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

ANALYSIS OF ATTACKS IN VARIOUS SIGNCRYPTION METHODS USING DIFFIE-HELLMAN PROBLEM (DHP)

J. Priyanka[1] and M. Ramakrishnan[2]

[1]School of Information Technology Madurai Kamaraj University, Madurai
[2]Professor and Chairperson School of Information Technology, Madurai Kamaraj University, Madurai

Abstract

Signcryption is a cryptographic primitive that will achieve both authenticity and confidentiality by logically single step. It has its attention in cryptography because of its lower computational cost and communication overhead. Many signcryption schemes were proposed so far. The security of many cryptosystems is based on the Diff-Hellman Assumption (DHA). The motivation of Diff-Hellman Problem (DHP) is, many security system use mathematical operations that are fast to compute but hard to reverse. If the cryptographic system is solved DHP then the system is easy to broke, in this paper the various attacks in the different signcryption methods such as generalized, attribute, and online/offline signcryption are critically analyzed and compared using DHP.
Keywords: *signcryption, generalised, attribute, online/offline, Diffie-Hellman Assumption*

Introduction

Zheng (1997) propossed the concept called signcryption, it is a cryptographic primitive that will achieve both authenticity and confidentiality by logically single step. It has its attention in cryptography because of its lower computational cost and communication overhead than the sign-then-encryption. The traditional cryptographic of all public key infrastructures also applicable to extended the concept of signcryption namely identity based signcryption (Malone Lee, 2002) certificateless signcryption (M. Barbosa and P. Farshim, 2003),recently signcryption were attracted by its various methods of cryptography depending on the application requirement like , attripute based signcrption (Gagné, M et al.,2010.) gives fine-grained access control by key-policy and ciphertext-policy access by the users the main motivation of attribute based signcryption were combine the features of attribute based encryption and attribute based signature. By generalised signcryption (Han Yiliang and Yang Xiaoyuan .,2006)one can perform signature , encryption and signcryption as per need, online and offline signcryption (An J.H., et al.) reduce the time complexity by the process, in this the overall process is divided into two phases (ie) online and offline, complex operations are done under offline phase to reduce the time complexity. The signcryption security proof will involve the confidentiality and unforgeability, security of the cryptographic scheme is provable by various computational assumption like discrete logarithm (DL), Diffie-Hellman and learn with errors (LWE).

Diffie-Hellman assumption is used to check once secure communication through public channel, if the method can solve the Diffie-Hellman problem it is said to be insecure

against Diffie-Hellman assumption. Signcryption is a one of the public key cryptosystem, the communication using signcryption is made through public channel, security proof of every signcryption depends on Diffie-Hellman assumption. Through Diffie-Hellman assumption the security of confidential and unforgeability is analysed by indistinguishable of ciphertexts under adaptive chosen ciphertext attack (IND-CCA) and existential unforgeability under adaptive chosen message attack (EUF-CMA).

Signcryption is combination of Encryption and signature, the aim of the scheme is to combine the security parameters of these two cryptographic methods with minimum cost and minimum computation overhead. proposed by Zheng in 1997, (Malone lee., 2002) extended the concept of id based cryptograpgy to id based signcryption, it is the combination of id based signature and id based encryption, id based signature is proposed by (Shamir.,1997) and id based encryption is proposed by (Boneh and Franklin ., 2001) to overcome the key escrow problem the first certificateless cryptography (Al-Riyami and Paterson, 2003) is proposed. Extended the concept of certificateless cryptography to certificateless signcryption (M. Barbosa and P. Farshim, 2003), the partial key is generated by KGA. Many certificateless signcryption and id based signcryption has been proposed.

The rest of this paper is organized as follows. Some preliminary works are given in Section 2. The formal model of traditional signcryption,security model and formal security proof based on DBDH and CDH assumption is described in Section 3. The analysis of various signcryption and their security proof is described in Section 4. . Finally, the conclusions are given in Section 5.

