IMPLEMENTATION OF PROVABLY-SECURE DIGITAL SIGNATURE SCHEME BASED ON ELLIPTIC CURVE

Dhanashree Toradmalle
Research Scholar: Department of CSE
K L E Foundation, Guntur, Andhra Pradesh, India
dhanashree.kt@gmail.com

Jayabhaskar M
Associate Professor: Department of CSE
K L E Foundation, Guntur, Andhra Pradesh, India
jayabhaskar@kluniversity.in

B Sathyanarayana
Professor: Department of Computer Science & IT,
Sri Krishnadevaraya University, India
bachalasatya@yahoo.com

Abstract - Digital Signatures are viewed as the foundation of the online exchanges of the computerized world. They guarantee non repudiation for the activities of the sender and furthermore ensure security. Over some undefined time frame the digital signatures have developed and numerous enhancements have been finished by scientists to the standard plans. This paper develops an understanding of variants in accordance to their computational costs and response to attacks. The authors present a scheme which withstands the drawbacks of its pre-decessor the Jhong's digital signature, implements the solution and proves it to be sturdy with regard to computational costs as compared to other methods and also taking care of the attacks. The results depict the proposed scheme to be worthy either at signature generation, signature verification in terms of its computational costs or its ability to stand the attacks. Overall, the proposed scheme stands tall in all aspects.

Keywords: Digital signature, RSA, ECC, ECDSA

1. Introduction

Today with the online exchanges which are producing huge information the duty regarding the information sent over transmission is pivotal. A digital signature [1-2] is necessary to correspondence.

1.1. *Why Digital Signatures?*

- No requirement for commonly believed specialists like certification authorities [3-4].
- Digital rights management (DRM) [5], including specialized, lawful, social, and business angles, ought to give a premise to controlling and ensuring the new asset data, i.e., the computerized resources of individuals, organizations, and government associations.
- In complexity to physical proof, digital signatures are anything but difficult to transmit, file, search, and check.
- Digital marks guarantee to give an exquisite answer
- For the non-repudiation issue in the digitally operating economy.
- Due to the guessed security of the fundamental cryptographic systems [6], digital signatures additionally guarantee significantly higher security contrasted with conventional signatures, and, henceforth, less disputes and less complex debate goals.
- A boundless desire for digital signatures is that they permit evading the requirement for physical proof and witnesses.

1.2. *What is a Digital Signature?*

The digital signature depends on public key encryption [7-8] innovation. It's essential rule [9] is basic and it works in the accompanying advances:

(1) The sender makes a fixed length digital digest from the message and encrypts it with his private key to shape his digital signature.

(2) The digital signature is then annexed to the message and sent to the beneficiary with the message.

(3) While the receipt computes the first message by Hash work and get digital digest H1 and afterward decrypts the signature expression by the sender's public key and gains H2.

(4) If HI is equivalent to H2, the beneficiary realizes that it is the holder of the sender's private key who sent the message.

1.3. *Algorithms used in a Digital Signature are*

(1) Hash Algorithms [9]: Hash function H maps a variable length message M as input and produce a fixed sized hash value. h= H (M)

Various hash algorithms, their characteristics and hash size are listed below:

Table 1. Hash algorithms in Digital Signatures

Name of Algorithm	Type and Characteristics	Hash Size
Secure Hash Algorithm 1 (SHA1)	FIPS approved; other versions (SHA256, SHA384, SHA512) provide longer outputs	160 bits
Message Digest 5(MD5)	Potential weakness is that it can be used as a keyed hash	128 bits
RACE Integrity Primitives Evaluation Message Digest 160 (RIPEMD-160)	Developed as part of the EC's Research and Development in Advanced Communications Technologies in Europe (RACE)	160 bits
TIGER Hash	Designed for efficient operation on 64-bit platforms	192 bits

(2). Digital Signature Algorithm:

Digital Signature Algorithm (DSA), Rivest Shamir-Adleman (RSA) [7], and Elliptic Curve DSA (ECDSA)[9]which are caught in FIPS PUB 186-2 are three Digital Signature algorithms. These algorithms are utilized for digital signature alongside their qualities and minimum key sizes are recorded in table beneath.

