SIGNCRYPTION- AN EXPERIMENTAL APPROACH FOR DUAL SECURITY IN SINGLE ALGORITHM

Prof.(Dr.) M.L. Sharma[1], Dr. Sunil Maggu[2], Shikha Gupta[3]Sarthak Verma[4]

Maharaja Agarsen Institute of Technology, Rohini[1,2,3,4]

ABSTRACT

In the computerized period of data innovation everyone needs to store information in information server with the goal that numerous individuals can get to it. When a remote client attempt gets to it through a questionable system then we consider is our information secure or not? There are numerous extents to verify our message. Signcryption is one of the flourishing issues in the field of security. Zheng presents signcryption by joining the systems of encryption and computerized signature in one stage which diminishes the computational expense and correspondence overhead. Signcryption likewise confirms the sender without perusing the substance of the message by the outsider. Numerous scientists have given their signcryption plan to accomplish security objectives like sending mystery, similar to classification, unforgeability, honesty, forward mystery and open confirmation non-denial yet a considerable lot of them have their very own confinements. In his paper, we have proposed a novel signcryption plot which is actualized utilizing java and furthermore accomplishes the security objectives.

I. INTRODUCTION

Current cryptosystem gives the way to information security for data while transmitting it over a shaky channel. At the point when information is transmitted over the web we should give respectability, classification, legitimacy and non-revocation [1] for it. In more established days encryption and advanced marks are assuming an imperative job in accomplishing message privacy and information uprightness however freely. Generally the message is utilized to sign first utilizing advanced signature and after that the message is scrambled to accomplish both the privacy and information uprightness. The plan is normally known as a mark then-encryption plot. The plan having two issues: Low productivity and the surprising expense of such reproduction.

In Modern Era, to take care of the over two issues another cryptographic technique is utilized called signcryption. Signcryption satisfies both the usefulness of digital signatures and encryption in a single logical step, yet with a decreased expense than Sign-then-Encryption.

The principal Signcryption is purposed by Zheng in 1997 it accomplishes the majority of the security objectives of cryptosystem however it bombs forward mystery of message privacy.

In 1998 Zheng and Imai proposed another variant of signcryption conspire dependent on Elliptic bend that spares half of the computational expense and 40% of correspondence cost contrasted with conventional Sign-then-Encryption plot.They are numerous signcryption schemes having their own merits and demerits, the vast majority of them incorporate confidentiality, unforgeability, Integrity and Non-repudiation. Some of them give further traits, for example, open auditability and Forward securitywhile others don't give them.

In this paper, we presented another signcryption convention that bolsters all the security objectives like message privacy, credibility, trustworthiness, unforgability, non-disavowal, open evidence and forward mystery of the message. We have executed the above convention utilizing java language.

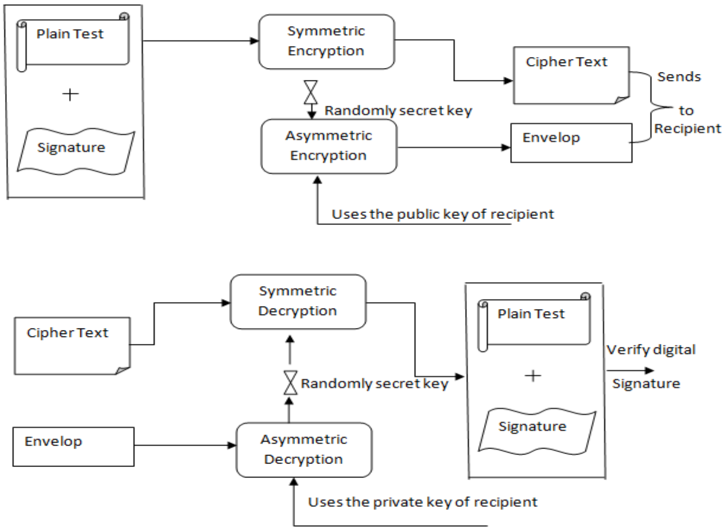


Fig: 1 – Sign then Encryption

II. RELATED WORK

Zheng's signcryption scheme depended on DLP (Discrete Logarithmic issue where the sender creates the symmetric key by utilizing the public key of the recipient. In the wake of getting the figure content and computerized signature the sender utilizes his private key to unscramble the message. Zheng and Imai proposed another signcryption conspire dependent on the elliptic bend discrete logarithm issue (ECDLP) that accomplished comparable usefulness. Both the plans needed forward mystery, open undeniable nature and encoded message verification.

Gamage, Leiwo and Zheng suggested a scheme dependent on DLP that empowered firewalls to validate encoded messages without unscrambling them and needed forward mystery.

