[12] C.M.Li,T.Hwang and N.Y.Lee, "Remark on the threshold RSA signature scheme", *Advances in Cryptology-Proceedings of CRYPTO* '93,LNCS,Vol.773,Springer-Verlag, 1993.

[13] D.Chaum and E.van Heyst, Group signature, In advances in Cryptology-Eurocrypt, 1992, pp. 390-407.