Journal of Southeast University (English Edition) Vol. 37, No. 3, pp. 251 – 257 Sept. 2021 ISSN 1003—7985

Novel dynamic anti-collusion ciphertext policy attribute-based encryption scheme in 5G D2D environment

Xu Xiangjie Jiang Rui

(School of Cyber Science and Engineering, Southeast University, Nanjing 210096, China)

Abstract: To share data securely with secure attribute revocation, anti-collusion, and dynamic user management in the 5G device-to-device (D2D) environment, a novel dynamic anti-collusion ciphertext policy attribute-based encryption (NDA-CP-ABE) scheme in the 5G D2D environment is proposed. On the basis of the ciphertext policy attribute-based encryption algorithm, fine-grained access control and secure attribute revocation are realized, and the confidentiality of data is guaranteed. A polynomial function is adopted in the ciphertext generation phase to realize dynamic user management. A random number is used to prevent a collusion attack among the legitimate user equipment (UE), revoked UE, and external network attackers. Finally, on the basis of the Diffie-Hellman problem, the NDA-CP-ABE scheme is formally proved, and the simulation performances are compared with those of similar schemes. The results show that data can be securely shared through a D2D channel with secure attribute revocation, anti-collusion, and dynamic user management. Moreover, compared with similar schemes, the NDA-CP-ABE scheme has higher efficiency in encryption, decryption, and storage.

Key words: device-to-device (D2D); attribute revocation; user management; dynamic anti-collusion ciphertext policy attribute-based encryption (NDA-CP-ABE); access control

DOI: 10.3969/j.issn.1003 – 7985.2021.03.003

The widespread application of the 5G mobile network greatly increases the amount of user equipment (UE), which brings much overhead to 5G base stations. Device-to-device (D2D) communication is considered a promising technology that releases the pressure on 5G base stations because the UE can communicate directly with each other without being directly involved in the 5G infrastructure. In addition, D2D communication can alleviate the mobile traffic explosion problem[1] and solve the problem of a spectrum resource shortage in a wireless communication system. However, data security is difficult to guarantee.

To realize data confidentiality protection in a data-sharing system, the data access control method is widely used. However, the traditional method of access control has multiple copies of ciphertext for different users with different keys, which may cause much storage overhead. Sahai et al.[2] proposed the concept of the attribute-based encryption (ABE) algorithm, which has two types: ciphertext policy attribute-based encryption (CP-ABE)[3] and key policy attribute-based encryption (KP-ABE)[4]. CP-ABE schemes[5–9] became promising for their efficient and fine-grained data access control. However, these schemes cannot realize attribute revocation. Yang et al.[10] proposed a cloud storage system based on CP-ABE to realize efficient data access control with attribute revocation. However, the users whose attributes were revoked may threaten the security of the scheme through a collusion attack.

The schemes[11–14] could achieve attribute revocation but could not realize dynamic user management. Wei et al. proposed an attribute-based access control scheme for multi-authority cloud storage[15] by adopting the binary tree to dynamically remove the user from the system. However, this algorithm incurred more computational overhead. Han et al. proposed a CP-ABE scheme that realized the application of hidden policy and white-box traceability[16]. However, although the illegal and invalidated users could be removed from the system in this scheme when new users joined the system, the proposed algorithm would become inapplicable. Thus, this scheme could only realize partial user management.

5G access and handover security, IoT security, D2D security, V2X security, and network slice security are five aspects of security for the current 3GPP 5G network[17]. 5G D2D communication provides efficient and low-latency service for the UE and should be designed to meet security requirements, such as low computational cost, secure and effective device discovery, confidentiality and integrity protection, secure group communication, and fine-grained access control of devices. To solve the problem of data confidentiality in D2D communication, Zhang et al.[18] proposed a secure data-sharing protocol, which merged the advantages of public-key cryptography

Received 2021-01-28, **Revised** 2021-07-01.

Biographies: Xu Xiangjie (1995—), male, graduate; Jiang Rui (corresponding author), male, doctor, associate professor, R. Jiang@seu.edu.cn.

Foundation items: The National Natural Science Foundation of China (No. 61372103), the Natural Science Foundation of Jiangsu Province (No. SBK2020020282), the Program of Key Laboratory of Information Network Security of the Ministry of Public Security (No. C19607), the Program of Key Laboratory of Computer Network Technology of Jiangsu Province.

Citation: Xu Xiangjie, Jiang Rui. Novel dynamic anti-collusion ciphertext policy attribute-based encryption scheme in 5G D2D environment [J]. Journal of Southeast University (English Edition), 2021, 37(3): 251 – 257. DOI: 10.3969/j.issn.1003 – 7985.2021.03.003.

and symmetric encryption to achieve data security in D2D communication. However, the protocol could not support fine-grained data access control. Yan et al. [19] proposed a flexible data access control scheme in D2D communications to realize secure data communication among UE, but the computational cost of the scheme was high. Li et al. [20] proposed a data access control scheme with multi-authority CP-ABE encryption in D2D communication. However, the multiple authorities may waste the network resources because the distributed authorities were not suitable for the D2D communication scenario.

