An Efficient Security Protocol based on ECC with Forward Secrecy and Public Verification

Anjali Pandey
M. Tech Scholar, Dept. of CSE
Centurion University of Technology and Management

Sumanjit Das
Asst. Prof., Dept. of CSE Centurion University of Technology and Management.

ABSTRACT

The novel technique titled as “signcryption” announced by Yuliang Zheng, completes both the functionality of signature scheme and encryption scheme in single logical step with a reduced amount of computational cost and communication overhead than Signature-then-encryption scheme. A number of signcryption scheme has previously been announced by many researchers nonetheless each scheme has their own restriction. This paper is grounded on an elliptic curve cryptosystem (ECC) implemented using java technology with reduced amount of computational cost and communication overhead than the existing techniques. It not only offers the integrity, authenticity, confidentiality, unforgeability, non-repudiation beside that forward secrecy and public verification. By forward secrecy of message confidentiality, unauthorized person cannot be able to mine the original message content even if the long-term private key of the sender is compromised. It doesn’t be affect the confidentiality of the previously stored message. By the public verification, Anyone can confirm the sender signature without reading the content of message since the message is in encrypted format .As our proposed scheme takes a comparable amount of computational cost, it can be applied in lower computational power devices like smart card based applications ,e-voting etc.

Keywords

Elliptic Curve Cryptosystem, Digital Logarithmic Problem, Signcryption, Digital Signature, Encryption, Decryption.

1. INTRODUCTION

Currently the utilization of internet is increasing rapidly. The user exchange the data such as: e-mail information, services, buy or sell products, communities, online chat, and downloading software etc. so that the techniques offered with 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, Unforgeability and some additional issues (public verification and forward secrecy) must be satisfied whenever a message is sent in an insecure network. Traditional Signature-then-encryption techniques are 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 a message is encrypted into an unreadable arrangement by using an encryption scheme to keep confidentiality of the message. The techniques grounded on Signature-then-encryption were most popular previously. But the key shortcoming of this scheme is, it takes more communication overhead and computational cost as it performs the digital signature and message encryption in two unlike logical steps. Since the utilization of internet is increasing rapidly, at the same time it needs to get better the computational cost and communication overhead. The novel technique in public key cryptography named as “signcryption” based on DLP announced by Yuliang Zheng [1], 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. Signcryption technique using elliptic curve cryptosystem (ECC) by Zheng [3] saves 58% of computational cost and 40% less on average computation time. The Zheng [3] scheme includes two phases i.e. signcryption and unsigncryption. In signcryption phase shown in fig1 ,sender digitally sign the message by using a digital signature algorithm and the original message is transformed 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. And send the above information to the receiver. In the receiver side i.e. Unsigncryption phase shown in fig2, the encrypted secret key is generated by the private key of the recipient and with the help of secret key the message is decrypted into readable format and verifies the signature.

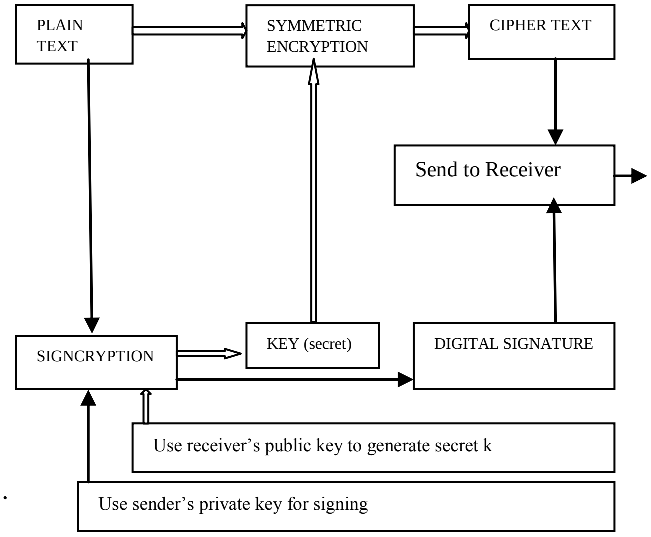


Fig. 1 Zheng [3] Signcryption phase.

