Signcryption Scheme that Utilizes Elliptic Curve for both Encryption and Signature Generation

Ramratan Ahirwal
Assistant Professor
Department of C.S.E.
Samrat Ashok Technological Institute Vidisha (M.P.)

Anjali Jain
M.Tech Scholar
Department of C.S.E.
Samrat Ashok Technological Institute Vidisha (M.P.)

Y. K. Jain, PhD.
Head of Department
Department of C.S.E.
Samrat Ashok Technological Institute Vidisha (M.P.)

ABSTRACT

Signcryption is a relatively new technique in public key cryptography, that perform both the functions of digital signature and encryption in a single step ,in a way that is more efficient than signing and encrypting separately. Signcryption scheme can achieve authentication and encryption simultaneously, it successfully prevents mutual cheating in message transmission. In this paper a Signcryption scheme is suggested which is based on Elliptic Curve Cryptography (ECC). Main benefit of the proposed scheme is that it uses only elliptic curve for both encryption and signature generation. Message transmission is in the form of a point P(m) embedded in Elliptic Curve and encrypted by point addition which is efficient and safe. In this paper a new signature generation technique has been introduced that requires less time as compared to signature generated by hashing scheme. The signature can be verified without decryption of the message thus, provides encrypted message authentication, and hence reduces the algorithm complexity. The aim of this paper is to specify signcryption schemes on elliptic curves over finite fields, and to examine the efficiency of such schemes. Signcryption scheme based on elliptic curves represents a remarkable saving in computational cost and in communication overhead.

Keywords

Cryptography, Digital signature, Elliptic curves, Encryption, Public key cryptography, Signcryption.

1. INTRODUCTION

In cryptography, signcryption scheme is a public-key primitive that concurrently perform the functions of both digital signature and encryption.

Encryption and digital signature are two basic cryptographic tools that can guarantee the confidentiality, integrity, and non-repudiation. Until the previous decade, they have been viewed as important but separate building blocks of various cryptographic systems. In public key schemes, a traditional method is digitally signing a message then followed by an encryption (signature-then-encryption approach) that can have two problems: Lower efficiency and high cost of such summation, and the case that any arbitrary scheme cannot assurance the security. Signature generation and encryption consume more machine cycles, and also produces "expanded" bits to an original message. Computational time generally required for signature verification and decryption is more because two distinct operations have to be performed. Hence the cost of a cryptographic operation on a message is usually measured in the form of message expansion rate and the computational time invested by both the sender and the receiver. With the current standard signature then encryption approach, approximate cost of delivering a message in a safe and authenticated way is essentially the sum of the cost for digital signature and that for encryption. As realized both by practitioners and theorists in data security, for traditional sign-then-encryption, cryptanalytic attacks have been increasing at a significant speed in recent times, and increasingly large problem in security applications where efficiency both in terms of computational time and communication overhead is a critical issue. Such applications include those based on smart cards which generally employ only less powerful CPUs than do their counterparts in desk-top or notebook computers. To solve the above problem, in [1] a new paradigm in public key cryptography, called signcryption, has been proposed.

A signcryption scheme is a cryptographic method that performs two distinct operations (signature and encryption) simultaneously, at a cost smaller than required by signature-then-encryption method. This means that at least some features of its efficiency (for example the computation time) is better than any hybrid of digital signature and encryption schemes, under a particular model of security.

More recently, the importance of signcryption in real- world applications has gained appreciation by experts in data security. Since 2007, a technical committee within the International Organization for Standardization (ISO/IEC JTC 1/SC 27) has been developing an international standard for signcryption techniques [17].

Literature Review

Various signcryption schemes [1-7] are introduced throughout the years, each of the scheme having its own benefits and drawbacks, while offering different level of security services and computational costs. The first signcryption scheme was introduced by Yuliang Zheng.

Zheng [1] presented a new cryptography technique named ''Signcryption'' which combines the functions of both digital signature and encryption algorithm for authentication and confidentiality. In the signcryption scheme, introduced by Zheng the sender uses the receiver's public key to derive a secret key for symmetric encryption. After the receiver receives the cipher text and digital signature, he uses his private key to derive the same secret key.

