A Study on signcryption Scheme Based on Eliptic Curve

Anjali Pandey
M.Tech Scholar, Dept. of Computer Science & Engineering
CENTURION UNIVERSITY OF TECHNOLOGY AND MANAGEMENT
Bhubaneswar, India
16.anjalipandey@gmail.com

Sumanjit Das
Dept. of Computer Science & Engineering.
CENTURION UNIVERSITY OF TECHNOLOGY AND MANAGEMENT
Bhubaneswar, India
sumanjit@cutm.ac.in

Abstract— Data exchange is more essential to share information in the age of information technology to achieve the different tasks. As the transmission media is unreliable it need protection of that data moves in an unsecure communication network is a crucial issue for the reason that it may get tempered by third party [1]. Everyone desires their messages must be travel in the network in a secure fashion. The message does not tempered by any unauthorized one. So our focal is how we can add more security to the messages than the existing so that it can fulfill the user requirements without any damage. There are various cryptographic techniques be present which offers security to the messages [2]. Traditional Signature then encryption technique is responsible for security to the messages by performing signature scheme and encryption scheme in two unlike logical steps. As it achieves signature and encryption scheme in two unlike logical steps it takes more computational cost and communication overhead. The novel technique titled as "signcryption" by Yuling Zheng, accomplishes both the functionality of signature scheme and encryption scheme in single logical step with a reduced amount of computational and communication cost than Signature-then-encryption scheme [1]. A number of signcryption schemes are previously announced by many researchers Nonetheless each scheme has their own restriction [2]. This paper contain cryptanalysis of different signcryption schemes based on the security goals like integrity, authentication, confidentiality, unforgeability beside that forward secrecy and public verification., where one can confirm the sender signature without reading the content of messages since the messages is in encrypted format and the cannot be able to mine the original message content even if the long-term private key of the sender is compromised [4].

Keywords- elliptic curve cryptography, signcryption, digital signature and encryption.

I. INTRODUCTION

Currently the utilization of internet is increasing rapidly. The user exchanges the data such as e-mail information, services, buy or sell products, communities, online chat, and downloading software etc. So that the techniques offered to protection of such data travel in the internet must be improved than the existing. There are a variety of issues such are integrity, confidentiality, authenticity and non-repudiation and some additional issues (public verification and forward secrecy) must be satisfied whenever a message is sent in an unsecure network [2]. Traditional Signature-then-encryption technique is responsible for message confidentiality and integrity of the message. In Signature-then-encryption technique a digital sign is put into the message by using a digital signature scheme to attain the data integrity and then message is encrypted into an unreadable arrangement by using an encryption scheme to keep confidentiality of the message [8]. The techniques grounded on Signature-then-encryption were most popular previously. But the key shortcoming of this scheme is, it takes more communication cost and computational time as it performs the digital signature and message encryption in two unlike logical steps [7]. Since the utilization of internet is increasing rapidly, at the same time it needs to get better the communication cost and overhead. The novel technique in public key cryptography named as "signcryption" announced by Yuling Zheng, accomplishes together the functionality of signature scheme and encryption scheme in single logical step with a reduced amount of computational and communication cost than Signature-then-encryption scheme [11]. In Signature-then-encryption scheme fig1 sender digitally sign the message by using a digital signature algorithm and the original message is transform into an unreadable format using the secret key generated by using symmetric encryption afterwards the secret key is again encrypted to achieve more security by using the public key of recipient generated by asymmetric encryption [12]. And send the above information to the receiver.

