Journal of Information Hiding and Multimedia Signal Processing ©2016 ISSN 2073-4212
Ubiquitous International Volume **7**, Number **6**, November **2016**

A New Provable Secure Certificateless Aggregate Signcryption Scheme

Shou-Lin Yin[1], Hang Li[1*] and Jie Liu [1,2]

[1]Software College
Shenyang Normal University
No.253, HuangHe Bei Street, HuangGu District, Shenyang, P.C 110034 - China
352720214@qq.com;zxcvfdsa5024@foxmail.com;nan127@sohu.com
*Corresponding author:zxcvfdsa5024@foxmail.com

[2]Department of Information Engineering
Harbin Institute of Technology
92 West Straight Street In Nangang District of Harbin Harbin,150001-China

Received July, 2016; revised August, 2016

Abstract. *These existed signcryption schemes have low aggregate signcryption efficiency. So in this paper, we propose a new certificateless aggregate signcryption scheme. The new method can reduce the computation number of bilinear pairings and improve the signcryption efficiency. It also can set any one from the users as an aggregator, and then the appointed aggregator will launch the signcryption protocol. Then the message is encrypted and aggregated. Finally, we give the security proof and make comparison to verify the effectiveness of our new scheme.*

Keywords: Certificateless aggregate signcryption; Bilinear pairings.

1. **Introduction.** Signcryption[1,2] can guarantee confidentiality, integrity, non-repudiation and authentication all signature and encryption function for message in a single logical step. It is more effective than traditional signature schemes. Malone-Lee[3] proposed a signcryption scheme based on identity, but this scheme dose not have semantic security[4]. Then many signcryption schemes were proposed[5-7].

In 2008, Selvi[8] proposed a signcryption scheme based on identity and gave the security proof. When number of signcryption was larger, ordinary signcryption had a low efficiency. Aggregation signcryption could aggregate several ciphertexts and provided batch verification, which greatly reduced the information transformation power consumption and the effectiveness of signcryption verification. So it was very suitable for the many-to-one mode in large-scale distributed communication. Ren[9] put forward a proven security signcryption scheme. In order to improve the efficiency of signcryption and shorten the length of ciphertext, Rao [10] proposed a new attribute-based signcryption (ABSC) scheme for LSSS-realizable access structures utilizing only 6 pairings and making the ciphertext size constant. Ch [11] proposed an efficient lightweight signcryption scheme based on HECC which fulfills all the security requirements. Cheng [12] proposed a corrected version of Liu et al's[13] scheme and proved his scheme was indistinguishable against adaptive chosen ciphertext attacks and was existentially unforgeable against chosen message attacks in the standard model.

However, the above signcryption schemes use lots of bilinear pairings computation, the effective is very low. In order to improve the efficiency of certificateless aggregate signcryption, we present a new certificateless aggregate signcryption(NCAS) scheme based on Exclusive OR (XOR). NCAS improves computation efficiency by reducing the computation number of bilinear pairings. What's more, we give the formal security proof under random oracle model for NCAS scheme. The new scheme has indistinguishability against adaptive chosen cipher-text attacks and beingness and unforgeability of adaptive chosen message attacks. We also make an analysis for cipher-text length and computational cost.

The followings are the structures of this paper. There are preliminaries in section2. Section3 is security model. We detailed introduce the new certificateless aggregate signcryption scheme in section4. Section5 demonstrates the new scheme's performance and followed by a conclusion in section6.

2. **Preliminaries.** Assuming that G_1 is a addition cyclic group of order q, G_2 is a multiplication cyclic group of order q, where q is a λ-bit prime. p is a generator of G_1. And discrete logarithm problems in G_1 and G_2 are difficulty. e is a bilinear pairing $e : G_1 \times G_2$ satisfying the following properties: bilinear, degenerative and computability.

- Computational Diffie-Hellman Assumption(CDHA): given (aP, bP) for unknown $a, b \in_R Z_q^*$, computing abP is difficulty.
- Computational Billinear Diffie-Hellman(CBDH): given (P, aP, bP, cP) for $a, b, c \in_R Z_q^*$, computing $e(P, P)^{abc}$ is difficulty.

