An Elliptic Curve based Signcryption Protocol using Java

Sumanjit Das
Assistant Professor,
Dept. of ComputerScience & Engg,
Centurion University of Technology and
Management, Bhubaneswar, INDIA

Biswajit Samal
Lecturer,
Dept. of Computer Science & Engg.
Centurion University of Technology and
Management, Bhubaneswar, INDIA.

ABSTRACT

Now a day's information technology is a part of day to day's life. Everybody wants to store data in soft format in a central place so that it can be accessed any point of time. When a remote user tries accessing it through an unreliable network then data may not be secure. There are many techniques to secure data or message. Signcryption is one of the booming issues in the field of security. In 1997 Zheng introduce signcryption scheme by combining the techniques of digital signature then encryption in one step which reduces the computational cost and communication overhead [1]. Signcryption also verifies the sender without reading content of the message by third party [10]. Many researchers have given their signcryption scheme to achieve security goals like forward secrecy, like confidentiality, unforgeability, integrity, forward secrecy and public verification non repudiation but many of them having their own limitations [2, 8, 16]. In this paper a novel signcryption scheme proposed which is implemented using java and also achieves all the security goals.

General Terms

Computer Science, Cryptography, Algorithms et. al.

Keywords

Cryptography, forward secrecy, signcryption, ECC.

1. INTRODUCTION

Today's cryptosystem provides the resources for data security for information while transmitting it over an insecure channel. When a data is transmitted over the internet we must provide integrity, confidentiality, authenticity and non-repudiation [1] for it. Previously encryption and digital signatures are played an important role in achieving message confidentiality and data integrity but independently. Traditionally the message is used to sign first using digital signature and then the message is encrypted to achieve both the confidentiality and data integrity. The scheme is commonly known as signature-then-encryption scheme [2, 5]. The scheme having two problems: Low efficiency and high cost of such simulation.

To solve the above two problems a new cryptographic method is used called signcryption. [1, 2] Signcryption fulfill the both the functionality of digital signature and encryption in a single logical step, but with a reduced cost than Sign-then-Encryption.

The first Signcryption is purposed by Zheng in 1997 it achieves most of the security goals of cryptosystem but it fails forward secrecy of message confidentiality.

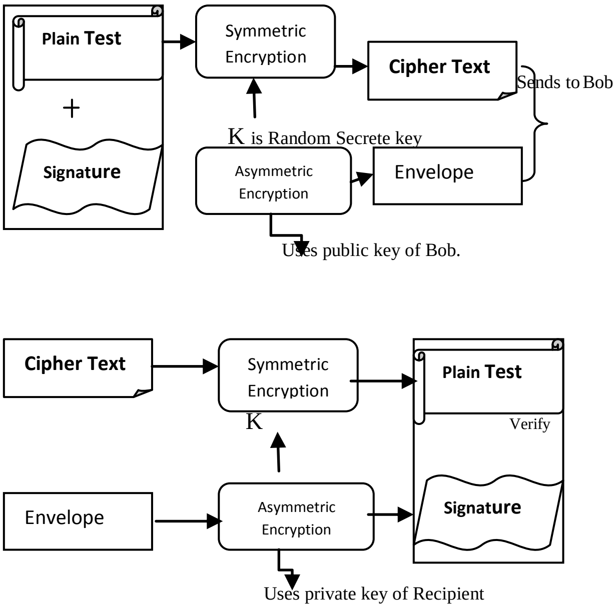


Fig 1: Represents the signature then encryption scheme

In 1998 Zheng and Imai proposed another version of signcryption scheme based on Elliptic curve that saves 50% of computational cost and 40% of communication cost compared to traditional Sign-then-Encryption scheme [1, 8]. They are many signcryption schemes having their own advantages and demerits most of them include confidentiality, unforgeability, Integrity and Non repudiation [3, 16]. Some of them provide further attributes such as public verification and Forward security while other does not provide them [4, 6].

This paper introduced a new signcryption protocol that support all the security goals like message confidentiality, authenticity ,integrity ,unforgability ,non repudiation, public verifiability and forward secrecy of the message [2,3]. It's also implemented the above protocol using java language.

2. RELATED WORK

Zheng's signcryption scheme was based on DLP (Discrete Logarithmic problem where sender generates the symmetric key by using the public key of the receiver. After receiving the cipher text and digital signature the sender uses his private key to decrypt the message. Zheng and Imai proposed another signcryption scheme based on the elliptic curve discrete logarithm problem (ECDLP) that achieved similar functionality [1, 3]. Both the schemes lacked forward secrecy, public verifiability and encrypted message authentication.