Bao and Deng proposed a signcryption plot with mark obvious by the open key of the beneficiary. Bao-Deng scheme depended on DLP. It needed forward secrecy and encrypted message validation as the message must be sent to an outsider together with the secret number and key to settle a conflict.

To conquer the shortcomings in Zheng-Imai plot, CHEN Ke-fei and LI Shi-qun proposed two signcryption variations dependent on ECDLP; one with just open obviousness and another with just forward mystery. Each plan had just a single of the ideal properties and both needed encoded message confirmation.

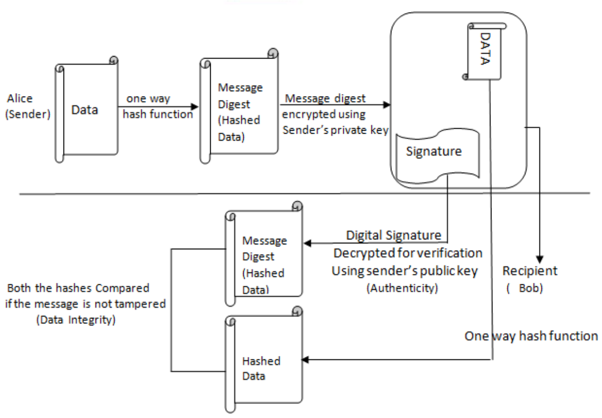
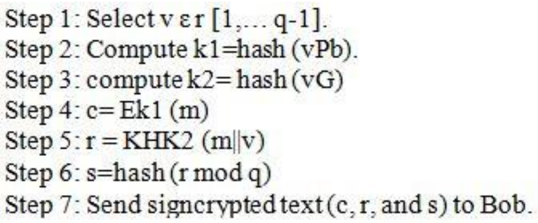


Fig 2: Credibility and data integrity check using digital signature.

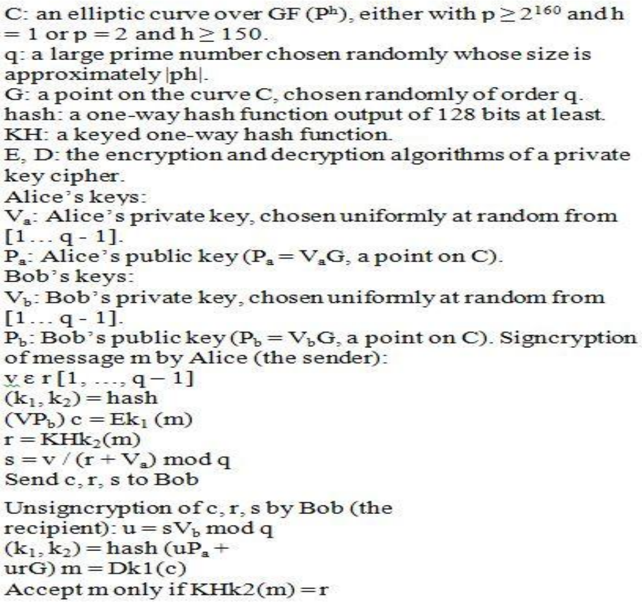
A. Zheng-Imai Elliptic Curve Signcryption Scheme

The Two most well-known schemes are ECSCS1 and ECSCS2 dependent on elliptic curved are purposed by Zheng – Imai[]. We are examining just ECSCS1. The case is similar for the other ECSCS2.


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, and s) to Bob.

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

Public Parameters:

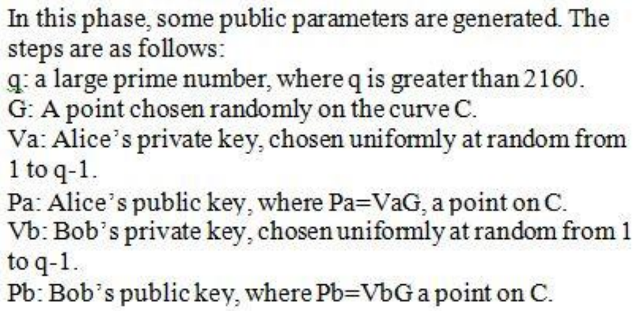

C: an elliptic curve over GF (P^h), either with $p \geq 2^{160}$ and h = 1 or p = 2 and h ≥ 150.
q: a large prime number chosen randomly whose size is approximately |ph|.
G: a point on the curve C, chosen randomly of order q.
hash: a one-way hash function output of 128 bits at least.
KH: a keyed one-way 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) mod q
Send c, r, s to Bob

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

PROPOSED SCHEME

We have purposed a new scheme based on elliptic curve cryptosystem. 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 asfollows.

