# A Novel Signcryption Scheme Based on ECC with Public Verification and Encrypted Message Authentication

[I]Sumanjit Das, [II]Santosh Kumar Sahu, [III]Santosh Narayan Pati
[I]Asst.Professor, CSE, Centurion University
[II]M.Tech Scholar BPUT
[III]Lecturer SIT, BPUT

## Abstract

*Data exchange is more essential to achieve the different tasks. 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. 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 fulfil the user requirements without any damage. There are various cryptographic techniques be present which offers security to the messages. Traditional Signature-then-encryption technique be 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" in 1997 announced 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. A number of signcryption schemes are previously announced by many researchers Nonetheless each scheme has their own restriction. This thesis grounded on elliptic curve cryptography (ECC) implemented in java, not only offers the 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.*

## Keywords

*Elliptic curve cryptography, signcryption, digital signature, encryption, ecc, cryptography*

## I. Introduction

Modern cryptosystem provides the means for data security for information while transmitting it over an insecure channel. When a data is transmitted over an insecure channel we must provide integrity, confidentiality, authenticity and non-repudiation [7].

In older days to enabling secure communications between a sender and one or more recipients the sender scrambling a message (with a computer program and a secret key) and leaving the recipient to unscramble the message (with the same computer program and a key, which may or may not be the same as the sender's key). We have a number of encryption algorithms those can be broadly classified into two categories: Secret/Symmetric Key Cryptography and Public Key Cryptography. The difference between these two is that to communicate with n people private key cryptography requires $(n \times (n-1))/2$ number of keys whereas; public key cryptography requires only n number of key pairs (one private and one public key).

The conventional method for sending a message from sender to receiver in a secure manner is called Symmetric key cryptography System. This is also called as secret key cryptography. Symmetric key cryptography is based on sharing of secret key between two users for sending a message in an encrypted format from sender to recipient .The disadvantages of this system is that the sender and the recipient must trust some communication channel to transmit the secret key to prevent from exposé.

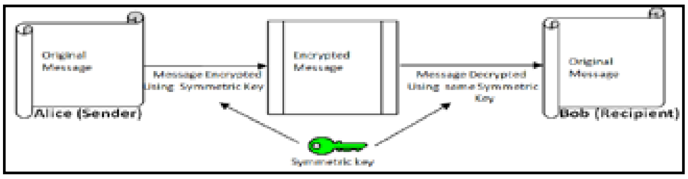

Figure 1: Symmetric Key Encryption.

To overcome the demerits of Symmetric key Cryptosystem public key cryptography discovered nearly two decade ago and has revolutionized to transfer a message in a secure and authenticated way. Public key cryptography was introduced in 1976 by Whitfield Diffie and Martin Hellman [19] .The public key cryptography system based on pairs of keys called public key and private key. The public key is published while the private key is kept secret with the sender. This is also called as asymmetric cryptography and two different keys are used by the sender and recipient. The public key algorithms relay on one key (secret key/private key) for encryption but related key (public key) is used for decryption. It has important characteristics i.e. it is infeasible to determine the decryption key given only knowledge of the cryptographic algorithm and the encryption key.

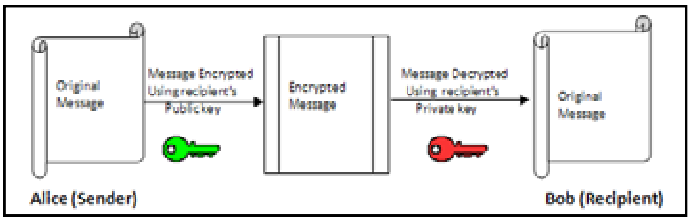
Original Message
Message Encrypted Using recipient's Public key
Encrypted Message
Message Decrypted Using recipient's Private key
Original Message
Alice (Sender)
Bob (Recipient)

Fig. 2: Public key Encryption.

