Lightweight Certificate less Signcryption Scheme Based on Elliptic Curve

Dhanashree Toradmalle, Jayabhaskar Muthukuru, B Sathyanarayana

Abstract: ***As of late, many new signcryption techniques are executed on elliptic cryptosystem (ECC) to lessen the calculation loads for devices with low computation requirements. This essential requirement has motivated the authors to present an efficient Signcryption scheme based on elliptic curve cryptography. The proposed system encompasses all the primary security parameters viz., confidentiality, authentication, integrity, unforgeability, non-repudiation and forward secrecy making the method widely accepted in several resource constrained applications.***

Index Terms: Digital signature, elliptic curve digital signature, Forward Secrecy, Signcryption, Unsigncryption,.

I. INTRODUCTION

With the coming of internet business, it has progressed towards becoming amazingly fundamental to handle the delicate issues of bearing information security, particularly in the consistently sprouting open system condition of the present-day time. The scrambling advancements of the revered cryptography are commonly utilized to protect information security broadly. The term 'cryptography' alludes to the procedure of protecting the mystery information against access by deceitful people in situations where it is humanly difficult to outfit physical security. The three essential objectives [1] of information security are:

- Confidentiality: Information or data can't be accessed by unapproved clients. This is ensured by confidentiality.
- Integrity: Unapproved adjustment of information at the season of transmission is assured by this essential objective of system security.
- Authentication: Arranged assets are continually open to approved gatherings when required with the availability objective.

The essential cryptographic instruments for achieving privacy, trustworthiness, confirmation, and non-denial are message encryption and digital signature. Encryption enables privacy to be accomplished. Digital signature cultivates trustworthiness, confirmation and non-renouncement which are the pillars of Security.

A. *Digital Signature:*

A Digital Signature [2] is wanted to assure to the recipient that the message was sent by sender and nothing changed at the period of transmission. They comprise of two-stages. To utilize a protected hashing calculation on the message is the initial step. Following, the unscrambling to a hash coordinating the message is performed when a signature is checked by the public key. Utilizing the public key that hash must be deciphered if it were encoded with the private marking key.

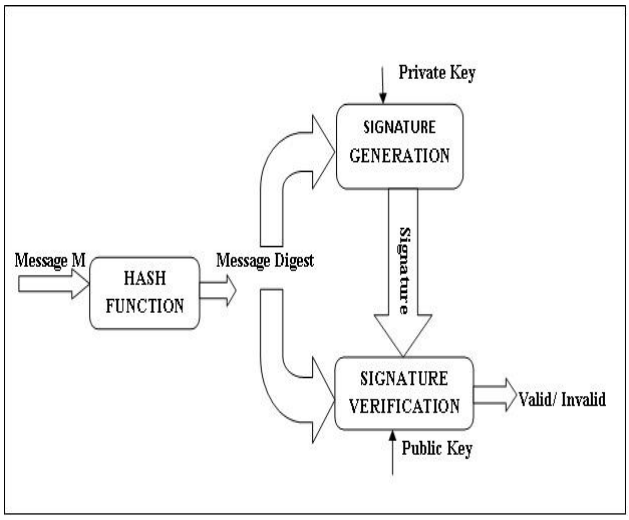

Fig. 1 Digital Signature Process

B. Signature-Then-Encryption:

This is a conventional strategy for giving privacy and validation by utilizing two sequential calculations [3].

- In initial step sender signs the message utilizing his/her private key for verification and further scrambles the message utilizing public key of recipient.
- The beneficiary confirms the signature that point decodes the message at its end.

This system is known as signature-then-encryption

Signature-Then-Encryption Approach Shortcomings: The below mentioned are the hindrances of conventional signature- then-encryption are as far as:

- Computational exercises
- Number of bits
- Size of the entire data group

In conventional signature then-encryption, above shortcomings are overcome with signcryption.

II. THEORY

A. Signcryption

Researchers are working in different areas of Signcryption. The syntactic meaning of Signcryption is presented in [4][5].

