An Elliptic Curve-based Signcryption Scheme with Forward Secrecy for Encryption Authentication in Cloud Computing

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 cryptographic basic which all the while give both the capacity of digital signature and public key encryption in a distinct logical step. Elliptic curve cryptosystem (ECC) have as of late got huge consideration by research because of their low computational and communicational overhead.Elliptic curve cryptography (ECC) is the hardest computational issues, the elliptic curve discrete logarithm issue and elliptic curve Deffie-Hellman issue are the most solid cryptographic method in ECC. The upsides of ECC that it requires more limited key length contrasted with other public-key calculations. In this way, that its utilization in low-end frameworks, for example, brilliant cards in view of its effectiveness and restricted computational and communicational overhead. We present new signcryption plans dependent on elliptic curve cryptography. The security of proposed plans depends on elliptic bend discrete logarithmissue (ECDLP) and elliptic bend Diffie-Hellman issue (ECDHP). The proposed plans give different alluring security prerequisites like secrecy, credibility, non-renouncement and forward security just as picked ciphertext assault and unforgeability

Keywords*: Signcrytion, ECC, Forward secretary, Cloud Computing.*

I. Introduction

These days, the utilization of cloud based administrations for enormous scale is acquiring a growing interest. The National Institute of Standards and Technology (NIST) [1] characterizes the distributed computing as a model for empowering universal, helpful, on request network admittance to a common pool of configurable figuring assets. These assets can be capacity limits that are controlled, distributed and overseen by the Cloud Service Provider (CSP). Hence, by moving their information to the cloud, clients eliminate the weight of building and keeping a neighborhood stockpiling foundation. All things considered, they just need to pay their CSP for the assigned assets. Microsoft Windows Azure stockpiling administrations [2] what's more, Amazon's Simple Storage Service (S3) [3] are acceptable models. In fact, these suppliers offer to their customers the plausibility to store, recover and share information with other clients in a straightforward manner. Tragically, notwithstanding its benefits, distributed storage brings a few security issues. Information secrecy shows up as the greatest worry for clients of a distributed storage framework. Indeed, the customers' information are overseen out of their administration. Kamara and Lauter [4], and Chow et al. [5] concurred that scrambling re-appropriated information by the customer is a decent choice to alleviate such worries of information secrecy. Subsequently, the customer saves the decoding keys far from the cloud supplier. The secrecy provisioning turns out to be more unpredictable with adaptable information dividing between a gatherings of clients. It requires effective sharing of unscrambling keys between various approved clients. So that, solitary approved clients can

acquire the cleartext of information put away in the cloud.

In this paper, another elliptic bend based signcryption conspire is presented that all the while gives the traits of message confidentiality,authentication, integrity, unforgeability, non-repudiation,forward security, public obviousness, and forward mystery of message secrecy. It is a confirmed plan since it sends a certain verified key foundation.The security of proposed plans depends on elliptic bend discrete logarithm issue (ECDLP) and elliptic bend Diffie-Hellman issue (ECDHP). The proposed plans give different attractive security prerequisites like secrecy, authenticity, non-repudiationand just as picked ciphertext assault and unforgeability.

