


# An End-to-End Encrypted Cache System with Time-Dependent Access Control

Keita Emura<sup>1</sup> <sup>a</sup> and Masato Yoshimi<sup>2</sup>

<sup>1</sup>National Institute of Information and Communications Technology (NICT), Japan

<sup>2</sup>TIS Inc., Japan

**Keywords:** Encrypted Cache System, Time-Dependent Access Control, Naor-Naor-Lotspiech Framework, Implementation.

**Abstract:** Due to the increasing use of encrypted communication, such as Transport Layer Security (TLS), encrypted cache systems are a promising approach for providing communication efficiency and privacy. Cache-22 is an encrypted cache system (Emura et al. ISITA 2020) that makes it possible to significantly reduce communication between a cache server and a service provider. In the final procedure of Cache-22, the service provider sends the corresponding decryption key to the user via TLS and this procedure allows the service provider to control which users can access the contents. For example, if a user has downloaded ciphertexts of several episodes of a show, the service provider can decide to provide some of the contents (e.g., the first episode) available for free while requiring a fee for the remaining contents. However, no concrete access control method has been implemented in the original Cache-22 system. In this paper, we add a scalable access control protocol to Cache-22. Specifically, we propose a time-dependent access control that requires a communication cost of  $O(\log T_{\max})$  where  $T_{\max}$  is the maximum time period. Although the protocol is stateful, we can provide time-dependent access control with scalability at the expense of this key management. We present experimental results and demonstrate that the modified system is effective for controlling access rights. We also observe a relationship between cache capacity and network traffic because the number of duplicated contents is higher than that in the original Cache-22 system, due to time-dependent access control.


## 1 INTRODUCTION

Cache systems are vital to reduce communication overhead on the Internet. However, it is not trivial to provide cache systems over encrypted communications because a cache server (CS) must verify whether it has a copy of a particular encrypted content, although information about the content is not revealed due to encryption. Thus, due to the increasing use of encrypted communication, such as Transport Layer Security (TLS), encrypted cache systems are a promising approach for providing communication efficiency and privacy.

Leguay et al. (Leguay et al., 2017) proposed an encrypted cache system called CryptoCache. Although the contents are encrypted, CryptoCache allows users requesting the same content to be linked. Thus, Leguay et al. proposed an extension that prevents this linkability by employing a public key encryption

(PKE) scheme. Emura et al. (Emura et al., 2020b; Emura et al., 2022) further extended CryptoCache by proposing an encrypted cache system called Cache-22. The Cache-22 system not only provides unlinkability without employing PKE, but also presents a formal security definition in a cryptographic manner.

The Cache-22 system is briefly explained as follows and illustrated in Figure 1 in Section 2.1. It is assumed that all communications are protected by TLS. A tag is assigned to each content, and it is assumed that no information about the content is revealed by the tag (e.g., it can be generated using hash-based message authentication code (HMAC), because it is a pseudorandom function (Bellare, 2015)). The service provider (SP) encrypts content and stores the ciphertext and corresponding tag on a CS. When a user requests the content, the user sends a request to the SP. Then, the SP sends the corresponding tag back to the user. The user then sends the tag to the CS. If the tag is stored on the CS, the CS sends the corresponding ciphertext to the user and the user information to

<sup>a</sup>  <https://orcid.org/0000-0002-8969-3581>

the SP. Finally, the SP sends the corresponding decryption key to the user. Because the size of the tag is much smaller than the size of the content (ciphertext), the Cache-22 system makes it possible to significantly reduce communications between a CS and the SP. Because the Cache-22 system can employ any cipher suite, seven cipher suites, including National Institute of Standards and Technology (NIST) Post-Quantum Cryptography (PQC) candidates (Aragon et al., 2018; Bos et al., 2018; Chen et al., ; D’Anvers et al., ) are employed.