In Modern Era to solve the above two problems a new cryptographic technique is used called signcryption. Signcryption simultaneously fulfill the both the functionality of digital signature and encryption is a single logical step, but with a cost smaller than required by traditional method called Sign-then-Encryption [1,2,3].The first Signcryption was purposed by Zheng in 1997 [1]. It achieves most of the security goals of cryptosystem but it fails the forward secrecy of message confidentiality. 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 [3]. They are many signcryption schemes having their own advantages and demerits most of them include confidentiality, unforgeability, Integrity and Non repudiation. Some of them provide further attributes such as public auditability and Forward secrecy while others do not provide those [7]. Now a day the important of signcryption has gained in data security and the committee within the International Organization for Standardization (ISO/ IEC JTC 1/SC 27) has been developing an international standard for signcryption technique [8].

In this paper we 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. We have implemented the above protocol using java Language and then compare our scheme with Zheng's signcryption.

## II. Mathmetical Background

### A. Elliptic Curves Over Real Numbers

An elliptic curve over real numbers may be defined as the set of points (x,y) which satisfy an elliptic curve equation of the form: y2 = x3 + ax + b,

Where x, y, a and b are real numbers.

Each choice of the numbers a and b yields a different elliptic curve. For example, a = -4 and b = 0.67 gives the elliptic curve with equation y2 = x3 - 4x + 0.67; the graph of this curve is shown below:

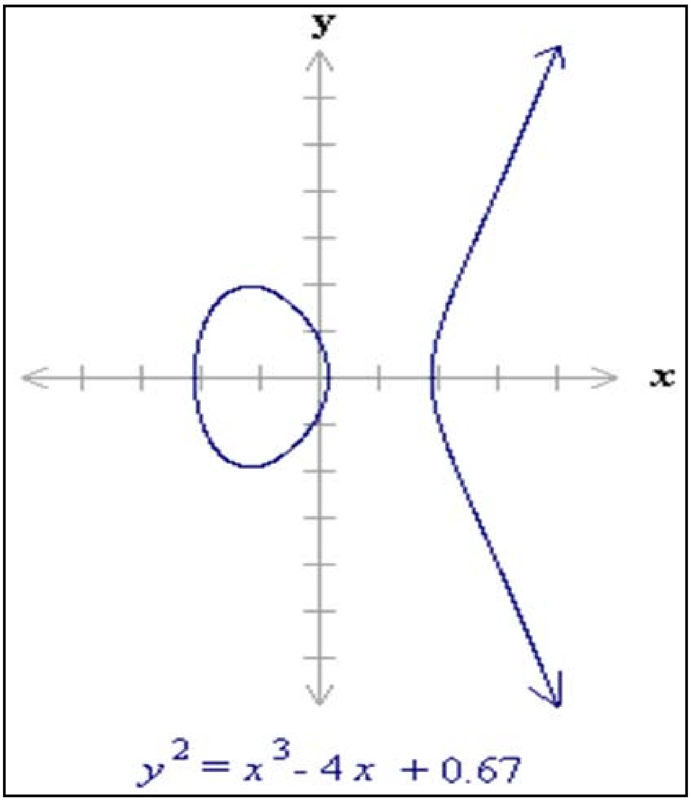

Fig. 2.2 : An Elliptic Curve over real numbers

If x3 + ax + b contains no repeated factors, or equivalently if 4a3 + 27b2 is not 0, then the elliptic curve y2 = x3 + ax + b can be used to form a group. An elliptic curve group over real numbers consists of the points on the corresponding elliptic curve, together with a special point O called the point at infinity.

### Adding distinct points P and Q

The negative of the point P = ($x_P$, $y_P$) is the point -P = ($x_P$, -$y_P$ mod p). If P and Q are distinct points such that P is not -Q, then P + Q = R where

s = ($y_P$ - $y_Q$) / ($x_P$ - $x_Q$) mod p

$x_R$ = $s^2$ - $x_P$ - $x_Q$ mod p and $y_R$ = -$y_P$ + s($x_P$ - $x_R$) mod p

Note that s is the slope of the line through P and Q.

### B. Doubling the Point P

Provided that yP is not 0,

2P = R where

s = (3xP2 + a) / (2yP ) mod p

xR = s2 - 2xP mod p and yR = -yP + s(xP - xR) mod p

### C. Elliptic Curve Over F (2m)

Recall that is one of the parameters chosen with the elliptic curve and that s is the slope of the line through P and Q.

