

AN EFFICIENT AND SECURE DIGITAL MULTI-SIGNATURE PROTOCOL BASED ON ECC

D. Sudha Devi¹, K. Thilagavathy² and Preethi Sai Krishnan³

^{1,3}Department of Computing, Coimbatore Institute of Technology, Coimbatore, India

²Department of Physics, Coimbatore Institute of Technology, Coimbatore, India

ABSTRACT

Digital Signatures play a crucial role today as it ensures authentication, integrity and non-repudiation of a digital message. Many researches are ongoing based on elliptic curve cryptography due to its significant high performance. In this paper we propose an efficient and secure digital multi-signature protocol based on elliptic curve cryptography. The proposed protocol is efficient with reduced time complexity as compared to Chen et al.[14], Sahu and Sharma [18] and Chande and Thakur's [20] digital multi-signature schemes. Also the proposed protocol overcomes the insider attack as specified by Liu et al. [19] in the Chen et.al's digital multi-signature scheme.

KEYWORDS

Authentication, Digital Multi-Signature, Elliptic Curve Cryptography, Elliptic Curve Discrete Logarithm Problem, Group signature, Hash function

1. INTRODUCTION

Digital Signature is a mathematical scheme which is meant for ensuring the properties such as authentication, integrity and non-repudiation of a digital message. Authenticity ensures that the signer is not impersonated; integrity ensures that the received message is not altered and non-repudiation ensures that the signer cannot deny the authenticity of the signature. Digital signatures are seem to be equivalent to handwritten signatures and are difficult to forge.

In the digital signature schemes proposed by Rivest et al. [1], Elgamal [2] and Sahmir [3], a single person generates a signature and anyone can verify the validity of the signature. Koblitz [4] and Miller [5] proposed Elliptic Curve Discrete Logarithm Problem (ECDLP) independently as a new cryptographic scheme which plays a significant role in cryptographic techniques. In Johnson et al. [6] it is revealed that Vanstone proposed Elliptic Curve Digital Signature Algorithm (ECDSA) in 1992, in response to National Institute for Standards and Technology [7] and was accepted in 1998 as an International Standards Organization (ISO 14888-3) standard [8], as an American National Standards Institute (ANSI X9.62) standard [9] in 1999 and as Institute of Electrical and Electronics Engineers (IEEE - I363-2000) standard [10] and NIST's FIPS (FIPS 186-2) standard [11] in 2000. In 2000, Nyang and Song [12] explicated a verification protocol for smart card which was based on zero-knowledge proof.

Generally the signer of a message is a single person who formulates a signature with the private key that can be verified by a verifier using the corresponding public key. But there are cases in which multiple persons acts as signer and is referred as a multi-signature scheme. A multi-signature can be effectively generated with the cooperation of all persons in the group and can be

verified by a verifier using the group public-key. Initially Itakura and Nakamura [13] proposed a public key cryptosystem for digital multi-signatures. Many other Digital multi-signature schemes were proposed by Chen et al. [14], Harn and Ren [15] and Yang et al. [16] using elliptic curve cryptosystem and RSA algorithm. Domínguez and Encinas [17] offered Java implementation for RSA based multi-signature scheme. Sahu and Sharma [18] proposed a multi-signature scheme based on Elliptic Curve Crypto system. Chande and Thakur [20] proposed a Multi-Signature scheme based on ECC for the wireless Network. Amir et. al [21] proposed a Digital Signature Scheme using hash function and discrete logarithm.

The rest of the paper is organized as follows. Section 2 deals with the proposed Digital Multi-Signature protocol. Security and Performance analysis of the proposed protocol is discussed in section 3 and section 4 concludes this paper. Section 5 discusses on the future work.

2. PROPOSED DIGITAL MULTI-SIGNATURE PROTOCOL

The working of a Digital Signature scheme is depicted in Figure 1. The signer generates a message digest using a hash function and encrypts the digest with his private key. The document and the signature are sent and the verifier calculates the message digest using the hash function. The received signature is decrypted with the signer's public key. The calculated digest is compared with the decrypted signature and if the condition satisfies, the verifier validates the signature else rejects the signature.

