International Journal of Electrical and Computer Engineering (IJECE)
Vol. 9, No. 4, August 2019, pp. 3228~3231
ISSN: 2088-8708, DOI: 10.11591/ijece.v9i4.pp3228-3231

Certificateless and provably-secure digital signature scheme based on elliptic curve

Dhanashree Toradmalle[1], Jayabhaskar Muthukuru[2], B. Sathyanarayana[3]
[1,2]Department of CSE, KLEF, India
[3]Department of Computer Science and IT, Sri Krishnadevaraya University, India

Article Info

Article history:

Received Jul 26, 2018
Revised Mar 22, 2019
Accepted Apr 3, 2019

Keywords:

Digital signature
Elliptic curve
Elliptic curve digital signature algorithm
Forward secrecy

ABSTRACT

With the internet today available at the user's beck, and call data or Information Security plays a vital role. Confidentiality, Integrity, Availability, and Non-repudiation are the pillars of security on which every application on the web is based on. With these basic requirements the users also need the security in low resource constrained environments making it more challenging for the security experts to design secured cryptographic algorithms. Digital Signatures play a pivotal role in Authentication. They help in verifying the integrity of the data being exchanged. Elliptical curves are the strongest contenders in Digital Signatures, and much research is being done to enhance the method in many ways. The paper briefs a secured and improved ECDSA Elliptical Curve Digital Signature Algorithm which is an improved and secured version of the Digital Signature Algorithm.

Copyright © 2019 Institute of Advanced Engineering and Science.
All rights reserved.

Corresponding Author:

Dhanashree K Toradmalle,
Department of CSE,
Koneru Lakshmaiah Education Foundation (KLEF),
Vaddeswaram, Andhra Pradesh 522502, India.
Email: dhanashree.kt@gmail.com

1. INTRODUCTION

A digital signature [1] is a technique by which the Sender can sign an electronic report for the Verifier to keep as a confirmation that the message was to be sure sent initially from the Sender. The National Institute of Standards and Technology (NIST) have proposed Digital Signatures as standards which are worldly accepted. The primary choices available for public key systems are:

- RSA
- Diffie-Hellman (DH) or Digital Signature Algorithm
- Elliptic Curve Digital Signature Algorithm

RSA is a framework that was distributed in 1978 by Rivest, Shamir, and Adleman, based on the difficulty of factoring large integers. Whitfield Diffie furthermore, Martin Hellman proposed the general population key framework presently called Diffie-Hellman Key Exchange in 1976.DH and DSA work for key agreement and Digital signature respectively and can be consolidated to do verified key agreement. They are based on the difficulty of solving the discrete logarithm problem in the multiplicative group of integers modulo a prime p. In 1985 elliptic curve groups were presented by Neal and Koblitz as an alternate for multiplicative groups modulo p. Elliptic curve based digital signatures overcame all the drawbacks of its predecessors with smaller key size thus entering the foray of applications with resource constraints. [2]. The major areas of IoT applications [3] face challenges for resource constrained applications which will surely benefit from the ECDSA based IoT applications in terms of security. The wireless sensor networks are another domain where ECC based applications are in vogue [4]

Elliptical Curve Cryptography [ECC] optimizes encryption and decryption processes of several methods. The procedure of ECC comprises of following phases [5]:

- Determining the prime points on the elliptic curve
- Forming the public and private key
- Encoding
- Encryption
- Decryption
- Decoding

Various authors have represented the elliptical curve digital signature algorithm (ECDSA) with relating equations in their literature [6-8]. They use their own conventions to present the ECDSA scheme. However, primarily ECDSA needs the accompanying significant calculations:

- Generation of a key combine (private key, public key),
- The calculation of a signature,
- And, the confirmation of the signature

There are many advantages of ECDSA over its predecessors [9]:

- More Secure
- Low computation resources
- Small key sizes

In real-time three cases occur most ordinarily inside the method of communication:

- Message has been tampered.
- The sender denies causing the message.
- The receiver faux the message

ECDSA though is the most groundbreaking of all the asymmetric digital signature strategies, specialists are putting every one of their endeavours to make it more grounded to withstand different difficulties. Scientists have also proposed Elliptic curve Digital signature scheme based on certificates [10]. The following are the parameters to strengthen the ECDSA where research is going on:

- Forward Secrecy [11-12]:

  Digital Signatures empower the Signer to ensure the security of messages marked in the past regardless of whether his mystery key is uncovered today.
- Attacks on Security:

  Various attacks like forgery attack [13], replay attack [14], man in the middle attack pose a danger to security.

