International Conference on Computer Science and Intelligent Communication (CSIC 2015)

Cryptanalysis of Attribute-Based Data Sharing Scheme for data access security in Cloud Computing

Aoting Hu, Rui Jiang*
School of Information Science and Engineering, Southeast University
NanJing, China
531888137@qq.com, R.Jiang@seu.edu.cn

Songyang Wu
Key Lab of Information Network Security
Ministry of Public Security
Shanghai, China
wusongyang@stars.org.cn

***Abstract*—With the development and the implementation of the data outsourcing technology in cloud computing, there are increasing demands and concerns for the data access security. Recently, Hur proposed a scheme and claimed the following achievements: 1) the key escrow problem. 2) realizing fine-grained user revocation. However, through our security analysis, there are three security flaws in Hur's scheme. Firstly, the scheme cannot ensure fine-grained user revocation security. We present two attacks, passive attack directed by revoked user and collusion attack, to illustrate its vulnerability, which will lead to disclosing the subsequent encrypted information for a revoked user.Secondly,we find out that the scheme cannot ensureuser secure join as it claimed, which means newly joined user is able to decrypt the message before his joining. Similarly, we present two attacks, passive attack directed by newly joined user and collusion attack, which lead to leakage of previous encrypted data for the new joining user. Thirdly, the key escrow problem cannot be solved completely in the scheme based on Dolev-Yao model, which means there is not any secure channel between the communication entities in, especially between the cloud server and users.Finally, in order to solve the above three security shortages in Hur's scheme, in this paper, we propose three countermeasures, which are efficient to withstand our proposed attacks.**

Keywords—Data sharing, CP-ABE, passive attack, collusion attack,revocation

I. Introduction

There is a trend for sensitive user data to be stored by third parties on the Internet. To achieve the fine-grained access control in encrypted data, Sahai and Waters [1] introduced a new type of Identity-Based Encryption (IBE) scheme called Attribute-Based Encryption (ABE). John Bethencourt [2] proposed a system for realizing complex access control on encrypted data named Ciphertext-Policy Attribute-Based Encryption (CP-ABE). However, the advantage of the CP-ABE comes with major drawback which is known as key escrow and key revocation. Therefore, several attribute revocable ABE schemes have been proposed [3], [4]. They realize attribute revocation based on timed rekeying mechanism which means they update periodically instead of revoking attributes immediately. Another user-revocation scheme [5], [6] recognized when user was revoked from only one attribute group, he lost all the access rights to the data sharing system. However, the two schemes also have limitation with the loss of availability. In [7] and [8], the authors also addressed fine-grained user revocation by exploiting the KGC to generate update secret key component. Thus, the key escrow problem is also inherent in these scheme. In [9], Hur proposed an access control mechanism which is capable of achieving fine-grained user revocation by exploiting the cloud server generate users' secret key component and update the ciphertext. In [10], Hur proposed a novel scheme which can both addressed fine-grained user revocation and key-escrow problem.

However, our security analysis shows that his protocol[10] has several security flaws and is vulnerable to our attacks. Firstly, his scheme cannot ensure fine-grained user revocation security under passive attacks and collusion attacks. Secondly, we find out that his scheme cannot ensure user safety join as he claimed. Thirdly, according to Dolev-Yao model, secure channel between the cloud server and users does not exist, so the key escrow problem cannot be solved completely in his scheme if the KGC listened for information in communication channel.

The contributions of this paper are as follows:

1) Our security analysis shows that Hur's scheme cannot ensure user revocation security. We provide two attacks against user revocation flaws. Firstly, passive attacks directed by revoked user will lead to disclosing the subsequent encrypted information by satisfying the ciphertext access policy with only one attribute. The revoked user download the old ciphertext and updated ciphertext from the cloud server and save it.Then, he uses the ciphertext and his secret key to computing the necessary component and decrypt the subsequent data. Secondly, that is collusion attacks directed by revoked user and the cloud server (or some unauthorized users). The cloud server obtained the new attribute group key and deliver it to revoked user, so he can update his secret key and decrypt the ciphertext. Otherwise, other user who possess the updated attribute obtain the new attribute group key and deliver it to revoked user, so the revoked user can update his secret key and decrypt the ciphertext.