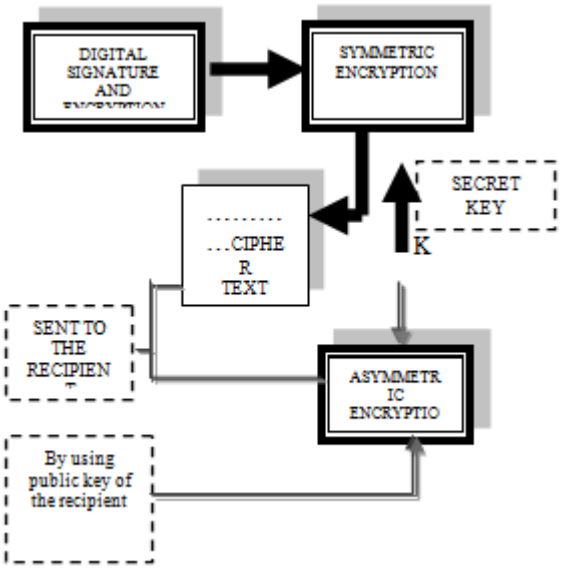
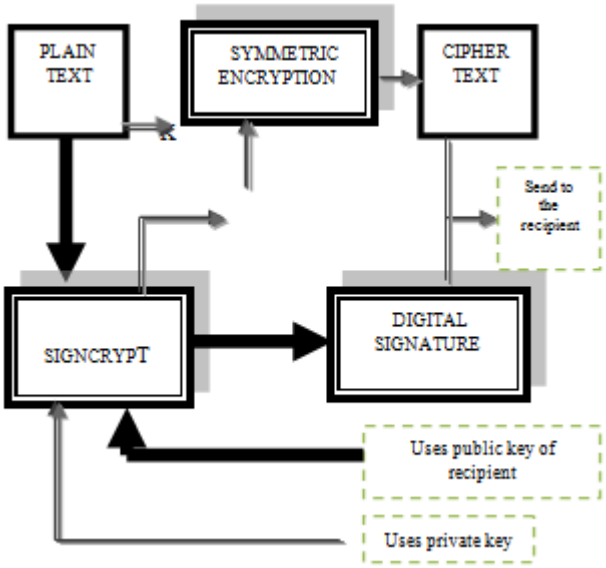


Fig1: Signature then encryption scheme.

In the receiver side, the encrypted secret key is generated by the private key of recipient and by the help of secret key the message is decrypted into readable format and verifies the signature.



II. PROPERTIES OF SIGNCRYPTION

A. Confidentiality

Through confidentiality, we signify that only the intended recipient of a signcrypted message should be able to examine its contents. Except the intended recipient no one is able to read the contents of the message.

B. Authenticity

Through authenticity, we signify that the recipient of a signcrypted message is capable to confirm the sender's identity. Unauthorized one should not be able to send a message, claiming to be someone else.

C. Non-repudiation

Nonrepudiation is the declaration that somebody cannot refute something, normally, nonrepudiation refers to the capability to ensure that a party to a communication cannot deny the authenticity of their signature on a document or the sending of a message that they originated.

D. Forward Secrecy

By forward secrecy, we signify that an unauthorized one cannot interpret signcrypted messages, even with access to the sender's private key. The confidentiality of signcrypted messages is protected, even if the sender's private key is compromised.

