INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 4.295
(Volume 4, Issue 5)
Available online at: www.ijariit.com

A survey on signcryption schemes in CCA and CMA

S. Navin Prasad
navida5k@gmail.com
Nagarathinam Angalammal College of Arts and Science, Madurai, Tamil Nadu

Dr. R. Ganesan
rganesanmaths@yahoo.co.in
Government Arts College, Melur, Tamil Nadu

Dr. C. Rekha
rekhasaravanan98@gmail.com
Government Arts College, Melur, Tamil Nadu

ABSTRACT

This paper surveys 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 fulfills 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, Certificate-less 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 a study on various security models of different signcryption schemes and their security proof under CCA and CMA.

Keywords— *Signcryption, ID based Signcryption, Certificate-less Signcryption, CCA, CMA*

1. INTRODUCTION

Cryptography is the most ideal approach to anchor the data frame assaults. An anchored correspondence of data has been demonstrated and this can be accomplished by different cryptographic natives like open key cryptography, private key cryptography, Digital Signature et cetera. An arrangement of cryptographic natives used to give data security administrations. Essential security administrations are ought to give Confidentiality, Integrity, Un-forgeability, and Non-revocation. Classification is keeping the data mystery from who is on the whole unapproved. Honesty is affirming that data has not been changed by unapproved. Un-forgeability is the assurance that the correspondence with the approved sender. Non-Repudiation is to demonstrating the sender has sent the signcrypted content. Signcryption is a cryptographic crude that proposed by Zheng in 1997 that all the while plays out the elements of both encryption and advanced mark, which is more effective than the conventional mark then encryption [18]. Signcryption is a valuable cryptographic crude that accomplishes privacy and unforgeability in a proficient way. Signcryption plans like ID based, Certificate-less, generalized and total signcryption plans must give the data security against assaults like Chosen Cipher content Attack (CCA), Chosen Message Attack (CMA), and Chosen Plaintext Attack (CPA). In a built up Public key cryptography (PKC), any client speaks with others must acquire their open key that related with proprietor declaration, which is a mark that issued by the trusted. Declaration Authority (CA) that is expected to ensure the connection between the general population key and the personality of the client. This technique has the issue like computational expense and authentication administration issues. Shamir[14] previously presented the idea ID based cryptography (ID-PKC) in 1984, ID-PKC can take out the need for declarations and the client can straightforwardly produce people in general key by utilizing email address, IP address or some other related personality data, yet it requires a confided in outsider called Key Generation Center (KGC) create the client's Private key. Tragically, enter escrow issue occurred in character based cryptography, that is, KGC knows the private key to unscramble the figure message and get the message. In 2003, Al-Riyami and Paterson [1] proposed another cryptographic crude, declaration less open key crypto framework, which keeps away from the key escrow issue and authentication administration that happens in ID-PKC. The ID based signcryption plot was proposed by Malone-Lee [10] in 2002. Numerous ID based signcryption plans have been proposed from that point forward, embracing a wide range of methodologies, in this manner lessening computational expense and furthermore diminishing the figure content size. Declaration less signcryption plot was proposed by Barbosa and Frashim [2] in 2008. It is the principle reason to unravel the key escrow that acquired from IBC without utilization of the conventional PKC.

Summed up encryption is contrasted from conventional signcryption that is a versatile crude which accomplishes both Confidentiality and realness in a characterized structure generalized signcryption plans are given the elements of the mark, encryption, and encryption which will take care of issues that occur in installed frameworks and remote sensor systems [8]. Advance such a large number of consolidated summed up signcryption plans are viable to take care of issues against the assaults.

Signcryption schemes are mainly focused on providing information security against the Chosen Cipher text Attack (CCA) and Choose 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 cipher text. In an adaptively chosen cipher text attack (CCA2), the attacker makes the cipher text choice for adaptively that is depending on the prior decryption results.

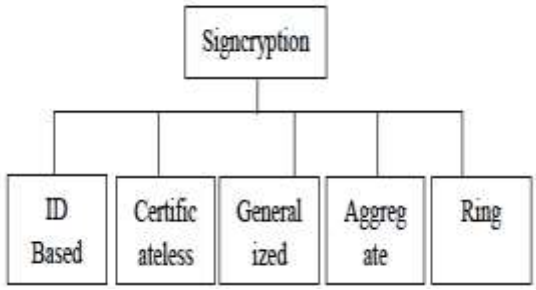

Fig. 1: An overview of signcryption schemes

As per scientific model security against the versatile picked figure content assault is spoken to as Indistinguishable against Chosen Cipher content Attack (IND – CCA2). Picked Message Attack (CMA), the assailant initially learns marks on messages of the aggressor's decision to perceive the decoded message by existentially unforgeable against versatile picked message assaults.