**Adding Access Control to Cache-22:** In the final procedure of the Cache-22 system, the SP sends the corresponding decryption key to the user. Emura et al. (Emura et al., 2020b; Emura et al., 2022) claimed that this procedure allows the SP to control which users can access the contents. For example, if a user has downloaded ciphertexts of several episodes of a show, the SP can allow some of the contents (e.g., the first episode) to be available for free while requiring a fee for the remaining contents. However, the authors did not provide a concrete access control method.

A naive solution is to add an authentication protocol, such as classical ID/password authentication, before the SP sends the corresponding decryption key to the user. This method is effective; however, it is not scalable. That is, the SP must send the decryption key individually for  $N$  users, which leads to a communication cost of  $O(N)$ .

## 1.1 Our Contribution

In this paper, we add a scalable access control protocol to the Cache-22 system. Specifically, we propose time-dependent access control, which requires a communication cost of  $O(\log T_{\max})$  using the Naor–Naor–Lotspiech (NNL) framework (Naor et al., 2001) where  $T_{\max}$  is the maximum time period. In the original NNL framework, each user is assigned to a leaf node of a binary tree which provides broadcast encryption in which the encryptor specifies who can decrypt the ciphertext. In our proposed protocol, each time period is assigned to a leaf node (multiple users are assigned to the same node if they have the same access rights). Briefly, let  $TI = [1, T_{\max}]$  be a time interval where  $T_{\max} \in \mathbb{N}$  and assume that  $T_{\max} = 2^m$  for some  $m \in \mathbb{N}$ . Then, each time  $t \in TI$  is assigned to a leaf node of a binary tree that has  $2^m$  leaves. This time period indicates how long the content is available. For example,  $t$  can represent a day, a week, a month, and so on. The SP encrypts each content according to the time it is available. This NNL-based time-dependent control technique has been employed in other cryptographic primitives, such as attribute-based encryption

for range attributes (Attrapadung et al., 2016) and group signatures with time-bound keys (Emura et al., 2020a). However, to the best of our knowledge, no encrypted cache system with this technique has been proposed so far.

## 2 PRELIMINARIES

### 2.1 Cache-22 System

In this section, we introduce the Cache-22 system. A tag is assigned to each content, and it is assumed that no information about the content is revealed by the tag. The SP encrypts the content and stores a tag and ciphertext pair on the CS. In the implementation proposed by (Emura et al., 2020b; Emura et al., 2022), there are multiple CSs due to the color-based cooperative cache system (Nakajima et al., 2017). For the sake of simplicity, we consider the case of a single CS. We assume that all communications between a user, CS, and SP are encrypted with TLS. Let  $(\text{Enc}, \text{Dec})$  be a IND-CPA secure SKE scheme, where for a key  $k \in \mathcal{K}$  and a message  $M \in \mathcal{M}$ ,  $\text{Dec}_k(C) = M$  holds, where  $C \leftarrow \text{Enc}_k(M)$ ,  $\mathcal{K}$  is the key space, and  $\mathcal{M}$  is the message space. Here, IND-CPA stands for indistinguishability under chosen-plaintext attack. The upper-order 128 bits of tag are used as the initial vector (IV) for AES-GCM (Iwata and Seurin, 2017). Then, IV is not reused for other encryption since the tag is pseudorandom. Let  $\text{CacheTbl}$  be the cache table managed by the CS which has the structure  $\text{CacheTbl} = \{(\text{tag}_i, C_i)\}$ , and is initiated as  $\emptyset$ . Although we simply denote  $\text{CacheTbl} = \{(\text{tag}_i, C_i)\}$  here, we can employ any cache system. We also assume that a user knows the content name  $c\_name$ , and that the SP can decide the corresponding content  $\text{content}_i \in \mathcal{M}$  from  $c\_name$ . The flow of the Cache-22 system is illustrated in Figure 1, and the formal description of the system is provided as follows. The Cache-22 system consists of  $(\text{GenTable}, \text{ContentRequest}, \text{SendContent}, \text{CacheRequest}, \text{SendKey}, \text{ObtainContent})$ . It should be noted that the SP sends the corresponding decryption key to a user via the  $\text{SendKey}$  algorithm. Because the SP needs to know the destination, each user sends own identity  $ID$  to the CP in the  $\text{SendContent}$  protocol.