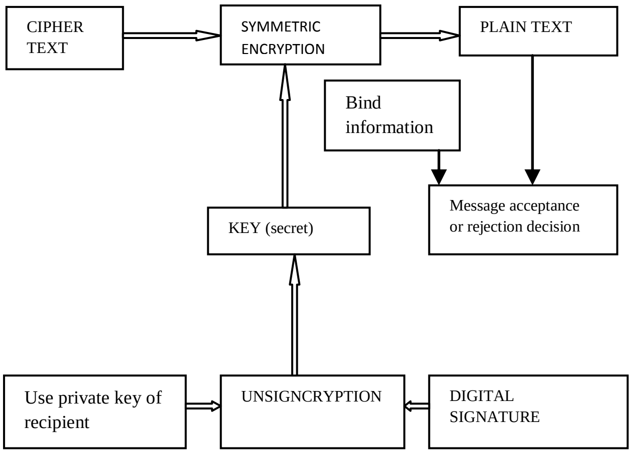


Fig. 2 Zheng [3] Signcryption phase.

2. ARTICLE REVIEW

Zheng [1] announced a new cryptography technique titled as ‘‘Signcryption’’ based on discrete logarithmic problem, which is responsible to achieve the functions of both digital signature and encryption scheme for authentication and confidentiality in single logical step. In Zheng [1] scheme, originator of communication uses the receiver’s public key to generate a secret key for message encryption. The receiver receives the cipher text and digital signature and he uses his private key to derive the same secret key. By using the secret key the receiver decrypts the message and verifies the signature.Feng Bao and Robert H. Deng [2] scheme is based on DLP. It enhanced the zheng [1] scheme so that judge can verify authenticity of signature without the need of recipient‘s private key. The identity of the sender is verified by the public key of the sender. Chandana Gamage, Jussipekka Leiwo, and Zheng [4] scheme is based on discrete logarithm problem (DLP).it provides the third party verification without having the original text. Judge can verify the authenticity of the originator without any knowledge of the original content of the message because it is in encrypted format. Y. Zheng and Imai[3] scheme is based on the elliptic curve technique because ,when compared to signature then encryption ,elliptic curve signcryption can save 58% in computational cost and 40% in communication overhead. And it provides more security than RSA and DSA technique. Ren-Junn Hwang, Chih-hua Lai, Feng-Fu Su [5] scheme based on ECC not only provides message confidentiality, authentication, integrity, unforgeability and non-repudiation but also forward secrecy of message confidentiality and trusted third party signature verification .It uses elliptic curve point multiplication two times in signcryption phase and three times in unsigncryption phase. M. Dutta, A. K. Singh, A Kumar [6] scheme grounded on Elliptic Curve Cryptosystem provides all the security issues along with forward secrecy and public verification.it uses elliptic curve point multiplication three times in signcryption phase and two times in unsigncryption phase. M. Toorani, A.A. Beeheshti Shirazi [7] is based on ECC which offer all the security issues but it consumes additional time in unsigncryption phase as it uses elliptic curve point multiplication four times.

3. THE PROPOSED SCHEME

The proposed scheme is based on Elliptic Curve cryptosystem implemented in java technology which is supportive to all platform .Proposed scheme includes three phases such are signcryption phase shown in fig 3, unsigncryption phase shown in fig 4 and judge verification phase . This scheme fulfil all the security issues such are: message confidentiality, authenticity, integrity, unforgeability, non-repudiation beside that forward secrecy and public verification to the message and having reduced amount of computational cost and communication overhead than the existing techniques. With this technique anyone can verify the sender’s signature without using the private key of the receiver. And also not be able to read the original message because it is in coded format. This scheme uses elliptic curve point multiplication twice to signcrypt the message and twice to unsigncrypt the message.

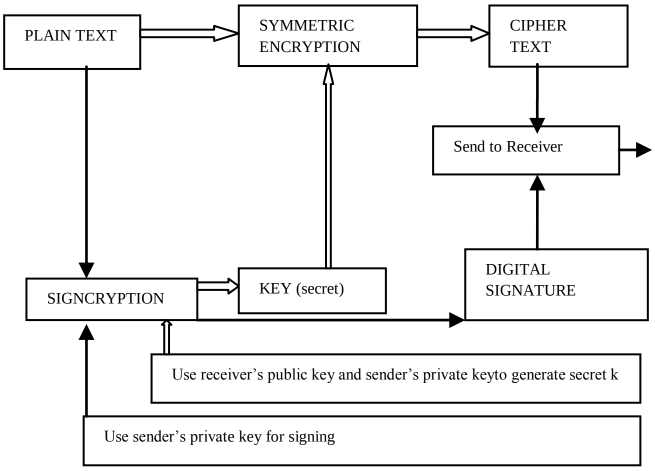

PLAIN TEXT
SYMMETRIC ENCRYPTION
CIPHER TEXT
Send to Receiver
DIGITAL SIGNATURE
SIGNCRYPTION
KEY (secret)
Use receiver’s public key and sender’s private keyto generate secret k
Use sender’s private key for signing

Fig. 3 Signcryption phase of proposed scheme.