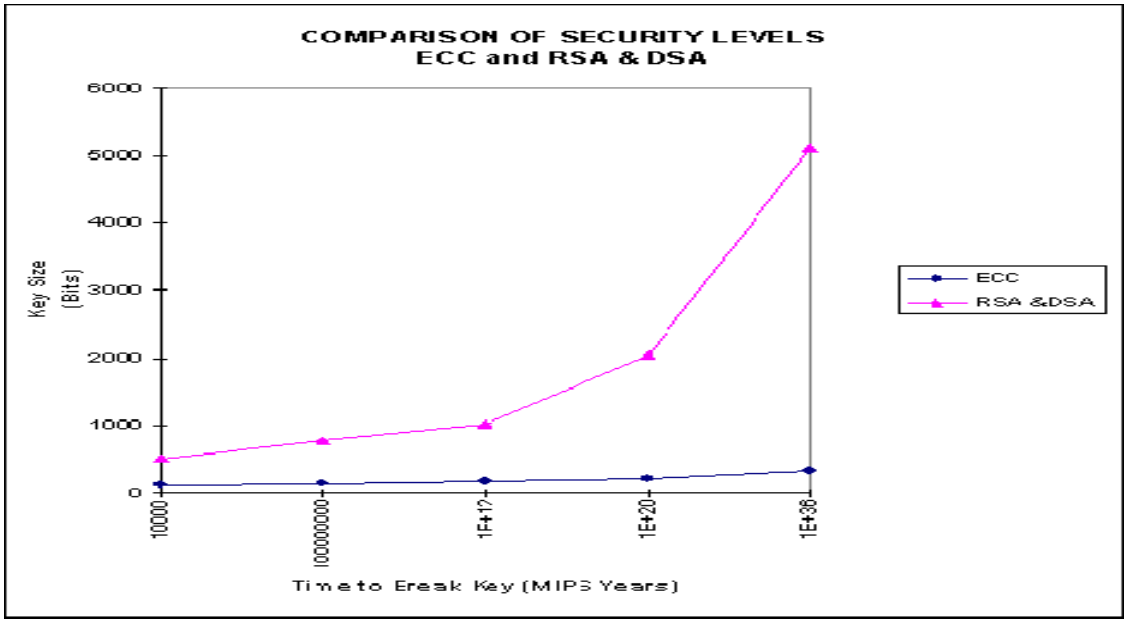
E. Integrity

Message integrity guarantees that the message has not been changed. The receiver of the message should be able to verify that the message is original one.

F. Public Verification

Third party can be able to verify the recipient identity of message without the knowledge of sender's private key and third party can be judge or farewell.

III. COMPARISION OF ECC AND RSA



The signcryption based on ECC are more secure than based on RSA as given by many researchers depending on the time required to break it. It is also observed that breaking an ECC is practically impossible and the time taken by ECC is very less than traditional RSA base schemes.

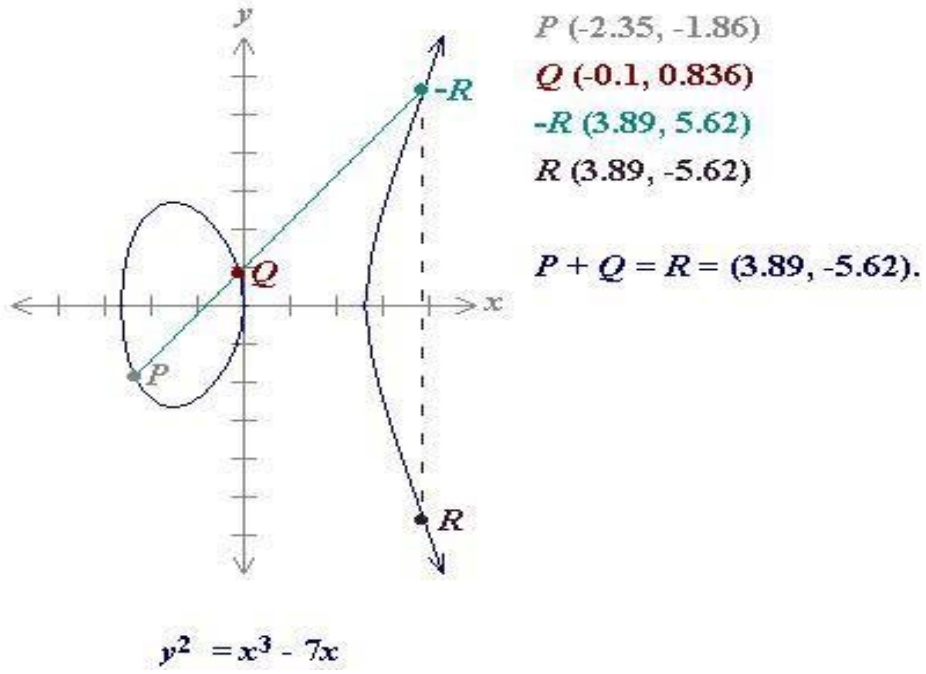
IV. Elliptic Curve Cryptosystem

Elliptic Curve Cryptography (ECC) was announced by Neal Koblitz and Victor Miller. This technique has great advantages than other cryptosystem. The size of the key necessary for encryption and digital signatures is far less than other technique, takes Less time for encryption, lower bandwidth usage, faster implementations, lower power requirements, and smaller hardware processor requirements.