- $\text{GenTable}(1^\kappa, 1^\lambda, \text{SetOfContents})$ : The table generation algorithm (run by the SP) takes as input security parameters  $\kappa, \lambda \in \mathbb{N}$  and a set of contents  $\text{SetOfContents} = \{\text{content}_i\}_{i=1}^n$ . Randomly choose  $k_{c,i} \leftarrow \mathcal{K}$  and compute  $\text{tag}_i \leftarrow \text{HMAC}_{k_{\text{hmac}}}(\text{content}_i)$  for each  $\text{content}_i \in \mathcal{M}$ .

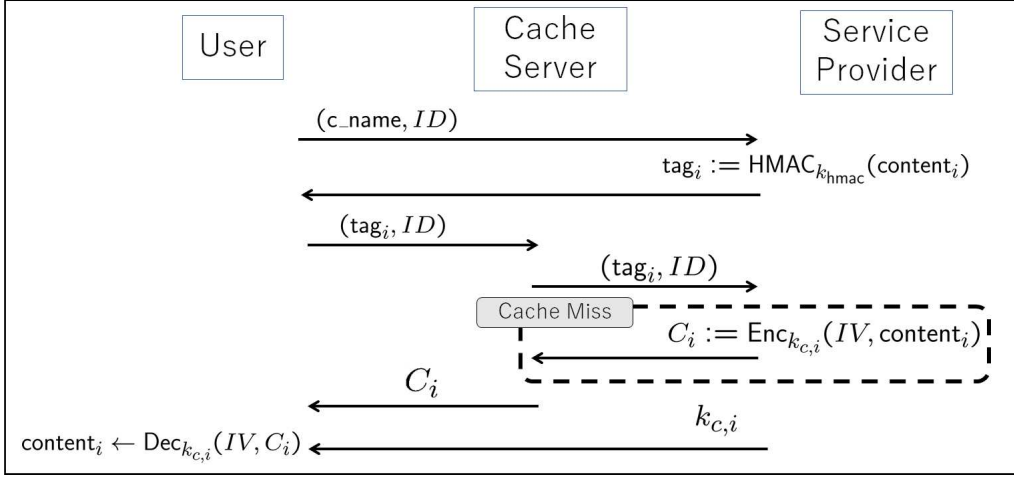


Figure 1: Cache-22 System (Emura et al., 2020b; Emura et al., 2022).