Table 2. Digital Signature Algorithms

Name of Algorithm	**Type and Characteristics**	**Minimum Key size**
Digital Signature Standard (DSS)	FIPS 186-2 digital signature Digital signature based on SHA1 hash, unencumbered (no patents, no licenses)	1024 bits
RSA Digital Signature	RSA digital signature (FIPS approved) Previously patented digital signature	1024 bits
Elliptic Curve Digital Signature (ECDSA)	Digital signature based on elliptic curve key technology uses smaller keys than other public key technologies	160 bits

1.4. *Cryptography:*

The encryption [10] and decryption are important phases of the cryptography and both require the utilization of some secret data for example key. Cryptography includes two principles Symmetric and Asymmetric [11] draws near:

(1) Symmetric-key cryptography: Same secret key is utilized for both encryption and decryption.

(2) Asymmetric-key cryptography: Two distinct keys are utilized for example one for encryption and other for decryption

Table 3. Cryptographic Algorithms

Kind of Cryptography	Examples
Hash Functions	MD4-5, SHA-0-1-2, RIPDEM
Symmetric Key Cryptography	DES, AES, 3DES, RC4
Public Key Cryptography	ECC, RSA, DSA, ElGammal

Table 4. Key sizes of Cryptographic Algorithms

Private key size (bits)	Public Key Size (bits)		MIPS To attack	Protection Lifetime
	ECC	RSA/DH/DSA		
80	160	1024	10^{12}	Until 2010
112	224	2048	10^{24}	Until 2030
128	256	3072	10^{28}	Beyond 2030
256	384	7680	10^{47}	-
512	512	15360	10^{66}	-

Table 5. Public Key Cryptosystems & Their Underlying Mathematical Problems

Cryptosystems	Mathematical Problem	Description
RSA, Rabin Williams	Integer factorization	Given a number n, find its prime factors
ElGammal, DSA, Diffie Hellman	Discrete logarithm	Given a prime n, and numbers g and h, find x such that h = gx mod n
ECDSA, EC Diffie-Hellman	Elliptic curve discrete logarithm	Given an elliptic curve E and points P and Q on E, find x such that Q = x.P

Table 6. Public Key Cryptosystems & Their Underlying Mathematical Problems

ECC Key Size(bits)	RSA Key Size(bits)	Key Size Ratio
163	1024	1:6
256	3072	1:12
384	7680	1:20
512	15360	1:30

1.5. *Why ECC [9]?*

(1) Less number of bits:

(2) Wide selection of finite fields and curves:

(3) Power Consumption:

(4) Computational Efficiency

ECC is used as a secured and sturdy method in various applications [12-14]. ECC is also used in combination with encryption standards like AES [15] or other cryptographic methods [16] to give better performance. So, we can say without any doubt that ECC is the stronger and the faster (efficient) amongst the present techniques

2. Literature Survey

ECDSA has undergone many modifications in the last few decades to make it secure, efficient and to adapt to a whole range of applications. Some variants to ECSDA are discussed below:

The digital signature which today lays the foundation of any method following non repudiation with ECC was first introduced by Scott Vanstone (1992) [17]. Duplication in signatures was a major concern handled by John Malone-Lee et al. (2003) [18] Qiuxia Z et al. (2011) [19] modified the ECDSA method to add security so that major pitfalls are overcome which added hurdles in the application of ECDSA demanding very high security requirements. Shweta Lamba et al (2013) [20] focusses more on the need of minimizing the ECC operations in ECDSA to make the method more efficient in terms of time. Following the same footsteps of providing a more efficient ECDSA Sumanth Koppula, et al (2016) [21] succeeded in removal of modular inverse operations in the signature generation and signature verification phases which take more computation time. Their method worked well for devices with computational constraints. Sensor networks also need security in resource short conditions.

To support such demands Sindhu B et al. (2016) [22] presented a secure digital signature scheme based on EC for IOT (Internet of Things). Today, tremendous applications of wireless sensor Sensor networks have flooded the market. With such a high utilization ratio it is critical to assure the safe communication between the participating stations. This prime factor of the sensor stations on low force utilization and less asset is handled by a lightweight cryptographic calculation which is structured well so that it's a perfect to build a riskless WSN plot. The work presented by the Hong Jhong et al (2016) [23] in their proposal describes an improved elliptic bend cryptography digital signature scheme by methods for upgrading the multiplicative inverse module of ECDSA, in light of ECC lightweight cryptographic calculation which is structured well so that it's a perfect to build a riskless WSN plot.

