IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 19, Issue 3, Ver. VI (May - June 2017), PP 71-75
www.iosrjournals.org

Cryptanalysis and Further Improvement of a Certificate less Aggregate Signature Scheme

Pankaj Kumar[1], Vishnu Sharma[2], Vinod Kumar[3], Ankush Kumar[4]
[1,2]*School of* Computing *Science and Engineering, Galgotias University, India*
[3]*Department of Mathematics, P.G.D.A.V. College, University of Delhi, New Delhi, India*
[4]*Department of Mathematics, Shivaji College, University of Delhi, New Delhi, India*

Abstract: *Certificateless aggregate signature reduces nsignatures on n distinct messages from n distinct users into a compact single length signature. Recently Deng et al proposed CLAS Scheme which is an improvement of Hou et al scheme and claims that their scheme is secure against type I type II adversary but unfortunately it is found insecure by against the"Honest but Curious" attack by adversary II. In this paper, we demonstrate that Deng et al proposed CLAS scheme is insecure against type II adversary and suggest an improved CLAS scheme.*

Keywords: *Keywords: Digital Signature, Cryptography, Cryptanalysis, Security attacks.*

I. Introduction

Aggregate signature scheme is helpful for the real time application such as limited bandwidth and low computation. Boneh et al [1] proposed the concept of aggregate signature scheme in 2003. Certificate signature allows mapping nsignatures on *n* distinct messages from *n* distinct users into a single length signature. Al-riyami and Paterson [2] proposed the concept of certificateless public key cryptography (CL-PKC) in 2003 which theyprovide the solution of key escrow problem that inherit from the Identity based public key cryptography. In CL-PKC, third party called Key Generation Center (KGC) involves for generating the user's partial private key and user select their private key by using the secret value. Result of this activity escape with the key escrow problem because user secret key is not completely known by the Private Key Generator (PKG) as in Identity based cryptography. Identity based public key cryptography scheme was introduced by Shamir et al [3] in 1984 which gives the solution of key authentication of sender but creates the well-known problem key escrow problem. In identity based cryptography third party Private Key Generator (PKG) generate the whole private key of the user while user select his public by any identity such as email or license number, address number etc that create the key escrow problem. According to the Al-riyami and Paterson [2], CLAS scheme have two types of adversary called type I and type II. Type I adversary has potential to replace the public key of user while have no control on the master key of the user. Type II adversary knows the master key of the KGC while it cannot replace the public key of the user. Furthermore, Huang et al [5] classify these adversaries on their potential power such as Super type, Strong type, Normal type adversary I and adversary II and proposed two CLAS scheme in which first scheme is secure against Normal type I and Super type II where second scheme is secure against Super type I and type II. Liu et al [6] proposed an CLAS scheme in which they proves their scheme is unforgeable against adaptive chosen message attack but Zheng and Wang [7] found insecure Liu et al [6] CLAS scheme by applying concrete attacks with type II adversary. Xiong et al [8] proposed an certificateless aggregate signature scheme and that their CLAS scheme is secure against adaptive chosen message attack of type I and Type II adversary but Hou et al [10] found their scheme is insecure and gives an improvement CLAS scheme. Cheng et al [9] also proves that Xiong et al [8] scheme is also insecure against honest but curious and malicious but passive attack. Deng et al [4] proves that Hou et al [10] scheme is insecure against malicious but passive attack and gives an improvement CLAS scheme and show that this scheme is secure against malicious but passive attack. In this paper we prove that Deng et al [4] is insecure against the honest but curious attack by type II adversary while it is secure against malicious but passive attack.

***Paper organization*:**In Section 2, we presents a review of Deng et al [4] CLS scheme and CLAS scheme and apply an attack honest but curious on Deng et al aggregate with same attack on Deng et al [4] aggregate signature scheme in section 3. Section 4 suggests a modified CLAS scheme to improve Deng et al [4]. Finally, the conclusions are presents in Section 5.