Attacks break the security and non-repudiation attributes of the ECDSA. Xianmin Wei et al [15], states improvements in ECC but fails to capture the security aspects in attacks by just focusing on the modular operations. Neetesh Saxena et al [9] proposes variants to ECDSA which focus on efficiency again, underestimating the attacks on security. Jie Liu and Jianhua Li [16] exhibits a cryptanalysis of Chang et al's. Digital signature scheme, which was professed to oppose forgery attacks without utilizing any oneway hash capacity or padding any redundancy. Further they also propose improved signature plans, in which the length of the digital signature is a lot shorter. Lei Niu [17] presents progressively forgery attacks to tell unmistakably the best way to obtain the attacks. Jianhong Zhang and Shengnan Gao [18] breakdown the blind signatures and demonstrate that they are definitely not secure; finally giving a solution for the same. Xinghua Zhang [19] discusses an enhanced technique to overcome forgery attacks. Long Zhaohua et al [20] restrict the "*Man-in-the-Middle*" attacks but requires three entities participating in identification authentication process in the wireless network, such as Station (STA), Access Point (AP), and Authentication Server (AS) which is an overhead to the application.

2. PROPOSED ALGORITHM

The Middle Man or intruder can without a lot of stretch modify or supervene upon the message that can't be perceived by the receiver, by merely adjusting the hash value Researchers are acting on the on top of problems keeping in mind the necessities of ECDSA that are smaller key size and high security. The afore mentioned Jhong's scheme [21] tries to attain potency by reducing the reserve standard inverse operations however it fails to attain security; because the intruder will simply alter the message and replace the present message hash value with changed hash value and thereby it fails to attain security attributes of a digital signature scheme. Dhanashree K Toradmalle et al [22] gives a point by point cryptanalysis of the Jhong's plan and shows how Jhong's technique is inclined to man in the center assault We along these lines propose a plan which guarantees that the Forward Secrecy and Intruder assaults can be taken care of and ensure a powerful ECDSA. The proposed Algorithm is stated as follows:

2.1. 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.

2.2. 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≤ p ≤ n −1.
b. Determine the value of z = H(m)
c. Determine f = ((z + p) ⊕ (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).

2.3. 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.

3. RESULTS AND DISCUSSIONS

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:

$$\begin{aligned} W &= s * G - z * K \\ &= ((z * r) + f) * G - z * K \\ &= z * r * G + f * G - z * K \\ &= z * K + f * G - z * K \\ &= f * G \end{aligned}$$

x-coordinate (W) = x-coordinate (f * G)

Hence, v = d

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

4. CONCLUSION

The Elliptical curve digital signature is being redeveloped and increased by several researchers to create it sturdy to resist the protection loopholes. The projected technique suggests a safer and sturdy ESDSA scheme that delivers a robust ECDSA within the context of forward secrecy and attack situations

REFERENCES

[1] Sung-Ming Yen and Chi-Sung Laih, "Improved Digital Signature Algorithm," *IEEE Transactions On Computers*, vol. 44, no. 5, May 1995.

[2] Kirstin Lauter, "The Advantages of Elliptic Curve Cryptography For Wireless Security," *IEEE Wireless Communications*, Feb 2004.

[3] Yousra Abdul Alsahib S. aldeen, Kashif Naseer Qureshi, "New Trends in Internet of Things, Applications, Challenges, and Solutions," *TELKOMNIKA (Telecommunication, Computing, Electronics and Control)*, vol. 16, no. 3, pp. 1114-1119, Jun 2018.

[4] Younsung Choi, "Cryptanalysis on Privacy-aware Two-factor Authentication Protocol for Wireless Sensor Networks," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 8, no. 1, pp. 605-610, Feb 2018

[5] Dicky Nofriansyah, Afzalur Syaref, Widiarti R Maya, Ganefri Ganefri, Ridwan, "Efficiency of 128-bit Encryption and Decryption Process in Elgamal Method Using Elliptic Curve Cryptography (ECC)," *TELKOMNIKA (Telecommunication, Computing, Electronics and Control)*, vol 16, no 1, pp. 352-360, Feb 2018.

