# FASE: Fine-Grained Accountable and Space-Efficient Access Control for Multimedia Content With In-Network Caching

Peixuan He, Kaiping Xue, *Senior Member, IEEE*, Jiayu Yang, Qiudong Xia, Jianqing Liu, *Member, IEEE*, and David S. L. Wei, *Senior Member, IEEE*

***Abstract*—To reduce the duplicated traffic and improve the performance of distributing massive volumes of multimedia contents, in-network caching has been proposed recently. However, as in-network content caching can be directly utilized to respond users' requests, multimedia content retrieval is beyond content providers' control and makes it hard for them to implement access control and service accounting. In this paper, we propose a Fine-grained Accountable and Space-Efficient access control scheme, called FASE, for multimedia content distribution. FASE allows content providers to be fully offline while making the best of in-network caching. In FASE, the attribute-based encryption at multimedia content provider side and access policy based authentication at the edge router side jointly ensure secure fine-grained access control. Our scheme is efficient in both space and time. By designing one time chameleon signature (OTCS), users can keep anonymous during the authentication, and their privileges can be conveniently revoked when needed. Besides, secure service accounting is implemented by letting edge routers collect service credentials generated during users' request process. Through formal security analysis, we prove the security of our scheme. Simulation results demonstrate that our scheme is efficient with acceptable overhead.**

***Index Terms*—Multimedia content security, access control, in-network caching, attribute-based encryption, access policy.**

## I. Introduction

IT IS reported by Cisco that multimedia traffic will take up 82% of all total global IP traffic by 2022, 7% increase from 2017 [1]. Such massive volumes of multimedia contents also introduce a huge amount of redundant traffic and cause insufficient bandwidth utilization in the traditional IP network architecture. To adapt to this content-intensive trend and solve these problems, an innovative network architecture, namely information centric networking (ICN) [2], [3], has been proposed. The main idea of ICN is to leverage in-network caching and content name routing to achieve the objectives of redundant traffic elimination, high bandwidth utilization, and quick response to user's request.

In-network caching is an excellent choice for multimedia content providers (MCPs) to enhance users' experience and make their content subscription services more competitive. With in-network caching, when users request contents, the nearby routers that cache one corresponding copy will respond them directly instead of fetching the contents from remote MCPs. In the traditional IP architecture, what MCPs concern most is access control and service accounting. MCPs do not expect users to access their repositories without permissions. Due to the complex composition of users, MCPs often adopt complex and comprehensive (i.e., fine-grained) access policies. Meanwhile, MCPs need to collect feedback information (e.g., the number of requests for a specific content) to enable themselves to respond the market feedback in time and improve their services. For example, when a popular video occurs, MCPs can quickly spread this video to multiple CDNs (Content Delivery Networks) and let users have a better viewing experience.

However, when introducing in-network caching, many requests may not reach MCPs as users can access the copies in cache-enabled routers without MCPs' consents or even awareness. Therefore, it is difficult for MCPs to conduct fine-grained access control and service accounting with in-network caching. Besides, in the in-network caching scenario, since bandwidth and caching space are valuable resources for Internet Service Provider (ISP), service accounting becomes important in the sense that ISP needs the information of served requests to charge MCPs for the consumed resources. Last but not least, since cache-enabled routers can respond users directly, it is easy for routers to know which content was requested and even who requested [4]. Thus, users' privacy preservation is another problem that we need to consider and solve. All in all, how to conduct fine-grained access control and secure service accounting for in-network cached

Manuscript received February 1, 2021; revised May 8, 2021; accepted July 4, 2021. Date of publication July 12, 2021; date of current version December 9, 2021. This work is supported in part by the National Natural Science Foundation of China under Grant No. 61972371 and Youth Innovation Promotion Association of the Chinese Academy of Sciences (CAS) under Grant No. Y202093. The associate editor coordinating the review of this article and approving it for publication was D. Huang. *(Corresponding author: Kaiping Xue.)*

Peixuan He is with the Department of Electronic Engineering and Information Science, University of Science and Technology of China, Hefei 230027, China, and also with Security Research Department, Bytedance Corporation, Beijing 100098, China.

Kaiping Xue is with the School of Cyber Security, University of Science and Technology of China, Hefei 230027, China, and also with the Cyberspace Security Research Center, Pengcheng Laboratory, Shenzhen 518055, China (e-mail: kpxue@ustc.edu.cn).

Jiayu Yang and Qiudong Xia are with the School of Cyber Security, University of Science and Technology of China, Hefei 230027, China.

Jianqing Liu is with the Department of Electrical and Computer Engineering, University of Alabama in Huntsville, Huntsville, AL 35899 USA.

David S. L. Wei is with the Department of Computer and Information Science, Fordham University, Bronx, NY 10458, USA.

Digital Object Identifier 10.1109/TNSM.2021.3096428

contents while also achieving privacy preservation becomes an important but challenging issue.

There have been a few works proposed to address these issues. Firstly, *about access control*, some of these schemes achieve effective access control by restricting users' abilities in decrypting the contents. Attribute-based encryption (ABE) [5], [6] and broadcast encryption [7], [8] are such cryptographic techniques which are widely used to achieve secure access control over in-network caching. Nevertheless, these schemes are vulnerable to denial-of-service (DoS) attacks, causing network resources to be quickly consumed up by malicious requests. In light of this, some other schemes let certain entities (e.g., MCPs, cache-enabled routers or extra servers) authenticate users' requests before sending the contents to authorized users [9]–[11]. However, an increased computation and communication overhead is incurred due to the frequent interactions. Meanwhile, the storage overhead is also huge because of the massive number of contents. Combining the advantages of these two kinds of solutions, a two-layer access control framework was proposed in our previous works [12], [13], where MCPs encrypt contents by broadcasting encryption while edge routers authenticate requests by group signatures. However, this solution is unable to efficiently achieve fine-grained access control. Secondly, *about service accounting*, to the best of our knowledge, our previous work [12], [13] is yet the only one to utilize group signatures as trusted service credentials to address this issue. Although this scheme uses the batch verification to reduce the authentication overhead, when the number of groups and credentials is large, the overhead of signature verification is still significant. Lastly, *as for privacy preservation*, some schemes prevent external attackers from compromising users' privacy [4], [14] through leveraging the technologies of network coding, random forwarding, artificial delay and so on, while other schemes utilize group signature [13] or ring signature [15] to make users anonymous to curious routers, but the overhead brought by these algorithms is nontrivial for routers.

Motivated by the above observation, in this paper, we propose a Fine-grained Accountable and Space-Efficient access control scheme, called FASE, for in-network multimedia content caching. In FASE, MCPs encrypt contents using ciphertext policy-attribute based encryption (CP-ABE) [16]–[18] before content publication for fine-grained access control. To refrain MCPs from always being online and thwart DoS attacks, edge routers are empowered to authenticate users' requests so that only legitimate requests are allowed to access the cached contents. Note that adopting the existing content-based authentication at edge routers is not feasible since it brings significant storage overhead to edge routers. Considering the number of contents is much larger than that of access policies, we propose an access policy-based challenge response authentication mechanism so that edge routers can only store the outsourced keys that MCP generates for every access policy.

Besides, *privacy preservation, privilege revocation*, and *efficient service accounting* are three other major issues that need to be addressed. For privacy-preserving consideration, we leverage the collision of chameleon hash and Bloom filter to let users be authenticated without leaking their identities. Inspired by the idea of one-time signature [19], users' trapdoor key used to find the collision of chameleon hash can only be used once so that different signatures from a specific user cannot be associated by ISP. In such a way, we design a lightweight and anonymous signature algorithm, called one-time chameleon signature (OTCS). With the introduction of OTCS, privilege revocation can be effectively achieved by revoking the users' ability of generating valid signatures. Besides, the information left by chameleon hash can be collected as trusted service credentials to make it possible for MCPs to perform efficient service accounting (at $\mu s$ level) and pay ISP for the resources consumed. Finally, in order to further reduce the computation overhead of edge routers, hash chain is utilized to authenticate users' continuous requests. Our contributions can be summarized as follows:

- We propose an efficient, secure and accountable access control scheme for multimedia content with in-network caching by combining CP-ABE with authentication on edge routers. The edge-side authentication is based on access policy such that it largely decreases the storage overhead of edge routers, and MCPs can be offline during the authentication.
- We further provide a solution to enable MCPs to implement secure service accounting. MCPs extracts useful information from service credentials collected by edge routers, and the embedded users' signatures are able to prevent edge routers from forging credentials for more profits.
- We design an efficient privacy-preserving signature algorithm, OTCS, by combining one-time signature with chameleon hash function. With the introduction of OTCS, the overhead of service accounting process is kept low, and user revocation can be conveniently implemented, making the whole system more robust.

This paper inherits the basic idea of our conference paper [20] and also solves the three important problems left over from the conference paper: privacy preservation, privilege revocation and efficient service accounting. They differ in the following aspects: i) Instead of using the BLS (Boneh-Lynn-Shacham) algorithm [21] in our conference paper, which needs to reveal users' identities for authentication, in this paper, we redesign the signature algorithm used in the authentication process (called OTCS) which helps achieve anonymous authentication and preserve users' privacy. ii) Considering the costly overhead of attribute revocation method in CP-ABE, we provide a novel and efficient privilege revocation mechanism by making revoked users unable to generate valid OTCS. iii) Through the leaked trapdoor key used to generate OTCS in authentication process, we improve the service accounting process in our scheme and content providers only need several lookup operations, of which the overhead is largely reduced. iv) We state the security analysis more rigorously and conduct more intensive experiments to demonstrate that our system is secure and efficient.

The rest of the paper is organized as follows. In Section II, we review the related work in the in-network caching paradigm. Then we describe the system model, security assumption, and design goals in Section III, and

present the preliminaries in Section IV. The details of our scheme are shown in Section V. After that, we give the security and performance analysis in Section VI and Section VII, respectively. Finally, we conclude this work in Section VIII.

## II. Related Work

In this section, we introduce the related work from the following three aspects: secure content delivery, service accounting, and privacy preservation.