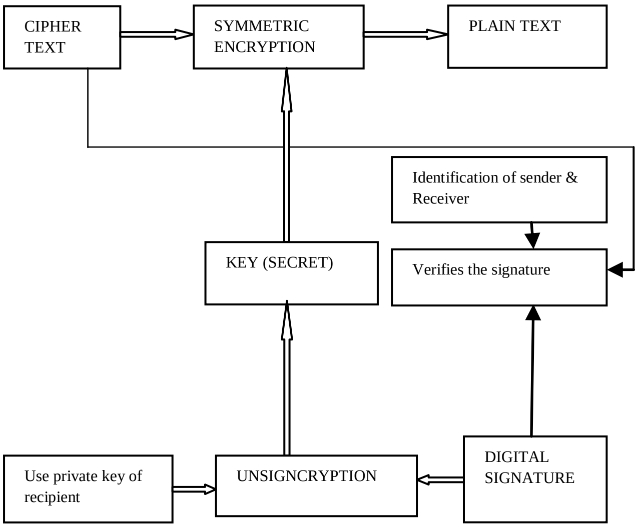


Fig. 4 Unsigncryption phase of proposed scheme

3.1 Phases of our proposed scheme.

3.1.1 Initialization Phase

The public parameter used in our proposed scheme are:

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

a, b : two integer elements which are smaller than q and satisfy $4a^3 + 27b^2 \bmod q \neq 0$.
F : the selected elliptic curve over finite field q: $y^2 = x^3 + ax + b \bmod q$.
ECC_p : 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, $n \cdot ECC_p = O$ and $n > 2^{160}$.
H : a one-way hash function.
$ENCRYPT_k(.)/DECRYPT_k(.)$:symmetric encryption and decryption using the key k.

The sender Alice picked uniformly at random from [1..q – 1] which is treated as private key $PRIV_A$ of her. then she compute the public key $PUB_A=PRIV_A \times ECC_p$. The receiver bob picked uniformly at random from [1..q – 1] which is treated as private key $PRIV_B$ of his .then he compute the public key $PUB_B=PRIV_B \times ECC_p$

3.1.2 Signcryption Phase

Step 1: Verifies Bob's public key PUB_B by using his certificate.
Step 2: Selects an integer RAND, where RAND϶ n-1
Step 3: Compute KEY = (KEY_1 , KEY_2) = hash(PUB_B × (RAND+ $PRIV_A$)).
Step 4: Compute K = H (KEY_1 || ID_A|| KEY_2|| ID_B).
Step 5: Generate cipher text C = $ENCRYPT_K$(M).
Step 6: Compute r = H (C || ID_A|| ID_B).
Step 7: Compute R = r × ECC_p.
Step 8: Compute S = (RAND + $PRIV_A$) / r mod q.
Now alice send (C, R, S) to bob.

3.1.3 Unsigncryption Phase

Step 1: Verifies Alice's public key PUB_A by using her certificate.
Step 2: Compute KEY = (KEY_1, KEY_2) = Hash(S×R×$PRIV_B$)
Step 3: Compute K = Hash (KEY_1 || ID_A|| KEY_2||ID_B).
Step 4: Generate plain text M = $DECRYPT_K$(C).
Step 5: Compute r = Hash (C|| ID_A||ID_B).
Step 6: Check R (received from Alice) = = r × ECC_p.
If true ,then message is accepted.
otherwise message is rejected .

3.1.4 Judge Verification Phase

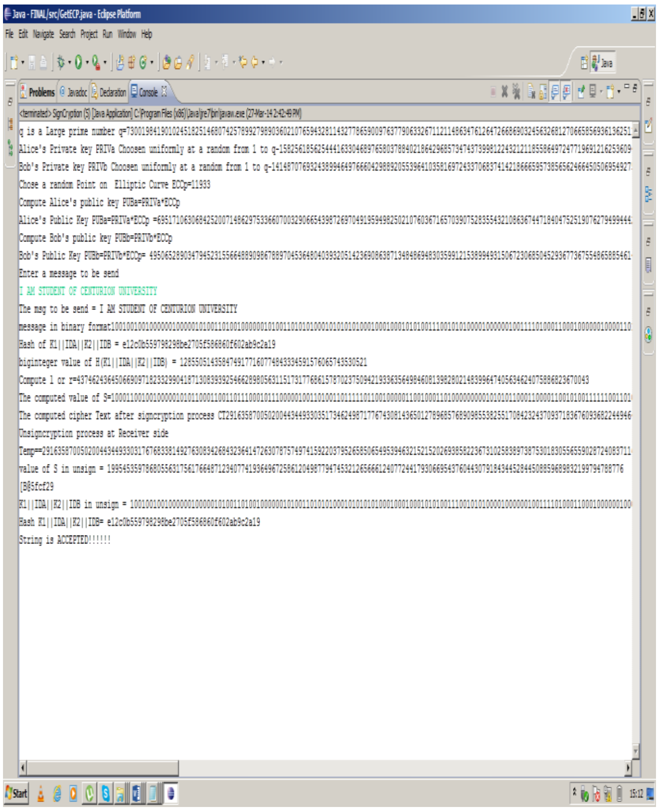
In our proposed scheme, the Bob delivers (C, R, S) to the judge to decide that the message M is sent by the Alice or not, when dispute occurs. The judge performs the following steps:
Step 1: Compute r = Hash (C|| ID_A||ID_B).
Step 2: Check if R(received from bob) = = (r × ECC_p), then the sender Alice send the message to Bob surely.

