Elliptic Curve Public Key Algorithm Based on Fourier Matrix

Xiaopeng Yang[1]

1 Department of mathematics
Shaanxi Xueqian Normal University
Xi'an, 710100, China

***Abstract* — In order to meet the high performance requirements of modern e-commerce and e-government, an efficient hierarchical group-signature scheme is proposed. Firstly, in the program, elliptic curve signature scheme is improved to avoid time-consuming modular inversion and modular multiplication, to reduce the once-point multiplication, and to improve the efficiency of signature and authentication algorithms, and on this basis, a highly efficient group signature scheme is constructed, and at last, message rating scale is introduced, and an efficient hierarchical group-signature scheme based on elliptic curve is presented. The analysis shows that the program has greatly reduced the time of hierarchical group-signature and verification, and when compared with the existing programs, it has higher efficiency and safety, but also has the advantages of elliptic curves cryptography, suitable for smart systems with strong practicality.**

Keywords - hierarchical group signature; group signature; elliptic curve; authority; knowledge signature

I. INTRODUCTION

In 1991, the concept of group-signature [1] was firstly proposed by Chaum and Heyst, in a scheme of group-signature, any member of a group can sign the message representing the entire group, when a dispute arises, the group administrator can determine the signature's true identity. In most of the existing group signature schemes, it is assumed that group members have the same rights, but this does not solve the case often occurred in the e-commerce and e-government: the company's management members often need to perform competence within the duties, and only sign files within the scope of competence of their own. Min [2] firstly proposed the hierarchical group signature scheme that group members have varying signature authority, and any group member cannot make a valid signature for a message beyond their signature authority, and the verifier can verify the signature through disclosed message permission flag. The scheme uses bilinear pairings to construct an identity-based group signature scheme, and in the verification of signature, it requires power operation and multiple modular multiplication and point multiplication, but the efficiency of the program needs to be improved. Elliptic curve signature scheme is improved in this paper to avoid modular inversion and modular multiplication, to reduce the once-point multiplication, and to shorten the time of signature and verification, and on the basis of this elliptic curve digital signature, a highly efficient group signature scheme based on elliptic curve is constructed, and message rating scale is introduced.

The predetermined message level and the corresponding level are stored in this table, the signature ability of group members are endowed by the group administrator in accession of the group, and when a group member signs a message, the method of zero-knowledge is employed to prove the signature privileges that he is provided with. An efficient hierarchical group-signature scheme based on elliptic curve is presented, and the program has advantages of short key, fast speed, small storage space and small bandwidth, etc, applicable in intelligent systems.

II. PREPARATORY WORK

The definition and properties of group-signature scheme are shown in literature [3], and the definition and properties of similar hierarchical group-signature are as follows:

(1) SETUP: it can generate a public key Y of group and a secret key S of group administrator.

(2) JOIN: it is an agreement between the user and group manager, allowing users to become a new member of the group. Output of protocol is a group member's identity certificate and a corresponding secret key.

(3) AUTHORIZE: authority administrator (group administrator) builds message rating scale, and in accordance with a member' actual permissions, permissions are assigned to group members, and he can sign the corresponding message class $p_i = g^{x_i}$. This article will use the knowledge signature to prove the authority owned by a group member, and any members cannot sign beyond their competence, even their names are signed, the signature will not be recognized.

(4) SIGN: When a message m, a group member's identity certificate and secret key are entered, the group signature of the message m is output.

(5) VERIFY: When the message m, the message signature and public key Y of group is input, the judgment on the validity of signatures is output.

(6) OPEN: When the message m, message signing and group manager's secret key S are input, the signer's identity is output.

Hierarchical group signature should have the following properties, and its unforgeability is stronger than the

standard group signature, but has relatively weak unlinkability:

(1) Unforgeability: Without knowing the group members' private key or not available required authorization, any attacker cannot successfully forge a valid authorized group-signature.

(2) Anonymity: In addition to the group administrator, it is computationally infeasible for anyone to determine the actual signer of a given group-signature.

(3) Traceability: if necessary, the group administrator can open a signature to identify the signer and the signer cannot prevent the opening of a valid signature.

