A Disordered Multiple Group Signature Scheme Based on Discrete Logarithm

Hua Huang
Information technology and Creative Design Institute, Qingyuan Polytechnic, Guangdong, China

***Abstract*—Based on the SCR algorithm authentication and signature, the majority can be calculated in the preprocessing phase is completed, the higher the efficiency, safety lies in the difficulty of computing discrete logarithms. Based on this algorithm and the discrete logarithm theory, we designed a multi-disorder group signature scheme, with a strong practical. Finally, analysis of the safety and performance of this schemes.**

Keywords-discrete logarithms; multiple group signature; security

I. Meaning and Function of the Digital Signature

A digital signature is a one-way function by the packet to be transmitted to authenticate the source of messages for processing to obtain and verify whether the packets change an alphanumeric string. Digital signatures can be solved repudiation, forgery, tampering and posing problems, specific requirements: a sender can not deny afterwards signature packets sent, the recipient can verify the signature packets sent by the sender, the receiver can not forge the sender's message signature, the recipient can not send those packets part tampering, the network a user can not impersonate another user as a sender or receiver.

A. Digital Signature Algorithm

Currently the main use digital signatures are digitally signed using asymmetric encryption and symmetric encryption two algorithms.

1) Using asymmetric encryption algorithm for digital signature

a) Meaning algorithm: This algorithm uses two keys: a public key (public key) and private key (private key); were used for data encryption and decryption, that if the public key to encrypt data, only with the corresponding private key to decrypt; if the private key used to encrypt the data, only with the corresponding public key can decrypt.

b) Signing and verification process: First with the sender's public one-way function of a packet transform, digital signature, and then use the issue with annexed packets after a private key to encrypt the digital signature. The recipient with the sender's public key to decrypt the digital signature conversion to obtain a digital signature plaintext. Sender's public key is a trusted technology management body, the certification authority (CA: Certification Authority) published.

Recipient expressly obtained through a one-way function calculation, will also be given a digital signature, digital signature and then compare the two, if the same, then prove that the signature is valid, otherwise invalid.

This approach allows anyone with the sender's public key can verify the digital signature is correct. Because the sender's private key confidentiality, so that the recipient can verify the results to either reject the message, but also makes it impossible to forge signatures and messages modification packets, because the digital signature is the entire message conducted on behalf of a group of packets is characterized by fixed-length code, the same person for different messages will have different digital signature. This solves a bank check sent through the network, and the recipient may make changes to the amount of the check in question, but also to avoid the possibility of the sender to avoid responsibility.

2) Symmetric encryption algorithm digital signature

a)Meaning algorithm: Encryption and decryption keys used for symmetric encryption algorithms are generally the same, even if the difference may also be easily made of any one of them derive another. In this algorithm, encryption and decryption keys used by both sides to be kept secret. Since the calculation speed is widely used in large amounts of data such as file encryption, such as the RD4 and DES.

b) Signing and verification process: Lamport invented a symmetric encryption algorithm called Lamport-Diffie: the use of the number of bits (n) a packet of length is twice the keys A, to produce the signature authentication information, that is randomly selected number 2n B, by the this number of B 2n signature key once encryption transformation to give another set of 2n number of C.

Sender from the first packet of the packet M Start, check the i-th bit of M, if it is 0, take the key of A bit i, if it is one of the first to take the key A i + 1 bits ; until all the packets checked. Selected n key bits form the final signature.

When the receiver verifies the signature, is also the first from the beginning of the first order. If the message M, M if bit i is 0, it is considered the signature information in Group I is the first i-bit key of A If the key a 1 was the first i + 1 place; until all the packets verification has been completed, we get n key, because the recipient has a sender authentication information C, so you can use to get the n key to verify the authentication information to confirm whether the packet is sent by the sender.

Since this method is that it is signed by bit, as long as one is altered, the recipient will not get the correct digital signature, so the security is better, the drawback is: signature is too long (for packets to be re-signing compression can reduce the length of the signature); the signature key and corresponding authentication information can not be reused, otherwise very insecure.

II. MULTIPLE GROUP SIGNATURE

Research by the signature of the above figures that, for the message authentication and anti-repudiation, digital signature scheme is a more effective method. Sometimes more than a message to be signed, namely multi-signature[1].

With the requirements of various applications, group signature obtained academic attention following the Seoul group signature produced many variants, such as group blind signature, subgroup signature, threshold group signature, but these special group signature also can not meet the actual needs , such as when on a message that we in many cases the need for multiple signatures, some or all of the signature subject is a group, the multi-group signature[3][4] is what we need, but the domestic research in this area is still blank. It based on the discrete logarithm theory by introducing appropriate mechanisms designed a disordered multi-species group signature scheme, to ensure the efficiency of the situation, with high security and strong practicability.

A. Initialization

Multiple signature may be ordered, it may be disordered Based Scoresby Carolina algorithm[1][5] designed a multi-order group signature scheme, specific programs are as follows:

Assuming the message M will have n groups in the signatures are identified as P1, P2, . . , P_n. Signature Management Center SMC (Signature Management Center) is responsible for sending a message to be signed, the signature verification and coordination of the final signature to complete signature. SMC first choose two large prime numbers p and q, such that q is a prime factor of p-1, $q \geq 2^{140}$, $p \geq 2^{512}$, then choose a ($a \neq 1$), meet $a^q \equiv 1 \pmod p$, then select a a one-way hash function H: $Z_p \times Z \rightarrow \{0,1, \ldots, 2^{t-1}\}$ (t parameters as recommended t> 72)[1]. Finally SMC to p, q, a, H publicly for the various groups of participants used in the signing process. Each parameter in the signature of an internal initialization groups: select $N=\alpha\beta=(2k\alpha'+1)(2k\beta'+1)$, which $\alpha, \beta, \alpha', \beta', k$ is different from the large prime number, g is of order k, e and d is an integer, and $ed = 1 \bmod \varphi(N)$ wherein $\varphi(N) = (\alpha - 1)(\beta - 1)$, $\gcd(e, \varphi(N)) = 1$, h is a one-way Hash function, IDG administrator for the group GA identity information.