An elliptic curve with the underlying field F($2^m$) is formed by choosing the elements a and b within F($2^m$) (the only condition is that b is not 0). As a result of the field F($2^m$) having a characteristic 2, the elliptic curve equation is slightly adjusted for binary representation: y2 + xy = x3 + ax2 + b Elliptic curve groups over F($2^m$) have a finite number of points, and their arithmetic involves no round off error. This combined with the binary nature of the field, F($2^m$) arithmetic can be performed very efficiently by a computer. The following algebraic rules are applied for arithmetic over F2$^m$).

## III. Related Work

The history of cryptography defines the level of developments on it. But it's not for the use of common purpose. Now a days it developed in many terms like signcryption which is the most authentic one in the world of security. Many researchers given their proposal for signcryption based on modular exponential and some are based on elliptic curves.

The first Signcryption cryptography technique was proposed in 1997 by Yuliang Zheng[1]. To get the authenticity and confidentiality features of cryptography he combines the features of digital signature and encryption algorithm. In his signcryption scheme, the 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. This scheme was based on discrete logarithm problem.

Another surprising property of the proposed signcryption schemes is that it enables us to carry out fast, secure, unforgeable and non-repudiatable key transport in a single block whose size is smaller than |p|. In particular, using either of the two signcryption schemes, we can transport highly secure and authenticated keys in a single ATM cell (48 byte payload + 5 byte header).

In the full paper he had shown how to adapt a signcryption scheme into one for broadcast communication which involves multiple recipients. Unlike signature-then–encryption, the verifiability of a signcryption is in normal situation limited to Bob, the recipient as his secret key is required for unsigncryption. At the first sight, the limited verifiability of a signcryption, namely the direct verifiability by the sender only (and indirect verifiability by a judge with the cooperation of Bob), may be seen as a drawback of signcryption. Here he had strongly argue that the limited direct verifiability will not pose any problem in practice and hence should not be an obstacle to practical applications of signcryption.His scheme need only a total of 3 computational computations,one for signcrypting and two for unsigncrypting.At last he had written in the conclusion of his paper that “We have not been successful in searching for signcryption scheme employing RSA or other public key cryptosystem.Therefore it remains a challenging open problem to design signcryption schemes based on factorization and other computationally hard problems.So it is clear that Zheng scheme satisfies the security properties of Unforgeability, Non-Repudiation and Confidentiality but it lacks forward Secrecy and a Strong verification technique that is without using the private key of Bob.

Jung et al. [21] analysis showed that Zheng’s [1] scheme does not provide forward secrecy property. Message confidentiality is lost when the sender’s private key disclosed. He also introduced a new signcryption scheme based on discrete logarithm problem with forward secrecy. In his note he had modified Zheng’s Scheme so that the receipient’s private key is no longer needed in signature verification.However the computational cost is higher than that of the Zheng’s Scheme but lower than that of the signature-then-encryption Scheme. He had given a modified version of Zheng’s signcryption Scheme based on the Elgamal type of public key cryptosystem.

It overcomes the problem of Zheng’s signcryption scheme of not being suitable for applications where a signature need to be validated by a third party only using the public key as in usual signature scheme by introducing an independent judge. That is done by proving the equality of discrete logarithms. However confidentiality is lost in this case. Bao and Deng scheme requires a total of 5 exponential computations instead of 6 as in the traditional signature-then-encryption method. Also it achieves the same effect as in signature-then-encryption. That is sender sends (c,r,s) and after receiving (c,r,s),Bob first obtains the plaintext message m using his private key. Now Bob has Alice’s signature (m,r,s).This signature can be verified by anyone using only Alice’s public key.

This scheme was based on DLP. 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. Proposed another signcryption scheme based on the elliptic curve discrete logarithm problem (ECDLP) over finite fields that achieved similar functionality[2]. There analysis shows that the scheme saves 58% computational cost and saving about 40% communication cost than the traditional signature-then-encryption scheme[2] .Both the schemes lacked forward secrecy, public verifiability and encrypted message authentication. The elliptic curve DSS called as ECDSS has been described in this paper along with its two shortened version known as SECDSS1 and SECDSS2.Also it takes into account a bind_info part in the computation of r which may contain the public keys and public key certificates of both Alice the sender and Bob the receiver.