1 Preliminaries

1.1 Bilinear mapping

Definition 1 (bilinear mapping) Let G_1, G_2 and G_3 be three multiplicative cyclic groups of the same prime order p. Let e: $G_1 \times G_2 \rightarrow G_3$ denote a bilinear map defined with the properties of bilinearity, non-degeneracy, and computability[21]. In bilinearity, $e(u^a, v^b) = e(u, v)^{ab}$, $\forall u \in G_1$, $\forall v \in G_2$, and $a, b \in Z_p$, where Z_p denotes an integer group with prime order p. In non-degeneracy, $\exists u \in G_1$, $\exists v \in G_2$ such that $e(u, v) \neq I$, where I is the identity element of G_3. In computability, for any element $u \in G_1$, $v \in G_2$, there is a polynomial-time algorithm to calculate $e(u, v)$.

1.2 Decisional bilinear Diffie-Hellman problem

Definition 2 (DBDH problem) Let g be a generator of group G with prime order p and $a, b, c, d \in Z_p$ be randomly chosen. Make $g^a, g^b, g^c \in G_p$ public. It is difficult to distinguish between $(g, g^a, g^b, g^c, e(g, g)^{abc})$ and $(g, g^a, g^b, g^c, e(g, g)^d)$ [22].

Definition 3 The function Fu, which outputs $z \in \{0, 1\}$, has advantage ε for solving the DBDH problem in group G, supposing that

$$\| P_r[\mathrm{Fu}(e(g, g)^{abc}) = 0] - P_r[\mathrm{Fu}(e(g, g)^d) = 0] \| \geqslant \varepsilon$$

1.3 Linear secret sharing scheme

Definition 4 (linear secret sharing scheme) A secret sharing scheme over a set of parties P is called a linear secret sharing scheme (LSSS) if the shares for each party form a vector over Z_p, and there is a matrix $\boldsymbol{M}$ called the share-generating matrix[23]. The matrix $\boldsymbol{M}$ has m rows and n columns. For $i = 1, 2, \ldots, l$, the i-th row $\boldsymbol{M}_i$ of $\boldsymbol{M}$ is labeled as $\rho(i)$, where ρ denotes the function from $i = 1, 2, \ldots, m$ to P. Given a column vector $\boldsymbol{v} = \{s, y_2, \ldots, y_n\}$, where $s \in Z_p$ is the secret to be shared and $y_2, y_3, \ldots, y_n \in Z_p$ are randomly chosen; $\boldsymbol{Mv}$ is the vector of m shares of the secret s according to the scheme. The party $\rho(i)$ obtains the share $\lambda_i = (\boldsymbol{Mv})_i$ of s from $\boldsymbol{Mv}$.

2 NDA-CP-ABE Scheme

2.1 System model

Fig. 1 presents the system architecture of the NDA-CP-ABE scheme in the 5G D2D environment. The system includes four kinds of entities: Trusted Authority, Core Server, Cloud, and UE, whose functions and characteristics are introduced as follows.

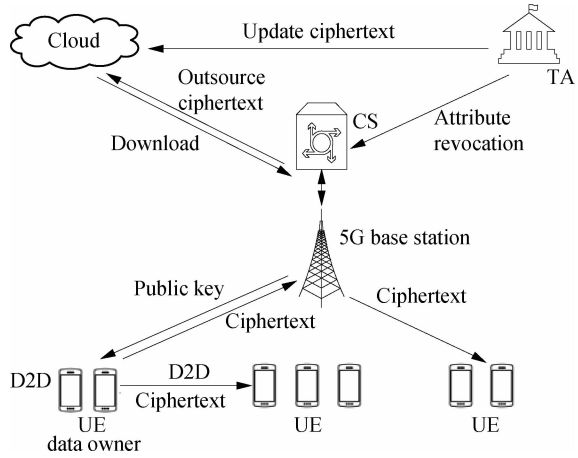

Fig. 1 System architecture of the NDA-CP-ABE scheme

Trusted Authority (TA) is a trusted entity and is responsible for generating the security parameter. The TA outputs the secret keys and the corresponding update keys to the UE and performs the user management and attribute revocation process. Core Server (CS) is the core server of the 5G infrastructure and provides high-speed Internet service. The CS controls the normal operation of the base stations, which is responsible for transferring data to the other entities, including the D2D devices. The Cloud is responsible for storing the data uploaded from the UE. It also provides the ciphertext update service for attribute revocation and user management. UE communicate with each other through the D2D channel. The data owner of the UE defines the access policy and directly transmits the ciphertext (C_T) to the other UE. The data owner of the UE can also outsource the ciphertext to the Cloud for further use.

2.2 Construction of the NDA-CP-ABE scheme

2.2.1 System initialization

The steps of system initialization are as follows.

1) D2D setup. The CS generates a public/private key pair (p_i, s_i) for each UE_i, where p_i is the public key and s_i is the secret key for D2D discovery. Then the CS sends the key pair (p_i, s_i) to UE_i through the secure channel.

