MATEC Web of Conferences **44**, 02017 (2016)
DOI: 10.1051/matecconf/20164402017

Improvement of an Eliptic Curve Based Threshold Proxy Signature Scheme

Xiao Yu Miao

Zhejiang University of Media and Communications, Hangzhou 310018, China

Abstract. In 2006, Pomykala et al. proposed an elliptic curve based threshold proxy signature scheme as well as a proxy-protected version. They claimed their scheme had the properties of secrecy, unforgeability, non-repudiation and signer's identification. In this study, we showed inter conspiracy attack on the basic scheme and gave another attack on the proxy-protected version. We pointed out that even if the central authority is engaged, the basic model is not a proxy-protected one. We also proposed an improved scheme that can resist the known attacks to achieve higher security, and gave the security analysis of the improved scheme in detail.

1. INTRODUCTION

The concept of proxy signature was first introduced by Mambo et al. in 1996[1]. Proxy signature schemes have been suggested to be used in many applications. The concept of threshold proxy signature was proposed in 1997[2,3] , from then on it has been widely studied[4-7]. The threshold proxy signature scheme is a variant of the proxy signature scheme that the signing power is delegated to a proxy group. In a (t,n) threshold proxy signature scheme, the proxy signature key is shared among a group of n proxy signers delegated by the original signer. Any t or more proxy signers can opperatively sign a message on behalf of the original proxy signer, but t-1 or fewer proxy signers can not.

In 2006, Pomykala et al. proposed an elliptic curve based threshold proxy signature scheme as well as a proxy-protected version[6]. They claimed their scheme had the properties of secrecy, unforgeability, non-repudiation and signer's identification. They ponited out that the proxy-protected version could assure the proxy-protection property.

In this paper, we give attacks on Pomykala et al.'s scheme in detail and we also point out that even if the central authority is engaged, the basic model is not proxy-protected, and gave an improved scheme that can resist the known attacks.

2. Brief Review of Pomykala et al.'s Scheme

The scheme is based on the elliptic curve cryptosystem whose security is based on the elliptic curve discrete logarithm problem(ECDLP) in the finite Abel group $E(F_p)$, where P is a prime power. Q (on the elliptic curve E) is a point of order divisible by a large prime number.

Let P_0 be the original signer , and a set $P=\{P_1,\cdots,P_n\}$ be the proxy group of n proxy signers, H and H' be two one-way hash functions.

Each proxy signer P_i has a private key $a_i \in F_p$ and the corresponding public key $A_i = a_i Q$ ($i=0,1,\cdots,n$). The original proxy signer P_0 composes a message ω called proxy warrant that contains the valid time of the delegation, the identities of the original signer and the proxy signers, etc.

2.1 Group Secret Key Generation Phase

The original proxy signer P_0 prepares a warrant ω, chooses a random integer $r < ordQ$, computes $R = rQ$.

Then P_0 computes the group secret key $d = a_0 H + r$, which satisfies $dQ = HA_0 + R$, where $H = H(\omega, R)$.

2.2 Group Secret Key Share Phase

The original proxy signer P_0 selects a polynomial $f_0(x) = c_{0,t-1}x^{t-1} + \cdots + c_{0,1}x + d$, where each $c_{0,i}$ is a random integer.

Next the original proxy signer P_0 computes $C_{0,i} = c_{0,i}Q$, i=1,…,t-1 as his obligations, and broadcasts them to the proxy group.

Xiao-Yu Miao: miaoxiaoyu.1987@163.com

The original proxy signer P_0 computes P_i's group secret key share as $y_{i0} = f_0(x_i)$, where x_i denotes P_i's public identity. Then P_0 sends y_{i0} to each P_i via a secure channel.

With the obligations, each proxy signer P_i verifies the validity of y_{i0} by checking whether or not $y_{i0}Q = HA_0 + R + \sum_{j=1}^{t-1} C_{0,j} x_i^j$, accepts the group secret key share if and only if the verification equation holds.

2.3 Proxy Signature Generation Phase

Without loss of generality, let $B = \{P_1, \cdots, P_t\}$ be the subset of t proxy signers from the group $P = \{P_1, \cdots, P_n\}$.

(1) Each proxy signer $P_i \in B$ selects a secret polynomial $f_i(x) = c_{i,t-1}x^{t-1} + \cdots + c_{i,1}x + c_{i,0} + a_i$, where $c_{i,k}$ is a random integer $< ordQ$ in F_p, for $k = 0,1,\cdots,t-1$, and a_i is the secret key of P_i for i=1,…,t.