(4) Unlinkability: In the case without opening the signature, it is impossible to determine whether two distinct group signatures are signed by the same signer, but it is knowable whether two signatures are signed by the signer of the same rights.

(5) Exculpability: anyone, including the group administrator, cannot make a valid group signature in the name of the other group members.

(6) Coalition-resistance: it is unable to elect a valid group signature that cannot be tracked even if some group members collude together.

NOTE: If a right is only granted to a member, then multiple signatures signed with the permission are not unrelated, but the signature is still anonymous; if various distinct permissions can be granted to one member, then the signature of different rights signed by the same member cannot be excluded.

A. Knowledge Signature

Knowledge signature is that signer demonstrates to others that he knows a secret without divulging the secret itself in the non-interactive status, and knowledge signature is now widely used in the group signature. In this paper, the knowledge signature employed in this article is based on Schnorr structure [4-5].

Assuming $G =< g >$ is the cyclic group of order n, g is a generator of G, and y is an element in G. g-based the discrete logarithm of y is the smallest positive integer x to make $g^x = y$ truthful.

Definition 1 For $(c, s) \in \{0,1\}^k \times Z_n^*$, $c = H(m \| y \| g \| g^s y^c)$ is met, which is called knowledge signature of g-based message m discrete logarithm of element $y \in G$, indicated as $SKREP[(\alpha) : y = g^\alpha](m)$, if the secret value x = logg (y) is known, then such a signature is easy to compute. Randomly selected r, c and s can be calculated like this

$$c := H(m \| y \| g \| g^r)$$

$$s := r - cx (\mathrm{mod}\, n)$$

If the secret value x = logg (y) is unknown, the calculation of such knowledge signature is difficult. This article will use the knowledge signature to prove that the group members have some privileges, but do not leak the value at the same time.

B. Message Rating Scale [6-10]

Division of member privileges: a group can be conceived as an agency or organization, provided with the objective classification, able to construct a tree according to this objective rating. Each layer of the tree represents a privilege, and the tree can have numerous members, which is namely that different members may have the same rights, and the superior-subordinate relationship is mapped to the parent-child relationships of tree.

Distribution of rights: for permission manager in program, he can be the group manager or an independent third party, responsible for the message class table and distribution of privileges. Assumed that there s total of s permissions in group, supposing that cyclic group is G, order is q, and g is a randomly chosen generator of G. Permissions manager (This program is the group manager) chooses unequal number $x_1, x_2, \cdots, x_s$ from zq * randomly to calculate $g^{x_i} = p_i (i = 1, 2, \cdots, s)$, and this number of s corresponds to the permission one by one. In registration of a member, the group administrator assigns him appropriate x_i as his authority based on actual privileges of the members.

Division of message rating: the division of message rating is closely related to division of competence, if a group member is provided with permission sign x_i, then all message rating flags he can sign are $p_i = g^{x_i}$. Message division list is some of the data recorded, storing the message characteristics and the information of corresponding level. Certifier of signature can access these data records attaining the rank of the message, as shown in Figure 1.

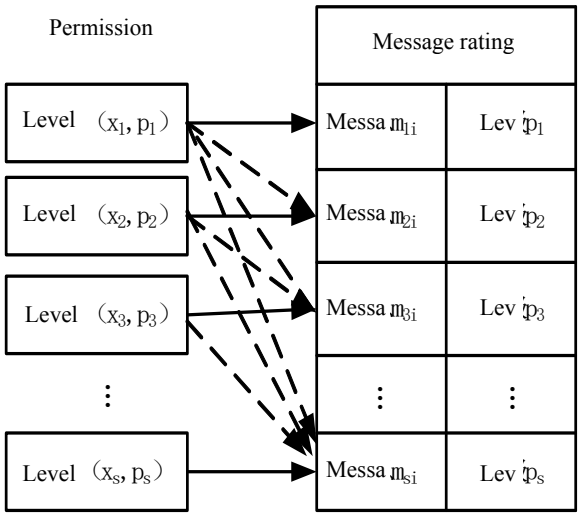

Figure 1. Message rating scale

In Figure 1, the privilege of the first grade is x_1; the privilege of the second grade is x_2; the privilege of the third

grade is x_3 . In group signature scheme of the paper, members x_1 with first grade permissions can generate a valid signature on the message m_{1i}. Solid lines in diagram show that the members with high level of competence cannot sign peer low-level message, because the distribution of competences set that messages of specific levels must be signed by members with specific permissions. Dashed lines in diagram show that: Senior members can be sign the lower level message, choosing the permissions assigned method according to the actual situation, and this program is only for the analysis of solid-line program.

