International Journal of Informatics and Communication Technology (IJ-ICT)
Vol. 3, No. 1, February 2014, pp. 67~72
ISSN: 2252-8776

Proxy-Protected Proxy Multi-Signature Based on Elliptic Curve

Manoj Kumar Chande*, Balwant Singh Thakur**
*Department of Applied Mathematics, Shri Shankaracharya Institute of Professional Management & Technology
P.O. Sejbahar, Mujgahan, Pin Code: 492015, Raipur, Chhattisgarh, India
**School of Studies in Mathematics, Pt. Ravishankar Shukla University
Pin Code: 492010, Raipur, Chhattisgarh, India

Article Info
Article history:
Received Nov 21, 2013
Revised Jan 23, 2014
Accepted Jan 26, 2014

Keyword:
Algorithm (ECDSA)
Elliptic curve digital signature
Elliptic curve discrete
Logarithm problem (ecdlp)
Multi-signature
Proxy signature
Proxy-protected signature.

ABSTRACT
In this work, we propose a proxy-protected proxy multi-signature scheme based on Elliptic Curve Digital Signature Algorithm (ECDSA), which aims at providing data authenticity, integrity, and non-repudiation to satisfy the basic properties of partial delegation proxy signature described by Mambo et al. as well as strong proxy signature properties defined by Lee et. al. The proposed signing/verifying scheme combines the advantages of proxyprotected signature and multi-signature scheme. The security of the proposed schemes is based on the difficulty of breaking the elliptic curve discrete logarithm problem (ECDLP). The scheme proposed is faster and secure than the multi-signature based on factoring or discrete logarithm problem (DLP). The final multi-signature of a message can be verified individually for each signer or collectively for a subgroup or entire group as well. Finally, the proposed proxy-protected proxy multi-signature schemes can be used in E-commerce and E-government application, which can be implemented using low power and small processing devices.

Corresponding Author:
Manoj Kumar Chande
Department of Applied Mathematics
Shri Shankaracharya Institute of Professional Management & Technology
Email: manojkumarchande@gmail.com

1. INTRODUCTION

The special purpose and very useful variant of digital signature i.e. proxy signature was introduced by Mambo, Usuda and Okamoto [14]. A proxy signature scheme is a cryptographic primitive involving three entities: an original signer O, a proxy signer P and a verifier V . It allows the original signer to delegate his/her signing capability to a designated proxy signer. Then the proxy signer can sign some specific kinds of messages on behalf of the original one. On the basis of the delegation types, the proxy signature can be classified as full delegation, partial delegation and delegation by warrant. Depending on whether the original signer generate the same proxy signatures as the proxy signers do, there are two kinds of proxy signature schemes.

(a) Proxy-unprotected: In this type of proxy signature the proxy signer P, generates proxy signatures only with the proxy signature key given by the original signer O. So the original signer can also generate the same proxy signatures, therefore the original signer must consign trustworthy enough persons as his proxy signers. Verifiers validate proxy signatures only with the public key of the original signer and pay attention to legality of the warrant.

(b) Proxy-protected: In this type, proxy signer P, generates proxy signatures not only with the proxy signature key given by the original signer O, but also with the private key of himself/herself. Anyone else, including

the original signer, cannot generate the same proxy signatures. Verifiers validate the proxy signatures with the public keys of both the proxy signer and the original signer. The proxy-protected signature schemes can provide more security level than the proxy-unprotected signature.

Many of the proposed proxy signature schemes are not up to the mark regarding efficiency, security and feasibility for real time applications [6, 7, 9, 10, 11], because these proxy schemes cannot be really proved sufficiently strong, secure, and unbreakable against newly particular intentional attacks. To overcome these disadvantages, Chang, Chen and Chen [3], proposed a proxy-protected signature scheme by altering slightly the existing Elliptic Curve Digital Signature Algorithm (ECDSA) [17], which is pretty well known by its security properties.

The concept of proxy multi-signature was first introduced by Yi, Bai and Xiao [19]. In this kind of primitive, a proxy signer can generate a signature for a message on behalf of two or more original signers. After Yi, Bai and Xiao's [19], work, several proxy multi-signature schemes have been proposed [2, 5, 18].

