International Journal of Computer

(IJC)

ISSN 2307-4523 (Print & Online)

http://ijcjournal.org/

Proxy Promised Signcrypion Scheme Based on Elliptic Curve Crypto System

Insaf Ullah [a]*, Noor Ul Amin [b], Arif Iqbal Umar [c], Hizbullah khattak [d]

[a,b,c,d] *Department of Information technology Hazara University, Mansehra, KP, Pakistan.*

[a] *Email: insafktk@gmail.com*

[b] *Email: namin@hu.edu.pk*

[c] *Email: arifiqbalumar@yahoo.com*

[d] *Email: hizbullahkhattak@yahoo.com*

Abstract

With the rapid growth in internet technology anonymity, repudiation and smacking the contents of messages are required for illegal businesses such as money laundering etc. In this paper we design and analyze a proxy promised signcrypion scheme based on elliptic curve cryptosystem. In this system the sender/original signer can give the authority of signcrypion to another entity namely proxy signcrypter and he generates promised signcryptext on the place of sender. The scheme is accomplished aim to improve the previous crypto-systems, due to the elliptic curve small system parameter, small public key certificates, faster implementation, low power consumption and small hardware processor requirements. This ECC based scheme provides high security and efficiency.

Keywords: proxy signature; promised signature; proxy signcrypion; promised signcrypion; elliptic curve.

1. Introduction

Dispatching and receiving Data/information through harm full channel needs safety. Data is the necessary part of any business organization. Now to safe data we require confidentiality which is provided by encryption algorithm. Authenticity is ensured by digital signature algorithm and integrity by one way hash function.

---

* Corresponding author.

Before sending data the sender first encrypt data and then calculate signature of cipher text this method is called signature then encryption.it is time consuming and required more machine cycle.to remove these limitations Zheng coin a word signcrypion [1]. It combines both digital signature and encryption in a single step with low computation and communication cost. But in some situation we collectively required rights delegations and deniability properties. For delegation of rights Membo introduce proxy signature scheme [2]. It enable the sender of a message to give the signing authority to another signer called proxy and he sign a message on behalf of sender.gamage extended proxy signature into proxy signcrypion [3],which combine both proxy signature and encryption in single logical step. For deniability Dwork proposed a deniable authentication [4]. It enables the sender to communicate secret with receiver without disclosing his privacy. Shin convert deniable authentication into promised Signcrypion which provides the property of anonymity and deniability [5]. According to promise property anyone can generate the promise Signcryptext but third party cannot prove the source of Signcryptext.in some situation we required deniability, anonymity and delegation of rights at the same time. Since there was no scheme to achieves these all property at once. For this we design a new scheme which fulfilling the above requirements called proxy promised signcrypion based on elliptic curve.

2. Related work

Zhang and Dong's [6] proposed a new scheme called public verifiable proxy signcrypion. The design scheme meets the security properties of public verifiability and forward secrecy. H. Elkamchouchi and his colleagues [7] introduce a proxy signcrypion scheme which work on the bases of Shin digital signature algorithm verifiable signcrypion. It ensures the security requirements confidentiality, authenticity and public verifiability. H. Elkamchouchi and his colleagues [8] contribute a proxy signcrypion for delegation of rights.it meet strong security because of it based on hard problems. Hearn and Jian [9] introduce a cryptographic base scheme supporting by PGP and S/MIME. The proposed scheme meet the property of denaiability.in proposed scheme only the intended receiver can validate the contents of message. The drawback of a proposed scheme is it needs more time for computation. Hwang and Jen [10] proposed Non-Interactive Fair Deniable Authentication Protocols with Indistinguishable Confidentiality and Anonymity. The proposed scheme realizes the security desires such as message confidentiality, anonymity and protection. The main disadvantage of the scheme is it is very time consuming. Mario and his colleagues [11] proposed a forwardly secure deniable authentication scheme. It provides the repudiation property. The limitation of this scheme is high computation cost. Chun hua and his colleagues [12] proposed a scheme that contributes the security models of certificate less deniable authentication protocol plus deniable authentication protocol work with certificate less cryptography.

3. Proposed scheme

This section presents our newly design proxy promissed signcryption scheme based on the hardeness of elliptic curve discrete logrithm problem.In this scheme the original signcrypter tranfer there sigcrypting ability to another person called proxy and the proxy signcrypter calculate the signcrypted cryptograme on the behalf of sender/original signcrypter.it contains key generation phase,sender/original signcrypter,proxy verification,proxy promised signcryption and unsigncryption phase.