III. ELLIPTIC CURVE DIGITAL SIGNATURE SCHEME AND ITS IMPROVEMENT

The most famous one in elliptic curve cryptography is Elliptic Curve Digital Signature Algorithm (ECDSA) [11], and this paper has improved ECDSA to avoid time-consuming inverse operation in its process of signature generation and signature verification, thereby increasing the speed of signature generation and verification to some extent.

A. *Elliptic Curve Digital Signature Algorithm (ECDSA)*

(1) System initialization phase

Step1: choose an elliptic curve E in the FP, and take a point P that belongs to E, with order of n;

Step2: Take integer $d \in [1, n-1]$;

Step3: Calculate $Q = dP$.

(2)Signature generation stage

Step1: Take integer k to make $k \in [1, n-1]$;

Step2: Calculate $kP = (x, y)$, $R = x \bmod n$, and if $R = 0$, then go to Step1;

Step3: Calculate $k^{-1} \bmod n$;

Step4: Calculate the hash value $e = h(m)$ of message, $S = k^{-1}(e + dR) \bmod n$. If $S = 0$, then go to Step1.

(3) Signature verification phase

Step1: Obtain public key (P, E, n, Q) to verify R、 $S \in [1, n-1]$;

Step2: Calculate $e = h(m)$;

Step3: Calculate $t = S^{-1} \bmod n$;

Step4: Calculate $u = et \bmod n$ and $u' = rt \bmod n$;

Step5: Calculate $uP + u'Q = (x_1, y_1)$;

Step6: Calculate $V = x_1 \bmod n$

Step7: Verify $V = R$, if it is truthful, the signature is valid, or the signature is invalid.

B. *Improved Elliptic Curve Digital Signature Algorithm*

(1) System initialization phase

Step1: Choose an elliptic curve E in the FP, and take point G that belongs to E, with order of n;

Step2: Take integer $d \in [1, n-1]$;

Step3: Calculate $Q = dG$

(2)Signature generation stage

Step1： Take integer k to make $k \in [1, n-1]$

Step2: Calculate $kG = (x, y)$, $R = x \bmod n$, and if $R = 0$, then go to Step1;

Step3: Calculate the hash value $e = h(m \| R)$ of message;

Step4： $S = k^{-1}(e + dR) \bmod n$. If $S = 0$, then go to Step1.

(3) Signature verification phase

Step1: Obtain public key (G, E, n, Q) to verify R、 $S \in [1, n-1]$;

Step2: Calculate $e = h(m \| R)$;

Step3： $X = (e - S)G + Q = (x_1, y_1)$;

Step3: $X = (e - S)G + Q = (x_1, y_1)$;

Step4: Calculate $V = x_1 \bmod n$

Step5： Verify $V = R$, if it is truthful, the signature is valid, or the signature is invalid.

C. *Correctness proof of improved algorithm*

If the signature (R, S) of message M is generated by legitimate signer, it is firstly to calculate

$e = h(m \| R)$

$S = (e + d - k) \bmod n$

Then $k = (e + d - S) \bmod n$. Hence:

$X = u_1 G + Q$

$= (e - S)G + Q$

$= eG - SG + dG$

$= (e + d - S)G$

$= kG$

Then $V = R$, that is, the signature is legitimate.

D. *Efficiency comparison of the program before and after improvement*

The modular inversion, modular multiplication and point multiplication are mainly considered in algorithm efficiency, and the others can be ignored, and the efficiency before and after improvement is as shown in Table 1.

