A New Access Control System Based on CP-ABE in Named Data Networking

Tao Feng, Jiaqi Guo
(Corresponding author: Jiaqi Guo)

School of Computer and Telecommunications, Lanzhou University of Technology
287, Lanping Road, Qilihe District, Lanzhou 730050, China
(Email: flyingfairy@163.com)

(Received Mar. 22, 2017; revised and accepted June 26 & July 29, 2017)

Abstract

Named Data Networking (NDN) paradigm introduces a novel security communication model where any router in the network can store mass data, which is convenient for consumers to obtain data from any nearby router. However, such a radical change causes new challenges for NDN access control since the data publisher loses control over the published data. In most of the existing access control mechanisms in NDN, publishers are required to be always online to authenticate consumers, also revocation and user privacy is considered scarcely. Focusing on those problems, the work of this paper is proposing a new access control system in NDN, which comprises the framework and algorithm, security definition and proof. The basic of this paper is a decentralized ciphertext-policy attribute based encryption (CP-ABE) scheme under prime order groups, which solves the above problems effectively. In this new scheme, indirect revocation can be combined with the in-network storage technique in NDN properly. Privacy is guaranteed by using the partially-hidden access structure to realize recipient anonymity. Finally, it is proved to be static security.

Keywords: Access Control; CP-ABE; NDN; Privacy-reserving; Revocable

1 Introduction

In current Internet, consumers are mainly interest in accessing and consuming content, irrespective of where the content comes from and who publishes the content. It is difficult for the traditional TCP/IP network to meet the new requirements, such as supporting massive content distribution, mobility, security and so on. Therefore, researchers consider changing the network architecture radically. Information Centre Networking (ICN) [30] is a candidate of future Internet which employs a content-oriented mechanism instead of host-oriented mechanism. NDN [31] is an emerging ICN project, as the same, it treats content as core element. NDN relies on in-network storage which makes the same content distribute to multiple locations in the network, so it is convenient for consumers to get content from any neighbor router.

Considering the particular architecture of NDN, especially the in-network storage, access control is very important for the security in NDN. Once data is published in the network, it will be stored in any router where it passes by. So the publishers face the risk of losing control of published data. Therefore, more and more researchers pay attention to access control in NDN [28].

However, most existing NDN access control schemes need publishers always online to authenticate consumers, which is impractical and leads to bad effects on in-network storage of routers. What's more, in these schemes, revocation is not considered and even the publisher-always-online problem is not resolved. Using Attribute-based Encryption (ABE) can overcome this problem [2, 32]. However, a trusted central authority (CA) is needed in such schemes, which has all the keys of the system, it is prejudicial to system security. In addition, the access structure included in ciphertext also reveal the sensitive information of users.

To address the problems above, a new access control model in NDN is constructed and an efficient NDN access control scheme is proposed. This scheme is decentralized, revocable and privacy-preserving without breaking the in-network storage mechanism of NDN. For publishers, they can develop the access policy by themselves; and for consumers, they can easily get the data from nearby routers; for both of them, their sensitive privacy information included in access structure will be hidden. In general, the system proposed in this work has the following goals:

Decentralization. A secure access control system in NDN is presented based on a CP-ABE scheme [23] which has multiple attribute authorities (AAs) but without a central authority (CA), so that it is more practical. Also, the scheme is on the base of prime order groups with high efficiency.

Revocability. An indirect revocation approach is proposed for the above scheme based on periodically updating attribute-based keys of the non-revoked consumers. Both backward and forward security is achieved.

Privacy-preserving. Anonymous access structures are used to make the sensitive information hidden, namely the attribute values are hidden. So this scheme realizes recipient anonymity and privacy-preserving.

The structure of this work arranged as follows. In Section 2 are some works about access control in NDN and ABE schemes. Some preliminaries are presented in Section 3. The system model, security requirements, security assumptions and security game are all given in Section 4. The formal algorithms of this scheme are described in Section 5. Sections 6 and 7 analyzes security and performance respectively. Finally, conclusion and prospect are in Section 8.

2 Related Works

2.1 Access Control in NDN

Differ from the IP network, in NDN, requesting and publishing content are both based on content name rather than IP address. In order to retrieval content effectively, there are two kinds of packets in NDN as shown in Figure 1. The interest packet carries the requirement of the consumer, while the data packet carries content.

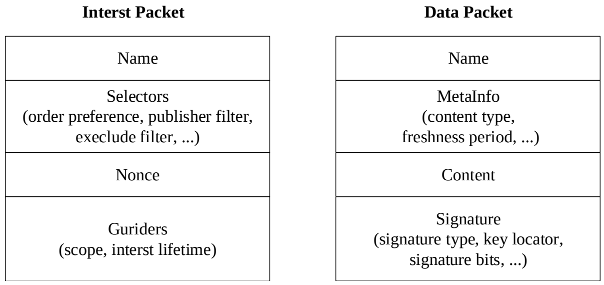
Interst Packet
Name
Selectors
(order preference, publisher filter, execlude filter, ...)
Nonce
Guriders
(scope, interst lifetime)
Data Packet
Name
MetaInfo
(content type, freshness period, ...)
Content
Signature
(signature type, key locator, signature bits, ...)

Figure 1: Packets in NDN architecture

In NDN, the publisher signs a packet for its integrity and authenticity, but fine-grained access control is also required. Thanks to in-network storage, routers can satisfy corresponding requirements in interest packets irrespective of whether the interests are from authorized or unauthorized consumers. So access control in NDN cannot be implemented by a single entity. Therefore, Jacobson *et al.* [31] mentioned that access control in NDN can be achieved based on encryption. Data encryption is an effective way of access control, but the traditional encryption cannot be used in NDN efficiently, since the number of consumer increases, and the encrypted copies of each data will also increase proportionally.

The existing access control schemes in NDN are showed in Table 1. In schemes [7, 9, 11, 26, 29], an always online publisher is required for authenticating consumers, but it is impractical and affects the in-network storage mechanism in NDN. Revocation is not considered in schemes [9, 11, 17, 29], and in schemes [25], although it solves the problem of user revocation, a proxy server is also required to be always online, and the formal algorithm and security proof are not given. The access control mechanisms without effective revocation can't be used in practice. An effective revocable access control scheme accommodates the in-network storage mechanism in NDN has not been reported.

2.2 ABE Schemes

In 2005, the concept of ABE first appeared in the scheme of fuzzy identity-based encryption [24]. Using ABE, publishers can share data with specific consumers without their public keys and identities [27]. Two more practical ABE schemes were constructed on the first ABE scheme, key-policy ABE (KP-ABE) [10, 19] and ciphertext-policy ABE (CP-ABE) [3,14]. This paper considers publisher developing and performing access control policy, so CP-ABE is used because the access structure is included in ciphertext. Recently, the original ABE has been improved, and various practical ABE schemes have been proposed which can achieve multi-AA, revocation, hidden access structure and so on.

Chase *et al.* proposed the first multi-authority ABE scheme [5], then some multi-authority CP-ABE schemes had been presented [16,22], but the CA in these schemes has all the keys of the system. Then Chase and Chow [6] presented a scheme where CA is not needed, but it is only constructed on AND structure. Subsequently, a fully decentralized CP-ABE scheme without CA [15] is presented in 2011. In 2015, an improved large-scale decentralized multi-authority CP-ABE scheme is proposed [23], which is based on prime order groups and it is more efficient in practice.