Preliminaries

Diffie-Hellman Assumption

Let p be a large prime number such that the discrete logarithm problem defined in Z^*p is hard. Let GZ^*p be a cyclic group of prime order q and g is assumed to be a generator of G.G is prime order, and security parameters p

Definition1

Computational Diffie-Hellman problem (CDH):

On input g, g^m, g^n, computing g^{mn}. An algorithm that solves the computational Diffie-Hellman problem is a probabilistic polynomial time Turing machine

Input : g, g^m , g^n

Outputs : g^{mn} (with non-negligible probability)

Computational Diffie-Hellman assumption means that there is no such a probabilistic polynomial time Turing machine. This assumption is believed to be true for many cyclic groups, such as the prime sub-group of the multiplicative group of finite fields.

Definition2

Decisional Diffie-Hellman Assumption (DDHA):

Consider a multiplicative cyclic group G of order q, with generator g. A probabilistic polynomial-time adversary has a negligible probability of distinguishing

(g^m, g^n, g^{mn}) for random m , n ∈ Z^*q

And (g^m, g^n, g^o) for random m,n,o ∈ Z^*

Formal Model of Signcryption

In general the signcryption consists of three algorithms.

Key Genration (KG): KG generate users public key PK and secrete key SK from pulic paramerter {param},

param←{p, q, g}

KG{param}→{PK_a,SK_a,PK_b,SK_b}

Signcryption(SIG) :SIG takes input parameter param , message M and then convert into cipher text c with the help of receiver public key PK_b and sender secrete key SKa

c←{M,PKb,SK_a}

UnSigncryption(USIG): USIG takes cipher text c and verify the signature of the sender with sender public key PK_a and convert the cipher text to original message

Formal Security Models

A proper signcryption scheme will achieve the security properties of both encryption and signature (i.e) Confidentiality and Unforgettability.

Definition3

Confidentiality:

The signcryption is said to have indistinguishability of ciphertexts under adaptive chosen ciphertext attack (IND-CCA) if no polynomially bounded adversary A has non-negligible advantage of winning the following game.

1. We choose a key pair (PK,SK) according to the key generation algorithm KG and give PK to A.
2. We (privately) choose a random bit $b \leftarrow \{0,1\}$.
3. A is allowed (any number of times) to query an oracle that computes the functionality $USIG_{SK}$.
4. Challenge: A outputs two messages, m_0 and m_1.
5. Response: We give A the ciphertext c=$SIG_{pk}(m_b)$
6. Same as step 3, but with the restriction that A cannot ask the decryption oracle for the decryption of c.
7. A outputs b' (i.e, a guess for our b).

Definition 4

Unforgeability

The signcryption is said to have the existential unforgeability against adaptive chosen messages attacks under key-exposure (EUF-CMA) if no polynomially bounded adversary can win the following game

1. The challenger runs the key generation algorithm KG to generate a public/private key pair (PK, SK), SK is kept secret while PK is given to the forger F.
2. Queries F performs a series of oracle queries in an adaptive fashion. The following queries are allowed:
   a) Sign oracle queries in which F submits a message m ∈ M to the challenger and obtains a signature σ on message m under the public key pk.
   b) Hash queries in which F submits a string and obtains its corresponding hash value (here, we deal with the hash function as ideally random function).
3. Output At the end of the game, F outputs a message and signature pair (m, σ).
4. We say that F wins the game if (m, σ) is a valid message-signature pair with the restriction that m has never been asked to the sign oracle.