B. Join the Group Members and Generate the Key Pair of

Each participant has public and private keys, participants P_i (i = 1,2, . . . , n) to select a random number $S_i \in$ {1,2 . . . , q} as a private key Pi is then calculated $V_i = a^{-s_i} \bmod p$, Pi is the corresponding public key [2][5]. Each signer's public key to send it to the SMC to register all public and also public. Group public key (N, e, g, k, h, ID_G), the private key (d, α', β') for the group. et ID_A for the identity of the group members A, A random selection $k_A \in (0, k)$, calculation $y_A = g^{k_A \bmod N}$, y_A as the A's public key, the (ID_A, y_A) issued to G_A, G_A calculation $x_A = (ID_G y_A)^{-d} \bmod N$ and x_A transfer to A secret, the private key (k_A, x_A) of A is, at the same time (ID_A, k_A, x_A) save G_A.

C. Multi-Disordered Group Signature Scheme

That is, regardless of disorderly multisignature signature between the signer has, together to complete the signature of a message. For multi-signature in this way, in order to prevent malicious signatures delay and better prevent birthday attacks (Birthday attack) [5], SMC in addition to the signature process for a given time and verified by external identity code, and the x^i (with the first scenario x^i) generated jointly completed by the SMC and signer P_i. SMC randomly generated number n k^i ($0 < k^i < q$), then $E^i = H(k^i)$ is sent to P_i (i = 1,2, . . . n), a randomly selected integer r_i P_i after receipt of r_i ($0 < r_i < q$), calculated $x_i = a^{r_i E_i} (\bmod p)$ and sent to the x^i SMC. SMC is $x = x_1 x_2 \cdots x_n (\bmod p)$ calculated and $e = H(M, T_{start}, x)$ (start time of the signature identification) after the {M, e} circulated signer P_i (i = 1,2, . . . n).P_i calculated $y_i = r_i + s_i e (\bmod q)$ and the y_i and identity code back to SMC, the first time-out and authentication after SMC received and verified by the record yi continue waiting for the other signature that all overtime be verified upon arrival, and is calculated $y = \sum_{j=1}^{n} y_j (\bmod q)$ and $V = \prod_{j=1}^{n} V_j \bmod p$ and field by to determine whether the establishment of equality, if equality holds is recognized signature y.

Programme Proof: Euclid algorithm and the initial conditions of this article are:

$$x' = a^{y} V^{e} (\bmod p)$$

$$= a^{\sum_{j=1}^{n} y_j \bmod q} (\prod_{k=1}^{n} V_k \bmod p)^{e} (\bmod p)$$

$$= a^{\sum_{j=1}^{n} (r_j + s_j e (\bmod q)) (\bmod q)} (\prod_{k=1}^{n} V_k \bmod p)^{e} (\bmod p)$$

because $V_i = a^{-s_i} \bmod p$ and so $x' = x (\bmod p)$. programs have evidence.

III. SECURITY AND PERFORMANCE ANALYSIS

According Scoresby satisfied algorithm theory, the probability of cracking the algorithm is 2^{-t} (t for the security parameters and t> 72) [2]. Within each group, if each individual pseudo joint signature because of the complete (ID_j, x_j, y_j) ,saved in G^A, where j = {A, B,. . . }, $y_j = g^{k_j} \bmod N$ If you want to turn validation, such as $\tilde{k}_2 = s_2 x_j^{-r} \bmod N$ and $V = (ID_G)^r g^{s_1} s_2^e \bmod N$ the first calculation, check $g^{s_1} = V \tilde{k}_2^{-e} y_j^r \bmod N$ whether to set up to achieve, still have to face the problem of computing discrete logarithms. In the disordered multi-signature scheme, x_i is generated for each signer and co-signer participation by the SMC, so trying to solve x^i, r^i much more difficult than solving the discrete logarithm difficult.

From the above we can see the design process, adding time limits and identification mechanisms are based on the cost of traffic-consuming, but most are still calculated at the time of pretreatment, and increased computing basically on a linear level, will not bring a big impact on the efficiency of the signature.

IV. SUMMARY

In this paper, a digital signature algorithm to study A on the basis of design based on discrete multi-disordered group signature number, and the program has proved that with a strong practical in reality, should be in the application according to the specific needs of security-related data handling will be considered as a whole.

REFERENCES

[1] Bruce Schneier .Applied Cryptography (second Edition)[M]. China Machine Press.2000, (1):366-367.

[2] C.P. Schnorr. Efficient Signature Generation for Smart Card [J].Journal of Cryprology,1991,4(3):161-174.

[3] Anna Lisa Ferrara, Matthew Green.Practical Short Signature Batch Verification.[C] Proceedings of the The Cryptographers' Track at the RSA Conference on Topics in Cryptology,2009.

[4] B den Boer.A Boddelaers Collisions for the compression function of MD-5[C].In: T Helleseth Ed.Advances in Cryptology, Proc.Eurocrydt'93, Lecture Notes in Computer Science 765, New York: Springer-Verlag, 1994:293-304.

[5] Boneh D., Lynn B., Shacham H.Short signatures from the Weil pairing.[C] In : Boyd C. ed. . Advances in Cryptology-Asia-crypt. Lecture Notes in Computer Science 2248. Berlin :Springer,2001:514～532.