2) Secure D2D discovery. UE_1 generates $R = r \| I_1 \| t_1$ and $T_1(R)$, where r denotes UE_1's request for D2D discovery; I_1 is UE_1's identity information; t_1 is the time stamp; and $T_1(R)$ is a signature of R with s_1. The SHA256 signature algorithm is used to generate the signature for the UE. Then, UE_1 broadcasts the request of $R \| T_1(R)$. After receiving the request from UE_1, UE_2 checks the received R with the R computed by verifying $T_1(R)$. After successful verification, UE_2 generates $R_S = r' \| I_2 \| t_2$ and $T_2(R_S)$, where r' denotes UE_2's response for discov-

ery; t_2 is the time stamp; I_2 is UE_2's identity information; and $T_2(R_S)$ is the signature of R_S with s_2. Then, UE_2 returns $R_S \| T_2(R_S)$ to UE_1. UE_1 checks the received R_S with the R_S computed by verifying $T_2(R_S)$. After successful verification, the D2D communication channel is opened. The data owner UE_1 constructs the secure D2D channel and shares data with UE_2, UE_3, …, UE_n. In the same way, the discovery procedures among UE_2, UE_3, …, UE_n can be finished.

3) TA setup. The TA initializes the system with the TA setup algorithm: TA Setup $(1^\lambda) \rightarrow (S_K, P_K, \{V_k, P_k\}, \tau_T)$, which inputs the security parameter λ and outputs $S_K = (\alpha, \beta)$, $P_K = (e(g, g)^\alpha, g^\beta)$. S_K and P_K are the secret key and public key of the TA, respectively. The TA also outputs $\{V_k = v_k, P_k = [g^{v_k} H(\gamma_k)]^\beta\}$, which are the secret version key and public key of each attribute γ_k, respectively. τ_T denotes the minimum time difference threshold in the system.

4) UE setup. The UE sends its identity information N to the TA, and then the TA conducts the UE Setup algorithm, UE Setup $(N) \rightarrow (GPK_N, GSK_N)$, to compute and return each UE's global public key $GPK_N = g^N$ and global secret key $GSK_N = z_N$.

5) Time synchronization. Each sender of the entities records the current time τ_1 when every piece of information is to be sent and appended τ_1 to the information. Upon receiving the information from other entities, the receiver entity should obtain the current time τ_2. If $|\tau_1 - \tau_2| < \tau_T$, the conversation continues. Otherwise, the receiver entity returns $\tau_1 \| \tau_2 \| e$ to the sender entity. e denotes the error code of the current conversation.

2.2.2 Secret key generation

In this subsection, the TA generates the secret keys for each UE. The detailed secret key generation step is as follows.

The TA assigns the valid UE a set of attributes S_j and then generates the UE's secret key SK_j:

$$SK_j = (K_j, K_{j,k}) = [K_j = g^{1/z_j + u/\alpha}, K_{j,k} = (g^{v_k} H(\gamma_k))\beta u_j]$$

where $\forall j \in S_U$, $\gamma_k \in S_j$, u_j is randomly chosen, and S_U denotes the set of all the UE. After generating the secret keys, the TA securely sends the secret keys to the corresponding UE. The attribute set S_j consists of many attributes according to the UE's gender, nationality, academic degree, or much other information of different levels.

2.2.3 Ciphertext generation

In this section, UE_i (data owner) defines the data access policy and encrypts the data according to the corresponding attributes. The detailed encryption process is as follows.

UE_i first chooses a random value s and then sends g^s to the TA, where s is the secret value in the LSSS. After receiving g^s, the TA computes $g^{\alpha s}$ and constructs the polynomial function $f_p(x) = \prod_{j=1}^{m}(x - z_j) = \sum_{i=0}^{m} a_i x^i \pmod q$ and the exponential function $\{W_0, W_1, \ldots, W_m\} = \{g^{a_0}, g^{a_1}, \ldots, g^{a_m}\}$. After that, the TA constructs $E = \{g^{\alpha s} W_0, W_1, \ldots, W_m\}$, and sends E to UE_i. UE_i then generates the ciphertext: $C_T = (C, D_i, E, E_i) = \{C = Me(g, g)^{\alpha s}, D_i = g^{r_i}, E = \{g^{\alpha s} W_0, W_1, \ldots, W_m\}, E_i = g^{\lambda_i}(P_k) - r_i\}$, where $i \in \{1, 2, \ldots, l\}$, the value r_i and vector $\boldsymbol{v} = (s, y_2, \ldots, y_n)$ are randomly chosen, and $\lambda_i = (\boldsymbol{Mv})_i$ is a share of secret s. UE_i shares C_T with the other UE such as UE_j, directly through the D2D channel. To backup C_T, UE_i outsources C_T to the Cloud.

2.2.4 Data decryption

After receiving C_T, UE_j first obtains $E = \{g^{\alpha s} W_0, W_1, \ldots, W_m\}$ from C_T and computes $F = g^{\alpha s} W_0 \prod_{i=1}^{m}(W_i)^{z_j^i} = g^{\alpha s}$ and then calculates token T_K with secret key SK_j and C_T as follows:

$$T_K = \frac{e(F, K_j)}{\prod_{i \in I}[e(E_i, GPK_j) e(D_i, K_{j,i})]^{\omega_i}} = e(g, g)^{s\alpha/z_j}$$

where $I = \{i: \rho(i) \in I_A\}$; I_A denotes the set of attributes that satisfy the access structure; and $\{\omega_i\}_{i \in I_A}$ are the chosen constants that can reconstruct the secret s on the condition that $\{\lambda_i\}_{i \in I_A}$ are valid shares of s. After determining T_K, UE_j can decrypt the ciphertext with $GSK_j = z_j$ and C as follows: $M = C/T_K^{z_j} = Me(g, g)^{\alpha s}/e(g, g)^{\alpha s}$.