The elliptic curves can be categorized into two classes, non-prime and prime elliptic curves .The elliptic curve cryptography is based on the elliptic curve equation which is given as: $y^2 = x^3 + ax + b$

To plot an elliptic curve one needs to compute:

$y = \text{sqrt}(x^3 + ax + b)$



So, value of y is calculated for each value of x, symmetric about y = 0 where values of a and b will be given. Groups are defined based on the set E (a, b) for values of a & b such that $4a^3 + 27b^2 \neq 0$.

A. Non - Prime Curves

Here, is a point of infinity called as the "Zero Point" which is the third point of intersection of a straight line across the elliptic curve. One point that is to be noted is when three point on elliptic curve lie on a straight line they sum up to zero. There are some rules for operation addition '+'for elliptic curve points to follow. Those all are listed down as:

1) If point is O then

O = -O

2) If point P on the curve then

P + O = P

3) If two are P and negative of then that is. P ≡ (x,y) and -P ≡ (x,-y)

P+ (-P) = P - P = O

4) If P and Q are two distinct points the addition is as follows:

a) Draw a straight line between P and Q

b) Extend the line and find the third point of intersection with the elliptic curve 'R'

c) To form the Group adds these three points as:

P + Q = -R

Thus, P + Q are the mirror image of the point R.

5) If both the points are the same point P then the steps is as follows:

a) Draw a tangent through point P

b) P + P = 2P = -R

B. Prime Curves

In case of these curve the cubic is applied. For prime curves a large prime number p is assumed, and values of all of the variables and coefficients are selected within the range of 0 to p-1 such that the following condition is satisfied. The condition is:

$y^2 \bmod p = (x^3 + ax + b) \bmod p$

Example: a = 1, b = 1, x = 9, y = 7, p = 23

$7^2 \bmod 23 = (9^3 + 9 + 1) \bmod 23$

3 = 3

V. ANALYSIS OF SIGNCRYPTION SCHEMES

A. Y. Zheng and Imai

The schema is based on the elliptic curve technique as compared to traditional signature then encryption schemes the elliptic curve based signcryption can save 58% in computational cost and 40% in communication overhead and it provides more security then RSA and DSA technique.

Parameters public to all:

C: an elliptic curve over GF (p^m), either with p >= 2^150 and m=1or p =2 and m>= 150 (public to all).

q: a large prime whose size is approximately of |pm| (public to all).

G: a point with order q, chosen randomly from the points on C (public to all).

Hash: a one-way hash function whose output has, say, at least 128 bits.

KH: a keyed one-way hash function.

(E, D): the encryption and decryption algorithms of a private key cipher.

Alice's keys:

Va : Alice's private key, chosen uniformly at random from [1…..q – 1].

Pa: Alice's public key (Pa = vaG, a point on C).

Bob's keys:

Vb : Bob's private key, chosen uniformly at random from [1…..q-1].

Pb : Bob's public key (Pb = vbG, a point on C).

Signcryption of m by Alice the Sender

Step 1: V є R [1……..q -1]

Step 2: (k1, k2) = hash (v Pb)

Step 3: c =Ek1 (m)

Step 4: r = KHk2 (m)

Step 5: s = (v/ (1+ va)) mod q

Now alice send (c,r,s) to bob.

Unsigncryption of m by bob the receiver

Step 1: u є s Vb mod q

Step 2: (k1, k2) =hash(uPa +urG)

Step 3: M=Dk1 (c)

Step 4: Accept m only if KHk2 (m) = r

This signcryption scheme that is based on elliptic curve, which saves about 58% computational cost and saving about 40% communication cost than traditional signature then encryption scheme based on elliptic curve. This schema provides all the security issue accept forward secrecy of message confidentiality and public verification.

But it does not provide authentication of encrypted message.