3.2 Correctness of proposed scheme

The key KEY generated by the sender is as
KEY = (KEY_1, KEY_2) = Hash (PUB_B × (RAND+ $PRIV_A$)).
= Hash ($PUB_{\mathbf{B}}$ × ((S× r) - $PRIV_A$ + $PRIV_A$))
= Hash ($PUB_{\mathbf{B}}$ × S× r).
= Hash ($PRIV_B$ × ECC_p × r × S).
=Hash ($PRIV_B$ × R × S), which is same as the symmetric key at receiver side.

4. IMPLEMENTATION OF OUR PROPOSED SCHEME IN JAVA:

Steps of our proposed scheme in java platform.
Step 1 :Taking q as a large prime number of length 512 bit.
BigInteger q=BigInteger.probablePrime(keysize,rndm1);
Step 2 : compute private key of sender i.e. $PRIV_A$.
BigInteger $PRIV_A$=BigInteger.probablePrime(keysize,rndm2);
Step 3: compute private key of sender i.e. $PRIV_B$.
BigInteger $PRIV_B$=BigInteger.probablePrime(keysize,rndm2);
Step 4: compute the value of ECC_p.
ECCp = GetECP ();
Step 5: compute public key of sender i.e. PUB_A.
BigInteger PUB_A = $PRIV_A$.multiply(ECC_p);
Step 6: compute public key of receiver i.e. PUB_B.
BigInteger PUB_B = $PRIV_B$ .multiply(ECC_p);
Step 7: Taking a random number i.e. RAND.
Step 8: Calculate KEY.
M=T.multiply(PUB_B.);
BigInteger KEY=new BigInteger (SHA1(M),16);
Where T= RAND+ $PRIV_A$
Step 9: Calculate K.
BigInteger KEY=new BigInteger (SHA1(V),16);
Where V = KEY_1 || ID_A|| KEY_2|| ID_B .
Step 10 : BigInteger r=new BigInteger (SHA1(S),16);
Where S= C || ID_A|| ID_B .
Step 11: Calculate s.
Step 12: encrypt the message using K.
Step 13: Calculate R= r . ECC_p.


Java - FINAL/src/GetECP.java - Eclipse Platform
File Edit Navigate Search Project Run Window Help
Java
Problems Javadoc Declaration Console

```
<terminated> SignCryption (5) [Java Application] C:\Program Files (x86)\Java\jre7\bin\javaw.exe (27-Mar-14 2:42:49 PM)
q is a Large prime number q=7300198419010245182514680742578992798903602107659432811432778659009763779063326711211486347612647266869032456326812706658569361362S1
Alice's Private key PRIVa Choosen uniformly at a random from 1 to q-158256185625444163304689765803788402186429685734743739981224321211855864972477196912162S3609
Bob's Private key PRIVb Choosen uniformly at a random from 1 to q-1414870769324389946497666042988920553964103581697243370683741421866659573856562466450506954927
Chose a random Point on  Elliptic Curve ECCp=11933
Compute Alice's public key PUBa=PRIVa*ECCp
Alice's Public Key PUBa=PRIVa*ECCp =69517106306842520071486297533660700329066543987269704919594982502107603671657039075283554321086367447184047525190762794994444
Compute Bob's public key PUBb=PRIVb*ECCp
Bob's Public Key PUBb=PRIVb*ECCp= 4950652890347945231556648890986788970453648040393205142369086387134848694830359912153899493150672306850452936773675548658854 61
Enter a message to be send
I AM STUDENT OF CENTURION UNIVERSITY
The msg to be send = I AM STUDENT OF CENTURION UNIVERSITY
message in binary format1001001001000000100000101001101001000000101001101010100010101010100010001000101010011100101010000100000010011110100011000100000010000110
Hash of K1||IDA||K2||IDB = e12c0b559798298be2705f586860f602ab9c2a19
biginteger value of H(K1||IDA||K2||IDB) = 1285505143584749177160774843334591576065743530521
Compute 1 or r=437462436450669097182332990418713083939254662898056311517317768615787023750942193363564984608139828021483996474056346240758868236700 43
The computed value of S=10001100100100000101011000110011011100010111000001001101001101111101100100000110010001101000000000101010110001100001100101001111110011010
The computed cipher Text after signcryption process CT29163587005020044344933035173462498717767430814365012789685768909855382551708423243709371836760936822449460
Unsigncryption process at Receiver side
Temp==291635870050200443449330317676833814927630834268432364147263078757497415922037952658506549539946321521520269385822367310258389738753018305565590287240837110
value of S in unsign = 19954535978680556317561766487123407741936496725861204987794745321265666124077244179306695437604430791843445284450885968983219979478877 6
[B@5fcf29
K1||IDA||K2||IDB in unsign = 100100100100000010000010100110100100000010100110101010001010101010001000100010101001110010101000010000001001111010001100010000000100
Hash K1||IDA||K2||IDB= e12c0b559798298be2705f586860f602ab9c2a19
String is ACCEPTED!!!!!!
```