Hwang,Lai and Fu-Su[4] An efficient signcryption scheme based on elliptic curve has been proposed in this paper. The signcryption scheme combines digital signature and encryption functions. The proposed scheme takes lower computation and communication cost to provide security functions. It not only provides message confidentiality, authentication, integrity, unforgeability, and non-repudiation, but also forward secrecy for message confidentiality and public verification. In the proposed scheme, the judge can verify sender’s signature directly without the sender’s private key when dispute occurs. His scheme can be applied to mobile communication environment more efficiently because of the low computation and communication cost. Moreover the secret key of the proposed scheme is only related to recipient’s private key. It protects the confidentiality of message even if the private key of the sender disclosed. It is the forward secrecy function that is provided by his signcryption scheme. In addition, the proposed scheme provides publicly verifiable function. By the publicly verifiable function, the judge can verify sender’s signature directly without the sender’s private key when dispute occurs.The proposed scheme spends lower time in computation, especially for sender. It contains four phases: initialization phase, signcryption phase, unsigncryption phase and judge verification phase. In the initialization phase, system generates and publishes domain parameters of elliptic curve, and each user generates his own private key and the related public key. Each user should get the certification of his public key from the certificate authority (CA). In signcryption phase, the sender Alice signs and encrypts a message. Then she sends the signcrypted text to the recipient Bob. In the unsigncryption phase, the recipient Bob derives secret key to decrypt plain text. He also verifies the signature. In the judge verification phase, a judge decides whether the sender Alice sent the signcrypted message or not, when dispute occurs.

The proposed scheme provides seven security functions: message confidentiality, authentication, integrity, unforgeability, non-repudiation, forward secrecy of message confidentiality and public verification. Most of its results were based on two problems: the elliptic curve discrete logarithm problem (ECDLP) and the elliptic curve Diffie–Hellman problem (ECDHP). Though this scheme provides forward secrecy, message confidentiality and public verification still it has a lower performance than Zheng’s scheme.

Gamage,Leiwo and Zheng[5] Gamage, Leiwo and Zheng proposed a scheme based on DLP that enabled firewalls to authenticate encrypted messages without having to decrypt them i.e without disclosing the message. He had shown that with a small change to the original signcryption scheme it is possible to modify the Bao-Deng scheme to carry out signature verification without accessing the plain text. There is a single Prover and a single Verifier in this scheme.The advantage of this new mode of operation for signcryption is the cipher text only signature verification that preserves confidentiality of the original message without altering sign-then-encrypt paradigm. The computational cost is higher than in original scheme of Zheng [1] but lower than Bao-Deng modified scheme and thus standard sign-then-encrypt schemes. The transmission cost saving of the original signcryption scheme is preserved.

## IV. Observation

So finally it has been observed that out of all signcryption schemes stated above the signcryption scheme given by Zheng and Imai [2] supports all the four major security goals, discussed in the introduction Chapter, takes a considerable amount of computational and communication overhead. But it does not support forward secrecy, public verifiability and encrypted message authentication. So our objective is to propose a new scheme such that it will take a comparable computational and communication cost and should provide forward secrecy, public verifiability and encrypted message authentication.

## V. The Proposed Scheme

### A. The proposed signcryption scheme with public verification and forward secrecy

The proposed signcryption scheme was based on elliptic curve cryptosystem. In this thesis the scheme provides all the basic features of security functions such as message integrity, message confidentiality, non-repudiation, sender's authenticity, encrypted message authenticity, forward secrecy and public verification, with a cost less than or comparable with the existing schemes.

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 as follows.

### B. Algorithm for Proposed Scheme:

The proposed scheme consists of three phases like Initialization, Signcryption, and Unsigncryption.

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 want to send a message m to Bob. 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 + Pa))
R = hash (c, k2)
k1 = hash(VbS(r + Pa))
m = DK1(c)
Accept m only if rG = R

### C. Analysis of the Proposed Scheme

The implementation protocol is executed at a random by taking messages of different length. The above table shows the message length in terms of number of characters and time taken by signcryption phase to encrypt the plain text into cipher text as well as the time taken by unsigncryption phase to decrypt the cipher text back into plain text.