II. Review of the Deng et al [4] CLS Scheme

The symbol table is given below.

TABLE 1 Symbol used in scheme

Symbols	Description
s	The master key of KGC
P	Generator of the group
n , q	Natural number
P_{pub}	The public key of KGC
ID_i	The User's identity
usk_{ID_i}	The Users secret key
psk_{ID_i}	The partial private key of identity ID_i
$Params$	The system parameters generated by KGC
(usk_{ID_i}, upk_{ID_i})	The user's secret / public key pair of identity ID_i
upk_{ID_i}	The public key of identity ID_i
m_i	The message corresponding to user's identity ID_i
σ_i	Signature on the message m_i with user's identity ID_i
V	Signature of user corresponding to user's ID_i
KGC	Key Generation Center
CLS	Certificateless Signature
CLAS	Certificateless Aggregate Signature

In this section we give a brief review of Deng et al CLAS scheme. Deng et al CLS scheme consist of five algorithms *Masterkeygen, Partialkeygen, Userkeygen, Sign, Verify.*

Masterkeygen: on taking a security input k , KGC starts the algorithm as follow:

i) Generate two groups one is cyclic additive group G_1 and second is cyclic multiplicative group G_2 having the same order q with two generator P, Q of G_1 and a bilinear pairing $e: G_1 \times G_2 \rightarrow G_T$

ii) Select a random number $s \in Z_q^*$ and computes $P_{pub} = sP$, taking s as a master key of KGC and P_{pub} as a public key of KGC.

iii) Select four hash functions $H_1 : \{0,1\}^* \rightarrow G_1, H_2 : \{0,1\}^* \rightarrow G_1, H_3 : \{0,1\}^* \rightarrow Z_q^*, H_4 : \{0,1\}^* \rightarrow Z_q^*$.

iv) Generates the system parameters say $Params$ are $\{q, G_{1,} G_2, e, P, Q, P_{pub}, H_1, H_2, H_3, H_4\}$ and keep secretly master key s by KGC.

Partialkeygen: After taking input user's identity ID_i , The KGC first computes the user's partial private key $psk_{ID_i} = sQ_{ID_i}$ where $Q_{ID_i} = H_1(ID_i)$ and forward it to the user via a secure way.

Userkeygen: The user chooses a random number $x_{ID_i} \in Z_q^*$ and set as secret key usk_{IDi} , then computes its public key $upk_{ID_i} = usk_{IDi}.P$

Sign: The user with identity ID_i takes the $Params$, the partial private key psk_{ID_i} , corresponding secret key usk_{IDi} and then performs the following steps to generate the signature:

i) Select a random number $r_i \in Z_q^*$ and computes

$U_i = r_i.P$, $h_{1i} = H_3(m_i, ID_i, upk_{iD_i}, U_i)$, $h_{2i} = H_4(m_i, ID_i, upk_{iD_i}, U_i)$, $K = H_2(q, P, P_{pub})$

ii) Compute: $V_i = psk_{ID_i} + h_{1i} r_i P + h_{2i} x_i K$

iii) Provides a signature (U_i, V_i) on message m_i .

Verify: Given a signature (U_i, V_i) with message m_i corresponding public key upk_{ID_i} regarding the identity ID_i verifier performs the following steps:

i) Computes $U_i = r_i.P$, $h_{1i} = H_3(m_i, ID_i, upk_{iD_i}, U_i)$, $h_{2i} = H_4(m_i, ID_i, upk_{iD_i}, U_i)$, $K = H_2(q, P, P_{pub})$

ii) Verify the following equation

$e(V_i, P) = e(Q_{ID_i} + h_{1i} U_i, P_{pub})\ e(h_{2i} upk_{ID_i}, K)$

If it satisfied then accept the signature.

