Institute of Advanced Engineering and Science

International Journal of Information & Network Security (IJINS)
Vol. 3, No. 1, February 2014, pp. 33 – 39
ISSN: 2089-3299

An Elliptic Curve Based Multi-Signature Scheme For Wireless Network

Manoj Kumar Chande* **and Balwant Singh Thakur****
*Department of Applied Mathematics, Shri Shankaracharya Institute of Professional Management And 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 Oct 20th, 2013
Revised Dec 10th, 2014
Accepted Jan 25th, 2014

Keyword:
Elliptic Curve Digital Signature Algorithm (ECDSA)
Elliptic Curve Discrete Logarithm Problem (ECDLP)
Multi-Signature

ABSTRACT

In this paper we propose a design of multi-signature scheme for wireless networks and it is based on an improved elliptic curve digital signature algorithm. Wireless communications perform better with the elliptic curve cryptosystem because of their efficiency regarding speed, low bandwidth and high security. Multi-Signature is the special purpose signature in which multiple signer jointly sign a message or messages. Security of the scheme relies on elliptic curve discrete logarithm problem (ECDLP). Our scheme is more secure and has improved efficiency of computation than with the existing schemes.

Corresponding Author:
Manoj Kumar Chande
Department of Applied Mathematics,
Shri Shankaracharya Institute of Professional Management And Technology
P.O. Sejbahar, Mujgahan, Pin Code: 492015, Raipur, Chhattisgarh, India.
manojkumarchande@gmail.com

1. INTRODUCTION

In our daily life whether it is our workplace, home or some other place like shops, means of wireless communication is present in every place and plays its crucial role. In this age of information the need of wireless network and data traffic in networks grow rapidly and this brings more concern about security of these wireless networks and the information that is on the flow. The bandwidth requirement for wireless communication is less in comparison with the traditional wired communication. The equipments used by the end user are having very limited capacity of computation and power like mobile phones. In this situation the elliptic curve cryptosystems is suitable and has advantage over other cryptosystems in trend, because of its features [8].

Elliptic Curve Cryptosystem (ECC) was independently introduced by Victor Miller [11] and Neal Koblitz [7], in the year 1985. Elliptic curves rise naturally in many branches of mathematics and are closely linked with the theory of elliptic functions, from which they derive their name. Elliptic curve cryptosystem has gained advantage over other cryptosystems like RSA [13] and Elgamal [2] because of the features like: (a) Robust Security, (b) Faster Computation, (c) Less storage space required and (d) Shorter Key size.

Modern days technology rely on algorithms that do computation quickly and cheaply. One of them is Elliptic Curve Digital Signature Algorithm (ECDSA). The ECDSA is the elliptic curve analogue of the Digital Signature Algorithm (DSA). ECDSA was first proposed in 1992 by Scott Vanstone [14]. It was accepted in 1998 as an ISO standard and is under consideration for inclusion in some other ISO standards. It was also accepted in 1999 as an ANSI standard and in 2000 as IEEE and NIST standards. Organizations go for ECDSA because of its high reputational security. The security of ECDSA is based on the intractability of elliptic curve discrete logarithm problem (ECDLP).

The points on the elliptic curve form a group G, the elliptic curve discrete logarithm problem is to find the integer x, for group elements P and Q, such that $Q = xP$. The security of 322-bit ECDSA is equal to the 1024-bit RSA signature and the length of certification is 62 bytes, RSA has 256 bytes and the DSA is 168 bytes.

Itakura and Nakamura [6], were first who introduced multi-signature scheme. However their scheme has an efficiency issue because the generation and the verification cost of the multi-signature increases linearly with the number of signers. Since then, various multi-signature schemes have been realized. Some of them are multi-signature schemes that are based on RSA assumption given by Harn and Kiesler [4, 5] and Okamoto [12], Wang, Miao, Doi and Okamoto [15] constructed form bilinear maps, based on discrete logarithm problem assumption by Hardjono and Zheng [3]. In 2004, a multi-signature scheme based on the elliptic curve cryptosystem is given by Chen et al. [1], Later, Liu and Liu [9] and many multi-signature schemes are given by researchers.