Table 1: Analysis of the purposed scheme based on Time

The message of different length i.e. from 4 characters to 1000 characters has been taken at different instance. Also the signcryption time and unsigncryption time has been also noted down. From the above it is clear that when the message length is increasing approximately by 2 times , at the same time there is slightly change (nearly same) in the signcryption time as well as unsigncryption time. Also a graph has been plotted showing out signcryption and unsigncryption time as below.

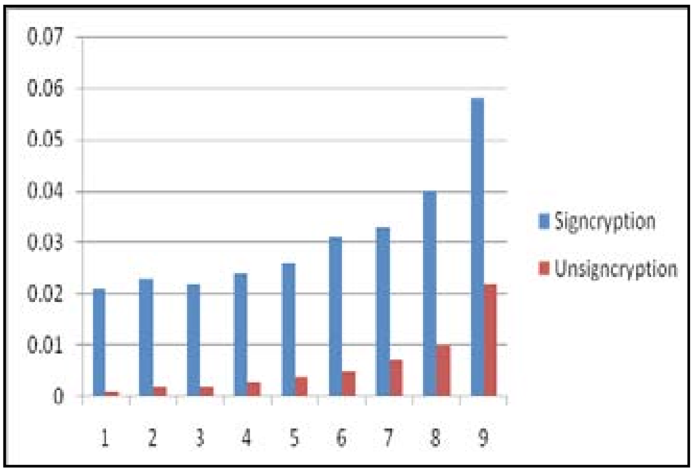

Fig. 3: Proposed Signcryption Time Versus Unsigncryption Time

### D. Comparative Analysis of the proposed scheme versus different scheme based on time

Table 2: comparative analysis of RSA based Sign then Encryption versus purposed signcryption time.

| (number of character) | RSA based Sign then Encryption | 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 |

It has been shown a comparative analysis between the time required for RSA based Sign then Encryption and the purposed scheme. From the comparison it is clear that the the signcryption time of the purposed scheme only half of the time required by RSA based Sign then Encryption time. We have shown the actual computation for RSA based Sign then Encryption scheme as well as the proposed protocol by implementing the scheme using java.

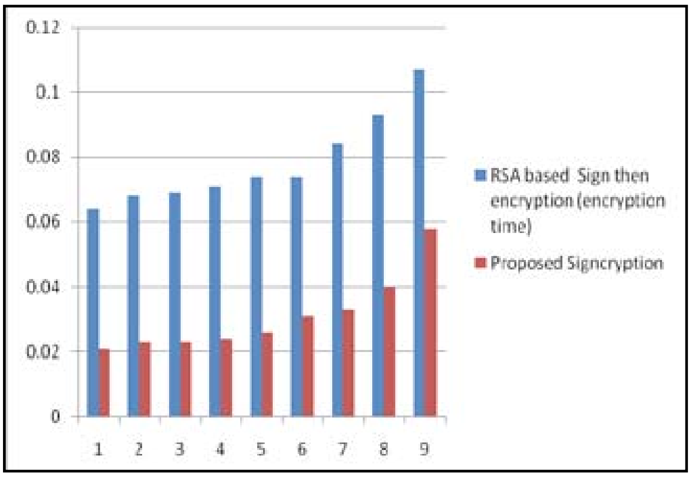

Figure 4: Comparison of RSA based Sign then Encryption scheme versus proposed scheme based on signcryption time.

Table 3: comparative analysis of RSA based Sign then Encryption (decryption) time versus purposed unsigncryption time.

| message Length (number of character) | of RSA based Sign then Encryption (decryption) | Proposed Unsigncryption |
|---|---|---|
| 4 | 0.039 | 0.001 |
| 8 | 0.041 | 0.002 |
| 16 | 0.042 | 0.002 |
| 32 | 0.042 | 0.003 |
| 80 | 0.043 | 0.004 |
| 160 | 0.043 | 0.005 |
| 300 | 0.044 | 0.007 |
| 500 | 0.045 | 0.01 |
| 1000 | 0.058 | 0.022 |

Similarly we have also taken a comparison study between the decryption phase of RSA based Sign then Encryption (decryption) scheme and our protocol. We have taken same messages lengths that are used for signcryption. The purposed scheme shows that the time required for unsigncryption comparatively very less as that of RSA based Sign then Encryption (decryption) scheme which shows that the purposed protocol is more efficient in computation. This is shown clearly from the below graph.