Revocation is a challenge problem in ABE-based access control system [18]. Directly revocation is applied in [1], while in [4] an indirectly revocation is proposed. Effectively revocation is added in KP-ABE scheme in the indirect mode [12].Cui and Deng used the indirectly revocation technique into a decentralized CP-ABE scheme to realize fine-grained revocation [8]. In NDN, the ciphertext updating caused by directly revocation cannot be completed synchronously in each cache of NDN routers. Therefore, the indirect revocation mechanism is more suitable for NDN.

The first CP-ABE scheme with anonymity proposed in 2008 [21], where the access policy only supports AND gates structure. Recently, a CP-ABE scheme with anonymous access structure is proposed [13], which can be expressed as any LSSS [20] matrix and fully security.

Based on Rouselakis's work [23], combining with in-network storage strategy in NDN, this paper proposes a

Table 1: Summary of the access control schemes in NDN

Schemes	**Based on**	**Revocation**	**Always-online Publisher**
Chen *et al.*[5]	Encryption	Re-encryption	Need
Wood *et al.* [29]	Proxy re-encryption	Not consider	Need
Tan *et al.*[7]	Encryption	Considered	Need
Hamdane *et al.* [11]	Encryption & Credential	Not consider	Need
Ghali *et al.* [9]	Interest-based	Not consider	Need
Li *et al.* [17]	Signature-based	Not consider	Not need
Silva *et al.* [25]	Attribute encryption & Proxy re-encryption	Proxy re-encryption	Proxy is Needed

new access control system for NDN using decentralized CP-ABE, which is revocable and privacy-preserving.

3 Preliminaries

3.1 Access Structure

Definition 1 (Access Control [13]). *Let $\{P_1, \ldots, P_n\}$ be a set of all parties. A collection $\mathbb{A} \subseteq 2^{\{P_1,\ldots,P_n\}}$ is monotone if $\forall B, C$: if $B \in \mathbb{A}$ and $B \subseteq C$, then $C \in \mathbb{A}$. An access structure is a collection $\mathbb{A}$ of non-empty subsets of $\{P_1, \ldots, P_n\}$, i.e., $\mathbb{A} \subseteq 2^{\{P_1,\ldots,P_n\}} \backslash \{\varnothing\}$. Authorized sets are the sets in $\mathbb{A}$, and unauthorized sets are the sets not in $\mathbb{A}$.*

In this work, the parties represent attributes in our scheme. And we only consider monotone access structure, which means that consumers will not lose their previous decryption privileges if they get more attributes.

3.2 Linear Secret Sharing Scheme (LSSS) [20]

Definition 2 (Linear secret sharing scheme (LSSS) [13]). *Let $\mathcal{U}$ denote a set of parties, $\mathcal{U}$ is the attribute universes in our context. Let $\boldsymbol{A}$ be a matrix of size $l \times n$. Let $\rho : \{1, \ldots, l\} \to \mathcal{U}$ be a function that maps a row to a party for labeling. A secret sharing scheme $\prod$ over a set of parties $\mathcal{U}$ is a linear secret-sharing scheme over $\mathbb{Z}_p$ (p is a prime) if:*

1) *The shares of a secret $s \in \mathbb{Z}_p$ for each attribute form a vector over $\mathbb{Z}_p$.*

2) *For each access structure $\mathbb{A}$ on $\mathcal{U}$, there exists a matrix $\mathbf{A} \in \mathbb{Z}_p^{l\times n}$, called the share-generating matrix for $\prod$. For all $i = 1, \ldots, l$, the function ρ labels the rows of $\boldsymbol{A}$ with attributes from $\mathcal{U}$, i.e., the i^{th} row of $\boldsymbol{A}$ is labeled by $\rho(i)$. When we consider the column vector $\vec{v} = (s, r_2, \ldots, r_n)$, where $s \in \mathbb{Z}_p$ is the secret to be shared, and $r_2, \ldots, r_n \in \mathbb{Z}_P$ are randomly chosen, then $\boldsymbol{\lambda} = \boldsymbol{A}\vec{v} \in \mathbb{Z}_p^{l\times 1}$ is the vector of l shares of the secret s according to $\prod$. The share $\boldsymbol{l}ambda_i = \boldsymbol{A}_i\vec{v}$ belongs to party $\rho(i)$.*

As addressed in [13], each secret-sharing scheme (not only the linear ones) should satisfy the reconstruction requirement (each authorized set can reconstruct the secret) and the security requirement (any unauthorized set cannot reveal any partial information about the secret). More concretely, let $S \in \mathbb{A}$ be an authorized set, let I be the set of rows whose labels are in S and define $I = \{i|\rho(i) \in S\} \subset \{1, \ldots, l\}$. Then there exist constants $\{c_i \in \mathbb{Z}_p\}$ such that, if $\{\lambda_i\}$ are valid shares of any secret s according to $\prod$, then $\sum_{i\in I} c_i\lambda_i = s$, i.e., $\sum_{i\in I} c_i\boldsymbol{A}_i = (1, 0, \ldots, 0)$. These constants $\{\lambda_i\}$ can be found in time polynomial in the size of share-generation matrix $\boldsymbol{A}$. But for unauthorized sets, no such $\{\lambda_i\}$ constants exist.

3.3 Bilinear Groups and Complexity Assumption

Our scheme is constructed on bilinear groups of prime order, and its security is proved based on q-Decisional Parallel Bilinear Diffie-Hellman Exponent 2 (q-BPBDHE2).

Let G and G_T be two multiplicative cyclic groups of prime order p, where the group operation is efficiently computable in the security parameter. Let g be a generator of G and $e : G \times G \to G_T$ be a bilinear map that satisfies the following properties:

1) **Bilinearity**: for all $g, f \in G$ and $a, b \in \mathbb{Z}_p$ it is true that $e(g^a, f^b) = e(g, f)^{ab}$.

2) **Non-degeneracy**: $e(g, g) \neq 1_{G_T}$.

3) **Computability:** The group operations in G and the bilinear map $e : G \times G \to G_T$ are both efficiently computable.

Definition 3 (q-BPBDHE2 [23]). *G is a bilinear group of order p and g is a generator of G. The q-BPBDHE2 problem in group G is defined as follows: Choose random values $s, a, b_1, b_2, \ldots, b_q \in Z_p^*$ and $R \in G_T$, and given*

$$D =((p, g, G, e, g^s, \{g^{a^i}\}_{i\in[2q],i\neq q+1}, \{g^{b_j a^i}\}_{(i,j)\in[2q,q],i\neq q+1},$$
$$\{g^{\frac{s}{b_i}}\}_{i\in[q]}, \{g^{\frac{sa^ib_j}{b_{j'}}}\}_{(i,j,j')\in[q+1,q,q],j\neq j'})$$

The assumption states in G that no polynomial-time distinguisher can distinguish the distribution $(D, e(g,g)^{sa^{q+1}})$ from the distribution (D, R) with more than negligible advantage.

4 Access Control System in NDN

4.1 Access Control System Model

This paper considers a NDN environment consisting of AAs, data publisher, NDN routers and data consumers. The system model of this NDN access control system is showed in Figure 2.

1) **Attribute Authorities (AAs):** Each AA creates a pair of public-private key in setup phase using public parameters, and excepting this, no other global coordination is needed. Each AA is independent from other AAs and manages different attributes. In this scheme, each AA can control any number of attributes, while each attribute can be managed only by one AA. While receiving a request for the attribute-related key from a consumer, AA responds the key under current time period. Additionally, at the beginning of each time period, they update the attribute-related keys for the non-revoked consumers based on a revocation list.