Fig 5. Output of our Proposed Scheme

5. SECURITY ANALYSIS OF OUR PROPOSED SCHEME

The proposed scheme provides all the security issues such are confidentiality, integrity, authentication, unforgeability and non-repudiation along with the forward secrecy and public verification.

5.1 Confidentiality*:* Confidentiality states only the intended recipient of a signcrypted message should be able to examine its contents. In our scheme, if the attacker wishes to read the message then he/she must has to derive the key says, KEY. To get the value of KEY , he/she will try to catch it in many tactics:

Tactic 1: Attacker tries to find the value of KEY by using the statement $KEY = (KEY_1 , KEY_2) = hash(PUB_B \times (RAND+ PRIV_A))$. But the value of RAND and $PRIV_A$ is private for alice which is not known by anyone except alice in addition one-way hash function is collision resistant so it is very difficult to derive the KEY.

Tactic 2: Using another statement, Attacker tries to figure the value of KEY. Firstly he/she simply derive the value of J (if he/she knows about hash function) from the statement $KEY = (KEY_1 , KEY_2) = hash(S\times R\times PRIV_B)$. However it requires the value of $PRIV_B$, which is not possible because it is only known by bob .

Tactic 3: In another way, using the statement $S = (RAND + PRIV_A) / r \mod q$ Attacker tries to figure the value of KEY by finding the value of RAND but it is not possible because private key of alice ($PRIV_A$) and r is involved.

5.2 Authenticity: Authenticity says that the recipient of a signcrypted message is proficient to confirm the sender's identity. Our proposed scheme achieve authenticity property of the message security. The receiver can validate whether the message is sent by Alice or not by checking R(received from alice) = = r × ECC_p or not ,if yes then recipient confirms that the signature is given by alice.

5.3 Integrity: Message integrity says that the message has not been changed. The receiver of the message should be able to verify that the message is original one. Our proposed scheme achieve integrity property of the message security. Assume that the attacker changed the cipher text C to C' and sent it to bob. Bob calculate the digest value of $r = H (C \| ID_A\| ID_B)$ and check R(received from alice) = = r × ECC_p ,which is obviously not same because previously calculated r is not original one. In this way recipient should be able to verify that the received message is not original.

5.4 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. . Our proposed scheme achieves Forward Secrecy of message confidentiality. Assume that the attacker get previously recorded value (C,R,S) ,the attacker cannot be able to decrypt the previous message even if he/she knows the value of long term private key of alice i.e. $PRIV_{A.}$ Let he/she tries to get the value of KEY by using the statement

$$KEY= hash(PUB_{\mathbf{B}} \times (RAND+ PRIV_A)).$$
$$=hash (PUB_{\mathbf{B}}\times ((S\times r)-PRIV_A+PRIV_A))\ldots \ldots\ldots(1)$$

So the attacker has to solve ECDLP to get the value of r which is essential to decrypt the previous message.

5.5 Public Verification: Public Verification says Third party can be able to verify the recipient identity of message without the knowledge of sender's private key. Our proposed scheme achieve public verification of message security. In our prosed scheme third party can verify the message is actually sent by alice when dispute occurs by performing $r = H (C \| ID_A\| ID_B)$ and then check R (received from bob) = = r × ECC_p or not. If equal then message is sent by alice. In all the above calculation original message (M) is not involved so that the message is not transparent to the third party.

