ISSN 2320 2610

Volume 3, No.2, March - April 2014

International Journal of Multidisciplinary in Cryptology and Information Security

Available Online at http://warse.org/pdfs/2014/ijmcis01322014.pdf

PROVABLY SECURE SELF PROXY SIGNATURE SCHEME USING BILINEAR PAIRING

Neetu Sharma*
School of Studies in Mathematics,
Pt. RavishankarShukla University
Raipur (C.G.) 492010 India
Emai:- nitusharma013@gmail.com
Birendra Kumar Sharma
School of Studies in Mathematics,
Pt. RavishankarShukla University
Raipur (C.G.) 492010 India

ABSTRACT

Delegation of signing rights is common practice in real world. Self-proxy signature is a solution of delegation of signing capabilities to signer herself recursively. The cryptographic treatment on Self-Proxy signature was initially introduced by Kim *et al*. in 2007. Security of recently proposed Self-Proxy signature schemes based on solving ECDLP (Elliptic curve discrete logarithm problem). In this paper we propose the first provably secure Self-Proxy signature scheme using elliptic curve cryptography (ECC) and bilinear pairings also we analyze security and efficiency of our scheme. We claim that our new self-proxy signature is more efficient than self-proxy signature scheme of Nedal Tahat et al[12].

2000 AMS Subject Classification No. 94A60

Key words : Cryptography, Self-proxy signature scheme, Elliptic curve cryptosystem, Chosen message attack, Bilinear pairing.

1. INTRODUCTION

Proxy signature schemes have found numerous practical applications, particularly in distributed computing where delegation of rights is quite common, such as ecash systems, mobile agents for electronic commerce, mobile communications, grid Computing, global distribution networks, and distributed shared object systems. In 1996, Mambo, Usuada, and Okamoto introduced proxy signature scheme and gave security analysis [1]. Furthermore, various extensions of the basic proxy signature primitive have been considered. These include threshold proxy signatures [2], blind proxy signatures [3], proxy signatures with warrant recovery [4], nominative proxy signatures [5], one-time proxy signatures [6], and proxy anonymous proxy signatures [7].

In a self proxy signature scheme a signer, Alice delegates her signing capability to herself recursively. Using this scheme, Alice generates many proxy private/public key pairs, uses them simultaneously and revokes the temporary keys easily. Furthermore, it is easy to revoke the temporary private/public key pair. A self proxy signature scheme is a useful tool in the real world. For example, a person may use a legal seal and many other seals simultaneously. After registering, the legal seal is used in an important work, and the other seals are used for normal works. To use seals like this, the person protects the legal seal and uses another one for only a particular work.

In 2007, Kim et al.[8]proposed a novel secure self-proxy signature scheme based on DLP (Discrete Logarithm Problem). In 2010, S. Selvi et al [9] proved that the Kim et al [8] scheme is existentially forgeable and proposed the first ID based self proxy signature scheme. In 2012, Vandani Verma [10] proposed ID based self proxy signature scheme that is more efficient than Selvi et al. [9] scheme. In 2012, Mashhad [11] proposed a novel secure self proxy signature scheme based on DLP. The security of Mashhad's self proxy signature scheme based on the difficulty of solving the discrete logarithm problem.

Recently Elliptic Curve Cryptography (ECC) have been received great attention the reason is that its cipher key is much shorter than other cryptographies on the premise of same security. ECC hasn't been attacked by sub exponent algorithm till now. So the scheme depends on difficulty of solving ECDLP is believed to be safer than those based on DLP. In 2013,Nedal Tahat et al.[12] proposed an Efficient Self Proxy Signature Scheme Based on Elliptic Curve Discrete Logarithm Problems. The scheme require less number of operations than Mashhadi's scheme [11] and so is more efficient than Mashhadi's scheme.

In the last couple of years, the bilinear pairing has become flourishing area in cryptography, namely Weil pairing and Tate pairing are important tools for construction of ID-based cryptographic scheme. In order to speed up the signature generation and verification, and to provide strong security, we proposed an efficient and secure digital signature scheme using ECC and bilinear pairings

The rest of this paper is as follows: In section 2, we discuss some basic preliminaries of our scheme. In section 3, we propose new secure Self-Proxy signature scheme using bilinear pairing and in section 4, we analyze the security properties of our new scheme. In section 5, we give efficiency of our scheme. Finally we conclude our work in last section.