### A. Secure Content Delivery

The explosive growth of multimedia contents has made secure content delivery a hot topic, and many schemes have been proposed in cloud storage scenarios. Xue *et al.* [5] proposed a controlled collaborative access control scheme to cope with the issue that some contents need to be decrypted by several entities. Wang *et al.* [6] eliminated the trusted key authority in CP-ABE by designing a two-party key issuing protocol. Zuo *et al.* [22] designed a two-factor mechanism to protect the cryptographic key used in ABE, and provided an efficient revocation solution. However, it is worth noting that directly applying these solutions to the in-network caching scenario is not lightweight enough which are subject to potential attacks that aim to exhaust network resources by sending massive requests (i.e., DoS attack).

Besides, a lot of access control schemes were proposed for secure content delivery in the in-network caching scenario. Abdallah *et al.* [23] required MCPs to authenticate user's request, and the request will be satisfied by cache-enabled routers after successful authentication. Fan *et al.* [24] let a trusted third party to authenticate user's request. In the scheme proposed by Li *et al.* [10], authentication was conducted at routers when the cache-hit occurred. Li *et al.* [25] proposed to leverage lightweight one-time signature to conduct authentication. Although these are feasible solutions, they often bring significant computation and communication overhead. Li *et al.* [26], Misra *et al.* [7], and Bernardini *et al.* [27] utilized ABE, broadcast encryption, and proxy re-encryption, respectively to achieve secure access control. However, solely relying on encryption will open the whole network to the public which is hard to resist DoS attacks. To solve these problems, Zheng *et al.* [28] proposed a scheme which combined authentication at MCPs and proxy re-encryption at edge routers, but it did not take full advantage of in-network caching and also brought in large overhead. Our previous work [12], [13] largely improved its performance by letting edge routers authenticate user's requests and designing lightweight broadcast encryption. Similarly, based on edge authentication, Sultan *et al.* [29] proposed a new encryption algorithm to achieve access control over hierarchical contents. And Tourani *et al.* [30] designed a tag-based access control framework, which binds the users' access rights with tags received from content providers. So routers determine whether they forward contents to users according to the validity of the tags embedded in requests. However, this scheme can not efficiently achieve fine-grained access control.

### B. Service Accounting

Service accounting mainly deals with the billing issue between service providers and consumers. It has been widely discussed in the traditional TCP/IP network and cloud computing scenario. Courcoubetis *et al.* [31] first proposed a charging schemes based on usage. Ma [32] then proposed a hybrid charging model, in which consumers pay a fixed bill for a basic service, and if they pursue a better QoS, they need to pay the bill based on their usage. Lučanin *et al.* [33] designed a pricing model considering CPU frequency as the main resource. Sharma *et al.* [34] took both resource usage and inherent risks of the cloud provider into account, and proposed a risk-adjusted cloud resources pricing model. However, all of these schemes assume that consumers trust the resource consumption data provided by service providers. Since the interests of service providers and consumers often contradict, this assumption is not practicable.

In recent years, similar question has been discussed in the scenario where the network is equipped with ubiquitous caching, like ICN. Ghali *et al.* [35] and Tourani *et al.* [36] adopted the same thought, where Internet Service Provider (ISP) forwards user's request to content provider to inform that this request has been served. Nevertheless, in these schemes, it is easy for ISP to forge user's request for more profits. To solve this problem, Xue *et al.* [13] and Sultan *et al.* [29] proposed to utilize users' signatures as service credentials, respectively. But the overhead of service accounting in these two schemes is a little high.

### C. Privacy Preservation

With in-network caching, users' privacy faces two kinds of threats: one from external attackers and the other from internal curious routers. Specifically, external attackers can infer users' access history through file retrieval delay while curious routers can learn users' identities and the contents they required through the received requests. Acs *et al.* [14] first analyzed the scope and feasibility of the attack launched by external attackers, and they proposed to make content name random and introduce some artificial delay to prevent such an attack. Similarly, Wu *et al.* [4] advised to add some random delay for each response. However, these solutions can not effectively prevent inside attacks from routers. To address this attack, Xue *et al.* [13] and Yu *et al.* [15] proposed to utilize anonymous signature algorithms like group signature and ring signature, but these anonymous signature algorithms bring huge overhead to routers which often affects the efficiency of the whole system.

Meanwhile, due to the built-in security mechanism of ICN, data publishers' privacy is also threatened. Recently, Ramani *et al.* [37] proposed to utilize attribute-based signature (ABS) to replace the traditional public key signatures used in ICN to achieve publishers' anonymity.

## III. System Model, Security Assumption and Design Goals

### A. System Model

Our system model mainly consists of three components: Multimedia Content Providers, Internet Service Provider and Users. Fig. 1 illustrates the construction of our system.

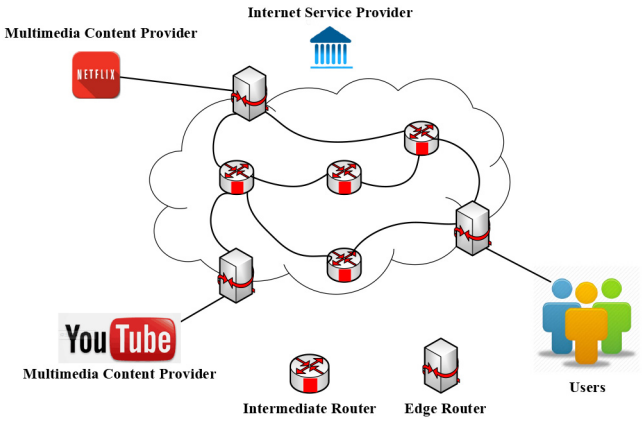



Fig. 1. System Model.

MCPs provide users with multimedia content subscription service and assign secret keys for registered users. ISP manages the core network that is capable of in-network caching and routing by content names like ICN. ISP provides network access service to both MCPs and users. The routers in the network can be categorized into intermediate routers and edge routers. Intermediate routers are cache-enabled and only focused on forwarding and caching whereas edge routers do not cache the contents but they store the outsourced keys received from different MCPs and authenticate users' requests at the very beginning. Users consume multimedia contents by sending requests with corresponding content names. It is noted that ISP provides cache space and collects feedback information to help MCPs improve their services. Therefore, it is reasonable for MCPs to pay ISP according to the amount of served requests.

### B. Security Assumption

In our system, we assume MCPs are trusted and they are responsible for the security of the multimedia contents they own. Users are considered to be untrusted and they always try to gain access to the contents beyond their privileges individually or in collusion. Meanwhile, some unauthorized users may send massive number of innocuous requests to exhaust network resources maliciously.

ISP is assumed to be semi-trusted. On one hand, ISP is curious about the contents that routers store and the identities of the requesters for some purposes, e.g., sending advertisements to these requesters. On the other hand, ISP is greedy about economical profits and may fake the amount of served requests by generating a lot of faked service credentials. Nevertheless, it is also rational because ISP concerns about its own credibility and if the detection possibility of misbehavior is non-negligible (e.g., 1%), we assume ISP will not take the risk of cheating MCPs. In order to keep absolute deterrence, MCPs still need to verify service credentials received from ISP.

Overall, the threats that our scheme face include: breaking confidentiality, DoS attack, privacy inference, and generating faked service credentials.

### C. Design Goals

To guarantee that content providers are able to control users' access while getting feedback information, our access control scheme should achieve the following design goals:

- *Data confidentiality:* For one thing, malicious users and curious routers, either individually or in collusion, should not be able to decrypt the contents with no authorized access. For another thing, our scheme should support access revocation, and users who are in the revocation list are unable to decrypt any contents.
- *Accountability:* The scheme is required to let content providers collect feedback information securely from ISP to achieve accountability, i.e., ISP is unable or deterred to provide forged feedback information to cheat content providers for more profits.
- *Anonymity:* The private information (e.g., users' preferences) should not be revealed to any entities other than content providers. It means curious entities (including ISP and external attackers) are not able to obtain users' identities either from side channel or directly. Also, different requests from the same user would not be known by routers or providers that these requests are from the same user.

## IV. Preliminaries

### A. Bilinear Map

Let $\mathbb{G}, \mathbb{G}_T$ be two multiplicative cyclic groups of the same prime order $q$. A bilinear map can be described as $e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$, which has the several properties:

1) *Computability:* there exists an efficient algorithm to compute $e(u, v)$ for any $u, v \in \mathbb{G}$.

2) *Bilinearity:* for all $a, b \in \mathbb{Z}_q$ and $u, v \in \mathbb{G}$, we have $e(u^a, v^b) = e(u, v)^{ab}$.

3) *Non-degeneracy:* $e(g, g) \neq 1$, where $g$ is the generator of $\mathbb{G}$.

Our Scheme works under the Discrete Logarithm (DL) Assumption [38], whose definition is as follows:

*Definition 1 (DL Assumption):* Let $S = (q, \mathbb{G}, \mathbb{G}_T, e(\cdot, \cdot))$ be a bilinear group system. Given $(S, g, g^x)$ as input, where $g \in \mathbb{G}$ and $x \in \mathbb{Z}_q$, to output $x$ is difficult. Formally, we say a probabilistic polynomial-time (PPT) adversary $\mathcal{A}$ has a non-negligible advantage $\epsilon$ to solve DL if

$$Pr[\mathcal{A}(S, g, g^x) = x] \geq \epsilon.$$

### B. Ciphertext-Policy Attribute-Based Encryption

CP-ABE is a cryptographic design [16] in which users' secret keys are bonded with attribute sets, and the contents published by content owners are restricted by access structures. Users can only decrypt the contents if the access structures can be satisfied by their attribute sets. A basic CP-ABE scheme consists of four algorithms as follows:

*Setup($\mathcal{U}$) $\rightarrow$ ($PK$, $MK$):* The setup algorithm takes universal set of attributes $\mathcal{U}$ and the implicit security parameter as input. It outputs public parameters *PK* and a master key *MK*.

*Encrypt(M, PK, $\mathbb{A}$) $\rightarrow$ CT:* The encryption algorithm takes a message plaintext *M*, an access structure $\mathbb{A}$ over the universe of

attributes, and public parameters *PK* as input. Then it outputs the corresponding ciphertext *CT* of the message that implicitly contains $\mathbb{A}$.

*KeyGen(S, MK, PK)* $\rightarrow$ *SK:* The key generation algorithm takes a set of attribute *S*, a master key *MK*, and public parameters *PK* as input. It outputs a private key *SK*.

*Decrypt(CT, SK, PK)* $\rightarrow$ *M or* $\perp$*:* The decryption algorithm takes ciphertext *CT*, secret key *SK*, and public parameters *PK* as input. If the attribute set *S* of secret key *SK* satisfies the access structure $\mathbb{A}$ of *CT*, it outputs the message *M*; Otherwise, it outputs $\perp$.