3. **Security model.** We first give two definitions for security model of certificateless aggregate signcryption (CAS): confidentiality and unforgeability. Table1 is the explanation for some parameters used in this paper.

TABLE 1. Parameters explanation

Symbol	Explanation
$\hbar$	challenger
l_1, l_2	adversary
σ_i	signcrypt value
ID_i, ID_j	identity
ID_B	user
m_i	plaintext
M	message
P_0, P_{pub}	system public key
$s \in Z_q^*$	main key
U_i	user
Δ	state information
L	list
b	bit
R_i	key

Definition 1. For a NCAS scheme, if there is no any polynomial orders of magnitude adversary l_1(l_1 can win with non-ignorable advantage in indistinguishability against adaptive chosen cipher-text attacks game), then the scheme has the security properties of indistinguishability against adaptive chosen cipher-text attacks[13-15].

1. System initialization. Challenger $\hbar$ generates a system public parameter and sends it to adversary l_1, and saves the system main key.

Stage 1. Adversary can adaptively make the following polynomial orders of magnitude query.

(a) Secret value query. l_1 inputs $(ID_i, R_{1,i})$ to make query and gets secret value $(s_{1,i}, s_{2,i})$.

(b) Signcryption query. l_1 inputs (ID_i, ID_B, m_i) to make query and gets signcryption $\sigma_i = (v_i, c_i, R_i) = Signcrypt(ID_i, ID_B, m_i)$.

(c) De-signcrypt query. l_1 inputs signcryption σ_i and identity (ID_i, ID_j) to make query. $\hbar$ can make de-signcrypt and sends the (σ_i, ID_i, ID_j) to $\hbar$.

Stage 2. Similarly to stage 1, $\hbar$ can adaptively make the polynomial orders of magnitude query. And $\hbar$ cannot query the private key of ID_B or make de-signcrypt query.

Guess stage. At last, $\hbar$ submits a bit b'. If $b' = b$, then $\hbar$ wins this game. The advantage of adversary in this game is:

$$adv(\hbar) = |Pr[b' - b] - 0.5|. \tag{1}$$

Definition 2. For a NCAS scheme, if there is no any polynomial orders of magnitude adversary l_1(l_1 can win with non-ignorable advantage in adaptive chosen message attacks game), then the scheme has the beingness and unforgeability properties of adaptive chosen message attacks.

- System initialization. Challenger $\hbar$ generates a system public parameter Ω and sends it to adversary l_2, and saves the system main key.
- Query stage. Adversary l_2 executes the query similar to definition 1.
- Guess stage. Adversary l_2 generates a triple (σ_i, ID_i, ID_B), where secret value of ID_B has not been queried. σ_i is not the result by query. So if the result of $unsigncrypt(\sigma_i, ID_i, ID_B)$ is False, then adversary l_2 will win this game.

4. **New certificateless aggregate signcryption.** Detailed processes of NCAS are as follows.