(2) Then each proxy signer P_i computes and broadcast $C_{i,k} = c_{i,k}Q$ as his obligations, for $k = 0,1,\cdots,t-1$.

(3) Each P_i computes $H' = H'(\omega, R, M, B)$, $y_{ji} = H' f_i(x_j)$, and sends y_{ji} to P_j by a secret channels, for j=1,…,t-1, $i \neq j$.

(4) Each proxy signer P_j verifies the t-1 values from other proxy signers by checking the eqtions

$$y_{ji}Q = H'\left(A_i + \sum_{k=0}^{t-1} x_j^k C_{j,k}\right), \quad \mathrm{i} = 1,2,\cdots,\mathrm{t}, \quad i \neq j.$$

If all of the above equations hold, each proxy signer P_j computes $s_j = \sum_{i=1}^{t} y_{ji}$, for j=1,…,t.

In fact,

$$s_j = \sum_{i=1}^{t} y_{ji} = H' f(x_j)$$

$$= H'\left(x_j^{t-1}\sum_{i=1}^{t} c_{i,t-1} + \cdots + \sum_{i=1}^{t} c_{i,0} + \sum_{i=1}^{t} a_i\right)$$

Then

$$F(x) = f(x)Q$$

$$= x^{t-1}\sum_{i=1}^{t} C_{i,t-1} + \cdots + x\sum_{i=1}^{t} C_{i,1} + \sum_{i=1}^{t} C_{i,0} + \sum_{i=1}^{t} A_i.$$

Let $C_k' = \sum_{i=1}^{t} C_{i,k}$, $k = 0,1,\cdots,t-1$, $A' = \sum_{i=1}^{t} A_i$.

(5) Each proxy signer P_j computes his partial proxy signature on M as

$\sigma_j = y_{j0} + \sum_{i=1}^{t} y_{ji} = y_{j0} + s_j$, j=1,…,t.

Then each proxy signer P_j sends his partial proxy signature σ_j to other proxy signers via secret channels.

The shares can be verified by checking the equations

$$\sigma_j Q = HA_0 + R + \sum_{k=1}^{t-1} x_j^k C_{0,k} + \sum_{P_j \in B}\left[H'\left(A_j + \sum_{k=0}^{t-1} x_j^k C_{j,k}\right)\right], j = 1,2,\cdots,t.$$

(6) If all of the above equations hold, the threshold proxy signature on M is $(M, C_0', A', \sigma, \omega, B, R)$, where $\sigma = \sum_{j=1}^{t} \sigma_j \lambda_j^B(0)$, $\lambda_j^B(0) = \prod_{k\neq j}^{k=1,\cdots,t} \frac{-x_k}{x_j - x_k}$.

2.4 Verification of the Signature

To verify the threshold proxy signature $(M, C_0', A', \sigma, w, B, R)$, firstly, the verifier checks the warrant ω. If the validity has expired, the signature is invalid.

Otherwise, the verifier computes $H = H(\omega, R)$ and $H' = H'(\omega, R, M, B)$, checks the verification equation $\sigma Q = HA_0 + R + H'(C_0' + A')$. The verifier accepts the signature if and only if the verification equation holds.

3. Crptanalysis of Pomykala et al.'s Scheme

3.1 Inter Conspiracy Attack on Pomykala et al.'s Scheme

Firstly, we ponit out that the Pomykala et al.'s scheme is vulnerable to the inter conspiracy attack as following.

Let $T = \{P_{i_1}, \cdots, P_{i_t}\}$ be an arbitrary subset of t proxy signers from $P = \{P_1, \cdots, P_n\}$, and $(M, C_0', A', \sigma, w, B, R)$ be a valid signature by $B = \{P_1, \cdots, P_t\}$.

Then the proxy signers in T can reconstruct the proxy signature key using Lagrange interpolation formula

$$d = \sum_{j=1}^{t} f_0(x_j)\lambda_j^B(0), \quad \lambda_j^B(0) = \prod_{k\neq j}^{k=1,\cdots,t} \frac{-x_k}{x_j - x_k}.$$

Then any user $P_c \in T$ can generate a forged threshold proxy signature of any message M' on behalf of the original signer P_0 as $(M', C_0', A', \sigma', \omega, B, R)$, where

$\sigma' = d + \frac{H_C'(\sigma - d)}{H'}$, $H_C' = H'(\omega, R, M', B)$, $H' = H'(\omega, R, M, B)$. The forged signature

$(M', C_0', A', \sigma', \omega, M', B, R)$ can pass the certification in the valid delegation period, because

$$\sigma' Q = dQ + \frac{H_c'(\sigma - d)}{H'} Q$$
$$= HA_0 + R + H_c' F(0)$$
$$= H(\omega, R)A_0 + R + H'(\omega, R, M', B)(C_0' + A')$$

3.2 Attack on the Proxy-protected Version

Pomykala et al. claimed that if the central authority is not engaged, the basic model is not a proxy protect one. In the following part we'll show that the Pomykala et al.'s scheme doesn't satisfy the proxy-protected property even if a central authority is engaged.

