ISSN 2278-7763

An Efficient identity based Multi-receiver Signcryption Scheme using ECC

Shweta Khullar[1], Vivek Richhariya[2], Vineet Richhariya[3]

[1]Department of Computer Science, LNCT, Bhopal, India; [2]Department of Computer Science, LNCT, Bhopal India; [3]Department of Computer Science, LNCT, Bhopal, India.
Email: [1]shwetakhullar20@gmail.com,[2]vivekrich@yahoo.com,[3]vineet_rich@yahoo.com

ABSTRACT

Signcryption is a technique of performing signature and encryption in a single logical step. It is a secure and efficient technique of providing security between the sender and the receiver so that the data send by the sender should be made secure from various types of attacks such as desynchronization attacks, identity disclosure attack and spoofing attacks. Although there are many technique implemented for the generation of signature and encryption. Here a new and efficient technique of signcryption has been implemented in a multireceiver environment on the basis of identity of the receiver. The proposed work given here is the implementation of signcryption scheme using elliptic curve cryptography where the authentication between sender and the receiver is based on the identity of the receiver.

Keywords : Digital Signature, Signcryption, multireceiver, PKG, unforgeability, Non-repudation, Integrity.

1 INTRODUCTION

The term Signcryption is referred as a technique of encrypting the data with the use of signatures in area of public key cryptography. This technique concurrently fulfils both the functional advantages of digital signature and public key encryption in a single step. In this way computational cost is significantly lower than that required by the traditional 'signature and encryption' technique.

Today the concept of securing the message and the authenticity of the sender's private data is important to achieve. Although there are many techniques implemented for the security of sender's private data. A new way of securing the data is using the process of signing the data and then encrypts it, but the technique increases the computational costs and communication overhead [1]. So to reduce these computational cost and communication overhead the next step is to combine the signature-then-encryption within a single logical step which was first performed by Yuliang Zheng in 1997 [2].

A signcryption technique is a combination of digital signature which is used for authentication and public key cryptography which is used for securing the message. Digital signature is a brand of authentication. It is widely used to judge or authenticate the valid source of data or identifying the original nodes that generate the message. While public key cryptography is message security mechanism that helps to provide confidentiality and secure delivery of message. Both are work independently, first message was digitally signed (or authenticated by sender) and then encrypted before sending. This is traditionally known as sign then encryption. But later on they are combined together and can be named as signcryption.

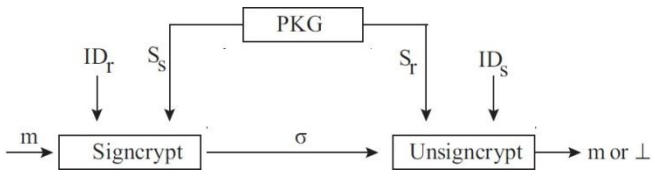
A signcryption scheme typically consists of three algorithms: Key Generation (Gen), Signcryption (SC), and Unsigncryption (USC). Key Generation (Gen) generates a couple of keys for user, signcryption (SC) is normally a probabilistic algorithm, and Unsigncryption (USC) is almost certainly to be deterministic. Any signcryption scheme should have correctness, Accuracy and Security as main properties [3].

Bellare et al. [4] has proposed a multireceiver signcryption scheme in which there are n receivers where each of the receivers contains a pair (ski, pki) i.e private and public key pair. The pki can be used by the sender to encrypt a message Mi to obtain a ciphertext Ci for i=1,2….n and then sends (C1,C2……Cn) as ciphertext. The receiver i then extracts Ci and decrypt the ciphertext using ski.

A multireciever signcryption is a technique of sending the message to the receiver using the identity of the receiver. As show in the given figure is multireceiver identity based signcryption technique where the message to be send will have signcrypt using the identity of the receiver. Here the PKG is private key generator used to generate private key for the sender and receiver. The receiver when wants to access the data will have sign and authenticate and decrypt the data.

The sigcryption using identity based multireceiver provides security from various attacks such as unforgeability, identity disclosure attack and various attacks.

ISSN 2278-7763



1.1 Properties of Signcryption

Confidentiality and Authenticity
During the process signcrypting the data a confidentiality is maintained between user and receiver so that the chances of attack have been reduced. A signcrytion is a process where the user when sends the data then the parameters should be made secure and if anyone wants to access these parameters authentication is required. Authenticity is a technique of access the data with permission means if anyone in the network may want to access the data should have authenticate first whether it is a valid user or not.