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

2. BACKGROUND

The fundamental security requirements for a signcryption conspire are 'Message Confidentiality' and 'Non-disavowal'. Message Confidentiality implies that no enemy can take in the message in the signcrypted content. We say that a signcryption plot offers Non-renouncement on the off chance that it keeps the sender of a signcrypted content from denying his mark. At the end of the day, without the ownership of the full private key of a sender, it's not possible for anyone to produce substantial signcrypted messages for the benefit of the sender. Precise meanings of Message Confidentiality and Non-revocation are characterized by utilizing security models.

Encryption schemes meeting strong notions of security typically introduce redundancy into their cipher texts, and as a consequence cipher texts may be deemed invalid during decryption. A scheme's correctness ensures that honestly generated cipher texts will always decrypt correctly, hence we expect decryption to 'fail' only for cipher texts that are corrupted during transmission or are adversarially generated.

Semantic secure against chosen message attacks is widely believed as the correct security level for the message authentication signature scheme. Encryption scheme and signature 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 is specific to the encryption scheme and that another part of it be specific to the signature scheme.

3. ID BASED SIGNCRYPTION SCHEME

A Signcryption scheme is secure only if confidentiality and un-forgeability 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 a 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 QTA that is made public. There is also a 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 which gives the ID.
- Signcrypt IDa sends a message m to ID bit generates appropriate ciphertext σ using Signcrypt. Signcrypt takes as input IDa, IDb and m to produce a signature.

The message space is {0,1}n for some n€ N.

Un signcrypt IDb has received a cipher text σ from IDa, then Un signcrypt to decrypt cipher text into plaintext. Unsigncrypt takes IDa, SIDb, and σ to return a message m or invalid

ID based signcryption conspire in the standard model are proposed by the yu et al, and the semantic security secrecy under the Decisional Bilinear Diffie– Hellmanproblem (DBDH) and its unforgeability under the Computational Diffie–Hellman supposition. In any case, it appeared to un secure of CCA2 and CMA in Bo Zhang and Zhang et al. Zhang et al [21] proposed signcryption conspire in the standard model that accomplishes the CMA yet shaky in CCA2. Numerous such plans were proposed however which later appeared to be shaky in the models. Zhang [22] Security ideas in view of DBDH yet both privacy and unforgeability are in anchored that demonstrated in the later plans.

Selvi et al [15] defined the security notions for the identity based signcryption that semantically secure in indistinguishability adaptive chosen cipher text attacks, IND-IBSCCCA2 and existentially unforgeable against adaptive chosen messages attacks (EUF-IBSCCMA).

This method achieves the security of getting a provably secure scheme by the combination of an ID based signature scheme and an ID based encryption scheme both in the standard model. Also shown that Li et al's schemes [11] are not secure in the standard model. In 2012, Selvi et al. [15] presented the first provably secure ID based signcryption scheme in the standard model. This scheme satisfied the strongest notions of security available for the ID based signcryption schemes.

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

Ming et al demonstrate that Li et al's plan isn't anchored in their security display. Liet al's plan does not fulfill firmly existential un-forgeability. Li et al's ID-based signcryption plot [11] isn't

semantically anchor under picked figure content assault and unforgeable under picked message assault. Ming et al's distinguish the blunders in the Li et al security models. Firmly existential unforgeability [4] implies that the foe can't produce any mark unique in relation to those created by the challenger. Practically speaking, given a mark on some message, nobody can infer different marks on a similar message

4. CERTIFICATE-LESS SIGNCRYPTION SCHEME

Certificate less signcryption conspire was proposed by Barbosa and Frashim [2] in 2008. It is the principle reason to illuminate the key escrow that acquired from IBC without utilization of the conventional PKC. The two issues in customary open key foundation and personality based open key cryptography can be precluded by presenting authentication less open key cryptography (CL-PKC), which can be considered as a middle between conventional open key framework and character based cryptography. Notwithstanding, the provable security objectives of their plan were gotten by considering the arbitrary prophet demonstrate. It is outstanding that provable security is one of the fundamental prerequisites for open key cryptography. Consequently, the declaration less signcryption conspire in isn't really for all intents and purposes secure. The distinctive testament less signcryption model can be proposed for accomplishing the security.

