Volume 4 Issue 1 July 2016 ISSN: 2321 – 788X

A SURVEY ON SIGNCRYPTION SCHEMES IN CCA AND CMA

N.P.Navena[1] and Dr.M. Ramakrishnan[2]

[1]Department of Computer Application, School of Information Technology, Madurai Kamaraj University, Madurai

[2]Head, Department of Computer Application, School of Information Technology, Madurai Kamaraj University, Madurai

Abstract

This paper survey the literature study on Chosen Ciphertext Attack (CCA) and Chosen Message Attack (CMA) on various signcryption schemes. Signcryption is a new paradigm in public key cryptography that simultaneously fulfils both the functions of digital signature and public key encryption in a logically single step and with a cost significantly lower than that required by the traditional "signature then encryption" approach. Signcryption schemes like ID based, Certificateless and generalized signcryption must provide the information security against CCA and CMA. To acquire CCA security in confidentiality and CMA security in unforgeability, it should be strengthened against attack. The main objective of this paper is to conduct study on various security models of different signcryption schemes and their security proof under CCA and CMA.

Keywords: *Signcryption, ID based Signcryption, Certificateless Signcryption, CCA, CMA*

Introduction

Cryptography is the best way to secure the information form attacks. A secured communication of information has been proven and this can be achieved by various cryptographic primitives like public key cryptography, private key cryptography, Digital Signature and so on. A set of cryptographic primitives used to provide information security services. A basic security services are should provide Confidentiality, Integrity, Unforgeability and Non-repudiation. Confidentiality is keeping the information secret from who are all unauthorized. Integrity is certifying that information has not been altered by unauthorized. Unforgeability is the guarantee that the communication with authorized sender. Non-Repudiation is to proving the sender has sent the signcrypted text.

Signcryption is a cryptographic primitive that proposed by Zheng in 1997 that simultaneously performs the functions of both encryption and digital signature, which is more efficient than the traditional signature then encryption [18]. Signcryption is a useful cryptographic primitive that achieves confidentiality and unforgeability in an efficient manner.

Signcryption schemes like ID based, Certificateless, Generalized and aggregate signcryption schemes must provide the information security against attacks like Chosen Ciphertext Attack (CCA), Chosen Message Attack (CMA), and Chosen Plaintext Attack (CPA). In a estabilished Public key cryptography (PKC), any user communicate with othersmust

obtain their public key that associated with owner certificate, which is a signature that issued by the trusted.

Certificate Authority (CA) that is needed to guarantee the relationship between the public key and the identity of theuser. This method has the problem like computational cost and certificate management problems.

Shamir[14] first introduced the concept ID based cryptography (ID-PKC) in 1984, ID-PKC can eliminate the need of certificates and the user can directly generate the public key by using email address, IP address or any other related identity information, but it requires a trusted third party called Key Generation Center (KGC) generate the user's Private key. Unfortunately, key escrow problem happened in identity based cryptography, that is, KGC knows the private key to decrypt the cipher text and get the message. In 2003, Al-Riyami and Paterson [1] proposed a new cryptographic primitive, certificatelesspublic key cryptosystem,which avoid the key escrow problem and certificate management that occurs in ID-PKC.

The ID based signcryption scheme was proposed by Malone-Lee [10] in 2002. Many ID based signcryption schemes have been proposed since then, adopting many different strategies, thereby reducing computational cost and also reducing the ciphertext size. Certificateless signcryption scheme was proposed by Barbosa and Frashim [2] in 2008. It is the main purpose to solve the key escrow that inherited from IBC without use of the traditional PKC.

Generalized signcryption is differ from traditional signcryption that is an adaptive primitive which achieves both Confidentiality and authenticity in a defined structureGeneralized signcryption schemes are provide the functions of signature, encryption and signcryption which will solve problems that happen in embedded systems and wireless sensor networks [8]. Further so many combined generalized signcryption schemes are effective to solve problems against the attacks.