We are thankful to Koblitz [8] and Miller [16], who observed the intractability of discrete logarithm on elliptic curves (ECDLP) over finite fields, elliptic curve cryptography becomes an important topic in public key cryptography. Due to the low computation and storage costs of ECDLP based schemes, large numbers of researchers intend to find more efficient solutions based on ECDLP than that on DLP.

Motivated by the details mentioned above, we would like to propose a new construction of proxy-protected proxy multi-signature scheme, which is based on Chang, Chen and Chen [3], proxy-protected signature scheme. The security of this scheme rely on the hardness of elliptic curve discrete logarithm problem (ECDLP). A proxy multisignature scheme in which only the proxy signer can create valid proxy multi-signature is called a proxy-protected proxy multi-signature scheme.

The organization of our paper is as follows: In Section–2 we give the proxy-protected proxy signature of Chang and Chen, based on ECDSA. Section–3 is about our proposed proxy-protected proxy multi-signature scheme. Section–4 deals with security and computational analysis of the proposed scheme and finally we draw some conclusion in Section–5.

2. PROXY-PROTECTED PROXY SIGNATURE SCHEME BASED ON ECDSA BY CHANG AND CHEN

The critical point of Mambo-Usuda-Okamoto [13], scheme is that, it is unable to protect proxy signer's authority, because the original signer may pretend proxy signer to sign on document, which means their scheme is not reliable in practice.

To overcome with such deficiency, in the year 2008, Chang and chen [3], proposed a novel proxy-protected scheme based on ECDSA. This scheme is a variant of ECDSA with properties of proxy signatures and adopts the approach in which only the proxy signer can create the proxy signature. Although the proxy-unprotected scheme is more efficient, but is only applicable when the original signer and the proxy signer both are reliable. It means the proxy-protected proxy signature schemes could prevent forgery attempted by the original signer, as well as against malicious proxy signers.

Notations:

Throughout this paper, we will use the following notations to explain and analyze the schemes.

O : An original signer
P : A proxy signer.
V : A verifier
P : A prime number
F_p : Finite prime field
E_p : An elliptic curve defined over F_p
q : The number of points on E_p
G : A point on Ep having prime order q
α : A private key with $0 \leq \alpha \leq q - 1$
$h(.)$: A one-way hash function

The parameters are defined in an elliptic curve E_p modulo a prime p, as public-key cryptography. For more detail about elliptic curve and their algebraic operations refer [1].

2.1. Proxy-protected proxy signature based on ECDSA

The protocol of proxy-protected ECDSA as follows. Let O be the original signer have private key and public key Q = G, and P is a designated proxy signer.

2.2. Proxy Generation and Delivery

(i) Proxy signer P, select a random number k_p, such that $1 < k_p < q$. Compute $G' = k_p G \bmod q$ and send G' to O.

(ii) Original signer select a random number k_o, such that $1 < k_o < q$.

(iii) Compute $R_o = k_o G$, and set $(x_1, y_1) = k_o G'$.

(iv) Compute $e = x_1 \bmod q$, and set $s_o = \alpha\, e + k_o \bmod q$.
If $x_1 = 0$, then goto step (ii), else send (R_o, s_o) to proxy signer P.

2.3. Proxy Verification and Proxy Key Generation

(i) Proxy signer P set $(x_2, y_2) = k_p R_o$ and $e' = x_2 \bmod q$, and accept the delegation iff $R_o = s_o G - e' Q$.

(ii) After accepting the delegation proxy signer will compute $s'_p = s_o k_p^{-1} \bmod q$. This s'_p is his proxy key.

To avoid man-in-middle attack, the Certificate Authority (CA), can be involved; P send the certificate request of proxy key to the CA. According to certificate policy, CA identifies P and then forwards the certificate request to the CA for signing proxy certificate.

2.4. Signing by the Proxy Signer

(i) Proxy signer select a random number k, such that $1 < k < q$. Compute $(x_3, y_3) = kG'$ and set $r = x_3 \bmod q$.

(ii) compute $s = k^{-1}(h(m) + s'_p\, r) \bmod q$. If $r = 0$ or $s = 0$, then goto step (i).