2) **Data publisher:** A data publisher can develop access policy by himself, and then encrypts data according to this policy and the current time period, and specifies how long (i.e., the current time period) the content can be cached in routers through “freshness period” in data packet. The attribute policy is sent with ciphertext but the attribute values are always hidden.

3) **NDN routers:** They can provide data storage service by its own storage strategy, and give consumers data packets according to their interest packets. Moreover, they can also delete the data packets according to the “freshness period” in data packets.

4) **Data consumers:** Each consumer with a GID is represented by an attribute set. Consumers can ask the AAs for attribute-related keys under the current time period. A consumer can obtain the encrypted data from his neighbor router or the publisher, and then according to the access structure in ciphertext, if he has an attributes set matching the access structure and all the attribute-related keys are under the right time period can decrypt the ciphertext. No one can learn about the specific access structure.

4.2 Definition of the Access Control Scheme

This scheme includes the following five parts: GlobalSetup, AASetup, KeyGen & KeyUpdate, Encrpt and Decrpt. Revocation is an important part in access control system. In the ABE-based access control system, revocation occurs when a consumer leaves from the system by himself, a leaker was deleted by system, a consumer’s attribute expired, or an attribute in the system was abolished. In our scheme, the attribute-based keys of the non-revoked consumers should be updated periodically, and the period is static and determined by the system requirements, for example updated every month. The publisher encrypts the data under his own policy and the current time period. Each attribute is comprised of two parts, name and value. In addition, a revocation list for each attribute value is needed in the system, which stores the GIDs of all the revoked consumers associated with the attribute value, and is stored by the corresponding AA.

GlobalSetup$(1^{\kappa}) \rightarrow GP$: κ is the security parameter, GP is the output representing public global parameters. The attribute name universe $\mathcal{U}$, AA universe $\mathcal{U}_{\theta}$, global identifier universe $\mathcal{GID}$ and a publicly computable function F ($F : \mathcal{U} \rightarrow \mathcal{U}_{\theta}$ map each attribute name to a unique authority) are all included in GP and $\theta \in \mathcal{U}_{\theta}$.

AASetup$(GP, \theta) \rightarrow \{apk_{\theta}, ask_{\theta}\}$: $AA(\theta \in \mathcal{U}_{\theta})$ runs it which takes in GP and generates its public-secret key pair $(apk_{\theta}, ask_{\theta})$.

KeyGen & $KeyUpdate(GP,\ GID,\ u,\ v_u,\ Time,\ rl_{v_u},\ ask_{\theta}) \rightarrow \{SK^{Time}_{GID,v_u}\}$: The consumer asks for an attribute-related key from the corresponding authority θ, and θ runs this algorithm which takes in the consumer’s global identifier $GID(GID \in \mathcal{GID})$, a name u of attribute and its value v_u , the current time period Time, a revocation list rl_{v_u} related to v_u and ask_{θ} of θ. It generates a key SK^{Time}_{GID,v_u} for this consumer.

Encrpt$(GP, \mathrm{M}, (\boldsymbol{A}, \rho, \mathcal{T}), Time, \{apk_{\theta}\}) \rightarrow$ CT: Publisher runs this algorithm, which takes in the content M, the current time period $Time$, the access structure developed by the publisher $(\boldsymbol{A}, \rho, \mathcal{T})$ and a public key set $\{apk_{\theta}\}$of the corresponding authorities. It outputs the ciphertexts CT, and the part of access structure $(\boldsymbol{A}, \rho)$ are passed with CT, but the attribute values $\mathcal{T}$ are always hidden.

Decrpt$(GP, \mathrm{CT}, \{SK^{Time}_{GID,v_u}\}) \rightarrow$ M: when a consumer obtains an encrypted data, he runs this algorithm, which takes in CT and an attribute-related key set $\{SK^{Time}_{GID,v_u}\}$ of the consumer GID corresponding to different attributes value. The consumer checks which attributes are used to match the access structure, and then employs these keys to decrypt the ciphertexts, but never know the specific access structure.

4.3 Security Requirements

1) Effective access control:
Publishers publish their sensitive content to NDN and have an expressive access policy for published content, so that the specific consumers can decrypt it. Each consumer can obtain the encrypted data packet from the neighbor router or the publisher, but

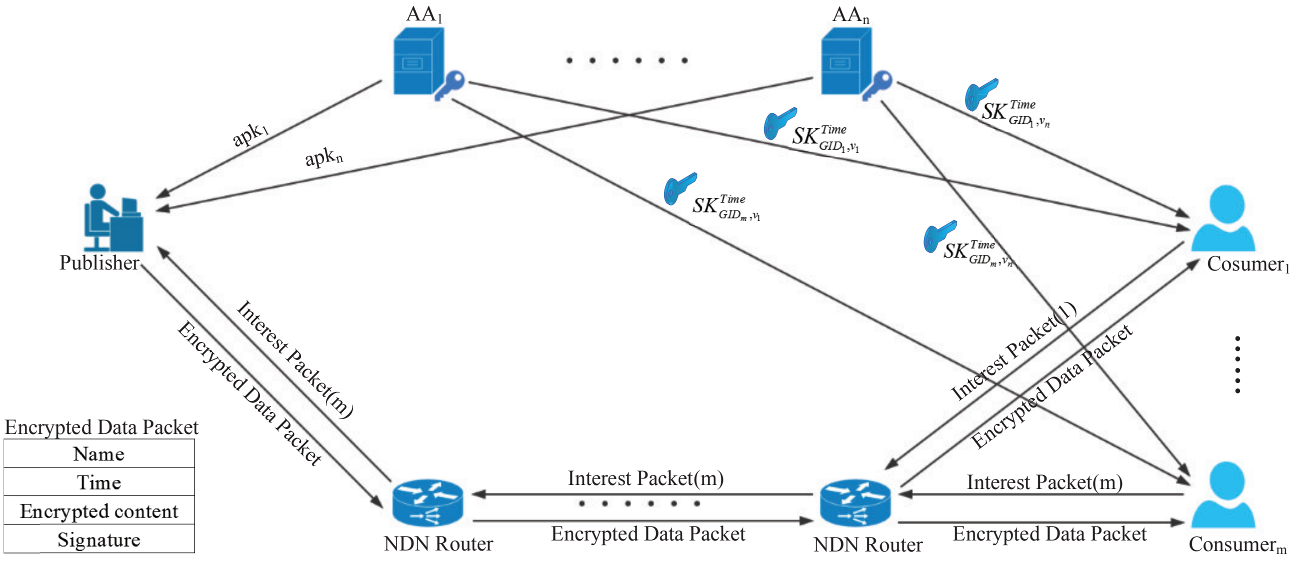

Figure 2: Architecture of our NDN access control system

only the authorized consumers can decrypt it.

2) Collusion resistance:
Sometimes, although an unauthorized consumer cannot decrypt the ciphertext alone, several of them may decrypt it by collaborating with each other, which is called collusion attack. This access system is required to against this sort of attack.

3) Back security and forward security:
This access control system is required that both backward security and forward security are guaranteed. That is, if the private key is compromised, the ciphertext encrypted in the last time period and next period are not affected.