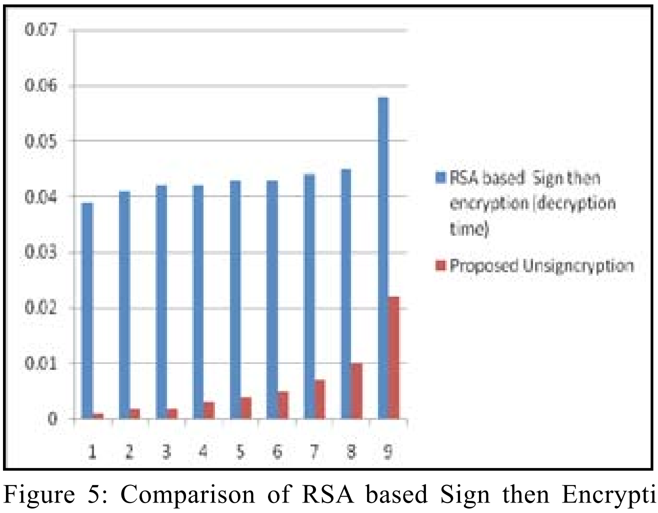

Figure 5: Comparison of RSA based Sign then Encryption (decryption) time versus proposed scheme based on unsigncryption time.

**Comparative analyasis of different scheme**

In our purposed scheme we try to reduce signcryption time. A comparison of the proposed scheme with different signcryption scheme based on ECPM i.e number of elliptic curve point multiplication operation has been shown in table The purposed scheme takes only 2 ECPM operations for signcryption and 3 ECPM for unsigncryption. The elliptic curve point multiplication needs 83ms and modular exponentiation operation needs 220 ms for average computational time in the Infineon's SLE66CUX460P security controller [4].

Table 4: comparison based on average computational time of different signcryption scheme

| Signcryption schemes | Avarage Signcryption Time(ms) | Avarage Unsigncryption Time(ms) |
|---|---|---|
| Zheng | 220 | 440 |
| Zheng & Imai | 83 | 166 |
| Bao & Deng | 440 | 660 |
| Gamage et al | 440 | 660 |
| Jung et al | 440 | 660 |
| M Toorani & A.A Beheshti | 166 | 332 |
| Proposed scheme | 249 | 166 |

**E. Security properties of proposed scheme:**

**Unforgeability:**

It is computationally infeasible to forge a valid signcrypted text (c, R, s) and claim that it is coming from Alice without having Alice's private key va.

**Non-repudiation:**

If the sender Alice denies that she sent the signcrypted text (c, R, s), any third party can run the verification procedure above to check that the message came from Alice.

**Public verifiability:**

Verification requires knowing only Alice's public key. All public keys are assumed to be available to all system users through a certification authority or published directly. The receiver of the message does not need to engage in a zero-knowledge proof communication with a judge or to provide a proof.

**Confidentiality:**

Confidentiality is achieved by encryption. To decrypt the cipher text, an adversary needs to have Bob's private key (vb).

**Forward secrecy:**

An adversary that obtains va will not be able to decrypt past messages. Previously recorded values of (c, R, s) that were obtained before the compromise cannot be decrypted because the adversary that has va will need to calculate r to decrypt. Calculating r requires solving the ECDLP on R, which is a computationally difficult.

**Encrypted message authentication:**

The proposed scheme enables a third party to check the authenticity of the signcrypted text (c, R, s) without having to reveal the plaintext m to the third party. This property enables firewalls on computer networks to filter traffic and forward encrypted messages coming from certain senders without decrypting the message. This provides speed to the filtering process as the firewalls do not need to do full unsigncryption to authenticate senders. It also provides additional confidentiality in settling disputes by allowing any trusted/untrusted judge to verify messages without revealing the sent message m to the judge.

## VI. Conclusion

The Zheng signcryption scheme set out to achieve greater efficiency by combining encryption and signature schemes; the focus has subsequently shifted to other issues, such as security and non-repudiation. The issue of security is of key importance, since it has implications for all systems which use encryption and signatures together.