2) We find out that Hur's scheme cannot ensure user join security as he claimed which means the newly joined user can decrypt the ciphertext before his joining. We provide two attacks against user join flaws as before.

3) According to Dolev-Yao model [11], the key-escrow problem cannot be solved for the reason that secure channel between cloud server and user is unrealistic in real communication channel. If the KGC listened for user's secret key component delivered by the cloud server from communication line, it can decrypt all the message uploaded in the cloud server without satisfying any access structure.

4) Based on three security flaws mentioned before, we present three countermeasures accordingly to prevent the scheme from our attacks. We presentthe suggestions on user revocation security, collusion attacks and key-escrow problem.

In this paper, we firstly review the Attribute-Based Data Sharing Scheme proposed by Hunbeon Hur in Section 2. In Section 3 we demonstrate how attacks workedspecific to user revocation flaws and user join flaws. Also, an attack directed by the KGC based on Dolev-Yao model directing at the flaws of key-escrow will be presented later. Then, countermeasures against Hur's protocol areput forward in Section 4. Section 5 gives conclusions.

II. Brief Review of Hur's Scheme

In this section, we briefly describe the Attribute-Based Data Sharing Scheme proposed by Hunbeon Hur[10].

A. Scheme description

*1) System setup:*The KGC choose a random exponent $\beta \in_R \mathbb{Z}_p^*$. The master public and private key pair is given by $(PK_K = h = g^{\beta}, MK_K = \beta)$. The data-storing center choose random exponents $\alpha, \gamma \in_R \mathbb{Z}_p^*$ .The mater public and private pair is given by $(PK_D = e(g,g)^{\alpha}, MK_D = g^{\alpha})$. Then publihes $PK_D^{agree} = g^{\gamma}$ while keep γ as secret.

*2) Key generation:*The KGC chooses random $r_j \in_R \mathbb{Z}_p^*$ for each attribute $j \in S$. Then, it computes the attribute keys and outputs them for a user u_t as $SK_{K,u_t} = (\forall j \in S\colon D_j = g^{r_t} \cdot H(j)^{r_j}, D_j{}' = g^{r_j})$. The data-storing center outputs $SK_{D,u_t} = D = g^{\frac{\alpha+r_t}{\beta}}$ and the user u_t can obtain its whole secret key set as $SK_{u_t} = \left(SK_{D,u_t}, SK_{K,u_t}\right)$. The data-storing center also outputs another $KEK = SK_{u_t}^{agree} = H(ID_t)^{\gamma} = Q_t^{\gamma}$ for the user.

3) Data encryption: The ciphertext encrypted by the data owner is $CT = (\mathcal{T}, \tilde{C} = Me(g,g)^{\alpha s}, C = h^s, \forall y \in Y\colon C_y = g^{q_y(0)}, C_y{}' = H(\lambda_y)^{q_y(0)})$. After the construction of CT, the data owner sent it to the data-storing center.

*4) Data re-encryption:*After the data owner upload the message, the cloud server re-encrypt the message. The algorithm progresses as follows:For all $G_y \in G$, chooses a random $K_{\lambda_y} \in \mathbb{Z}_p^*$. Then, the cloud re-encrypts CT and generates $CT' = (\mathcal{T}, \tilde{C} = Me(g,g)^{\alpha s}, C = h^s, \forall y \in Y\colon C_y = g^{q_y(0)}, C_y{}' = (H(\lambda_y)^{q_y(0)})^{K_{\lambda_y}})$ .The cloud selects random $\rho, R \in_R \mathbb{Z}_p^*$, and $\forall u_t \in G$, computes $x_t = H_1(e(Q_t^{\rho}, PK_D^{agree}))$.For all $G_y \in G$, constructs the polynomial function $f_y(x) = \prod_{i=1}^{m}(x - x_i) = \prod_{i=0}^{m} a_i x^i (mod\, p)$, where $G_y = \{u_1, \dots, u_m\}$; and the exponential function $\{P_0, \dots, P_m\} \equiv \{g^{a_0}, \dots, g^{a_m}\}$, where m represents the number of users in the attribute group.Constructs$Hdr_y = \{K_{\lambda_y} \cdot P_0^R, P_1^R, \dots, P_m^R,\}$, and generates a header message $Hdr = (g^{\rho}, \forall y \in Y\colon Hdr_y)$ .On receiving any data request query from a user, the data-storing center respond with (Hdr, CT') to the user.