4) Privacy-preserving:
In many applications, some specific attributes carry sensitive information, but the access structure included in ciphertext is public. So, it is required that the access structure should not reveal consumer's sensitive information to realize user privacy.

4.4 Security Model

This scheme is improved the CP-ABE scheme in [23] basically, and its security is proved based on q-Decisional Parallel Bilinear Diffie-Hellman Exponent 2 (q-BPBDHE2) [23], and a static (or non-adaptive) security model is also used. As defined in [23], in the static security model, the adversary will send all queries to the challenger the first time after knowing the public parameters. Furthermore, the adversary is allowed to destroy a set of AAs for the purpose of malicious attacks, and the adversary selects these AAs after knowing the public parameters and remain unchanged during the course of the game. The formalized security game is specified below:

Global Setup: Challenger runs GlobalSetup$(1^\kappa) \rightarrow GP$ and gives GP to adversary.

Adversary's Queries: Then the adversary responds with:

- A set $\mathcal{C}_\theta \subseteq \mathcal{U}_\theta$ of corrupt AAs chosen by the adversary and their respective public keys $\{apk_\theta\}_{\theta \in C_\theta}$ which can be created in a malicious way but in correct type.
- A set $\mathcal{N}_\theta \subseteq \mathcal{U}_\theta$ of the non-corrupt AAs which is disjoint from $\mathcal{C}_\theta \subseteq \mathcal{U}_\theta$. And the adversary queries their public keys.
- A sequence $\{(\mathcal{S}_i, GID_i), Time\}_{i=1}^m$ for querying the secret keys, in which GID_i is a consumer's global identity and $\mathcal{S}_i \subseteq \mathcal{U}$ is an attribute set. The adversary queries a pair $\{(\mathcal{S}_i, GID_i), Time\}$ means that he asks for the secret keys for the consumer GID_i under the current time period $Time$, and the consumer's attribute set is $\mathcal{S}_i$. That is, the identities $\{GID_i\}$ are distinct and all the keys are come from a non-corrupt AA, i.e.,$F(\mathcal{S}_i) \cap \mathcal{C}_\theta = \varnothing$.
- Two messages $\mathrm{M}_0, \mathrm{M}_1$ with equal length and a challenge access structure $(\boldsymbol{A}, \rho, \mathcal{T})$ ($\boldsymbol{A}$ is a LSSS matrix of access structure, ρ is a function mapping the rows in $\boldsymbol{A}$ to attribute names). It is required for each GID_i, the access structure $(\boldsymbol{A}, \rho, \mathcal{T})$ cannot be satisfiede by $\mathcal{S}_i \cup \mathcal{S}_{\mathcal{C}_\theta}$, where $\mathcal{S}_{\mathcal{C}_\theta}$is a collection of all the attributes managed by corrupt AAs. So, the adversary cannot decrypt the challenge ciphertext by combining a secret key given to him with the keys from the corrupt AAs to win the game.

Challenger's Replies: The challenger throws a random coin $\beta \in \{0, 1\}$ and replies with:

- The public keys $\{apk_\theta\}_{\theta \in \mathbb{N}_\theta}$ corresponding to the non-corrupt authorities $\mathcal{N}_\theta$.
- The secret keys $\{(SK^{Time}_{GID_i,\mathcal{S}_i})\}_{i=1}^m$ corresponding to $\{(\mathcal{S}_i, GID_i), Time\}_{i=1}^m$.
- The challenge ciphertext Encrypt(GP, M_β, $\{apk_\theta\}$ $\{\boldsymbol{A}, \rho, \mathcal{T}\}$) $\rightarrow$ CT$*$, in which $\{apk_\theta\}$ is the set of all the corresponding AA's public keys.

Guess: The adversary guesses β' for β as output.

The advantage of the adversary in the game is defined as $\Pr[\beta = \beta'] - 1/2$, that is the probability of the adversary guessing correctly.

Definition 4. *The scheme is statically secure if no polynomial time adversary has a non-negligible advantage to win the above security game.*

5 Construction

The detailed algorithms of this scheme are constructed as follows,

GlobalSetup$(1^\kappa) \rightarrow GP$: It takes the security parameter κ as input. First, it chooses a bilinear group G which order is a prime p and generator is g. Three Hash functions are used in this algorithm, $H_0 : \{0,1\}^* \rightarrow \mathbb{Z}_p$, $H_1 : \mathbb{Z}_P^* \rightarrow G$, $H_2 : \mathcal{U} \rightarrow G$, H_0 maps time period to elements of $\mathbb{Z}_p$, H_1 and H_2 maps global identities GID and attribute names to G respectively. Finally, it defines $F : \mathcal{U} \rightarrow \mathcal{U}_\theta$. GP= $\{p, G, g, q, H_0, H_1, H_2, \mathcal{U}, \mathcal{U}_\theta, F\}$ are global parameters as output. If not specified, GP is given as an input in the following algorithms.

AASetup$(GP, \theta) \rightarrow \{apk_\theta, ask_\theta\}$**:** In this algorithm, each AA ($\theta \in \mathcal{U}_\theta$) chooses two random exponents $\alpha_\theta, y_\theta \in \mathbb{Z}_p$. It keeps $ask_\theta = \{\alpha_\theta, y_\theta\}$ as its secret key. The AA publishes its pulic key $apk_\theta = \{e(g,g)^{\alpha_\theta}, g^{y_\theta}\}$.

KeyGen&KeyUpdate(GP**,** GID**,** θ**,** u**,** v_u**,** $Time$**,** rl_{v_u}**,** ask_θ) $\rightarrow \{SK^{Time}_{GID,v_u}\}$**:** AA runs this algorithm and takes in the consumer's global identifier GID, the attribute name u and the corresponding attribute value v_u, the current time period Time, the revocation list related to v_u and the authority's secret key to create or update a key for the consumer. The attribute is managed by the specific authority, i.e., $u \in F^{-1}(\theta)$. It first chooses a $\gamma \in \mathbb{Z}_p$ randomly and generates the attribute-related key under the current time period as output: $SK^{Time}_{GID,v_u} = \{K = g^{\alpha_\theta H_0(Time)} H_1(GID \parallel Time)^{y_\theta} H_2(u)^\gamma, K' = g^{v_u \gamma}\}$.

Encrpt$(GP, \mathrm{M}, (\boldsymbol{A}, \rho, \mathcal{T}), Time, \{apk_\theta\}) \rightarrow$ CT : Publisher runs this algorithm, takes in a content M with sensitive information, an access policy $(\boldsymbol{A}, \rho, \mathcal{T})$ with $\boldsymbol{A} \in \mathbb{Z}_p^{l \times n}$, where ρ is a function mapping the rows in $\boldsymbol{A}$ to the attribute names and $\mathcal{T} = (t_{\rho(1)}, \cdots, t_{\rho(l)}) \in \mathbb{Z}_p^l$ is the corresponding attribute values, the current time period $Time$ and the public key sets $\{apk_\theta\}$ of the related AAs. Also, the function is defined as $\delta : [l] \rightarrow \mathcal{U}_\theta$ as $\delta(\cdot) = F(\rho(\cdot))$, that is, mapping the rows of $\boldsymbol{A}$ to AAs.

