A threshold proxy blind multi signature scheme based on bilinear pairings

Zemei Chen ,Guocai Wang

School of Information Science and Engineering ,CSU

Changsha ,China

***Abstract**--The scheme combines a threshold proxy multi signature scheme and a blind signature one, it does not only distribute the power of the proxy signers ,but also realize the anonymity and non-trail in signature by using a blind signature scheme. Based on this new method, and using bilinear pairings ,a threshold proxy blind multi signature scheme based on bilinear pairings is presented. Because of using bilinear pairings ,the security and the speed of threshold proxy blind multi signature have been greatly enhanced.*

Key words--Bilinear pairings ; Threshold proxy signature ; Multi signature ; Blind signature

In 1982,Chaum first introduced a conception of blind signature which allows the sender to have a given message signed by the signers without revealing any information about the message or its signature. So it has a major application value in areas such as Electronic commerce ,Numeral cash and Electronics vote .

In realization of the digital signature, people often delegates his/her signing capability to a responsible agent for some reason ,and allows the agent to sign on his/her behalf .Also ,in the realistic world ,it is frequently taken place that several signers delegate their signing capabilities to a group agents to represent them for signing by a threshold signature scheme. This style called the threshold proxy multi signature .

At present , a scheme which puts blind signature and threshold proxy multi signature together is few ,and particularly a threshold proxy blind multi signature scheme based on bilinear pairings is absent .Just aiming at this point ,in this paper ,we introduce a new scheme called a threshold proxy blind multi signature scheme, and analyze the security and efficiency of it .

1 bilinear pairings

1.1 the conception of bilinear pairings

We define G_1 and G_2 as a add cluster and a multiple cluster separately and the order of them is the prime number q, then define P as the generator of G_1. We suppose the scattered logarithm problem of these clusters are hard work and define e: $G_1 \times G_1 \rightarrow G_2$ is this bilinear pairings which is content with these characteristics :

(1) The character of bilinear pairings: $e(aP,bQ) = e(P,Q)^{ab}$ is content to all $P,Q \in G_1$ and all $a,b \in Z$.

(2) The character of not degeneration : $e(P,Q)=1$,for any $Q \in G_1$,there will be P=O.

(3) The character of calculating: for all $P,Q \in G_1$, a effective arithmetic is existed to calculate e(P,Q).

Considering there are a great many discussions of signature schemes based on elliptic curve nowadays, we choose wail pairings or reconstructed Tate pairings which are based on elliptic curve to construct the bilinear pairings.

1.2 mathematics problems

For this G_1 cluster ,we define some cryptography problems following .

(1) The scattered logarithm (DL) problem: given $P,Q \in G_1$, find integer n out to make P=nQ if this n is existed .

(2) Computational Diffie-Hellman(CDH) problem: given triple group $(P,aP,bP) \in G_1^3$ where $a,b \in Z_q^*$, find abP out.

(3) Decisional Diffie-Hellman(DDH) problem: given quad group $(P,aP,bP,abP) \in G_1^4$ where $a,b,c \in Z_q^*$,decide whether c=ab(mod q) is established or not .

(4) Gap Diffe-hellman(GDH) problem: it is a kind of problem that GDH is a difficult problem but DDH is a easy one.

2 the threshold proxy blind multi signature scheme based on bilinear pairings

2.1 establishment of systematical parameters

We define q is the order of G_1 and G_2, and G_1 and G_2 are the clusters that are content with the supposes in section 1.1.Here, we choose G_1 as a add cluster that is formed with elliptic curve in a finite field ,and its generator is G: $G_1 \times G_1 \rightarrow G_2$ is a safe bilinear pairings ,we choose two Hash functions $H:\{0,1\}^* \rightarrow G_1$ and $H_1:\{0,1\}^* \rightarrow Z_q^*$.

(1) A_i(i=1,2…….m) express m original signers , the private keys of them are $k_i \in Z_q^*$, corresponding public keys are $P_{Ai}=k_iG$, identity markings are I_{Ai}.

(2) B_j(j=1,2……..n) express n proxy signers ,the private keys of them are $d_j \in Z_q^*$, corresponding public keys are $P_{Bj}=d_jG$, identity makings are I_{Bj}.

(3) All public keys above are authenticated and published by CA.

(4) The scheme is made up of four phases ,they are proxy private key generation phase, sharing of proxy private key phase ,signing phase and verification phase .