[6] S.R. Subramanya and Byung K. Yi, "Digital Signatures," *IEEE Potentials*, vol. 25, no. 2, pp. 5-8, Apr 2006.

[7] Elaine B. Barker, "Digital Signature Standard," *National Institute of Standards and Technology (NIST)*, 2013.

[8] Majid Khabbazian, T. Aaron Gulliver, Vijay K. Bhargava, "A new Techniques for Improving the speed of Double Point Multiplication," *PACRIM. 2005 IEEE Pacific Rim Conference on Communications, Computers and signal Processing*, 2005.

[9] Neetesh Saxena, Narendra S. Chaudhari, Jaya Thomas, "Solution to An Attack on Digital Signature in SMS Security," *2013 5th International Conference on Modeling, Simulation and Applied Optimization (ICMSAO)*, 2013.

[10] Chae Hoon Lim, Pil Joong Lee, "A Study on the Proposed Korean Digital Signature Algorithm", in *ASIACRYPT '98 Proceedings of the International Conference on the Theory and Applications of Cryptology and Information Security: Advances in Cryptology*, 2000, pp. 175-186.

[11] B.B. Amberker, Prashant Koulgi, N.R. Sunitha, "Modified Forward Secure Signatures for Mobile Computing Applications," *International Conference on wireless and optical communications network, IEEE,* 2006.

[12] Hong Jingxin, "A New Forward-Secure Digital Signature Scheme," *International Workshop on Anti-Counterfeiting Security and Identification, IEEE,* 2007.

[13] Xinghua Z., "Security Analysis and The Improvement of the sequential multi-signature scheme based on discrete logarithm," *International Conference on Consumer Electronics Communications and Networks, IEEE*, 2013.

[14] Wei Chao, Zhihua Hu, "Security Analysis and Improvement of Dual Signature in Electronic Payment System," *2011 International Conference on Intelligence Science and Information Engineering, IEEE*, 2011.

[15] Xianmin Wei, Peng Zhang, "Research on Improved ECC Algorithm in network and Information Security," *International Journal of Security and Its Applications*, vol. 9, no. 2, pp. 29-36, 2015.

[16] Jie Liu and Jianhua Li, "Cryptanalysis and Improvement on a Digital Signature Scheme without using One-way Hash and Message Redundancy," *International Conference on Information Security and Assurance, IEEE*, 2008.

[17] Lei Niu, Yong Yu, Jianbing Ni, Ying Sun, "Further Cryptanalysis of a Signature Scheme with Message Recovery" *International Conference on Intelligent Networking and Collaborative Systems, IEEE*, 2012.

[18] Jianhong Zhang, Shengnan Gao, "Cryptoanlaysis of a Self-certified Partially Blind Signature and a Proxy Blind Signature," *WASE International Conference on Information Engineering, IEEE*, 2009.

[19] Xinghua Zhang, "Security Analysis and The Improvement of the sequential multi-signature scheme based on discrete logarithm," *3rd International Conference on Consumer Electronics, Communications and Networks, IEEE*, 2013.

[20] Long Zhaohua, Wang Guofeng, "Multi-element Authentication method based on ECDA for Wireless Network," *International Symposium on Knowledge Acquisition and Modeling Workshop, IEEE,* 2008.

[21] 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.

[22] 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.

BIOGRAPHIES OF AUTHORS

Dhanashree K. Toradmalle is working as an Associate Professor in Shah & Anchor Kutchhi Engineering Colleg, Mumbai.She is currently pursuing her Ph. D in Computer Science Engineering from K L E Foundation, Guntur, Andhra Pradesh. Her research areas include Computer Networks and Security.

M. Jayabhaskar is working as an Associate Professor in K L E Foundation, Vaddeswaram, India. His research area includes Network Security.

B. Sathyanarayana received his B. Sc Degree in Mathematics, Economics and Statistics from Madras University, India in 1985, Master of Computer Applications from Madurai KamarajUniversity in 1988. He did his Ph. D in Computer Networks from Sri Krishnadevaraya University, Ananthpuramu, A.P. India. He has 24 years of teaching experience. His Current Research Interest includes Computer Networks, Network Security and Intrusion Detection. He has published 30 research papers in National and International journals.