II. Forward Secrecy

A convention is said to give forward secret if the trade-off of long term keys doesn't bargain past meeting keys that have been set up before the com-guarantee of the drawn out key [6]. Forward mystery appears to have been instituted by Günther [7] regarding a personality based convention he proposed. Truth be told Günther utilized the term amazing forward mystery; anyway since the word 'awesome' has implications with genuine security which are not important here, we will utilize the more straightforward term in the same way as various different creators. It ought to be noticed that there is by all accounts a conflict in the meaning of forward mystery since we can discover a writing where forward mystery is planned to imply that a mysterious encryption key utilized in a meeting should be safely disposed of after the meeting to forestall an adversary from acquiring the encryption key in any capacity and listening in any future sessions ensured by a similar encryption key [8]. In this paper, nonetheless, we utilize just the previous meaning of forward mystery, which shows up more for the most part concurred one.We additionally note that there is a fairly comparative idea called forward security to address another meaning of losing long haul private keys [9]. A mark conspire with forward security shields clients from the danger of mark fraud in the event that their unique keys have been undermined. The fundamental plan to carry out forward security is to refresh the mark key itself every now and again to decrease the danger of key openness. This may contributes likewise to the forward mystery when the case the mark key is utilized for verification and key foundation also, in light of the fact that the restricted life span of the mark key decreases the danger of significant meeting key trade off down to the lifetime of the mark key. In any case, notwithstanding, forward security is certifiably not an adequate conditions for forward mystery thinking about that the divulgence of the mark key would bargain any meeting keys processed utilizing the mark key. All in all, on the off chance that we keep our attention on a specific long haul private key (anyway long it lives), at that point it is just forward mystery that shields the important meeting keys from the trade-off of the drawn out private key. In light of this, we contend that the fundamental characteristic of forward mystery is symmetrical to that of forward security. It ought to be seen, nonetheless, that there is by all accounts rather free differentiation, which reflects, as we have effectively depicted, the way that forward security might be viewed as a feeble alternative to advance mystery from a functional perspective.

In contrast to numerous different objectives of safety conventions, forward mystery may must be dealt with all the more essentially. Its importance in the genuine applications significantly shifts through the two points of correspondence types and client types. In the correspondences between a private client and a public business element, it is more the client than the business element that is worried about classification for the past communications, and consequently is more worried about forward mystery. Then again, forward mystery generally requires some extra calculations of key cryptography, and subsequently may be a very costly cryptographic assistance in certain sorts of interchanges, for instance, voice correspondences or message broadcasting in some worth added administrations.

III. Proposed Work:

All through this paper, X is the sender, Y is the receiver, and Z is the malignant attacker. Our proposed signcryption plot is described in the fallowing steps where a portion of its conveyed documentations are depicted in Figure 1. It comprises of three stages: *Initialization, Signcryption, and Confirmation.*The instatement stage incorporates choosing the space boundaries, producing the private/public keys, and getting an endorsement for the public key of every client. In signcryption stage, X signcrypts her message and sends it to Y. The confirmation stage is utilized just when any debate happens in which the appointed authority chooses whether X has sent the signcrypted message to Y or not.

X Signcryption

Verifiy of $Cert_B$ *and* PU_B
Choosing $r \in_R [1,n-1]$
$R = Rg = (x_R, y_R)$
$K = (r + \widetilde{x_R} PA_A) PU_B = (x_Y, y_K)$

$k = H(x_K || ID_A || y_K || ID_B)$
$C = E_k(M)$
$t = H_k(M ||x_R||ID_A ||y_R ||ID_B)$
$t\ PA_A - r(mod\ n)$

Notation:

ϵ_R	-	*Chosen Randomly*
M	-	*Plain Text*
C	-	*Cipher Text*
s	-	*Digital Signature*
H	-	*Hash function*
PU	-	*Public Key*
PA	-	*Private Key*
ID_x	-	*Identifier of x*
ID_y	-	*Identifier of y*

Initialization:

Domain parameters of the proposed conspire comprise of an appropriately chosen elliptic bend E characterized over a limited field Fq with the Weierstrass condition of the structure $y^2=x^3+ax + b$, and a base point G ϵ E(Fq) in which q is a huge indivisible number. To make the elliptic bend non-solitary, a, b ϵ Fq ought to fulfil $4a^3 + 27b^2 \neq 0(mod\ q)$ To prepare for little subgroup assaults, the point G ought to be of a superb request n, or proportionally $nG = O$and we ought to have$n>4$ ensure against other known assaults on unique classes of elliptic bends, n ought not gapq^i-1 for all $1 \leq i \leq V$ ($V = 20$)$n \neq q$ should be satisfied, and the curve must be not a singular. Keep in touch of of ECDLP to the Pollard-rho and Pohlig-Hellman algorithms), n must satisfy $n > 2^{160}$