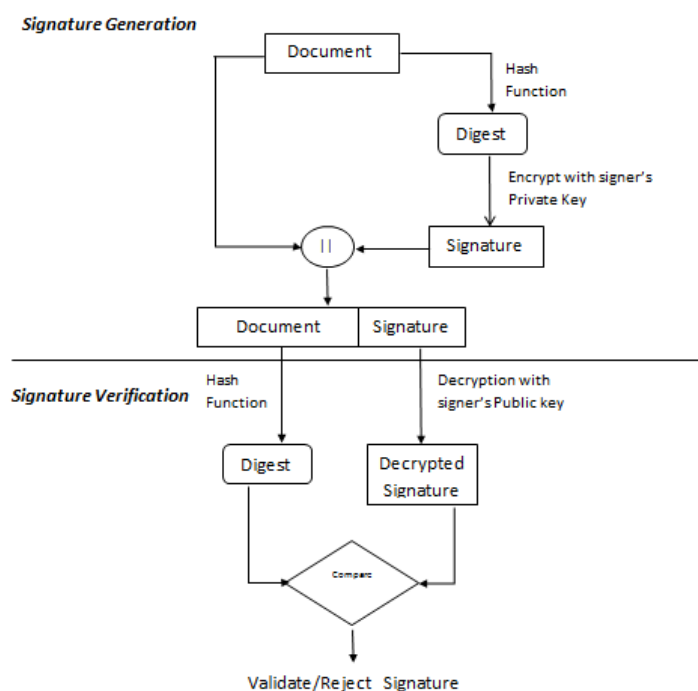


Figure 1. Overview of Digital Signature

The Digital Multi-Signature protocol proposed in this paper can be effectively used where a group of members need to sign a document for approval after doing some modifications in the document. For example users in a hierarchy, belonging to a security class has write permission on a file. After manipulating the file, all the users in that security class should sign the file which could be verified by the data owner for further processing of the file. In such case, utilizing a

digital multi-signature scheme is mandatory to ensure authenticity, integrity and non-repudiation properties of the digital document.

In this paper, we propose an efficient and secure Digital Multi-Signature protocol which consists of a Setup phase, Key generation phase, Multi-Signature generation phase and Multi-Signature verification phase as follows:

2.1. SETUP PHASE

1. A field size q which defines the finite field E_q , where $q = p$, if p is an odd prime or $q=2^m$ where q is a prime power.
2. Let a, b be two parameters of elliptic curve which defines the equation $E_q: y^2+xy=x^3+ax^2+b$.
3. A finite point on elliptic curve having largest order n is chosen as a base point P .

2.2. KEY GENERATION PHASE

Let $M_i, 1 \leq i \leq N$, be the members of a group. Each member of the group generates the keys as follows:

1. Select a random integer d_i from the interval $[1, n-1]$, which is the private key.
2. Compute the public key as $X_i = d_i P$.
3. Send the computed X_i to the other member of the group and the group admin completes the task by summing up all X_i 's as follows:

$$X = \sum_{i=1}^N X_i$$

2.3. MULTI-SIGNATURE GENERATION PHASE

Each member of the group generates the multi-signature as follows:

1. Select a random integer k_i from the interval $[1, n-1]$.
2. Compute $Y_i = k_i P$.
3. Send Y_i to the other member of the group and finally the group admin sums up all Y_i 's as follows:

$$Y = \sum_{i=1}^N Y_i$$

4. Using one-way hash function the message m is converted into an integer e as, $e = h(m)$
5. Compute $s_i = (k_i + ed_i) \bmod n$
6. Send s_i to the other member of the group and the group admin determines 's' as follows:

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

7. Send (s, Y) to the verifier.

2.4. MULTI-SIGNATURE VERIFICATION PHASE

The verifier receives (s, Y) and validates as follows:

1. Computes one-way hash function with the received message to get the digest as follows:
 $e=h(m)$
2. Computes $v1 = sP$
3. Computes $v2 = Y + eX$
4. The verifier validates the signature if $v1 = v2$ else reject it.