3. Proposed method

By just changing the hash value, the Middle Man or interloper can without a ton of stretch alter or supervene upon the message that can't be seen by the recipient. Remembering the necessities of ECDSA that are littler key size and high security researchers are following up on the issues .The up to referenced Jhong's plan [23] attempts to achieve power by decreasing the save standard inverse operations, but it neglects to accomplish security; in light of the fact that the intruder will essentially adjust the message and supplant the current message hash an incentive with changed hash value and in this way it neglects to achieve security traits of digital signature scheme. Dhanashree K Toradmalle et al [24] gives a point by point cryptanalysis of the Jhong's arrangement and shows how Jhong's method is vulnerable to man in the middle attack We thusly propose an arrangement which ensures that the Forward Secrecy and Intruder ambushes can be dealt with and guarantee an amazing ECDSA. The proposed Algorithm is introduced by Dhanashree K Toradmalle et al in [25] as follows:

1) Key generation

Using generating point G and random integer number r the public key K is computed as follows:

a. Choose a random integer number r in interval [0, n-1].

b. Compute K = r * G

c. The key-pair combination is (r, K) where r is the Private Key and K is the Public key.

2) Signature generation

To sign on message m utilizing the domain parameter and Private key the accompanying advances are performed by the Signer:

a. Selects a random integer p (secret key) with $1 \leq p \leq n - 1$.

b. Determine the value of z = H(m)

c. Determine $f = ((z + p) \oplus (p + r))$

d. Determine d = x-coordinator (f * G)

e. Determine s = (z * r) +f mod n. If s = 0 then return to step 1.

f. Signature for the message m is (d, s).

3) Signature verification

At the Receiver side the message m ought to be validated with the following steps:

a. Firstly, confirm that s is an integer in the interim $[1, n - 1]$

b. Compute the hash value z of the message/document m

c. W = (x1, y1) = s * G – z * K

d. v = x-coordinate(W)

Finally, authenticate the signature by checking whether the equivalence v = d holds

In the event if the signature for the message m is (d, s) and was genuinely generated by the authorized Sender then s = (z * r) + f mod n. The correctness of the algorithm can be tested using the following proof:

W = s * G – z * K
= ((z * r) + f) * G – z * K
= z * r * G + f * G – z * K
= z * K + f * G – z * K
= f * G
x-coordinate (W) = x-coordinate (f * G)
Hence, v = d

Thus, method proposed by Hong Jhong et al [23], is deficient in surpassing the man in the middle attack, which is overcome by the above proposed proof.

4. Results of the proposed method

Key Generation

G=(48439561293906451759052585252797914202762949526041747995844080717082404635286,361342509
56749795798585127919587881956611106672985015071877198253568414405109)

EllipticCurve: y^2 = x^3 +
115792089210356248762697446949407573530086143415290314195533631308867097853948x +
41058363725152142129326129780047268409114441015993725554835256314039467401291 (mod
115792089210356248762697446949407573530086143415290314195533631308867097853951)

Private Key r =
115792089210356248762697446949407573530086143415290314195533631308865484340366

Public Key K =
(64070388292226317886083782502994530357706271618903557416432268953467836967156,145553697986
03565601617000461766331801960413885522907208433355533988093305315)

Signature Generation

p = 691073039

m = Paul hated school. He did not do his home work

z = 947124683639364379868979251846050436554410637 44

f = 94712468453124629082035744297401305932282297985

f * G =
(41656467641898598658239959141925700712163423128878235868865075420876131965418,111446883862
22828794262233994126168962829579648758753277620059813129454711 1184)

d=41656467641898598658239959141925700712163423128878235868865075420876131965418

s=41784218361396297610597838221766822795591931738237480582538036561267391844907

Signature Verification

d=41656467641898598658239959141925700712163423128878235868865075420876131965418

s=41784218361396297610597838221766822795591931738237480582538036561267391844907

m = Paul hated school. He did not do his home work

z = 94712468363936437986897925184605043655441063744

s*G=(63834385106482118401410928650226898771167478588255082401886455990144870353303,4456501
36270177081291553925209020399276635883642986163627044256491882 2013818)

z*K=(41756382440400949538169385491142826015744583883111230538544845021332048094305,1108902
87173084794171806106118057098114534038187812745819589257400176714670445)