*Definition 2 (Access Structure):* Let $\{P_1, P_2, \ldots, P_n\}$ be a set of parties. A collection $\mathbb{A} \subseteq 2^{\{P_1, P_2, \ldots, P_n\}}$ is monotone if $\forall B, C$: if $B \in \mathbb{A}$ and $B \subseteq C$, then $C \in \mathbb{A}$. An access structure (respectively, monotone access structure) is a collection (respectively, monotone collection) $\mathbb{A}$ of non-empty subsets of $\{P_1, P_2, \ldots, P_n\}$, i.e., $\mathbb{A} \subseteq 2^{\{P_1, P_2, \ldots, P_n\}} \backslash \{\varnothing\}$. The sets in $\mathbb{A}$ are called authorized sets, and the sets not in $\mathbb{A}$ are called unauthorized sets.

Specifically, in our context, the role of a party is specified in its attributes. Besides, by utilizing the method mentioned in [39], any monotonic boolean formula can be converted into an LSSS representation, which is defined as follows:

*Definition 3 [Linear Secret Sharing Schemes (LSSS)]:* A secret sharing scheme $\Pi$ over a set of parties $\mathcal{P}$ is called linear (over $\mathbb{Z}_q$) if

1) The shares for each party form a vector over $\mathbb{Z}_q$.

2) There exists a matrix $\mathbb{M}$ with *l* rows and *n* columns, called the share-generating matrix for $\Pi$. For all $i = 1, \ldots, l$, the *i*th row of $\mathbb{M}$ is labeled by a party $\rho(i)$ ($\rho$ is a function from $\{1, \ldots, l\}$ to $\mathcal{P}$). 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 $\vec{\lambda} = \mathbb{M} \times \vec{v}$ is the vector of *l* shares of the secret *s* according to $\Pi$. The share $\lambda_i$ belongs to party $\rho(i)$.

### C. Bloom Filter

A Bloom filter is a space-efficient hash-based data structure [40], which is designed to test whether an element is in a set. The essential steps of Bloom filter are as follows:

- **Initialization** It generates a bit array *B* of *m* bits, initialized to be 0 for all positions. Then it chooses a set of *d* hash functions: $h_1, h_2, \ldots, h_d$.
- **Insert** To insert an element *x* into the Bloom filter, it uses each hash function to map *x* to a location in *B*, and sets this location to be 1, i.e., it sets $B[h_i(x)] = 1$ for $i = 1, 2, \ldots, d$.
- **Test** To test whether an element *y* is in the set, it checks whether each of the corresponding hash positions (i.e., $B[h_i(y)]$ for $i = 1, 2, \ldots, d$) is 1. If this is the case, *y* is considered as a membership of the set.

Note that Bloom filter is a probabilistic data structure that has false positive rate, which means that an element that is considered to be in the set may not be in it. Given *n* elements stored in a *m*-bit Bloom filter with *d* different hash functions, the corresponding false positive rate is:

$$p \approx \left(1 - e^{-\frac{dn}{m}}\right)^d.$$

Therefore, we can see that given *n* and *m*, the number of hash functions that can achieve minimum false positive rate is $\frac{m}{n} ln2$.

### D. Chameleon Hash

The chameleon hash is a special type of hash function that allows to find collisions, but it has the similar one-way property as standard hash functions. Chameleon hash contains a trapdoor and collisions can be generated efficiently with the knowledge of trapdoor, while without the trapdoor, it is hard to find collisions. Chameleon hash is first introduced by Krawczyk *et al.* [41] and it consists of three algorithms as follows:

*KeyGen(*$1^\kappa$*)* $\rightarrow$ *(hk, tk):* The key generation algorithm takes as input the security parameter $\kappa \in \mathbb{N}$, and outputs a public key *hk* and private trapdoor key *tk*.

*CHash(hk, m, r)* $\rightarrow$ *h:* The CHash algorithm takes the public key *hk*, message *m*, and a random number *r* as input, and outputs the corresponding chameleon hash value *h*.

*CHCol(tk, (h, m, r),* $m'$*)* $\rightarrow$ $r'$*:* Given a valid tuple (*h*, *m*, *r*) and a new message $m'$, the CHcol algorithms outputs the collision $r'$ that makes $CHash(hk, m', r') = h$.

## V. Construction of FASE

### A. Overview

In FASE, MCPs encrypt the contents using CP-ABE before publication to ensure that unauthorized users are unable to access the original contents. Through CP-ABE, they can arbitrarily combine attributes to achieve fine-grained access control. However, encryption itself is not sufficient to keep the system robust because intermediate routers are supposed to respond all users' requests including those from malicious users, which may quickly consume up network resources. In light of this, in FASE, edge routers authenticate users' requests at the very beginning through an access-policy based challenge-response mechanism for high space efficiency. Specifically, MCP generates an outsourced key for every used access policy. According to the access policies of contents that users request, edge routers utilize corresponding outsourced keys to generate challenges. Only users who can access the contents are able to return correct responses and only their requests will be routed to the intermediate routers. In such a way, authentication is performed by edge routers so that MCP can be offline, and network resources are thus protected from DoS attacks. Besides, a new signature algorithm, one-time chameleon signature (OTCS), is proposed, which combines one-time signature and chameleon hash signature. With OTCS, FASE can make the edge-side authentication anonymous. Moreover, we utilize the hash chain technology to associate present requests with their former ones and convert the complex challenge-response based authentication to a lightweight hash authentication for subsequent requests to reduce the authentication overhead.

For simplicity, we only consider the scenario where MCP transcodes multimedia contents into a multimedia stream at a

constant bit rate before encryption, but our scheme is inherently compatible with existing adaptive streaming protocols such as DASH [42] and other novel protocols [43] designed for ICN. It is noted that our scheme is compatible with all the other ABE schemes and the access policy mentioned in this paper is also similar with the ones in traditional ABE schemes. Here we utilize the ABE scheme mentioned in [44] as an example.

### *B. System Initialization*

First, MCP initializes the system and outputs necessary public keys and secret trapdoor keys as follows:

- MCP generates a bilinear map group system $S = (q, \mathbb{G}, \mathbb{G}_T, e(\cdot,\cdot))$, where $g$ is a generator of $\mathbb{G}$.
- MCP chooses a prime number $p$ such that $p = kq + 1$, where $k \in \mathcal{R}$, and an element $\bar{g}$ of order $q$ in $\mathbb{Z}_p$.
- MCP randomly chooses two numbers $\alpha, a \in \mathbb{Z}_q$ and computes $w = g^{\alpha}, y = e(g,g)^{\alpha}, z = g^{a}$.
- For each attribute $Att_i \in \mathcal{U}$, $i = 1, \ldots, |\mathcal{U}|$, MCP selects a random element $h_i \in \mathbb{G}$ as its public key, where $\mathcal{U}$ is the universal set of attributes managed by MCP.
- MCP continuously generates a set of secret trapdoor keys $\bar{x}_1, \bar{x}_2, \ldots, \bar{x}_n$, and their corresponding public keys $\xi_i = \bar{g}^{\bar{x}_i} \ mod \ p$ for $i = 1, 2, \ldots, n$.
- MCP selects random number $m, r \in \mathbb{Z}_q$ to regulate the chameleon hashes $CH_i = \bar{g}^m \xi_i^r \ mod \ p$ that users need to generate collision during the authentication phase.

Finally, MCP publishes the public parameters as: $PK = \{S, g, p, \bar{g}, y, z, m, r, h_1, \ldots, h_{|\mathcal{U}|}, HK, H, H_1, F, Enc(\cdot)\}$, where *HK* denotes the set of all of the public keys corresponding to secret trapdoor keys, *H* is a standard hash function like SHA-256, $H_1$ is a one-way hash function:$\{0,1\}^* \rightarrow \mathbb{Z}_q$, *F* represents the set of hash functions $\{f_1, f_2, \ldots, f_n\}$ used in the Bloom filter, and $Enc_k(\cdot)$ is a secure symmetric encryption algorithm with the secret key *k*. Meanwhile, MCP stores the master key $(w, a)$ securely and keeps secret trapdoor keys $\{\bar{x}_i\}_{i=1}^n$ for further use.

### *C. User Registration*

When user $U_i$ with identity $ID_i$ registers to MCP, MCP assigns corresponding attributes according to her role. For example, when a user loggs in to the system, MCP assigns attribute "Member" to her. Denote the set of attributes assigned to a user as $S_i$. Then MCP selects a random number $t \in \mathbb{Z}_q$ and computes the secret key $SK_i$ for user *i* as follows:

$$K = wz^t, L = g^t; \forall x \in S_i, K_x = h_x^t.$$

Then, MCP randomly chooses $l$ trapdoor keys $\bar{x}_1, \bar{x}_2, \ldots, \bar{x}_l$ that are not used, of which the set is denoted as $SK_i'$. Finally, MCP sends the keys $(SK_i, SK_i')$ to the user after registration. Note that $SK_i$ is used to decrypt the received contents while $SK_i'$ is used to generate valid OTCSs, of which the elements can only be used once.

Besides, in order to conduct service accounting and user revocation, MCP needs to record the association among user identity, secret trapdoor keys and public keys, by using a user information table (UIT) of 3-tuple $(ID_i, SK_i', PK_i')$, where $PK_i'$ is the set of the public keys corresponding to $SK_i'$.

TABLE I
OUTSOURCED KEY LIST

| Access Policy | Ciphertext | Outsourced Key |
|---|---|---|
| $H(\mathbb{A}_1)$ | $ABE_{\mathbb{A}_1}(\delta_1)$ | $H(\delta_1)$ |
| $H(\mathbb{A}_2)$ | $ABE_{\mathbb{A}_2}(\delta_2)$ | $H(\delta_2)$ |
| $\cdots$ | $\cdots$ | $\cdots$ |

### *D. Key Outsourcing*

We let edge routers authenticate users' requests using secret keys granted from MCP so that MCP is allowed to be offline during the authentication. Specifically, before providing multimedia content service, for each used access policy $\mathbb{A}_i$, MCP chooses a random element $\delta_i \in \mathbb{G}_T$ and generates an outsourced key $H(\delta_i)$. Then it encrypts the random element $\delta_i$ using the corresponding access policy $\mathbb{A}_i$ as follows.