2.2.5 Attribute revocation

When the attribute γ_k of UE_μ is revoked, the TA generates a new attribute version key $V_k' = v_k'$ and the new attribute update key $A_k = \beta(V_k' - V_k)$ for the attribute γ_k, and then TA calculates the key update key for the non-revoked UE to update the secret key to the latest version: $U_{j,k} = g^{u A_k}$. The TA then sends $U_{j,k}$ to the non-revoked UE. Meanwhile, the TA updates the public key of the revoked attribute γ_k to the latest version: $P_k' = P_k g^{A_k}$. Upon receiving the update key $U_{j,k}$, the non-revoked UE runs the secret key update algorithm to update SK_j to the latest version: $SK_j' = (K_j', K_{j,k}') = (K_j' = K_j, K_{j,k}' = K_{j,k} U_{j,k})$. For any attribute which is not revoked, $K_{j,k}' = K_{j,k}$.

The TA then generates $U_k' = D_i^{-A_k/\gamma}$ to update the corresponding C_T and constructs the polynomial function $f_p'(x) = \prod_{j=1, j \neq \mu}^{m}(x - z_j)$ and the exponential function $\{W_0, W_1, \ldots, W_{m-1}\} = \{g^{a_0}, g^{a_1}, \ldots, g^{a_{m-1}}\}$. Subsequently, the TA constructs $E' = \{g^{\alpha s} W_0, W_1, \ldots, W_{m-1}\}$, and sends E' to the Cloud.

After receiving E', the Cloud randomly chooses a value r_i' in Z_p and then updates $C_T' = (C, D_i', E', E_i')$, where $E' = \{g^{\alpha s} W_0, W_1, \ldots, W_{m-1}\}$. For the attributes that are revoked, $E_i' = E_i(P_k')^{-r_i'} U_k'$, $D_i' = D_i g^{r_i'}$.

2.2.6 User management

When UE_μ in the UE set S_U is removed from the system for certain reasons, the TA should remove it directly without updating other legitimate UE's secret keys.

The TA first constructs the polynomial function $f'_p(x) = \sum_{i=0}^{m-1} a_i x^i \pmod q$ and the exponential function $\{W_0, W_1, \ldots, W_{m-1}\} = \{g^{a_0}, g^{a_1}, \ldots, g^{a_{m-1}}\}$. Then, the TA constructs E' to the Cloud. After receiving E', the Cloud updates the ciphertext C_T. The remaining legitimate UE, such as UE_j, can download C_T from the cloud and then compute F. Subsequently, UE_j calculates $T_K = e(F, K_j) \Big/ \prod_{i \in I_A} [e(E_i, g^j) e(D_i, K_{j,i})]^{\omega_i}$ and finally decrypts $M = C/T_K^{z_j}$.

When a new user UE_n wants to enter the system, the TA constructs the polynomial function $f'_p(x) = \sum_{i=0}^{m+1} a_i x^i \pmod q$ and the exponential function $\{W_0, W_1, \ldots, W_{m+1}\}$. Then, the TA constructs $E' = \{g^{\alpha s} W_0, W_1, \ldots, W_{m+1}\}$ and sends E' to the Cloud. After receiving E', the Cloud updates the ciphertext C_T. UE_n downloads C_T from the cloud, and computes $F = g^{\alpha s}$. Then, UE_n calculates $T_K = e(g, g)^{s\alpha/z_n}$ and finally obtains M.

3 Formal Security Analysis

3.1 Proof of correctness

Theorem 1 The NDA-CP-ABE scheme is correct; that is, legitimate UE can successfully decrypt C_T, and can achieve safe attribute revocation and user management.

Proof If UE_j, which holds sufficient attributes, satisfies the access policy Fu, it obtains C_T and secret keys SK_j to compute $F = g^{\alpha s} W_0 \prod_{i=1}^{m} (W_i)^{z_j} = g^{\alpha s}$ to obtain $F = g^{\alpha s}$ and then calculates $T_K = e(F, K_j) \Big/ \prod_{i \in I_A} [e(E_i, g^j) e(D_i, K_{j,i})]^{\omega_i}$, where $e(K_j, F) = e(g, g)^{su_j} e(g, g)^{s\alpha/z_j}$, $\prod_{i \in I_A} [e(E_i, g^j) e(D_{1,i}, K_{j,k})]^{\omega_i} = e(g, g)^{u_j \sum_{i \in I_A} \lambda_i \omega_i} = e(g, g)^{su_j}$.

UE_j then decrypts the ciphertext to obtain the plaintext $M = C/T_K^{z_j}$. Therefore, UE_j can successfully decrypt the ciphertext corresponding to its attribute set.

3.2 Proof of security

Theorem 2 The NDA-CP-ABE scheme can resist a chosen-ciphertext attack (CCA). If an adversary has an advantage ε that can be neglected in polynomial time for attacking the NDA-CP-ABE scheme with at most q_k, q_c, and q_d numbers of queries in the Secret Key Generation phase, Ciphertext Generation phase, and Data Decryption phase, respectively, with maximum time t; then the challenger can solve the DBDH problem with an advantage of $P_r = \varepsilon(1 - q_k/2^n)/(q_k q_e q_d)$, which can be neglected in polynomial time.