It chooses vector $\vec{v} = (s, v_2, \cdots, v_n)^T$, $\vec{v}' = (s', v_2', \cdots, v_n')^T$ and $\vec{\omega} = (0, \omega_2, \cdots, \omega_n)^T$, $\vec{\omega}' = (0, \omega_2', \cdots, \omega_n')^T$ at first, where s, $v_2, \cdots, v_n$, $s', v_2', \cdots, v_n' \in \mathbb{Z}_p$ and $\omega_2, \cdots, \omega_n$, $\omega_2', \cdots, \omega_n' \in \mathbb{Z}_p$ are chosen randomly. According to LSSS, let λ_x denote the share of s, i.e. $\lambda_x = \boldsymbol{A}_x \vec{v}$, and ω_x denote the share of 0, i.e. $\omega_x = \boldsymbol{A}_x \vec{\omega}$, where $\boldsymbol{A}_x$ is the x-th row of $\boldsymbol{A}$.

For each $x (x \in [l])$ of $\boldsymbol{A}$, choose $r_x, r_x' \in \mathbb{Z}_p$ randomly. The ciphertext is computed as:

$$\begin{aligned} C_0 = & Me(g,g)^s \quad C_0' = e(g,g)^s \\ \forall x \quad & C_{1,x} = e(g,g)^{\lambda_x} e(g,g)^{\alpha_{\rho(x)} H_0(Time) r_x t_{\rho(x)}} \\ & C_{2,x} = g^{-r_x t_{\rho(x)}} \\ & C_{3,x} = g^{y_{\rho(x)} r_x t_{\rho(x)}} g^{\omega_x} \\ & C_{4,x} = H_2(\rho(x))^{r_x} \\ & C_{1,x}' = e(g,g)^{\lambda_x'} e(g,g)^{\alpha_{\rho(x)} H_0(Time) r_x' t_{\rho(x)}} \\ & C_{2,x}' = g^{-r_x' t_{\rho(x)}} \\ & C_{3,x}' = g^{y_{\rho(x)} r_x' t_{\rho(x)}} g^{\omega_x'} \\ & C_{4,x}' = H_2(\rho(x))^{r_x'} \end{aligned}$$

It outputs ciphertext CT as:

$$\begin{aligned} \mathrm{CT} = (& (\boldsymbol{A}, \rho), C_0, C_0', \{C_{1,x}\}, \{C_{1,x}'\}, \{C_{2,x}\}, \{C_{2,x}'\}, \\ & \{C_{3,x}\}, \{C_{3,x}'\}, \{C_{4,x}\}, \{C_{4,x}'\}) \end{aligned}$$

Finally, the publisher signs the data packet and publish it or waits for the consumer's request.

Decrpt$(GP, \mathrm{CT}, \{SK^{Time}_{GID,v_u}\}) \rightarrow \mathrm{M}$: When a consumer obtains the encrypted data packet, after verifying the signature of publisher to ensure the integrity and authenticity of the content. Then, the consumer runs this algorithm calculates $\min_{(\boldsymbol{A},\rho)}$ from $(\boldsymbol{A}, \rho)$, in which $\min_{(\boldsymbol{A},\rho)}$ is the minimum subsets matches $(\boldsymbol{A}, \rho)$. It then checks if there is a $\mathcal{L} \in \min_{(A,\rho)}$ that satisfies

$$\begin{aligned} C_0' = \prod_{x \in L} & (C_{1,x}' \cdot e(K, C_{2,x}') \cdot e(H_1(GID \parallel Time), C_{3,x}') \cdot \\ & e(K', C_{4,x}'))^{c_x} \end{aligned}$$

Where $\sum_{x \in L} c_x \boldsymbol{A}_x = (1, 0, \cdots, 0)$. If no element in $\min_{(\boldsymbol{A},\rho)}$ makes the above equation holds, which means the consumer is unauthorized, then outputs $\perp$, that is, it is failed to decrypt. Otherwise, the consumer calculates constants $c_x \in \mathbb{Z}_p$ such that

$\sum_{x\in I} c_x \boldsymbol{A}_x = (1,0,\ldots,0)$ and computes:

$$\prod_x (C_{1,x}\cdot e(K, C_{2,x})\cdot e(H_1(GID \parallel Time), C_{3,x})\cdot$$
$$e(K', C_{4,x}))^{c_x} = e(g,g)^s$$

Since $\lambda_x = \boldsymbol{A}_x\vec{v}$ and $\omega_x = \boldsymbol{A}_x\vec{\omega}$, such that $(1,0,\ldots,0)\cdot\vec{v} = s$ and $(1,0,\ldots,0)\cdot\vec{\omega} = 0$. Then M can be recovered as $\mathrm{M} = C_0/e(g,g)^s$.

In the construction, each available AA updates the consumer's attribute-related key periodically. It means that all consumers should contact AAs to get new private keys periodically. This can be extremely complex if the number of users is large. To avoid establishing the secure channel, let each AA encrypt the new key for the non-revoked consumer with its GID and the previous time period, and pass the encrypted key to the consumer.

6 Security Analysis

6.1 Correctness

Theorem 1. *This scheme is correct.*

Proof. If there is a $\mathcal{L} \in \min_{(A,\rho)}$,

$$\begin{aligned}
& C'_{1,x}\cdot e(K, C'_{2,x})\cdot e(H_1(GID \parallel Time), C'_{3,x}) \\
& \qquad \cdot e(K', C'_{4,x}) \\
= \; & e(g,g)^{\lambda'_x}\cdot e(g,g)^{\alpha_{\rho(x)}H_0(Time)r'_x t_{\rho(x)}}\cdot \\
& e(g^{\alpha_{\rho(x)}H_0(Time)}H_1(GID \parallel Time)^{y_{\rho(x)}}H_2(\rho(x))^{\gamma}, \\
& g^{-r'_x t_{\rho(x)}})\cdot e(H_1(GID \parallel Time), g^{y_{\rho(x)}r'_x t_{\rho(x)}}g^{\omega'_x}) \\
& \cdot e(g^{\gamma t_{\rho(x)}}, H_2(\rho(x))^{r'_x}) \\
= \; & e(g,g)^{\lambda'_x}\cdot e(g,g)^{\alpha_{\rho(x)}H_0(Time)r'_x t_{\rho(x)}}\cdot \\
& e(g,g)^{-\alpha_{\rho(x)}H_0(Time)r'_x t_{\rho(x)}}\cdot \\
& e(H_1(GID \parallel Time), g)^{-y_{\rho(x)}r'_x t_{\rho(x)}}\cdot \\
& e(H_2(\rho(x)), g)^{-\gamma r'_x t_{\rho(x)}} \\
& \cdot e(H_1(GID \parallel Time), g)^{y_{\rho(x)}r'_x t_{\rho(x)}}\cdot \\
& e(H_1(GID \parallel Time), g)^{\omega'_x}\cdot e(g, H_2(\rho(x)))^{\gamma r'_x t_{\rho(x)}} \\
= \; & e(g,g)^{\lambda'_x}\cdot e(H_1(GID \parallel Time), g)^{\omega'_x}
\end{aligned}$$

Then calculates $c_x \in \mathbb{Z}_p$ such that $\sum_{x\in L} c_x \boldsymbol{A}_x = (1,0,\ldots,0)$.

$$\sum_{x\in L}\lambda'_x c_x = \sum_{i\in I}\mathbb{A}_i\cdot\vec{v}'\cdot c_x = \vec{v}'\cdot(1,0,\ldots,0) = s',$$
$$\sum_{x\in L}\omega'_x c_x = \sum_{i\in I}\mathbb{A}_i\cdot\vec{\omega}'\cdot c_x = \vec{\omega}'\cdot(1,0,\ldots,0) = 0.$$