5.6 Non-repudiation: Non-repudiation 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. Our proposed scheme achieve non-repudiation of message security. When dispute occurs between alice and bob, bob send (C,R,S) to third party, who conclude the signature formed by alice by computing R = r × ECC_p.

5.7 Unforgeability: Unforgeability states, it is computationally infeasible for an attacker to produce the signcrypted text of the sender because it requires private key of the sender which is known to only the authorized sender. if he try to generate the private key of the sender then he has to solve the ECDLP which is computationally infeasible.

6. ANALYSIS OF COMPUTATIONAL COST

Our proposed scheme consume reduced amount of computational cost for both signcryption and unsigncryption phase. The data given in TABLE II shows the comparative analysis of computational cost of various existing signcryption techniques including our proposed scheme. The proposed scheme is more efficient than the existing schemes as it takes only two elliptic curve point multiplication at sender side and two in receiver side. According to Infineon's SLE66CUX640P security controller [11], elliptic curve point multiplication takes 83 ms for computation. Various existing signcryption techniques takes different computational cost shows in TABLE 1 and in fig 6 as chart format .our proposed scheme takes 166ms of computation in both the sender and receiver side with satisfying all the security goals.

Table 1: Comparison based on average computational time of major operation.

Schemes	Sender average. computational time in ms	Recipient average computational time in ms
Dutta, Singh, A. Kumar[6]	3×83=249	2×83=166
M.Toorani, Shirazi[7]	2×83=166	4×83=332
Zheng[1]	1×220=220	2×220=440
Zheng & Imai[3]	1× 83=83	2×83=166
Bao & Deng[2]	2×220=440	3×220=660
Gamage et al[4]	2×220=440	3×220=660

Ren-Junn Hwang [5]	2×83=166	3×83=249
Jung et. al.[8]	2×220=440	3×220=660
Our proposed scheme	2×83=166	2×83=166

Table II: Comparison based computational cost of different existing scheme.

Various scheme	Sender/ receiver	EXP	DIV	ECPM	ECPA	MUL	ADD	KH(.)
Gamage et al[4]	Alice	2	1	.	.	.	1	2
	Bob	3	.	.	.	1	.	2
M. Dutta, A .K. Singh[6]	Alice	.	1	3	.	1	1	3
	Bob	.	.	2	1	.	.	3
Toorani,A.A Shirazi[7]	Alice	.	.	2	.	2	2	2
	Bob	.	.	4	2	.	.	2
Zheng[1]	Alice	1	1	.	.	.	1	2
	Bob	2	.	.	.	2	.	2
Zheng & Imai[3]	Alice	.	1	1	.	1	1	2
	Bob	.	.	2	1	2	.	2
Bao & Deng[2]	Alice	2	1	.	.	.	1	3
	Bob	3	.	.	.	1	.	3
Jung et. Al[8]	Alice	2	1	.	.	.	1	2
	Bob	3	.	.	.	1	.	2
Ren Junn-Hwang[5]	Alice	.	.	2	.	1	1	1
	Bob	.	.	3	1	.	.	1
Our scheme	Alice	.	1	2	1	.	2	2
	Bob	.	.	2	.	1	.	2

Exp: modular exponential operation. Div: modular division operation. ECPM: elliptic curve point multiplication operation. ECPA: elliptic curve point addition operation. Mul: modular multiplication operation. Add: modular addition operation. Hash (.): one way Hash function.

Table III: Comparison based on security issues supported by the different scheme including our proposed scheme

Security issues Scheme	Confidentiality	Integrity	Unforgeability	Non-repudiation	Forward security	Public Verification
M. Dutta, A.K. Singh[6]	YES	YES	YES	DIRECTLY	YES	YES
M. Toorani, Shirazi[7]	YES	YES	YES	DIRECTLY	YES	YES
Zheng[1]	YES	YES	YES	ANOTHER PROTOCOL	NO	NO
Zheng & Imai[3]	YES	YES	YES	ANOTHER PROTOCOL	NO	NO
Bao & Deng[2]	YES	YES	YES	DIRECTLY	NO	YES
Jung et. Al[8]	YES	YES	YES	ANOTHER PROTOCOL	YES	NO
Ren-Junn-Hwang[5]	YES	YES	YES	DIRECTLY	YES	NO
Gamage et al[4]	YES	YES	YES	DIRECTLY	NO	YES
Our proposed scheme	YES	YES	YES	DIRECTLY	YES	YES