The proxy signature for the message m is (G', R_o, e', r, s).

2.5. Verification of the Proxy Signature

(i) V the verifier check that $r, s \in [1, q-1]$.

(ii) Compute:

$$w = s^{-1} \bmod q, \quad u_1 = h(m)\, w \bmod q,$$
$$u_2 = r\, w \bmod q, \quad u_3 = e'\, u_2 \bmod q,$$
$$X = (x'_3, y'_3) = u_1 G' + u_2 R_o + u_3 Q.$$

(iii) If $X = \mathrm{O}$, then reject the signature, else accept the signature iff $x'_3 = x_3 = r$.

A verifier has to use both the original signer's public key and proxy key certificate to verify the proxy signature.

The proxy-protected ECDSA could be also deployed in ECDSA by taking parameters $G' = G$, $R_o = 0$ and $e' = 1$. Furthermore, the proxy-protected ECDSA also maintains the properties of strong proxy signature [9, 10].

3. PROXY-PROTECTED PROXY MULTI-SIGNATURE BASED ON ECDSA

In this section we propose proxy-protected proxy multi-signature by following chang and chen [3], proxyprotected proxy signature scheme which is based on ECDSA. Here the system parameters are same as in proxyprotected proxy signature based on ECDSA. We apply a function *h*(.), which is a collision resistant hash function and able to protect with man-in-middle attack as well as birth-day attacks [15].

For each $1 \le i \le t$, the original signer O_i secretely selects a random number, $1 \le \alpha_{o_i} \le q-1$, as his private key and compute the corresponding public key $Q_i = \alpha_{o_i} G$ and since Q_i's are public keys therefore original signers O_i's can also compute $Q = \sum_{i=1}^{n} Q_i \bmod q$.

Step I: Subproxy key generation

(a) Proxy signer P, select a number k_{p_i}, such that $1 < k_{p_i} < q$, compute $G'_i = k_{p_i} G \bmod q$ and then send G'_i to original signers and also compute $G' = \sum_{i=1}^{n} G'_i \bmod q$.

(b) For each $1 \le i \le t$, original signer O_i selects a random number $1 \le k_{o_i} \le q-1$.

(c) Computes $R_{o_i} = k_{o_i} G$ and set $(x_{o_i}, y_{o_i}) = k_{o_i} G'$.

(d) Compute $e_{o_i} = x_{o_i} \bmod q$.

(e) Set $s_{o_i} = \alpha_{o_i} e_{o_i} + k_{o_i} \bmod q$. if $x_{o_i} = 0$, the select k_{o_i} again.

Step II: Subproxy key delivery

For each $1 \le i \le t$, original signer O_i sends (R_{oi}, s_{oi}) to the proxy signer in a secure manner.

Step III: Subproxy verification
For each $1 \leq i \leq t$, the proxy signer computes $(x_{p_i}, y_{p_i}) = k_{p_i} R_{o_i}$ and set $e_{p_i} = x_{p_i} \bmod q$, accept delegation only when, $R_{o_i} = s_{o_i} G - e_{p_i} Q_i$ and calculate $e_p = \sum_{i=1}^{n} e_{p_i} \bmod q$, otherwise he rejects it and request a valid one corresponding to the signer O_i, who gives the invalid subproxy key or terminate this protocol.

Step IV: Proxy key generation
If the proxy signer validates all (R_{o_i}, s_{o_i}), in which $1 \leq i \leq t$, then he computes $s'_p = \sum_{i=1}^{n} s'_{p_i} = \sum_{i=1}^{n} s_{o_i} k_{p_i}^{-1} \bmod q$, as a valid proxy key and $R_o = \sum_{i=1}^{n} R_{o_i} \bmod q$.

Step V: Signing by the proxy signer
(a) Proxy signer select a random number $1 \leq k'_{p_i} \leq q-1$, compute $(x'_{p_i}, y'_{p_i}) = k'_{p_i} G'$, set $r_{p_i} = x'_{p_i} \bmod q$ and $r_p = \sum_{i=1}^{n} r_{p_i} \bmod q$.