The organization of our paper is given as follows. We review Elliptic Digital Signature Algorithm (ECDSA) in section-2, in section-3 we give the Improvised Elliptic Digital Signature Algorithm (ECDSA-I), Section-4 is about design of multi-signature scheme, Section-5 deals with security and computational analysis of the proposed multi-signature scheme and finally we draw some conclusion in Section-6.

2. ELLIPTIC CURVE DIGITAL SIGNATURE ALGORITHM (ECDSA)

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

Notations:

O	:	An original signer.
V	:	A verifier.
$\mathbb{F}_p$	:	Finite field.
E_p	:	An elliptic curve defined over a finite field.
G	:	A base point on E_p having prime order q.
x_0	:	A private key of original signer O, with $0 \leq x_0 \leq q-1$.
Q	:	A public key of original signer O.
$h(.)$	:	A one-way hash function.

The ECDSA consists of three phases: (I) Key Generation, (II) Signature Generation and (III) Signature Verification. Now we give the three phases in detail and the steps required to complete the signature algorithm.

Phase (I) Key Generation For ECDSA:

The suitable chosen elliptic curve E_p defined over a finite field $\mathbb{F}_p$ of characteristic p and a base point $G \in E_p(a,b)$ with an order n.

(i) Select a random integer x_0 such that, $1 \leq x_0 \leq n-1$.

(ii) Compute $Q = x_0 G$.

So key pair is (x_0, Q), where x_0 is a private key and Q is a public key of the signer.

Phase (II) ECDSA Signature Generation:

To sign a message m, signer O does the following steps:

(i) Select an integer α such that, $1 \leq \alpha \leq n-1$.

(ii) Compute $\alpha\, G = (x_1, y_1)$.

(iii) $r = x_1 \bmod n$, if $r = 0$, then select new α.

(iv) Calculate $\alpha^{-1} \bmod n$ and $e = h(m)$.

(v) Compute $s = \alpha^{-1}(\, e + x_0 r\,)$, if $s = 0$ then go to step (i).

The signature for the message m is (r, s).

Phase (III) ECDSA Signature Verification:

To verify O′s signature (r, s) on message m, verifier V follows the steps:

(i) Verifier checks whether $1 \leq r, s \leq n-1$, or not, if not then signature is invalid.

(ii) Compute $e = h(m)$ and s^{-1}.

(iii) Compute $u = e\,s^{-1} \bmod n$ and $v = rs^{-1} \bmod n$.

(iv) Compute $w = (x_2, y_2) = u\,G + v\,Q$, if $w = 0$ then stop, otherwise compute $t = x_2 \bmod n$.

(v) The signature is valid if and only if $t = r$.

The signature is valid one iff, $t = r$.

$$\begin{aligned} w &= u\,G + v\,Q \bmod n \\ &= es^{-1}\,G + rs^{-1}x_0\,G \bmod n\,. \\ &= s^{-1}(\,e + x_0 r\,)G \bmod n \\ &= \alpha\,G \end{aligned}$$

Therefore $u\,G + v\,Q = \alpha\,G$ and so $t = r$, which is required.

3. IMPROVED ELLIPTIC CURVE DIGITAL SIGNATURE ALGORITHM (ECDSA-I)

In the year 2006, Zhong, Guanzhong and Deming [17], gave an efficient ECDSA based signature scheme for wireless network with an improved ECDSA algorithm. The improved ECDSA scheme is also comprised of three phases: (I) Key Generation, (II) Signature Generation and (III) Signature Verification as follows:

Phase (I) Key Generation For ECDSA-I:

The suitable chosen elliptic curve E_p defined over a finite field $\mathbb{F}_p$ of characteristic p and a base point $G \in E_p(a, b)$ with an order n.