5) Data decryption: When a user receives the ciphertext (Hdr, CT') from the data-storing center. Firstly, he computes$x_t = H_1(e(g^{\rho}, SK_{u_t}^{agree}))$. Then, he computes$K_{\lambda_j} \cdot P_0^R \cdot \prod_{i=1}^{m}(P_i^R)^{x_t^i} = K_{\lambda_j}$. Lastly, u_t updates its secret key with the attribute group keys as follows: $SK_{u_t} = (D = g^{\alpha + r_t/\beta}, \forall j \in S\colon D_j = g^{r_t} \cdot H(j)^{r_j}, D_j' = (g^{r_j})^{1/K_{\lambda_j}})$ .If and only if the user match the condition defined by data owner, the user can obtain $DecryptNode\left(CT, SK_{u_t}, R\right) = e(g,g)^{r_t s}$ and decrypt the ciphertext by computing $\tilde{C}/e(C,D)/A = M$.

B. Key update:

When a user comes to hold or drop an attribute, data-storing center rekeys the corresponding attribute group key. Suppose a user comes to hold or drop an attribute λ_i , The data-storing center selects a random $s' \in \mathbb{Z}_p^*$, and a $K_{\lambda_i}{}' \neq K_{\lambda_i}$. Then, it re-encrypts the ciphertext using the public parameters PK as $CT' = (\mathcal{T}, \tilde{C} = Me(g,g)^{\alpha(s+s')}, C = h^{(s+s')}, C_i = g^{(q_i(0)+s')}, C_i' = H(\lambda_i)^{(q_i(0)+s')^{K_{\lambda_i}'}}, \forall y \in Y \setminus \{i\} : C_y = g^{(q_y(0)+s')}, C_y{}' = H(\lambda_y)^{(q_y(0)+s')^{K_{\lambda_y}}})$.The data-storing center generates a new polynomial function $f^i(x)$ with updated attribute group G_i. Then it computes a newHdr $= (g^{\rho}, Hdr_i,$ $\forall y \in Y \{i\} : Hdr_y)$.Then, the legal user can access the attribute key $K_{\lambda_i}{}'$ from updated Hdr and updated his private key component as $D_i' = \left((g)^{r_i 1/K_{\lambda_i}}\right)^{K_{\lambda_i}/K_{\lambda_i}'} = (g)^{r_i 1/K_{\lambda_i}'}$ and decrypt the message.

III. Cryptanalytic Flaws In Hur's Protocol

A. Attacks on user revocation

1) Passive attack: Passive attack directed by revoked user means a revoked user is capable of decipher the subsequent data by taking advantage of parameters he already have and avoiding the whole attribute-based decryption.