Zheng [2] introduced another signcryption scheme that is based on elliptic curve, which saves about 58% computational cost and saving about 40% communication cost than signature-then-encryption scheme based on elliptic curve.

Jung et al. [3] 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.

Bao and Deng [4] enhanced Zheng's [1] signcryption scheme, so that the judge can verify the authenticity of signature without the need of recipient's private key.

Gamage et al. [5] modified Zheng's [1] signcryption scheme such that anyone can verify the signature of cipher text. Their scheme is capable of verifying signature without disclosing the content of the original message.

Zhang, Ji, and Wang proposed the first protocol for threshold generation of Zheng's signcryption scheme in 2002 [10]. In this scheme, only specific recipient can verify the signature.

Gan, Li, and Chen proposed a publicly verifiable threshold signcryption method[11] which is based on DLP (Discrete Logarithm Problem) .

Mohsen Toorani and Ali Asghar Beheshti Shirazi proposed an Elliptic Curve-based Signcryption Scheme with additional Forward Secrecy property.[14].

Elsayed Mohamed and Hassan Elkamchouchi proposed Elliptic Curve based Signcryption scheme that provides Encrypted Message Authentication and Forward Secrecy [15] that is needed by firewalls. Firewalls can securely filter the signcrypted messages through them without performing full unsigncryption to verify the sender's identity.

Laura Savu [16] this paper describes a new signcryption method which is based on the Schnorr digital signature algorithm and also various signcryption scheme that already exist.

In this paper, a new signcryption scheme based on elliptic curve is proposed. Elliptic curve cryptography (ECC) has been implemented as our basic algorithm to provide signcryption. In this signcryption scheme, only elliptic curve is used for encryption and signature generation purpose. For signature calculation new and easy technique (Mean, Variance, and Centre of gravity (c.g)) have been used that require less time than signature generated by hashing scheme. The specific receiver can verify the validity of the signature before decrypting the cipher. Our scheme saves great amount of computational cost especially for receiver. Reason behind using ecc is, currently, the elliptic curve cryptography is being used in a wide variety of applications. The elliptic curve based cryptosystem (ECC) [18, 19] can attend to a desire security level with significantly smaller keys than those of required for their counterparts.

2. Elliptic curve cryptography (ECC) [2]

Neal Koblitz and Victor Miller in 1985 from the University of Washington proposed a new public key cryptosystem namely the elliptic curve cryptography (ECC). Both of them suggested elliptic curve for the use of cryptography. The original ElGamal public key encryption and digital signature schemes are defined over finite fields. Neal Koblitz and Victor Miller then with IBM found that discrete logarithm on Elliptic curves over finite fields appeared to be intractable and hence ElGamal encryption and signature schemes defined on finite fields have natural counterparts on these curves.

2.1. Elliptic curve groups over a finite field

Let GF(p^m) be the finite field of p^m elements, where p is a prime and m an integer, an elliptic curve over GF(p^m) is defined as the set of solutions (x, y), where x, y $\in$ GF(p^m), to a cubic equation $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ with a_1, a_2, a_3, a_4, $a_6 \in$ GF(p^m), together with a special point O called the point at infinity. In cryptographic practice, two types of elliptic curves are of intrest: (1) curves over GF(2^m) with $m >$ 150, and (2) curves over GF(p) with p a large prime.

The performance of ECC [13] mostly depends on the efficiency of finite field computations and fast algorithms for elliptic scalar multiplications. In addition to the numerous known algorithms for these computations, the performance of ECC can be enhanced by selecting particular fundamental finite fields and/or elliptic curves. For ECC, limited form of elliptic curve that is defined over a finite field is of interest. Of particular interest for cryptography is what is referred to as the elliptic group mod p, where p is a prime number. This is defined as follows. Choose two nonnegative integers, a and b, less than p that satisfy:

$$4a^3 + 27\,b^2 \pmod{p} \neq 0.$$

Then Ep(a, b) denotes the elliptic group mod p whose elements (x, y) are pairs of nonnegative integers less than p satisfying: $y^2 \neq x^3 + ax + b \pmod{p}$ together with the point at infinity O. The elliptic curve discrete logarithm problem can be described as follows. Choose a prime p and an elliptic curve.

Q= xP where xP represents the point P on elliptic curve added to itself x times. Then the elliptic curve discrete logarithm problem is to find x given P and Q.