Signature Verifiability and Non-repudiation
Non-repudiation refers to a state of affairs where the purported maker of a statement will not be able to successfully challenge the validity. The term is often seen in a legal setting wherein the authenticity of a signature is being challenged [5]. During the process of signcryption phase sender will generate parameters r and s for the signature. Signature Verifiability is a technique of signcryption where the sender needs to encryption with his signatures and then at the receiver need to verify these signatures.

Forward Secrecy
It means the attacker us unable to read the data even with the help of user's private key. During the process of signcryption the sender uses his public key to encrypt the data and receiver uses his private key to decrypt the data. During the transmission of data from user to the receiver third party can't access the data even with the help of his private key.

ELLIPTIC CURVE CRYPTOGRAPHY

ECC follows Public Key Encryption technique and the security provided is based on the hardness of Discrete Logarithm Problem (DLP) called Elliptic Curve Discrete Logarithm Problem (ECDLP). According to ECDLP, $kP = Q$, where P, Q are the points on an elliptic curve and k is a scalar. If k is significantly large then it is unviable to calculate k when the values of 'Q','P' is known.

2 RELATED WORK

Jianhong Zhang, Zhipeng Chen and Min Xu proposed a new signcryption scheme based on ID-based Multireceiver Threshold Signcryption scheme [1]. The scheme is an efficient technique based on multireceiver identity of receiver. The technique used here is based on random oracle model where multireceiver can access the data using the identity of the receiver and hence support the properties of confidentiability and unforgeability.

The signcryption scheme given here provides public verifiability and prevents from attacks in the network [5]. The scheme also provides third party authentication where the technique implemented here is based on random oracle model and removes the disadvantages of work done in [6] and [7].

An efficient and certificate less Signcryption Scheme has been proposed in [8]. The technique provides comparison from various techniques and provides best signcryption scheme for CLSC scheme. The technique used here based on certificate less signcryption but provides more efficiency and prevents from various attacks.

An efficient identity-based broadcast signcryption scheme has been proposed which is based on short ciphertext size and public ciphertext authenticity of the data [9]. The security issues and different attacks are on the basis of random oracle model and it has reduced computational cost and time.

An identity-based anonymous signcryption scheme for multiple receivers has been proposed which implements the concept of novel cryptographic primitive [10]. The scheme used here is used for the standard model and provides prevention from various security attacks such as unforgeability and mutual authentication. The technique also gives security proof regarding Deffie-Hellman problem.

The identity based multireceiver scheme is also implemented for the MANET where the main security and privacy concern is on the prevention from various attacks [11]. The ID-based multireceiver signcyption scheme when implemented for the multireceiver in an Ad-hoc Network can be used in a wide variety of applications.

A secure signcryption scheme for random oracle model is proposed based on the concept of aggregation [12]. The scheme used here provides various security issues and prevention from various attacks. The technique used here for the aggregation is by taking the aggregate of n number of receivers by taking n users.

Signcryption is a technique of using signature and encryption within a single logical step. Here the proposed work is based without random oracle model [13]. The scheme provides non-repudiation with respect to plaintext. The scheme also provides and verify using third party authentication.

A probably-secure improved scheme to correct the vulnerable and also give the unforgeability & confidentiality of improved scheme under the existing security assumption. Multireceiver Identity Based Signcryption [14]. The scheme provides an efficient way of signcryption the message having an extra authentication and prevention from various security attacks.

A revocable ID-based signcryption scheme is proposed which provides an authentication and prevention from attacks [15]. The scheme proposed here provides prevention from various possible threat and attacks. The scheme implemented here

ISSN 2278-7763

proves security issues regarding BDH and CDH schemes.

Cryptanalysis of an Identity Based Signcrypion scheme without Random Oracle model is proposed in [16]. Here in this technique an efficient technique of signcryption has been proposed which removes some of the weaknesses of the signryption scheme proposd in [17]. The technique not only removes some of the weakness but also proved prevention from various attacks.

Multireceiver Identity Based Signcryption Scheme

Here in this technique of signcryption a single or multiple messages has been signcrypted which can be decrypted using multiple receivers. The sender uses the identity of the receiver to signcrypt the messages and when the message is send to the receiver first of all the identity of the receiver is checked then only it can decrypt the message.

3 PROPOSED SCHEME

Initialization Phase

During the initial set up of the Elliptic curve we choose an elliptici curve equation

$$y^2 = x^3 + ax + b$$

This satisfies the equation,

$$4a^3 + 27b^2 \neq 0$$

Key Generation Phase

Key generation is an important part where we have to generate both public key and private key. The sender uses the receiver's public key for the encrypting of the message and the receiver uses his private key to decrypt the message.

Now, we have to select a number as private key 'x' within the range of 'n'.

Now we generate the public key using private key and Base point given as:

y = x * P

x = The random number that we have selected within the range of (1 to n-1). P is the Base point on the curve.