This paper introduces elliptic curve based signcryption schemes for secure and authenticated message delivery, which fulfils all the functions of digital signature and encryption with a cost less than that required by the current standard signature-then-encryption method. The Zheng and Imai scheme is the most efficient signcryption scheme based on ECC. But the drawback of the above scheme is that it does not provide forward secrecy. So it is necessary to provide forward secrecy.

There are few schemes which can provide forward secrecy but the computational cost and communication overhead is more. The cost of the proposed schemes are comparatively lower than other schemes in terms of computational and communication overhead. ECC has been used for the implementation of our algorithm because of its unique property of ECDLP which is significantly more difficult than either the IFP or DLP. Proposed schemes save more computational cost for the sender to suit the application of limited computing power like smart card based applications, mobile devices, etc.

Koblitz suggested to use the generalization of Elliptic Curves (EC) for cryptography, the so-called Hyperelliptic Curves (HEC) [17]. While ECC applications are highly developed in practice, the use of HEC is still of pure academic interest. However, one advantage of HECC [17] resides on the fact that the operand size for HECC is at least a factor of two smaller than the one of ECC. More precisely, while typical bit-lengths for ECC are at least 160 bits, for HECC this lower bound is around 80 bits (in the case of genus 2 curves). This fact makes HECC a very good choice for platforms with limited resources. Now we should look forward to develop schemes based on HECC which is an open challenge for us.

## 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.*

[2] *Y. Zheng, H. Imai, "How to construct efficient signcryption schemes on elliptic curves",*

*In Information Processing Letters 68.pages 227-223,Melbourne,Australia,1998.*

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

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

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

[6] *Mohsen Toorani and Ali Asghar Beheshti Shirazi , "An elliptic curve-based signcryption scheme with forward secrecy". Journal of Applied Sciences, pages 1025 -1035, 2009.*

[7] *Mohsen Toorani and Ali Asghar Beheshti Shirazi, "Cryptanalysis of an elliptic curve-based signcryption scheme". International journal of network security volume10, pages 51-56, 2010.*

[8] *International Organization for Standardization, "IT Security Techniques—Signcryption," ISO/IEC WD 29150, 2008.*

[9] *Elsayed Mohamed and Hassan Elkamchouchi, "Elliptic Curve Signcryption with Encrypted Message Authentication and Forward Secrecy" IJCSNS International Journal of Computer Science and Network Security, Volume 9, January 2009.*

[10] *Wang Yang and Zhang, " Provable secure generalized signcryption". Journal of computers, Volume 5, pages 807-814, 2010.*

[11] *Laura Savu, "Combining Public Key Encryption with Schnorr Digital Signature" Journal of Software Engineering and Applications, 2012, Volume 5, pages 102-108.*

[12] *Sumanjit Das, Prasant Kumar Sahoo , "Cryptanalysis of Signcryption protocol based on Elliptic Curve", International Journal of Modern Engineering Research (IJMER) Volume 3, Issue.1, ISSN: 2249-6645 , pages 89-92,Jan-Feb 2013*

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

[14] *William Stallings, " Cryptography and Network security: Principles and Practices". Prentice Hall Inc., second edition, 1999.*

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

[16] *Anjali Jain ,Ramratan Ahirwal & Y. K. Jain, Signcryption Scheme that Utilizes Elliptic Curve for both Encryption and Signature Generation International Journal of Computer Applications , Volume 62,No.9, pages 975-8887,January 2013.*

### *Author's Profile*

*Sumanjit Das presently working as Asst. Professor in the department of Computer Science and Engineering, Centurion University of Technology and Management, Bhubaneswar. The author is having 9 international publications, 02 numbers of national seminar presentations and attended many national workshops in different fields of computer science.*

*Santosh Kumar Sahu, M.tech scholar at TITE, Bput working in the above area of research for his M.Tech thesis. Presently he is working as lecturer in Arya School of Management and Technology, Bhubaneswar.*

*Santosh Narayan Pati working as Lecturer in the department of computer science and engineering in SIT, BPUT, Bhubaneswar.*