The original proxy signer P_0 can forge a signature using a previous signature $(M, C_0', A', \sigma, w, B, R)$ and the corresponding group secret key d, on behalf of B as follows.

The original signer P_0 computes a valid warrant ω' of any message M', chooses $r' < ordQ$, computes $R' = r'Q$, $H_1 = H(\omega', R')$. Let $d' = a_0 H_1 + r'$ be the group secret key.

The forged threshold proxy signature is $(M', C_0', A', \sigma', \omega', B, R')$, where

$\sigma' = d' + \frac{H_2(\sigma - d)}{H'}$, $H_2 = H'(\omega', R', M', B)$, $H' = H'(\omega, R, M, B)$.

Then we show that the forged signature $(M', C_0', A', \sigma', \omega', B, R')$ can pass the certification. Obviously, the warrant ω' can always pass the verification because it is generated validly by the original signer. And by computing $H_1 = H(\omega', R')$ and $H_2 = H'(\omega', R', M', B)$, the forged signature satisfies the verification equations

$$\sigma' Q = d' Q + \frac{H_2(\sigma - d)}{H'} Q$$
$$= H_1 A_0 + R' + H_2(C_0' + A')$$

4. The improved threshold proxy signature scheme

The group secret key generation phase and group secret key share key share phase are the same as those in Pomykala et al.'s Scheme.

The proxy signature generation phase is as following.

Let C be an appointed clerk, who is one of the proxy signers in P, and $B = \{P_1, \cdots, P_t\}$ be the subset of proxy signers from $P = \{P_1, \cdots, P_n\}$, who actually make the threshold proxy signature on behalf of P_0.

(1) The t proxy signers of B cooperate to reconstruct the proxy signature key using the Lagrange Interpolation Formula:

$$d = \sum_{j=1}^{t} f_0(x_j) \lambda_j^B(0), \quad \lambda_j^B(0) = \prod_{k \neq j}^{k=1,\cdots,t} \frac{-x_k}{x_j - x_k}.$$

(2) Each proxy signer $P_i \in B$ chooses a random integer $k_i < ordQ$ as his secret information. Then P_i computes and broadcast $K_i = k_i Q$, let $K = \sum_{i=1}^{t} K_i$.

P_i computes $\delta_i = d + a_i + k_i H(K_i, M)$, let δ_i be his partial secret key.

(3) Each proxy signer $P_i \in B$ chooses a polynomial $f_i(x) = c_{i,t-1} x^{t-1} + \cdots + c_{i,1} x + c_{i,0} + \delta_i$,

where $c_{i,k} < ordQ$, $k = 0,1,\cdots,t-1$, is a random integer. Computes and broadcasts $C_{i,k} = c_{i,k} Q$ for $k = 0,1,\cdots,t-1$.

P_i computes $H' = H'(\omega, K, M, B)$ and $y_{ji} = H' f_i(x_j)$, sents y_{ji} to P_j via secret channels, where j=1,…,t-1, $i \neq j$.

(4) Each P_j verifies t-1 values by checking the equations

$$y_{ji} Q = H' \left(\sum_{k=0}^{t-1} x_j^k C_{i,k} + HA_0 + R + A_i + K_i H(K_i, M) \right)$$

If all of the equations hold, P_j computes $s_j = \sum_{i=1}^{t} y_{ji} = H' f(x_j)$, and his partial signature $\sigma_j = k_j + s_j \lambda_j^B(0)$, where

$$f(x) = x^{t-1} \sum_{i=1}^{t} c_{i,t-1} + \cdots + \sum_{i=1}^{t} c_{i,0} + \sum_{i=1}^{t} \delta_i.$$

Then P_j sends δ_j to the clerk C.

(5) The clerk verifies these partial signatures by checking the equations

$$\sigma_j Q = K_j + H'[\mathrm{x_j^{t-1}} C_{t-1}' + \ldots + x_j C_1' + t(HA_0 + R)$$
$$+ \mathrm{A}' + \sum_{i=1}^{t} K_i H(K_i, M)] \lambda_j^B(0)$$

where $C_k' = \sum_{i=1}^{t} C_{i,k}$, $A' = \sum_{i=1}^{t} A_i$

(6) If all equations hold, the clerk computes $\sigma = \sum_{j=1}^{t} \sigma_j$.