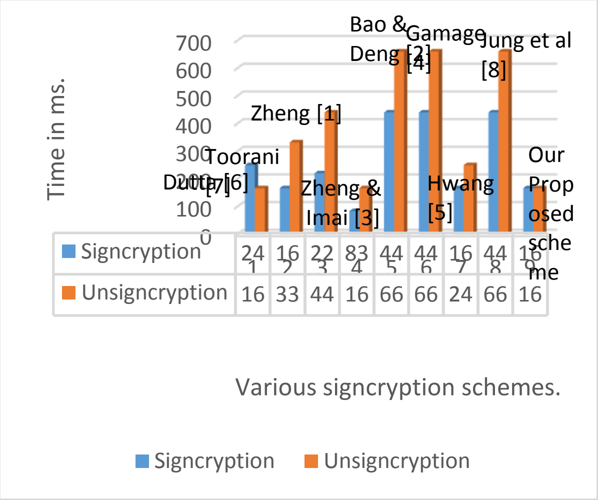


Fig.6. Comparison based on the average computational time various schemes including our proposed scheme.

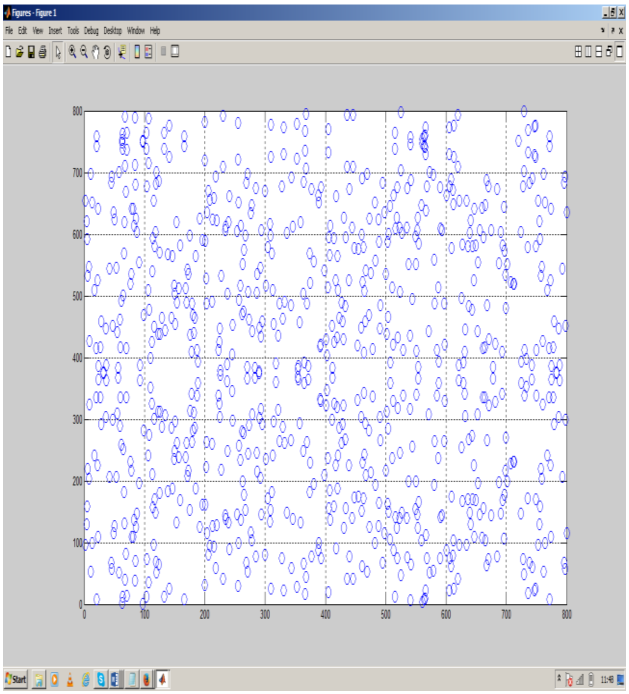


Fig.7. Possible points on the curve where a=59, b=78 and p=751 satisfying $y^2 = x^3 + ax + b \pmod p$ and $4a^3 + 27b^2 \bmod p \neq 0$.

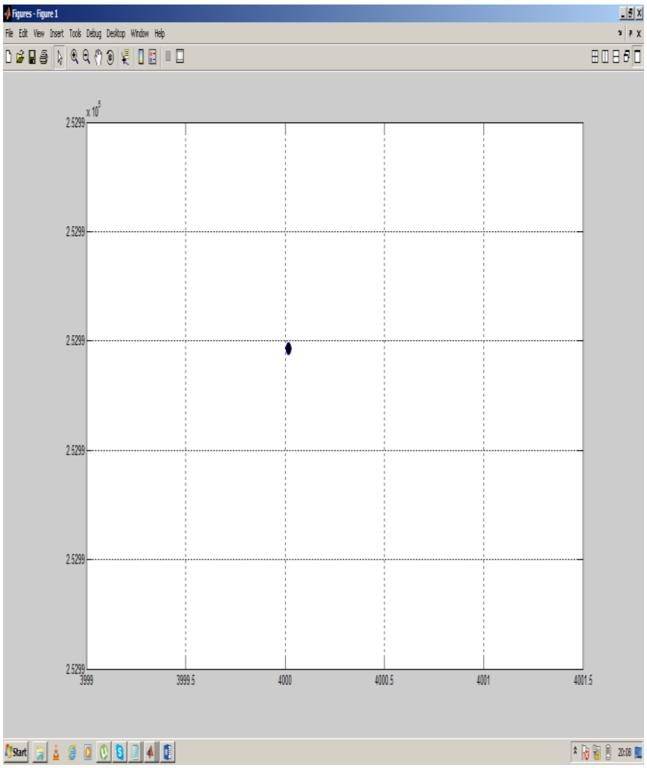


Fig.8. Showing the public key of sender PUB$_A$=PRIV$_A$ × ECC$_p$= (4.0000e+003, 2.5299e+005) where PRIV$_A$ $_=$318(randomly chosen) and taking ECC$_p$=(4, 621).