2.1 Deng et al [4] CLAS scheme

CLAS scheme consist of seven steps in which five algorithms *Masterkeygen, Partialkeygen, Userkeygen, Sign, Verify* are same as CLS scheme and two extra algorithms say Aggregate and Aggregate verify are involved in CLAS scheme whose description is given below:

1) *Aggregate*: for an aggregating set of n users $\{U_1, U_2 ....,U_n\}$ with their identities $\{ID_1, ID_2 ....,ID_n\}$ and the corresponding public keys $\{upk_1, upk_2, ...,upk_n\}$, and with signature pairs $\{(m_1, \sigma_1 = (U_1, V_1)), ...(m_n, \sigma_n = (U_n, V_n))\}$, then aggregator computes $V = \sum_{i=1}^{n} V_i$ and results an aggregate signature as $\sigma = (U_1, U_2 ....,U_n, V)$.
2) *Aggregate Verify*: for verify an aggregate signature $\sigma = (U_1, U_2 ....,U_n, V)$ signing by n users $\{U_1, U_2 ....,U_n\}$ with their identities $\{ID_1, ID_2 ....,ID_n\}$, verifier performs the following steps:

i) Computes $Q_{ID_i} = H_1(ID_i)$, $h_{1i} = H_3(m_i, ID_i, upk_{iD_i}, U_i)$, $h_{2i} = H_4(m_i, ID_i, upk_{iD_i}, U_i)$, $K = H_2(q, P, P_{pub})$

ii) Verify

$$e(V, P) = e(\sum_{i=1}^{n}(h_{1i}.U_i + Q_{ID_i}), P_{pub}) \,.\, e(\sum h_{2i}.upk_{ID_i}, K)$$

III. Cryptanalysis of Deng et al [4] CLS scheme

In this subsection we discuss the type II attack on behalf we claim that proposed CLS scheme is insecure. Since KGC knows the master key, then KGC compute the value $r_i P_{pub} = r_i sP = sr_i P = sU_i$. Since s and U are publicly known and with the help of known value sU_i we calculate $r_i P_{pub}$. With the help of master key KGC can compute the partial private key of user psk_{ID_i}, by $psk_{ID_i} = sQ_{ID_i}$ while $Q_{ID_i} = H_1(ID_i)$ is known quantity. h_{1i} and h_{2i} are the hash value then h_{2i}^{-1} also compute. Now he can compute the fix value $x_i K = h_{2i}^{-1}(V^* - psk_{ID_i} - h_{1i} sU_i^*)$ by capturing the signature (U^*, V^*) onmessage m_i, $h_{1i} = H_3(m_i^*, ID_i, upk_{iD_i}, U_i^*)$ $h_{2i} = H_4(m_i^*, ID_i, upk_{iD_i}, U_i^*)$. Since KGC don't know the user's secret key but he knowns about the fix value $x_i K$ then he can forge user's signature on any message in aggregate set. The description of this attack is given below:

Intercept partial signature: in the first step KGC intercept the signature of user U_i with the identity ID_i corresponding public key upk_{ID_i} and find the signature (U^*, V^*).

Compute fix value:

i) Compute $h_{1i} = H_3(m_i^*, ID_i, upk_{iD_i}, U_i^*)$ $h_{2i} = H_4(m_i^*, ID_i, upk_{iD_i}, U_i^*)$, $K = H_2(q, P, P_{pub})$

ii) Compute $r_i^* P_{pub} = r_i^* sP = sr_i P = sU_i^*$

iii) Computes $x_i K = h_{2i}^{-1}(V^* - psk_{ID_i} - h_{1i} sU_i^*)$

Forge partial signature: Now KGC perform the following step to forge CLS signature $(U_i^{'}, V_i^{'})$ on message $m_i^{'}$.

i) Select $U_i^{'} \in G_1$, and extract the value of sU_i from $r_i P_{pub}$.

ii) Computes $h_{1i} = H_3(m_i^{'}, ID_i, upk_{iD_i}, U^{'})$ $h_{1i} = H_4(m_i^{'}, ID_i, upk_{iD_i}, U_i^{'})$, $K = H_2(q, P, P_{pub})$

iii) Computes $V_i^{'} = psk_{ID_i} + h_{1i} sU_i^{'} + h_{2i} x_i K$

Then he provides an output $(U_i^{'}, V_i^{'})$ on the message $m_i^{'}$.