(i) Select a random integer x_0 such that $1 \leq x_0 \leq n-1$.

(ii) Compute $Q = x_0 G$.

So key pair is (x_0, Q), where x_0 is a private key and Q is a public key of signer.

Phase (II) ECDSA-I Signature Generation:

To sign a message m, signer O does the following steps

(i) Select an integer α such that $1 \leq \alpha \leq n-1$.

(ii) Compute $\alpha\,G = (x_1, y_1)$.

(iii) $r = x_1 \bmod n$, if $r = 0$, then select new α.

(iv) Calculate $\alpha^{-1} \bmod n$ and $e = h(m)$.

(v) Compute $s = \alpha + ex_0\,r$, if $s = 0$ then go to step (i).

The signature for the message m is (r, s).

Phase (III) ECDSA-I Signature Verification:

To verify O′s signature (r, s) on message m, verifier V follows the steps:

(i) Verifier checks whether $1 \leq r, s \leq n-1$, or not , if not then signature is invalid.

(ii) Compute $e = h(m)$.

(iii) Calculate $w = sG - er\,Q = (x_2, y_2)$, and $v = x_2 \bmod n$.

(iv) The signature is valid if and only if $r = v$.

In the verification phase, if $r = v$, the signature (r, s) and the message m is authentic. The message generated by original signer O then

$$\begin{aligned} w &= s\,G - er\,Q \mod n\,. \\ &= (\,(\alpha + erx_0) \mod n\,)\,G - er\,Q \mod n \\ &= (\,(\,\alpha + erx_0\,) \mod n\,)\,G - erx_0\,G \mod n \\ &= \alpha\,G \\ &= (x_1, y_1) \end{aligned}$$

$\therefore\ w = (x_2, y_2) = \alpha\,G = (x_1, y_1)$ and so $r = v$, which is required for signature verification.

4. PROPOSED MULTI-SIGNATURE SCHEME

The proposed multi-signature consists of four phases, which are system initialization, system key generation, multi-signature generation and multi-signature verification. The following participators involve in this scheme:

(a) Senders: Wireless client $\mathrm{C_i'}$s.

(b) Signature Entity: Wireless client $\mathrm{C_1}, \mathrm{C_2}, \ldots \mathrm{C_n}$.

(c) Authentication Center (AC).

(d) Verification Server (VS).

The authentication server AC receives the signature request from the client $\mathrm{C_i'}$s, then selects field parameters and one way hash function and sends the message to signature entity $\mathrm{C_i}$. As AC receives the individual signature from $\mathrm{C_i'}$s, generates global signature and sends it to VS.

Phase (I) System Initialization:

The AC, perform the following procedure as soon as he receives request from client $\mathrm{C_i'}$s.

(i) Select parameters and hash function h.

(ii) Archives for users are created and appoint n authorized users $\mathrm{C_1}, \mathrm{C_2}, \ldots \mathrm{C_n}$, to sign the message respectively.

Phase (II) Generation of Key:

All the signature entity $\mathrm{C_i}$, follow the steps

(i) Select a large random integer $d_i \in [1, n-1]$, as his private key.

(ii) Every signer compute $R_i = d_i\,G$, and sends to AC.

On the basis of information given in archives, the identity of signer and validity of public key is verified by AC. The AC computes system's public key

$$R = \sum_{i=1}^{n} R_i.$$

Phase (III) Multi-Signature Generation:

Each signature entity $\mathrm{C_i}$, generates his/her signature and sends it to AC, then the final multi-signature is computed by AC. Generation of final multi-signature is shown by the following steps

(i) Every signer $\mathrm{C_i}$ selects a large integer $\alpha_i \in [1, n-1]$, computes the point $Q_i = \alpha_i\,G = (x_i, y_i)$, $r_i = x_i \mod n$. If $r_i = 0$, then select new α_i.

