A Survey on ECC ID Based Signcryption Schemes

Mr.S.Navin Prasad, Assistant Professor & Head, Department of Computer Science, Nagarathinam Angalammal Arts and Science College, Madurai, Tamil Nadu, India.

Dr.C.Rekha, Assistant Professor, Department of Computer Science, Government Arts College, Melur, Tamil Nadu, India.

Abstract - Signcryption is another cryptographic methodology which gives confirmation and encryption all the while in a solitary sensible advance. The point is to decrease the expense of mark then encryption approach. This expense incorporates computational expense what's more, correspondence cost. Besides some Signcryption plans depend on RSA while some depend on elliptic bend. This paper gives a basic audit of the signcryption plans dependent on elliptic bends, since signcryption plans dependent on elliptic bend cryptography saves more computational time and correspondence cost. Likewise, the elliptic bend based signcryption plans are reasonable for asset obliged applications. This work investigates the benefits and impediments of the extraordinary signcryption plans dependent on elliptic bends.

Keywords: ***Signcryption, Elliptic Curve Cryptography, Encryption, Authentication Cloud Computing*.**

I. INTRODUCTION

Cloud computing is a blend of significant level workers that are practically associated together. The Cloud Computing is an administration that conveys over the web. It permits clients to lease furthermore, access the applications, programming improvement, and organization apparatuses climate, network-open stockpiling preparing, etc [1]. For the most part, Cloud computing is helpful, on-request network admittance to shared registering assets. The central part of Cloud computing is that the information is being brought together or dispersed in the cloud data set. The information is put away at far off areas and accessible on-request that permits the clients to get to information without introducing any extra applications at any PC through web openness.

Confidentiality and authenticity are two primary natives of cryptography and figured it out through encryption plans and digital signature plots separately. Intelligently two natives are autonomous. Out in the open key setting, the encryption utilizes the public key of the collector though signature utilizes discharge or private key of the sender. To accomplish both confidentiality and realness we utilize sign-then-scramble approach which includes both encryption just as signature. In 1997, Zheng [13] gave the idea of signcryption, which performs encryption and mark both in a solitary sensible advance. Computationally, signcryption is more productive than 'sign-then-encode' approach. The utilization of signcryption diminishes the quantity of steps, decreases the length of cipher text and in particular, it lessens the execution intricacy by joining the two modules of encryption and mark into a solitary module of signcryption. Zheng's unique signcryption conspire is discrete logarithm based. In 1998, Zheng and Imai [14] gave a signcryption conspire dependent on elliptic bends. The primary personality based signcryption conspire was proposed by Malone-Lee [8] in 2002. From that point forward, a few character based signcryption calculations have been proposed [2, 4, 5, 7, 8, 9]. Nonetheless, not every one of these plans are upheld by formal models and security confirmations in the arbitrary prophet model. Boyen [2] gave the security thoughts for signcryption as: message secrecy, signature non-renouncement, cipher text unlink ability, ciphertext validation, also, ciphertext obscurity. Among the plans upheld by security confirmations in formal security models, Chen and Malone Lee's proposition [4] turns out to be generally effective development; notwithstanding, it loses cipher text unlink ability

All the above signcryption plans function admirably when client needs both secrecy furthermore, genuineness. In any case, not all messages require both classification and legitimacy. In the event that just one of the two functionalities is required then the signcryption conspire isn't proficient. In this situation, as indicated by Zheng, signcryption might be supplanted with signature/encryption calculation. Hence, to determine the issue, we need to utilize three cryptographic calculations signcryption, encryption and signature according to require. Anyway it may not be possible in a few applications like inserted frameworks and pervasive figuring. In 2006, Han and Yang [6] proposed the plan to utilize a similar plan as a signcryption conspire, as an encryption plot and as a mark conspire according to necessity. They named the new crude as summed up signcryption. There plot depends on elliptic bends. Wang et al [12] developed the plan [6] and gave security ideas of summed up signcryption plot. It is to be noticed that none of these plans is personality based. Here we propose an ID Based Generalized Signcryption (IDGSC) plot.