(b) Compute: $s_{p_i} = k_{p_i}^{'-1}(h(m) + s'_{p_i} r_{p_i}) \bmod q$ and $S_p = \sum_{i=1}^{n} s_{p_i} \bmod q$. If $r_{p_i} = 0$ or $s_{p_i} = 0$, then go back to step (a).

The proxy-protected proxy multi-signature for message m is (G', R_o, e_p, r_p, S_p).

Step VI: Verification of proxy-protected proxy multi-signature
(a) Verifier V checks whether $r_{p_i}, s_{p_i} \in [1, q-1]$.

(b) Compute:

$$w_i = s_{p_i}^{-1} \bmod q$$
$$w = \sum_{i=1}^{n} s_{p_i}^{-1} \bmod q.$$
$$u_1 = \sum_{i=1}^{n} u'_i = \sum_{i=1}^{n} h(m) w_i \bmod q,$$
$$u_2 = \sum_{i=1}^{n} u''_i = \sum_{i=1}^{n} r_{p_i} w_i \bmod q.$$
$$u_3 = \sum_{i=1}^{n} u'''_i = \sum_{i=1}^{n} e_{p_i} u''_i \bmod q.$$
$$X = (x''_p, y''_p) = u_1 G' + u_2 R_o + u_3 Q.$$

(c) If $X = O$, then reject the signature, else accept the signature iff $x''_p = \sum_{i=1}^{n} x'_{p_i} = \sum_{i=1}^{n} r_{p_i} = r_p$

In this subsection we will prove the correctness of our proposed signature scheme.
Theorem 1 *If the delegation certificate (R_{o_i}, s_{o_i}), is valid for all i, then $R_{o_i} = s_{o_i} G - e_{p_i} Q_i$. Where $R_{o_i} = k_{o_i} G$, $s_{o_i} = \alpha_{o_i} e_{o_i} + k_{o_i} \bmod q$, $(x_{p_i}, y_{p_i}) = k_{p_i} R_{o_i}$ and $e_{p_i} = x_{p_i} \bmod q$.*

proof: We first prove that $e_{o_i} = e_{p_i}$.

$$(x_{o_i}, y_{o_i}) = k_{o_i} G' = k_{o_i} k_{p_i} G = k_{p_i} R_{o_i} = (x_{p_i}, y_{p_i})$$
$$\therefore \quad e_{o_i} = x_{o_i} \bmod q = x_{p_i} \bmod q = e_{p_i}$$
$$\because \quad s_{o_i} = \alpha_{o_i} e_{o_i} + k_{o_i} \bmod q$$

Replace e_{p_i} for e_{o_i}, in the above equation, the we get

$$s_{o_i} = \alpha_{o_i} e_{p_i} + k_{o_i} \bmod q$$

on rearranging the above equation as, $k_{o_i} = s_{o_i} - \alpha_{o_i} e_{p_i} \bmod q$; then to verify R_{o_i}

$$R_{o_i} = k_{o_i} G \bmod q = (s_{o_i} - \alpha_{o_i} e_{p_i}) G \bmod q = s_{o_i} G - e_{p_i} Q_i$$

Theorem 2 *If the proxy signer generates the proxy signature correctly, the it will pass the proxy signature verification.*

proof: We have a valid proxy signature

$$s_{p_t} = k'^{-1}_{p_t}(h(m) + s'_{p_t} r_{p_t}) \bmod q$$

on rearranging the above equation

$$\begin{aligned} k'_{p_t} &= s^{-1}_{p_t}(h(m) + s'_{p_t} r_{p_t}) \bmod q \\ &= s^{-1}_{p_t}(h(m) + (s_{o_t} k^{-1}_{p_t}) r_{p_t}) \bmod q, && (\because s'_{p_t} = s_{o_t} k^{-1}_{p_t} \bmod q) \\ &= s^{-1}_{p_t}(h(m) + (\alpha_{o_t} e_{p_t} + k_{o_t}) k^{-1}_{p_t} r_{p_t}) \bmod q && (\because s_{o_t} = \alpha_{o_t} e_{p_t} + k_{o_t} \bmod q) \end{aligned}$$