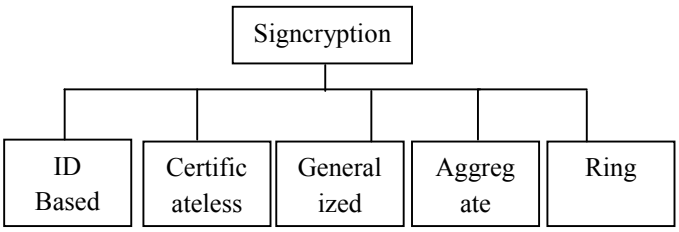

Figure 1 An Overview of Signcryption Schemes

Signcryption schemes are mainly focus on providing the information security against the Choosen Ciphertext Attack (CCA) and Choosen Message Attack (CMA). Chosen Cipher-text Attack (CCA) may be adaptive or non-adaptive. In a non adaptive CCA or Lunchtime

attack (CCA1), the attacker may do not use the decrypted plaintext to inform their choice for more ciphertext. In a adaptive chosen cipher text attack (CCA2), the attacker make the cipher text choice for adaptively that is depending on the prior decryption results. According to mathematical model security against the adaptive chosen ciphertext attack is represented as Indistinguishable against Chosen Ciphertext Attack (IND – CCA2). Chosen Message Attack (CMA), the attacker first learns signatures on messages of the attacker's choice to recognize the decrypted message by existentially unforgeable against adaptive chosen message attacks.

The Main goal of this paper is to provide a proper analysis of signcryption schemes in standard model against the attacks like IND-CCA2 and EUF-CMA by comparing the schemes.

Background

The basic security needs for a signcryption scheme are 'Message Confidentiality' and 'Non-repudiation'. Message Confidentiality means that no adversary can learn the message in the signcrypted text. We say that a signcryption scheme offers Non-repudiation if it prevents the sender of a signcrypted text from repudiating his signature. In other words, without the possession of the full private key of a sender, nobody can generate valid signcrypted texts on behalf of the sender.Precise definitions of Message Confidentiality and Non-repudiation are defined using security models.

Encryption schemes meeting strong notions of security typically introduce redundancy into their ciphertexts, and as a consequence ciphertexts may be deemed invalid during decryption. A scheme's correctness ensures that honestly generated ciphertexts will always decrypt correctly, hence we expect decryption to 'fail' only for ciphertexts that are corrupted during transmission or are adversarially generated. Semantic secure against chosen message attacksis widely believed as the correct security level for message authendication signature scheme. Encryption scheme andsignature scheme are combined to prove the security in the CCA and CMA by the security game. The Signcryption schemes considered by security methods this result requirements that part of the public key be specific to the encryption scheme and that anotherpart of it be specific to the signature scheme.

ID Based Signcryption Scheme

A Signcryption scheme is secure only if confidentiality and unforgeability should satisfy the properties. ID based signcryption based on the ID based cryptography introduced by Shamir[14] based on user's identity such as phone number or email address as public key. Malone lee[10] proposed the ID based signcryption based on the random oracle model. Then various ID based signcryption scheme models are proposed. The ID based signcryption

scheme uses four algorithms: Setup, Extract, Signcrypt and Unsigncrypt. The Functions of these

- **Setup**On Input security parameter k, Setup is used by the TA to generate the global parameters. Among the parameters produced by setup is a key QTAthat is made public. There is also corresponding master key t that is kept secret.
- **Extract**Given on input of an ID representing the identity, TA uses Extract to generate the corresponding master key Srdwhich gives the ID.
- **Signcrypt**IDasend a message m to IDbit generates appropriate ciphertext σ using Signcrypt. Signcrypt takes as input IDa, IDb and m to produce a signature. The message space is {0,1}nfor some n€ N.
- **Unsigncrypt**IDb has received a ciphertext σ from IDa, then Unsigncrypt to decrypt ciphertext into plaintext. Unsigncrypt takes IDa, SIDb and σ to return a message m or invalid ciphertext ±.

Consistency constraint that if

$$\sigma \leftarrow Signcrypt(S_{ID_a}, ID_b, \mathrm{m}) \text{ then}$$

$$m \leftarrow Unsigncrypt(ID_a, S_{ID_b}, \sigma).$$

ID based signcryption scheme in the standard model are proposed by the yu et al, and the semantic security confidentiality under the Decisional Bilinear Diffie-Hellmanproblem (DBDH) and its unforgeability under the Computational Diffie–Hellman assumption. But it was shown to unsecure of CCA2 and CMA in Bo Zhang and Zhang et al. Zhang et al [21] proposed signcryption scheme in the standard model that achieves the CMA but insecure in CCA2. Many such schemes were proposed butwhich later shown to be insecure in the models. Zhang [22] Security notions based on DBDH but both confidentiality and unforgeability are insecured that proved in the later schemes.