According to the method proposed in [39], MCP can turn the access policy into an LSSS access structure $(\mathbb{M}, \rho)$, where $\rho$ is a function which maps the rows of $\mathbb{M}$ to attributes. Let $\mathbb{M}$ be an $l \times n$ matrix. It randomly generates a vector $\vec{v} = \{s, y_2, \ldots, y_n\} \in \mathbb{Z}_q^n$, where the values will be used to share the encryption exponent *s* secretly. MCP computes $v_i = \vec{v} \cdot \mathbb{M}_i$ for $i = 1, \ldots, l$, where $\mathbb{M}_i$ is the *i*-th row of the matrix $\mathbb{M}$. Then it selects *l* random numbers $\gamma_1, \ldots, \gamma_l$ and computes the ciphertext of $\delta_i$ as follows:

$$C = \delta_i \cdot y^s, C' = g^s, C_i = z^{v_i} h_{\rho(i)}^{-\gamma_i}, D_i = g^{\gamma_i}, \forall i \in [1, l].$$

We denote the ciphertext of $\delta_i$ under the access policy $\mathbb{A}_i$ as $ABE_{\mathbb{A}_i}(\delta_i)$. Finally, MCP broadcasts the outsourced key related information $\Lambda = \{H(\mathbb{A}_i), ABE_{\mathbb{A}_i}(\delta_i), H(\delta_i)\}_{i=1}^m$ through the broadcast channel, assuming that there exits *m* different access policies. The edge routers store $\Lambda$ in the outsourced key list as Table I for further authentication.

Besides, to enable edge routers to verify users' signatures efficiently, MCP generates valid public key index *I*s for users in different areas (e.g., communities or towns) according to Algorithm 1, and then sends different edge routers the corresponding index *I*. Note that the index *I* is a Bloom filter which stores the valid public keys owned by users, and it can help edge routers reduce a great scale of computation and storage overhead. For reflecting the valid public key information better, MCP is required to generate new indexes periodically according to the used public key in service credentials, which will be demonstrated in the later subsection, and new obtained keys.

### *E. Content Generation*

For efficient transmission, multimedia files are split into several chunks, where each chunk has a unique content name, and the names of different chunks in the same file have the same prefix [3]. In this paper, for ease of description, we do not distinguish *content* and *chunk*. Besides, to make it convenient for edge routers to identify the access policy of a multimedia content, MCP needs to add side information in the name of

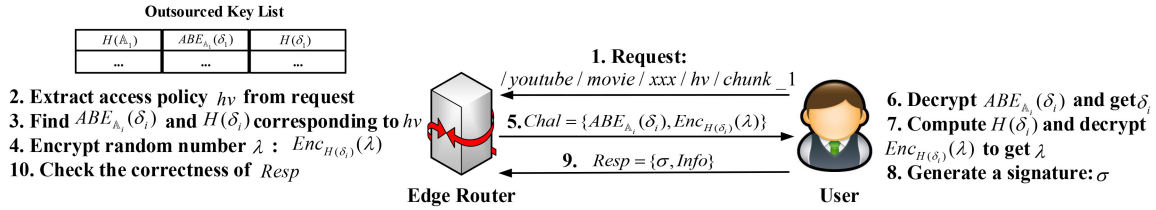



Fig. 2. Example of Request Authentication Process.

**Algorithm 1:** Valid Public Key Index Generation

**Input**: User's identify $ID_i$ in a certain area; Public parameter ($HK$, $F$).
**Output**: Valid Public Key Index $I$.

```
Initialize I with 0;
for each ID_i do
    Find the corresponding PK'_i in the UIT;
    for each element ξ in PK'_i do
        for i ← 1 to d do
            if I[f_i(ξ_i)] ≠ 1 then
                Set I[f_i(ξ)] = 1;
            end
        end
    end
end
Return I.
```

the content. For example, if the original name of a multimedia content is */youtube/moive/xxx/chunk_1* and its access policy is *Member and No Less Than 18 Years Old*, MCP is required to compute the hash value $hv = H$("*Member and No Less Than* 18 *Years Old*") and modify the name of the content as */youtube/moive/xxx/hv/chunk_1*.

Before MCP responds a request, it transcodes the original multimedia content into a media stream at a predesigned bit rate and encrypts the stream $M$ using symmetric encryption by randomly chosen symmetric key $CT = Enc_k(M)$. Then it encrypts the symmetric key using the CP-ABE encryption process mentioned in Section V-D under an access policy $\mathbb{A}_i$ to obtain the ciphertext $CT' = ABE_{\mathbb{A}_i}(k)$. To this end, the multimedia stream $M$ is stored as $(CT, CT')$ in the intermediate routers.

### F. Request Authentication

Like the scheme proposed in our previous work [13], in order to prevent malicious requests from consuming up network resources, here only the requests authenticated by edge routers are allowed to enter into the core network.

Here, edge routers conduct an access-policy based challenge-response to authenticate users' requests, which is illustrated by Fig. 2. Specifically, when an edge router receives a request for a specific chunk in a multimedia file from $U_j$ for the first time, it generates a challenge as follows:

- Extract the hash value of access policy $hv$ from the content name according to the request.
- Find the corresponding item $< H(\mathbb{A}_i), ABE_{\mathbb{A}_i}(\delta_i), H(\delta_i) >$ satisfying $hv = H(\mathbb{A}_i)$ in the outsourced key list.
- Select a random number $\lambda \in \mathbb{Z}_q$ and encrypt it using the outsourced key $k' = H(\delta_i)$ as $CS = Enc_{k'}(\lambda)$.

Afterwards, the edge router sends the challenge $chal = \{ABE_{\mathbb{A}_i}(\delta_i), CS\}$ to the user.

Upon receiving the challenge, the user whose attribute set satisfies LSSS access structure $(\mathbb{M}, \rho)$ corresponding to access policy $\mathbb{A}_i$ is able to decrypt $ABE_{\mathbb{A}_i}(\delta_i)$ to get $\delta_i$. The detailed decryption process is shown as follows.

Suppose $U_j$ is authorized, let $\mathbb{M}_{ID_j}$ be a sub-matrix of $\mathbb{M}$, where each row of $\mathbb{M}_{ID_j}$ represents a specific attribute in $U_j$'s attribute set $S_j$. Denote $I$ as $I = \{i : \rho(i) \in S_j\}$, where $I \subset \{1, 2, \ldots, l\}$. It is easy for the user to find a set of constants $\{w_i \in \mathbb{Z}_q\}_{i \in I}$ such that $\Sigma_{i \in I} w_i v_i = s$, where $\{v_i\}$ is the set of valid shares of secret $s$, by computing $\vec{w} = (1, 0, \ldots, 0) \cdot M_{ID_j}^{-1}$. Through the parameters $\{w_i \in \mathbb{Z}_q\}_{i \in I}$, the user further computes:

$$\frac{C \cdot \Pi_{i \in I} \Big( e(C_i, L) e\Big(D_i, K_{\rho(i)}\Big)\Big)^{w_i}}{e(C', K)} = \frac{\delta_i \cdot y^s \cdot \Pi_{i \in I} e(g, g)^{tav_i w_i}}{y^s e(g, g)^{ast}} = \delta_i.$$

Thus, $U_j$ can recover the outsourced key $k' = H(\delta_i)$ and decrypt $CS$ to obtain the authenticator $\lambda$. Finally, $U_j$ generates an OTCS to show that he/she is an authorized user as follows.

- Generate a hash chain with proper length, of which the first and last elements are denoted as $H_f, H_l$, respectively.
- Compute the corresponding value $m' = H_1(\lambda || Info)$, which is used to generate collision of chameleon hash, i.e., OTCS. Here, *Info* is the feedback information which contains timestamp *TS*, multimedia content name *CN*, randomly chosen unused public key $\xi_j$, and the last element of hash chain $H_l$.
- Compute OTCS $\sigma = \frac{m + \bar{x}_j r - m'}{\bar{x}_j} \ mod \ q$, where $\bar{x}_j$ is the secret trapdoor key corresponding to $\xi_j$. Note that this process is actually a collision computation for chameleon hash $g^{m + \bar{x}_j r}$.

Later, $U_j$ sends the response $resp = \{\sigma, Info\}$ to the edge router. Note that by utilizing OTCS algorithm, *resp* does not include users' identities. Besides, every time when users use OTCS algorithm to generate signatures, they need to choose a new key. Thus, the edge router is incapable of linking different requests from the same user. Therefore, users remain anonymous during the authentication process.

**Algorithm 2:** Response Verification

**Input**: Received response *resp*; Valid Public Key Index $I$; Current time $TS'$; Public parameter $(\bar{g}, m, r)$.
**Output**: Valid or Invalid.

```
if TS' − TS > ΔT for allowed time interval ΔT then
    Return Invalid;
end
// Check the validity of public key ξ_i;
for i ← 1 to d do
    if I[f_i(ξ_j)] ≠ 1 then
        Return Invalid;
    end
end
// Check the validity of OTCS σ;
if ḡ^m ξ_j^r ≠ ḡ^{H_1(λ||Info)} ξ_j^σ then
    Return Invalid;
end
Return Valid.
```

When receiving the response from $U_j$, the edge router verifies *resp* by running Algorithm 2. If the algorithm returns valid, it forwards the request to core network; otherwise, it denies the request. Through the received response *resp*, the edge router reveals the secret trapdoor key used by $U_j$ by computing: $\bar{x}_j = \frac{m - H_1(\lambda||Info)}{\sigma - r} \ mod \ q$. Then, it maintains a table to store the secret trapdoor key $\bar{x}_j$, a prefix of the content name $f$ (for identifying the file to which the chunk belongs), latest received hash value $H_{lt}$, and a counter *len*. Here the edge router sets $f, H_{lt}, len$ as a prefix of *CN*, $H_l$, and "1", respectively.

With the hash chain technique, it becomes convenient for $U_j$ to request subsequent chunks of the same multimedia file with no need of the complex challenge-response mechanism. For these subsequent chunks, $U_j$ only needs to use the hash chain in reverse order and sends the request piggybacked by the new element $H_{new}$ of the hash chain. Owing to the one-way property of hash chain, if the edge router finds an item satisfying $H_{lt} = H(H_{new})$ with the same prefix of content name *f*, it can assure that $U_j$ is an authorized user and forwards the request to core network. Meanwhile, the edge router updates $H_{lt}$ in the table as $H_{new}$ and increases the corresponding counter.