The private keys of x and y are the arbitrarily selectedintegers $w_A, w_B \in [1, n-1]$.The comparing public keys are determined as $W_A = w_A G$ and $W_B = w_B G$. x and y are extraordinarily distinguished by the exceptional identifiers IDA and IDBrespectively. They additionally get the endorsements $Cert_A$ and $Cert_B$ from the Certificate Authority (CA) for their public keys W_A and W_B . On the off chance that CA isn't associated with the public key age that is by and large the case, it is important for CA to check that every substance truly has the comparing private key of its asserted public key. This can be refined by a zero-information verification. It ought to likewise be checked that the public keys have a place with the fundamental bunch. From this point forward, it is likewise expected that the members approach a real duplicate of the CA's public key, to utilize it with the end goal of endorsement approval. The cycle of endorsement approval incorporates

(a) Verifying the uprightness and legitimacy of the declaration by checking the CA's mark on the endorsement.
(b) Verifying that the declaration isn't terminated.
(c) Verifying that the declaration isn't denied.

Signcryption

x produces the signcrypted text (R, C, s) byfollowing the beneath steps:

(1) Checks the legitimacy of CertB uses for W_B
(2) $r \in [1, n-1]$
(3) Computes $R = rG = (x_R , y_R)$.
(4) $K=(r+\tilde{x}_R w_A)W_B = (x_K, y_K)$ where $\tilde{x}_R = 2^{\lceil f/2 \rceil} + (x_R \bmod 2^{\lceil f/2 \rceil})$ in which $f = \lceil \log_2 n \rceil + 1$ is the bit length of encryption as k = H (x_K || ID_A || y_K || ID_B) in which H is used to generate the number of secret key for symmetric encryption.
(5) the ciphertext as $C = E_k (M)$
(6) the ciphertext as $C = E_k (M)$ $s = tw_A - r(mod\ n)$ in which $t = HMAC_k (M || x_R || ID_A || y_R || ID_B)$
(7) Sends the signcrypted as (R, C, s) to

Confirmation:

At the point when y guarantees that he has gotten the signcrypted text (R, C, s) from x and a debate happens, the confided in outsider (confirmation) needs y to give (R, C, s, M , k) . Weave is essentially equipped for removing M and k from the recently saved (R, C, s). The adjudicator follows the accompanying strides to mediate on what y claims.

(1)Checks the legitimacy of Cert An and utilizes it for checking W_A .
(2)Verifies $M = D_k (C)$. On the off chance that this isn't the situation, y isn't right
(3) Computes $t = HMAC_k (M || x_R || ID_A || y_R || ID_B)$
(4) Verifies the mark of x by checking the $sG + R = tW_A$ condition. In the event that this condition isn't fulfilled, y isn't right. Something else, x has sent (R, C, s) to y.

Security of Proposed System

The proposed conspire gives a wide assortment of safety credits as it is portrayed in Table 1. The drawn out private key of x is engaged with the meeting key age so the meeting key has versatility to divulgence of mystery esteem r. Legitimacy confirmation of the static

and fleeting public keys, and the endorsements are deliberately considered so a few sorts of assaults are frustrated. The proposed plot gets its security from a few segments:

1) The security ascribes of the meeting key foundation,

2) The security ascribes of the authentications,

3) The security ascribes of conveyed block figure, single direction hash capacity, and HMAC,

4) Intractability of ECDLP because of the chose space boundaries.