The first thing in this procedure is to encode the plaintext message m to be sent, as an x-y point Pm. It is the point Pm that will be encrypted as a cipher text and subsequently decrypted. Simply encoding the message as the x or y coordinate of a point, is not possible, because not all such coordinates are in Ep(a, b). There are approaches to encoding. [13]

3. Proposed Elliptic curve based signcryption schemes

As mentioned earlier, ElGamal public key encryption and digital signature schemes and their variants can all be extended to elliptic curves in a straight-forward way.

The proposed Signcryption scheme is based on ECC with performance advantages over the traditional Signature and then Encryption schemes. Computation involved when applying the Signcryption, Unsigncryption algorithms and communication overhead is much smaller than signature-then-encryption schemes. Signcryption is a technology that protects confidentiality and authenticity, seamlessly and simultaneously. For example, when you log in to your online bank account, signcryption prevents your username and password from being seen by unauthorized individuals. At the same time, it confirms your identity for the bank. Proposed

signcryption method uses elliptic curve for both encryption and signature generation. Proposed signcryption scheme typically consists of three algorithms: Key Generation (Gen), Signcryption (SC), and Unsigncryption (USC).

1. Key Generation (Gen): Gen generates a pair of keys for any user. Global public elements: E_P(a,b) Elliptic curve with parameters a, b, p where p is a prime number or an integer of the form 2^m. G point on elliptic curve whose order is large value n.

User randomly generates the pair of private and public key. The sender randomly selects an integer as her private key then computes public key.

Private key $K_{pri,A}$ $K_{pri,A} < n$.

Public Key $K_{pub,A}$ $K_{pub,A} = K_{pri,A} * G$.

The recipient selects keys by the same way as sender.

Private key $K_{pri,B}$ $K_{pri,B} < n$.

Public key $K_{pub,B}$ $K_{pub,B} = K_{pri,B} * G$

2. Signcryption (SC): SC is generally a probabilistic algorithm. Message *m* of arbitrary length is Signcrypted using Signcryption algorithm (ECC). This gives you a Signcrypted output *c*.

Signcryption algorithm (ECC) is used to encrypt the original message with the help of receiver's public key .Then this message is to be sent to the receiver.

$M_{cipher} = [(K_{random} G), (M + K_{random} K_{pub,B})]$

This algorithm will generate pair of encrypted points.

After this mean S_1, variance S_2 and (c.g) S_3 of these encrypted points are taken (New signature technique).

Mean (M_{cipher}), Var(M_{cipher}), C.G(M_{cipher}) Therefore S_1, S_2, S_3 will act as signature. Than S = [S_1 S_2 S_3] used as signature and sended to B by some secure link.

2.1 Proposed signature technique: Formula's used and security of signature parameters is described below:

Mean: (**S_1**) the arithmetic mean is the "standard" average, often simply called the "mean. The arithmetic mean of a set of numbers x_1, x_2, ..., x_n is typically denoted by , x'pronounced "x dash".

$$x' = \frac{1}{n} . \sum_{i=1}^{n} x_i$$

Proposed scheme uses ecc for encryption, encrypted points are in (x,y) coordinate form. Both the coordinates are used for mean calculation. Mean would be calculated as summation of all x and y coordinate values divided by total number of points.

Variance: (**S_2**) The average of the **squared** differences from the Mean.

$Var(X) = \sigma^2 = \Sigma (X_i - x',)^2 / n.$

Both the coordinates are used for variance calculation. (x,y) coordinates values are subtracted from the mean.

Centre of gravity: (S_3) The center of mass R of a system of particles of total mass M is defined as the average of their positions r_i, weighted by their masses m_i. In our context position r_i is the distance of encrypted points from centre.

$$R = \frac{1}{M} \sum m_i r_i$$

2.2 Security of signature parameters of proposed scheme:

In this paper a new signature generation technique has been proposed, so security of new technique has to be proved.

(i). Is it possible that two different messages can have same signature parameters (mean, variance and c.g).

Two different messages can't generate same signature parameter, these three parameters in combination is unique for every message. The reason behind using three parameters is mean of two messages can be same but Mean, Variance and C.G cannot be same. Since signature is calculated over encrypted points, during encryption of message a random number is used in that process that is unique every time so encrypted points will be different every time. So mean, variance and c.g will be different for different messages. Example of above scenario is given in Table 1.