Proof Suppose that there is an adversary who has advantage ε for attacking the NDA-CP-ABE scheme.

Setup the challenger generates $S_K = (\alpha, \beta)$, $P_K = (e(g, g)^{\alpha}, g^{\beta})$, which are the secret key and public key of the TA, respectively, and $\{V_k = v_k, P_k = [g^{v_k} H(\gamma_k)]^{\beta}\}$, which are the secret version key and public key of each attribute γ_k, respectively. Then, the adversary selects a set of attributes S_k that satisfy the access structure. The challenger then sends the public keys to the adversary of the attribute set S_k.

Phase 1 is that the adversary selectively refers (j, S_j) in S_A to the challenger to obtain the corresponding secret key SK_j. The challenger then calculates the secret key as follows: $SK_j = [K_j = g^{1/z_j + u/\alpha}, K_{j,k} = (g^{v_k} H(\gamma_k))^{\beta u_j}]$.

The adversary refers to two messages m_0 and m_1 of equal length but cannot decrypt the challenge message properly with the queried keys and any other keys from S_k. The challenger then randomly chooses a bit of b in $\{0, 1\}$, encrypts it under the access structure, and then sends C_T to the adversary.

Phase 2 is similar to Phase 1. The adversary refers (j, S_j) in S_A to the challenger to obtain the corresponding secret key SK_j. However, the secret key does not satisfy the access policy.

When the adversary ends Phase 2, it provides a guess b' of b. The probability that the adversary will win the game for all arbitrary attribute sets the adversary chooses is $P_1 = (C_n^k + C_n^{k+1} + \ldots + C_n^n)/(C_n^0 + C_n^1 + \ldots + C_n^n) < 1$, and the probability of $S_j \neq S_k$ is that $P_2 = 1 - q_k/2^n$. There are q_k, q_e, and q_d numbers of queries in the secret key generation phase, ciphertext generation phase, and data decryption phase, respectively, with advantage ε. Therefore, the advantage ε' in solving the DBDH problem is $\varepsilon' < \varepsilon(1 - q_k/2^n)/(q_k q_e q_d)$. The challenger cannot solve the DBDH problem with advantage ε'. Therefore, the adversary cannot breach the NDA-CP-ABE scheme in the polynomial time with a non-neglected advantage. Therefore, NDA-CP-ABE can resist the CCA.

3.3 Collusion attack resistance

Theorem 3 NDA-CP-ABE is secure with collusion attack resistance; that is, it can prevent the collusion attack among the legitimate UE, the revoked UE, and the external attackers.

Proof For the legitimate UE and the revoked UE, the attribute $k \in S_1$ of UE_1 is revoked, and UE_2 is the legitimate UE with attribute set S_2. The ciphertext is encrypted with $W = S_1 \cup S_2$. The key update key, $U_{j,k} = g^{uA_k}$, is associated with every UE's identity. Therefore, UE_1 and UE_2 cannot update their secret key to the latest version and cannot decrypt the ciphertext.

For the legitimate UE and external attacker, UE_3 is the legitimate UE with attribute set S_3, and UE_4 is the network attacker. The ciphertext is encrypted with $W = S_3 \cup S_4$, where S_4 denotes the extra attribute set needed to decrypt the ciphertext for UE_3. The secret key SK_j is associated with u_j, which is randomly chosen. Therefore, UE_3 and UE_4 cannot decrypt the C_T, either collectively or individually.

For the collusion attack between the revoked UE, $\gamma_5 \in S_5$ of UE_5 and $\gamma_6 \in S_6$ of UE_6 are revoked. The ciphertext is encrypted with $W = S_5 \cup S_6$. The secret key SK_j and update key $U_{j,k} = g^{u_j A_k}$ are associated with u_j, which is randomly chosen. Therefore, UE_5 and UE_6 cannot share the secret keys related to their attributes to decrypt the ciphertext.

3.4 Attribute revocation security

Theorem 4 The scheme can achieve attribute revocation security.

Proof When the attribute set $\{\gamma_k\} \subset S$ of UE_μ is revoked, C_T should be updated to the latest version: $C'_T = (C, D_i, E', E'_i)$, where $E' = \{g^{\alpha s} W_0, W_1, \ldots, W_{m-1}\}$. For the attributes that are revoked, $E'_i = E_i(P'_k) - r'_i U'_k$, $D'_i = D_i g^{r'_i}$. UE_μ calculates the exponent of U'_k with difficulty. Additionally, because of the revoked UE's blindness by the random number r'_i, the component $(P'_k)^{-r'_i}$ cannot be canceled out. Therefore, the revoked UE cannot successfully attack the NDA-CP-ABE scheme, and the NDA-CP-ABE scheme can realize attribute revocation security.

3.5 User management security

Theorem 5 The NDA-CP-ABE scheme can realize secure, dynamic, and efficient user management.

Proof When UE_μ is directly removed from the system, the ciphertext is updated to the latest version C'_T. UE_μ calculates the component E' with difficulty, which prevents UE_μ from computing F, which is necessary to decrypt the ciphertext because $F \neq g^{\alpha s}$. Therefore, UE_μ cannot decrypt the updated ciphertext. UE_μ strives to obtain the plain text of the ciphertext.