Formal Security Proof

Theorem 1

Assume there is an IND-SC-CCA adversary that is able to distinguish two valid ciphertexts, then there exists a distinguisher D can solve an instance of the Decisional Bilinear Diffie-Hellman problem

Proof

The distinguisher D receives a random instance (P, aP, bP, cP, μ) of the Decisional Bilinear Diffie-Hellman problem. His goal is to decide whether $\mu = \hat{e}(P, P)^{abc}$ or not. D will run *A* as a subroutine and act as *A*s challenger in the IND-CCA2 game. D

KG oracle:

1. The the distinguisher D runs KG oracle to generate the system public parameters and to generate multiple key pairs$\{PK_a^*, PK_b^*, SK_a^*, SK_b^*\}$ the secret key SK_a^*, SK_b^* is kept secret where public key PK_a^*, PK_b^* is given to adversary A. These key pairs are the challenge key pairs.
2. Phase 1: A makes polynomially bounded number of queries to the following oracles.
3. SIG oracle:
   A produces messages $M=\{m_{i,}$where i=1,2,....n}and n arbitrary public keys $PK_x^*=\{PK_{xi}^l$,where i=1,2,.....n} and requires the result of the operation∏ = SIG {M, SK_y^*, PK_{xi}.....PK_{xn}} for an attacked user's private key SK_y^* where y ε[1,n] . distinguisher D runs SIG algorithm and returns the output ∏ to A.
4. USIG Oracle:

A produces a ciphertext ∏, an arbitrary public key PK_a of the sender and requires the result of USIG $\{\prod, SK_y^*, PK_a\}$ for the attacked users's private key SK_y^* where y [1,n].distinguisher D USIG algorithm and returns the output to A.

5. After getting all information the A submits two equal length of messages $m0^*$ and $m1^*$, *an arbitrary private key* SK_a^* *and* randomly chooses a bit b_i= {0, 1} to compute a ciphertext $\prod^* = SIG\{M_b^*, SK_a^*, PK_{x1}^*, ...PK_{xn}^*\}$under the attacked users's public keys PK_{xj} where jε[1,n]. D returns $\prod^*$ to *A* as a challenge.

Phase 2:

6. *A* is allowed to make polynomially bounded number of new queries as in phase 1 with the restriction that *A* should not query the USIG$\{\prod^*, SK_{xj}^*, PK_a^*\}$ where jε[1,n]
7. After *A* has made a sufficient number of queries, *A* returns its guess: a bit. If then D outputs 1 as the answer to the DBDH problem. Otherwise, it outputs 0. Since the adversary is denied access to the USIG oracle with the challenge signcryption, for *A* to find that *mi* is not a valid ciphertext, *A* should have queried the KG Oracle with $wi = e(Wi, SK_b)$. Here *SKB* is the private key of the receiver, and it is $aXB = (bP)\ a = abP$. Also, D has set $Wi = cP$. We have $wi = e(Wi, SKB) = e(cP, abP) = e(P, P)^{abc}$

Theorem 2

In the random oracle model, the proposed SC is secure against any probabilistic polynomial time adversary A for EUF-SC-CMA if the Decisional Biliner Diffie-Hellman Problem is hard.

Proof

1. A can adaptively perform queries to the same oracles as those defined in theorem 1
2. At the end of the game, A produces a ciphertext $\prod^*$ and n arbitrary receivers's key pairs SK_{bi}^*, PK_{bi}^* where i =1,2,...n A wins the game if the result of USIG$\{\prod^*, SK_{bi}^*, PK_a^*\}$ where iε[1,n] is a valid message m_i^* under the attacked user's public key PK_a^* and the -th receiver's secret key SK_{bi}^* and $\prod^*$ is not the output of $SIG\{M^*, SK_a^*, PK_{b1}.....PK_{bn}\}, M^*=\{m_1^*, m_2^*, ...m_n^*\}$

Analysis of Attribute Based Signcryption

Formal Model of Attribute Based Signcryption (ABS)

*(*Setup, sExtract, dExtract, Signcrypty, Unsigncrypt*)*

Setup *(Sparam)* The Trusted Authority (TA) chooses security parameter Sparam and creates system public parameters params and system master key MK according to Sparam.. The master key MK is kept secret, and params are made public. The description of the attribute universes *Ue, Us* and the message space *M* are included in the public parameters params.