3.1. Key Generation

Sender Choice randomely x_a where $0<x_a<p$ as the private key and also determine there public key Y_a: $Y_a = x_a G$

Proxy Choice randomely x_p where $0<x_p<p$ as the private key and also determine there public key Y_p: $Y_p = x_p G$

Reciver Choice randomely x_b where $0<x_b<p$ as the private key and also determine there public key Y_b: $Y_b = x_b G$

3.2. Sender/Original Signcrpter

In this phase the original signer deligates the sigcrpted authority to another signcrypter called proxy.

- Randomly chose R
- Compute $A = R.G$
- Compute$\lambda = \big(R - x_a.h(A, m_w)\big) mod\ p$

Send (A, λ, m_w) to proxy

3.3. Proxy verification

In this phase the proxy verify that the message from original signcrypter or not.

- Compute $A' = \lambda.G + h(A, m_w).Y_a$

3.4. Proxy Promised Signcrypion

In this phase the proxy generate promised signcrypion of a message and then send to verifier.

- Randomly generate two integer's value a and b from [1……p-1]
- Computes $\upsilon = h_1(\alpha.G||\text{m})$
- Computes $s' = \big(a + \upsilon.x_p\big) mod q$
- Computes $S = s'.G\ modq$
- Computes key $K = h_2(s'.Y_b)$
- Gain cipher text using this algorithm $C = E_k(m||\text{b})$
- Send (C, υ, S)

3.5. Promise Un-Signcrypion

- Compute key $K = h_2(X_b.S)$

- Recovers the plaintext m using the same symmetric algorithm $m||\mathrm{b} = D_k(C)$
- Compute $\gamma = S - \upsilon Y_p$
- Compute $\upsilon' = h_1(\upsilon||\mathrm{m})$
- Accepts message m if $\upsilon = \upsilon'$

4. Security analysis of proposed proxy promised signcrypion scheme

The design scheme meet the security properties such as confidentiality, integrity of the warrant, unforgeability of a warrant, integrity of a message, authentication of a message, Deniability, Deniability, Intended Receive and Sender anonymity.

4.1. Confidentiality

The scheme ensures the property of confidentiality. If the attacker wants to decrypt the cipher text and get original contents of message. For this he must first get the secret session key$K = h_2(s'.Y_b)$.If he calculates key K, then it should be going after the following cases.

Case 1: the eavesdropper may effortlessly construct k from (1). For this the attacker wants $s'$from (2).now the construct s' is equal to solve ECDLP (elliptic curve discrete logarithm problem) which is computationally hard for eavesdropper.

$$K = h_2(s'.Y_b) \qquad (1)$$

$$S = s'.G \qquad (2)$$

Case 2: the attacker can easily calculate s' using (3).for this it required the randomly generated number α from (4) and the proxy private key x_p from (5).now it is equal to solve two unknown variable from same equation which is computationally infeasible for attacker.

$$s' = \left(a + \upsilon.x_p\right) \qquad (3)$$

$$\upsilon = h_1(a.G||\mathrm{m}) \qquad (4)$$

$$Y_p = x_p.G \qquad (5)$$

4.2. Warrant Integrity

The design scheme also ensures the integrity of warrant. Before sending the sender calculate the one way hash function of a warrant message$h(A, m_w)$, sends to proxy .when attacker wants to change m_w as $m_w'.let$ $h'(A,\ m_w')$ then he must calculate λ using (6) for this it needs the sender private key x_a of sender from Eq. (7) and R from Eq. (8) . Generating x_a and d is infeasible for attacker and equivalent to solve two HECDLP .proxy can use the Eq. (9) for integrity if it hold equality then the message is not change otherwise change.

$$\lambda = \left(R - x_a . h(A, m_w)\right) \qquad (6)$$

$$Y_a = x_a . G \qquad (7)$$

$$A = R . G \qquad (8)$$

$$A = \lambda . D + h(A, m_w) . Y_a \qquad (9)$$

4.3. Warrant unforgeability

Our proposed scheme meets the property of warrant unforgeability. The attacker can calculate the valid signature for warrant using (6) .For this he required R and sender private key x_a. Now finding of these two is hard and computationally infeasible for attacker.

4.4. Massage Integrity

In our proposed proxy promised signcrypion before sending the proxy first compute collision resistant hash function of message$v = h_1(a.G||\mathrm{m})$ and then refer to recipient. If the attacker wants to convert cipher text c into c' then it must change m into m'.but we use a collision resistant one way hash function which is computational infeasible for attacker.