Table 1 ID Based Signcryption Schemes in Standard Model

Scheme	Confidentiality	Unforgeability	Type of Attack
Yu et al.	IND-CCA2	SUF-CMA	IND-CCA2 and SUF-CMA insecure
Jin et al.	IND-CCA2	EUF-CMA	IND-CCA2 and EUF-CMA insecure
Zhang	IND-CCA2	SUF-CMA	IND-CCA2 insecure
Li et al.	IND-CCA2	EUF-CMA	IND-CCA2 and EUF-CMA insecure

IND-CCA2 - Indistinguishability under Adaptive Chosen Ciphertext Attack
EUF-CMA - Existential Unforgeability under Chosen Message Attack
SUF-CMA - Strong Existential Unforgeability under Chosen Message Attack

Selvi et al [15] defined the security notions for the identity based signcryption that semantically secure in indistinguishability adaptive chosen ciphertext attacks, IND-IBSC-CCA2 and existentially unforgeable against adaptive chosen messages attacks (EUF-IBSC-CMA). This method achieves the security of getting a provably secure scheme by the combination ofan ID based signature scheme and an ID based encryption scheme both in the standard model. Also shown thatLi et al's schemes [11] are not secure in the standard model. In 2012, Selvi et al. [15] presented the firstprovably secure ID based signcryption scheme in the standard model. This scheme satis_ed the strongest notions ofsecurity available for the ID based signcryption schemes.

Later Li et al[11] discussed about ID based signcryption scheme and claimed that their scheme was provably secure in standard model, i.e semantically secure under adaptively chosen-ciphertext attack(IND-IBSC-CCA2) and existential unforgeable under adaptively chosen-message attack (EUF-IBSC-CMA). These method prove previously defined ID based signcryption methods are insecure against CCA and CMA. Game theory that proves the adversary cannot arbitrarily forge the ciphertext on any message on behalf of the sender.

Ming et al show that Li et al's scheme is not secure in their security model. Liet al's scheme does not satisfy strongly existential unforgeability. Li et al's ID-based signcryption scheme [11] is notsemantically secure under chosen-ciphertext attack andunforgeable under chosen-message attack. Ming et al's identify the errors in the Li et al security models. Strongly existential unforgeability [4] means that the adversary cannot forge any signature different from thosegenerated by the challenger. In practice, given a signature on some message, no one can derive other signatureson the same message.

The Signcrypt and Unsignrypt algorithm prove by ciphertext $\sigma^* = \sigma_1^*, \sigma_2^*, \sigma_3^*, \sigma_4^*, \sigma_5^*$ is of the forms,

$$\sigma_1^* = M_b.\mathrm{e}(\mathrm{g1}.\mathrm{g2})^{\mathrm{k}^*},$$

$$\sigma_2^* = g^{k^*},$$

$$\sigma_3^* = (u' \prod_{i \varepsilon Ur*} ui)^{\mathrm{k}^*},$$

$$\sigma_4^* = d_{s2}^* \ ,$$

$$\sigma_5^* = d_{s1}^*.(m' \prod_{j \epsilon M*} m_j)^{k^*} \ ,$$

Message indices j such that

$$m^* = H(\sigma_1^*, \sigma_2^*, \sigma_3^*, \sigma_4^*, u_s^*, u_r^*)$$

The adversary A first obtains a valid ciphertext $\sigma^* = \sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5$throughissuing a signcrypt query on any message M under thesender with identity us and the receiver with identityu_r. Then, we can easily obtain another valid ciphertext $\bar{\sigma} = \bar{\sigma}_1, \bar{\sigma}_2, \bar{\sigma}_3, \bar{\sigma}_4, \bar{\sigma}_5$ on the same message M under (u_s; u_r) using the same method. Therefore, the ($\sigma^* = \sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5$)and ($\bar{\sigma} = \bar{\sigma}_1, \bar{\sigma}_2, \bar{\sigma}_3, \bar{\sigma}_4, \bar{\sigma}_5$) are both valid ciphertexts of messageM. So, Liet al. scheme is also not strongly existentially unforgeable.