II. RELATED WORK

2.1 Signcryption

The efficient way to carry out two fundamental operations of security i.e. encryption and digital signature simultaneously is termed as signcryption. Separately carrying out operations for encryption and digital signature is very expensive in terms of computational cost and communication overhead due to the computation on large numbers and extended bits produced during and after the operations. Y.Zheng [4] showed that that signcryption saves about 50% computational cost and 85% communication overhead. A signcryption scheme consists of three algorithms namely: Key Generation, Signcryption and Unsigncryption [5]. The Key Generation algorithm generates the key pair for the sender and the receiver. Signcryption algorithm is a probabilistic algorithm which produces signature and ciphertext. And Unsigncryption algorithm is deterministic in nature which verifies the authenticity of signature and performs decryption. Any signcryption scheme should satisfy correctness, efficiency and security properties [6]. Correctness: A signcryption scheme is said to be correct if it verifies the signature correctly and recovers the plaintext from ciphertext. Efficiency: A signcryption scheme is considered to be efficient if its computational cost and communication overhead is less than that of traditional signature-then-encryption approach. Security: A signcryption scheme is secure if it provides confidentiality, integrity, encrypted message authentication, non-repudiation, unforgeability, forward secrecy and public verification. In the next section of this paper different Signcryption schemes based on elliptic curves are discussed and their advantages and limitations are highlighted.

2.2 ECC Basics

In 1985 Niel Koblitz and Victor Miller from the University of Washington proposed the elliptic bend cryptosystem [3]. Elliptic bends over limited fields gave off an impression of being unmanageable. Elliptic bend can be characterized over Fq and F_2^m [7]. For straightforwardness in cryptographic activities we will examine just Elliptic bends over Fq [7]. A limited field is a bunch of components that have a limited request (number of elements).The request of Galois Feld (GF) [3] is typically an indivisible number or a force of an indivisible number. An elliptic bend E over Fq is the arrangement, everything being equal (x, y) ϵ Fq X Fq to a condition called Weierstrass condition

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

Where a, b ϵ Fq and $4a^3 + 27b^2 \neq 0$, along with an exceptional point ∞ called the point at vastness.

It is notable that E is an (additively composed) abelian group with the point ∞ filling in as its personality component. The two key activities over elliptic bends are elliptic bend point expansion and point elliptic bend point augmentations. Elliptic bend point augmentation is viewed as the most expensive activity in elliptic bend math.

III. LITERATURE REVIEW

Diverse signcryption plans have been proposed of which some depend on secluded exponentiation and other utilize elliptic bends. "Signcryption" was presented by Y.Zheng [4] in the year 1997. This essential plan was in light of discrete logarithmic issue and incorporates particular exponentiation. Zheng showed that signcryption saves about half computational expense and 85% correspondence cost than the conventional mark then-encryption conspire. Zheng plot was changed by certain specialists as they added a few additional highlights to this essential signcryption plot.

First Elliptic Curve based signcryption plot was proposed by Zheng and Imai [9] which gives all the essential security highlights, with cost not exactly as needed by "signaturethen-encryption" which saves about 58% computational expense what's more, about 40% correspondence cost than signature-thenencryption. They pick ECC on the grounds that elliptic bend based arrangements are normally founded on the trouble of Elliptic Curve Discrete Logarithmic Problem (ECDLP). As it depends on elliptic bend cryptosystem the key size utilized is more modest as contrasted with different plans, which is one of the benefits of this plan yet forward mystery was absent from this plan

Yiliang Han [10] introduced another signcryption dependent on elliptic bend cryptosystems that consolidates ECDSA and PSCE-1. The proposed signcryption conspire gives public check and can be confirmed by the outsider after the beneficiary eliminates his key data. It is shown that that the plan is secure against the versatile picked ciphertext attack. It very well may be utilized to advance a message to different beneficiaries all the while in a safe and confirmed manner. This new signcryption utilizes a uniform elliptic bend cryptosystem stage rather than four sorts of cryptosystem segments: hash work, keyed hash work, symmetric figure and elliptic bend.

Hwang [11] proposed an effective signcryption conspire in light of elliptic bend which takes lower computational expense furthermore, correspondence overhead simultaneously gives message secrecy, validation, honesty, unforgeability, non-disavowal, forward mystery for message secrecy and public confirmation. Mohsen Toorani and Ali Asghar [12] assessed Hwang's signcryption plot and demonstrated that it includes a few security defects and inadequacies as it bombs all the ideal and fundamental security qualities of a signcryption conspire. The plan has powerless meeting key foundation and legitimacy check of public keys and authentications is absent.