So,

$$\begin{aligned}
& \prod_{x\in\mathcal{L}}(e(g,g)^{\lambda'_x}e(H_1(GID \parallel Time), g)^{\omega'_x})^{c_x} \\
= \; & e(g,g)^{\sum_{x\in I}\lambda'_x c_x}e(H_1(GID \parallel Time), g)^{\sum_{x\in I}\omega'_x c_x} \\
= \; & e(g,g)^{s'} = C'_0
\end{aligned}$$

Similarly, calculates

$$\prod_{x\in\mathcal{L}}(C_{1,x}\cdot e(K, C_{2,x})\cdot e(H_1(GID \parallel Time), C_{3,x})\cdot$$
$$e(K', C_{4,x}))^{c_x} = e(g,g)^s$$

Finally, M can be recovered as

$$\begin{aligned}
& C_0/\prod_{x\in\mathcal{L}}(e(g,g)^{\lambda_x}e(H_1(GID \parallel Time), g)^{\omega_x})^{c_x} \\
= \; & C_0/e(g,g)^s = \mathrm{M}
\end{aligned}$$

□

6.2 Static Security

In this scheme, publisher can develop his own access policy at will for the sensitive information. Each AA can publish attribute-related keys for the consumers. Each consumer can obtain the published data packet from neighbor router conveniently without affecting in-network storage mechanism, and only the authorized consumers can decrypt the content, while unauthorized consumers can get none of useful information from the acquired data packet.

The static security of this scheme will be proved from q-DPDDHE2 assumption under the static security model. First, the following lemma will be proved.

Lemma 1. *Supposing that the scheme in [23] is a statically secure scheme, then this scheme is a static secure one.*

Proof. Assuming there is a polynomial-time $\mathscr{A}$ who has advantage ε against this scheme in the static security game. Then how to build a simulator $\mathscr{B}$ that has advantage ϵ against the scheme in [23] is as follows. Let $\mathscr{C}$ be the challenger in [23]. □

GlobalSetup: The challenge $\mathscr{C}$ sends the global parameters $GP = \{p, G, g, H_0, H_1, H_2, \mathcal{U}, \mathcal{U}_\theta, F\}$ to the simulator $\mathscr{B}$. $\mathscr{B}$ passes GP to the adversary $\mathscr{A}$.

Adversary's Queries: The adversary $\mathscr{A}$ chooses a set $\mathcal{C}_\theta \subseteq \mathcal{U}_\theta$ of corrupt AAs and generates the related public keys in the scheme [23] as $\{apk'_\theta\}_{\theta\in\mathcal{C}_\theta}$. For each $\theta \in \mathcal{C}_\theta$, A sets the keys of corrupt AAs in our scheme as $apk_\theta = \{apk'_\theta\}$. $\mathscr{A}$ responds to $\mathscr{B}$ with:

- A set of corrupt AAs $\mathcal{C}_\theta \subseteq \mathcal{U}_\theta$ and $\{apk_\theta\}_{\theta\in\mathcal{C}_\theta}$.
- A non-corrupt AAs set $\mathcal{N}_\theta \subseteq \mathcal{U}_\theta$.
- A sequence $\{(S_i, GID_i), Time\}_{i=1}^m$ with the following restrictions: if $i \neq j$, then $GID_i \neq GID_j$, $S_i \subseteq \mathcal{U}$ and $F(S_i) \cap \mathcal{C}_\theta = \varnothing$. A pair $\{(S_i, GID_i), Time\}$ means that $\mathscr{A}$ requests the secret key for the consumer with global identity GID_i under the current time period Time, the consumer's attributes set is S_i.

- Two messages $\mathrm{M}_0, \mathrm{M}_1$ with equal length, and a challenge access structure $(\boldsymbol{A}, \rho)$. $\mathcal{S}_{\mathcal{C}_\theta}$ is a collection of all the attributes managed by corrupt AAs. For each $i \in [m]$, the attribute in S_i cannot be combined with the attribute in $S_{\mathcal{C}_\theta}$ (i.e., $S_{\mathcal{C}_\theta} \cup S_i$) to satisfy $(\boldsymbol{A}, \rho)$.

Challenger's Replies: When the simulator $\mathscr{B}$ receives the above responds, it sends $\mathcal{C}_\theta$, $\{apk_\theta\}_{\theta \in \mathcal{C}_\theta}$, $\mathcal{N}_\theta$, $\{(S_i, GID_i), Time\}_{i=1}^m$, $\mathrm{M}_0, \mathrm{M}_1$ and $(\boldsymbol{A}, \rho)$ to $\mathscr{C}$ for requesting the corresponding public keys, secret keys and challenge ciphertext in the scheme in [23]. Then, $\mathscr{C}$ replies the public keys $\{apk'_\theta = (e(g,g)^{\alpha_\theta}, g^{y_\theta})\}$ for all $\theta \in \mathcal{N}_\theta$, the secret keys $SK'_{GID_i,S_i} = \{(g^{\alpha_\theta} H_1(GID_i)^{y_\theta} F(i)^t, g^t)_{i \in s_i}\}$, for all $i \in [m]$, the challenge ciphertext $\mathrm{CT}' = (C_0 = \mathrm{M}_\beta e(g,g)^s$, $\{C_{1,x} = e(g,g)^{\lambda_x} e(g,g)^{\alpha_{\rho(x)} r_x}\}$, $\{C_{2,x} = g^{-r_x}\}$, $\{C_{3,x} = g^{y_{\rho(x)} r_x} g^{\omega_x}\}$, $\{C_{4,x} = F(\rho(x)^{t_x}\}_{x \in \{1,2,\ldots,l\}})$. Then $\mathscr{B}$ generates the public keys, the secret keys and challenge ciphertext in our scheme as follows:

- For each $\theta \in \mathcal{N}_\theta$, $\mathscr{B}$ sets the public keys as $\{apk_\theta = (e(g,g)^{\alpha_\theta}, g^{y_\theta})\}$.
- For each $i \in [m]$ and $u \in \mathcal{S}_i$, a random value t is chosen randomly by $\mathscr{B}$, the current time period $Time$, then calculates $K = g^{\alpha_\theta H_0(Time)} H_1(GID \parallel Time)^{y_\theta} H_2(u)^\gamma$, $K' = g^{v_u \gamma}$. Finally, $\mathscr{B}$ sets the attribute-related keys as $SK^{Time}_{GID,v_u} = \{K = g^{\alpha_\theta H_0(Time)} H_1(GID \parallel Time)^{y_\theta} H_2(u)^\gamma, K' = g^{v_u \gamma}\}$.
- For $x \in \{1,2,\ldots,l\}$, $\mathscr{B}$ calculates $C_0 = Me(g,g)^s$, $C'_0 = e(g,g)^s$, $C_{1,x} = e(g,g)^{\lambda_x} e(g,g)^{\alpha_{\rho(x)} H_0(Time) r_x t_{\rho(x)}}$, $C_{2,x} = g^{-r_x t_{\rho(x)}}$, $C_{3,x} = g^{y_{\rho(x)} r_x t_{\rho(x)}} g^{\omega_x}$, $C_{4,x} = H_2(\rho(x))^{r_x}$, $C'_{1,x} = e(g,g)^{\lambda'_x} e(g,g)^{\alpha_{\rho(x)} H_0(Time) r'_x t_{\rho(x)}}$, $C'_{2,x} = g^{-r'_x t_{\rho(x)}}$, $C'_{3,x} = g^{y_{\rho(x)} r'_x t_{\rho(x)}} g^{\omega'_x}$, $C'_{4,x} = H_2(\rho(x))^{r'_x}$. B sets the challenge ciphertext as

$$\begin{aligned}\mathrm{CT} =&((\boldsymbol{A}, \rho), C_0, C'_0, \{C_{1,x}\}, \{C'_{1,x}\}, \{C_{2,x}\},\\ &\{C'_{2,x}\}, \{C_{3,x}\}, \{C'_{3,x}\}, \{C_{4,x}\}, \{C'_{4,x}\}).\end{aligned}$$

Finally, $\mathscr{B}$ sends $\{apk_\theta = (e(g,g)^{\alpha_\theta}, g^{y_\theta})\}$, $\{SK^{Time}_{GID_i,S_i}\}_{i=1}^m$ and the challenge ciphertexts CT to $\mathscr{A}$.