According to the ID based signcryption Ming et al. prove the weakness in Li et al scheme, that complexity of the algorithm can be increase, so attacker can easily identified the ciphertext message.

Certificateless Signcryption Scheme

Certificateless signcryption scheme was proposed by Barbosa and Frashim [2] in 2008. It is the main purpose to solve the key escrow that inherited from IBC without use of the traditional PKC. The two problems in traditional public key infrastructure and identity-based public key cryptography can beprohibited by introducing certificateless public key cryptography (CL-PKC), which can be conceived as an intermediatebetween traditional public key infrastructure and identity-based cryptography. However,the provable security goals of their scheme were obtained by considering therandom oracle model. It is well knownthat provable security is one of the basic requirements for public key cryptography.Hence, the certificateless signcryption scheme inis not necessarily practically secure. The different certificateless signcryption model can be proposed for achieving the security.

CLSC security scheme should challenge the attacks of both Type I Adversaries and Type II Adversaries. A Type I Adversary does not have access to the master key of the KGC, but he has the ability toreplace the public key of any user with a value of his selection. A Type II Adversary has access to the master key of theKGC but is not allowed to perform public key replacement. The research reveals that challenging to design a secure scheme against Type I adversaries. CLSC scheme security against Type I adversary should satisfy these conditions.

1. Even if a sender uses a false public key of a receiver to generate a signcrypted text, a Type I Adversary still cannot extractthe plaintext from the signcrypted text.

2. Type I Adversary who replaces the public key of the sender cannot impersonatethe sender to generate a valid signcrypted text on behalf of the sender.

A CLSC scheme is defined by a six-tuple of probabilisticpolynomial-time algorithms. Four of these algorithms, the ones correspondingto key management operations, are identical to those defined for certificatelessencryption:

1. Setup(1k)

This is a global set-up algorithm, which takes as input the security parameter 1k and returns the KGC's secret key Msk and global parameters params including a master public key Mpk and descriptions of messagespace MCLSC(params), ciphertext space CCLSC(params) and randomness spaceRCLSC(params). This algorithm is executed by the KGC, which publishesparams.

2. Extract-Partial-Private-Key(ID; Msk; params)

An algorithm which takesas input Msk, paramsand an identifier string ID$\in$ {0,1}* representing auser's identity, and returns a partial secret key D. This algorithm is run bythe KGC, after verifying the user's identity.

3.Generate-User-Keys(ID; params)

An algorithm which takes an identity andthe public parameters and outputs a secret value x and a public key PK.This algorithm is run by a user to obtain a public key and a secret valuewhich can be used to construct a full private key. The public key is published without certification.

4.Set-Private-Key(D; x; params)

A deterministic algorithm which takes asinput a partial secret key D and a secret value x and returns the full privatekey S. Again, this algorithm is run by a user to construct the full privatekey. The signcryption and de-signcryption algorithms are as follows:

5. Sc(m; SS; IDS; PKS; IDR; PKR; params; r)

This is the signcryption algorithm.On input of a message m$\in$MCLSC(params), sender's full private key SS,identity IDS and public key PKS, the receiver's identity IDR and publickey PKR, the global parameters params and possibly some randomness r $\in$ RCLSC(params), this algorithm outputs a ciphertext c$\in$CCLSC(params) or anerror symbol $\perp$.

6.Dsc(c; SR; IDR; PKR; IDS; PKS; params).

The deterministic de-signcryption algorithm. On input of a ciphertext c, receiver's full private key RS, identityIDR and public key PKR, the sender's identity IDS and public key

PKS and theglobal parameters params, this algorithm outputs a plaintext m or a failuresymbol$\perp$.