Han et.al [13] proposed Elliptic Curve Based Generalized Signcryption (ECGSC) with a unique element that gives secrecy or validation independently under the state of explicit data sources. In this plan an outsider can check the signcrypted text openly by utilizing elliptic bend advanced mark calculation (ECDSA)

E.Mohamed and H.Elkamchouchi [14] proposed an elliptic bend based signcryption conspire which gives forward mystery and scrambled message validation for firewalls. In this plan an appointed authority can straightforwardly check the sender's mark on signcrypted messages without sender's private key and without unscrambling the message. This plan consolidates the security properties with reserve funds in computational intricacy also, data transmission overhead.

Esam A. A. A. Hagras [16] proposed a proficient Forward Secure Elliptic Curve Signcryption Key Management (FSECSKM) Scheme for Heterogeneous Wireless Sensor Organizations (HWSN). But message privacy, validation, unforgeability and non-renouncement, the proposed conspire likewise gives forward mystery, public check, and scrambled message validation

Ramratan Ahirwal [17] proposed a signcryption conspire in view of Elliptic Curve Cryptography. In this work another signature age procedure is presented which requires less time when contrasted with signature produced by hashing conspire besides the mark can be checked without decoding of the message along these lines, giving scrambled message validation.

F.Amounas [19] introduced an improved signcryption conspire in view of elliptic bend discrete logarithmic issue (ECDLP). The plan gives all the security properties these security properties with a saving in calculation cost contrasted with the customary mark then-encryption plot, which makes the new plan more proper for conditions with restricted processing power.

Suman Bala et.al [20] proposed an elliptic bend signcryption key administration conspire for remote sensor networks which gives forward mystery. This plan is expected to address key administration issue in remote sensor organizations. The proposed conspire gives all the security credits along with forward mystery however this plan can't give encoded message confirmation.

IV. ANALY SIS OF SIGNCRYPTION SCHEMES

The investigation of various signcryption plans is spread out as Table 1. The investigation shows the center, benefits and the impediments of the proposed signcryption plans dependent on elliptic bends. The investigation shows how the improvement of signcryption plans dependent on elliptic bend have occurred beginning from the principal conspire proposed by Zheng and Imai

Table 1. Elliptic Curve based Signcryption Schemes an Analysis

Sno	Authors	Proposed Work	Advantages
1	Y. Zheng Hideki Imai [9]	To Design the concept of ECC	Recoveries 58% computational expense and 40% correspondence cost. The key size utilized is more modest as contrast with different plans
2	R.J.Hwang Chih-Hua Lai Feng-Fu Su [11]	Developing an Best Signcryption Scheme based on ECC	The plan gives all the security ascribes including forward mystery, public obviousness and encoded message validation.
3	Yiliang Han [13]	Plan dependent on that gives secrecy or confirmation independently under the state of explicit inputs	This method is good for computation purpose and communication purpose
4	E.Mohamed [14]	This method provides the forward security for message authentication for firewall	This method provides Forward security for firewall
5	M. Toorani A.A. B.Shirazi [15]	To secure the data from various attack using Signcryption	This proposed work is done by ECC to secure the data form the various attacks
6	Ramratan Ahirwal [17]	To determine signcryption plans on elliptic bends over limited fields, and to inspect the productivity of such plans.	Gives all the security credits what's more, the proposed plan can be Utilized for a gathering.
7	F.Amounas [19]	Planning minimal expense elliptic bend based signcryption plans	More affordable than different plans as number of elliptic bend point duplications are less.

Table 2. Security Characteristics of ECC based Signcryption Schemes

Signcryption Schemes	Confidentiality	Integrity	Authentication	Unforgeability	Nonrepudiation	Forward Secrecy	Public Verification
Y. Zheng Hideki Imai [9]	✓	✓	✓	✓	✓	×	×
R.J.Hwang Chih-Hua Lai Feng-Fu Su [11]	✓	✓	✓	✓	✓	×	✓
Yiliang Han [13]	✓	✓	✓	✓	✓	×	✓
E.Mohamed [14]	✓	✓	✓	✓	✓	✓	✓
M. Toorani A.A. B.Shirazi [15]	✓	✓	✓	✓	✓	✓	✓
Ramratan Ahirwal [17]	✓	✓	✓	✓	✓	✓	✓
F.Amounas [19]	✓	✓	✓	✓	✓	✓	✓

V. CONCLUSION

Signcryption dependent on elliptic bends is reasonable for the applications which use gadgets having confined memory and transfer speed with low registering power. The goal of this paper is to investigate the qualities and shortcomings (assuming any) of distinctive elliptic bend based signcryption plans. The investigation appeared in Table 1 followed by the examination appeared in Table 2 gives an unmistakable image of various signcryption plans in view of elliptic bend. By the investigation of Table 1 and Table 2 one can undoubtedly make a decision about the extraordinary signcryption plans examined in the writing survey. Consequently the investigation acted in this paper is significant for the analysts, understudies and experts who are working in the space of signcryption.