After $U_j$ completes the request, the edge router stores $< \bar{x}_j, Info, H_{lt}, len >$ as a service credential for future service accounting.

### G. Content Decryption

When $U_j$ obtains the encrypted multimedia stream $(CT, CT')$, she recovers the symmetric key *k* using the secret key $SK_j$ by using the CP-ABE decryption process mentioned in Section V-F. With the recovered symmetric key, $U_j$ is able to decrypt $CT'$ and get the plaintext *M*. Finally, the original multimedia content is obtained by decoding *M*.

### H. Service Accounting

To help MCP learn the exact amount of requests that are served and other useful feedback information, edge routers should send service credentials to MCP regularly and MCP stores them according to an ascending order of $\bar{x}_j$ to check whether there exists duplicated credentials. For every credential MCP receives, it needs to check whether $H^{len-1}(H_{lt}) = H_f$. Then it verifies the validity of $\bar{x}_j$, i.e., it checks whether $\bar{x}_j$ is the secret trapdoor key generated by itself. MCP can use Bloom filter to conduct $\bar{x}_j$ verification for better space efficiency. To reduce the overhead caused by the massive number of service credentials, MCP only samples a small proportion of the received credentials to verify. Note that during the service accounting, MCP only needs to conduct several hash and lookup operations, which are lightweight and feasible for MCP. Compared with the service accounting in existing schemes [12], [29], our scheme is much more efficient.

If the verification passes, MCP pays ISP according to the sum of *len* in all the credentials, i.e., the amount of served requests. Then MCP can analyze the feedback information $Info_i$ to get more details like users' preference and improve its content subscription service.

### I. Access Revocation

It is well known that attribute revocation in CP-ABE system is complex with heavy communication and computation overhead [45]. Therefore, in this scheme, we bypass the revocation mechanism in CP-ABE, and utilize a simple black list to revoke user's right in signature generation.

Specifically, by using the similar method of valid public key index generation, MCP generates a revoked public key index $I'$ of revoked users in each area and distribute it to the corresponding edge routers. After edge routers checking the validity of public key $\xi_j$ in the response according to Algorithm 2, they are required to check whether it has been revoked by verifying whether $I'[f_i(\xi_j)] = 1$ for $i = 1 \ to \ d$. Only if the public key is valid and has not been revoked, edge routers will continue to check the validity of OTCS; Otherwise, they will consider that the user is not authorized, and then drop the request. In order to timely reflect the status of users' privileges, the revoked public key index $I'$ is required to be updated once a day.

## VI. Security Analysis

We analyze the security properties of our scheme from the following five aspects.

### A. Data Confidentiality

The data confidentiality of our scheme relies on CP-ABE, which can withstand the attack launched by malicious users and ISP either individually or in collusion. The details of formal security proof can be found in [44].

### B. DoS Attack Resistance

*Lemma 1:* FASE is secure to prevent DoS attack launched by unauthorized users from exhausting resources in core network.

*Proof:* To resist DoS attack, edge routers enforce an access-policy based challenge-response authentication. To pass the authentication, users must generate the correct response $\{\sigma, Info\}$ for the received challenge, which can be divided into two steps: 1) compute correct random number $\lambda$ chosen by edge routers, 2) generate the valid signature based on this number. Then we will prove that malicious users are unable to achieve either of these two steps as follows.

***1) The likelihood of computing correct random number $\lambda$ for any malicious user is negligible.*** We use the Random Oracle heuristic and hybrid arguments to prove it. The input (i.e., received challenge) of the malicious user is:

$$ABE_{\mathbb{A}_i}(\delta_i), Enc_{H(\delta_i)}(\lambda),$$

which is denoted as $c_1, c_2$, respectively. The malicious user needs to output $\lambda'$ satisfying $\lambda' = \lambda$. Denote the input tuple as hybrid $\mathbf{H}_0$, then we consider the following hybrids:

- **Hybrid $\mathbf{H}_1$**: It replaces $\delta_i$ in $c_1$ with a random number in $\mathbb{G}_T$. We can have $\mathbf{H}_0 \overset{c}{\approx} \mathbf{H}_1$ because of the ciphertext indistinguishability of CP-ABE.
- **Hybrid $\mathbf{H}_2$**: In the Random Oracle heuristic, the hash function $H(\delta_i)$ in $c_2$ can be considered as a random oracle $RO(\delta_i)$, so it replaces $\lambda$ in $c_2$ with a random number in $\mathbb{Z}_q$, and we can have $\mathbf{H}_1 \overset{c}{\approx} \mathbf{H}_2$.

Because there is no information related to $\lambda$ under above conditions, the possibility of guessing the correct random number $\lambda$ is negligible, which is $(\frac{1}{2})^{|q|}$. Therefore, no malicious users can win in the original hybrid $\mathbf{H}_0$ with a non-negligible possibility.

***2) The likelihood of generating a valid signature for any malicious user is negligible.*** Forging a valid OTCS through the eavesdropped information or forging public/secret key pair have two ways to generate a valid signature, which are denoted as **Way I** and **Way II**, respectively.

*Way I:* Suppose there is an adversary $\mathcal{A}$ with a non-negligible advantage $Adv_{\mathcal{A}}$ to forge a valid signature through the information eavesdropped. It means that, given the following input chameleon hash $g^{m+\bar{x}_i r}$, $m'$ and valid signatures generated by authorized users, $\mathcal{A}$ is able to generate a valid signature (i.e., find a collision for the chameleon hash) with an unused and unknown secret trapdoor key $\bar{x}_i$. With valid signatures, $\mathcal{A}$ can only get used secret trapdoor keys but it is impossible for $\mathcal{A}$ to infer the unused secret trapdoor key $\bar{x}_i$. Therefore, if $\mathcal{A}$ can win the game, it can compute the secret trapdoor key $\bar{x}_i$ through above information with the same advantage $Adv_{\mathcal{A}}$, which obviously contradicts with the DL assumption.

*Way II:* Before checking the validity of OTCS, edge routers are required to test whether the public key is valid and has not been revoked by checking the two Bloom filters $I$ and $I'$. To break the security of this authentication process, an adversary $\mathcal{A}$ needs to forge a valid OTCS by forging a valid public/secret key pair. Here a valid public/secret key pair means that the public key will be considered as a membership in $I$, and will not be considered as a membership in $I'$. We denote the false positive rates of $I$ and $I'$ as $p_1$ and $p_2$, respectively, and we have

$$p_1 \approx \left(1 - e^{-\frac{d_1 n_1}{m_1}}\right)^{d_1} \text{ and } p_2 \approx \left(1 - e^{-\frac{d_2 n_2}{m_2}}\right)^{d_2}.$$

Therefore, the possibility of generating a valid public/secret key pair for $\mathcal{A}$ is $p = p_1(1 - p_2)$. Since MCPs can choose proper parameters of Bloom filter to keep the false positive rate as low as possible, $p$ will not be high enough to launch DoS attack. To demonstrate it more clearly, we show the relationship among $p_1, p_2$ and $p$ as shown in Fig. 3. We can see that $p$ is mainly controlled by $p_1$. When $p_1$ is low enough, $\mathcal{A}$ can only forge a valid key pair with a low possibility.

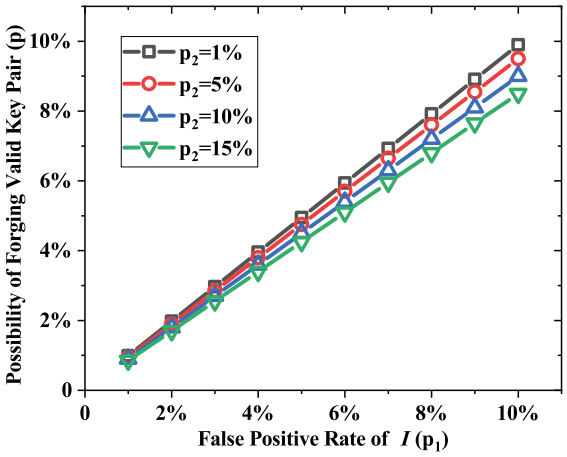



Fig. 3. Possibility of Forging a Valid Key Pair under Different Parameters.

Overall, it is impossible for malicious users to get correct $\lambda$. Even if it can successfully get $\lambda$, the possibility of generating a valid signature is still very low. Therefore, any malicious user is basically unable to launch DoS attack in FASE, and Lemma 1 is proved. ■

It is noted that our scheme focuses on addressing the DoS attacks launched by unauthorized users. As for those launched by authorized users, ISP can utilize some known methods like [46], [47] to mitigate the damages. By combining one of the methods with lowering these users' credits or asking them for paying the resources they consume, the damages of DoS attacks launched by authorized users can finally be greatly reduced.

### C. Anonymity

In the OTCS verification process, edge routers can only get the public key $\xi_j$ and secret trapdoor key $\bar{x}_j$ to generate the corresponding signature. Since the correlation between key pair and user identity is only known to MCPs, edge routers are unable to extract the signer's identity from the responses they receive.

Besides, unlinkability can also be achieved in FASE, which means that given two different responses, edge routers are incapable of distinguishing whether these two responses are generated by the same user. Since every time a user requests a content in FASE, he/she generates the corresponding response by utilizing a new public/secret key pair. Therefore, this conclusion can be easily drawn.

### D. Replay Attack Resistance

In the authentication process, a timestamp *TS* is included in user's response, so replay attacks can be easily detected by checking whether the time interval $TS - TS'$ is allowed, where $TS'$ is the time when edge routers receive the response.

### E. Service Accountability

To enable MCPs to learn the information of users' requests (e.g., the amount and distribution of requests) and improve the quality of service that MCPs provide, edge routers send service credentials $< \bar{x}_j, Info, H_{lt}, len >$ to MCPs. Because MCPs pay ISP according to the amount of requests served, edge routers may risk in forging some credentials by choosing a random number to pretend to be a valid secret trapdoor key.

*Lemma 2:* FASE can achieve secure service accountability, meaning that ISP is deterred to submit any number of faked service credentials for more profits.