- Step 1. System initialization. Supposing security parameter k, prime $q \geq 2^k$. $(G_1, +)$ and $(G_2, +)$ are cyclic groups of order q. Bilinear mapping $e : G_1 \times G_1 \to G_2$; $H_1 : 0, 1^* \times G_1 \to G_1$; $H_2, H_3 : 0, 1^* \times G_1 \to Z_q^*$; $H_4 : G_1 \times 0, 1^* \to G_1$ are four impact resistance hash functions. P is a generator of G_1. KGC randomly selects $s \in Z_q^*$ as system main key. Setting system public key $P_0 = sP$, message space $M = 0, 1^*$. System public parameter $\Omega = G_1, G_2, e, q, P, P_0, H_1, H_2, H_3, H_4$.
- Step 2. Generate user key. User U_i selects random number $s_{1,i} \in Z_q^*$ as a secret value. Then it computes public key $R_{1,i} = s_{1,i}P$.
- Step 3. Extract part private key of user. User U_i sends message to KGC. KGC first calculates $R_{2,i} = H_1(ID_1, R_{1,i})$, then calculates part private key $s_{2,i} = sR_{2,i}$. $s_{2,i}$ will be sent to corresponding user U_i trough secure channel. So the signature private key and public key of user are $(s_{1,i}, s_{2,i})$ and $(R_{1,i}, R_{2,i})$ respectively.
- Step 4. Individual signcryption. Aggregation signers select the entity U_0, its identity is ID_0. User U_i makes signcryption for message m_i, then sends it to user ID_B. The process is as follows:
  - U_0 randomly selects $u_0 \in Z_q^*$ and calculates $R_0 = u_0P$, then outputs R_0.
  - After U_i receives R_0, it randomly selects $r_i \in Z_q^*$.
    1. Compute $R_i = r_iP$.
    2. Compute $a_i = e(r_iP_{public}, R_{2,B})$.
    3. Compute $c_i = H_2(\alpha_i, ID_B) \oplus (ID_i||m_i)$. (In this paper, we stipulate that both sides of XOR have the same length.)

4. Compute $h_{i1} = H_3(ID_i||m_i, ID_B)$ and $h_{i2} = H_4(R_0, \Delta)$. Where $\Delta \in 0, 1^*$ is status messages.
5. Compute $v_i = s_{2,i}h_{i1} + (r_i + s_{1,i})h_{i2}$.
   So U_i sends the signcryption $\sigma_i = (v_i, c_i, R_i)$ of message m_i to ID_B.

- Step 5. Aggregation signcryption. Aggregation signer U_0 receives n signcryption $\sigma_i = (v_i, c_i, R_i)(i = 1, 2, \cdots, n)$. Compute $v = \sum_{i=1}^{n} v_i$, therefore, aggregation signcryption is $\sigma =< c_i, R_{ii=1}^{n}, V >$.
- Step 6. De-signcryption. ID_B executes de-signcryption.
  - Calculate $\alpha_i = e(R_i, s_{2,B}) = e(r_i P_{public}, R_{2,B})$.
  - Calculate $ID_i||m_i = H_2(\alpha_i, ID_B) \oplus c_i$.
  - Calculate $h_{i1} = H_3(ID_i||m_i, ID_B)$ and $h_{i2} = H_4(R_0, \Delta)$.
  If $e(V, P) = e(\sum_{i=1}^{n} h_{i1}R_{2,i}, P_0)e(h_{i2} \sum_{i=1}^{n}(R_i + R_{1,i}))$ is true, then it outputs message $ID_i||m_i$. Otherwise, the signcryption is invalid.

5. **Security and performance analysis.**

5.1. **Security analysis.**

Theorem 5.1. *Correctness of the NCAS scheme.*

$$e(V, P) = e(\textstyle\sum_{i=1}^{n}(s_{2,i}h_{i1} + (r_i + s_{1,i})h_{i2}), P) \tag{2}$$

$$= e(\textstyle\sum_{i=1}^{n} s_{2,i}h_{i1}, P)e(\sum_{i=1}^{n}((r_i + s_{1,i})h_{i2}), P) \tag{3}$$

$$= e(\textstyle\sum_{i=1}^{n} h_{i1}R_{2,i}, P_0)e(h_{i2}, \sum_{i=1}^{n}(R_i + R_{1,i})). \tag{4}$$

Theorem 5.2. *Based on CDHA and CBDH assumption, NCAS scheme satisfies IND-CCA2 security.*

Proof. l owns (P, aP, bP, cP). Adversary $\hbar$ makes a following interaction with l.
System initialization. l sets $P_0 = aP$ and selects system parameter
$G_1, G_2, e, q, P, P_{,0}, H_1, H_2, H_3, H_4$, then sends it to $\hbar$.