W=(41656467641898598658239959141925700712163423128878235868865075420876131965418,111446883
8622282879426223399412616896282957964875875327762005981312945471 11184)

v=41656467641898598658239959141925700712163423128878235868865075420876131965418

v = d

Signature is accepted

5. Comparative Study

The cost and efficiency of ECDSA schemes depends on the number of operations used in the methods. The Elliptic Curve point multiplication, elliptic curve point addition, modular inverse and modular multiplication together are the operations that determine the computational cost of the scheme. The computational cost for signing and verification of variant schemes under study with the proposed scheme are calculated as discussed by Morteza Nikooghadam et al. [26] and presented in the Table 7 and Table 8. Further the type of attacks that the system involves are also presented in Table 7.

Table 7. Comparison of computational cost for Signature generation in variants of ECDSA with security plans

Scheme	ECPM	ECPA	INV	MUL	Computation cost in terms of Multiplication	Attack
Sumanth Koppula et al[21]	2	0	0	4	31.073	NA
Hong Zhong et al[23]	1	0	0	1	30	MIM
PROPOSED SCHEME	1	0	0	1	30	NA

Abbreviations:

Elliptic Curve Point Multiplication (ECPM)
Elliptic Curve Point Addition (ECPA)
Modular inverse (INV)
Modular Multiplication (MUL)
Known Message Attack: MA
Man-in- the-middle Attack: MIM
NA: No Attack

Table 8. Comparison of computational cost for Signature Verification in variants of ECDSA with security plans

Scheme	ECPM	ECPA	inv	mul	Computation cost in terms of Multiplication
Sumanth Koppula et al[21]	2	1	0	1	59.12
Hong Zhong et al[23]	2	1	0	0	58.12
PROPOSED SCHEME	2	1	0	0	58.12

6. Conclusion

Due to the vast application domain in key areas, Security plays a significant role in the success of every application over the internet. For decades now researchers have been adopting various means to build sturdy digital signature schemes to resist the protection loopholes. At the same time, they are also trying to reduce the computational costs involved by minimizing the number of elliptic curve mathematical operations. The organized study of different variants is analyzed for its computational cost and security aspect in terms of withholding the attacks. The proposed method overcomes the drawback of its peer Jhong's scheme. The Jhong's scheme which is vulnerable to man in the middle attack is surpassed by the proposed scheme. It also gives better results compared to other variants either in terms of computational cost involved in signature generation or verification or withstanding the attacks. Thus, the merits of the proposed scheme make it stand out when compared with its counterparts.

References

[1] R.L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystem," Comm ACM, vol. 21, pp. 120-126, Feb. 1978.

[2] S R Subramanya and Byung K Yi, "Digital Signatures", IEEE Potentials Volume: 25, Issue: 2, March-April 2006

[3] Thomas F Rebel,Olaf Darge, Wolfgang Koenig, " Approaches for Digital Signature Legislation", Trends in Distributed Systems For electronic Commerce, Internationa IFIP/GI Working Conference TREC'98, Hamburg Germany June 1998 Proceedings.

[4] Sangram Ray, G.P. Biswas, "A Certificate Authority (CA)-based cryptographic solution for HIPAA privacy/security regulations", Journal of King Saud University – Computer and Information Sciences (2014) 26, 170–180

[5] S R Subramanya and Byung K Yi, "Digital Rights Management", IEEE Potentials, Volume: 25, Issue: 2, March-April 2006

[6] Hankerson, A. Menezes, S. Vanstone, Guide to Elliptic Curve Cryptography Springer 2004), ISBN 0-387-95273-X.

[7] R. L Rivest, A Shamir and L Adleman, " A Method for Obtaining Digital Signatures and PublicKey Cryptosystems", Communications of the ACM Vol.21,Issue 2,February 1978.