*Proof:* In our scheme, MCPs conduct probabilistic verification on $\bar{x}_j$ in credentials. Suppose MCPs' check rate is $\beta$ and edge routers only submit one faked credential every time when MCPs receive $n$ credentials, then the detection probability of misbehavior is:

$$p = 1 - \binom{n-1}{n\beta} \Big/ \binom{n}{n\beta} = \beta,$$

which is a non-negligible value for a reputed company. Note that when MCPs utilize Bloom filter to check the validity of $\bar{x}_j$, $p$ will increase to $p' + (1-p')\beta$, where $p'$ is the false positive rate of Bloom filter. Besides, edge routers are deterred to modify the length of hash chain and submit duplicated credentials because the detection probability of these behavior is 100%.

Therefore, Lemma 2 is proved. ■

## VII. Performance Analysis

### A. Simulation Environment

To evaluate the performance of our scheme, we implement our scheme in the named data network (NDN) simulated by ndnSIM 2.3 [48], which is a typical network architecture with in-network caching and name-based routing. All the simulations are conducted on the Ubuntu 16.04 LTS with a 3.6GHz Intel Core i7 processor and 20GB RAM by using Pairing-Based Cryptography library with type-A curve and OpenSSL library.

The simulated network topology is generated by using BRITE and 10% of total nodes are set to edge routers. The link between any two routers has bandwidth selected randomly from 1 to 5 Gbps and delay selected randomly from 1 to 5 ms. The number of user nodes is 20% of the number of routers. Each user node connects to an edge router through a link with 100 Mbps bandwidth and 1 ms delay. The intermediate routers are equipped with cache space for 200 chunks and LRU cache policy. MCP is located centrally in the network and able to respond to every request containing its prefix. Each user requests chunks of a multimedia file continuously and does not request the next chunk until the current request is satisfied.

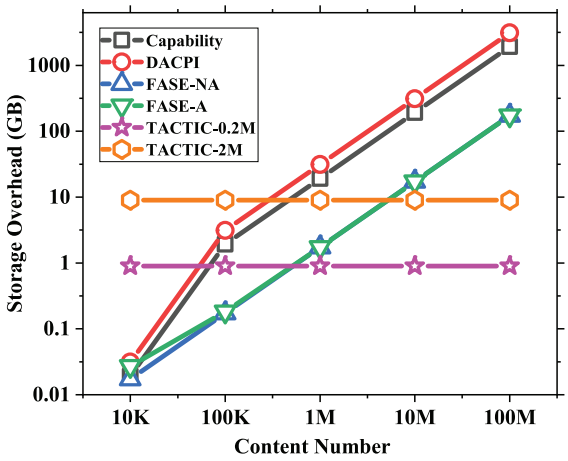



Fig. 4. Storage Overhead Comparison.

### B. Storage Overhead

We compare the overall storage overhead in the network among Capability [10], DACPI [11], TACTIC [30], and our proposed FASE. These schemes except FASE utilize content-based authentication to achieve access control. Specifically, Capability needs to store a hash value for every content in each cache-enabled router. Similar to Capability, in DACPI, besides the need to store a hash value for each content, it also requires storing an additional secret value. We utilize SHA-256 to implement these two solutions. TACTIC requires each router to store a bloom filter so as to facilitate the authentication process.

In order to decrease storage overhead, we designed an access policy-based authentication that only edge routers are responsible for authentication. Therefore, in FASE, only edge routers need to store authentication information for every access policy. In practice, the number of access policy used by an MCP is much less than the number of contents it publishes, so FASE can save massive storage space for ISP.

Fig. 4 shows the results of storage overhead comparison, where the number of access policy is 10% of the number of contents, the number of nodes is set as 600 and attribute number used by CP-ABE is set as 10. Here, we denote FASE with and without service accountability feature as FASE-A and FASE-NA, respectively. We consider in FASE-A, index $I, I'$ store 20,000 and 2,000 items respectively. With the 150KB $I$, 15KB $I'$ and 4 different hash functions, the false positive rate of $I$ and $I'$ can be acceptable, which is less than 9%. The bloom filter used in TACTIC has the exactly same false positive rate as the ones used in *FASE-A*.

We can see that although FASE-A needs to store extra 2 indices, it still outperforms DACPI when the number of contents is small. When the number of contents increases, the storage space occupied by the extra 2 indices is insignificant, compared with the overall storage overhead. Therefore, FASE-A and FASE-NA have similar performance when the number of contents is large, and both of them significantly outperform the DACPI and Capability. As for the storage overhead of TACTIC, it doesn't change with content number, but it changes

TABLE II
MAIN COMPUTATION COST OF MULTIMEDIA CONTENT PROVIDERS

| Phase | Operation | Time (ms) |
|---|---|---|
| System Initialization | Key Pair $(\bar{x}_i, \xi_i)$ Generation | 1.344/pair |
| | Other Public Parameters Generation | 3.421 |
| User Registration | Secret Key Generation | 2.684+1.344$n$ |
| Key Outsourcing | Information $\Lambda$ Generation | (1.458+4.038$l$)$m$ |
| | Valid Public Key Index Generation | $3.62 \times 10^{-4} dn'$ |
| Content Generation | Ciphertext Generation | 1.458+4.038$l$ |

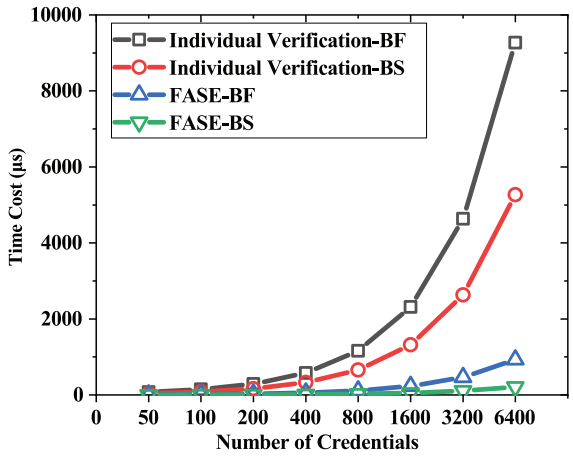



Fig. 5. Verification Time Cost vs. Number of Credentials.

with the number of items the bloom filter contains. TACTIC-0.2M and TACTIC-2M represent the schemes that the bloom filter contains 0.2 million items and 2 million items respectively. The result shows that FASE-NA and FASE-A don't care about the number of users in the system and they perform better than TACTIC when the content number is small. On the contrary, TACTIC is sensitive to the number of users (i.e., the number of items the bloom filter contains) but it performs better when the content number is large.

### C. Computation Overhead

For MCPs, computation overhead is incurred in system initialization, user registration, key outsourcing, content generation, and service accounting. Table II shows the main computation cost in the first four phases. Here, we denote the number of attributes embedded in users' secret keys, the average number of attributes in different access policies, the number of access policies, and the number of generated key pair as $n$, $l$, $m$ and $n'$, respectively.

We can see that except for key pair $(\bar{x}_i, \xi_i)$ generation and valid public key index generation, the computation overhead in MCPs is low. Even though MCPs need to generate massive number of key pairs continuously, the overhead is acceptable because it can be executed in parallel and offline. Besides, deriving $\Lambda$ only needs to be conducted once and even can be done offline. Therefore, it will not bring much burden to MCPs either.

Next, we evaluate computation overhead in the service accounting phase with total 200 million secret keys. In our scheme, MCPs can choose to use normal search algorithms like binary search or use Bloom filter to conduct service credential verification. Besides, to reduce the overhead of verifying service credentials in MCPs, in our scheme, MCPs choose a small portion of the received service credentials to conduct batch verification. In this simulation, the sample probability is set as 10%. Here, we utilize suffix *-BF,-BS* to represent different ways of service credential verification, i.e., using Bloom filter and binary search, respectively. From Fig. 5, compared with individual verification, our scheme achieves better performance. Specifically, when MCPs receive 6,400 service credentials, they can finish verification within 927 $\mu s$ and 211 $\mu s$ by using Bloom filter and binary search respectively, which is highly efficient for MCPs. Although binary search outperforms Bloom filter in time cost, Bloom filter can save 96.25% storage overhead, and only needs 1.2 GB for all the 200 million secret keys. Therefore, MCPs can choose a proper method to conduct service accounting according to their server status.

TABLE III
COMPUTATION COST OF SERVICE ACCOUNTING COMPARISON

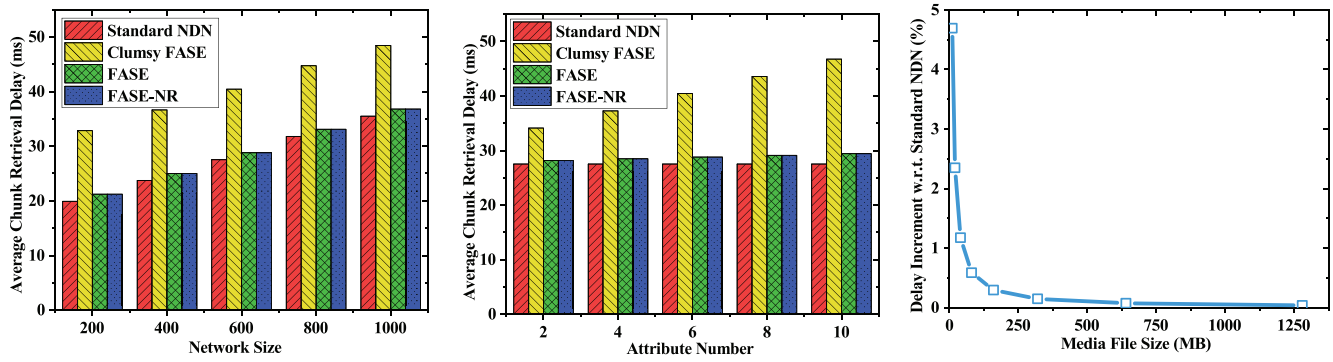
| # of credentials | Scheme | Time |
|---|---|---|
| 1600 | SEAF | 5.7 s |
| | Sultan's Scheme | 3.1 s |
| | FASE-BS | 52.5 $\mu s$ |
| 3200 | SEAF | 11.2 s |
| | Sultan's Scheme | 6.1 s |
| | FASE-BS | 105.0 $\mu s$ |
| 6400 | SEAF | 23.1 s |
| | Sultan's Scheme | 12.3 s |
| | FASE-BS | 210.0 $\mu s$ |

Besides, we compare FASE with SEAF [12] and Sultan's scheme [29] in terms of the computation overhead of the service accounting. Out of fairness consideration, we adopt the most efficient way of each scheme, i.e., SEAF with batch verification, Sultan's scheme with batch verification and FASE-BS. The results are shown in Table III, we can see that FASE-BS is about 0.1 million times faster than SEAF and about 60 thousand times faster than Sultan's scheme. Overall, the computation cost of MCPs is satisfactory in FASE.