Table 1: Signature Calculation Technique

Message 1			Message 2		
ABCD			1234		
Encrypted points			Encrypted points		
X	Y		X	Y	
734	199		514	550	
93	120		421	389	
603	164		219	713	
378	172		203	169	
233	256		407	29	
MEAN	VARIAN-CE	C.G	MEAN	VARIAN-CE	C.G
295.2	45863.7	1353874.4	360.9	42368.3	1529072.7

Two different messages are taken in this example, message is in the form of x and y coordinates values. Then mean, variance and c.g of these values are taken that act as signature of the message.

(ii). Is it possible to recover original message from this signature parameters.

Having signature parameters one cannot identify original message, and also it's not possible to recover original message from this parameters. Calculating mean, variance and c.g of given points is quite simple but inverse process is quiet difficult. These parameters act like one way function (calculating in forward direction is easy but in reverse direction is difficult).

3. Unsigncryption (USC): USC is most likely to be deterministic.The receiver can apply Unsigncryption algorithm on c to verify the message *m.* This Unsigncryption is unique to the message m and the sender. Receiver receives

the signcrypted text ,then this signature parameters is calculated over signcrypted text before decrypting and compare with the existing parameters (received through secure channel) If S_1= mean(M_{cipher}) S_2= var(M_{cipher}) S_3= cg(M_{cipher}) , if matches this proves signature is correct and also message integrity is maintained (encrypted message authentication takes place). Then message is decrypted using receiver's private key.

$M_{cipher} = [(K_{random} G), (M + K_{random} K_{pub,B})]$

first part of cipher text is multiplied by receivers private key $K_{pri,B}$.

$[K_{pri,B} * (K_{random} G), (M + K_{random} K_{pub,B})]$

$K_{pri,B} * G = K_{pub,B}$

Then $[(K_{random} K_{pub,B}), (M + K_{random} K_{pub,B})]$

$(M + K_{random} K_{pub,B}) - (K_{random} K_{pub,B}) = M$

second part is subtracted from first part the result is plaintext (M) that is received by receiver from sender.

3.1 The proposed algorithm can be described in following steps:

1. Sender randomly generates the pair of private and public key.

2. Then it generates the cipher pair of points i.e. all points on elliptic curve, that is used for mapping plain text to cipher text.

3. Sender takes the receivers public key $K_{pub,B}$, that is used for encrypting the message. Receiver's public key is used to provide confidentiality.

4. Now the sender encrypts the message by using receivers key and cipher pair of points. Cipher text is produced using this formula.

5. After generating the cipher message for message the mean, variance & the c.g of the cipher is calculated.

6. Since each key parameters produces unique cipher pair of point's generations the key characteristics could be defined by their statistics non-reversibly and hence it could be used as signature of sender.

7. When the receiver gets cipher message it before decrypting it tests for variations in these parameters and verifies the signature. Then decrypt the message using its private key.

4. Properties: Any signcryption scheme should have the following properties [8]

Properties that are satisfied by proposed algorithm.

Correctness: The algorithm is well verifiable as shown above. Unique unsigncryptability [2]—Given a message m of arbitrary length, the algorithm S signcrypts m and outputs a signcrypted text c. On input *c*, the algorithm U unsigncrypts c and recovers the original message un-ambiguously.

Efficiency: The computational costs and communication overheads of a proposed signcryption scheme is smaller than those of the best known signature-then-encryption schemes with the same provided functionalities.

Security: Proposed signcryption scheme simultaneously fulfill the security attributes of an encryption scheme and digital signature. And many additional properties: Confidentiality, Unforgeability, Integrity, and Non-repudiation, Public verifiability and Forward secrecy of message confidentiality

Confidentiality: The proposed algorithm is based on ECC which most difficult to crack in the presently available techniques. Confidentiality is provided using receivers public key so without the receivers private key, message can't be disclosed to anyone.

Unforgeability: This is not possible for an adaptive attacker to masquerade an honest sender in creating an authentic signcrypted text that can be accepted by the unsigncryption algorithm. Because of the reason that any attacker doesn't no what all parameters are involved in signcrypting a text.