B. Ren-Junn Hwang,Chih-hua Lai,Feng-Fu Su

The scheme not only provides message confidentiality, authentication, integrity, unforgeability and non-repudiation but also forward secrecy of message confidentiality and trusted third party signature verification than the traditional signature then encryption scheme. The process of communication is as follows.

In initialization phase the parameters are as follows:

q: a large prime number, where $q > 2^{160}$.

a,b : two integer elements which are smaller than q and satisfy $4a^3 + 27b^2 \bmod q$.

F: the selected elliptic curve over finite field q: y2 = x3 + ax + b mod q.

G: a base point of elliptic curve F with order n.

O : a point of F at infinite.

n: the order of point G, where n is a prime, $n \cdot G = O$ and $n > 2^{160}$.

H : a one-way hash function.

Ek(.)/Dk(.): symmetric encryption/decryption algorithm with private key k

Signcryption Phase

Step 1: Verifies Bob's public key UB by using his certificate.

Step 2: Randomly selects an integer r, where r < n.

Step 3: Computes R = r · G = (r1, r2).

Step 4: Computes K = r · UB = (k, l).

Step 5: Uses the symmetric encryption algorithm to generate cipher text C = Ek(M)

Step 6: Uses the one-way hash function to generate h = H (M||r1), where r1 is generated in Step 3.

Step 7: Computes s = dA –h.r mod n.

Step 8: Sends the signcrypted text (C, R, s) to Bob.

Unsigncryption phase

Bob receives the signcrypted text (C, R, s) decrypts the cipher text C by performing symmetric decryption algorithm with secret key k. the receiver also verifies the signature of sender. Bob gets the plain text as follows.

Step 1: Verifies Alice's public key UA by using her certificate.

Step 2: Computes K = dB · R = (k, l).

Step 3: M = Dk(C), where the secret key k is computed in Step 2.

Step 4: Uses the one-way hash function to compute h = H(M||r1), where r1 is the x-coordinate value of the point R.

Step 5: Verifies s · G + h · R is equal to UA or not. If it is true then accept M is correct plain text which is sent by Alice; otherwise reject M.

Verification phase

By some reasons, we need the trusted third party such as judge or farewell to decide that the sender Alice sent M to the recipient Bob. In this scheme, the recipient Bob only provides (M, R, s) to the judge, when dispute occurs. The judge decides whether the sender Alice ever sent the message to the recipient Bob or not based on (M,R, s). The judge performs the following steps to make the decision.

Step 1: Verifies Alice's public key UA by using her certificate.

Step 2: Uses the one-way hash function to generate h = H (||r1).

Step 3: If s · G + h · R equal to UA then the sender Alice sent (M, R, s) to the recipient Bob otherwise she did not send this message to the recipient Bob.

This scheme provides security functions like message confidentiality, authentication, integrity, unforgeability, non-repudiation, forward secrecy of message confidentiality and public verification without using sender private key.

TABLE 1 Comparison based on average computational time of major operation in same secure level the elliptic curve multiplication only needs 83ms & the modular exponential operation takes 220 ms for average computational time [8].

Schemes	Sender Average (computational time in ms)	recipient Average (computational time in ms)
Zheng	**220**	**440**
Zheng & imai	**83**	**166**
Bao & Deng	**440**	**660**
Gamage et al	**440**	**660**
Jung et all	**440**	**660**
R-J Hwang et al	**166**	**249**

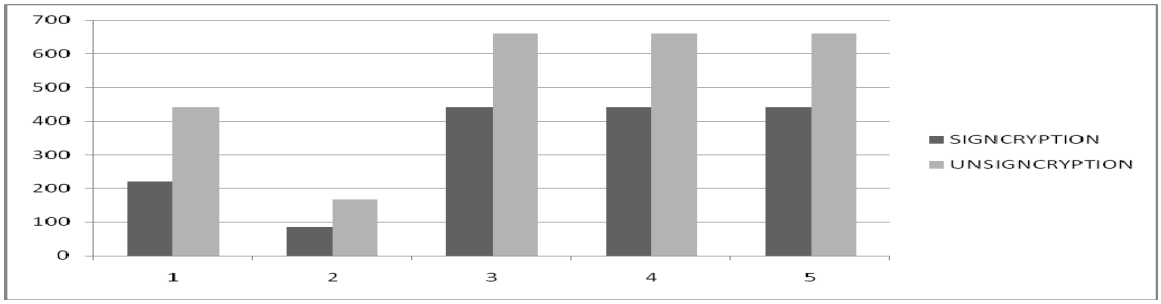


Fig-2 Comparisons based on time.