2.5. PROOF:

The consistency of the proposed Digital Multi-Signature is ensured as follows:

$$\begin{aligned}
 v1 &= sP \\
 &= (\sum_{i=1}^N s_i \text{ mod } n)P \\
 &= (\sum_{i=1}^N k_i)P + e(\sum_{i=1}^N d_i)P \\
 &= (\sum_{i=1}^N Y_i) + e(\sum_{i=1}^N X_i) \\
 &= Y + e X \\
 &= v2
 \end{aligned}$$

The proof shows that the digital signature is validated smoothly.

3. DISCUSSION ON SECURITY AND PERFORMANCE ANALYSIS

3.1 SECURITY ANALYSIS

Attack 1:

If an adversary tries to derive the private key d_i from X_i , then he has to solve Elliptic Curve Discrete Logarithm Problem (ECDLP). That is, the adversary cannot derive d_i from d_iP which is the strength of elliptic curve cryptosystem.

Attack 2:

An adversary tries to forge the signature (s, Y) for a message m as $(z+s, Y)$. To forge the valid signature, he selects a number randomly and appropriately for z but could not evaluate and prove that $(z+k+ed)P$ equals $Y+eX$. Hence forged message results in failure.

Attack 3:

If an adversary tries to forge the signature with the verification equation $v1=sP$, then again he has to solve Elliptic Curve Discrete Logarithm Problem since the strength of the verification equation relies on the strength of elliptic curve cryptosystem.

Attack 4:

In Chen et al's scheme, since the key generation and signature generation is done by the same signer say U_n who is the last signer in the multi-signature scheme. Liu et.al [19] proves that this scheme is vulnerable to insider attack. That is, the signer U_n could sign a legal signature which other signers have signed and forge a signature himself which could be accepted by the verifier.

In the proposed scheme since the last signer is usually the trusted group admin who is going to monitor every signer in the group, the above stated attack can be avoided.

The group admin, if suspected can randomly check and ensure whether a signer in the group has signed the message. If a signer U_n , tries to forge a signature himself as $X_N = X - \sum_{i=1}^N X_i$ and sends X_n to group admin, then it can be identified by the group admin as follows:

Let U_s be a signer in the group and if the group admin wants to audit whether this signer has signed the document, then the group admin evaluates the following formula to verify it.

$$\begin{aligned} & sP - (Y - Y_s) - eX \\ &= (\sum_{i=1}^N s_i \text{ mod } n)P - (Y - Y_s) - eX \\ &= [(\sum_{i=1}^N k_i)P + e(\sum_{i=1}^N d_i)P] + (\sum_{i=1}^N Y_i - Y_s) + e(\sum_{i=1}^N X_i) = Y_s \end{aligned}$$

If the group admin does not get the audited signer’s public key as a result of the evaluation, then it is ensured that either the audited signer has not signed the document or the signature is forged. Since this evaluation can be done for all the signers in the group randomly at each time, the insider attack as specified by Liu et al. is overcome in the proposed protocol.

3.2 PERFORMANCE ANALYSIS

The proposed protocol is compared with the signature schemes proposed by Nyang and Song, Chen et al., Sahu and Sharma, and Chande and Thakur’s schemes. Table 1 depicts the notations and its description used for performance analysis. Table 2 represents the computational time of various operations.

Table 1. Notations and its Description.

Notation	Description
T_{ec-mul}	Time complexity for executing a number and elliptic curve point multiplication
T_{ec-add}	Time complexity for executing addition of two points in an elliptic curve
T_{ec-sub}	Time complexity for executing subtraction of two points in an elliptic curve
T_{exp}	Time complexity for executing modular exponentiation
T_{mul}	Time complexity for executing modular multiplication
T_{add}	Time complexity for executing modular addition
T_{inv}	Time complexity for executing modular inversion
T_{hash}	Time complexity for executing hash function

Table 2. Various operation units converted into T_{mul} .

$$T_{exp} \approx 240 T_{mul} \quad T_{ec-mul} \approx 29 T_{mul} \quad T_{ec-add} \approx 0.12 T_{mul} \quad T_{add} \text{ is negligible}$$

Table 3 shows the comparison between various digital multi-signature schemes and the proposed protocol on the basis of time complexity. From Table 3, it is revealed that the time complexity of the proposed digital multi-signature protocol is comparatively less than other signature schemes thereby proves the high efficiency of the signature generation and verification of the proposed protocol.