UE_j is supposed to be the newly joined UE. The TA first constructs $f'_p = \prod_{j=1}^{m-1}(x - z_j)$. The Cloud updates C'_T, and UE_j can compute $F' = g^{\alpha s}$. The decryption token is $T_K = e(g, g)^{s\alpha/z_j}$. Then, UE_j can obtain the plaintext $M = C/T_K^{z_j}$. Therefore, the new UE dynamically joins the system.

3.6 Security comparison

In this section, the security performance of NDA-CP-ABE is compared with Xue et al.'s scheme[13] (Scheme 1), Wei et al.'s scheme[15] (Scheme 2), Han et al.'s scheme[16] (Scheme 3), Yan et al.'s scheme[19] (Scheme 4), and Li et al.'s scheme[20] (Scheme 5) in terms of attribute revocation, collusion attack resistance, user management, and whether these schemes support the 5G D2D environment in Tab. 1. Therein, "√" and "×" mean that the scheme can and cannot meet the corresponding security goal, respectively.

According to Tab. 1, the NDA-CP-ABE scheme can successfully realize collusion attack resistance, secure attribute revocation, and secure user management in the 5G D2D environment. However, Scheme 1 cannot realize dynamic user management and is not fit for the 5G D2D scenario; Scheme 2 cannot realize secure attribute revocation and is not fit for the 5G D2D scenario; Scheme 3 can only realize partial user management because the algorithm in Scheme 3 cannot support the new users to dynamically enter the system. In addition, Scheme 3 cannot realize attribute revocation, collusion attack resistance, and fitness for the 5G D2D scenario. Scheme 4 cannot realize attribute revocation, collusion attack resistance and dynamic user management. Scheme 5 cannot realize secure attribute revocation and dynamic user management.

Tab. 1 Security Comparison

Scheme	Attribute revocation	Collusion attack resistance	User management	5G D2D environment
Scheme 1[13]	√	√	×	×
Scheme 2[15]	×	√	√	×
Scheme 3[16]	×	×	Partial	×
Scheme 4[19]	×	×	×	√
Scheme 5[20]	×	√	×	√
NDA-CP-ABE	√	√	√	√

4 Performance Analysis

The performances of computational overhead and storage overhead are compared in this section by comparing the NDA-CP-ABE scheme with the schemes in Refs. [13, 15 − 16, 19 − 20]. The simulation is conducted on an Ubuntu 16.04 system with a 2.20 GHz processor and 4.00 GB RAM.

4.1 Computational overhead

This section compares the NDA-CP-ABE scheme for computational overhead with the schemes in Refs. [13, 15 − 16, 19 − 20] in terms of encryption and decryption. The computational cost of multiplicative operation c_m, exponential operation c_e, hash function c_h, and the pairing operation c_p in the group G is considered. The number of attributes n_a ranges from 2 to 20, and the number of UE n_u in the system is 100.

4.1.1 Encryption overhead

The computational cost for encryption among six schemes is compared in Fig. 2. The computational cost of

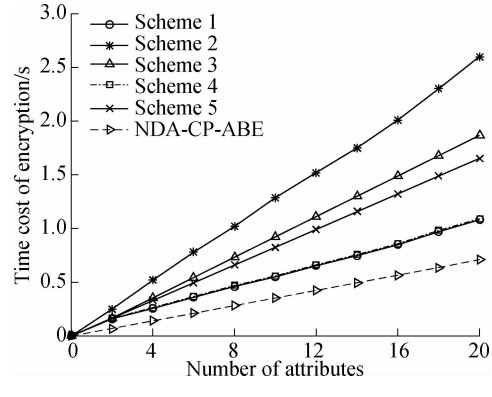

Fig. 2 Comparison of encryption time

the NDA-CP-ABE scheme($(3c_e + c_h)n_a + c_m$) is smaller than that of Scheme 1 ($(2c_e + c_m)n_a$). Although the former has ($n_a - 1$) more multiplicative calculations, the latter has n_a more hash calculations, and n_a more exponential calculations. In addition, the encryption cost of the NDA-CP-ABE scheme is much less than those of Scheme 2 to Scheme 5 which are $(6c_e + 4c_m + c_h)n_a + (c_e + c_m)n_u$, $(5c_e + 3c_m)n_a + 3c_m + 3c_e$, $(2c_e + 2c_m)n_a + c_e$, and $(5c_e + 2c_m)n_a$, respectively.

4.1.2 Decryption overhead

The computational cost for decryption among the six schemes is compared in Fig. 3. The decryption cost of the NDA-CP-ABE scheme($(2c_p + c_m + c_e)n_a + c_m + 2c_e$) is less than that of Scheme 1 ($(3c_p + 2c_m)n_a + c_e$). Although the former has ($n_a + 1$) more exponential calculations, the latter has n_a more paring calculations and ($n_a - 1$) more multiplicative calculations. The computational cost of the NDA-CP-ABE scheme is much less than those of Scheme 2 and Scheme 3 which are $(4c_p + 4c_m + c_e + c_h)n_a$ and $(3c_p + 2c_m + c_e)n_a + 2c_p + 3c_e + 5c_m$. The decryption cost of the NDA-CP-ABE scheme is less than that of Scheme 4 ($(2c_p + 3c_m)n_a$). Although the former has ($n_a + 2$) more exponential calculations, the latter has ($2n_a - 1$) more multiplicative calculations. The decryption cost of NDA-CP-ABE is slightly higher than that of Scheme 5 ($(3c_p + c_e)n_a$) because the latter has n_a more paring calculations while the former has ($n_a + 1$) more multiplicative calculations and two more exponential calculations. However, Scheme 5 cannot realize secure attribute revocation and dynamic user management.