Guess: $\mathscr{A}$ guesses $\beta' \in \{0,1\}$ as output. Then $\mathscr{B}$ outputs β'.

And in [23], the following lemma has been proved.

Lemma 2. *If the q-DPBDHE2 holds, the scheme in [23] is statically security in random oracle model.*

Theorem 2. *If the q-DPBDHE2 holds, then this scheme is statically security in the random oracle model.*

Proof. It can be proved directly from **Lemma 1** and **Lemma 2.** □

6.3 Collusion Resistance

Theorem 3. *This scheme can against the collusion attack by the unauthorized consumers.*

Proof. It can be against the collusion attacks by combining a consumer's key components together by distinct global identity GID. Furthmore, when encrypting a message, besides specifing a access stucture, the data publisher also needs to specify the current time period, and a consumer whose attribute-related key satisfies the structure and under the current time period can decrypt the ciphertext. Since the time is same for each consumer, so that the revoked consumers may decrypt the newly created ciphertext by combining his key with the updated information of non-revoked consumers, so it is necessary to prevent the consumers from collusion. Therefore, $SK^{Time}_{GID,v_u} = \{K = g^{\alpha_\theta H_0(Time)} H_1(GID \parallel Time)^{y_\theta} H_2(u)^\gamma, K' = g^{v_u \gamma}\}$ are generated as the attribute-related key.The time period and a consumer's global identity are bound together as $H_1(GID \parallel Time)$ which is different from each other but related to his or her own identity. □

6.4 Back Security and Forward Security

Theorem 4. *This scheme can guarantee back security and forward security.*

Proof. The attribute-related keys and ciphertexts are updated periodically, and the value of parameter $Time$ is different for each time period. Therefore, the ciphertext encrypted in previous time period cannot be decrypted with the updated private keys of the current time period, which ensures the backward security. In this time period, the re-encrypted ciphertext in this time period cannot be decrypted with the attribute-related keys distributed in previous time period, which guarantees the forward security. □

6.5 Privacy-preserving

Theorem 5. *The scheme can realize recipient anonymity to protect privacy of users.*

Proof. In the access policy $(\boldsymbol{A}, \rho, \mathcal{T})$, $\boldsymbol{A}$ is the access matrix, ρ is a function mapping the rows in $\boldsymbol{A}$ to attribute names, $\mathcal{T}$ is the concrete attribute value. In our scheme, the attribute value $\mathcal{T}$ is always hidden, but the rest of the access structure $(\boldsymbol{A}, \rho)$ is sends with the ciphertext. No one can learn the specific access structure in the ciphertext, so even legitimate consumers don't know which attributes are used to decrypt the data. Therefore, no one knows who can decrypt the ciphertext to realize recipient anonymity, and thus it protects the user privacy. □

7 Characteristics Comparison

The scheme in [23] is a large-universe multi-authority CP-ABE scheme based on prime order groups which reduces the computational complexity observably. Based on the scheme in [23], this paper combine the indirect revocation method and the NDN architecture to realize revocation in NDN. Meanwhile, this scheme is preserving-privacy through using the partially hidden structure technique. As shown in Table 2, a comparison of characteristics of this paper with those in [8, 13, 23] is described. [23] is the basic scheme we implement and improvement, the scheme in [8] is a multi-authority CP-ABE scheme with indirectly revocation, and the scheme in [13] is an anonymity one. From Table 2, we can observe our scheme is fully functional, it is a decentralized CP-ABE scheme supporting both revocation and anonymity. Also the prime order groups brings it efficient and practical features.

We use $|\mathcal{U}|$ denote the size of attribute universe. The number of attribute authorities is denoted by $|\mathcal{U}_\theta|$, an LSSS access structure with an $l \times n$ matrix is represented by l, the number of attributes in the consumer's key is denoted by $|\mathcal{S}|$, and the number of rows used in decryption is denoted by $|I|$. Table 3 summarizes the efficiency of our scheme and the other schemes.

In contrast to the basic scheme [23], the public and private key size in this paper are not changed, but since the need of redundant ciphertexts for hidden structure, the ciphertext length and bilinear operation for decryption are twice as much as the basic scheme. This work is built on prime order groups, and the paring operation in prime order group is significant faster than that in composite order groups [23], so the computation overhand is acceptable.

8 Conclusion

This paper designs a new access control system in NDN including the system model, working principle, security definitions and properties in NDN. A new scheme of multi-authority revocable NDN access control based on CP-ABE is implemented by specific security assumption, which solves revocation problem of access control in NDN effectively and protects the privacy of consumers. The attribute-related keys are updated indirectly in each time period, and the keys are renewed periodically by using both the freshness period in the data packet and the in-network caching mechanism of NDN. The revoked consumers cannot obtain the update keys so that user revocation is achieved. Meanwhile, thanks to the decentralization, attribute revocation is easy to be done by the corresponding AAs which control the revoked attributes without any interaction to other AAs. As the access control policy itself will reveal the consumer's sensitive information, we introduce the method of partially hidden access control structure, which will not increase the consumer's key length and guarantee the consumer's privacy. Finally, the security is proved under the static security model.

Acknowledgments

This work is supported by the National Nature Science Foundation of China (No. 61462060), (No. 61461027), the Natural Science Foundation of Gansu Province of China (No. 1610RJYA008). The authors gratefully acknowledge the anonymous reviewers for their valuable comments.

References

[1] N. Attrapadung and H. Imai, "Conjunctive broadcast and attribute-based encryption," in *Third International Conference on Pairing-Based Cryptography (Pairing'09)*, pp. 248–265, 2009.

[2] M. Bayat, M. Aref, "An attribute based key agreement protocol resilient to KCI attack," *International Journal of Electronics and Information Engineering*, vol. 2, no. 1, pp. 10–20, 2015.

[3] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in *IEEE Symposium on Security and Privacy (SP'07)*, pp. 321–334, 2007.

[4] A. Boldyreva, V. Goyal, and V. Kumar, "Identity-based encryption with efficient revocation," in *ACM Conference on Computer and Communications Security*, pp. 417–426, 2008.

[5] M. Chase, "Multi-authority attribute based encryption," in *Conference on Theory of Cryptography*, pp. 515–534, 2007.

[6] M. Chase and S. M. Chow, "Improving privacy and security in multi-authority attribute-based encryption," in *ACM Conference on Computer and Communications Security*, pp. 121–130, 2009.