Gamage, Leiwo and Zheng proposed a scheme based on DLP that enabled firewalls to authenticate encrypted messages without having to decrypt them and lacked forward secrecy.

Bao and Deng proposed a signcryption scheme with signature verifiable by the public key of the recipient. Bao-Deng scheme was based on DLP [2]. It lacked forward secrecy and encrypted message authentication as the message had to be sent to a third-party together with secret number and key to settle a dispute [5, 7].

To conquer the weaknesses in Zheng-Imai scheme, CHEN Ke-fei and LI Shi-qun proposed two signcryption variants based on ECDLP [8], one with only public verifiability and another with only forward secrecy. Each scheme had only one of the desired properties and both lacked encrypted message authentication [13].

2.1 Zheng-Imai Elliptic Curve Signcryption Scheme

The Two most popular schemes named as ECSCS1 and ECSCS2 based on elliptic curved are purposed by Zheng – Imai [1]. We are discussing only ECSCS1. The case is similar for the other ECSCS2 [1].

If Alice wants to send a message m to Bob he has to signcrypts m as follows. So that the effect was similar to signature then encryption.

Public Parameters:
C: an elliptic curve over GF (P^h), either with $p \geq 2^{160}$ and h = 1 or p = 2 and h $\geq$ 150.
q: a large prime number chosen randomly whose size is approximately |ph|.
G: a point on the curve C, chosen randomly of order q.
hash: a one-way hash function output of 128 bits at least..
KH: a keyed one-way hash function.
E, D: the encryption and decryption algorithms of a private key cipher.
Alice's keys:
V_a: Alice's private key, chosen uniformly at random from [1… q - 1].
P_a: Alice's public key ($P_a = V_aG$, a point on C).
Bob's keys:
V_b: Bob's private key, chosen uniformly at random from [1… q - 1].
P_b: Bob's public key ($P_b = V_bG$, a point on C).
Signcryption of message m by Alice (the sender):
v ε r [1, …, q – 1]
$(k_1, k_2) = hash(VP_b)$
$c = Ek_1$ (m)
$r = KHk_2(m)$
$s = v / (r + V_a) \bmod q$
Send c, r, s to Bob

Unsigncryption of c, r, s by Bob (the recipient):
$u = sV_b \bmod q$
$(k_1, k_2) = hash(uP_a + urG)$
m = Dk1(c)
Accept m only if KHk2(m) = r

3. PROPOSED SCHEME

The purposed new scheme was based on elliptic curve cryptosystem and implemented in java. Here each user should get the certification of his public key from the certificate authority (CA) and are uniquely identified by their unique identifiers IDA and IDB.In our scheme we have taken same parameter as of Zheng-Imai and it works as follows.

Initialization phase:

In this phase, some public parameters are generated. The steps are as follows:

q: a large prime number, where q is greater than 2160 .

G : A point chosen randomly on the curve C.

Va: Alice's private key, chosen uniformly at random from 1 to q-1.

Pa: Alice's public key, where Pa=VaG, a point on C.

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

Pb: Bob's public key, where Pb=VbG a point on C.

Signcryption of m by Alice:

Assume that Alice (Sender) want to send a message m to Bob (Receiver). Alice generates the digital signature (R, s) of message m and uses the symmetric encryption algorithm and a secret key k for encrypt of m. c will the cipher text. Alice generate the signcrypted text (c,R,s) as follows:

Step 1: Select v ε r [1,… q-1].

Step 2: Compute k1=hash (vPb).

Step 3: compute k2= hash (vG)

Step 4: c= Ek1 (m)

Step 5: r = KHK2 (m||v)

Step 6: s=hash (r mod q)

Step 7: Send signcrypted text (c, r, s) to Bob.

Unsigncryption of c, r, s by Bob:

Bob receives the signcrypted text (c, r, s). He decrypts cipher text 'c' by performing decryption algorithm with secret key k. He also verifies the signature. Bob gets the plain text as follows.

$K2 = hash(s(r + P_a))$

$R = hash (c, k_2)$

k1 = hash(VbS(r + Pa))

m = DK1(c)

Accept m only if rG = R

4. IMPLEMENTATION IN JAVA

In the purposed signcryption scheme, some security packages are included to manipulate cryptographic functions.

Steps to initialize public Parameters:

Step 1: Generate q a large prime number of length 512 bit.