Definition (Signcryption Scheme):

Notations:

GenS: A sender key generation calculation

GenR: A receiver key generation calculation

Revised Manuscript Received on August 05, 2019.

Dhanshree K Toradmalle, Department of CSE, KLE Foundation, India
Jayabhaskar Muthukuru, Department of CSE, KLE Foundation, India
B Sathyanarayana, Department of Computer Science & IT, Sri Krishnadevaraya University, India

SKs : The sender private key
PKs : The sender public key
SKr : The recipient private key
PKr : The recipient public key
s : signcrypt text
m : message

The signcryption scheme is a gathering of four (effective) calculations = (GenS; GenR; Signcrypt; Unsigncrypt) for key space k, message space m, and signcrypt text space s,

- We compose (SKs; PKs) GenS; which yields a sender key-pair (SKs; PKs) individually.
- We build (SKr ; PKr) GenR ; which yields a recipient key-pair (SKr; PKr), individually.
- We compose s; Signcrypt(SKs ; PKr ; m). It is a signcryption calculation, signified Signcrypt, which takes as information a sender private key SKs, a recipient public key PKr, and a message m, and yields a signcrypt text s.
- We create m; Unsigncrypt(SKr ; PKs ; s). It is an unsigncryption calculation, which takes as information a recipient private key SKr, a sender public key PKs, and a signcrypt text s, and yields a message m.

The rightness condition requires that for all sender key sets (SKs; PKs) in the help of GenS, what's more, for all recipient key sets (SKr ; PKr in the help of GenR, and for all messages m it holds that

Unsigncrypt(SKr ; PKs ; (Signcrypt(SKs ; PKr ; m)) = m

B. Related work in Signcryption:

Zheng (1997) [6] proposed a verified encryption crude called signcryption, to diminish the expense of the traditional "signature-then- encryption" approach, the method consolidates the functionalities of both encryption and digital signature in a solitary sensible advance. Zheng's signcryption conspire depended on Discrete Logarithm Problem (DLP) over a limited field. Zheng and Imai (1998) [7], afterward, proposed a variation of the plot dependent on the elliptic curve simple of DLP (ECDLP). There are several signcryption methods proposed since 1997[8] with enhancements. Likewise, new properties past the fundamental security objectives have been presented as of late, to name a few:

- Identity Based Signcryption: Shamir [9] in 1984 proposed the concept of Identity based cryptosystems. The systems use self assertive strings for example email address as public keys. It is a simplified approach towards public key and certificate management.
- Certificateless Signcryption: Al-Ryiami and Paterson [10] presented certificateless cryptography (CLC) which still keeps the testament free property of ID based Public Key systems. By taking care of the key escrow issue in ID based cryptography certificateless public key cryptography dispenses with endorsement the board in customary public key foundation also. Certificateless signcryption is a standout amongst the most significant natives in certificateless public key cryptography which accomplishes secrecy and validation at the same time.
- Attribute based Signcryption[11]: A scheme where the decentralized expert A can create a property based key pair for the delicate information proprietor autonomously. In the proposed scheme, the sensitive information proprietor can share delicate information through indicating an attribute-based access control structure with the goal that any clients whose qualities fulfill it tends to be permitted to get to the delicate information without realizing the sensitive information proprietor's one of a kind identity information.
- Heterogeneous Signcryption [12]: In a homogeneous system clients work either in an IBC based and PKI based environment , which means both sender and receiver both work in same environment. But for heterogeneous communications this may act as an obstacle. A heterogeneous signcryption system supports communication amongst clients working in different environments. The signcryption scheme proposed [12] doesn't provide forward secrecy.