'y' is the public key and 'x' is the private key.

Signcryption Phase

For signcryption, the same elliptic curve parameter is used that was used for key generation and mutual authentication.

For the signcryption process, we have used the algorithm given by [Elsayed Mohamed et.el in his work "Elliptic Curve Signcryption with Encrypted Message Authentication and Forward Secrecy"] except they select at random number v from 1.... q-1, while we are using here the identity value to generate random number the key k1 and k2.

k1 = hash(ID.P)

k2 = hash(ID.Qrec)

c = E k2(m)

r = hash (c, k1)

s = ID / (r + Dsen) mod n

R = rP

p=HASH (c||R||s)

Send (c,R,s) to Receiver

UnSigncryption Phase

Receiver receives (c,R,s)

$c||R||s \leftarrow h^{-1}(p)$

k1 = hash(s(R + Qsen))

=sR+s.Qsen

= ID/(r+Dsen)).rP+(ID/(r+Dsen)).Qsen

= ID.rP/(r+Dsen))+(ID.Qsen/(r+Dsen))

= ID.rP+ID.Qsen/r+Dsen

= ID.rP+ID.Dsen.P/r+Dsen

=ID.P(r+Dsen)/r+Dsen

=ID.P

= k1 =hash(ID.P)

r = hash (c, k1)

k2 = hash(Drec.s(R + Qsen))

=Drec.sR+S.Qsen

=Drec.ID.P

=Drec.P.ID

=Qrec.ID

= k2 =hash(Qrec.ID)

m = Dk2(c)

Accept c only if rP = R

4 RESULT ANALYSIS

Confidentiality	Integrity	Unforgeability	Non-repudiation	Forward secrecy	Additional authentication
YES	YES	YES	DIRECTLY	YES	YES

As shown in the above table is the different types of security analysis that our proposed scheme supports. The security analysis is discussed with respect to the security features which the proposed protocol should satisfy.

Key Generation based on 112 bit elliptic curve parameters

Public key :(3891202400346826197829678134320334, 1102331985183872123584216988231028)

Secret key: 219083506530280040363010588254775 8 (3891202400346826197829678134320334, 1102331985183872123584216988231028)

Key Generation based on 160 bit elliptic curve parameters

Publickey:(1255891545992026542620254936478383946016390782342,1256523562429701394736385179047555823 81807820156)

Secret key:

711990739313931553601225181763646733544836181374 (1255891545992026542620254936478383946016390782 42,1256523562429701394736385179047555823281807821 56)

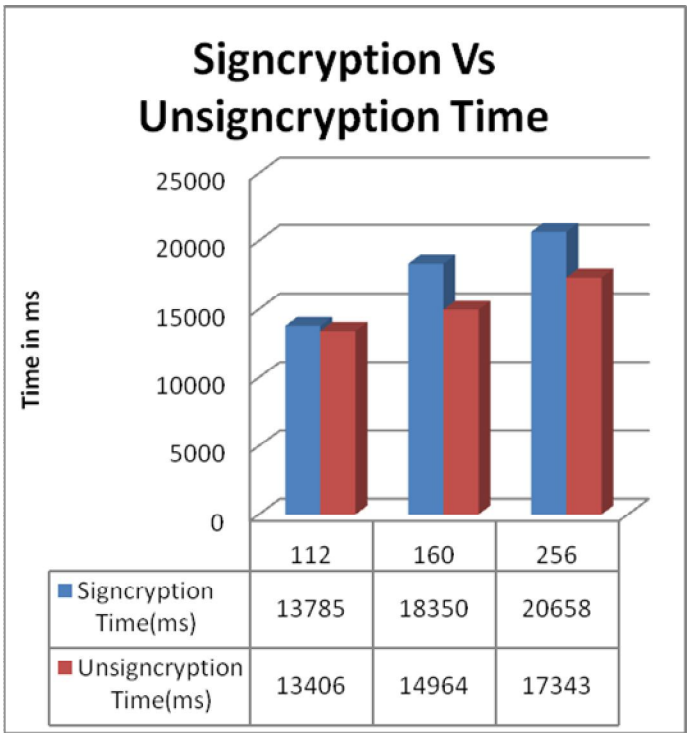
ISSN 2278-7763

Key Generation based on 256 bit elliptic curve parameters

Publickey:(104167787095909466095273472806018779
460591157327780067694917407162431743855,95154954
765086710128599082517990437052550866855877955671151838
3154726931224) secp256r1
Secret-
key:735469399421700011146571627601099789003554859099678
718018899213632650058929(104167787059094660952734728060
187797904605911573277800676949174071624317438 55,
951549546765086710128599082517990437052550866853587795 5
671151838315472693 1224) secp256r1.