TABLE I EFFICIENCY COMPARISON LIST OF THE PROGRAM BEFORE AND AFTER IMPROVEMENT

	Signature stage Computation	Validation phase Computation	Total
ECC Original ECC scheme	1 operation of modular inversion One operation of modular multiplication 1 operation of point multiplication	1 operation of modular inversion 2 operations of modular multiplication 2 operations of point multiplication	2 operations of modular inversion 3 operations of modular multiplication 3 operations of point multiplication
After improvement	1 operation of point multiplication	1 operation of point multiplication	2 operations of point multiplication

From the perspective of the computation of algorithm, if the data size of modular multiplication is n, the complexity of 1 operation of point multiplication is $O(n^2 \log_2 n)$, and that of 1 operation of modular multiplication is $O(n^2)$, and 1

computation of 1 modular inversion is equivalent to nine times of modular multiplication [12]. The above table shows that the total computation of the original elliptic curve digital signature scheme is 2 operations of modular inversion, 3 operations of modular multiplication, and 3 operations of point multiplication, and the total time complexity is $(3\log_2 n+21)n^2$. The total computation of improved elliptic curve digital signature scheme is: 2 operations of point multiplication, and the total time complexity is: $2n^2\log_2 n$. According to the table analysis available, the program avoids the time-consuming operations of modular inverse and modular multiplication, reducing the time point multiplication, significantly improving computing speed, shortening the time of signature and verification, and effectively improves the efficiency of the algorithm, thus this elliptic curve scheme is an efficient solution.

IV. HIERARCHICAL GROUP-SIGNATURE SCHEME BASED ON ELLIPTIC CURVE

Based on the improved elliptic curve, an efficient hierarchical group signature scheme is proposed.

A. System Initialization

System initialization is completed by the group administrator, and a large prime number p is taken, randomly chosen $a,b\in Z_p$ to construct an elliptic curve $y^2 = x^3 + ax + b$ meeting: points $\#E(Z_p)$ can be divided exactly by a large prime number $n(n\geq 2^{160})$, and a point G with order of n on $E(Z_p)$ is taken as a base point, and H is a safe Hash function. Ψ represents conversion of point $P(x,y)$ on an elliptic curve to x, denoted as $(P)_x$. Private group manager A takes a private key $k_A\in Z_n^*$, computing public key $K_A = k_A\mathrm{G}$, and private key saves private key, and the other parameters p, a, b, n, G, YA and H are all public.

B. Membership Registration and Authorization

Step1: New member B takes k_B randomly to calculate $K_B = k_B G$, in which private key is k_B, and public key is K_B, and then the status symbol ID_B of K_B and new member B is distributed to the group administrator A.

Step2: Group administrator makes random selection of $u\in Z_n^*$ to calculate $ID_C = H(u\,\|\,ID_B)G$, and the group administrator ends the secrets to the member B, and ID_C bounds identity of member B who then produces and publishes group signature with ID_C.

Step3: Group administrator saves the three elements of each new member, and namely, (ID_B, ID_C, u) is saved when a dispute arises, it can determine the true identity of the signer.

Step4: Group administrator randomly selects $v\in Z_n^*$ to calculate $V = vG\neq 0$

$$s_A = k_A H((ID_C)_x\,\|\,(V)_x) + v(\mathrm{mod}\,n)$$

Step5: Group administrator A sends (V, s_A) to B, while the group administrator gives appropriate user right to new member B, in which $p_i = g^{x_i}$, and the identity certificate for the new member is $(K_B, ID_C, V, s_A, (x_i, p_i))$.

C. Signature Generation

Step1: For the message m with rights of p_i, the group member B does the following operations based on their members' credentials and permissions:

Randomly select $r\in Z_n^*$ to calculate

$$\mathrm{R} = rG\neq 0$$

$$e = H(m\,\|\,(R)_x)$$

$$s = e + k_B - r\mathrm{mod}n$$

$$I = ID_C + ID_B + k_B K_A$$

$$\mathrm{SK} = \mathrm{SKREP}[(\alpha):\mathrm{p_i} = g^{\alpha}](m\,\|\,R\,\|\,e\,\|\,s\,\|\,I)$$

$$\sigma = (m, s, R, I, K_B, SK)$$

Step2: Group member B sends group signature: $\sigma = (m, s, R, I, K_B, SK)$ to verifier of signature.