Verification:

$$e(V_i^{'}, P) = e(psk_{ID_i} + h_{1i} sU_i^{'} + h_{2i} x_i K, P)$$
$$= e(psk_{ID_i} + h_{1i} sU_i^{'}, P)\; e(h_{2i} x_i K, P)$$

$$= e(sQ_{ID_i} + h_{1i} sU_i^{'}, P)\ e(h_{2i} x_i P, K)$$
$$= e(Q_{ID_i} + h_{1i} U_i^{'}, sP)\ e(h_{2i} upk_{ID_i}, K)$$
$$= e(Q_{ID_i} + h_{1i} U_i^{'}, P_{pub})\ e(h_{2i} upk_{ID_i}, K)$$

3.1 Cryptanalysis of Deng [4] CLAS scheme

KGC can compute $r_i P_{pub}$ and $x_i K$ of any user's signature by the above method mention used to forge the CLS scheme. Then he can club the entire signatures to forge the aggregate signature.

Now KGC calculates $V^{**} = \sum_{i=1}^{n} V^{'}$ and provide the output $(U_1^{'}, U_2^{'}..........., U_n^{'}, V^{**})$ as the forge aggregate signature.

For $i \in [1,n]$, $Q_i = H_1(ID_i)$, $h_{1i} = H_3(m_i^{'}, ID_i, upk_{iD_i}, U_i^{'})$, $h_{1i} = H_4(m_i^{'}, ID_i, upk_{iD_i}, U_i^{'})$, $K = H_2(q, P, P_{pub})$

Forge aggregate signature is valid if it satisfied the following equation.

$$e(V^{**}, P) = e(\sum_{i=1}^{n} (h_{1i}.U_i^{'} + Q_{ID_i}), P_{pub})\ e(\sum h_{2i}.upk_{ID_i}, K)$$

IV. Improved Certificateless Signature Scheme

We propose a modified CLAS scheme to remove the weakness of Deng et al CLAS scheme.

***Masterkeygen*:** on taking a security input k , KGC starts the algorithm as follow:

i) Generate two groups one is cyclic additive group G_1 and second is cyclic multiplicative group G_2 having the same order q with two generator P, Q of G_1 and a bilinear pairing $e : G_1 \times G_2 \to G_T$

ii) Select a random number $s \in Z_q^*$ and computes $P_{pub} = sP$, taking s as a master key of KGC and P_{pub} as a public key of KGC.

iii) Select four hash functions $H_1 : \{0,1\}^* \to G_1$, $H_2 : \{0,1\}^* \to G_1$, $H_3 : \{0,1\}^* \to Z_q^*$, $H_4 : \{0,1\}^* \to Z_q^*$.

iv) Generates the system parameters say $Params$ are $\{q, G_{1,} G_2, e, P, Q, P_{pub}, H_1, H_2, H_3, H_4\}$ and keep secretly master key s by KGC.

***Partialkeygen*:** After taking input user's identity ID_i , The KGC first computes the user's partial private key $psk_{ID_i} = sQ_{ID_i}$ where $Q_{ID_i} = H_1(ID_i)$ and forward it to the user via a secure way.

***Userkeygen*:** The user chooses a random number $x_{ID_i} \in Z_q^*$ and set as secret key usk_{IDi} , then computes its public key $upk_{ID_i} = usk_{IDi}.P$

***Sign*:** The user with identity ID_i takes the $Params$, the partial private key psk_{ID_i} , corresponding secret key usk_{IDi} and then performs the following steps to generate the signature:

iv) Select a random number $r_i \in Z_q^*$ and computes

$U_i = r_i.P$, $h_{1i} = H_3(m_i, ID_i, upk_{iD_i}, U_i)$, $h_{2i} = H_4(m_i, ID_i, upk_{iD_i}, U_i)$, $K = H_2(q, P, P_{pub})$, $T = H_2(q, P, P_{pub})$

v) Compute: $V_i = psk_{ID_i} + h_{1i} r_i T + h_{2i} x_i K$

vi) Provides a signature (U_i, V_i) on message m_i .