Initializationphase:



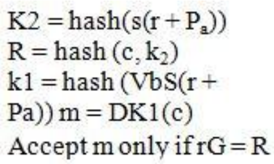
In this phase, some public parameters are generated. The steps are as follows:
q: a large prime number, where q is greater than 2160.
G: A point chosen randomly on the curve C.
Va: Alice's private key, chosen uniformly at random from 1 to q-1.
Pa: Alice's public key, where Pa=VaG, a point on C.
Vb: Bob's 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 want to send a message m to Bob. Alice generate 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:

Unsigncryption of c, r, s by Bob:

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

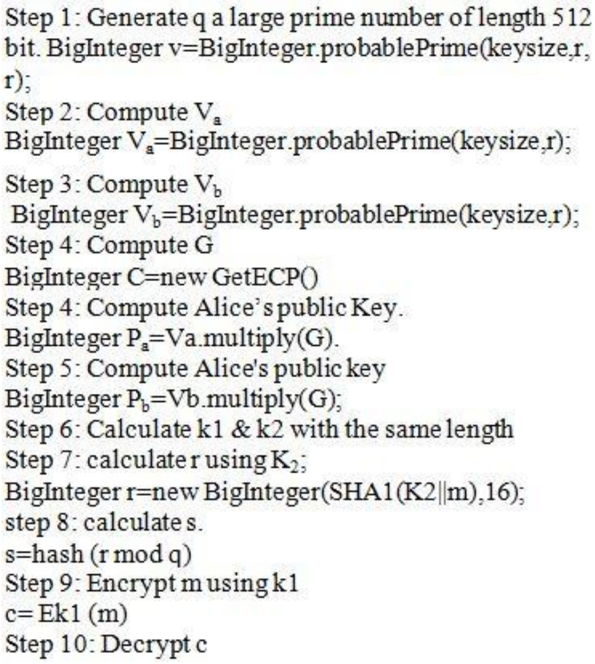


$K2 = hash(s(r + P_a))$
$R = hash\ (c, k_2)$
k1 = hash (VbS(r +
Pa)) m = DK1(c)
Accept m only if rG = R

III. IMPLEMENTATION IN JAVA

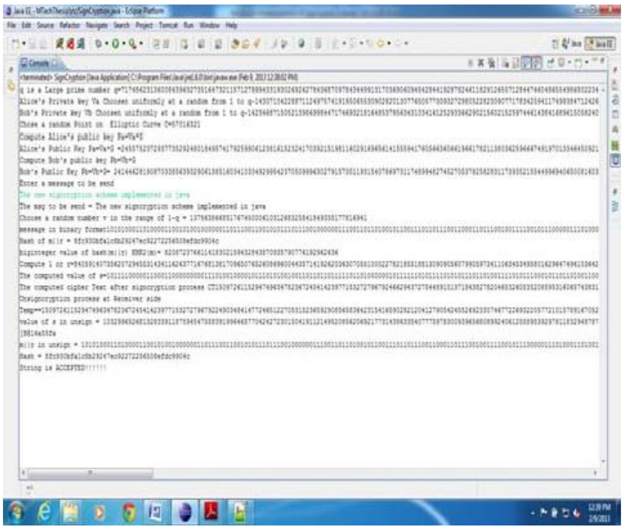
We have executed the purposed plan on java that confirms our convention. We have incorporated the security bundle to control cryptographic functions.

Steps to initialize public Parameters:



```
Step 1: Generate q a large prime number of length 512 bit. BigInteger v=BigInteger.probablePrime(keysize,r, 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: Compute 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.



Java EE - MTechThesis/src/SignCryption.java - Eclipse Platform
File Edit Source Refactor Navigate Search Project Tomcat Run Window Help
Console