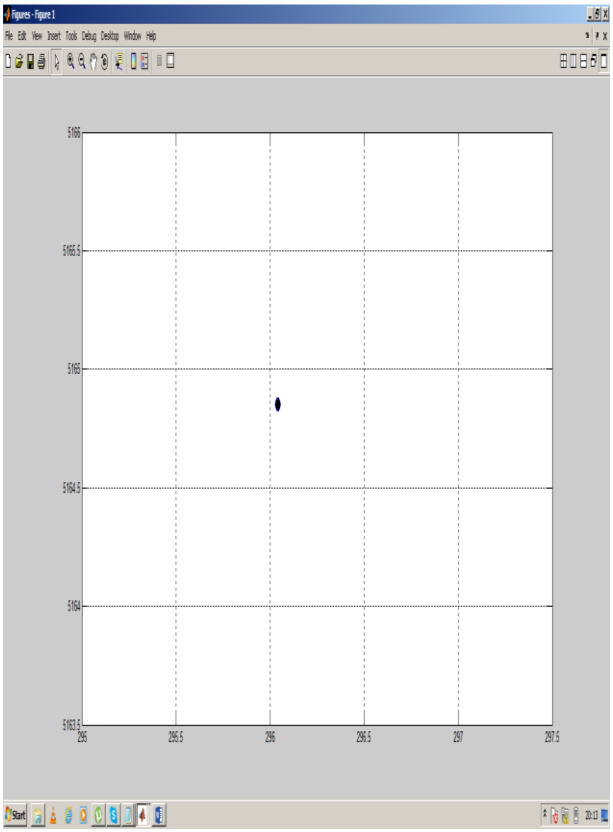


Fig.9. Showing the public key of receiver PUB$_B$=PRIV$_B$ × ECC$_p$= (296.0402, 5.1649e+003) where PRIV$_B$ $_=$951(randomly chosen) and taking ECC$_p$=(4, 621).

7. CONCLUSION AND FUTURE WORK

Our proposed technique is based on elliptic curve cryptosystem, which offer an effectual signcryption technique with additional security than the Digital Logarithmic Problem. It achieves all the security goals i.e. confidentiality, authenticity, integrity, non-repudiation and unforgeability along with public verification by which anyone can verify the signature without having any knowledge of original text message and forward secrecy of the message confidentiality with reduced amount of computational cost than the existing schemes. Our scheme is more efficient than the existing scheme as it needs two elliptic curve multiplication to signcrypt the message and uses two elliptic curve point multiplication to unsigncrypt the message. This scheme is implemented using java technology which can be beneficial in any platform. It is attractive for the security establishment in store-and forward application such as E-mail and Short Message Services. And it has great advantages to be deployed in resource- constraints devices such as: mobile phones. The future possibility of signcryption scheme can be built using hyper elliptic curve [16], which consumes much less amount of time than the elliptic curve.

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

[4] 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

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

[6] M. Dutta,A.K Singh, A. Kumar,”An efficient signcryption schemebased on ECC with forward secrecy and encrypted message authentication”, 3rd IEEE international Advance Computing Conference(IACC),2013

[7] Mohsen Toorani and Ali Asghar BeheshtiShirazi, “ An elliptic curve based signcryption with forward secrecy”, Journel of Applied Science, 9(6):1025-1035,2009.

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

[9] William Stalling, Cryptography and Network Security: Principle and Practices.Prentice Hall Inc.,Second Edition,1999.

[10] K.H Rosen, “Elementary Number Theory and Its Application,”2nd edition,Addison-Wesley,1988

[11] L. Batin, S.B Preneel, J. Vandewalle, Hardware architectures for public key cryptography, Integration the VLSI Journal 34 (1-2) (2003) 1-64.

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

[13] [13] J. Beak, R. steinfeld, Y. Zheng, Formal proofs for the security of signcryption, in: Proceedings of PKC’02LNCS 2274 , Springer-Verlag , 2002,pp. 81-98.

[14] D. Johnson , A. Menezes, S. Venstone , The elliptic curve digital signature algorithm (ECDSA), International Journal of Information Security 1(1) (2001) 36-63.

[15] Certicom Research, Standard for efficient cryptography, SEC1: elliptic curve cryptographyStandard for efficient cryptography group (SECG), sept 20, 2000.

[16] N. Kobiltz, Hyperelliptic cryptosystem, Journal of Cryptology, Volume 1, Number 3,pp. 139-150(1989).

[17] D. Boneh, R. J Lipton, Algorithm for black-box fields and their application to cryptography, in: Advancse in Cryptography: Crypto’ 96, 1996, pp. 283-297.