Then the threshold proxy signature on M is $(M, C_0', A', \sigma, \omega, B, \{K_i\}_B, R)$.

To verify the signature, firstly, the verifier checks the warrant ω, if the validity has expired, the signature is invalid.Otherwise, accept the signature if and only if

$$\sigma Q = K + H'[C_0' + A' + t(HA_0 + R) + \sum_{i=1}^{t} K_i H(K_i, M)]$$

5. Security analysis of the improved scheme

(1) The secrecy of the improved scheme refers to the elliptic curve discrete logarithm problem in the finite Abel group $E(F_p)$. If an attacker attempts to obtain the secret information of the signers, he must solve the elliptic curve discrete logarithm problem, which is more difficult than solving the discrete logarithm problem. Hence all the secret information is secure. And even if t out of n proxy signers conspire to obtain the group secret key d using the Lagrange Interpolation Formula, they cannot get the secret value k from the public value K, then cannot obtain the secret key a_0 of the original signer. Similarly, no one can get the secret k_i from K_i.

(2) Our proposal assures the proxy-protected. In the improved scheme, the original signer knows the group secret key d and the previous valid signature σ, but he cannot obtain the value $\sum_{i=1}^{t} k_i$ or $f(0)$ from K and σ, because the value $\sum_{i=1}^{t} k_i$ and $H'[\sum_{i=1}^{t} c_{i,0} + td + \sum_{i=1}^{t} a_i + \sum_{i=1}^{t} k_i H(K_i, M)]$ are undistinguishable to P_0. So he cannot forge a signature which can pass the verification on behalf of the proxy group B.

(3) The improved scheme is resistant against the inter conspiracy attack mentioned in section 3.

Now consider a proxy group T wants to forge a signature on another message M' on behalf of B. They select a previous signature σ, and obtain the group secret key d. But they cannot distinguish between $\sum_{j=1}^{t} k_j$ and $f(0)$, so they cannot change the message M for M' without being detected as presented in section 3. Consequently the inter conspiracy attack is also infeasible.

(4) The improved scheme has the properties of unforgeability and non-repudiation. From the above analysis we can see that the malicious users cannot forge a valid signature. Because only the original signer can generate the group secret and delegate the shares to the proxy signers, so he cannot deny having made it. Similarly, the proxy signers cannot deny their work either. Without the secret information of the proxy signers, the clerk cannot change the proxy signer's shares or generates a partial proxy signature on behalf of P_i.

Moreover, the valid time of the proxy delegation contained in the warrant ω stipulates the life time of the proxy shares. And from a valid signature $(M, C_0', A', \sigma, \omega, B, R_B, R)$ any users may confirm the actual proxy signers who generated the proxy signature.

6. Conclusion

In this paper, we showed two attacks on the Pomykala et al.'s scheme in detail, and we also showd that the Pomykala et al.'s scheme doesn't satisfy the proxy-protected property even if a central authority is engaged. We also proposed a new scheme that can resist the known attacks to achieve higher security.

Acknowledgement

This research was the concluding achievement of the research project of Zhejiang University of Media and Communications (ZC15XJ030), and was financially supported of research project of the State Press and Publication Administration of radio and television 《Research on key technology of digital television security monitoring and alarming system based on digital watermarking》（NO.2014-42）.

References

1. M. Mambo, K. Usuda and E. Okamoto： IEICE Transactions on Fundamentals, E79-A(9), 1996, 1338-1353.
2. S. Kim, S. Park, and D. Won: Proc.Information and Communications Security-ICIS'97, LNCS1334, Spring-Verlag, Berlin, 1997, 223-232.
3. K. Zhang: Proc.Information Security Workshop-ISW'97, LNCS1396, Spring-Verlag, Berlin, 1997,191-197.
4. Q. Xie: Applied Mathematics and Computeation, Vol.168(2),2005,776-782.
5. Z. H. Shao: Fundamenta Informaticae, Vol.104(4), 2010,385-392.
6. J. Pomykala, S. Barabasz: Fundamenta Informaticae, Vol.69(4),2006,411-425.
7. R. B. Lu, D. K. He, C. J. Wang: Cryptanalysis of an identity-based threshold proxy signature scheme with known signers, Journal of Electronics &Information Technology, Vol.30(1), 2008, 100-103.