D. Signature Verification

Step1: Verifier first inquires rating scale to attain the rank sign p_i of message m;

Step2: Certifier verifies the equation:

$s_{\mathrm{A}}\mathrm{G} = H((ID_C)_x\,\|\,(V)_x)K_A + V$,

If the equation is satisfied, it is proved that the signature is that signed by members of the group, or signature is refused.

Step3: Certifier verifies: $K_B = (s-e)G + R$. If equality holds, and $c = H(m\,\|\,p_i\,\|\,g\,\|\,g^s p_i^{\,c})$, then signature $\sigma = (m, s, R, I, K_B, SK)$ is received, or signature is refused.

E. Signature Open

When a dispute arises, group members' anonymity can be withdrawn to open signature to determine the true identity of the signer.

Step1: Group manager A computes

$E = I - k_A K_B$;

$F = I - ID_C - k_A K_B$;

Step2: Group manager A inquires three saved elements to find $F = ID_B$, $E = ID_B + ID_C$, and then ID_B is the real identity of the signer.

Step3: Group administrator sends (ID_B, u) to the verifier of signature to calculate $ID_C{}' = H(u\,\|\,ID_B)G$, if $ID_C = ID_C{}'$, it has proven the successful determination of the true identity of the group signers.

V. SECURITY ANALYSIS OF PROGRAM

A. Anonymity and Unlinkability

To determine the identity ID_B, the attacker, must be calculate ID_C =H(u||ID$_B$)G, facing problems of solving Elliptic Curve Discrete Logarithmic Problems (ECDLP) and one-way hash function. u is a parameter randomly selected by group administrator, and the attacker cannot determine the bound identity ID_C and real identity ID_B, and signature of group members is used to bind the identity ID_C. The attacker cannot determine the true identity of the signer, and therefore, the group signature scheme is featured by anonymity and unlinkability.

B. Unforgeability

Supposed that the attacker (attacker outside the group, group administrators, and other members of the group) would like to forge a signature, he must also know the random number r, signature key k_B, and user privilege x_i, in which the random number r is randomly selected with great difficulty in attack. Signature key k_B must be got through the calculation equation $K_B = k_B G$, which will be faced with ECDLP, thus the calculation is not feasible. In getting user permissions, $p_i = g^{x_i}$ must be calculated, which will face the discrete logarithm problem, and it is also infeasible computationally. In summary, the hierarchical group signature scheme has unforgeability.

C. Coalition-Resistance

If the group manager and other effective members in the group want to forge signatures jointly, they must know the signature secret key k_B and random parameter r, and Elliptic Curve Discrete Logarithmic Problems will be faced with in the calculation, which is computationally infeasible, so the program is characterized by coalition-resistance.

D. Traceability and Non-Repudiation

When a dispute arises, the group administrator can determine the true identity of the group members by calculating $E = I - k_A K_B$ and $F = I - ID_C - k_A K_B$, thus the anonymity is trackable, and the signer is undeniable for his own signature.

E. Arrogation-Resistance

All group members would like to produce a valid signature message beyond their own authority, and apparently, what he faces is the generation of correct knowledge signature *SK* and problems of discrete logarithm. Therefore, the program cannot produce a valid signature on the message beyond one's competence.

F. Performance Analysis and Comparison of Program

Next, a comparison is made between the proposed scheme and the existing hierarchical group-signature scheme, and in the comparison process, it only considers computationally intensive point multiplication, standard multiplication, pairing operation, for other operations have no big influence on the computation of the whole program, and therefore, they can be negligible. Computation in signing process of hierarchical group-signature scheme in literature is as follows: 1 operation of point multiplication, 10 operations of multiplication; calculation in process of signature verification is: 3 pairing operations; the calculation in process of signature open is: 3 pairing operations. Therefore, the total calculation is as follows: 1 operation of point multiplication, 10 operations of multiplication, and 6 operations of bilinear pairings. The calculation in signature process of new program proposed is: 1 operation of point multiplication and 1 operation of multiplication; the calculation in process of signature verification is: 2 operations of point multiplication, and 1 operation of multiplication; the calculation in process of signature open is: 2 operations of standard multiplication. Therefore, the total operation capacity of the new program is: 3 operations of point multiplication, and 4 operations of multiplication. As shown in Table 4.3 in the literature, when the embedding degree k = 6, the big prime number | r | = 160, the bilinear algorithm efficiency of Tate is 54758 operations of point multiplication. The computation of hierarchical group-signature scheme in literature [25-27] has far surpassed the proposed new program, and it thus can be seen that the new program saves a lot of computing time with high efficiency. In addition to the accession of permission rating scale and the authority proof of knowledge signature, this does not have much effect on the efficiency of the program, and the program is based on elliptic curves, thus the program is also provided with advantages of short key, high efficiency, small storage space and little demand for broadband, and less system overhead, etc.