```
<terminated> SignCryption [Java Application] C:\Program Files\Java\jre6.0\bin\javaw.exe (Feb 9, 2013 12:38:02 PM)
q is a Large prime number q=[illegible]
Alice's Private key Va Choosen uniformly at a random from 1 to q-[illegible]
Bob's Private key Vb Choosen uniformly at a random from 1 to q-[illegible]
Chose a random Point on  Elliptic Curve G=67016321
Compute Alice's public key Pa=Va*G
Alice's Public Key Pa=Va*G =[illegible]
Compute Bob's public key Pb=Vb*G
Bob's Public Key Pb=Vb*G= [illegible]
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 = [illegible]
message in binary format[illegible]
Hash of m||r = [illegible]
biginteger value of hash(m||r) KHK2(m)= [illegible]
Compute 1 or r=[illegible]
The computed value of s=[illegible]
The computed cipher Text after signcryption process CT[illegible]
Unsigncryption process at Receiver side
Temp==[illegible]
value of s in unsign = [illegible]
[B@14a55fa
m||r in unsign = [illegible]
Hash = [illegible]
String is ACCEPTED!!!!!!
```

Fig-3: output of the executed scheme

IV. ANALYASIS

A. Security

The signcryption conspire satisfies every one of the properties of security. It's additionally following the procedure of encryption and computerized signature yet in one stage. The security characteristics like Confidentiality, Unforgeability, Integrity, and non-revocation. Some signcryption plans give further qualities, for example, Public undeniable nature and Forward mystery of message classification. Such properties are the qualities that are required in numerous applications while others may not require them.

Confidentiality: It should be computationally infeasible for a versatile aggressor to increase any incomplete data on the substance of a signcrypted content, without learning of the sender's or assigned beneficiary's private key.

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

Non-repudiation: The beneficiary ought to be able to demonstrate to an outsider (for example a judge) that the sender has sent the signcrypted content. This guarantees the sender can't deny his already signcrypted writings.

Integrity: The beneficiary ought to have the capacity to confirm that the got message is the first one that was sent by the sender.

Public Verifiability: Any third party without any need for the private key of sender or recipient can verify that the signcrypted text is the valid signcryption of its corresponding message.

Forward Secrecy of message confidentiality: On the off chance that the long haul private key of the sender is undermined, nobody ought to have the capacity to haul out the plaintext of already signcrypted writings. In a customary signcryption conspire, when the long haul private key is undermined, all the beforehand issued marks won't be dependable any more. Since the danger of key presentation is winding up progressively intense as the cryptographic calculations are performed all the more much of the time on ineffectively secured gadgets, for example, cell phones, the forward mystery appears a fundamental quality in such frameworks.

TABLE: SHOWS 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].

	Confidentiality	Integrity	Unforgeability	Forward Security	Pub. verification
Zheng	Yes	Yes	Yes	No	No
Zheng and Imai	Yes	Yes	Yes	No	No
Bao& Deng	Yes	Yes	Yes	No	Yes
Gamage et al	Yes	Yes	Yes	No	Yes
Jung et al.	Yes	Yes	Yes	Yes	No
Han et al.	No	No	No	No	Yes
Hwang et al.	No	No	No	No	Yes
Proposed scheme	Yes	Yes	Yes	Yes	Yes

B. *Complexity of ProposedScheme*

The proposed signcryption scheme depends on elliptic bend time required for elliptic curve point increase has a significant effect in computational expense.

Schemes	Participant	ECPM	ECPA	Mod. Mul	Mod. Add	Hash
Zheng & Imai	Alice Bob	1 2	- 1	1 2	1 -	2 2
Han et al	Alice Bob	2 3	- 1	2 2	1 -	2 2
Hwang et al	Alice Bob	2 3	- 1	1 -	1 -	1 1
Proposed scheme	Alice Bob	2 3	1 -	- 1	- 1	2 2

TABLE II: COMPARISON OF SCHEMES ON BASIS OF COMPUTATIONAL COMPLEXITY.

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 III: 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 ININFINEON’S SLE66CU* 640P SECURITY CONTROLLER.[15].

CONCLUSION

In this paper, we dispatch another signcryption conspire dependent on elliptic bend which satisfies all properties of security objective like message confirmation, honesty, open check, unforgeability and non-disavowal. In the event that the sender reveals the private key nobody can extricate the first message. It additionally gives confirmation process by outsider to think about the sender. This signcryption conspire spares computational expense and correspondence overhead than the conventional mark then encryption plot. The plan is executed utilizing java which create key by picking an arbitrary point on the elliptic bend which makes increasingly secure. The executed plan can be valuable for online business condition. The point duplication of elliptic bend is less time whereas exponential point augmentation is all the more so it likewise decreases computational time. Open unquestionable status is particularly valuable in web based business situations as it empowers the exchanging accomplices to determine debate through any trusted or untrusted judge without connecting with the judge in a zero-learning verification correspondence and without uncover of any mystery data.

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 AsgharBeheshtiShirazi. 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 AsgharBeheshtiShirazi. An elliptic curve- based signcryption scheme with forward secrecy. Journal of Applied Sciences, 9(6):1025 -1035,2009.

[13] Mohsen Toorani and Ali AsgharBeheshtiShirazi. Cryptanalysis of an elliptic curve-based signcryption scheme. International journal of network security vol.10, pp51-56,2010.

[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 PrasantSahoo, cryptanalisys of signcryption protocols based on elliptic curve. IJMER,Vol.3, Issue-1, pp 89-92, 2013.