[7] T. Chen, K. Lei, and K. Xu, "An encryption and probability based access control model for named data networking," in *Performance Computing and Communications Conference*, pp. 1–8, 2015.

[8] H. Cui and R. H. Deng, "Revocable and decentralized attribute-based encryption," *The Computer Journal*, vol. 59, no. 8, pp. 1220–1235, 2016.

[9] C. Ghali, M. A. Schlosberg, G. Tsudik, and C. A. Wood, "Interest-based access control for content centric networks," *Proceedings of the 2nd ACM Conference on Information-Centric Networking (ACM-ICN'15)*, pp. 147–156, 2015.

[10] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," *Proceedings of the 13th ACM Conference on Computer and Communications Security*, pp. 89–98, 2006.

[11] B. Hamdane and S. G. El Fatmi, "A credential and encryption based access control solution for named data networking," in *IFIP/IEEE International Symposium on Integrated Network Management*, pp. 1234–1237, 2015.

[12] M. A. Hamza, J. F. Sun, X. Y. Nie, Z. Q. Qin, and H. Xiong, "Revocable ABE with bounded ciphertext

Table 2: Characteristics comparison in [8, 13, 23] and this scheme

schemes	**Bilinear groups**	**revocable**	**Multi-authority**	**Anonymous of access structure**	**security**
Rouselakis *et al.* [23]	Prime order	×	√	×	Static security
Cui *et al.* [8]	Composite order	Indirect revocation	√	×	Adaptively security
Lai *et al.* [13]	Composite order	×	×	Partially-hidden	Adaptively security
This scheme	Prime order	Indirect revocation	√	Partially-hidden	Static security

Table 3: efficiency comparison in [8, 13, 23] and this scheme

schemes	**Public key size**	**Private key size**	**Ciphertext size**	**Paring operations for decryption**
Rouselakis *et al.* [23]	$2\lvert\mathcal{U}_\theta\rvert$	$2\lvert\mathcal{S}\rvert$	$4l+1$	$3\lvert I\rvert$
Cui *et al.* [8]	$2\lvert\mathcal{U}_\theta\rvert$	$\lvert\mathcal{S}\rvert$	$3l+1$	$2\lvert I\rvert$
Lai *et al.* [13]	-	$\lvert\mathcal{S}\rvert+2$	$2(2l+2)$	$6\lvert I\rvert$
This scheme	$2\lvert\mathcal{U}_\theta\rvert$	$2\lvert\mathcal{S}\rvert$	$2(4l+1)$	$6\lvert I\rvert$

in cloud computing," *International Journal of Network Security*, vol. 19, no. 6, pp. 973–983, 2017.

[13] J. Z. Lai, R. H. Deng, and Y. J. Li, "Expressive CP-ABE with partially hidden access structures," in *ACM Symposium on Information, Computer and Communications Security*, pp. 18–19, 2012.

[14] C. C. Lee, P. S. Chung, M. S. Hwang, "A survey on attribute-based encryption schemes of access control in cloud environments," *International Journal of Network Security*, vol. 15, no. 4, pp. 231–240, July 2013.

[15] A. Lewko and B. Waters, "Decentralizing attribute-based encryption," in *Advances in Cryptology (EUROCRYPT'11)*, pp. 568–588, 2011.

[16] Q. Li, J. F. Ma, R. Li, X. Liu, J. B. Xiong, and D. W. Chen, "Secure, efficient and revocable multi-authority access control system in cloud storage," *Computers & Security*, vol. 59, no. C, pp. 45–59, 2016.

[17] Q. Li, X. W. Zhang, Q. J. Zheng, and R. Sandhu, "Live: Lightweight integrity verification and content access control for named data networking," *IEEE Transactions on Information Forensics & Security*, vol. 10, no. 2, pp. 308–320, 2015.

[18] C. W. Liu, W. F. Hsien, C. C. Yang, and M. S. Hwang, "A survey of attribute-based access control with user revocation in cloud data storage," *International Journal of Network Security*, vol. 18, pp. 900-916, 2016.

[19] H. Ma, T. Peng, Z. Liu, "Directly revocable and verifiable key-policy attribute-based encryption for large universe," *International Journal of Network Security*, vol. 19, no. 2, pp. 272–284, 2017.

[20] P. Muralikrishna, S. Srinivasan, N. Chandramowliswaran, "Secure schemes for secret sharing and key distribution using pell's equation," *International Journal of Pure & Applied Mathematics*, vol. 85, no. 5, pp. 933-937, 2013.

[21] T. Nishide, K. Yoneyama, and K. Ohta, "Attribute-based encryption with partially hidden encryptor-specified access structures," in *International Conference on Applied Cryptography and Network Security*, pp. 111–129, 2008.

[22] K. Riad, "Multi-authority trust access control for cloud storage," in *International Conference on Cloud Computing and Intelligence Systems*, pp. 429–433, 2016.

[23] Y. Rouselakis and B. Waters, "Efficient statically-secure large-universe multi-authority attribute-based encryption," in *International Conference on Financial Cryptography and Data Security*, pp. 315–332, 2015.

[24] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in *International Conference on Theory and Applications of Cryptographic Techniques*, pp. 457–473, 2005.

[25] R. S. D. Silva and S. D. Zorzo, "An access control mechanism to ensure privacy in named data networking using attribute-based encryption with immediate revocation of privileges," in *Consumer Communications and Networking Conference*, pp. 128–133, 2015.

[26] X. B. Tan, Z. F. Zhou, C. Zou, Y. K. Niu, and X. Chen, "Copyright protection in named data networking," in *Sixth International Conference on Wireless Communications and Signal Processing*, pp. 1–6, 2014.

[27] Y. Tian, Y. Peng, G. Gao, X. Peng, "Role-based access control for body area networks using attribute-based encryption in cloud storage," *International Journal of Network Security*, vol. 19, no. 5, pp. 720–726, 2017.

[28] R. Tourani, T. Mick, S. Misra, and G. Panwar, "Security, privacy, and access control in information-centric networking: A survey," *Networking and Internet Architecture*, 2016.

[29] C. A. Wood and E. Uzun, "Flexible end-to-end content security in ccn," in *Consumer Communications and Networking Conference*, pp. 858–865, 2014.

[30] G. Xylomenos, C. N. Ververidis, Va. A. Siris, N. Fotiou, C. Tsilopoulos, X. Vasilakos, Konstantinos V. Katsaros, and G. C. Polyzos, "A survey of information-centric networking research," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 2, pp. 1024–1049, 2014.

[31] L. X. Zhang, A. Afanasyev, J. Burke, V. Jacobson, K. Claffy, P. Crowley, C. Papadopoulos, L. Wang, and B. C. Zhang, "Named data networking," *ACM Sigcomm Computer Communication Review*, vol. 44, no. 3, pp. 66–73, 2014.

[32] Y. Zhao, P. Fan, H. Cai, Z. Qin and H. Xiong, "Attribute-based encryption with non-monotonic access structures supporting fine-grained attribute revocation in M-healthcare," *International Journal of Network Security*, vol. 19, no. 6, pp. 1044–1052, 2017.

Biography

Tao Feng received his D.E from Xidian Univerisity in 2008. He is now a professor and doctoral supervisor in Lanzhou Univerisity of Technology. His research interests include network and information security.

Jiaqi Guo received the B.E in information security from Xi'an University of Posts and Teleconmmunications in 2012. She is currently a postgraduate student in Lanzhou University of Technology. His current research interests include cryptography and network security.