CLSC security scheme should challenge the attacks of both Types 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 to replace 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 the 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 extract the plaintext from the signcrypted text.
2. Type I Adversary who replaces the public key of the sender cannot impersonate the sender to generate a valid signcrypted text on behalf of the sender.

A CLSC scheme is defined by a six-tuple of probabilistic polynomial-time algorithms.

Four of these algorithms, the ones corresponding to key management operations, are identical to those defined for certificate-less encryption:

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 message space MCLSC(params), ciphert ext space CCLSC(params) and randomness spaceRCLSC(params). This algorithm is executed by the KGC, which publish sparams.

2. Extract-Partial-Private-Key (ID; Msk; params)
An algorithm which takes as input Msk, params and an identifier string IDЄ {0,1}* representing a user's identity and returns a partial secret key D. This algorithm is run by the KGC, after verifying the user's identity.

3. Generate-User-Keys (ID; params)
An algorithm which takes an identity and the 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 value which 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 as input a partial secret key D and a secret value x and returns the full private key S. Again, this algorithm is run by a user to construct the full private key. 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 mЄMCLSC(params), sender's full private key SS, identity IDS and public key PKS, the receiver's identity IDR and public key PKR, the global parameters params and possibly some randomness r Є RCLSC(params), this algorithm outputs a cipher text cЄCCLSC(params) or an error symbol ⊥.

6. Dsc(c; SR; IDR; PKR; IDS; PKS; params).
The deterministic de-signcryption algorithm. On input of a cipher text c, receiver's full private key RS, identityIDR and public key PKR, the sender's identity IDS and public key PKS and the global parameters params, this algorithm outputs a plaintext m or a failure symbol.

Barbosa and Farshim construction is proven to be secure in the random oracle model but not the standard model and vulnerable to the key generation center (KGC) attacks. To overcome these disadvantage Liu et al proposed the certificate-less 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 analyzes 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 secure one-way encryption because Type I Adversary who replaces a receiver’s public key can decrypt any signcrypted message generated for that receiver and public key replacement attack may impersonate any sender to send a valid signcrypted message to a receiver. Thus, the original CLSC scheme of Liu et al. fail to achieve the requirements of confidentiality and non-repudiation and any of the security goals for a signcryption scheme.

Cheng et al proposed the amended variant of Liu et al's. The plot and demonstrate the unclear against versatile picked figure content assaults and is existentially unforgeable against picked message assaults in the standard model. We review the bilinear matching. Returning to the CLSC plan of Cheng et al Confidentiality can be demonstrate the CLSC conspire is unclear against versatile picked figure content assaults (IND - CLSC-CCA) in the standard model under the decisional BDH unmanageability supposition and existentially unforgeable against picked message assaults (EUF-CLSC-CMA) in the standard model under the CDH obstinacy suspicion that demonstrate by lemmas.

5. CONCLUSION

In this paper discussed the security issues against the CCA and CMA attacks. Surveys of ID based signcryption and certificate-less 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 Certificate-less signcryption paper show 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.

6. REFERENCES

[1] Al-Riyami S. S. and Paterson. K. G, 2003, "Certificate less 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, Report 2006/126.http://eprint.iacr.org/2006/126.pdf

[8] Han Yiliang, Yang Xiaoyuan. 2006. "New ECDSA-Verifiable 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 in the standard model," Computers and Electrical Engineering, vol. 38, pp. 413{421, 2012.

[11] Li.X, Qian.H, Weng.J, and Yu.Y, 2013. "Fully secure identity-based signcryption scheme with shorter signcryp text in the standard model," Mathematical and Computer Modelling, vol. 57, pp. 503-511,

[12] Mingwu Zhang, Pengcheng Li, Bo Yang, Hao Wang, and Tsuyoshi Takagi. 2010. "Towards confidentiality of id-based signcryption 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 signcryption scheme in the standard model". Computers & Electrical Engineering, 36(3):545{552, 2010.}

[20] Y. Yu, B. Yang, Y. Sun, and S. Zhu, 2009, "Identity based signcryption 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 the Standard Model" International Journal of Network Security, Vol.17, No.5, pp.597-606.

[23] Yang Ming, Yumin Wang, 2015, "Cryptanalysis of an Identity Based Signcryption Scheme in the Standard Model", international Journal of Network Security, Vol.18, No.1, PP.165-171.