Multiply both sides by G'

$$\begin{aligned} k'_{p_t} G' &= s^{-1}_{p_t} G'(h(m) + (\alpha_{o_t} e_{p_t} + k_{o_t}) k^{-1}_{p_t} r_{p_t}) G' \\ &= s^{-1}_{p_t} G' h(m) + (\alpha_{o_t} e_{p_t} s^{-1}_{p_t} G' + s^{-1}_{p_t} G' k_{o_t}) k^{-1}_{p_t} r_{p_t} \\ &= s^{-1}_{p_t} G' h(m) + (\alpha_{o_t} e_{p_t} s^{-1}_{p_t} G' k^{-1}_{p_t} r_{p_t} + s^{-1}_{p_t} G' k_{o_t} k^{-1}_{p_t} r_{p_t}) \\ &= s^{-1}_{p_t} G' h(m) + (\alpha_{o_t} e_{p_t} s^{-1}_{p_t} G r_{p_t} + s^{-1}_{p_t} G k_{o_t} r_{p_t}) \\ &= u'_i G' + u''_i \alpha_{o_t} e_{o_t} G + u''_i k_{o_t} G && (\because u'_i = h(m) w_i = h(m) s^{-1}_{p_t},\ u''_i = r_{p_t} w_i = r_{p_t} s^{-1}_{p_t}) \\ &= u'_i G' + u''_i \alpha_{o_t} e_{p_t} G + u''_i R_{o_t} && (\because e_{o_t} = e_{p_t},\ R_{o_t} = k_{o_t} G) \\ &= u'_i G' + u''_i R_{o_t} + u'''_i Q_i && (\because u'''_i = e_{p_t} u''_i,\ Q_i = \alpha_{o_t} G) \\ &= (x''_{p_t}, y''_{p_t}) \end{aligned}$$

$$\therefore (x''_{p_t}, y''_{p_t}) = (x'_{p_t}, y'_{p_t}),\ \because\ k'_{p_t} G' = (x'_{p_t}, y'_{p_t})$$

4. SECURITY AND COMPUTATIONAL ANALYSIS

In this section discussion about possible attacks against the security of proposed scheme is given. The security of proposed scheme is based on the difficulty of breaking the one-way hash function and on the complexity of solving the elliptic curve discrete logarithm problem.

(a) If an attacker might forges the proxy signature on the message m by selecting a random number k; and computing $(x'_{p_t}, y'_{p_t}) = kG'$ and setting $r_{p_t} = x'_{p_t} \bmod q$; the attacker needs proxy key $s'_{p_t} = s_{o_t} k'^{-1}_{p_t} \bmod q$ and k_{p_t} to forge signature $s_{p_t} = k'^{-1}_{p_t} h(m) + s'_{p_t} r_{p_t} \bmod q$. It is computationally infeasible to determine S_p without both s'_{p_t} and correct k'_{p_t}. In addition, the probability of s'_{p_I} and correct k'_{p_t} is $1/q$, which is negligible when q is large enough.

(b) To prevent the tactic of another malicious signer impersonating the authorized proxy signer to create a proxy key interactively with an original signer (man-in middle attack) by selecting another random number ko. We require only the certification of original/proxy signer's public keys by any kind of authority mechanism such as PKI mechanism. With the verification of public keys certificate, the verifier will reject all unauthorized proxy eys generated by the fake proxy signer.

(c) If an original signer becomes dishonest and tries to forge the proxy key, the proxy signer could use a blind factor k_o to blind $G' = k_oG \bmod q$ so that the original signer needs to solve k_o from $G' = k_oG \bmod q$. It is difficult to determine k_o according to the hardness of the elliptic curve discrete logarithm problem. Under socalled proxy-protected security property restriction, an original signer should not be able to derive the authorized proxy signer's proxy key; otherwise a verifier could not distinguish exactly whether the original signer or the proxy signer creates the proxy signature.

5. CONCLUSION

In this study an efficient proxy-protected proxy multi-signature scheme based on ECDSA is contributed. The proposed scheme satisfies not only the security of signature, but also the security properties of proxy signature and strong proxy signature. Moreover, the proposed scheme is based on modified ECDSA which reduces the calculation time and makes the signature scheme more efficient.