III. PROPOSED SCHEME

We present a scheme which is secure and reduces the overheads of computations guaranteeing a secured a signcryption scheme

SIGNCRYPTION:

Given a message m, a Sender's secret key SKs and Receiver's public key PKr the signcryption algorithm works as follows:

1)Select a random number r where r ∈ [1 to (p – 1)]

2)Calculate K = r. PKr = (k1, k2)

3)Calculate c = k1 ⊕ m

4)Calculate h = Hash (m || k2)

5)Calculate S = r. G - h. SKs.PKr

Signcrypted elements to be sent is (c, h, S)

UNSIGNCRYPTION:

Given a ciphertext c , a Receiver's secret key SKr and Sender's public key PKs the unsigncryption algorithm works as follows:

1) Compute K = (k1 , k2) = SKr (S + h . SKr. PKs)
   = S. SKr + h. SKr. SKr. PKs
2) Compute m1 = k1 ⊕ c
3) Compute h1 = Hash (m1 || k2)

If (h = h1) the receiver accepts the signature

CORRECTNESS:

(c, h, S) is a valid Signcrypted text . Following is the validation proof for the same:

K= S. SKr + h. SKr. SKr. PKs

= [r. G - h. SKs. PKr] . SKr + h. SKr. SKr. PKs

= r. G. SKr - h. SKs . PKr. SKr + h. SKr. SKr. PKs

= r. G .SKr - h. SKr

(SKs. PKr - SKr. PKs)

= r. G. SKr - h. SKr (SKs. G. SKr - SKr. PKs)

= r. G. SKr - h. SKr. SKr (SKs. G - PKs)

= r. G. SKr - h. SKr. SKr (PKs - PKs)

= r. G. SKr

= r. PKr

= (k1 , k2)

IV. RESULTS

This section represents implementation results of Elliptic Curve Signcryption over EC P-256.

Basepoint G = (48439561293906451759052585252797142027629495260417479958440807170824046352 86,36134250956749795798585127919587881956611106672985015071877198253568414405109)

Elliptic Curve: y^2 = x^3 + 11579208921035624876269744694940757353008614341529031419553363130886709785 3948x+41058363725152142129326129700472684091144410159937255548352563140394674012 91 mod (11579208921035624876269744694940757353008614341529031419553363130886709785)

Key Generation

Private key of Sender SKs = 11579208921035624876269744694940757353008614341529031419553363130886578487 8936

Public key of sender PKs = (34546132059688158410932150266538873501867788771095976492068276394496121968241,60329121553991804007580168194002321701220123547188577530904503600 8604)

Private key of Receiver SKr = 11579920892103562487626974469494075735300861434152903141955336313088663286628286

Public key of Receiver PKr = (10556588839603558825170323950947858748841883236085921178302920,21169823370631238626796324208359892627398508371169997674144497703034825175553)

SignCryption

r = 11557920892103562487626974469494075735300861434152903141955336313088670639905 86

K = (153952327319314373202029359062711477743609163102609849383759621446672961719 3,35892820234294566530164102043465832463153196101985373825375959983156217607003)

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

cipher text value c = a TFU ZRFRW JPY[\[xW JPY [\[xWVPW W_B S^ \^D \\[U91631026098493837596214466729617193

h = 11557920892103562487626974469492230342876873327477341120133510508148469987358 68

r.G = (10230078712017315578578211577482238438760122826272694070119545592510739262538 1,805743061405913198794115947167482898052512684297262842855367023279698142617 98)

h.SKs.PKr = (18147216090133929208681978885327640502533321183469819186151152815292930861 88,–53526804986407159059718105227421151085790623214662541192840979524449778900699)

S = (95864988563587561936946403903119011939328168439366846946120934884360853732636,95569482961263599393333391580765071576027277147799360837600187134933992994530)

UnSignCryption

S.SKr = (31043655389003774994574830332211988446923445020281826587569837694934644561 5,66711289897465646544717502618001114550248216168910897808865010282723508503 86)

h.SKr.SKr.PKs = (92547979592807058734992546533857204473482661876216705145997787683127243028013051,1001362857525857739988374552634557500408964914336944337575101922380667239739 21)

K = (153952327319314373202029359062711477743609163102609849383759621446672961719 3,35892820234294566530164102043465832463153196101985373825375959983156217607003)

Decrypt value (m1) Paul hated school. He did not do his home

h1= 11579208921035624876269744694922303428768733274773411201335105081484699873586 8

h = h1, Its Accepted

V. CONCLUSION

Signcryption is a cryptographic plan that joins the abilities of digital signature and public encryption in a solitary advance. It serves to all the while accomplish privacy, trustworthiness, validation, and non-renouncement since it is a blend of these two. The proposed method is a certificateless scheme which is executed considering the referenced prerequisites at low calculation costs with the goal that it will be broadly pertinent in an area of utilizations including resource constrained areas.