2. PRELIMINARIES

Definition 2.1.Elliptic Curve

Let $K = F_q$ be a finite field, where q is a power of some prime number The Weierstrass equation of an elliptic curve over K can be written in the following form:-

$$y^2 + cxy + dy = x^3 + ax + b$$
$$where a, b, c, d \in K$$

If $q > 3$ then by a linear change of variables above equation can be reduced in simpler form

$$y^2 = x^3 + ax + b with a, b \in GF(q) \ and$$
$$4a^3 + 27b^2 \neq 0,$$

An elliptic curve over K is the set of solutions of the Weierstrass equation with a point O, called point at infinity. An adding operation can be defined over the elliptic curve, which turns the set of the points of the curve into a group. The adding operation between two points is defined as follows.

In affine coordinates let $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ be two points on the elliptic curve, neither being the point at infinity over $GF(q)$. The inverse of a point P_1 is $-P_1 = (x_1, -y_1)$ .If $P_1 \neq P_2$ then $P_1 + P_2 = P_3 = (x_3, y_3)$ with

$$x_3 = \lambda^2 - x_1 - x_2, \qquad y_3 = \lambda(x_1 - x_3) - y_1$$

Where

$\lambda = \frac{y_2 - y_1}{x_2 - x_1}$, if $P_1 \neq P_2$

$= \frac{3x_1^2 + a}{2y_1}$, if $P_1 = P_2$ (doubling)

Bilinear Pairing and Some Problems[13]:-

Let G_1 be a cyclic additive group generated by P, whose order is a prime q, and

G_2 be a cyclic multiplicative group with the same order q: Let $e : G_1 \times G_1 \rightarrow G_2$ be a map with the following properties:

1. Bilinearity: $e(aP, bQ) = e(P, Q)^{ab}$ for all $P, Q \in G_1, a, b \in Z_q$.
2. Non-degeneracy: There exists $P, Q \in G_1$ such that $e(P, Q) \neq 1$, in otherwords, the map does not send all pairs in $G_1 \times G_1$ to the identity in G_2.
3. Computability: There is an efficient algorithm to compute $e(P, Q)$ for all $P, Q \in G_1$.

In our setting of prime order groups, the Non-degeneracy is equivalent to $e(P, Q) \neq 1$ for all $P, Q \in G_1$. So, when P is a generator of $G_1, e(P, P)$ is agenerator of G_2 ,Such a bilinear map is called a bilinear pairing (more exactly, called an admissible bilinear pairing).

We consider the following problems in the additive group $(G_1, +)$.

1. Discrete Logarithm Problem (DLP): Given two group elements P and Q, find an integer $n \in Z_q^*$, such that $Q = nP$ whenever such an integerexists.
2. Decision Diffie-Hellman Problem (DDHP): For $a, b, c \in Z_q^*$, given P, aP, bP, cP decide whether $c \equiv ab \bmod q$.
3. Computational Diffie-Hellman Problem (CDHP): For $a, b \in Z_q^*$ given P, aP, bP, compute abP.

Definition2.3.Weil pairing [13]:- Weil pairing $e_m : E[m] \times E[m] \rightarrow G$, where G is a multiplicative group of m^{th} roots of unity. Weil pairing is denoted by e_m, takes as input a pair of points $P, Q \in E[m]$ and gives as output an m^{th} root of unity $e_m(P, Q)$. The bilinearity of the Weil pairing is expressed by the equations

$$e_m(P_1 + P_2, Q) = e_m(P_1, Q)e_m(P_2, Q)$$
$$e_m(P, Q_1 + Q_2) = e_m(P, Q_1)e_m(P, Q_2)$$

The weil pairing has many useful properties:-

a) The values of the Weil pairing satisfy $e_m(P, Q)^m = 1$ for all $P, Q \in E[m]$.

b) The Weil pairing is alternative, which means that $e_m(P, P) = 1$ for all $P \in E[m]$.

c) The Weil pairing is nondegenerate, which means that if $e_m(P, Q) = 1$ for all $Q \in E[m]$ then $P = O$.

3. A NEW SELF PROXY SIGNATURE SCHEME

We propose an efficient self-proxy signature scheme using bilinear pairing. Our scheme is based on the normal proxy signature scheme in which a signer Alice delegates her capability to herself recursively. The propose scheme can be divided into four phases: the setup, key generation, and signature generation and verification phases.

3.1. System initialization Phase:-In the system initialization phase, the following commonly required parameters are generated to initialize the scheme.

a) A field size q, which is selected such that, q = p if p is an odd prime, otherwise, $q = 2^m$, as q is a prime power.

b) Two parameters $a, b \in F_q$ that define the equation of elliptic curve E over

$F_q\,(y^2 = x^3 + ax + b(mod q)$ in the case $q > 3$, where $4a^3 + 27b^2 \neq 0(mod q))$.

c) $h(,)$ a secure hash function.

d) For designating the signing authority, the signer prepares an appropriate warrant m_w. The warrant includes the identities of signer, and other useful information such as delegation period.