The proposed plot conveys a solid key foundation. Up to this point, many confirmed key trade conventions are presented, every one of them having their own issues and restrictions. The MQV conventions are conceivably the most productive of all known verified Diffie-Hellman conventions that utilization public-key confirmation. The MQV has been generally normalized, and has been chosen by the NSA to secure the grouped data of USA government. In spite of the fact that HMQV attempts to ruin the MQV's weaknesses by fundamentally presenting an extra hash work, it additionally has a few weaknesses. The elliptic bend based meeting key foundation interaction of the proposed plot doesn't by and large relate with that of and however it attempts to improve and match such thoughts for its own case. The meeting key foundation some portions of the proposed conspire has itself the accompanying security credits:

1. Known session key security: Every execution of the convention brings about a special meeting key. The meeting key will contrast for various meetings on the grounds that the transient irregular number r is presented in the meeting key foundation measure so the trade-off of one meeting key doesn't bargain the keys of different meetings. Since the private keys and identifiers of the two members are associated with the meeting key induction work, it will contrast regardless of whether X utilizes a similar arbitrary number r for signcrypting similar directive for various beneficiaries.

2. Resilience to the Unknown-Key Share assault: In a UKS assault, two gatherings process a similar meeting key yet have various perspectives on their friends in the key trade. This assault is doable when a key trade convention neglects to give anvalidated restricting between the meeting key and identifiers of the legitimate elements. In the proposed plot, legitimacy of authentications and furthermore the static and vaporous public keys are confirmed. The UKS assault is defeated on the grounds that the identifiers of both x and y are expressly associated with the meeting key inference work.

3. Resilience to the Key Compromise assault of stays secure. Under recalcitrance of the ECDLP, the KCI assault is impeded in the proposed plot. An enemy that could acquire w_A , should track down the comparing r

4. R to reason the relating meeting key that is by and large in store of tackling the ECDLP. Impersonation (KCI) assault: In a KCI Mallory who could get the private key of X (however doesn't have the private key y) attempts to mimic another legitimate gathering y to X. Protection from the KCI assault is a significant component sinceas long as Mallory can't effectively control X, any meeting that is set up by X

Table 1. The attributes of different type of signcryption

Signcryption Schemes	Confidentiality	Integrity	Unforgeability	Public Verifiability	Forward Secrecy
(Zheng, 1997)	Yes	Yes	Yes	No	No
(Jung et al., 2001)	Yes	Yes	Yes	No	Yes
(Zheng and Imai, 1998)	Yes	Yes	Yes	No	No
(Bao and Deng, 1998)	Yes	Yes	Yes	Yes	No
(Gamage et al., 1999)	Yes	Yes	Yes	Yes	No
(Han et al., 2004)	No [a]	No [a]	No [a]	Yes	No
(Hwang et al., 2005)	No [b]	No [b]	No [b]	Yes	No

Conclusion:

Our proposed plans dependent on ECDLP and ECDHP at the same time gives message secrecy, unforgeability, non-renouncement, honesty, validation also, forward security. The proposed plans accomplish the security properties with a saving in computational expense contrasted with the customary mark the encryption conspire which makes the new plan more fitting for climate with restricted power. At long last, the proposed plans have low computational and correspondence cost in this way, can be applied to a PDA climate all the more proficiently.In ID-based signcryption, a third is utilized to produce the private key of clients called a private key generator (PKG). There is an issue of key escrow in ID-based signcryption that key is held bonded, or put away, by an outsider. Thus, to keep away from this issue the proposed works can be plan in certificateless signcryption.

REFERENCE

[1] P. Mell and T. Grance, "The NIST Definition of Cloud Computing," National Institute of Standards and Technology, vol. 53, no. 6, p. 50, 2009. [Online]. Available: http://csrc.nist. gov/groups/SNS/cloud-computing/cloud-def-v15.doc

[2] D. Chappell, "Introducing the Windows azure platform," October, vol. 30, no. October, p. 2010, 2010. [Online]. Available: http://download.microsoft.com/download/C/0/ 2/C02C4D26-0472-4688AC13-199EA321135E/Introduce_ Azure_Services_Platform_1_2.pdf

[3] Amazon, "Amazon simple storage service (amazon s3)." [Online]. Available: http://aws.amazon.com/s3/

[4] S. Kamara and K. Lauter, "Cryptographic cloud storage," in Proceedings of the 14th international conference on Financial cryptograpy and data security, ser. FC'10. Berlin, Heidelberg: Springer-Verlag, 2010, pp. 136–149. [Online]. Available: http: //dl.acm.org/citation.cfm?id=1894863.1894876

[5] R. Chow, P. Golle, M. Jakobsson, E. Shi, J. Staddon, R. Masuoka, and J. Molina, "Controlling data in the cloud: outsourcing computation without outsourcing control," in Proceedings of the 2009 ACM workshop on Cloud computing security. ACM, 2009, pp. 85–90.