Public verifiability: Any third party or judge can verify that the signcrypted text is valid or not, without any requirement for the private key of sender or recipient because signature is calculated over encrypted message, so no need of decrypting the original message for verification.

Non-repudiation: Since the points presents in the cipher message are selected form the sequence of points generated by selected private key using shared ECC curve. Hence the user cannot deny because its unique for every key.

Integrity: The manipulation in the cipher text by third party can easily be identified because it will change its signature. The reason behind it is signature is calculated over encrypted points so, any change in cipher text will affect signature also.

Forward secrecy of message confidentiality: This property can be maintained by frequently changing the ECC generating parameters.

5. Simulation results:

Proposed algorithm is implemented using MATLAB. Simulated results are obtained when proposed technique is implemented. These are the simulated results for the following elliptic curve:

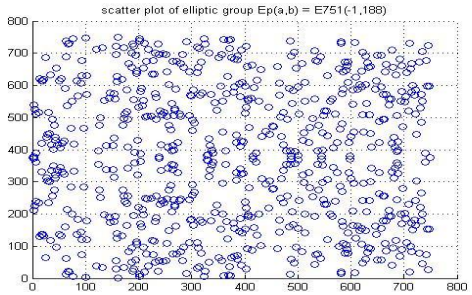


Figure 1: Points on elliptic curve

X-axis and Y-axis represents different values of x and y which are calculated with the help of equation $y^2 = x^3+ax+b \bmod p$.

This figure represents all the points generated by elliptic curve. This points are used for mapping purpose. Plain text point's p_m that will be encrypted as a cipher text points with the help of this points given in the scatter plot.

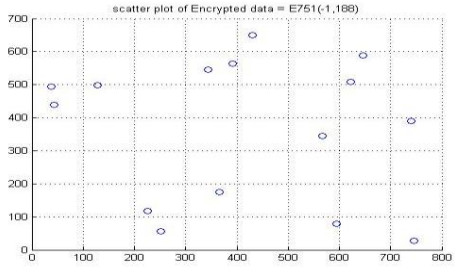


Figure 2: Message Points on elliptic curve

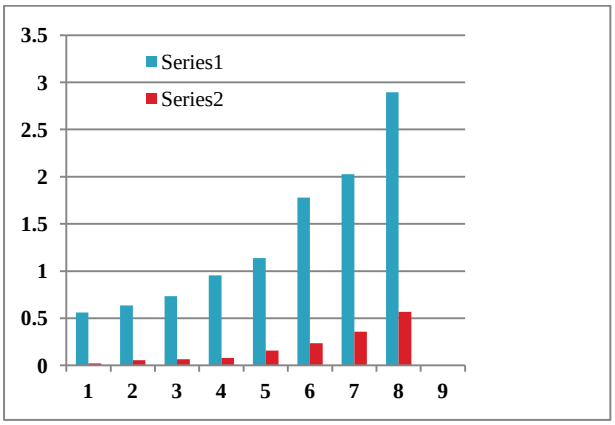
This figure represents all encrypted points that are encrypted with help of receiver's public key.

5.1 Analysis result of proposed scheme:

Table 2: Time analysis of proposed scheme.

Data Length (Bytes)	Proposed Signcryption time (sec)	Proposed UnSigncryption time (sec)
8	0.5624	0.023
16	0.635	0.0543
24	0.735	0.0654
32	0.954	0.0798
40	1.136	0.156
48	1.785	0.234
64	2.025	0.356
128	2.896	0.567

Table 2 shows time required for proposed signcryption and unsigncryption scheme for different message length. Total time required for signcrypting (encryption and signature) a message and unsigncrypting (decryption and signature) a cipher text to recover original message is described in table given below.