2.2 proxy private key generation phase

All members A_1A_2……..A_m in original signers group delegate their signing capability to a proxy signer B_j together ,the steps are following :

(1) A_i calculates $K_i= k_iH_1(m_w)$,then sends K_i and m_w to B_j. (m_w is an authorization certification that is sent to B_j by original signers group ,it includes the final time for deputizing ,the identity makings of original signers and proxy signer ,and the threshold number t , deputizing time .)

(2) Proxy signer B_j tests if m equations $e(K_i ,G)=e(H_1(m_w), P_{Ai})$.....(1) are established .

(3) If m equations above are all established, proxy signer B_j calculates $g_j=K_1+K_2+…….+K_m+d_j$, the g_j is the proxy private key of proxy signer , and proxy public key is $P_j=g_jG=P_{K1}+P_{K2}+.....+P_{Km}+P_{Bj}$.

2.3 Sharing of proxy private key phase

Each member B_j of proxy signer group is a banker ,they share proxy private key by (t,n) threshold signature scheme ,the proxy private key of B_j is g_j, the steps are following :

(1) Each B_j chooses a polynomial $f_j(x)$ at random to make $f_j(0)=g_j$,and we calculate the privacy sharing $f_j(I_{Bi})$.

(2) B_i will obtain proxy private key from n proxy signers .Noting $f(x)=f_1(x)+f_2(x)+.....+f_n(x)$, and the total proxy sharing private key that B_i obtained is $f(I_{Bi})=f_1(I_{Bi})+f_2(I_{Bi})+.....+f_n(I_{Bi})$, that is to say the proxy sharing private key that B_i obtained is $sk_i=f(I_{Bi})$, and B_i broadcasts the sharing public key $Psk_i=f(I_{Bi})G$.

2.4 signing phase

As usual ,we choose t members in proxy signer group to form the effective proxy signer group $\{B_1,B_2.....B_t\}$ to proceed signature for message m .

(1) Each signer B_i chooses $r_i \in Z_q^*$ at random , calculates $Z=H(m_w),U_i=r_iZ$, and sends U_i to consumer .

(2) Consumer calculates $U=U_1+U_2+.....+U_t$, and chooses $\alpha, \beta \in Z_q^*$ as blind gene to turn the message blindly, then he calculates $U'=\alpha U+\alpha\beta H(m_w),h=\alpha^{-1}H_1(m||U')+\beta$, sends h and U to every effective proxy signer .

(3) Each effective proxy signer B_i calculates $S_i'=\mu_i sk_i(U+hZ)$, among it , $\mu_i=\prod_{\substack{j=1\\ i\neq j}}^{t}\frac{-I_{Bj}}{I_{Bi}-I_{Bj}}$, and sends S_i' to consumer .

(4) After receiving S_i' ,consumer tests if t equation $e(S_i',G)=e(\mu_iU+\mu_ihH(m_w),Pk_i)$.....(2) is established , if all are established , consumer calculates $S'=\sum_{i=1}^{t} S_i'$, and proceeds blind off course $S=\alpha S'$, obtains the signature (S,m,m_w,U') at last.

2.5 verification phase

(1) After receiving the proxy blind signature of m ,first of all ,the receiver tests whether it is in the effective time ,if it is ,then do the next step, else, refuses it .

(2) Receiver tests if the equation $e(S,G)= e(U'+H_1(m||U')H(m_w),\sum_{i=1}^{n}P_i)$.....(3) is established ,if it is ,that the signature is legal .

Prove the exactness of equation (1),(2),(3):

Equation (1):

$$e(K_i, G) = e(k_iH_1(m_w), G) = e(H_1(m_w), P_{Ai})$$

Equation (2):

$$e(S_i', G) = e(\mu_i sk_i(U + hZ), G) = e((U + hZ)\mu_i, sk_iG)$$
$$= e(\mu_i U + \mu_i hH(m_W), Pk_i)$$