Suppose the access policy of plaintext M is (λ_a AND λ_b AND λ_c AND λ_d) which means a user who possess both attributes λ_a , λ_b , λ_c , λ_d satisfy the access policy. The ciphertext uploaded to the cloud server was$CT' = (\mathcal{T}, \tilde{C} = Me(g,g)^{\alpha s}, C = h^s, \forall y \in \{a,b,c,d\}\colon C_y = g^{q_y(0)}, C_y' = (H(\lambda_y)^{q_y(0)})^{K_{\lambda_y}})$. A user possesses the attributes $\{\lambda_a, \lambda_b, \lambda_c, \lambda_d\}$, the secret key of the user is $SK_{K,u_t} = (D = g^{\frac{\alpha+r_t}{\beta}}, \forall j \in \{a,b,c,d\}\colon D_j = g^{r_t} \cdot H(j)^{r_j}, D_j' = (g^{r_j})^{1/K_{\lambda_j}})$. After that, the user is revoked attribute λ_d and he lose the access right to the plaintext M. The ciphertext is updated to $CT'' = (\mathcal{T}, \tilde{C} = M'e(g,g)^{\alpha(s+s')}, C = h^{(s+s')}, C_d = g^{(q_d(0)+s')}, C_d' = H(\lambda_d)^{(q_d(0)+s')^{K_{\lambda_d}'}}, \forall y \in \{a,b,c\} : C_y = g^{(q_y(0)+s')}, C_y{}' = H(\lambda_y)^{(q_y(0)+s')^{K_{\lambda_y}}})$. The user can apply for the updated ciphertext from the cloud server because the cloud server don't authenticate the qualification of the user.

The user stored the old ciphertext (Hdr, CT') and new ciphertext(Hdr', CT'') so far. Next, he can decrypt the updated ciphertext through his own calculation.

a) To decrypt the ciphertext CT', the revoked user computed $DecryptNode\left(CT', SK_{u_t}, a\right) = e(g,g)^{r_t \cdot q_a(0)}$ from leaf node a to the root node R as

$DecryptNode(CT', SK_{u_t}, R) = e(g,g)^{r_t s}$ and decrypt the ciphertext by computing$\tilde{C} /(e(C,D)/A) = M.$ In possess of plaintext M, he computed $Me(g,g)^{\alpha s}/M$ and obtained $e(g,g)^{\alpha s}$.

b) The revoked user computing $DecryptNode(CT'', SK_{u_t}, a) = e(g,g)^{r_t \cdot (q_a(0)+s^{'})}$with updated ciphertext and his secret key.

c) Then, the revoked user can obtain $e(g,g)^{r_t s^{'}}$ by computing $e(g,g)^{r_t \cdot (q_a(0)+s^{'})}/e(g,g)^{r_t \cdot q_a(0)}$.In the same way, he can obtain $Me(g,g)^{\alpha s^{'}}$ and $C = h^{s^{'}}$ by computing $M^{'}e(g,g)^{\alpha(s+s^{'})}/e(g,g)^{\alpha s}, h^{(s+s^{'})}/h^s$.

d) In the end, he can decrypt the subsequent message using above parameters by computing$\frac{M^{'}e(g,g)^{\alpha s^{'}} \cdot e(g,g)^{r_t s^{'}}}{e\left(h^{s^{'}}, g^{\frac{\alpha + r_t}{\beta}}\right)} = M'$.

2) *Collusion attack:*

In this case, collusion attacks refers to a revoked user collude with another user (unauthorized user) or with the cloud server to decrypt the ciphertext.

a) Collude with the cloud server. When the user is revoked attribute λ_d, The cloud server picks a new attribute group key $K^{'}_{\lambda_d}$ and update the ciphertext. If the cloud server collude with the revoked user and gives him $K^{'}_{\lambda_d}$, he can updates his secret key.With the updated secret key, he can decrypt the updated ciphertext by calling decryption function.

b) Collude with other unauthorized user. Some unauthorized user may don't have access right to the plaintext of the message, but he possess the attribute λ_d. He can decrypt$K^{'}_{\lambda_d}$ by computing $K^{'}_{\lambda_d} \cdot P_0^R \cdot \prod_{i=1}^{m}(P_i^R)^{x_t^i} = K^{'}_{\lambda_d}$ after he obtain the new Hdr'. Then he delivered the $K^{'}_{\lambda_d}$ to the revoked user. The revoked user can update his secret key and decrypt the ciphertext.

B. *Attacks on user join*

1) *Passive attack:*

Passive attack directed by newly joined user means a user who joined an attribute group lately is capable of decipher the previous data after his join.