Generation Time Comparison

The graph shown above is the time comparison between signcryption of the message 'm' and the unsigncryption time on the basis of number of bit keys.



5 CONCLUSION

In this paper the signcryption scheme with multiple receivers has been implemented, though various signcryption schemes has been implemented but the results shows the efficient working of signcryption using multiple identity based receivers in terms of different types of attacks and is more authenticated as compared to the previous signcryption schemes. The signcryption scheme using multiple receivers using elliptic curve cryptography has better performance as compared to the other cryptography techniques.

REFERENCES

[1] Jianhong Zhang, Zhipeng Chen, Min Xu "On the Security of ID-based Multi-receiver Threshold Signcryption Scheme", In proceedings of 2nd International Conference on Consumer Electronics, Communications and Networks (CECNet), pp. 1944 – 1948, 2012.

[2] Y.Zheng. "Digital signcryption or how to achieve cost (signature & encryption) cost (signature)+cost (encryption)", Crypto'97, LNCS 1294, pp. 165-179, Springer-Verlag, 1997.

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

[4] M. Bellare, A. Boldyreva and S. Micali: Public key encryption in a multi-user setting: Security proofs and improvements, EUROCRYPT' 2000, LNCS # 1807, pp. 259-274, Springler-Verlag, 2000.

[5] http://en.wikipedia.org/wiki/Non-repudiation.

[6] S. Sharmila Deva Selvi, S. Sree Vivek, C. Pandu Rangan, "Identity Based Public Verifiable Signcryption Scheme", Proceedings of the 4th international conference on Provable security (ProvSec'10), Lecture Notes in Computer Science Volume 6402, pp 244-260, 2010.

[7] Feng Bao and Robert H. Deng. "A signcryption scheme with signature directly verifiable by public key". In Public Key Cryptography, volume 1431 of Lecture Notes in Computer Science, pages 55–59. Springer, 1998.

[8] Raylin Tso, Takeshi Okamoto, and Eiji Okamoto. Ecdsa-verifiable signcryption scheme with signature verification on the signcrypted message. In Information Security and Cryptology(Inscrypt 07), volume 4990 of Lecture Notes in Computer Science, pages 11–24. Springer, 2008.

[9] Gang Yu, Hongzhi Yang, Shuqin Fan, YongShen, Wenbao Han, "Efficient Certificate less Signcryption Scheme", Proceedings of the Third International Symposium on Electronic Commerce and Security Workshops(ISECS '10), pp. 55-59, 2010.

[10] Hien D.T., Tien T.N., Thu Hien T.T, "An efficient identity-based broadcast signcryption scheme", Proceedings of the 2010 Second International Conference on Knowledge and Systems Engineering (KSE '10), pp. 209-216, 2010.

[11] Bo Zhang, Qiuliang Xu, "An ID-based Anonymous Signcryption Scheme for Multiple Receivers", Proceedings of the 2010 international conference on Advances in computer science and information technology, pp. 15-27, 2010.

[12] Lei Wu, "An id-based multi-receiver signcryption scheme in MANET", Journal of Theoretical and Applied Information Technology, Vol. 46 No.1, pp. 120-124, dec-2012.

ISSN 2278-7763

[13] Jayaprakash Kar, "Provably Secure Identity-Based Aggregate Signcryption Scheme in Random Oracles", Cryptology ePrint Archive: Report 2013/037, Jan 2013. Available at: http://eprint.iacr.org/2013/037.pdf

[14] Prashant Kushwah and Sunder Lal, "Provable secure identity based signcryption schemes without random oracles", International Journal of Network Security & Its Applications (IJNSA), ISSN: 0974 – 9330, Vol.4, No.3, pp. 97-110, May 2012.

[15] Wei Yuan, Liang Hu, *Hongtu Li, Jianfeng Chu, Yuyu Sun* "Cryptanalysis and Improvement of Selvi et al.'s Identity-Based Threshold Signcryption Scheme", Journal of Networks, *ISSN 1796-2056,* Vol 6, No 11, pp. 1557-1564, Nov 2011.

[16] Bo ZHANG," Cryptanalysis of an Identity Based Signcryption Scheme without Random Oracles",2010.

[17] Y.Yu, B.Yang, Y. Sun, S.Zhou, Identity based signcryption scheme without random oracles [J]. Computer Standards & Interfaces. 2009, 31:56-62.

[18] GANG YU, XIAOXIAO MA, YONG SHEN, WENBAO HAN," PROVABLE SECURE IDENTITY BASED GENERALIZED SIGNCRYPTION SCHEME",2010.