Verify: Given a signature (U_i, V_i) with message m_i corresponding public key upk_{ID_i} regarding the identity ID_i verifier performs the following steps:

iii) Computes $U_i = r_i.P$, $h_{1i} = H_3(m_i, ID_i, upk_{iD_i}, U_i)$, $h_{2i} = H_4(m_i, ID_i, upk_{iD_i}, U_i)$, $K = H_2(q, P, P_{pub})$

iv) Verify the following equation

$$e(V_i, P) = e(Q_{ID_i} + h_{1i} U_i, P_{pub})\ e(h_{2i} upk_{ID_i}, K)$$

V. Conclusion

Recently, Deng et al [4] proposed an efficient improvedCLAS scheme of Hou et al [10] CLAS scheme. In this paper, we first give a detail review of Deng et al CLS and CLAS scheme then show that proposed CLAS is insecure against concrete attacks. We point out that the security leaks of the scheme that is depends on the user secret key usk_{ID_i} and a random number r_i select by the user but malicious KGC computes the fixed value $r_i P_{pub}$, $x_i K$ and forge the signature without the help of usk_{ID_i} and r_i. We proposed a certificateless signature scheme to remove the security leaks arise in Deng et al [4].

References

[1]. D. Boneh, C. Gentry, B. Lynn, H. Shacham, "Aggregate and Verifiably Encrypted Signatures from Bilinear Maps", E. Biham (Ed.), EUROCRYPT 2003, LNCS 2656, Springer-Verlag, Warsaw, Poland, 2003, pp. 416–432.

[2]. Al-Riyami, S., Paterson, K. "Certificateless Public Key Cryptography", Asiacrypt' 03, LNCS 2894, Springer-Verlag. (2003) pp. 452-473.

[3]. A. Shamir, "Identity Based Cryptosystems and Signature Schemes",G.R. Blakley, D. Chaum (Eds.), Crypto'84, LNCS 196, Springer-Verlag, Santa Barbara, California, USA, 1984, pp. 47–53.

[4]. J. Deng, C. Xu, H. Wu, G. Yang, "An Improved Certificateless Aggregate Signature", 2014 IEEE Internatational Conference on Computer and Information Technology pp 919-922.

[5]. X. Huang, Y. Mu, W. Susilo, D. S. Wong, W. Wu, "Certificateless Signatures: New Scheme and Security Models" The Computer Journal, Vol. 55 No.4, 2012 pp 457-474.

[6]. H Liu, S Wang, M Liang and Y Chen, "New Construction of Efficient Certificateless Aggregate Signatures", International Journal of Security and Its Applications Vol.8, No.1 (2014), pp. 411-422.

[7]. Y. Zhang, C. Wang " Comment on New Construction of Efficient Certificateless, Aggregate Signatures" International Journal of Security and Its Applications Vol.9, No.1 (2015), pp.147-154.

[8]. H. Xiong, Z. Guan, Z. Chen, F. Li "An Efficient Certificateless Aggregate Signature With Constant Pairing Computations" Inform. Sci. 219 (2013) 225–235.

[9]. Lin Cheng, Qiaoyan Wen, Zhengping Jin, Hua Zhang, Liming Zhou" Cryptanalysis and Improvement of a Certificateless Aggregate Signature Scheme " information sciences 295 (2015) pp 337-46

[10]. H.Hou, X.Zhang,X.Dong, "Improved Certificateless Aggregate Signature Scheme ", Journal of Shandong University (Natural Science), 48(9),pp. 29-34,2013.