Series 1 – Signcryption Time, Series 2 – UnSigncryption Time

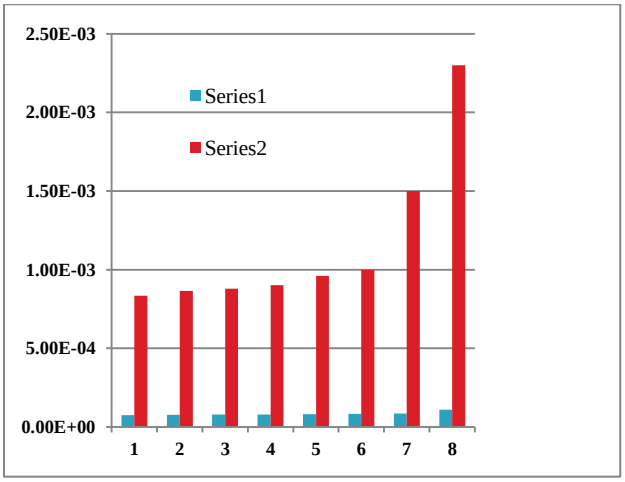
Figure 3: Proposed Signcryption versus Unsigncryption Time.

Signcryption and unsigncryption time for different messages is less according to proposed scheme. Encryption using ecc require less time as compared to other schemes. Signature generation using proposed scheme requires very less time because taking mean, variance and c.g of points is very fast as compared to other signature generation technique. Unsigncryption time is very much reduced in our proposed scheme because of encrypted message authentication.

Table 3: Comparative analysis of signature generation techinique.

Data Length (Bytes	Proposed Function Time(Sec.)	Hash Function Time(Sec.)
8	7.40E-05	8.35E-04
16	7.60E-05	8.65E-04
32	7.80E-05	8.78E-04
64	7.90E-05	9.01E-04
128	8.10E-05	9.60E-04
256	8.20E-05	1.00E-03
512	8.50E-05	1.50E-03
1024	1.10E-04	2.30E-03

Table 3 Describes the time required for the generation of signature pattern for proposed scheme as compared to other scheme, for messages having different length.



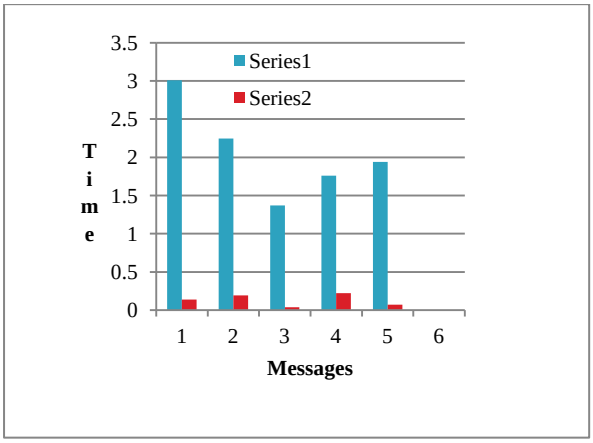
Series 1-Proposed signature scheme

Series 2-Hasing based signature generation,

Figure 4: Signature generation time based on two different methods.

Signature generation method of proposed scheme requires less time than signature generated by hashing scheme. Because proposed scheme uses simple mathematical operations (summation, average) to generate signature of the message as compared to other schemes. Proposed signature generation technique is quiet simple and requires less computational time as comparison with different schemes.

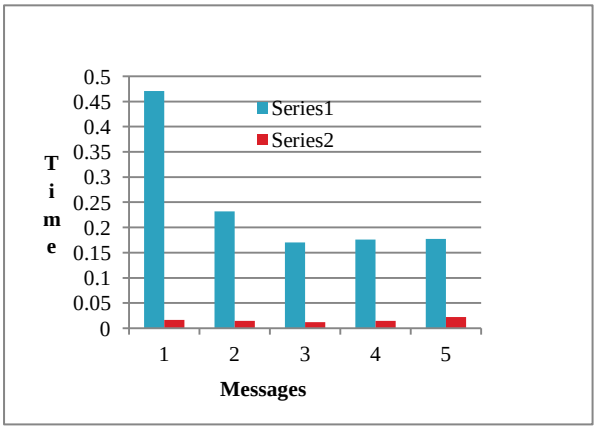
5.2 Comparative analysis of proposed scheme versus different scheme on the basis of time:



Series 1 – RSA based Sign-then encryption (encryption time)

Series 2 – Proposed Signcryption time.

Figure 5: Comparison of Rsa based sign-then encryption and proposed signcryption on the basis of encryption time



Series 1 – RSA based Sign-then encryption (decryption time)

Series 2 – Proposed UnSigncryption time.