- Retrieve  $IV$  from  $tag_i$ , and encrypt  $content_i$  such that  $C_i \leftarrow Enc_{k_{c,i}}(IV, content_i)$ . Output a table  $ConTbl = \{(content_i, tag_i, C_i, k_{c,i})\}$ .
- **ContentRequest**(User( $c\_name, ID$ ), SP( $ConTbl$ )): The ContentRequest protocol between a user and the SP takes as input a content name  $c\_name$  and the user identity  $ID$  from the user, and takes as input  $ConTbl$  from the SP.
    1. The user sends  $(c\_name, ID)$  to the SP via a secure channel.
    2. The SP decides  $content_i$  from  $c\_name$ , and retrieves the corresponding  $(content_i, tag_i, C_i, k_{c,i})$  from  $ConTbl$ .
    3. The SP sends  $tag_i$  to the user via the secure channel.
  - **SendKey**(User( $tag_i, ID$ ), CS( $CacheTbl$ )): The key sending algorithm run by the SP takes as input  $(ID, k_{c,i})$ . Send  $k_{c,i}$  to the user whose identity is  $ID$  via the secure channel.
  - **ObtainContent**( $tag_i, C_i, k_{c,i}$ ): The content obtaining algorithm run by a user takes as input  $(tag_i, C_i, k_{c,i})$ . Retrieve  $IV$  from  $tag_i$ . Output  $content_i \leftarrow Dec_{k_{c,i}}(IV, C_i)$ .
- As mentioned in the introduction, there is room for adding an access control system before running the SendKey algorithm.
- ## 2.2 NNL Framework
- In this section, we introduce the NNL framework which is called the complete subtree method. Let  $BT$  be a binary tree with  $N$  leaves. For a leaf node  $i$ , let  $Path(i)$  be the set of nodes from the leaf to the root. Let  $RSet$  be the set of revoked leaves. For non leaf node  $x$ , let  $x_{left}$  be the left child of  $x$  and  $x_{right}$  be the right child of  $x$ .
1. Initialize  $X, Y \leftarrow \emptyset$ .
  2. For all  $i \in RSet$ , add  $Path(i)$  to  $X$ .
  3. For all  $x \in X$ , if  $x_{left} \notin X$  then add  $x_{left}$  to  $Y$ . If  $x_{right} \notin X$  then add  $x_{right}$  to  $Y$ .
  4. If  $|Rset| = 0$  then add the root node to  $Y$ .
  5. Output  $Y$ .
- **CacheRequest**(CS( $tag_i, ID$ ), SP( $ConTbl$ )): The cache request protocol between the CS and the SP
    1. The user sends a request  $(tag_i, ID)$  to the CS via a secure channel.
    2. The CS checks whether  $tag_i$  is stored in  $CacheTbl$ .
      - If yes, the CS retrieves  $(tag_i, C_i)$  from  $CacheTbl$  by using  $tag_i$ , sends  $C_i$  to the user via the secure channel, and sends  $(tag_i, ID)$  to the SP via the secure channel.
      - If no, the CS runs the CacheRequest protocol with the SP (which is defined later), obtains  $C_i$ , stores  $(tag_i, C_i)$  to  $CacheTbl$ , and sends  $C_i$  to the user via the secure channel.

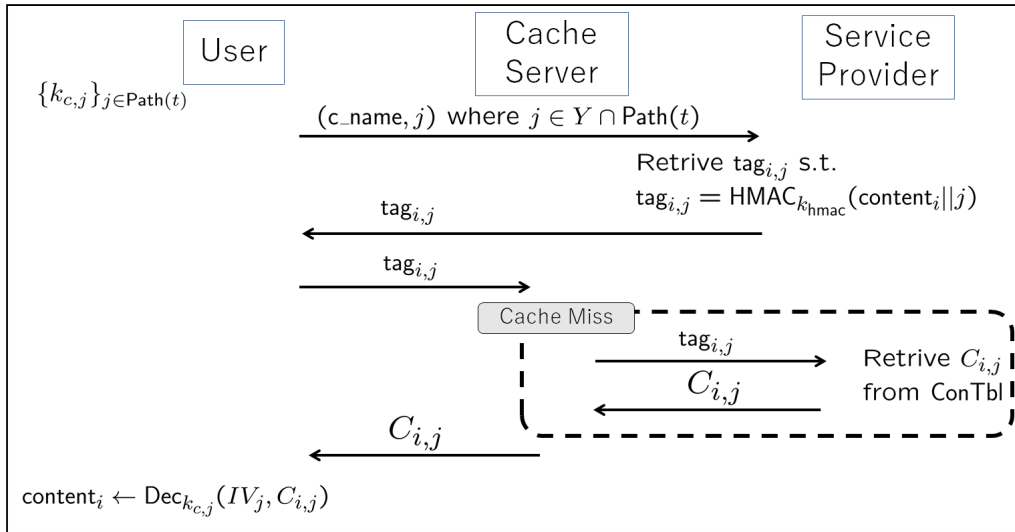


Figure 2: Cache-22 System with Time-Dependent Access Control.

We denote  $Y \leftarrow \text{CompSubTree}(\text{BT}, \text{RSet})$ . In the proposed time-dependent access control, a time period is assigned to a leaf, although each user is assigned to a leaf node in the original complete subtree method. Moreover, each leaf is sequentially revoked from the leftmost node. Then, the size of  $Y$  is estimated as  $|Y| = O(\log N)$  where  $N := T_{\max}$  in our protocol, which is scalable regardless of the number of revoked users in the system.