Sparam←{param ,MK} param→(Ue,Us, M)

**sExtract*(*params,MK,*sAS*)*:* The TA computes the signing key SKsAS with the input params,MK, a signing access structure *sAS* over *Us* and sends it to a legitimate signcryptor.

**dExtract*(*params,MK,*dAS*)*:* When a decryptor requests a decryption key, the TA creates a decryption access structure *dAS* over *Ue* according to his role in the system and computes the decryption key SK*dAS* with the input params,MK,*dAS* and sends it to the decryptor. Note that while the decryption access structure enables what type of ciphertexts the user can decrypt, the signing access structure is used to signcrypt a message.

**Signcrypt*(*params, *M*,SK*sAS* ,*Ws* ,*We*)*:* When a signcryptor wants to signcrypt a message *M M*, it selects a set *We* of encryption attributes that decide a group of legitimate recipients and an authorized signing attribute set *Ws* of its signing access structure *sAS* , i.e., *Ws* ? *sAS* . It executes this algorithm with the input params, *M*, signing key SK*sAS*, *Ws,We* and produces as output a signcryption ciphertext CT*(Ws ,We)*. Here, *We* is used to encrypt a message, and *Ws* is used to sign a message.

**Unsigncrypt *(*params, CT*(Ws ,We)*,SK*dAS)*:* On receiving a ciphertext CT *(Ws,We)* of some message *M,* the decryptor/ recipient performs this algorithm using his decryption key SK*dAS* along with public parameters params and the ciphertext CT*(Ws ,We)*. The algorithm will correctly recover the message *M* only if *We dAS* and the ciphertext CT *(Ws, We)* contains a valid signature.

Traditional attribute based signcryption not offer confidentiality against indistinguishability of ciphertexts under adaptive chosen ciphertext attack (IND-CCA). Our proof is based on Hu Xiong et all, 2015 scheme.

After receiving valid cipher text

CT ={ param, w_s,w_e, SKdAs }

={ U_e,U_s,w_s,w_e, SKdAs }

Here w_s is said to be set of attribute with their access structures of the users. Assume that adversary A get one of the access structure and therefore A has the private key SK_j for j $\in w_s$ corresponding to the attribute set.

Then A can decrept the message using unsigncrypt oracle

$$X = \prod_{j \in w_s} e(sk_j, pk_j)^{\Delta_j, s(0).}$$

$$= \prod_{j \in w_s} e(g \frac{q(j)}{tj}, g^{t_{j.s}})^{\Delta_{j.s(0)}} = e(g,g)^{a.s}$$

Traditional attribute based signcryption not offer existential unforgeability against adaptive chosen messages attacks under key-exposure (EUF-CMA)

After receiving valid cipher text the

CT ={ param, w_s,w_e, SKdAs }

={ U_e,U_s,w_s,w_e, SKdAs }

The adversary A can forge the cipher text
CT^* ={ $param^*$, w_s^*,w_e^*,$SKdAs^*$ }
={ U_e^*,U_s^*,,w_s^*,w_e^*,$SKdAs^*$} on message m^*.

Thus , X^* can be reconstructed as follows

$$X^* = \prod_{j \in w_s} e(sk_j, pk_j^*)^{\Delta_j, s(0).}$$

$$= \prod_{j \in w_s} e(g^{\frac{q(j)}{tj}}, g^{t_{j.s^*}})^{\Delta_{j.s(0)}}$$

$$= e(g,g)^{a.s^*}$$

Following table describes the various attribute based signcryption and their security assumption using DHA

S.No	Title	Author	Year	CMA	CCA
1	Secure sharing of Personal Health Records in cloud computing:Ciphertext-Policy Attribute-BasedSigncryption	Jianghua Liu et al.,	2015	✓	✓
2	Efficient attribute-based signature and signcryption realizing expressive access structures	Y. Sreenivasa Rao &Y. Sreenivasa Rao	2015	✓	✓
3	Attribute-based signcryption with hybrid access policy	Gang Yu & Zhenfu Cao	2015	✓	✓

Analysis of Online/Offline Signcryption
Formal Model of Online/Offline Signcryption(On/OffS)
(setup,Extract ,offlinesigncrypt,onlinesigncrypt,unsigncrypt)

Setup: Given a security parameter Sparam, the PKG(private key generator) generates the system's public parameters params. With these parameter the setup algorithm produce public key PK_a,PK_b and master secreat key MSK. PK is made public and MSK is kept secret.
.
Extract: In this algorithm takes users identity and the PKG computes the corresponding secret key SK_a, SK_b of users and transmits it to its owner in a secure way.