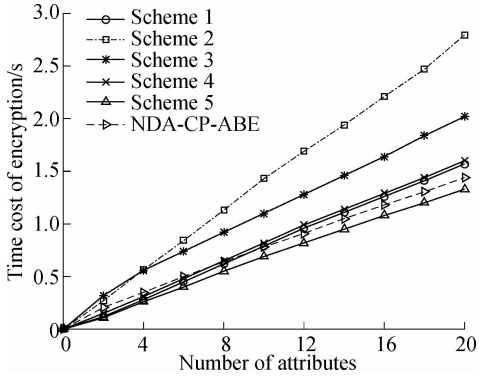

Fig. 3 Comparison of decryption time

4.2 Storage overhead

In this section, the NDA-CP-ABE scheme for storage overhead of the ciphertext is compared with the schemes in Refs. [13, 15 − 16, 19 − 20]. s_m denotes the size of the plaintext M. The storage overhead of the NDA-CP-ABE scheme ($(s_m + 2n_a + 1) \mid p \mid$) is smaller than those of Scheme 1 to Scheme 5 which are $(3n_a + 3 + s_m) \mid p \mid$, $(5n_a + 4 + s_m) \mid p \mid$, $(3n_a + 1 + s_m) \mid p \mid$, $(2n_a + s_m)n_j \mid p \mid$, and $(3n_a + 1 + s_m) \mid p \mid$, respectively. n_j denotes the number of junctions needed in Ref. [19]. Generally speaking, $n_j > 1$.

5 Conclusions

1) The secure sharing of data in the 5G D2D environment is realized. The ciphertext policy attribute-based encryption algorithm is adopted to realize safe data sharing. Only the UE with sufficient attributes that satisfy the access policy defined by the data owner can decrypt the ciphertext.

2) Secure attribute revocation in the 5G D2D environment is realized. When the attributes of the UE are revoked, the CP-ABE algorithm only updates other related UE's attribute keys to control the access rights. The revoked UE can no longer decrypt the ciphertext after the secure attribute revocation.

3) Dynamic and efficient user management in the 5G D2D environment is realized. The polynomial function algorithm is adopted to encrypt the data. When UE loses the permission to the data, the algorithm dynamically removes the UE from the system without updating other UE's relating attribute keys. When new UE obtains permission to enter the system, the algorithm assigns the UE the access right to the ciphertext without updating the existing UE's relating attribute keys.

4) The NDA-CP-ABE scheme can withstand a collusion attack among the legitimate UE, the revoked UE, and the external attackers with the secret value related to each piece of UE in the 5G D2D environment.

References

[1] Tan J, Liang Y, Zhang L, et al. Deep reinforcement learning for joint channel selection and power control in D2D networks[J]. *IEEE Transactions on Wireless Communications*, 2021, **20**(2): 1363 − 1378. DOI: 10.1109/TWC.2020.3032991.

[2] Sahai A, Waters B. Fuzzy identity-based encryption[C]//2005 24*th Annual International Conference on Theory and Applications of Cryptographic Techniques*. Aarhus, Denmark, 2005: 457 − 473. DOI: 10.1007/11426639_27.

[3] Bethencourt J, Sahai A, Waters B. Ciphertext-policy attribute-based encryption[C]//2007 *IEEE Symposium on Security and Privacy*. Oakland, CA, USA, 2007: 321 − 334. DOI: 10.1109/SP.2007.11

[4] Goyal V, Pandey O, Sahai A, et al. Attribute-based encryption for fine-grained access control of encrypted data [C]//2006 *ACM Conference on Computer and Communications Security*. Alexandria, VA, USA, 2006: 89 − 98. DOI: 10.1145/1180405.1180418.

[5] Xue K, Xue Y, Hong J, et al. RAAC: Robust and auditable access control with multiple attribute authorities for public cloud storage[J]. *IEEE Transactions on Information Forensics and Security*, 2017, **12**(4): 953 − 967. DOI: 10.1109/TIFS.2016.2647222.

[6] Li J, Lin X, Zhang Y, et al. KSF-OABE: Outsourced attribute-based encryption with keyword search function for cloud storage[J]. *IEEE Transactions on Services Computing*, 2017, **10**(5): 715 − 725. DOI: 10.1109/TSC.2016.2542813.

[7] Ning J, Cao Z, Dong X, et al. Auditable sigma-time out-

sourced attribute-based encryption for access control in cloud computing[J]. *IEEE Transactions on Information Forensics and Security*, 2018, **13**(1): 94 - 105. DOI: 10.1109/TIFS.2017.2738601.

[8] Mao X, Lai J, Mei Q, et al. Generic and efficient constructions of attribute-based encryption with verifiable outsourced decryption[J]. *IEEE Transactions on Dependable and Secure Computing*, 2016, **13**(5): 533 - 546. DOI: 10.1109/tdsc.2015.2423669.