Table 3. Comparison of various Digital Multi-Signature schemes.

Schemes	Multi-Signature generation Phase		Multi-Signature verification Phase	
	Time complexity	Complexity in terms of T_{mul}	Time complexity	Complexity in terms of T_{mul}
Nyang and Song [12]	$2T_{exp}+(3N-2)T_{mul}+$ 1 Hashing	$(3N+478)T_{mul}+$ 1 Hashing	$2T_{exp}+(N+1)T_{mul}$ + 1 Hashing + $NT_{inv}(N-1)T_{add}$	$(N+481)T_{mul}+ NT_{inv}+$ 1 Hashing
Chen et al. [14]	$2T_{ec-mul}+NT_{ec-add}+$ $2NT_{add}+2T_{mul}+$ 1 Hashing	$(0.12N+60)T_{mul}+$ 1 Hashing	$3T_{ec-mul}+2T_{ec-add}+$ 1 Hashing	$87.24T_{mul}+ 1$ Hashing
Sahu and Sharma [18]	$3T_{ec-mul}+NT_{add}+$ $NT_{mul}+1$ Hashing	$(N+87)T_{mul}+$ 1 Hashing	$3T_{ec-mul}+$ 1 Hashing	$87T_{mul}+1$ Hashing
Chande and Thakur [20]	$3T_{ec-mul}+NT_{ec-add}+$ $3T_{mul}+1$ Hashing	$(0.12N+90)T_{mul}+$ 1 Hashing	$2T_{ec-mul}+T_{mul}+$ 1 Hashing	$59T_{mul}+ 1$ Hashing
Proposed protocol	$T_{ec-mul}+NT_{ec-add}+$ $T_{add}+T_{mul}+NT_{add}$ 1 Hashing	$(0.12N+30)T_{mul}+$ 1 Hashing	$2T_{ec-mul}+T_{ec-add}+$ 1 Hashing	$58.12T_{mul}+ 1$ Hashing

4. CONCLUSIONS

Elliptic Curve Cryptography is one of the most promising methods in the public key cryptography field. It provides many advantages over other cryptographic methods. The proposed digital multi-signature protocol is constructed based on the strength of elliptic curve discrete logarithm problem. The proposed protocol overcomes the attack as specified by Liu et al. in the Chen et al.'s digital multi-signature scheme. Also the performance analysis proves that the proposed protocol is efficient with reduced time complexity compared to other digital multi-signature schemes.

5. FUTURE WORK

The extension of Digital signature is the Digital Multi-Signature in which more than one signer participates in signing a document. The proposed Digital Multi-Signature protocol is designed for a group of signers to sign the whole document cooperatively. There are circumstances, where these signers are expected to sign a particular section of a document rather than signing the whole document. There are many solutions available for this kind of Multi-Signature scheme with distinguished signing authorities. But an improved Elliptic Curve Based Multi-Signature scheme with distinguished signing authorities with reduced time complexity is required and has to be implemented in future which should yield better results than the existing Signature schemes.

REFERENCES

- [1] R.L. Rivest, A. Shamir, and L. Adleman, (1978) "A method for obtaining digital signatures and public-key cryptosystems", Communications of the ACM, vol. 21, no. 2, pp. 120–126.
- [2] T. Elgamal, (1985) "A public key cryptosystem and a signature scheme based on discrete logarithms," IEEE Transactions on Information Theory, vol. 31, no. 4, pp. 469-472.
- [3] A. Shamir, (1985) "Identity-based cryptosystems and signature schemes", Advances in Cryptology - CRYPTO'84, LNCS 196, Springer-Verlag, pp. 47–53.