Equation (3):

$$e(S, G) = e(\alpha S'G) = e(\alpha\sum_{i=1}^{t} S_i', G) = e(\alpha\sum_{i=1}^{t}\mu_i sk_i(U + hZ), G)$$
$$= e(\alpha\sum_{i=1}^{n} g_i(U + hZ), G) = e(\alpha(U + hZ), \sum_{i=1}^{n} g_iG)$$
$$= e(\alpha(U + hZ), \sum_{i=1}^{n} P_i)$$
$$= e(\alpha U + \alpha H(m_w)(\alpha^{-1}H_1(m \| U') + \beta), \sum_{i=1}^{n} P_i)$$
$$= e(\alpha U + H(m_w)H_1(m \| U') + \alpha\beta H(m_w), \sum_{i=1}^{n} P_i)$$
$$= e(U' + H_1(m \| U')H(m_w), \sum_{i=1}^{n} P_i)$$

3 the analysis of the threshold proxy blind multi signature scheme

3.1 the security of this scheme

The security of this scheme should be considered at these several factions following :

(1) In the verification phase, we use public keys to separate the authorities from original signers to proxy signers .

(2) In the scheme , the valid time and proxy range are restricted ,because that the original signers have configured the final time for deputizing and the rang of proxy messages already.

(3) In the scheme ,any group which is formed with less t members can not obtain group private key , even if the assailant obtains the private keys of t-1 members ,it is also difficult to obtain group private key .

(4) In the scheme , α and β in blind turn phase of consumer is chosen at random ,so H_1 in Z_q^* is also at random ,that the signer wants to obtain the message m through H_1 is based on elliptic curve discrete logarithm problem (ECDLP),so that each person who takes part in this signature can not obtain the content of the message ,and it assures the blind signature characteristics of the message ,

Through these points, we see that this scheme is safe for

signing messages under being content with the requirement of blind signature and threshold proxy multi one .

3.2 the efficiency of this scheme

The operations of this scheme include mainly the addition and the number multiplication of the points in G_1 ,the multiplication and division in Z_q^* ,the calculation of Hash functions ,the calculation of bilinear pairings ,and so on .comparing with the threshold signature and blind signature based on RSA or discrete logarithm ,the bilinear pairings we use are more effective for this scheme ,and have more application values .

4 Conclusion

we use bilinear pairings to form a new threshold proxy blind multi signature scheme in this paper and use the advantages of bilinear pairings in the application of cryptography , the characteristics of small quantity of airtight key ,high security and strong mobility in elliptic curve cryptography ,and we put blind signature and threshold proxy multi signature together ,so that it is effective for this scheme to protect the privacy right of the message through sending it,and it is useful for signers to turn the enjoy only of airtight key to the threshold enjoy together of it ,so that it improves the security of whole system .Of all ,the scheme possesses the characteristics of strong security and high effective .

References

[1] M Mambo,et al.Proxy Signatures, “Delegation of the power to sign Message,”IEICE Transactions on Fundamentals of Electronic Communication and Computer Science, E79-A(9):1338-1354, 1996.

[2] M Mabo,Usuda K Okamoto, “Proxy Signature for Delegating Signing Operation,”Proceedings of the 3rd ACM Conference on Computer and Communications, Security, ACM,New York, pp.48-57, 1996.

[3] LiJiang Yi ,GuoQiang Bai ,GuoZheng Xiao ,“proxy multi signature scheme : a new kind of proxy signature scheme,”Electronics Journal, pp.(4): 569-570, 2001,29.

[4] K Zhang,“Threshold proxy signature schemes, Information Security Workshop,”Japan, pp.191-197, 1997.

[5] JiGuo Li ,FuZhen Cao,YiChen Zhang et al ,“the password analysis and revision of proxy multi signature scheme,”High Technique Communication, 2000.pp .13 (4):1-5, 2003.

[6] ZuoWen Tan ,ZhuoJun Liu,ChunMing Tang,“proxy blind signature scheme based on scattered logarithm,”Software Journal , pp.14 (11): 1931-1935, 2003.

[7] ChunBo Ma,Jun Ao,DaKe He.,“Multi signature and group signature based on bilinear reflect ,” Computer Journal , pp.28 (9): 1558-1563, 2005.

[8] H.Krawczyk,“Simple forward-secure signatures from any signature scheme.,” In: Proc. Of the 7th ACM Conference on Computer and Communications Security(CCS2000), pp 108-115. ACM, 2000.

[9] MiYa JI A, “Another countermeasure to forgeries over message recovery signature,”IEICE Trans Fundamentals, pp.E80-A(11):2191-2200, 1997.

[10] Xuan Li ,RongHua Shi ,Mi Luo, “A improved scheme of proxy multi signature based on Mambo style ,”The Calculator engineering and application ,pp. 17,163, 2004.