In this section, suppose that access policy of plaintext M still be (λ_a AND λ_b AND λ_c AND λ_d) and a user possess the attribute $\{\lambda_a, \lambda_b, \lambda_c\}$ at first which means he have no right to decrypt the message. The ciphertext outsourced to data-storing center and re-encrypted as $\mathrm{CT}' = (\mathcal{T}, \tilde{C} = \mathrm{M}e(g,g)^{\alpha s}, \mathrm{C} = h^s, \forall \mathrm{y} \in \{\mathrm{a,b,c,d}\}: C_y = g^{q_y(0)}, (H(\lambda_y)^{q_y(0)})^{K_{\lambda_y}})$. In some instance, the user comes to hold attribute λ_d and become a legal user to plaintext M'. Meanwhile, the ciphertext uploaded to the data-storing center is updated to $\mathrm{CT}'' = (\mathcal{T}, \tilde{C} = \mathrm{M}'e(g,g)^{\alpha(s+s^{'})}, \mathrm{C} = h^{(s+s^{'})}, C_d = g^{(q_d(0)+s^{'})}, C_d^{'} = H(\lambda_d)^{(q_d(0)+s^{'})^{K^{'}_{\lambda_d}}}, \forall \mathrm{y} \in \{\mathrm{a,b,c}\} : C_y = g^{(q_y(0)+s^{'})}, C_y{}' = H(\lambda_y)^{(q_y(0)+s^{'})^{K_{\lambda_y}}})$. Also, a new polynomial function $f^d(x)$ generated by data-storing center added joined user's identity to the function. The secret key of joined user updated to $SK_{K,u_t} = (D = g^{(\alpha + r_t)/\beta}, D_d = g^{r_t} \cdot H(j)^{r_d}, D_d^{'} = (g^{r_d})^{1/K^{'}_{\lambda_d}}, \forall \mathrm{j} \in \{\mathrm{a,b,c}\}: D_j = g^{r_t} \cdot H(j)^{r_j}, D_j^{'} = (g^{r_j})^{1/K_{\lambda_j}})$

The user stored the old ciphertext $(\mathrm{Hdr}, \mathrm{CT}')$ and new ciphertext $(\mathrm{Hdr}', \mathrm{CT}'')$ so far. Next, he can decrypt the previous ciphertext through his own calculation.

a) The joined user computes $DecryptNode(CT^{''}, SK_{u_t}, a) = e(g,g)^{r_t \cdot (q_a(0)+s^{'})}$ by using updated ciphertext and updated secret key.Since that he is anauthorized user for all attribute group for message M, he computed $A = DecryptNode(CT'', SK_{u_t}, R) = e(g,g)^{r_t(s+s^{'})}$. In the end, he decrypted the message by computing $\tilde{C}/e(C,D)/A = M'$.

b) Then, the joined user computes $DecryptNode(CT', SK_{u_t}, a) = e(g,g)^{r_t \cdot q_a(0)}$ by usingthe previous ciphertext and his secret key.After that, hecomputes $e(g,g)^{r_t \cdot (q_a(0)+s^{'})}/e(g,g)^{r_t \cdot q_a(0)}$ to obtain $e(g,g)^{r_t s^{'}}$ .He computes $e(g,g)^{r_t(s+s^{'})}/e(g,g)^{r_t s^{'}}$ to obtain $e(g,g)^{r_t s}$.

c) Last, hedecrypts message M by computing$\tilde{C}/e(h^s, g^{(\alpha + r_t)/\beta})/e(g,g)^{r_t s} = M$.

2) *Collusion attack:*

Similarly, collusion attacks here refers to a newly joined user collude with other user (unauthorized user) or with the cloud server to decrypt the ciphertext before her joining.

a) Collude with the cloud server.When the user add attribute λ_d, The cloud server picks a new attribute group key $K^{'}_{\lambda_d}$ and update the ciphertext. If the cloud server collude with the revoked user and gives him the old attruibute group key K_{λ_d}, he can degenerate his secret key to $SK_{K,u_t} = (D = g^{(\alpha + r_t)/\beta}, \forall j \in \{a,b,c,d\}: D_j = g^{r_t} \cdot H(j)^{r_j}, D_j^{'} = (g^{r_j})^{1/K_{\lambda_j}})$. With the secret key, he can decrypt the previous ciphertext by calling decryption function.

b) Collude with other unauthorized user. If other unauthorized user always possess the attribute λ_d and he saves the previous attribute group key K_{λ_d}. Then, the joined user collude with him and degenerate his secret key and decrypt the previous ciphertext.