### 3 CACHE SYSTEM WITH TIME-DEPENDENT ACCESS CONTROL

In this section, we present our proposed protocol with time-dependent access control. Each content is encrypted with a time period  $t$ , and if a user is assigned to a time period  $t'$ , then that user is allowed to obtain contents encrypted with  $t$ , where  $t \leq t'$ . For the sake of simplicity, we assume that the access rights of all users are determined in advance. As a remark, we may be able to assume that all contents are encrypted and the SP stores all ciphertexts to the CS regardless of whether they are requested by a user or not. Then, a request sent by a user will always be successful (cache hits). However, this situation is unrealistic because the storage size of the CS will drastically increase. Thus, the SP adds new contents after receiving a user request.

Let  $T_{\max}$  be the maximum time period where  $T_{\max} \in \mathbb{N}$  and assume that  $T_{\max} = 2^m$  for some  $m \in \mathbb{N}$ . Each time period  $t \in \text{TI} = [1, T_{\max}]$  is assigned to a leaf node. If a user is assigned to a time period  $t$ ,  $\text{Path}(t)$

denotes the set of nodes from the leaf node (which is assigned to  $t$ ) to the root node. Let  $\text{CacheTbl}$  be initialized as  $\emptyset$ . In the original Cache-22 system, each tag is generated by the corresponding content such as  $\text{tag}_i \leftarrow \text{HMAC}_{k_{\text{hmac}}}(\text{content}_i)$ . In our proposed system, one content is multiply encrypted due to the NNL framework. To clarify which ciphertext should be sent to a user, each tag is generated by both the corresponding content and the corresponding index (determined by the NNL framework) such as  $\text{tag}_{i,j} \leftarrow \text{HMAC}_{k_{\text{hmac}}}(\text{content}_i || j)$ .

The proposed Cache-22 system with time-dependent access control consists of (KeyGen, SendKey, GenTable, ContentRequest, CacheRequest, SendContent, ObtainContent) as illustrated in Figure 2. Unlike to the original Cache-22 system, in the proposed system, all keys are generated in advance, i.e., they are independent of the contents. Thus, we add the KeyGen algorithm. Moreover, for a user with identity  $ID$ , the SP sends keys in accordance with the user's access rights. Thus, we run the SendKey algorithm before the GenTable algorithm.

- **KeyGen( $1^m$ ):** The key generation algorithm takes as a security parameter  $m \in \mathbb{N}$ . For  $j = 1, 2, \dots, 2^{m+1} - 1$ , randomly choose  $k_{c,j} \leftarrow \mathcal{K}$  and output  $\{k_{c,j}\}_{j=1}^{2^{m+1}-1}$ .
- **SendKey( $ID, t, \{k_{c,j}\}_{j=1}^{2^{m+1}-1}$ ):** The key sending algorithm run by the SP takes as input  $(ID, t, \{k_{c,j}\}_{j=1}^{2^{m+1}-1})$ . For all  $j \in \text{Path}(t)$ , send  $k_{c,j}$  to the user with identity  $ID$  via a secure channel.
- **GenTable( $1^k, 1^\lambda, \{k_{c,j}\}_{j=1}^{2^{m+1}-1}, \text{SetOfContents}$ ):** The table generation algorithm (run by the SP)

takes as input security parameters  $\kappa, \lambda \in \mathbb{N}$ , a set of keys  $\{k_{c,j}\}_{j=1}^{2^{m+1}+1}$ , and a set of contents  $\text{SetOfContents} = \{\text{content}_i\}_{i=1}^n$ . For  $i = 1, 2, \dots, n$ , let  $t_i \in [1, T_{\max}]$  be the time period of  $\text{content}_i$ . For all  $j \in \text{Path}(t_i)$ , compute  $\text{tag}_{i,j} \leftarrow \text{HMAC}_{k_{\text{hmac}}}(\text{content}_i || j)$ , retrieve  $IV_j$  from  $\text{tag}_{i,j}$ , and encrypt  $\text{content}_i$  such that  $C_{i,j} \leftarrow \text{Enc}_{k_{c,j}}(IV_j, \text{content}_i)$ . Output a table  $\text{ConTbl} = \{(\text{content}_i, \{(\text{tag}_{i,j}, C_{i,j}, k_{c,j})\}_{j \in \text{Path}(t_i)})\}$ .