BigInteger v=BigInteger.probablePrime(keysize,r);

Step 2: compute V_a

BigInteger V_a=BigInteger.probablePrime(keysize,r) ;

Step 3: compute V_b

BigInteger V_b=BigInteger.probablePrime(keysize,r) ;

Step 4: Compute G

BigInteger C=new GetECP()

Step 4:Compuet Alice's public Key.

BigInteger P_a=Va.multiply(G).

Step 5: Compute Alice's public key

BigInteger P_b=Vb.multiply(G);

Step 6:calculate k1 & k2 with the same length

Step 7: calculate r using K_2;

BigInteger r=new BigInteger(SHA1(K2||m),16);

step 8: calculate s.

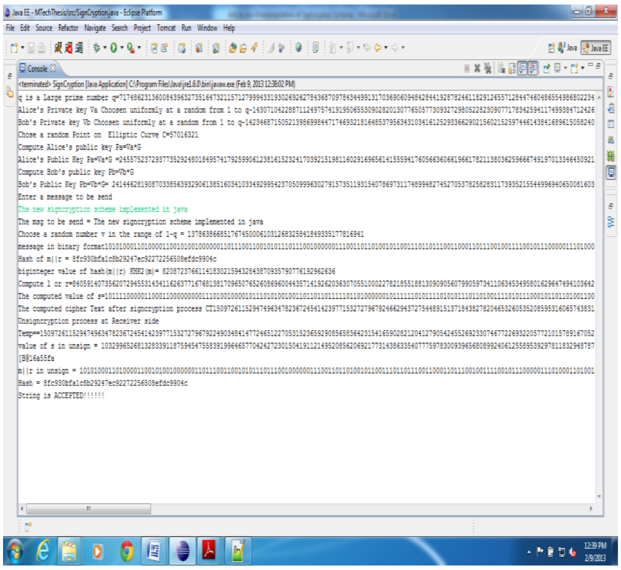
s=hash (r mod q)

Step 9: Encrypt m using k1

c= Ek1 (m)

Step 10: Decrypt c

If both the hash value is matched i.e. hash (m||r) at sender and hash (r||s) at receiver side is matched then the message is accepted otherwise rejected.



```
<terminated> SignCryption [Java Application] C:\Program Files\Java\jre1.6.0\bin\javaw.exe (Feb 9, 2013 12:38:02 PM)
q is a Large prime number q=717486231360084396327351647321157127999433193026926278436870978434499131703690609484284419287824611829126557128447460486554986802234
Alice's Private key Va Choosen uniformly at a random from 1 to q-14307104228871124975741919506553090282013077650577309327298052282309077178342594117499384712426
Bob's Private key Vb Choosen uniformly at a random from 1 to q-1423468715052139869984471746932181648537956343103416125293366290215602152597446143841689615058240
Chose a random Point on  Elliptic Curve C=57016321
Compute Alice's public key Pa=Va*G
Alice's Public Key Pa=Va*G =245575237293773529248018495741792599061238161523241703921519811602916965614155594176056636066196617821138036259666749197013346450921
Compute Bob's public key Pb=Vb*G
Bob's Public Key Pb=Vb*G= 24144628190870338563932906138516034103349299542370509996302791573511931540786973117489948274527053782582831173935215544996940650081603
Enter a message to be send
The new signcryption scheme implemented in java
The msg to be send = The new signcryption scheme implemented in java
Choose a random number v in the range of 1-q = 1378638668517674500061031268325841849335177816941
message in binary format1010100011010000110010100100000011011100110010101110111001000000111001101101001011001110110111001100011011100100111100101110000011101000
Hash of m||r = 8fc930bfa1c8b29247ec92272256508efdc9904c
biginteger value of hash(m||r) KHK2(m)= 820872376611418302159432843870935790776192962636
Compute l or r=8405914073562072945531434116263771676813817096507652608696004435714192620363070551000227821855188130909056079905973411063453495801629647494103642
The computed value of s=10111100000110001100000000011101001000010111010100100110110110111110110100000001011111101011110101011101101001111010111000101101101001100
The computed cipher Text after signcryption process CT1509726115294749634782367245414239771532727967924662943727544891513718438278204653260535208595316065743831
Unsigncryption process at Receiver side
Temp==1509726115294749634782367245414239771532727967922490348414772465122705315236592908565836423154165902821204127905424552692330746772269322057721015789167052
value of s in unsign = 10329965268132833911875945475583919964657704242723015041911214952085620692177314386335407775978300939656808992406125589539297811832948787
[B@16a55fa
m||r in unsign = 10101000110100001100101001000000110111001100101011101110010000001110011011010010110011101101110011000110111001001111001011100000111010001101001
Hash = 8fc930bfa1c8b29247ec92272256508efdc9904c
String is ACCEPTED!!!!!!
```

Fig 2: Output of the implemented scheme

5. ANALAYSIS

5.1 Security

The proposed signcryption scheme fulfills all properties of security. It's also following the process of encryption and digital signature but in one step. The security attributes like Confidentiality, Unforgeability, Integrity, and non-repudiation [1, 2, 3]. Some signcryption schemes provide further attributes such as Public verifiability and Forward secrecy of message confidentiality. Such properties are the attributes that are required in many applications while the others may not require them.