C. *Attacks on key-escrow problem*

According to Dolev-Yao model [13], the key-escrow problem cannot be solved completely for the reason that secure channel between cloud server and user is unrealistic in real communication channel. In Hur's paper, the key escrow problem is solved by escrow-free key issuing protocol, which is constructed using the secure two- party computation between the KGC and the data-storing center. According to Dolev-Yao model, saboteurs are "active" eavesdroppers that can tap the communication line to obtain messages and then try everything he can in order to discover the plaintext. Thus, it is unreasonable to suppose the cloud server and user shared a secure channel since that user could be far away from the cloud server. If the KGC taps the communication line between cloud server and one user and eavesdrop$D = g^{(\alpha + r_t)/\beta}$, they can decrypt every ciphertext downloaded from cloud server even without satisfying the access structure. Attacks proceed by the KGC as follows: First, the KGC download a ciphertext from the cloud server randomly as $\mathrm{CT}^{'} = (\mathcal{T}, \tilde{C}, \mathrm{C} = h^{s}, \forall \mathrm{y}: C_y, C_y{'})$;Then, it computes $\mathrm{e}(g^{\beta s}, g^{r_t/\beta}) = e(g,g)^{r_t s}$; Finally, itdecrypts the message by calculating $\tilde{C}/e\left(h^{s}, g^{(\alpha+r_t)/\beta}\right)/e(g,g)^{r_t s} = M$. It is worth noting the KGC just need to succeed in eavesdropping $D = g^{(\alpha+r_t)/\beta}$from one user, he can decipher the ciphertext stored in cloud server once for all.

IV. Countermeasures

In this section, several proposals will be put forward based on the cryptanalytic flaws in Hur's protocol raised before.

A. *Suggesions on user revocation scurity*

To prevent the attacks from revoked user and newly joined user, oursuggetion to make up for the cryptanalytic flaws is adjust the re-encryption method to $\mathrm{CT}' = (\mathcal{T}, \tilde{C} = \mathrm{M}' e(g,g)^{\alpha(s\cdot s^{'})}, \mathrm{C} = h^{(s\cdot s^{'})}, C_d = g^{(q_d(0)\cdot s^{'})}, C_d^{'} = H(\lambda_d)^{(q_d(0)\cdot s^{'})^{K_{\lambda_d}^{'}}}, \forall \mathrm{y} \in \{\mathrm{a,b,c,d}\} : C_y = g^{(q_y(0)\cdot s^{'})}, C_y{'} = H(\lambda_y)^{(q_y(0)\cdot s^{'})^{K_{\lambda_y}}})$. At this circumstance, the passive attacks directed by revoked user and joined user will be useless. When a revoked user use one of her attribute λ_a to decrypt, he computes $\mathrm{DecryptNode}\left(\mathrm{CT}, SK_{u_t}, \mathrm{a}\right) = e(g,g)^{r_t\cdot(q_a(0)\cdot s^{'})}$ and cannot extract $e(g,g)^{r_t s^{'}}$ anymore. As long as he cannot obtain $K_{\lambda_d}^{'}$ from updated Hdr', the ciphertext is unbreakable from her.As for newly joined user, the method is also applicable for the reason that he also need $e(g,g)^{r_t\cdot(q_a(0)+s^{'})}$ to be divisible.