[8] Mihir Bellare, Anand Desai, david Pointcheval and Phillip Rogaway, “Relations among Notions of security for Public Key Encryption Schmes”, Annual International Cryptology Conference CRYPTO’ 98: Advances in cryptology-CRYPTO’98 pp 26-45, Part of Lecture Notes in Computer Science Book Series(LNCS volume 1462)

[9] Don Johnson, Alfred Menezes,Scott Vanstone “ The Elliptic Curve Digital Signature Algorithm(ECDSA)”, Intrenational Journal of Information Security,Vol 1.pages36-63(2001)Springer

[10] Dixit, R., & Ravindranath, K. (2018). Encryption techniques & access control models for data security: A survey. International Journal of Engineering and Technology(UAE), 7(1.5 Special Issue 5), 107-110

[11] Gowtham Tumati, Yalamarthi Rajesh, Manogna T, J. Ram Kumar, “A New Encryption Algorithm Using Symmetric Key Cryptography”, International Journal of Engineering and Technology,2018

[12] Jayabhaskar Muthukuru & Prof. Bachala Sathyanarayana, “Fixed and Variable Size Text Based Message Mapping Techniques Using ECC”,Global Journal of Computer Science & Technology, Volume 12 Issue 3, February 2012

[13] T.Santhi Vandana,S.Venkateshwarlu, “ Eliptic Curve Cryptography Based Anonymous Authentication Scheme for Wireless Body Area Networks”, Journal of Advanced Research in Dynamical and Control Systems,Vol 11,Issue 2,2019

[14] M. S. N. G. K. Mounika, Arvind Yadav, S. Lokesh Anand, P. Satyannarayana, “ Upgrade of GSM Security Using Elliptic Curve Cryptography Algorithm”, International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-8 Issue-7 May, 2019

[15] Gayathri, P., Umar, S., Sridevi, G., Bashwanth, N., & Srikanth, R. (2017). Hybrid cryptography for random-key generation based on ECC algorithm. International Journal of Electrical and Computer Engineering, 7(3), 1293-1298. doi:10.11591/ijece.v7i3.pp1293-1298

[16] N. Sirisha and K.V.D. Kiran, “An Efficient and Lightweight Security Scheme for Big Data”, International Journal on Emerging Technologies,Dec 2019

[17] Vanstone S. A.: Responses to NIST’s Proposal. Communications of the ACM. 1992

[18] John Malone-Lee, Nigel P. Smart: Modifications of ECDSA. Springer LNCS. 2003: 1-12

[19] Qiuxia Z, Zhan L, Chao S: The implement of Digital Signature Algorithm Based on Elliptic Curve Cryptography. IEEE 2011

[20] Shweta Lamba, Monika Sharma: An Efficient Elliptic Curve Digital Signature Algorithm (ECDSA). International Conference on Machine Intelligence Research and Advancement;2013; IEEE

[21] Sumanth Koppula, Jayabhaskar Muthukuru, “Secure Digital Signature Scheme Based on Elliptic Curves for Internet of Things” International Journal of Electrical and Computer Engineering (IJECE) Vol. 6, No. 3, June 2016, pp. 1002 ~ 1010.

[22] B.Sindhu, Dr.R.M.Noorullah: Secure Elliptic Curve Digital Signature Algorithm for Internet of Things. Global Journal of Computer Science and Technology 2016

[23] Hong Zhong, Rongwen Zhao, Jie Cui, Xinghe Jiang and Jing Gao, "An Improved ECDSA Scheme for Wireless Sensor Network” International Journal of Future Generation Communication and Networking, vol. 9, no. 2, pp. 73-82, 2016.

[24] Dhanashree K. Toradmalle, Jayabhaskar Muthukuru, B. Sathyanarayana,"Cryptanalysis of an Improved ECDSA," International Journal of Engineering Research and Technology, vol. 11, no. 4, pp. 615-619, 2018.

[25] Dhanashree K. Toradmalle, Jayabhaskar Muthukuru, B. Sathyanarayana," Certificateless and provably-secure digital signature scheme based on elliptic curve”, International Journal of Electrical and Computer Engineering (IJECE) Vol. 9, No. 4, August 2019

[26] Morteza Nikooghadam, Ali Zakerolhosseini: An Efficient Blind Signature Scheme Based on the Elliptic Curve Discrete Logarithm Problem. The ISC Int'l Journal of Information Security 2009:125-131