REFERENCES

[1] I.F. Blake, et al., *Elliptic Curves in Cryptography*, Cambridge University Press, 1999.
[2] F. Cao and Z.F. Cao, "*Cryptanalysis on a proxy multi-signature scheme*", in proceedings of the IMSCCS06, pp. 316–319, 2006.

[3] Ming-Hsin Chang, et al., "Design of Proxy signature in ECDSA", *Eigth International Conference on Intelligent Systems Design and Applications, IEEE computer society*, pp. 17–22, 2008.
[4] X. Fu, et al., "A new type of proxy multi-signature scheme", *Journal of Xidian University*, vol. 28, no. 6, pp. 29–731, 2001.
[5] C. Hsc, et al., "New proxy multi-signature scheme", *Applied Mathematics and Computation*, vol. 162, no. 3, pp. 1201–1206, 2005.
[6] Min-Shiang Hwang, et al., "Generalization of proxy signature based on elliptic curves", *Computer Standards & Interfaces*, vol. 26, pp. 73–84, 2004.
[7] S. Kim, et al., "Proxy signatures Revisited", *Proc. of ICICS'97, Lecture Notes In Computer Science, Springer-Verlag*, vol. 1334, pp. 223–232, 1997.
[8] N. Koblitz, "Elliptic Curve Cryptosystems", *Math. Comp*., vol. 48, pp. 203–209, 1987.
[9] B. Lee, and K. Kim, "Strong proxy signatures", *IEICE Trans. Fundamentals*, vol. E82-A, no. 1, pp. 1–11, 1999.
[10] B. Lee, et al., "Strong proxy signature and its applications", *Proc. of SCIS 2001*, 11B–1, pp. 603–608, 2001.
[11] Wei-Bin Lee and Tzung-Her Chen, "Constructing a proxy signature scheme based on existing security mechanisms", *Information & Security, an International Journal*, vol. 12, no. 2, 250–258, 2003.
[12] Z.H. Liu, et al., "Secure proxy multi-signature scheme in the standard model", *ProvSec 2008, Lecture Notes Computer Science*, vol. 5324, Springer, Berlin, pp. 127–140, 2008.
[13] M. Mambo, et al., "*Proxy signatures for delegating signing operation*", Proceedings of the Third ACM Conference on Computer and Communications Security, pp. 48–57, 1996.
[14] M. Mambo, et al., "Proxy signatures: delegation of the power to sign message", *IEICE Transaction Functional*, vol. E-79-A, no. 9, pp. 1338–1354, 1996.
[15] A. J. Menezes, et al. *Handbook of Applied Cryptography*, CRC Press, 1996.
[16] V. S. Miller, "Use of elliptic curves in cryptography", In Advances in Cryptology-CRYPTO'85, Santa Barbara, CA, 1985, *Lecture Notes in Computer Science, Springer-Verlag, Berlin*, vol. 218, pp. 417–426, 1986.
[17] S. A. Vanstone, "Responses to NIST's proposal", *Communication of ACM*, vol. 35, pp. 50–52, 1992.
[18] Q.Wang and Z. Cao, "Formal model of proxy multi-signature and a construction", *Chinese Journal of Computers*, vol. 29, no. 9, pp. 1628–1635, 2006.
[19] L. Yi, et al., "Proxy multi-signature scheme: A new type of proxy signature scheme", *Electronics Letters*, vol.36, no.6, 527–528, 2000.

BIOGRAPHIES OF AUTHORS

Manoj Kumar Chande received the B.Sc. and M.Sc. degree in Mathematics from Pt. Ravishankar Shukla University, Raipur, Chhattisgarh, India in 1997 and 1999. He joined School of Studies in Mathematics, Pt. Ravishankar Shukla University, Raipur, Chhattisgarh, India for his doctoral research work.

Balwant Singh Thakur is an associate professor, School of Studies in Mathematics, Pt. Ravishankar Shukla University Raipur (C.G.), India. He has received his Ph.D. from Pt. Ravishankar Shukla University Raipur (C.G.), India in the year 1996.