Alice generates the pair (s, Q) of private key s and public key Q as follows:

She randomly pick an integer $s \in Z_q^*$, computes key $Q = sP\ (modn)$

Sends Q to the certificate authority (CA).

Then CA randomly chooses $t \in Z_q^*$,
Computes $C = tQ\ (modn)$and returns C to Alice.

Then Alice chooses a random number $k \in Z_q^*$, and computes $K = kP$. Then he computes $\sigma = \left(k + h(K)\right).s$ by his secret key and sends σ to CA.

Then CA checks the equality by computing $e(P, \sigma P)^t = e(C, K + h(K)P)$.

3.3. Self-Proxy Key Generation Phase:-

The signer Alice generates the temporary self-proxy private - public key pair by using her original signing key pair (s, Q) as follows:-

The signer Alice chooses random number $d_r \in Z_n^*$ and computes $R = d_r P\ (modn)$
and calculate $d_p = \sigma + h(K||m_w)d_r$ and obtain its corresponding self-proxy public key,

$$e_p = d_p P \text{(modn)}$$

Finally she publish e_p.

3.4. Self-Proxy Signature Generation Phase:-

To sign the message m the signer Alice chooses $t \in Z_n^*$ and computes $T = tP$ and

$$S = (t + h(K||m_w||m))d_p$$

Then send (m, T, S, R, m_w) to verifier Bob.

3.5. Self-Proxy Signature Verification Phase:-

For verifying the correctness of the proxy signature (m, T, S, R, m_w), the verifier has to perform the operations as below.

$$e(P, SP) = e\left(e_p, T + h(K||m_w||m)P\right)$$

If it is true, then the self- proxy signature is valid.

3.6. Correctness of scheme:-

Theorem 1. *In the system initialization phase the equation* $e(P, \sigma P)^t = e(C, K + h(K)P)$ *is correct.*

Proof:-We can check the correctness by the following equation:-

$$\begin{aligned} e(P, \sigma P)^t &= e\left(P, \left(\left(k + h(K)\right).s\ \right)P\right)^t \\ &= e\left(sP, \left(k + h(K)\right).P\right)^t \\ &= e(tQ, (kP + h(K)P)) \\ &= e(C, (K + h(K)P)) \end{aligned}$$

Theorem 2. *In the self-proxy signature verification phase the equation* $e(P, SP) = e(P, t + h(K||m_w||m)dp)$ *is correct.*

Proof:-We can check the correctness by the following equation:

$$\begin{aligned} e(P, SP) &= e(P, SP) \\ &= e\left(P, (t + h(K||m_w||m)d_p)P\right) \\ &= e\left(d_p P, (t + h(K||m_w||m))P\right) \\ &= e\left(e_p, tP + h(K||m_w||m)P\right) \\ &= e\left(e_p, T + h(K||m_w||m)P\right) \end{aligned}$$

4. SECURITY ANALYSIS

Unforgeability property. Proxy signer create proxy signing key with his/her secret key. Only the proxy signer is capable of creating a valid proxy signature. Suppose Cindy wants to forge a self-proxy signature for a message m , and claim dishonestly that has been generated by Alice. For this Cindy wants d_p and t, for calculating this he has to solve $e_p = d_p P$ and $T = tP$ which is based on solving ECDLP and solving ECDLP is infeasible.

Undeniability property.In the propose scheme, any valid self-proxy signature (m, T, S, R, m_w) for a message should be generated by Alice. This is because only Alice has the self private key . Moreover, the warrant and temporary self-proxy public key d_p are created by Alice and no Adversary can change them. When the self-proxy signature (m, T, S, R, m_w) is verified the warrant m_w is checked, and the public key of signer Q, the temporary self-proxy public key e_p, and the public informations are used in the verification phase. Thus, Alice cannot deny signing the self-proxy signature. Therefore the proposed scheme satisfies the undeniability property.

Distinguishability property . In the proposed scheme, when the self-proxy signature (m, T, S, R, m_w), is verified, Alice's public key and her identity are used in the verification phase ; therefore, we can consider it as a self proxy signature and not a normal signature. Thus, anyone can distinguish the self proxy signature from normal signatures. Thus the proposed scheme satisfies the distinguishability property.

5. EFFICIENCY

Table 1 defines our notation. The time complexity of the proposed protocol and some other protocol in terms of modular multiplication operation, modular bilinear pairing operation, modular elliptic curve multiplication, and modular square and one way hash function is shown in table 1.