We also evaluate the computation overhead brought to users and edge routers. As shown in TABLE IV, the most time-consuming operation for user is CP-ABE decryption which costs $0.735 + 1.579\bar{n}$ ms, where $\bar{n}$ is the number of attributes used for decryption. While it only takes about 16 ms to finish the request authentication when $\bar{n}$ is 10, which is efficient enough. For edge routers, the computation overhead in request authentication phase is much less than that of users, which is 2.7 ms for the first request and 0.362 $\mu s$ for subsequent requests.

### D. Network Simulation

Next, we evaluate the performance of FASE in the simulated network. We first compare the average chunk retrieval delay (i.e., the ratio of multimedia file retrieval delay to the number of chunks of the file) among standard NDN, FASE, FASE-NR (FASE without revocation mechanism) and clumsy




(a) Average Chunk Retrieval Delay vs. Network Size (b) Average Chunk Retrieval Delay vs. Number of Attributes (c) Average Chunk Retrieval Delay Increment vs. Media File Size

Fig. 6. The result of network Simulation.

TABLE IV
COMPUTATION COST IN REQUEST AUTHENTICATION

| Entity | Operation | Time (ms) |
|---|---|---|
| User | CP-ABE Decryption | $0.735+1.579\bar{n}$ |
| | Symmetric Key Computation | $3.62 \times 10^{-4}$ |
| | AES-256 Decryption | 0.02 (1K) |
| | OTCS Generation | 0.012 |
| Edge Router | Symmetric Key Computation | $3.62 \times 10^{-4}$ |
| | AES-256 Encryption | 0.02 (1K) |
| | Response Verification (1st request) | 2.694 |
| | Response Verification (subsequent requests) | $3.62 \times 10^{-4}$ |
| | Secret Trapdoor Key Extraction | 0.006 |

FASE (i.e., edge routers authenticate every request using the challenge-response authentication mechanism proposed).

Fig. 6(a) demonstrates the average chunk retrieval delay under different network sizes. In this simulation, we set the file size of contents to be 10 MB, chunk size to be 1 MB, and the number of attributes to be 6. As shown in Fig. 6(b), for all these schemes, the average content retrieval delay increases with growing network size. Among them, FASE only brings in a little bit more overhead than standard NDN and has no more than 6.5% increased file retrieval delay, which indicates that our scheme is efficient. Besides, FASE-NR achieves similar performance since the revocation mechanism has only a few hash operations, which is negligible compared with other heavy operations. Therefore, we can draw the conclusion that our revocation mechanism is highly efficient. However, for clumsy FASE, due to the huge overhead brought by the challenge-response authentication, the increased delay is linear to the number of attributes. Therefore, lightweight hash authentication is helpful to reduce the overhead of our system.

Fig. 6(b) illustrates the average chunk retrieval delay under different number of attributes, where the file size of a content is 10 MB, chunk size is 1 MB, and network size is 600. As shown in Fig. 6(b), except for clumsy FASE, other methods maintain a steady level when the number of attributes grows from 2 to 10. Similarly, FASE and FASE-NR also perform well. Even when the number of attributes is 10, only 7% extra chunk retrieval delay is introduced. However, the extra retrieval delay brought by clumsy FASE varies from 24% to 69.9% when the number of attributes increases from 2 to 10 due to the complex challenge-response authentication mechanism.

Next, we evaluate the average chunk retrieval delay increment compared with standard NDN. Fig. 6(c) depicts the result of FASE under different file sizes. The number of attributes, chunk size, and network size in this simulation is set to be 6, 1 MB, and 600, respectively. Although when the multimedia file only contains 1 chunk, the increased delay reaches a high level of about 49%, which is not satisfactory. However, from Fig. 6(c), we can see that with larger file size, users will send more requests and more hash authentication processes are used to counterfeit the overhead of challenge-response authentication. Thus, the file retrieval delay increment of our scheme decreases rapidly as the file size becomes larger. When the file size is 40 MB, the increased delay reduces to about 1%, which is an acceptable overhead.

## VIII. CONCLUSION

In this paper, we proposed a solution to provide secure fine-grained access control and service accounting to multimedia content providers in an in-network caching context. Specifically, we achieved the desired access control by combing CP-ABE and edge-side authentication, which makes our system more efficient and prevents malicious requests from running out network resources. The computation overhead of authentication is largely reduced with the design of hash chain while access policy based edge-side authentication helps cut down the storage overhead of edge routers. We also designed an efficient privacy-preserving signature algorithm, OTCS, to achieve anonymous authentication. Access revocation is achieved by maintaining a revoked key index through lightweight hash operations. The service credentials consisting of users' signatures and hash chain are collected by edge routers to enable MCPs to implement secure service accounting. Our security and performance analysis shows that our scheme has several security features and is efficient enough.

## REFERENCES

[1] "Cisco visual networking index: Forecast and trends, 2017–2022," Cisco, San Jose, CA, USA, White Paper, 2019. Accessed: Apr. 2021. [Online]. Available: https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html

[2] R. Tourani, S. Misra, T. Mick, and G. Panwar, "Security, privacy, and access control in information-centric networking: A survey," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 1, pp. 566–600, 1st Quart., 2018.

[3] V. Jacobson, D. K. Smetters, J. D. Thornton, M. F. Plass, N. H. Briggs, and R. L. Braynard, "Networking named content," in *Proc. 5th Int. Conf. Emerg. Netw. Exp. Technol. (CoNEXT)*, 2009, pp. 1–12.

[4] Q. Wu, Z. Li, G. Tyson, S. Uhlig, M. A. Kaafar, and G. Xie, "Privacy-aware multipath video caching for content-centric networks," *IEEE J. Sel. Areas Commun.*, vol. 34, no. 8, pp. 2219–2230, Aug. 2016.

[5] Y. Xue, K. Xue, N. Gai, J. Hong, D. S. L. Wei, and P. Hong, "An attribute-based controlled collaborative access control scheme for public cloud storage," *IEEE Trans. Inf. Forensics Security*, vol. 14, pp. 2927–2942, 2019.

[6] S. Wang, K. Liang, J. K. Liu, J. Chen, J. Yu, and W. Xie, "Attribute-based data sharing scheme revisited in cloud computing," *IEEE Trans. Inf. Forensics Security*, vol. 11, pp. 1661–1673, 2016.

[7] S. Misra, R. Tourani, F. Natividad, T. Mick, N. Majd, and H. Huang, "AccConF: An access control framework for leveraging in-network cached data in the ICN-enabled wireless edge," *IEEE Trans. Dependable Secure Comput.*, vol. 16, no. 1, pp. 5–17, Jan./Feb. 2019.

[8] S. Misra, R. Tourani, and N. E. Majd, "Secure content delivery in information-centric networks: Design, implementation, and analyses," in *Proc. 3rd ACM SIGCOMM Workshop Inf. Centric Netw. (ICN)*, 2013, pp. 73–78.

[9] Q. Li, R. Sandhu, X. Zhang, and M. Xu, "Mandatory content access control for privacy protection in information centric networks," *IEEE Trans. Dependable Secure Comput.*, vol. 14, no. 5, pp. 494–506, Sep./Oct. 2017.

[10] Q. Li, P. P. C. Lee, P. Zhang, P. Su, L. He, and K. Ren, "Capability-based security enforcement in named data networking," *IEEE/ACM Trans. Netw.*, vol. 25, no. 5, pp. 2719–2730, Oct. 2017.

[11] E. G. AbdAllah, M. Zulkernine, and H. S. Hassanein, "DACPI: A decentralized access control protocol for information centric networking," in *Proc. Int. Conf. Commun. (ICC)*, Kuala Lumpur, Malaysia, 2016, pp. 1–6.

[12] K. Xue, X. Zhang, Q. Xia, D. S. L. Wei, H. Yue, and F. Wu, "SEAF: A secure, efficient and accountable access control framework for information centric networking," in *Proc. Int. Conf. Comput. Commun. (INFOCOM)*, Honolulu, HI, USA, 2018, pp. 2213–2221.

[13] K. Xue *et al.*, "A secure, efficient, and accountable edge-based access control framework for information centric networks," *IEEE/ACM Trans. Netw.*, vol. 27, no. 3, pp. 1220–1233, Jun. 2019.

[14] G. Acs, M. Conti, P. Gasti, C. Ghali, G. Tsudik, and C. A. Wood, "Privacy-aware caching in information-centric networking," *IEEE Trans. Dependable Secure Comput.*, vol. 16, no. 2, pp. 313–328, Mar./Apr. 2019.

[15] Y. Yu, Y. Li, X. Du, R. Chen, and B. Yang, "Content protection in named data networking: Challenges and potential solutions," *IEEE Commun. Mag.*, vol. 56, no. 11, pp. 82–87, Nov. 2018.

[16] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in *Proc. Symp. Security Privacy (S&P)*, Berkeley, CA, USA, 2007, pp. 321–334.

[17] F. Guo, Y. Mu, W. Susilo, D. S. Wong, and V. Varadharajan, "CP-ABE with constant-size keys for lightweight devices," *IEEE Trans. Inf. Forensics Security*, vol. 9, pp. 763–771, 2014.

[18] Z. Liu, Z. Cao, and D. S. Wong, "Traceable CP-ABE: How to trace decryption devices found in the wild," *IEEE Trans. Inf. Forensics Security*, vol. 10, pp. 55–68, 2015.

[19] L. Lamport, "Constructing digital signatures from a one-way function," SRI Int., Palo Alto, CA, USA, Rep. CSL-98, 1979. Accessed: Apr. 2021. [Online]. Available: https://www.microsoft.com/en-us/research/publication/constructing-digital-signatures-one-way-function/

[20] P. He, K. Xue, J. Xu, Q. Xia, J. Liu, and H. Yue, "Attribute-based accountable access control for multimedia content with in-network caching," in *Proc. Int. Conf. Multimedia Expo (ICME)*, Shanghai, China, 2019, pp. 778–783.

[21] D. Boneh, B. Lynn, and H. Shacham, "Short signatures from the weil pairing," in *Proc. Int. Conf. Theory Appl. Cryptol. Inf. Security (AsiaCrypt)*, 2001, pp. 514–532.