[6]A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, Handbook of Applied Cryptography, CRC Press, 1997, p. 496.

[7] C. Günther, "An Identity-based Key-exchange Protocol", Advances in Cryptology Eurocrypt'89, Springer-Verlag, 1990, pp. 29-37.

[8]H. Abelson et al., "The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption",A Report by an Ad Hoc Group of Cryptographers and Computer Scientists, 1998. Available from http://www.cdt.org/crypto/risks98/

[9] M. Bellare and S.K. Miner, "A Forward-Secure Digital Signature Scheme", Advances in Cryptology Crypto'99, Springer-Verlag, 1999.

[10] Antipa, A., D. Brown, A. Menezes, R. Struik and S. Vanstone, 2003. Validation of elliptic curve public keys. In Proceedings of the 6th International Workshop on theory and Practice in Public Key Cryptography: Public Key Cryptography (PKC'03), London, UK, 6-8 January 2003. LNCS 2567,

[11]Springer-Verlag, Berlin/Heidelberg, pp.211-223. DOI: 10.1007/3-540- 36288-6_16.

[12] Bao, F. and R.H. Deng, 1998. A signcryption scheme with signature directly verifiable by public key. In Proceedings of Advances in Cryptology -

PKC'98, LNCS 1431, Springer-Verlag, Berlin, 1998, pp.55-59.

[13] Elkeelany, O., M.M. Matalgah, K.P. Sheikh, M. Thaker,G. Chaudhry, D. Medhi, and J. Qaddour, 2002. Performance Analysis of IPSec Protocol: Encryption and Authentication. In Proceedings of 2002 IEEE International Conference on Communications (ICC'02), Vol.2, pp.1164-1168, 28 April - 2 May 2002, New York City, USA.

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

[15] Han, Y., X. Yang and Y. Hu, 2004. Signcryption Based on Elliptic Curve and Its Multi-Party Schemes. 3rd ACM International Conference on Information Security (InfoSecu'04), 14-16 November 2004, Shanghai, China. ACM International Conference Proceeding Series, Vol.85, pp.216-217, NY, USA, 2004.

[16] Hankerson, D., A. Menezes and S. Vanstone (2004). Guide to Elliptic Curve Cryptography, 1st edition. Springer-Verlag, New York. ISBN: 0-387-95273-X.

[17] Hwang, R.-J., C.-H. Lai and F.-F. Su, 2005. Anefficient signcryption scheme with forward secrecy based on elliptic curve. Journal of Applied Mathematics and Computation (Elsevier Inc.), 167 (2): 870-881, 2005.

[18] Jung, H.Y., K.S. Chang, D.H. Lee and J.I. Lim, 2001. Signcryption schemes with forward secrecy. In Proceeding of Information Security Application-WISA 2001, Seoul, Korea, 13-14 September 2001, pp.403-475.

[19] Kaliski, B., 2001. An unknown key-share attack on the MQV key agreement protocol. ACM Transactions on Information and System Security (TISSEC), 4 (3): 275-288, August 2001, NY, USA.

[20] Krawczyk, H., 2005. HMQV: A high-performance secure Diffie-Hellman protocol. In Proceedings of Advances in Cryptology – CRYPTO'05. Springer- Verlag, Berlin, LNCS 3621, Nov. 2005, pp.546-566.