Figure 6 Comparison of Rsa based signcryption and proposed signcryption on the basis of decryption time

Figure 5 and 6 Represents time required for proposed signcryption scheme is less than signature–than–encryption scheme. Because signcryption scheme provides both the functions of encryption and signature in a single logical step.

5.3 Discrete Logarithm Signcryption versus sign-then encrypt :

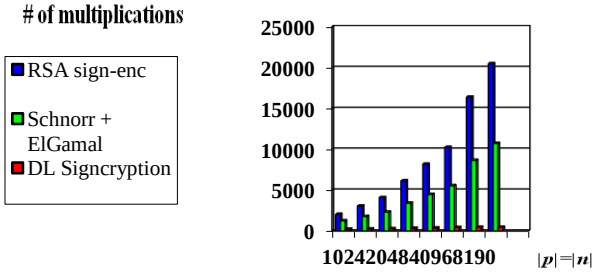


Figure 7: Computational complexity of different scheme.

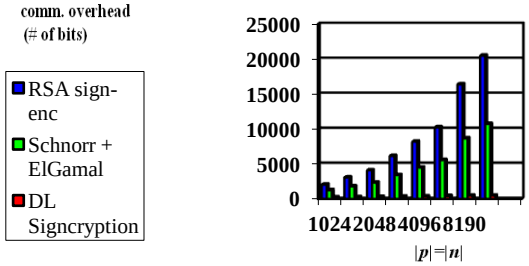


Figure 8: Communication overhead of different scheme.

Figure 7 and 8 Yuliang Zheng [12] Represents computational complexity and communication overhead of different algorithms. Computational complexity and communication overhead of algorithms that is based on Discrete logarithm problem (DLP) is less as compared to other schemes. As our proposed scheme uses ECC that is based on DLP, so computational complexity and communication overhead of our scheme is less as compared to different schemes that are not based on DLP.

5.4 Security analysis:

The main advantage of ECC over RSA and DSA is that the best algorithm known for solving the fundamental hard mathematical problem in ECC (the elliptic curve discrete logarithm problem (ECDLP) takes full exponential time, while RSA and DSA take sub-exponential time. This proves that considerably smaller parameters can be used in ECC than in other systems such as RSA and DSA, but with comparable levels of security.

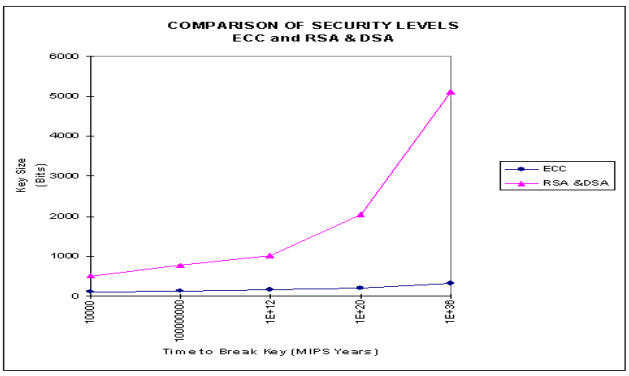


Figure 9: Comparision of security levels of different techniques.

ECC can present equal security with substantially smaller key sizes. Benefits of smaller key size- lower power consumption, as well as memory and bandwidth savings. Figure 9 compares, the time that is required to solve problem based on ECC and problem based on Integer factorization problem (IFP) or DLP. Here the time is measured in MIPS. As standard, it is generally accepted that 10^{12} MIPS years represents reasonable security at this time. MIPS year: computing time of one year on a machine capable of performing one million instructions per second. In Figure the time required to solve problem RSA and DSA are grouped together because the asymptotic running time for both is same. To achieve reasonable security, RSA and DSA should employ 1024-bit modulo, while a 160-bit modulus should be sufficient for ECC. Moreover, the security gap between the systems increases dramatically as the modulo sizes increases.

6. Conclusion and Future Extensions

This paper describes elliptic curve based signcryption method for safe and authenticated message delivery, which fulfills the functions of digital signature and encryption simultaneously, with a cost less than that required by the standard signature-then- encryption method. ECC has been used for the implementation, because of its unique property of ECDLP (Elliptic curve discrete logarithm problem) which is significantly more complicated than either the IFP (Integer factorizing problem) or DLP. Signcryption scheme has great advantages to be deployed in resource-constrained devices such as mobile phones, they can also lighten the computational burden on secure web servers .It is also suitable for security establishment in store-and-forward applications such as E-mail and Short Message Service.