Table 2 shows the efficiency comparison of our newly propose scheme with the scheme of Mashhadi's scheme [11] and Nedal Tahat et.al's scheme [12] scheme.

Table1. Time complexity of various operations

Notation	Definition
T_{BP}	Time complexity for the execution of a bilinear pairing.
T_{EC-MUL}	Time complexity for the execution of an elliptic curve multiplication.
T_{EXP}	Time complexity for the execution of a exponentiation.
T_h	Time complexity for the execution of a hash function.
T_{MUL}	Time complexity for the execution of a modular multiplication.
T_{SQU}	Time complexity for the execution of an square.

Table 2:- Comparison of efficiency

	Signature generation	Signature verification
Mashhadi's scheme[12]	$1T_{EXP}+$ $+2T_{MUL}+1T_h$	$3T_{EXP}+5T_{MUL}+2T_h$
Nedal Tahat et.al's scheme[13]	$1T_{EC-MUL}+$ $2T_{MUL}+1T_h$	$3T_{EC-MUL}+$ $2T_{MUL}+3T_{EC-ADD}+$ $2T_h$
Our's scheme	$1T_{EC-MUL}+$ $1T_{MUL}+1T_h$	$2T_{EC-MUL}+$ $2T_{MUL}+1T_{EC-ADD}+$ $1T_h+2T_{BP}$

6. CONCLUSION

In this paper, we propose provably secure self-proxy signature scheme, which is based on ECC and bilinear pairings. To the best of our knowledge, the propose scheme is the first provably secure self-proxy signature scheme using bilinear pairing. Nevertheless, in order to achieve our goal, we have paid some additional computation cost. Our scheme is computationally efficient as two bilinear parings and two elliptic curve scalar point multiplication operations are executed for signature verification,

REFERENCES

[1] M. Mambo, K. Usuda, and E. Okamoto. Proxy signatures: delegation of the power to sign messages, Transactions on Fundamentals of electronic communications and computer science. Vol. E79-A, pp. 1338-1354, 1996.

[2] J. Herranz and G. Sez. Verifiable secret sharing for general access structures, with application to fully distributed proxy signatures. In Proceedings of Financial Cryptography, LNCS. Springer-Verlag, 2003.

[3] S. Lal and A. K. Awasthi. Proxy blind signature scheme. Cryptology ePrint Archive, Report2003/072.

[4] S. Lal and A. K. Awasthi. A scheme for obtaining a warrant message from the digital proxy signatures. Cryptology ePrint Archive, Report 2003/073.

[5] H.-U. Park and L.-Y. Lee. A digital nominative proxy signature scheme for mobile communications. In ICICS 2001, volume 2229 of LNCS, 451C455. Springer-Verlag, 2001.

[6] . H. Kim, J. Baek, B. Lee, and K. Kim. Secret computation with secrets for mobile agent using one-time proxy signature. In Cryptography and Information Security, 2001.

[7] K. Shum and V. K. Wei. A strong proxy signature scheme with proxy signer privacy protection. In Eleventh IEEE International Workshop on Enabling Technologies, Infrastucture for Collaborative Enterprises , 2002.

[8] Y. Kim and J. Chang, \Self proxy signature scheme,"International Journal of Computer Science and Network Security, vol. 7, pp. 335-338, 2007.

[9] S.Sharmila Deva Selvi, S. SreeVivek, S. Gopinath, C.Pandu Rangan., "Identity Based Self Delegated Signature scheme. Proceeding NSS '10 Proceedings of the 2010 Fourth International Conference on Network and System Security Pages. 568-573 IEEE Computer Society Washington, DC, USA, 2010.

[10] Vandani Verma, An Efficient Identity based Self Proxy Signature Scheme with warrant, ijcsc Vol. 3, No. 1, , pp. 111-113, ISSN : 0973-7391, January-June 2012.

[11] S. Mashhadi, A novel secure self-proxy signature scheme**.** International Journal of Network security**,**vol.14, no.1, pp.22-26. 2012.

[12] Nedal Tahat, K. A. Alzu'bi and I. Abu-Falahah, An Efficient Self Proxy Signature Scheme Based on Elliptic Curve Discrete Logarithm Problems, Applied Mathematical Sciences, Vol. 7, no. 78, 3853 – 3860 , 2013.

[13] J. H.Silverman.: The arithmetic of elliptic curves, volume 106 of graduate texts in mathematics, springer-verlag, Newyork 1986.

[14] J. Hoffstein, J. Pipher., and J. H. Silverman, An introduction to mathematical cryptography, springer.