[9] Wang N, Fu J, Bhargava B K, et al. Efficient retrieval over documents encrypted by attributes in cloud computing [J]. *IEEE Transactions on Information Forensics and Security*, 2018, **13**(10): 2653 - 2667. DOI: 10.1109/TIFS.2018.2825952.

[10] Yang K, Jia X. Expressive, efficient, and revocable data access control for multi-authority cloud storage[J]. *IEEE Transactions on Parallel and Distributed Systems*, 2014, **25**(7): 1735 - 1744. DOI: 10.1109/TPDS.2013.253.

[11] Hur J, Noh D K. Attribute-based access control with efficient revocation in data outsourcing systems[J]. *IEEE Transactions on Parallel and Distributed Systems*, 2011, **22**(7): 1214 - 1221. DOI: 10.1109/TPDS.2010.203.

[12] Yeh L, Chiang P, Tsai Y, et al. Cloud-based fine-grained health information access control framework for lightweight IoT devices with dynamic auditing and attribute revocation[J]. *IEEE Transactions on Cloud Computing*, 2018, **6**(2): 532 - 544. DOI: 10.1109/TCC.2015.2485199.

[13] Xue Y, Xue K, Gai N, et al. An attribute-based controlled collaborative access control scheme for public cloud storage[J]. *IEEE Transactions on Information Forensics and Security*, 2019, **14**(11): 2927 - 2942. DOI: 10.1109/TIFS.2019.2911166.

[14] Li J, Yao W, Han J, et al. User collusion avoidance CP-ABE with efficient attribute revocation for cloud storage [J]. *IEEE Systems Journal*, 2018, **12**(2): 1767 - 1777. DOI: 10.1109/JSYST.2017.2667679.

[15] Wei L, Liu W, Hu X. Secure and efficient attribute-based access control for multiauthority cloud storage[J]. *IEEE Systems Journal*, 2018, **12**(2): 1731 - 1742. DOI: 10.1109/JSYST.2016.2633559.

[16] Han D, Pan N, Li K. A traceable and revocable ciphertext-policy attribute-based encryption scheme based on privacy protection[J]. *IEEE Transactions on Dependable and Secure Computing*, 2020, **99**. DOI: 10.1109/TDSC.2020.2977646.

[17] Cao J, Ma M, Li H, et al. A survey on security aspects for 3GPP 5G networks[J]. *IEEE Communications Surveys & Tutorials*, 2020, **22**(1): 170 - 195. DOI: 10.1109/COMST.2019.2951818.

[18] Zhang A, Chen J, Hu, R Q, et al. SeDS: Secure data sharing strategy for D2D communication in LTE-advanced networks[J]. *IEEE Transactions on Vehicular Technology*, 2016, **65**(4): 2659 - 2672. DOI: 10.1109/TVT.2015.2416002.

[19] Yan Z, Xie H, Zhang P, et al. Flexible data access control in D2D communications[J]. *Future Generation Computer Systems*, 2018, **82**(62): 738 - 751. DOI: 10.1016/j.future.2017.08.052.

[20] Li Q, Huang L, Mo R, et al. Robust and scalable data access control in D2D communications[J]. *IEEE Access*, 2018, **6**: 58858 - 58867. DOI: 10.1109/ACCESS.2018.2874066.

[21] Krawczyk H. HMQV: A high-performance secure Diffie-Hellman protocol[C]//*Advances in Cryptology—CRYPTO* 2005. Santa Barbara, CA, USA, 2005: 546 - 566. DOI: 10.1007/11535218_33.

[22] Wang J M, Lang B. An efficient KP-ABE scheme for content protection in information-centric networking[C]// 2016 *IEEE Symposium on Computers and Communication* (*ISCC*). Messina, Italy, 2016: 830 - 837. DOI: 10.1109/iscc.2016.7543839.

[23] Beimel A. *Secure schemes for secret sharing and key distribution*[D]. Israel: Department of Computer Science, Institution of Technology, 1996.

5G D2D 中新型防共谋密文策略属性基加密方案

徐相杰　蒋　睿

(东南大学网络空间安全学院, 南京 210096)

摘要: 为了在 5G 网络 D2D(设备到设备)环境中实现数据安全传输、安全的属性撤销、防共谋和动态的用户管理,提出了一种新型防共谋密文策略属性基加密方案(NDA-CP-ABE). 基于密文策略属性基加密算法,实现了数据细粒度的访问控制和属性的安全撤销,保障了数据的机密性,并在密文的生成阶段采用多项式方程来实现安全且高效的用户管理. 将随机数用于防止合法用户设备、被撤销用户设备和外部网络攻击者之间的共谋攻击. 最后基于 Diffie-Hellman 难题,对 NDA-CP-ABE 方案进行了形式化证明,并与同类型的方案进行了仿真性能比较. 比较结果表明,数据可以在 D2D 通道中安全传输,并且保障了属性撤销、防共谋和动态的用户管理. 此外,与其他同类型方案相比,NDA-CP-ABE 方案在加密、解密和存储方面更为高效.

关键词: D2D;属性撤销;用户管理;密文策略属性基加密;访问控制

中图分类号: TN918.4