[22] C. Zuo, J. Shao, J. K. Liu, G. Wei, and Y. Ling, "Fine-grained two-factor protection mechanism for data sharing in cloud storage," *IEEE Trans. Inf. Forensics Security*, vol. 13, pp. 186–196, 2018.

[23] E. G. AbdAllah, M. Zulkernine, and H. S. Hassanein, "Preventing unauthorized access in information centric networking," *Security Privacy*, vol. 1, no. 4, p. e33, 2018.

[24] C.-I. Fan, I.-T. Chen, C.-K. Cheng, J.-J. Huang, and W.-T. Chen, "FTP-NDN: File transfer protocol based on re-encryption for named data network supporting nondesignated receivers," *IEEE Syst. J.*, vol. 12, no. 1, pp. 473–484, Mar. 2018.

[25] Q. Li, X. Zhang, Q. Zheng, R. Sandhu, and X. Fu, "LIVE: Lightweight integrity verification and content access control for named data networking," *IEEE Trans. Inf. Forensics Security*, vol. 10, pp. 308–320, 2015.

[26] B. Li, D. Huang, Z. Wang, and Y. Zhu, "Attribute-based access control for ICN naming scheme," *IEEE Trans. Dependable Secure Comput.*, vol. 15, no. 2, pp. 194–206, Mar.–Apr. 2018.

[27] C. Bernardini, S. Marchal, M. R. Asghar, and B. Crispo, "PrivICN: Privacy-preserving content retrieval in information-centric networking," *Comput. Netw.*, vol. 149, pp. 13–28, Feb. 2019.

[28] Q. Zheng, G. Wang, R. Ravindran, and A. Azgin, "Achieving secure and scalable data access control in information-centric networking," in *Proc. IEEE Int. Conf. Commun. (ICC)*, London, U.K., 2015, pp. 5367–5373.

[29] N. H. Sultan, V. Varadharajan, S. Camtepe, and S. Nepal, "An accountable access control scheme for hierarchical content in named data networks with revocation," in *Proc. Eur. Symp. Res. Comput. Security (ESORICS)*, 2020, pp. 569–590.

[30] R. Tourani, R. Stubbs, and S. Misra, "TACTIC: Tag-based access control framework for the information-centric wireless edge networks," in *Proc. 38th IEEE Int. Conf. Distrib. Comput. Syst. (ICDCS)*, Vienna, Austria, 2018, pp. 456–466.

[31] C. Courcoubetis, F. P. Kelly, V. A. Siris, and R. Weber, "A study of simple usage-based charging schemes for broadband networks," *Telecommun. Syst.*, vol. 15, no. 3, pp. 323–343, 2000.

[32] R. T. B. Ma, "Usage-based pricing and competition in congestible network service markets," *IEEE/ACM Trans. Netw.*, vol. 24, no. 5, pp. 3084–3097, Oct. 2016.

[33] D. Lučanin, I. Pietri, S. Holmbacka, I. Brandic, J. Lilius, and R. Sakellariou, "Performance-based pricing in multi-core geo-distributed cloud computing," *IEEE Trans. Cloud Comput.*, vol. 8, no. 4, pp. 1079–1092, Oct./Dec. 2020.

[34] B. Sharma, R. K. Thulasiram, P. Thulasiraman, and R. Buyya, "Clabacus: A risk-adjusted cloud resources pricing model using financial option theory," *IEEE Trans. Cloud Comput.*, vol. 3, no. 3, pp. 332–344, Jul.–Sep. 2015.

[35] C. Ghali, G. Tsudik, C. A. Wood, and E. Yeh, "Practical accounting in content-centric networking," in *Proc. IEEE/IFIP Netw. Oper. Manage. Symp. (NOMS)*, Istanbul, Turkey, 2016, pp. 436–444.

[36] R. Tourani, S. Misra, and T. Mick, "Application-specific secure gathering of consumer preferences and feedback in ICNs," in *Proc. 3rd ACM Conf. Inf. Centric Netw. (ICN)*, 2016, pp. 65–70.

[37] S. K. Ramani, R. Tourani, G. Torres, S. Misra, and A. Afanasyev, "NDN-ABS: Attribute-based signature scheme for named data networking," in *Proc. 6th ACM Conf. Inf. Centric Netw. (ICN)*, 2019, pp. 123–133.

[38] N. P. Smart, "The discrete logarithm problem on elliptic curves of trace one," *J. Cryptol.*, vol. 12, no. 3, pp. 193–196, 1999.

[39] J. Li, K. Ren, and K. Kim, "$A^2$BE: Accountable attribute-based encryption for abuse free access control," IACR Cryptol. ePrint Archive, Lyon, France, Rep. 2009/118, 2009. [Online]. Available: http://https://eprint.iacr.org/2009/118.pdf

[40] B. H. Bloom, "Space/time trade-offs in hash coding with allowable errors," *Commun. ACM*, vol. 13, no. 7, pp. 422–426, 1970.

[41] H. Krawczyk and T. Rabin, "Chameleon signatures," in *Proc. Netw. Distrib. Syst. Security Symp. (NDSS)*, 2000, pp. 143–154.

[42] K. T. Bagci, K. E. Sahin, and A. M. Tekalp, "Compete or collaborate: Architectures for collaborative DASH video over future networks," *IEEE Trans. Multimedia*, vol. 19, no. 10, pp. 2152–2165, Oct. 2017.

[43] J. Saltarin, E. Bourtsoulatze, N. Thomos, and T. Braun, "Adaptive video streaming with network coding enabled named data networking," *IEEE Trans. Multimedia*, vol. 19, no. 10, pp. 2182–2196, Oct. 2017.

[44] B. Waters, "Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization," in *Proc. Int. Workshop Public Key Cryptogr. (PKC)*, 2011, pp. 53–70.

[45] K. Yang, X. Jia, and K. Ren, "Attribute-based fine-grained access control with efficient revocation in cloud storage systems," in *Proc. 8th ACM SIGSAC Symp. Inf. Comput. Commun. Security (CCS)*, 2013, pp. 523–528.

[46] A. Afanasyev, P. Mahadevan, I. Moiseenko, E. Uzun, and L. Zhang, "Interest flooding attack and countermeasures in named data networking," in *Proc. IFIP Netw. Conf. (IFIP Networking)*, Brooklyn, NY, USA, 2013, pp. 1–9.

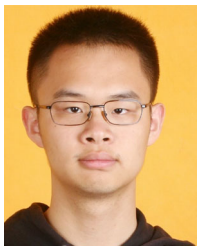
[47] A. Compagno, M. Conti, P. Gasti, and G. Tsudik, "Poseidon: Mitigating interest flooding DDoS attacks in named data networking," in *Proc. 38th Annu. IEEE Conf. Local Comput. Netw. (LCN)*, Sydney, NSW, Australia, 2013, pp. 630–638.

[48] S. Mastorakis, A. Afanasyev, I. Moiseenko, and L. Zhang, "ndnSIM 2.0: A new version of the NDN simulator for NS-3," NDN, Univ. California Los Angeles, Los Angeles, CA, USA, Rep. NDN-0028, 2015. Accessed: Apr. 2021. [Online]. Available: https://named-data.net/wp-content/uploads/2013/07/ndn-0028-1-ndnsim-v2.pdf

**Peixuan He** received the B.S. degree from the Department of Information Security and the master's degree from the Department of Electronic Engineering and Information Science form the University of Science and Technology of China in 2017, where he is currently an Engineer with Bytedance Security Research Department. His research interests include network security protocol design and analysis.

**Kaiping Xue** (Senior Member, IEEE) received the bachelor's degree from the Department of Information Security and the Ph.D. degree from the Department of Electronic Engineering and Information Science (EEIS) from the University of Science and Technology of China (USTC) in 2003 and in 2007, respectively. From May 2012 to May 2013, he was a Postdoctoral Researcher with the Department of Electrical and Computer Engineering, University of Florida. He is currently a Professor with the School of Cyber Security, USTC. His research interests include next-generation Internet architecture design, transmission optimization, and network security. He serves on the Editorial Board of several journals, including the IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, and the IEEE TRANSACTIONS ON NETWORK AND SERVICE MANAGEMENT. He has also served as a (Lead) Guest Editor for many reputed journals/magazines, including IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, *IEEE Communications Magazine*, and *IEEE Network*. He is an IET Fellow.

**Jiayu Yang** received the B.S. degree in information security from the School of Cyber Security, University of Science and Technology of China (USTC) in 2019, where she is currently pursuing the Ph.D. degree in information security from the School of Cyber Security. Her research interests include future Internet architecture design, transmission optimization, and network security.



**Qiudong Xia** received the B.S. degree from the Department of Information Security, University of Science and Technology of China (USTC) in 2018, and the master's degree in information security from the School of Cyber Security, USTC. His research interests include architecture design and security protection in ICN.

**Jianqing Liu** (Member, IEEE) received the B.Eng. degree from the University of Electronic Science and Technology of China, Chengdu, China, in 2013, and the Ph.D. degree from the Department of Electrical and Computer Engineering, University of Florida, Gainesville, FL, USA, in 2018. He is currently an Assistant Professor with the Department of Electrical and Computer Engineering, The University of Alabama in Huntsville. His research interests include wireless networking and network security in cyber–physical systems. He is a recipient of multiple best paper awards, including the Best Journal Paper Award from the IEEE Technical Committee on Green Communications & Computing in 2018.

**David S. L. Wei** (Senior Member, IEEE) received the Ph.D. degree in computer and information science from the University of Pennsylvania in 1991. From May 1993 to August 1997, he was on the Faculty of Computer Science and Engineering, The University of Aizu, Japan (as an Associate Professor and then a Professor). He is currently a Professor of Computer and Information Science Department, Fordham University. His research interests include cloud computing, big data, IoT, and cognitive radio networks. He has authored and coauthored more than 120 technical papers in various archival journals and conference proceedings. He was a guest editor or a lead guest editor for several special issues in the IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, the IEEE TRANSACTIONS ON CLOUD COMPUTING, and the IEEE TRANSACTIONS ON BIG DATA. He also served as an Associate Editor of *IEEE Transactions on Cloud Computing* from 2014 to 2018, and an Associate Editor of *Journal of Circuits, Systems and Computers* from 2013 to 2018.