- Stage 1. Query. $\hbar$ executes the following query.
  1. H_1 query. l maintains list $L_1 = (ID_i, R_{1,i}, R_{2,i}, x_i, c_i)$. L_1 is initiated to be 0. When $\hbar$ inputs $ID_i, R_{1,i}$, l does the following response.
     - If the corresponding query of $(ID_i, R_{1,i})$ has been in the list L_1, then it outputs $R_{2,i}$.
     - Otherwise, l randomly selects $c_i \in 0, 1$. Supposing the probability of getting $c_i = 0$ is δ, then the probability of getting $c_i = 1$ is $1 - \delta$. Randomly select $x_i \in Z_q^*$, if $c_i = 0$, l returns $R_{2,i} = x_i bP$. If $c_i = 1$, l returns $R_{2,i} = x_i P$. At last, $(ID_i, R_{1,i}, R_{2,i}, x_i, c_i)$ is put into L_1.
  2. H_2 query. l maintains list $L_2 = (\alpha_i, ID_B, h_i)$. L_2 is initiated to be 0. When $\hbar$ inputs (α_i, ID_B), l does the following response.
     - If the corresponding query of (α_i, ID_B) has been in the list L_2, then it outputs γ_i.
     - Otherwise, l randomly selects $h_i \in_R Z_g^*(i \neq 0)$. Output h_i. At last, α_i, ID_B, h_i is put into L_2.
  3. H_3 query. l maintains list $L_3 = (ID_i, m_i, ID_B, h_{i1})$. L_3 is initiated to be 0. When $\hbar$ inputs (ID_i, m_i, ID_B), l does the following response.
     - If the corresponding query has been in the list L_3, then it outputs F.
     - Otherwise, l randomly selects $h_{i1} \in_R Z_g^*(i \neq 0)$. Output h_{i1}. At last, $(ID_i, m_i, ID_B, h_{i1})$ is put into L_3.
  4. H_4 query. l maintains list $L_4 = (R_0, \Delta, \mu_i, h_{i2})$. L_4 is initiated to be 0. When $\hbar$ inputs (R_0, Δ), l does the following response.

   - If the corresponding query of R_0, Δ has been in the list L_4, then it outputs h_{i2}.
   - Otherwise, l randomly selects ($\mu_i \in_R Z_g^*(i \neq 0)$). Compute $h_{i2} = \mu_i P$. Output h_{i2}. At last, $(R_0, \Delta, \mu_i, h_{i2})$ is put into L_4.
5. Secrete value query. l maintains list $L_K = (ID_i, R_{1,i}, R_{i2}, s_{1,i}, s2, i)$. L_K is initiated to be 0. When $\hbar$ inputs $(ID_i, R_{1,i})$, l does the following response.
   - If the corresponding query has been in the list L_K, then it outputs $(s_{1,i}, s_{2,i})$. If $R_{1,i}$ is replaced, then it outputs F.
   - Otherwise, l randomly selects $s_{1,i} \in_R Z_g^*$ and outputs $(s_{1,i}, s_{2,i} = sR_{2,i})$. At last, it puts $(ID_i, R_{1,i}, R_{i2}, s_{1,i}, s_{2,i})$ into L_K.
6. Public key query. l inputs ID_i to make query and does the following response.
   - If ID_i has been in the list L_K, then it outputs $R_{1,i}$.
   - Otherwise, if $s_{1,i}$ is true, then compute $R_{1,i} = s_{1,i}P$. Otherwise, l randomly selects $s_{1,i} \in_R Z_g^*$ and outputs $(R_{1,i} = s_{1,i}P)$. At last, it puts $ID_i, R_{1,i}, s_{1,i}$ into L_K.
7. Public key replacement query. l inputs $(ID_i, R_{1,i}^*)$ to make public key replacement query and does the following response.
   - If ID_i has been in the list L_K, then $R_{1,i}^*$ replaces $R_{1,i}$. And $s_{1,i} = F$.
   - Otherwise, the new (ID_i, ID_B, m_i) will be added into L_K.
8. Signcryption query. l inputs (ID_i, ID_B, m_i) to make query. $\hbar$ does the following response after asking L_1.
   - If $c_i = 1$, it uses the original signcryption algorithm to encrypt message and outputs the result.
   - If $c_i = 0$, l cancels the query.
9. De-signcryption query. l inputs aggregation signcryption σ to make query. The receiver of signcryption is ID_B. $\hbar$ checks that whether L_1 is in the corresponding data $(ID_i, R_{1,i}, R_{2,i}, s_{2,i}, x_i, c_i)$ of signcryption users' ID_i. If L_1 is not in that, then l cancels the query. Otherwise, l uses the general de-signcryption algorithm to decrypt message.