Confidentiality: The proposed scheme should be computationally infeasible for an adaptive attacker to gain any partial information on the contents of a signcrypted text, without knowledge of the sender's or designated recipient's private key.

Unforgeability: It should be computationally infeasible for an attacker to masquerade an honest sender in creating an authentic signcrypted text that can be accepted by the unsigncryption algorithm.

Non-repudiation: In proposed scheme the recipient should have the capability to prove to a third party (e.g. a judge) that the sender has sent the signcrypted text. This ensures that the sender cannot deny his previously signcrypted texts.

Integrity: The recipient should be able to verify that the received message is the original one that was sent by the sender.

Public Verifiability: In proposed scheme the third party without any need for private key of sender or recipient can verify that the signcrypted text is a valid signcryption of its corresponding message or not.

Forward Secrecy of message confidentiality: If the long private key of the sender is compromised, no one should be able to pull out the plaintext of previously signcrypted texts. In a regular signcryption scheme, when the long private key is compromised, all the previously issued signatures will not be reliable any more. Since the threat of key exposure is becoming more acute as the cryptographic computations are performed more regularly on poorly protected devices such as mobile phones, the forward secrecy seems an essential attribute in such systems.

Table 1. Indicates the security features supported by existing signcryption schemes along with the proposed schemes. The proof is based on the fact that it is almost intractable to solve the elliptic curve discrete logarithmic problem (ECDLP) [3, 13].

	Confiden tiality	**Integrit y**	**Unforge ability**	**Forwar d Securit y**	**Pub. verific ation**
Zheng	Yes	Yes	Yes	No	No
Zheng and Imai	Yes	Yes	Yes	No	No
Bao & Deng	Yes	Yes	Yes	No	Yes
Gama ge et al	Yes	Yes	Yes	No	Yes
Jung et al.	Yes	Yes	Yes	Yes	No
Han et al.	No	No	No	No	Yes
Hwan g et al.	No	No	No	No	Yes
Propo sed schem e	Yes	Yes	Yes	Yes	Yes

5.2 Complexity of Proposed Scheme

The proposed signcryption scheme is based on elliptic curve time required for elliptic curve point multiplication makes the major difference in computational cost.

Table 2. comparison of schemes on basis of computational complexity.

Scheme s	**Partic ipant**	**EC PM**	**ECP A**	**Mod. Mul**	**Mod. Add**	**Hash**
Zheng & Imai	Alice	1	-	1	1	2
	Bob	2	1	2	-	2
Han et al	Alice	2	-	2	1	2
	Bob	3	1	2	-	2
Hwang et al	Alice	2	-	1	1	1
	Bob	3	1	-	-	1
Propos ed scheme	**Alice**	**2**	**1**	**-**	**-**	**2**
	Bob	**3**	**-**	**1**	**1**	**2**

Table 3. 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 in infineon's SLE66CU* 640P security controller.[15, 16].

Schemes	**Sender average. computational time in ms**	**Recipient average computational time in ms**
Zheng	1 * 220 = 220	2*220 = 440
Zheng & Imai	1* 83=83	2*83=166
Bao & Deng	2*220=440	3*220=660
Gamage et al	2*220=440	3*220=660
Jung et al	2*220=440	3*220=660
Proposed scheme	**2*83=249**	**3*83=166**

Table-4: Analysis result for the purposed scheme.

Message Length (no of character)	**Signcryption Time (sec)**	**Unsigncryption Time (sec)**
4	0.021	0.001
8	0.023	0.002
16	0.022	0.002
32	0.024	0.003
80	0.026	0.004

160	0.031	0.005
300	0.033	0.007
500	0.04	0.01
1000	0.058	0.022

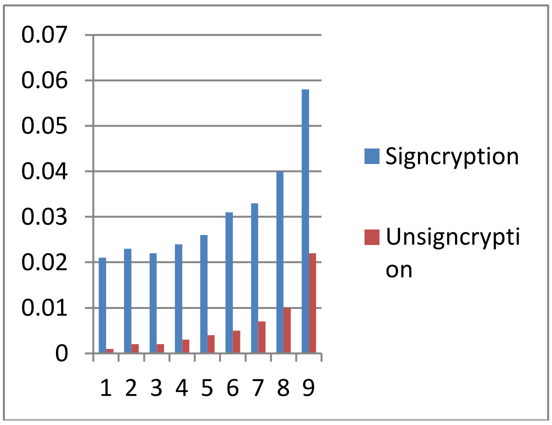


Fig 3: Analysis result for the purposed scheme

Table 5. Comparative analysis of proposed scheme versus different scheme on the basis of time. The comparative analysis is done under a specific system configuration which may very under different platform.