OffSigncrypt: This algorithm run by sender with the sender secreat key SK_a and receiver public key PK_b and receiver identity R_{id}. Note that we do not need the message

OnSigncrypt: Given a message m, a sender's identity S_{id}, a receiver's identity R_{id} and a offline signcryption d, this algorithm outputs a full ciphertext s. This algorithm is also executed by the sender.

Unsigncrypt: Given a ciphertext s, asender'sidentity S_{id} , a receiver's identity R_{id} and the receiver's private key SK_b , this algorithm outputs the plaint ext m or the symbol ? if s is an invalid ciphertext between identities S_{id} and R_{id}.

Following table describes the various online/offline signcryption and their security assumption using DHA

S.No	Title	Author	Year	CMA	CCA
1	Certificate less online/offline signcryption for the Internet of Things	Fagen Li et al.,	2015		
2	On the security of a certificateless online/offline signcryption for Internet of Things	Wenbo Shi et al.,	2015		
3	Identity-based online/offline signcryption for low power devices	Fagen Li et al.,	2012		

Analysis of Generalised Signcryption
Formal Model of Generalised Signcryption (GSC)
(setup, extract, GSC:signcryption mode, signature mode, encryption mode,UGSC)

Setup: Given a security parameter Sparam, PKG executes this algorithm and generates a master secreat key MSK and public parameters *params*. PKG publishes *params* and keep MSK secret.

Extract: In this algorithm takes users identity and the PKG computes the corresponding secret key SK_a ,SK_b of users and transmits it to its owner in a secure way.

GSC: This algorithm has three scenarios: signcryption, signature and encryption.

Signcryption mode: if user S transmits a message m confidentially and authenticately to R, the input is (MSK, m, R_{id}),
The output is σ = GSC (MSK, m, R_{id})

Signature mode: if user S wants to sign a message m without definite receiver, the input is (MSK, m, U_{id}) where U_{id} means the receiver is null.
The output is σ = GSC (SA, m, U_{id})

Encryption mode: if someone wants to send message m to R confidentially, the input is (MSK_u, m, R_{id}), where MSK_u means the sender is null.
The output is σ =GSC (MSK_u, m, R_{id})

UGSC: Given, if it is valid, the receiver R unsigncrypts the cipher text and returns *m* and (or) the signature on *m* by S, otherwise return means fail.

Following table describes the various Generalised signcryption and their security assumption using DHA

S.No	Title	Author	Year	CMA	CCA
1	Obtain confidentiality or/and authenticity in Big Data by ID-based generalized signcryption	Guiyi Wei et al.,	2015		
2	Provable certificateless generalized signcryption scheme	Caixue Zhou et al.,	2014		
3	Certificateless Generalized Signcryption	Huifang Ji et al.,	2012		
4	An efficient identity based generalized signcryption scheme	Prashant Kushwah et al.,	2011		

Conclusions

In this paper, we analysed various types of signcryption and their security proof of confidentiality against indistinguishability of ciphertexts under adaptive chosen ciphertext attack (IND-CCA) and existential unforgeability against adaptive chosen messages attacks under key-exposure (EUF-CMA) .our analysis shows that many signcryption falls under this two types of attack due to key exposure.