(ii) Signer C_i sends (r_i, Q_i) to AC. AC update archives with this information and then computes

$$Q = \sum_{i=1}^{n} Q_i = (x, y)$$

and $r = x \mod n$. Goto step (i) and choose α_i, again if $r = 0$, otherwise broadcasts (r, Q) to the other signer.

(iii) C_i calculates, $s_i = (\alpha_i + erd_i) \bmod n$ and transmits (r, s_i) to AC.

(iv) Individual signatures (r, s_i), are verified by AC using r, Q_i and R_i. Set $Q'_i = s_i G - erR_i$. If $Q'_i = Q_i$, then only the signature accepted by AC, else rejected.

(v) As AC finds all the signature valid, he computes

$$s = \sum_{i=1}^{n} s_i$$

then sends the final multi-signature (m, r, s), to the verifying server VS.

Each signer can respectively sign the message as in step (iii). The time to generate signature can be shortened and the efficiency of the entire signature system will be increased.

Phase (IV) Multi-Signature Verification:

After receiving (m, r, s) from AC, VS verify signature using public key R.

(i) Compute $e = h(m)$.

(ii) Taking $P = s\,G - er\,R = (x', y')$.

(iii) If verifier finds $P = Q$, then only the signatures are valid, otherwise ask to re-sign.

Table 1. Complete operations of our proposed scheme

Signer's C_i		**Authentication Server (AC)**
	Key Generation	
$d_i \in [1, n-1],\ R_i = d_i G$	$\xrightarrow{R_i}$	$R = \sum_{i=1}^{n} R_i$
	Multi-Signature Generation	
$\alpha_i \in [1, n-1]$ $Q_i = \alpha_i G = (x_i, y_i)$ $r_i = x_i \bmod n$ If $r_i = 0$, select new α_i	$\xrightarrow{(r_i, Q_i)}$	$Q = \sum_{i=1}^{n} Q_i = (x, y)$ $r = x \bmod n$ If $r = 0$, select new α_i,
	$\xleftarrow{(r, Q)}$	else send(r, Q) to signers
$s_i = (\alpha_i + e\ r\ R_i) \bmod p$	$\xrightarrow{(r, s_i)}$	Verify all (r, s_i) $Q'_i = s_i G - erR_i$. If $Q'_i = Q_i$, accept, else reject signature. If all signatures are valid, compute $s = \sum_{i=1}^{n} s_i$
	Send multi-signature (m, r, s) to verifier	
	Verifier	
	$e = h(m)$ P=sG-er R=(x', y') If $P = Q$, then only,the signatures is valid.	

The signature is valid one iff and only iff, $P = Q$.

$$\begin{aligned} P &= sG - erR \\ &= \sum_{i=1}^{n} s_i G - erR \\ &= \sum_{i=1}^{n} (\,\alpha_i + erd_i\,)G - erR \\ &= \sum_{i=1}^{n} \alpha_i G + er \sum_{i=1}^{n} d_i G - erR \\ &= Q \end{aligned}$$

5. SECURITY AND COMPUTATIONAL ANALYSIS

In this section we analyze security properties of the proposed multi-signature scheme in different aspects.

(A) If an attacker attempts to personate the authentic user $\mathrm{C_i}$, to sign the message, then attacker must have knowledge of the private key d_i, from the function $R_i = d_i G$. For this he has to face elliptic curve discrete logarithm problem and that is not going to be easy for him.

(B) As an attacker attempts to get the private-key d_i, from signature function s_i, the attacker must have to solve equation $s_i = \alpha_i + erd_i \bmod n$, but it's not possible for him because of two unknowns α_i and d_i.

(C) The proposed scheme resists replying attack, because whenever a message is sent to next signer, the sender must attach a unique signature and could not generate the same signature. There are numbers randomly selected by signer and the probability that each signer repeats the same number is extremely low. So in this way every multi-signature is unique.

(D) The amount of calculation and communication is reduced because, AC himself generates entire public key and multi-signature.