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. Whenever a message is required to send to group of people, there are various difficulties. Using our technique a single message is send to group of people. In case of group signcryption there is one sender and multiple receivers. If same message is required to send to different receivers, a group is created. Among this group member's group leader is selected. Then communication takes place between sender and group leader .Message transfer between this two takes place according to proposed scheme. Message is received, verified and decrypted by the group leader. After this there is a requirement of transferring this message to different members of group. For this purpose every group member has shared User id and password with the group leader. By submitting the correct User id, password to the group leader system any member of the group can obtain original message.

References

[1] Y. Zheng, "Digital signcryption or how to achieve Cost (Signature & Encryption) << Cost (Signature) + Cost (Encryption)", Advances in Cryptology–CRYPTO'97, LNCS 1294, Springer-Verlag, 1997, pp.165-179.

[2] Y. Zheng, and H. Imai, "How to construct efficient signcryption schemes on elliptic curves", Information Processing Letters, pp.227-233, Elsevier Inc., 1998,Vol.68.

[3] 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 .

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

[5] C. Gamage, J. Leiwo, and Y. Zheng, "Encrypted message authentication by firewalls," International Workshop on Practice and Theory in Public Key Cryptography (PKC-99), LNCS 1560, Springer-Verlag, March 1999 , pp.69-81.

[6] Y. Han, X. Yang, and Y. Hu, "Signcryption Based on Elliptic Curve and Its Multi-Party Schemes", 3rd ACM International Conference on Information Security (InfoSecu'04), pp.216-217.

[7] R.-J. Hwang, C.-H. Lai, and F.-F. Su, "An efficient signcryption scheme with forward secrecy based on elliptic curve," Journal of Applied Mathematics and Computation, Elsevier, 2005, Vol.167, No.2, pp.870-881

[8] M. Toorani ,"Cryptanalysis of an Elliptic Curve-based Signcryption Scheme", International Journal of Network Security, Jan. 2010,Vol.10, No.1, pp.51–56.

[9] Y. Sakai, K. Sakurai, H. Ishizuka, Secure hyperelliptic cryptosystems and their performance, in: Proc. 1998 International Workshop on Practice and Theory in Public Key Cryptography (PKC '98), Lecture Notes in Comput. Sci., Springer, Berlin, 1998,Vol. 1431 , pp. 164–181.

[10] F. Zhang, D. Ji, Y. Wang, "A Protocol for Threshold Generation of Signcryption", Proc of Chinacrypt'2002, Beijing: Publishing House of Electronics Industry, 2002, pp.193-202.

[11] Z. Gan, X. Li, K. Chen, "A Publicly Verifiable Threshold Signcryption Scheme", Proc of Chinacrypt'2004, Beijing: ,Science Publish House, 2004, pp.105-109.

[12] Yuliang Zheng "Updates on Signcryption", IEEE P1363 Meeting, UCSB 8/22/2002

[13] O.Srinivasa Rao "Efficent mapping method for elliptic curve cryptosystems", International Journal of Engineering Science and Technology,2010, Vol. 2(8), 3651-3656.

[14] Mohsen Toorani ,Ali Asghar Beheshti Shirazi "An Elliptic Curve-based Signcryption Scheme with Forward Secrecy" Journal of Applied Sciences, 2009,Vol. 9, No. 6, pp. 1025-1035.

[15] Elsayed Mohamed and Hassan Elkamchouchi "Elliptic Curve Signcryption with Encrypted Message Authentication and Forward Secrecy" IJCSNS International Journal of Computer Science and Network Security, January 2009, VOL.9 No.1

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

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

[18] Ram Shanmugam. Elliptic curves and their applications to cryptography: An introduction : Andreas enge, kluwer academic press, norwell, ma, 1999, pp. 164.isbn 0-7923-8589-6. Neurocomputing, 2001, 41(1-4):193 -193.

[19] Scott A. Vanstone. Elliptic curve cryptosystem - the answer to strong, fast public-key cryptography for securing constrained environments. Information Security Technical Report, 1997, 2(2):78 - 87.