4.5. Authenticity

The proposed scheme also meets the property of authentication. In design scheme when the attacker wants to compute a forge signature for a message then he first calculate a from (4), also the private key of a proxy x_p $from$ (5). Now it equals to finding two unknown values from same equation is computationally hard for attacker. The receiver checks the integrity of message using (10).

$$Y_p = s' . G - a . \frac{G}{v} \qquad (10)$$

4.6. Deniability

The design proxy promised signcrypion provides the property of repudiation. Because anyone uses the private key of receiver can generate the forge signature and cipher text. Eavesdropper can easily generate same signature and cipher text c'using the following steps.

- Attacker Compute K'=$H_2(s' . X_b)$.
- And Calculates $C' = E_k(m||\mathrm{b}')$.
- Then generate the forge promise Signcrypion of message m is (C', γ', S') where $v' = S' - v' Y_a$. And $K = K'$ so any one can generate the promised signcryptext of (C, v, S) which is lead to the repudiation

property.

4.7. Intended Receive

In our proposed scheme only the intended receiver can verify the validity of a message using following equations.

$$S = \upsilon + \upsilon Y_p \qquad (11)$$

$$\gamma = h(\upsilon) = h(\upsilon') \quad (12)$$

$$h(\upsilon||\mathrm{m}) = \mathrm{h}(\upsilon'||\mathrm{m}) \quad (13)$$

4.8. Sender anonymity

To know the source of message the attacker generates a forge promise (υ', S') of (υ, S) then randomly choose a bit string C' and then forge promise signcryptext C, υ, S .Thus one the sender and receiver can decrypt and validate signcryptext according to the promise property. But eavesdropper cannot validate using υ', S'.

5. Conclusion

This paper presents the new scheme called proxy promised signcrypion. The security of a scheme realizes on bases of a hardiness of elliptic curve cryptosystem. The scheme is suitable for constrained environment devices because of elliptic curve which has the property of rapid implementations, having little public key, shorter parameter, small power consumption and small hardware processing requirements.

References

[1]. Y. Zheng, “Digital Signcryption or How to Achieve Cost (Signature and Encryption) Cost (Signature) + Cost (Encryption),” Advances in Cryptology, LNCS, Vol. 1294. Springer-Verlag, pp.165–179, 1997.

[2]. M. Mambo, K. Usuda, and E. Okamoto, “Proxy signatures for delegating signing operation,” Proc. 3rd ACM Conf. Comput. Commun. Secur. - CCS ’96, pp. 48–57, 1996.

[3]. C. Gamage, J. Leiwo, and Y. Zheng, “An Efficient Scheme for Secure Message Transmission using Proxy-Signcryption,” in Proceedings of the 22nd Australasian Computer Science Conference ,pp.420-431, Springer,1999.

[4]. Dwork, C., Naor, M., & Sahai, “Concurrent zero-knowledge”. In Proceedings of the thirtieth annual ACM symposium on Theory of computing (pp. 409-418). ACM, 1998.

[5]. Hwang, Shin-Jia, and Yun-Hao Sung. "Confidential deniable authentication using promised Signcryption." Journal of Systems and Software 84, no. 10 (2011): 1652-1659.

[6]. Z. Zhang, “ A New publicly verifiable proxy signcryption scheme”, In Progress on Cryptography2004).

[7]. D. H. Elkamshoushy (2006) New proxy signcryption scheme with DSA verifier, Natl. Radio Sci. Conf. NRSC, Proc., no. Nrsc.

[8]. Elkamchouchi and his colleagues ,“a new efficient strong proxy Signcryption scheme based on a combination of hard problems”, IEEE International Conference on Systems, Man and Cybernetics, 2009.

[9]. Hwang, S. J., & Chi, J. F. , “Non-Interactive Fair Deniable Authentication Protocols with Indistinguishable Confidentiality and Anonymity”. Journal of Applied Science and Engineering, 16(3), 305-318,2013.

[10]. Harn, L., & Ren, J, “ Design of fully deniable authentication service for e-mail applications”. Communications Letters, IEEE, 12(3), 219-221, 2008.

[11]. Hwang, S. J., & Chi, J. F, “Non-Interactive Fair Deniable Authentication Protocols with Indistinguishable Confidentiality and Anonymity”. Journal of Applied Science and Engineering, 16(3), 305-318, 2013.

[12]. Di Raimondo, M., & Gennaro, R, “New approaches for deniable authentication”. Journal of cryptology, 22(4), 572-615,2009.

[13]. Jin, C., Xu, C., Zhang, X., Xie, Q., & Li, F. (2013). A novel certificateless deniable authentication protocol. IACR Cryptology ePrint Archive, 2013, 414.