VI. CONCLUSION

There are a variety of cryptographic techniques is in attendance to offer security to the messages however each has their own restrictions and limitations. This paper discussed signcryption schemes grounded on elliptic curve cryptography which can be supportive to any platform .This scheme fulfill all the security issues such as message confidentiality, authenticity, integrity, unforgebility, nonrepudiation beside the forward secrecy and public verification to the messages. Signcryption based on elliptic curve has an advantage of lower computational cost and communication overhead then the existing techniques. As this scheme offers public verification where one can verify the sender certification without reading the plain content of the message for the reason that the message is in encrypted format, it is more helpful in e-commerce surroundings. Occurrence of any dispute flanked by the partners, third one can check without any knowledge of message content, proof the signature of the sender. Another advantage of this scheme is to provide forward secrecy to the message .it means, even if the long-term private key of the sender is compromised no one be able to mine the original message content.

VII. REFERENCES

[1] Yuliang Zheng. Digital signcryption or how to achieve cost (signature encryption)Cost (signature), Cost (encryption).In CRYPTO '97Proceedings of the 17th Annual International Cryptology Conference on Advances in Cryptology, pages 165-179, London, UK, 1997. Springer-Verlag.

[2] F. Bao, R.H. Deng, "A signcryption scheme with signature directly verifiable by public key", Proceedings of PKC'98, LNCS 1431, Springer-Verlag, 1998, pp. 55–59.

[3] Gamage, C., J.Leiwo, Encrypted message authentication by firewalls. Proceedings of International Workshop on Practice of Theory in Public Key Cryptography, Berlin, 69-81, 1999

[4] Yuliang Zheng and Hideki Imai. How to construct efficient signcryption schemes on elliptic curves. Inf. Process. Lett., 68(5):227-233, 1998.

[5] Ren-Junn Hwang,Chih-hua Lai,Feng-Fu Su,An efficient signcryption scheme with forward secrecy Based on elliptic curve

[6] Jung. H. Y,K. S Chang, D. H Lee and J. I. Lim, Signcryption scheme with forward secrecy. Proceeding of Information Security Application-WISA, Korea, 403-475, 2001.

[7] X. Yang Y. Han and Y. Hu. Signcryption based on elliptic curve and its multi-party schemes. Proceedings of the 3rd ACM International Conference on Information Security (InfoSecu 04), pages 216-217, 2004.

[8] Henri Cohen and Gerhard Frey, editors. Handbook of elliptic and hyperelliptic curve cryptography. CRC Press, 2005.

[9] Hwang Lai Su. An efficient signcryption scheme with forward secrecy based on elliptic curve. Journal of applied mathematics and computation, pages 870-881, 2005.

[10] LEI Feiyu, CHEN Wen, CHEN Kefei, "A generic solution to realize public verifiability of signcryption", Wuhan University Journal of Natural Sciences, Vol. 11, No. 6, 2006, 1589-1592.

[11] Mohsen Toorani and Ali Asghar Beheshti Shirazi. Cryptanalysis of an efficient signcryption scheme with forward secrecy based on elliptic curve. Computer and Electrical Engineering, International Conference on, 428-432, 2008.

[12] Mohsen Toorani and Ali Asghar Beheshti Shirazi. An elliptic curve-based signcryption scheme with forward secrecy. Journal of Applied Sciences, 9(6):1025 -1035, 2009.

[13] Sumanjit Das and Biswajit Samal, An elliptic based signcryption protocol using java, IJCA, Vol-66, No-4, Feb' 2013.