   In the simulation process, l may generate two same length messages m_{i0} and m_{i1}. It randomly selects parameters and runs the signcryption algorithm to get signcryption and aggregation signcryption σ_i, U_i of message m_{ib}. Then it returns σ^* to adversary $\hbar$.

- Stage 2 is similar to stage 1. However, adversary $\hbar$ cannot make de-signcryption query for $\sigma^* =< c_i, R_{ii=1}^n, R, V >$ and also cannot make H_1 query and secret value query for ID_B.

  Finally, $\hbar$ returns Guess. If equation is true, then output 1. Otherwise, output 0. Because adversary $\hbar$ cannot make de-signcryption query for $\sigma^* =< c_i, R_{ii=1}^n, R, V >$, so it needs to use (α_i, ID_B) to make H_2 query. $\alpha_i = e(R_i, s_{2,B})$. $s_{2,B}$ is the private key of receiver. And $s_{2,B} = abP$. Set $R_1 = cP$. We can get: $\alpha_i = e(R_i, s_{2,B}) = e(cP, abP) = e(P, P)^{abc}$.

Theorem 5.3. *Under the random oracle model, if the discrete logarithm problem(DLP) is difficulty, then our new aggregation signcryption scheme is security for any polynomial time adversary $\hbar$.*

Proof. l has a DLP instance $(P, Q = s_{1,r})P$. The aim of l is to compute $s_{1,r}$. Assuming that a adversary $\hbar_2$ satisfies polynomial time condition. Its proof is similar to proof of theorem 1. The following is the different part.

Private key query. $\hbar_2$ inputs $(ID_i, R_{1,i})$ to make query. l does the following response. If the corresponding $R_{1,i}$ in L_1 has been replaced, then return F. Otherwise, $ID_i = ID_r$,

l recovers $(ID_i, R_{1,i}, R_{2,i}, s_{1,i}, s_{2,i})$ in list L_1 and returns $(ID_i, R_{1,i}, R_{2,i}, *, *)$. Otherwise, $ID_i \neq ID_r$, l recovers $(ID_i, R_{1,i}, R_{2,i}, s_{1,i}, s_{2,i})$ in list L_K and returns $(R_{1,i}, R_{2,i}, s_{1,i}, s_{2,i})$.

Finally, $\hbar_2$ returns a fake information which is contained in a ciphertext sent by ID_r to receiver ID_B. l uses decryption oracle machine to decrypt message, which can lead to disclose forger (ID_i, m_i, v_i). If l makes right guess, namely $ID_i = ID_r$ and $ID_B \neq ID_r$, then decryption is finished. If $\sigma =< c_i, R_{i i=1}^{\;n}, V >$ is an effective aggregation signcryption including (c_r, m_r, R_r, v_r), and σ will be sent to ID_B. Then new algorithm can use oracle to obtain two legal signcryption information (ID_r, m_r, v_r') and (ID_r, m_r, v_r''), they meet $V_r' = s_{2,r}h_{r1}' + (r_r + s_{1,r})h_{r2}'$ and $V_r'' = s_{2,r}h_{r1}'' + (r_r + s_{1,r})h_{r2}''$. Where $h_{r1}' \neq h_{r1}''$, $h_{r2}' \neq h_{r2}''$. l can calculate $s_{1,r}$ successfully. Therefore, our new scheme has existential unforgeability against adaptive chosen messages attacks.

5.2. **Performance analysis.** We make a comparison to FAAS[17], PSIAS[18], MMCAS[19] and PSCHS[20] with our NCAS method. The explanation of symbols in this section: p: bilinear operation. e: exponent operation. s: point multiplication operation in G_1. $|G_1|$: the element length of corresponding group. $|m|$: the length of message. $|U|$: the length of user identity. $|DEMK|$: the KEY length of DEM[21].