[21] Law, L., A. Menezes, M. Qu, J. Solinas and S. Vanstone, 2003. An efficient Protocol for Authenticated Key Agreement. Journal of Designs, Codes and Cryptography, 28:119-134, March 2003.

[22] Menezes, A., 2005. Another Look at HMQV. Nov. 2005. Available at: http://eprint.iacr.org/2005/205.pdf

[23] Menezes, A. and B. Ustaoglu, 2006. On the Importance of Public-Key Validation in the MQV and HMQV Key Agreement Protocols. 7th International Conference on Cryptology in India, Kolkata, India, 11-13 December 2006. In Proceedings of Advances in Cryptology– INDOCRYPT'06, Springer-Verlag, Berlin, LNCS 4329, 2006, pp.133-147

[24] Myers, M., R. Ankney, A. Malpani, S. Galperin and C. Adams, 1999. X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP. RFC 2560, June1999.

[25] NIST (National Institute of Standards and Technology), 2007. Special Publication 800-56A, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography. March 2007.

[26] NIST (National Institute of Standards and Technology), 2000. Digital Signature Standard. Federal Information Processing Standards Publication (FIPS) 186-2. January 2000.

[27] Pinkas, D. and R. Housley, 2002. Delegated Path Validation and Delegated Path Discovery Protocol Requirements. RFC 3379, Sep. 2002.

[28] Toorani, M. and A.A. Beheshti Shirazi, 2010. Cryptanalysis of an elliptic curve-based signcryption scheme. International Journal of Network Security, Vol.10, No.1, Jan 2010, pp.51-56.

[29] Tso, R., T. Okamoto and E. Okamoto, 2007. An Improved Signcryption Scheme and Its Variation. In Proceedings of 4th IEEE International Conference on Information Technology (ITNG'07), April 2007, pp.772-778.

[30]Wagstaff, S.S. (2003). Cryptanalysis of Number Theoretic Ciphers, 1st edition. Chapman & Hall/CRC. ISBN: 1-58488-153-4.

[31] Zeilenga, K., Lightweight Directory Access Protocol (LDAP): Schema Definitions for X.509 Certificates. RFC 4523, June 2006

[32] Rosen, K.H. (1988). Elementary Number Theory and Its Applications. 2nd edition, Addison-Wesley, Massachusetts. ISBN: 0201119587.

[33] Satizabál, C., R. Martínez-Peláez, J. Forné and F. Rico- Novella, 2007. Reducing the Computational Cost of Certification Path Validation in Mobile Payment. In Proceedings of Advances in Cryptology– EUROPKI'07, Springer-Verlag, Berlin, LNCS 4582, June 2007, pp.280-296

[34] Strangio, M.A., 2006. On the Resilience of Key Agreement Protocols to Key Compromise Impersonation. Advances in Cryptology– EUROPKI'06, Springer-Verlag, Berlin, LNCS 4043, 2006, pp.233- 247. DOI: 10.1007/11774716_19

[35] Zheng, Y., 1997. Digital signcryption or how to achieve Cost (Signature & Encryption) << Cost

(Signature) + Cost (Encryption). In Proceedings of the 17th International Conference on Advances in Cryptology– CRYPTO'97, 17-21 August 1997. Springer-Verlag,Berlin, LNCS 1294, 1997, pp.165-179.

S[36] Zheng, Y. and H. Imai, 1998. How to construct efficient signcryption schemes on elliptic curves. Information Processing Letters, 68: 227-233, Dec. 1998. Elsevier Inc., Amsterdam, Netherlands

[37] Stinson, D.R. (2006). Cryptography-Theory and Practice. 3rd edition. Chapman & Hall/CRC. ISBN: 1-58488-508-4.

Toorani, M. and A.A. Beheshti Shirazi, 2008. Cryptanalysis of an efficient signcryption scheme with forward secrecy based on elliptic curve. Proceedings of 2008 International Conference on Computer and Electrical Engineering (ICCEE'08), 20-22 December 2008, Phuket, Thailand, pp.428-432.