Barbosa and Farshim construction is proven to be secure in the random oracle model but not the standard model and vunlerable to the key generation center(KGC) attacks. To overcome these disadvantage Liu et al proposed the certificateless signcryption based on standard model scheme against the KGC attacks. CCA2 prove under the decisional bilinear diffie-hellman assumption, and also proven to be existentially unforgeable under the computational Diffie–Hellman intractability assumptions. Confidentiality and unforgeability acquired by the games against Type I and Type II adversaries.

Miao et al that analyse the security proof of Liu et al unfortunately, their Security proof is not sound and well defined that also discussed and their scheme fact that insecure and stated that fails to achieve the security goals for a signcryption scheme. Miao et al show that scheme does not meet the requirement of a secureone-way encryption because Type I Adversary who replaces a receiver's public key can decryptany signcrypted message generated for that receiverand public key replacement attackmay impersonate any sender to send valid signcrypted message to a receiver. Thus, the original CLSC scheme of Liu et al.fail to achievethe requirements ofconfidentiality and non-repudiationand any of the security goalsfor a signcryption scheme.

Cheng et al proposed the corrected version of the Liu et al.'s scheme and prove the indistinguishable against adaptive chosen ciphertext attacks and is existentially unforgeable against chosen message attacks in the standard model. We recall the bilinear pairing. Revisiting the CLSC scheme of cheng et al Confidentiality can be prove the CLSC scheme is indistinguishableagainst adaptive chosen ciphertext attacks (IND - CLSC-CCA) in the standard model under the decisional BDH intractability assumption and existentially unforgeable against chosen message attacks (EUF-CLSC-CMA) in the standard model under the CDH intractabilityassumption that prove by lemmas. For the Type 1 and Type 2 attacker Messages M0 and M1 with Identities $ID_S$and $ID_R$and choose the random bitγ□□□from {0, 1}and constructsa ciphertext of M_γ, and the public keys pk_{S*}, pk_{R*}be ID_{S*}, ID_{R*}'s and secret values

x_{S*}, x_{R*}, t_{S*} ε $Z_P$and R $\in$ {0; 1}^{n}such that M_γ $||R$ ϵr

Then computes as follows

$$\delta_1^* = \emptyset\ (M_\gamma\ ||R) Z^{x^2 R^*},$$

$$\delta_2^* = C,$$

$$\delta_3^* = C^{J(d_{R*})},$$

$$\delta_4^* = \left(g^{x^2 s^*}\right) / F(d_{s*})\ g^{ts*},$$

$$w^* = H\left(\delta_1^*, \delta_2^*, \delta_3^*, \delta_4^*, R,\ pk_{S*}, pk_{R*}\right),$$

Returns

ciphertext $\delta^* = \delta_1^*, \delta_2^*, \delta_3^*, \delta_4^*, \delta_5^*$

To the adversary and prove the security that challenged ciphertext δ^* that includes the random string R to remove the defects . The identity ID with n'=n . l bit length reduced to n dimensional vectors $d_{ID=(}d_{ID1,.....,}\ d_{IDn)}$. That will reduce the masker key size and increase the paring operations for the CCA and CMA security. But it has the disadvantage that master key can be easily identified because cheng reduces the key size that moves to attacker can easily identified the key and get the message and maximum pairing operation leads to increase computational cost in signcryption and unsigncryption stages.

Conclusion

In this paper discussed about the security issues against the CCA and CMA attacks. Surveys of ID based signcryption and certificateless signcryption against the CCA and CMA attacks are discussed and identified the insecurity in the previous proposals. According to ID based signcryption increase the complexity and Certificateless signcryption paper shows that security but it increases the computational cost. So the attacker can easily get the message. So we generate the secure signcryption by low computational cost and less complexity.