- $\text{ContentRequest}(\text{User}(c\_name, t, t_{\text{curr}}), \text{SP}(\text{ConTbl}))$ : The ContentRequest protocol between a user and the SP takes as input a content name  $c\_name$ , the time period of the user  $t$ , and the current time period  $t_{\text{curr}}$  from the user, and takes as input  $\text{ConTbl}$  from the SP.
  1. The user runs  $Y \leftarrow \text{CompSubTree}(\text{BT}, [1, t_{\text{curr}} - 1])$  where  $\text{BT}$  is a binary tree with  $2^m$  leaves. If  $Y \cap \text{Path}(t) = \emptyset$ , then abort.
  2. The user chooses  $j \in Y \cap \text{Path}(t)$ .
  3. The user sends  $(c\_name, j)$  to the SP via a secure channel.
  4. The SP decides  $\text{content}_i$  from  $c\_name$  and retrieves the corresponding  $(\text{tag}_{i,j}, C_{i,j})$  from  $\text{ConTbl}$  where  $\text{tag}_{i,j} \leftarrow \text{HMAC}_{k_{\text{hmac}}}(\text{content}_i || j)$ .
  5. The SP sends  $\text{tag}_{i,j}$  to the user via the secure channel. If there is no such entry, then return error.
- $\text{SendContent}(\text{User}(\text{tag}_{i,j}), \text{CS}(\text{CacheTbl}))$ : The content sending protocol between a user and the CS takes as input  $\text{tag}_{i,j}$  from the user, and takes as input  $\text{CacheTbl}$  from the CS.
  1. The user sends a request  $\text{tag}_{i,j}$  to the CS via a secure channel.
  2. The CS checks whether  $\text{tag}_{i,j}$  is stored on  $\text{CacheTbl}$ .
    - If yes, the CS retrieves  $(\text{tag}_{i,j}, C_{i,j})$  from  $\text{CacheTbl}$  by using  $\text{tag}_{i,j}$ , sends  $C_{i,j}$  to the user via the secure channel.
    - If no, the CS runs the CacheRequest protocol with the SP (which is defined later), obtains  $C_{i,j}$ , stores  $(\text{tag}_{i,j}, C_{i,j})$  to  $\text{CacheTbl}$ , and sends  $C_{i,j}$  to the user via the secure channel.
- $\text{CacheRequest}(\text{CS}(\text{tag}_{i,j}), \text{SP}(\text{ConTbl}))$ : The cache request protocol between the CS and the SP takes as input  $\text{tag}_{i,j}$  from the CS, and takes as input  $\text{ConTbl}$  from the SP.

1. The CS sends  $\text{tag}_{i,j}$  to the SP via the secure channel.
2. The SP retrieves the corresponding  $(\text{tag}_{i,j}, C_{i,j})$  from  $\text{ConTbl}$  by using  $\text{tag}_{i,j}$ , and sends  $C_{i,j}$  to the CS via the secure channel.

- $\text{ObtainContent}(\text{tag}_{i,j}, C_{i,j}, k_{c,j})$ : The content obtaining algorithm run by a user takes as input  $(\text{tag}_{i,j}, C_{i,j}, k_{c,j})$ . Retrieve  $IV_j$  from  $\text{tag}_{i,j}$ . Output  $\text{content}_i \leftarrow \text{Dec}_{k_{c,j}}(IV_j, C_{i,j})$ .

As a side effect, users do not need to send their identity to the CS in the proposed system. In contrast, in the original Cache-22 system, users must send their identity to the CS because the SP must send the corresponding decryption key to the user, and the CS thus needs to forward the identity to the SP to provide the destination. The proposed system can thus help hide the user's identity from the CS and preserve privacy.