(E) In this multi-signature scheme the improved ECDSA is used and no complicated calculation of inverse is required here as in the earlier. Signer have to compute $s_i = \alpha_i + erd_i \bmod n$, and has no other computation of messages or verification of signature received from the former signer. That is why the proposed signature scheme perform better, in comparison with other multi-signature schemes [10, 16].

6. CONCLUSION

The Digital Multi-Signature is a co-operative signature authentication protocol. Complicated process and large computation in stages of generation and verification of multi-signature make it cumbersome to imply these schemes in wireless networks environment. In this paper, we have presented a digital multi-signature scheme based on an improved elliptic curve digital signature algorithm (ECDSA). This scheme has the advantage of elliptic curve cryptosystem, such as shorter size of private keys, higher security and efficient computation, therefore this scheme is suitable to adapt in wireless networks. Furthermore, we have analyzed the security of the scheme. It can prevent the counterfeit attack and signature forgery attacks.

REFERENCES

[1] T. S. Chen et al, "Digital multi-signature scheme based on the elliptic curve cryptosystem", *J. Computer Science and Technology*, Vol.19, No. 4, pp. 570–573, 2004.
[2] T. ElGamal, "A Public Key Cryptosystem And A Signature Scheme Based On Discrete Logarithms", *IEEE Transaction On Information*, Vol. IT-31, No. 4, pp. 469–472, 1985.
[3] T. Hardjono and Y. Zheng, "A practical digital multisignature scheme based on discrete logarithms (extended abstract)", *In AUSCRYPT' 92, Springer*, pp. 122–132, 1993.
[4] L. Harn and T. Kiesler, "New scheme for digital multisignature", *IEEE Electronic Letters*, Vol. 25, No. 15, pp. 1002–1003, 1989.

[5] L. Harn L. and T. Kiesler, "RSA blocking and multisignature schemes with no bit expansion", *IEEE Electronic Letters*, Vol. 26, No. 18, pp. 1490–1491, 1990.
[6] K. Itakura K. and K. Nakamura, "New scheme for digital multisignature", *NEC Research and Development*, Vol. 71, pp. 1–8, 1983.
[7] N. Koblitz, "Elliptic Curve Cryptosystems", *Math. Comp.*, Vol. 48, pp. 203–209, 1987.
[8] Kirstin Lauter, "The Advantage of elliptic curve cryptography for wireless security", *Wireless Communications, IEEE Personal Communications*, Vol. 11, No. 1, pp. 62–67, 2004.
[9] D. Liu, et al., "Attack on digital multi-signature scheme based on the elliptic curve cryptosystem", *Journal of Computer Science and Technology*, Vol. 22, No. 1, pp. 92–94, 2007.
[10] Luo Liping, et al., "ELGamal Type Sequential Digital Multi-Signature Scheme Based on RSA", *Computer Engineering and Applications*, Vol. 42, No. 1, pp. 120–122, 2006.
[11] 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.
[12] T. Okamoto, "A digital multi-signature scheme using bijective public-key cryptosystems", *ACM Transaction On Computer System*, Vol. 6, No. 4, pp. 432–441, 1988.
[13] R. L. Rivest, et al., "A Method For Obtaining Digital Signatures And Public Key Cryptosystems", *Communication of ACM*, Vol. 21, No. 2, pp. 120–126, 1978.
[14] S. A. Vanstone, "Responses to NIST's proposal", *Communication of ACM*, Vol. 35, pp. 50–52, 1992.
[15] L. Wang, et al., "Id-based series-parallel multi-signature schemes for multi-messages from bilinear maps", *In WCC*, pp. 291–303, 2005.
[16] Lv Wanli and Zhongcheng, "A Robust Elliptic Curve Digital Multisignature Scheme", *Computer Engineering*, Vol. 30, No. 5, pp. 126–128, 2004.
[17] XU Zhong, et al., "An Efficient ECDSA-Based Signature Scheme For Wireless Networks", *Wuhan University Journal of Natural Sciences*, Vol. 11, No. 6, pp. 1707–1710, 2006.

BIOGRAPHY 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.