References

1. An JH, Dodis, Y, RabinT. On the security of joint signature and encryption.In: Advances in cryptology—EUROCRYP, Lecture notes in computer science, vol.2332, pp 83–107.
2. Al-Riyami S.S., Paterson K.G (2003), Certificateless public key cryptography. In: Proceedings of ASIACRYPT, Springer, Heidelberg in Computer Science, vol. 2894, pp 452–473.
3. Barbosa. M and Farshim.P (2008), Certificateless signcryption," in Proceedings of the ACM Symposium on Information, Computer and Communications Security, pp 369-372.
4. Boneh D, Franklin M,(2001)Identity-based encryption from the weil pairing. In: Advances incryptology—CRYPTO. Lecture notes in computer science, vol 2139, pp 213–29.
5. Caixue Zhou ,Wan Zhou ,Xiwei Dong(2014), Provable certificateless generalized signcryption scheme,Springer Science+Business Media 71, pp 331–346
6. Fagen Li,Yanan Han,Chunhua Jin,(2015),Certificateless online/offline signcryption for the Internet of Things,Springerlink.com:Wireless Netw.

7. Fagen Li, MuhammadKhurramKhan, KhaledAlghathbar, TsuyoshiTakagi,(2012), Identity-based online/offline signcryption for low power devices,Elsevier: Journal of Network and Computer Applications 35 ,pp 340–347.
8. Gagne M, Narayan S, Safavi-Naini R (2010), Threshold attribute based signcryption. Proceedings of the 7th International Conference on Security and Cryptography for Networks, Amalfi, Italy, pp 154–171.
9. Gang Yu and Zhenfu Cao (2015), Attribute-based signcryption with hybrid access policy, Springer Science+Business Media New York.
10. Guiyi Wei, Jun Shao, Yang Xiang, Pingping Zhu, Rongxing Lu,(2015),Obtain confidentiality or/and authenticity in Big Data by ID-based generalized signcryption, Elsevier:Information Sciences 318, pp 111–122
11. Han and Yang, (2006) ECGSC: elliptic curve based generalized signcryption, in: UIC, Lecture Notes in Computer Science, vol. 4159, pp. 956–965.
12. Huifang Ji, Wenbao Han, Long Zhao, (2012), Certificateless Generalized Signcryption, Elsevier: International Conference on Medical Physics and Biomedical Engineering 33, pp 962 – 967.
13. Hu Xiong, Ji Geng, Zhiguang Qin, and Guobin Zhu,(2015),Cryptanalysis of Attribute-based Ring Signcryption Scheme, International Journal of Network Security, Vol.17, No.2, PP.224-228.
14. Jianghua Liu, Xinyi Huanga, Joseph K. Liu,(2015), Secure sharing of Personal Health Records in cloud computing: Ciphertext-Policy Attribute-Based Signcryption, Elsevier Future Generation Computer Systems 52, pp. 67–76
15. Malone-Lee.J (2005), Improved Identity-based signcryption. PKC, Springer-Verlag, 362-379.
16. Prashant Kushwah, Sunder Lal, (2011), An efficient identity based generalized signcryption scheme, Elsevier: Theoretical Computer Science 412, pp 6382–6389.
17. Shamir.A, (1984), Identity-based cryptosystems and signature schemes," in Advances in Cryptology - Crypto'84, pp. 47-53.
18. Sreenivasa Rao.Y and Ratna Dutta,(2015),Efficient attribute-based signature and signcryption realizing expressive access structures, Springer-Verlag Berlin Heidelberg, pp 81–109
19. Wenbo Shi , Neeraj Kumar ,Peng Gong,Naveen Chilamkurti ,Hangbae Chang(2014),On the security of a certificateless online/offline signcryption for Internet of Things,Springer Science+Business Media New York:Peer-to-Peer Netw. Appl.pp:881–885.
20. Zheng, Y., Goos, G.,Hartmanis, J., and Leeuwen, J.V.,(1997). Digital signcryption or how to achieve cost (signature and encryption) cost (signature) + cost (encryption), *Advances in Cryptology - Crypto 97*, pp 291-312.