B. *Suggesionson collusion attack*

Collusion attacks proceeded by cloud server and revoked users or newly joined users should be avoided on account of that we cannot ensure user and the cloud server is fully trusted. One solution is that when there is user revocation or user join, the data owner is responsible for generating updated attribute secret key component which is bond to a polynomial with all user's (users with this attribute) identity and send it to the cloud server. The cloud server cannot decipher the attribute key component because it cannot generate the authorized user's parameter with its identity to satisfy the polynomial. Meantime, the data owner generate another part of ciphertext update parameter and sent it to the cloud sever to update ciphertext component. In this way, the cloud server is not capable of update any user's attribute key and collusion attacks is no longer exist.

C. *Suggesionson key-escrow problem*

According to Dolev-Yao model, we cannot rely on secure cannel to solve key- escrow problem for the reason that there is no secure channel in real communication environment. User's secret key generated by the cloud server should be delivered with secrecy. Under this circumstances, a trusted authority (like the KGC, or the KGC itself) should be introduced to authenticate the identity of the cloud server and users and generate the public and private key when they register to the authority. In possess of public and private key, the user's secret key can be encrypted with user's public key for confidentiality and encrypted with the cloud server's private key for source authentication.

V. Conclusion

In this paper, we have shown the three security flaws of the protocol proposed by Hur. Firstly, his scheme cannot ensure fine-grained user revocation security. We propose two attacks, passive attack directed by revoked user and collusion attack, to illustrate its vulnerability. Secondly, we find out that the scheme cannot ensure user secure join as it claimed, which means newly joined user is able to decrypt the message before his joining. Thirdly, the key escrow problem cannot be solved completely in the scheme based on Dolev-Yao model, which means there is not any secure channel between the communication entities in, especially between the cloud server and users. Finally, in order to solve the above three security shortages in Hur's scheme, in this paper, we propose three countermeasures, which are efficient to withstand our proposed attacks.

Acknowledgment

This work is supported by the National Natural Science Fou ndation of China(NO.61202448), and the Key Laboratory Prog ram of Information Network Security of Ministry of Public Sec urity (No.C14610).

References

[1] Sahai A, Waters B. Fuzzy identity-based encryption[M]//Advances in Cryptology–EUROCRYPT 2005. Springer Berlin Heidelberg, 2005: 457-473.J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68-73.

[2] Bethencourt J, Sahai A, Waters B. Ciphertext-policy attribute-based encryption[C]//Security and Privacy, 2007. SP'07. IEEE Symposium on. IEEE, 2007: 321-334.

[3] Cheung L, Newport C. Provably secure ciphertext policy ABE[C]//Proceedings of the 14th ACM conference on Computer and communications security. ACM, 2007: 456-465.

[4] Di Vimercati S D C, Foresti S, Jajodia S, et al. Over-encryption: management of access control evolution on outsourced data[C]//Proceedings of the 33rd international conference on Very large data bases. VLDB endowment, 2007: 123-134.

[5] Canetti R, Hohenberger S. Chosen-ciphertext secure proxy re-encryption[C]//Proceedings of the 14th ACM conference on Computer and communications security. ACM, 2007: 185-194.

[6] Liang X, Cao Z, Lin H, et al. Attribute based proxy re-encryption with delegating capabilities[C]//Proceedings of the 4th International Symposium on Information, Computer, and Communications Security. ACM, 2009: 276-286.

[7] Yu S, Wang C, Ren K, et al. Attribute based data sharing with attribute revocation[C]//Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security. ACM, 2010: 261-270.

[8] Naruse T, Mohri M, Shiraishi Y. Provably secure attribute-based encryption with attribute revocation and grant function using proxy re-encryption and attribute key for updating[J]. Human-centric Computing and Information Sciences, 2015, 5(1): 1-13.

[9] Hur J, Noh D K. Attribute-based access control with efficient revocation in data outsourcing systems[J]. Parallel and Distributed Systems, IEEE Transactions on, 2011, 22(7): 1214-1221.

[10] Hur J. Improving security and efficiency in attribute-based data sharing[J]. Knowledge and Data Engineering, IEEE Transactions on, 2013, 25(10): 2271-2282.

[11] Dolev D, Yao A C. On the security of public key protocols[J]. Information Theory, IEEE Transactions on, 1983, 29(2): 1