Table 2 shows the calculation about the five algorithms. And we can know that signcrypter with NCAS only needs one pairing operation and two point multiplication operations in signcryption stage less than FAAS, PSIAS, MMCAS and PSCHS. In de-signcryption stage, NCAS needs $n + 3$ pairing operations obviously superior to PSCHS. The pairing operation number is more than FAAS, PSIAS and MMCAS. In that our new scheme dose not need exponent operation, the total calculation is superior to FAAS, PSIAS and MMCAS when n is big.

Table 2. Calculation comparison with different schemes

Scheme	Signcryption	De-Signcryption
FAAS	3ne	(n+1)p+(3n-3)s
PSIAS	n(p+e)+2s	3ns+np
MMCAS	3ne+np+ns	np+ns
PSCHS	2n(e+p)	6np+ne
NCAS	n(p+2s)	(n+3)p

In order to specifically analyze running time, we use the A type elliptic curve to test in jpbc database. Setting message $m = 512$ bit, $|G_1| = |G_2| = |G_{k-1}| = 160$ bit, $|Z_q^*|$ bit. $n = 5$. Then we record the running time with the above schemes as table3 from MATLAB platform. Its unit is second.

Table 3. Calculation time comparison with different schemes

Scheme	Signcryption time	De-Signcryption time
FAAS	513.348194	531.508835
PSIAS	614.040094	579.664869
MMCAS	819.531384	306.183189
PSCHS	681.116829	1187.770164
NCAS	442.922349	271.107759

Table 3 shows that the running time with NCAS is less than other schemes. It is the optimal scheme.

Next, we compare the ciphertext length as table4. PSCHS only has the non-signcryption length. From the table, the obvious is that although FAAS has the shortest ciphertext length, it does not has the certificateless characteristic. When message space length is less than $|G_{k-1}| = |G_2|$, NCAS is the best choice.

TABLE 4. Calculation comparison with different schemes

Scheme	Length of Signcryption	Length of De-Signcryption
FAAS	$m(\|U\| + \|G_1\|)$	$n\|U\| + \|G_1\|$
PSIAS	$m(\|U\| + \|m\| + 3\|G_1\| + Z_q^*)$	$m(\|U\| + \|m\| + 2\|G_1\| + Z_q^*) + \|G_1\|$
MMCAS	$m(\|U\| + \|G_2\| + \|G_1\| + \|G_{k-1}\|)$	$m(\|U\| + \|G_2\| + \|G_1\|) + \|G_{k-1}\|$
PSCHS	$m(\|U\| + \|G_2\| + 2\|G_1\| + DEMK\|)$	
NCAS	$m(\|U\| + \|m\| + 2\|G_1\|)$	$m(\|U\| + \|m\| + \|G_1\|) + \|G_1\|$

6. **Conclusions.** This paper proposes a new certificateless aggregate signcryption scheme. The new scheme can specify any user as aggregators. And aggregators can make initiation protocol. It has the characteristic of certificateless cryptosystem by using bilinear pairings to realize the aggregation for signcryption. Under the random oracle model, we proof the unforgeability of new scheme based on cryptology difficult problem. Finally, we make comparison to computational cost and ciphertext length. Results show that the new scheme not only increase ciphertext length, it also improves the calculation efficiency of certificateless aggregate signcryption.

Acknowledgment. The authors also gratefully acknowledge the helpful comments and suggestions of the reviewers, which have improved the presentation.