References

1. Al-Riyami.S.S and Paterson.K.G, 2003, "Certificateless public key cryptography". In Advances in Cryptology-ASIACRYPT 2003, volume 2894 of LNCS, Springer-Verlag, pages 452–473.
2. Barbosa.M and Farshim.P. 2008. "Certificateless signcryption". Cryptology ePrint Archive: Report 2008/143, Available from: http://eprint.iacr.org/2008/143.
3. Bo Zhang, 2010,"Cryptanalysis of an identity based signcryption scheme without random oracles". Journal of Computational Information Systems, 6(6):1923{1931, 2010.
4. Chen, Malone-Lee, "Improved identity-based signcryption, in: Proceedings of Public Key Cryptography – PKC 2005", Les Diablerets, Switzerland, 2005, pp. 362–379.
5. ElGamal. 1985. "A public key cryptosystem and signature scheme based on discrete logarithms". IEEE Trans. Inform. Theory, 31:469–472.
6. Fagen Li, Yongjian Liao, Zhiguang Qin, and Tsuyoshi Takagi. 2012. "Further improvement of an identity-based signcryption scheme in the standard model". Comput. Electr. Eng., 38(2):413–421.
7. Han Y, Yang X. 2006. "ECGSC: Elliptic Curve Based GeneralizedSigncryption". Cryptology ePrint Archive, Reprot 2006/126.http://eprint.iacr.org/2006/126.pdf
8. Han Yiliang, Yang Xiaoyuan. 2006. "New ECDSA- Verifable generalized signcryption", Chinese Journal of Computer, 2006(11), pp.2003-2012.

9. John Malone-Lee. 2002.“Identity-based signcryption”. Cryptology ePrint Archive, Report 2002/098, 2002.http://eprint.iacr.org/.
10. Li, Y. Liao, Z. Qin, and T. Takagi, 2012. “Further improvement of an identity-based signcryption scheme inthe standard model," Computers and Electrical Engineering, vol. 38, pp. 413{421, 2012.
11. Li.X, Qian.H, Weng.J, and Yu.Y, 2013. “Fully secureidentity-based signcryption scheme with shorter signcryptext in the standard model," Mathematical andComputer Modelling, vol. 57, pp. 503-511,
12. Mingwu Zhang, Pengcheng Li, Bo Yang, Hao Wang, and Tsuyoshi Takagi. 2010. “Towards confidentiality of id-basedsigncryption schemes under without random oracle model”.Intelligence and Security Informatics, volume 6122 of Lecture Notes in Computer Science, pages 98{104. Springer Berlin / Heidelberg.
13. Rackoff.C and Simon.D, 1991, “Noninteractive zero-knowledge proof of knowledge and chosen ciphertext attack”. In Advances in Cryptology–Crypto ’91, pages 433–444.
14. Shamir.A.1985. “Identity-based cryptosystems and signature schemes”. In Advances in Cryptology, volume 196 of LNCS . Springer-Verlag. pp. 47–53
15. Selvi, Vivek, Rangan, 2010, “Security weaknesses in two certificateless signcryption schemes” 2010, in: Cryptology ePrint Archive, Report 2010/92.
16. Weng, Yao, Deng, Chen, Li, 2011.“Cryptanalysis of a certificateless signcryption scheme in the standard model”.Information Sciences 181 (3)(2011) 661–667.
17. Wenjian Xie and Zhang Zhang, 2009, “Efficient and Provably Secure Certificateless Signcryption from Bilinear Maps,” Available from eprint.iacr.org/2009/578.
18. Zheng.Y. 1997. “Digital signcryption or how to achieve cost (signature&encryption) << cost (signature) + cost (encryption)”, Advances in CRYPTO’ 97, Springer-Verlag, Berlin, pp. 165 179.
19. Zhengping Jin, Qiaoyan Wen, and Hongzhen Du.2010. “An improved semantically-secure identity-based signcryptionscheme in the standard model”. Computers & Electrical Engineering, 36(3):545{552, 2010.}
20. Y. Yu, B. Yang, Y. Sun, and S. Zhu, 2009, “Identity basedsigncryption scheme without random oracles," Computer Standards and Interfaces, vol. 31, pp. 56{62, 2009}.
21. Zhang, “Cryptanalysis of an identity based signcryption scheme without random oracles," Journal of Computational Information Systems, vol. 6, no, 6, pp.1923 {1931, 2010.
22. Cheng and Qiaoyan Wen, 2015, “An Improved Certificateless Signcryption in theStandard Model” International Journal of Network Security, Vol.17, No.5, pp.597-606.
23. Yang Ming, Yumin Wang, 2015, “Cryptanalysis of an Identity Based SigncryptionScheme in the Standard Model”, international Journal of Network Security, Vol.18, No.1, PP.165-171.