REFERENCES

1. William Stallings, “Cryptography and Network Security-Principles and Practice” Pearson,Sixth Edition 2014.
2. Hankerson, A. Menezes, S. Vanstone,“Guide to Elliptic Curve Cryptography ”,Springer First Edition,2004
3. Hwang, Ren-Junn, Chih-Hua Lai, and Feng-Fu Su.” An efficient signcryption scheme with forward secrecy based on elliptic curve.” Applied Mathematics and computation 167.2(2005): 870-881.
4. Joonsang Baek, Ron Steinfeld, and Yuliang Zheng, “Formal proofs for the security of signcryption”, Journal of cryptology, 20(2):203–235, 2007.
5. Christian Badertscher, Fabio Banfi, and Ueli Maurer “A Constructive Perspective on Signcryption Security” Springer 2018
6. Y. Zheng, “Digital signcryption or how to achieve cost (signature & encryption) <<cost (signature) +cost(encryption),” Advances in Cryptology-Crypto’97 Proceedings, LNCS 1294, Springer-Verlag, pp.165-179,1997.
7. Y. Zheng, H. Imai, “How to construct efficient signcryption schemes on elliptic curves,” Information Processing Letters, vol. 68, no. 5, pp. 227-233, 1998
8. Dhanashree Toradmalle Jayabhaskar Muthukuru, “A survey on elliptic curve based signcryption for Information security” Ponte International Journal of Sciences and Research, Vol. 73 No. 8, Aug 2017
9. A. Shamir, “Identity-Based Cryptosystems and Signature Schemes”, In Proc. CRYPTO 84, volume 196 of LNCS, pages 47-53. Springer-Verlag, 1984.
10. S. S. Al-Riyami, K. G. Paterson, “Certificateless public key cryptography, Advances in Cryptology” -ASIACRYPT 2003, Springer, pp. 452-473, 2003
11. Xianyong Meng Xiangyu Meng, “A Novel Attribute-Based Signcryption Scheme In Cloud Computing Environments ”, Proceedings of the IEEE International Conference on Information and Automation Ningbo, China, August 2016

12. Saritha Raveendranath, Aneesh a, "Efficient multi-receiver Heterogenous signcryption" IEEE WiSPNET 2016

AUTHORS PROFILE

Ms.Dhanashree K Toradmalle is working as an Associate Professor in Shah & Anchor Kutchhi Engineering College, Mumbai. She is currently pursuing her PhD in Computer Science Engineering from K L E Foundation (Deemed to be University), Guntur, Andhra Pradesh in Computer Science Engineering. Her research areas include Computer Networks and Security.

Dr. M Jaya Bhaskar has 7+ years of industry and 6+ years of teaching experience and has interests in real time issues in Networks which lead to research in Network and Data Security and further implementation of different security techniques like cryptography and signcryption. He completed his PhD in Elliptical Curve Cryptography Implementation Approaches for Efficient Smart Card Processing from Sri Krishnadevaraya University, Ananthpuram in 2013.He is currently working as Associate Professor in K L E Foundation (Deemed to be University), Guntur, Andhra Pradesh. His research areas include Network and Information Security

Prof. B. Sathyanarayana received his Master of Computer Applications from Madurai Kamaraj University in 1988. He did his Ph.D in Computer Networks from Sri Krishnadevaraya University, Ananthpuram, A.P. India. He has around 30 years of teaching experience. His Current Research Interest includes Computer Networks, Network Security and Intrusion Detection. He has guided many research scholars for PhD.He has published around 50 research papers in National and International journals