REFERENCES

[1] William Stallings 1993. Cryptography and Network security: Principles and Practices. Prentice Hall Inc.

[2] M.Satyanarayanan, “Pervasive Computing: Vision and Challenges”, IEEE Personal Communications, Volume 8 No.4, pp. 10-17, 2001

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

[4] Yuliang Zheng. 1997. Digital signcryption or how to achieve cost(signature encryption) « cost(signature) + cost(encryption). In Proceedings of the 17th Annual International Cryptology Conference on Advances in Cryptology CRYPTO '97, Springer-Verlag, pp. 165 -179.

[5]“Wikipedia”. http://en.wikipedia.org/wiki/ Signcryption, June 10, 2014

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

[7] Ram Shanmugam 1999. Elliptic curves and their applications to cryptography: An Introduction. Kluwer academic press.

[8] Lawrence C. Washington 2003. Elliptic Curves: Number Theory and Cryptography. CRC Press.

[9] Yuliang Zheng and Hideki Imai. “How to construct efficient signcryption schemes on elliptic curves”, Information Processing Letters, Volume 68 No.5, pp. 227 -233, 1998.

[10] Yiliang Han, Xiaoyuan Yang and Yupu Hu. 2004. Signcryption Based on Elliptic Curve and Its MultiParty Schemes. In roceedings of the 3rd international conference on Information security InfoSecu'04, pp.216-217.

[11] Ren-Junn Hwang, Chih-Hua Lai, and Feng-Fu Su, “An effcient signcryption scheme with forward secrecy based on elliptic curve”, Journal of Applied Mathematics and Computation, Volume 167 No.2, pp. 870 - 881, 2005.

[12] Mohsen Toorani and Ali Asghar Beheshti Shirazi. 2008. Cryptanalysis of an efficient signcryption scheme with forward secrecy based on elliptic curve. In Proceedings of International Conference on Computer and Electrical Engineering (ICCEE'08), pp. 428-432.

[13] Yiliang Han, Xiaoyuan Yang, Ping Wei, Yuming Wang, Yupu Hu, “ECGSC: Elliptic Curve Based Generalized Signcryption”, Ubiquitous Intelligence and Computing-Lecture Notes in Computer Science Volume 4159, 2006, pp 956-965.

[14] E.Mohamed and H. Elkamchouchi, “Elliptic Curve Signcryption with Encrypted Message Authentication and Forward Secrecy”, International Journal of Computer Science and Network Security, VOL.9 No.1, pp 395-398, 2009.

[15] Mohsen Toorani and Ali Asghar Beheshti Shirazi, “An elliptic curve-based signcryption scheme with forward secrecy”, Journal of Applied Sciences, Volume 9 No.6, pp. 1025 -1035, 2010.

[16] Esam A. A. A. Hagras, Doaa El-Saied, Dr. Hazem H. Aly, “A New Forward Secure Elliptic Curve Signcryption Key Management (FS-ECSKM) Scheme for Heterogeneous Wireless Sensor Networks”, International Journal of Computer Science and Technology, Volume 2 No 2, pp 19-23, 2011.

[17] Ramratan Ahirwal, Anjali Jain, Y. K. Jain, “Signcryption Scheme that Utilizes Elliptic Curve for both Encryption and Signature Generation”, International Journal of Computer Applications, Volume 62 No. 9, pp. 41-48, 2013.

[18] Sumanjit Das, Biswajit Samal, “An Elliptic Curve based Signcryption Protocol using Java”, International Journal of Computer Applications, Volume 66 No. 4, pp. 44-49, 2013.

[19] F. Amounas, H.Sadki and E.H. El Kinani, “An Efficient Signcryption Scheme based on The Elliptic Curve Discrete Logarithm Problem”, International Journal of Information & Network Security, Volume 2 No. 3, pp. 253-259, 2013.

[20] Suman Bala, Gaurav Sharma and Anil K. Verma, “An Improved Forward Secure Elliptic Curve Signcryption Key Management Scheme for Wireless Sensor Networks”, Lecture Notes in Electrical Engineering (Springer Link), Volume 215, 2013.