REFERENCES

[1] Lu X, Wen Q, Li W, et al. A Fuzzy Identity-Based Signcryption Scheme from Lattices, *[J], Ksii Transactions on Internet & Information Systems*, vol. 8, no. 11, pp. 4203-4225, November 2014.
[2] Yang L, Li J. Provably Secure Certificate-Based Signcryption Scheme without Pairings, *[J], Ksii Transactions on Internet & Information Systems*, vol. 8, no. 7, pp. 2554-2571, July 2014.
[3] Boyen X. Identity-Based Signcryption, Practical Signcryption. Springer Berlin Heidelberg, 2010, pp. 195-216.
[4] Yu G, Ma X, Shen Y, et al. Provable secure identity based generalized signcryption scheme, *[J], Theoretical Computer Science*, vol. 411, no. 40, pp.3614-3624, April 2010.
[5] Qi Z H, Yang H C, Huang H. An Efficient Identity-based Multi-signcryption Scheme, *[C], International Conference on Computer Information Systems and Industrial Applications. Atlantis Press*, pp. 308-310, May 2015.
[6] Pang L, Gao L, Li H, et al. Anonymous multi-receiver ID-based signcryption scheme, *[J], Iet Information Security*, vol. 9, no. 3, pp. 194-201, March 2015.
[7] Yan J, Wang L, Dong M, et al. Identity-based signcryption from lattices, *[J], Security & Communication Networks*, vol. 8,Issue 18,pp. 375-3770,December 2015.
[8] Selvi S S D, Vivek S S, Shriram J, et al. Identity Based Aggregate Signcryption Schemes, *[C] Progress in Cryptology - Indocrypt 2009, International Conference on Cryptology in India, New Delhi, India, 2009. Proceedings*, pp. 378-397, December 2009.
[9] Ren X Y, Qi Z H, Geng Y, Provably Secure Aggregate Signcryption Scheme[J], Etri Journal, vol. 34, no. 3, pp. 421-428, June 2012.
[10] Rao Y S, Dutta R. Efficient attribute-based signature and signcryption realizing expressive access structures, *[J], International Journal of Information Security*, vol. 15, no. 1, pp.1-29, February 2016.
[11] Ch S A, Uddin N, Sher M, et al. An efficient signcryption scheme with forward secrecy and public verifiability based on hyper elliptic curve cryptography,*[J], Multimedia Tools & Applications*, vol. 74, no. 5, pp.1711-1723, May 2015.
[12] Cheng L, Wen Q. An improved certificateless signcryption in the standard mode, *[J], International Journal of Network Security*, vol. 17, no. 5, pp. 597-606,Sept. 2015.
[13] Z. Liu, Y. Hu, X. Zhang, and H. Ma, Certificateless signcryption scheme in the standard model, *[J], Information Sciences*, vol. 180, no. 3, pp. 452-464,March 2010.

[14] Tang Q, Chen X. Towards asymmetric searchable encryption with message recovery and flexible search authorization, *[C]// ACM Sigsac Symposium on Information, Computer and Communications Security* pp. 253-264, 2013.

[15] Biswas D, Vidyasankar K. Privacy preserving and transactional advertising for mobile services, *[J]. Computing*, vol. 96, no. 7, pp. 613-630.

[16] You Z, Chen S, Wang Y. An efficient traffic data aggregation scheme for WSN based intelligent transportation systems[J]. Journal of Information Hiding & Multimedia Signal Processing, 2015, 6(6):1117-1129.

[17] WSun A D, Zhang Y Y.Aggregate signcryption scheme with full aggregation and constant ciphertext, *[J], Application Research of Computers*, vol. 32, no. 9, pp. 2820-2822, Sep. 2015.

[18] Wang D X, Teng J K. Provably secure identity-based aggregate signcryption scheme, *[J], Journal of Computer Applications*, vol. 35, no. 2, pp.412-415, Feb. 2015.

[19] iliang H, Fei C. The Multilinear Maps Based Certificateless Aggregate Signcryption Scheme, *[C], International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery. IEEE*, pp.92-99. Sept 2015.

[20] Yu H F, Yang B. Provably Secure Certificateless Hybrid Signcryption, *[J], Chinese Journal of Computers*, vol. 38, no. 4, April 2015.

[21] Abe MGennaro RKurosawa K.Tag-KEM/DEMa new framework for hybrid encryption, *[J], Journal of Cryptology* vol. 21, no.1, pp. 97-130, December 2008.