Message Length	Zheng's Signcryption	Proposed Signcryption
4	0.064	0.021
8	0.068	0.023
16	0.069	0.023
32	0.071	0.024
80	0.074	0.026
160	0.074	0.031
300	0.084	0.033
500	0.093	0.04
1000	0.107	0.058

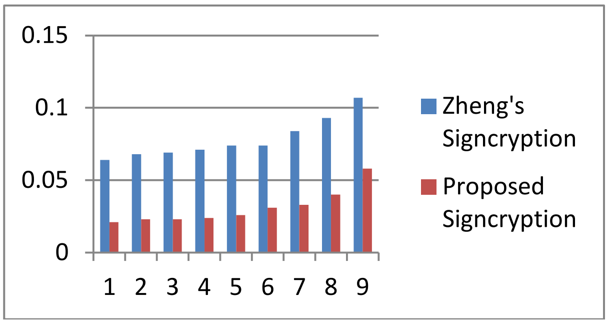


Fig 4: Comparison between Zheng's signcryption and proposed signcryption scheme.

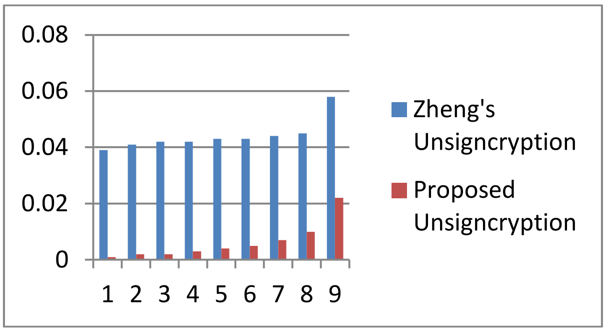


Fig 5: Comparison between Zheng's unsigncryption and proposed unsigncryption scheme.

6. CONCLUSION

In this paper a new signcryption scheme based on elliptic curve proposed which fulfills all properties of security goal like message authentication, integrity, public verification, unforgeability and non-repudiation [8, 15]. If the sender discloses the private key inattentively no one can extract the original message because it provides forward secrecy. The encrypted message can also verifiable by third party without reading content of message. This signcryption scheme reduces computational cost and communication overhead than the traditional signature-then encryption scheme [1, 3, 8]. The scheme is implemented using java technology which can be useful in any platform. The implemented scheme can be useful for e-commerce environment. Public verifiability is especially useful in e-commerce environments as it enables the trading partners to resolve disputes through any trusted or untrusted judge without interacting with the judge in a zero-knowledge proof communication and without disclose of any secret information [3, 11]. The proposed can be use in web server for short message services.

Signcryption schemes can also be built using hyperelliptic curves [9] (how to select secure hyper elliptic curves), and all the above analysis remains valid for these schemes. Proposed technique (Future possibility) can also be used for group signcryption.

7. REFERENCES

[1] Yuliang Zheng. Digital signcryption or how to achieve cost (signature encryption)Cost (signature), Cost (encryption). In CRYPTO '97: Proceedings 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] William Stallings. Cryptography and Network security: Principles and Practices. Prentice Hall Inc., second edition, 1999.

[5] 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.

[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] Mohsen Toorani and Ali Asghar Beheshti Shirazi. Cryptanalysis of an elliptic curve-based signcryption scheme. International journal of network security vol.10, pp 51-56,2010.

[14] Wang Yang and Zhang. Provable secure generalized signcryption. Journal of computers, vol.5, pp 807-814, 2010.

[15] Prashant Kushwah1 and Sunder Lal2, Provable secure identity based signcryption schemes without random oracles, International Journal of Network Security & Its Applications (IJNSA), Vol.4, No.3, May 2012.

[16] Sumanjit Das and Prasant Sahoo, cryptanalisys of signcryption protocols based on elliptic curve. IJMER,Vol.3, Issue-1, pp 89-92, 2013.