VI. CONCLUSIONS

Based on improvement of elliptic curve group-signature scheme, the signature algorithm and authentication algorithm in this paper have avoided the modular inverse and modular multiplication, reducing the time of once-point multiplication, and improving the efficiency of signature program and verification algorithm, and by introducing permission rating scale, this paper has proposed an efficient hierarchical group-signature scheme based on elliptic curve, and compared to existing programs, they have significantly reduced the computing time with small amount of calculation and fast processing speed, and also have virtues of high safety performance, small memory footprint, and low requirements for bandwidth. In addition, the scheme has resolved specific application environment with strong practicability, and has a wide range of applications in intelligent systems.

The authors confirm that this article content has no conflicts of interest.

REFERENCES

[1] Alex Tek, et al. "Advances in Human-Protein Interaction-Interactive and Immersive Molecular Simulations". InTech, 2012.

[2] Gangyi Zhu, et al. “SciCSM: Novel Contrast Set Mining over Scientific Datasets Using Bitmap Indices”. In Proceedings of the 27th international conference on scientific and statistical database management, ACM, 2015.

[3] Guanxiong Liu, Yishuang Geng, Kaveh Pahlavan, “Effects of calibration RFID tags on performance of inertial navigation in indoor environment”, 2015 International Conference on Computing, Networking and Communications (ICNC), Feb. 2015

[4] Jie He, Yishuang Geng and Kaveh Pahlavan, “Toward accurate human tracking: modelling time-of-arrival for wireless wearable sensors in multipath environment”, IEEE Sensor Journal, vol. 14, No. 11, pp. 3996-4006, 2014.

[5] J. He, Y. Geng and K. Pahlavan, “Modeling Indoor TOA Ranging Error for Body Mounted Sensors”, 2012 IEEE 23nd International Symposium on Personal Indoor and Mobile Radio Communications (PIMRC), Sydney, Australia Sep. pp. 682-686, 2012.

[6] Jie He, Yishuang Geng, Yadong Wan, Shen Li, Kaveh Pahlavan, “A cyber physical test-bed for virtualization of RF access environment for body sensor network”, IEEE Sensor Journal, vol. 13, No. 10, pp. 3826-3836, 2013

[7] Liguo Zhang, et al. “Double Image Multi-Encryption Algorithm based on Fractional Chaotic Time Series”. Journal of Computational and Theoretical Nanoscience. 2016.

[8] Na Lu, Caiwu Lu, Zhen Yang, Yishuang Geng, “Modeling Framework for Mining Lifecycle Management”, Journal of Networks, vol. 9, No. 03, pp. 719-725, 2014

[9] MA, Ruina, Zhihan LV, Yong HAN, et al., “Research and implementation of geocoding searching and lambert projection transformation based on WebGIS”. Geospatial Information, vol. 5, pp. 013, 2009.

[10] Shuang Zhou, Liang Mi, Hao Chen, Yishuang Geng, “Building detection in Digital surface model”, 2013 IEEE International Conference on Imaging Systems and Techniques (IST), Oct. 2012

[11] Song Yu, et al. A Rapid and High Reliable Identify Program for Nighttime Pedestrians.infrared physics & technology. 2015

[12] Tianyun Su, Zhihan Lv, Shan Gao, Xiaolong Li, and Haibin Lv. 3D seabed: 3D modeling and visualization platform for the seabed. 2014 IEEE International Conference on Multimedia and Expo Workshops (ICMEW). pp. 1-6. IEEE, 2014.