- [4] N. Koblitz, (1987) “Elliptic Curve Cryptosystem”, Mathematics of Computation, vol. 48, no. 177, pp 203-209.
- [5] Victor S. Miller, (1986)“Use of Elliptic Curves in Cryptography”, Advances in Cryptology – CRYPTO’85, LNCS 218, Springer-Verlag,pp. 417-426.
- [6] D. Johnson, A. Menezes, S. Vanstone, (2001) “The Elliptic Curve Digital Signature Algorithm (ECDSA), International Journal of Information Security, vol.1, pp. 36-63.
- [7] S. Vanstone, (1992)“Responses to NISTs Proposal”, Communications of the ACM, vol. 35, pp. 50-52.
- [8] ISO/IEC 14888-3,(1998) “Information technology – securitytechniques – digital signatures with appendix. Part 3: Certificatebased-mechanisms”, International Organization forStandardization, Geneva.
- [9] ANSI X9.62,(1999) “Public key cryptography for the financial services industry: the elliptic curve digital signature algorithm (ECDSA)”.
- [10] IEEE P1363, (1999) “Standard specifications for public-key cryptography”, Draft Version 13, November-12.
- [11] National Institute for Standards and Technology, (2000)“Digital Signature Standard (DSS)”, FIPS Pub.186-2.
- [12] D. Nyang and J. Song, (2000)“Knowledge-proof based versatile card verification protocol”, Computer Communication Review, ACM SIGCOM, vol. 30, pp. 39-44.
- [13] K. Itakura and K. Nakamura, (1983)“A public key cryptosystem suitable for digital multisignatures”, NEC Research and Development, vol. 71, pp. 1-8.
- [14] T. S. Chen, K. H. Huang, and Y. F. Chung, (2004)“Digital multi-signature scheme based on the elliptic curve cryptosystem,” Journal of Computer Science and Technology, vol. 19, no. 4, pp. 570.
- [15] L. Harn and J. Ren, (2008) “Efficient identity-based RSA multisignatures”, Computers & Security, vol. 27, pp. 12–15.
- [16] F.Y. Yang, J.H. Lo, and C.M. Liao, (2010) “Improvement of an Efficient ID-Based RSA Multisignature,” International Conference on Complex, Intelligent and Software Intensive Systems (CISIS), pp. 822–826.
- [17] F. J. B.Domiguez, L. H.Encinas, (2011) “Digital identity-based multisignature scheme implementation”, INFOCOMP 2011 : The First International Conference on Advanced Communications and Computation.
- [18] H. Sahu and B. K. Sharma, (2011) “An MSS Based on the Elliptic Curve Cryptosystem”, International Journal of Network Security, Vol.12, no.1, pp. 1–3.
- [19] D. Liu, P. Luo, and Y.Q Dai, (2007) “Attack on Digital Multi-Signature Scheme Based on Elliptic Curve Cryptosystem”, Journal of Computer Science and Technology, Vol.22, no.1, pp. 92-94.
- [20] M.K.Chande and B.S.Thakur, (2014) “An Elliptic Curve Based Multi-Signature Scheme For Wireless Network”, International Journal of Information & Network Security, Vol.3, no.1, pp. 33-39.
- [21] M. Amir, J. Ahmed, S. Bansal, A. K. Garg, and M. Singh, (2014) “Digital Signature Scheme Using Two Hash Functions”, International Journal of Science and Research, Vol.3, no.4, pp. 126-128.

AUTHORS

Sudha Devi is currently working as Assistant Professor in the Department of Computing, Coimbatore Institute of Technology, Coimbatore, India and is a Ph.D. scholar in Anna University of Technology, Chennai, India. Her research focuses on Cryptography and Network Security, Security in Cloud Computing.



Dr.K.Thilagavathy is currently working as Associate Professor in the Department of Physics, Coimbatore Institute of Technology, Coimbatore, India. She is handling classes for B.E/B.Tech students since 1992. She obtained her doctoral degree from Avinashilingam University for Women, Coimbatore in 2009. Currently she is involved in image processing and Information security projects.



Preethi Sai Krishnan is currently pursuing MSc. Software Engineering at Coimbatore Institute of Technology. Her area of interest are information security and problem solving techniques. Other interest includes working on parallel programming and algorithms.