## 4 IMPLEMENTATION AND RESULTS

### 4.1 Cipher Suite

First, we decide the underlying cipher suite as

- `TLS_Kyber_ECDSA_WITH_AES_256_GCM_SHA256`

We employed Kyber (Crystals-Kyber) (Bos et al., 2018) which was selected for NIST PQC standardization in July 2022. Kyber (Crystals-Kyber) is a lattice-based scheme and is secure under the MLWE assumption where MLWE stands for the module learning with errors. In our implementation, we employed Kyber512 to provide 128-bit security. Specifically, we installed the X25519Kyber512Draft00 key agreement in our experiment. As in the original Cache-22 system, the proposed system can employ other PQC such as BIKE (Aragon et al., 2018), NTRU (Chen et al., ), and SABER (D'Anvers et al., ).

We also considered the underlying SKE scheme and hash function to be secure against the Grover algorithm (Grover, 1998), we expanded the key length twice and employed AES256 (specifically, AES-GCM-256) and SHA256. As a remark, as in the original Cache-22 implementation, we did not consider post-quantum authentication.<sup>1</sup>

<sup>1</sup>We refer the comment by Alkim et al. (Alkim et al., 2016), “the protection of stored transcripts against future decryption using quantum computers is much more urgent than post-quantum authentication. Authenticity will most likely be achievable in the foreseeable future using proven pre-quantum signatures and attacks on the signature will not compromise previous communication”.



Table 1: Libraries included in the modules.

	Version	Description
Go	go1.18.6-devel-cf	Custom Go language ( <a href="https://github.com/cloudflare/go">github.com/cloudflare/go</a> , 2022)
CIRCL	v1.2.0	Collection of PQC primitives
labstack/echo	v4.9.0	WebAPI Framework
syndtr/goleveldb	v1.0.0	Non-volatile key-value store to configure LRU cache
math/rand	Standard	Zipf function to generate content requests by user

Table 2: Host configuration.

	Specifications	Description
Instance type	c5.4xlarge	up to 0.856 [USD/hour]
vCPU [Core]	16	Intel Xeon Platinum 8275CL @ 3.00GHz
Memory [GiB]	32	
Network [Gbps]	up to 10	
Operating system	Amazon Linux 2	Kernel 5.10.135-122.509
Number of hosts	3	for CS, SP, and User

Table 3: Experimental Setup.

Number of SPs	1
Number of CSs	1
	2,048
Number of users	(We uniformly assigned users to each effective leaf node defined by CompSubTree)
Number of requests in each $t$	$2^{17} = 131,072$ (each user requests 64 contents)
Number of contents	65,535
Cache capacity in CS (Maximum number of stored contents)	4,096, 8,192 and 16,384
Size of each content [MB]	1
Popularity of content	Zipf function in Go standard library <b>math/rand</b> with arguments $s = 3, v = 3,000$ . The arguments are determined by the cache hit ratio when it becomes 75% of the cache capacity 4,096.
$T_{\max}$	16 (depth of the binary tree is 5)

## 4.2 Implementing Components

To evaluate the cache system with the mechanism described in Section 3, we experimentally implemented a cache system that provides time-dependent access control. The cache system is an extended version of the Cache-22 system to enable the encryption and decryption of contents with multiple keys. Three types of program code sets were implemented, namely, SP, CS, and User, which correspond to the components in Figure 2. All modules in these components were written in the Go language using several libraries, as described in Table 1. We employed a custom Go language ([github.com/cloudflare/go](https://github.com/cloudflare/go), 2022)

that used CIRCL (Faz-Hernández and Kwiatkowski, 2019) patched by Cloudflare to introduce PQC primitives in addition to conventional TLS algorithms such as ECDSA and RSA.

We implemented the SP as a web server which received requests from users to obtain  $\text{tag}_{i,j}$  via  $(c\_name, j)$  as illustrated in Figure 2. We also implemented the CS as a web server to forward user requests to the SP or to return cached encrypted contents to users according to  $\text{tag}_{i,j}$ . User was a simulation program to emulate many users to get encrypted contents from the CS and decrypting them when they had the corresponding decryption key. Although users send requests for various contents, the popularity fol-

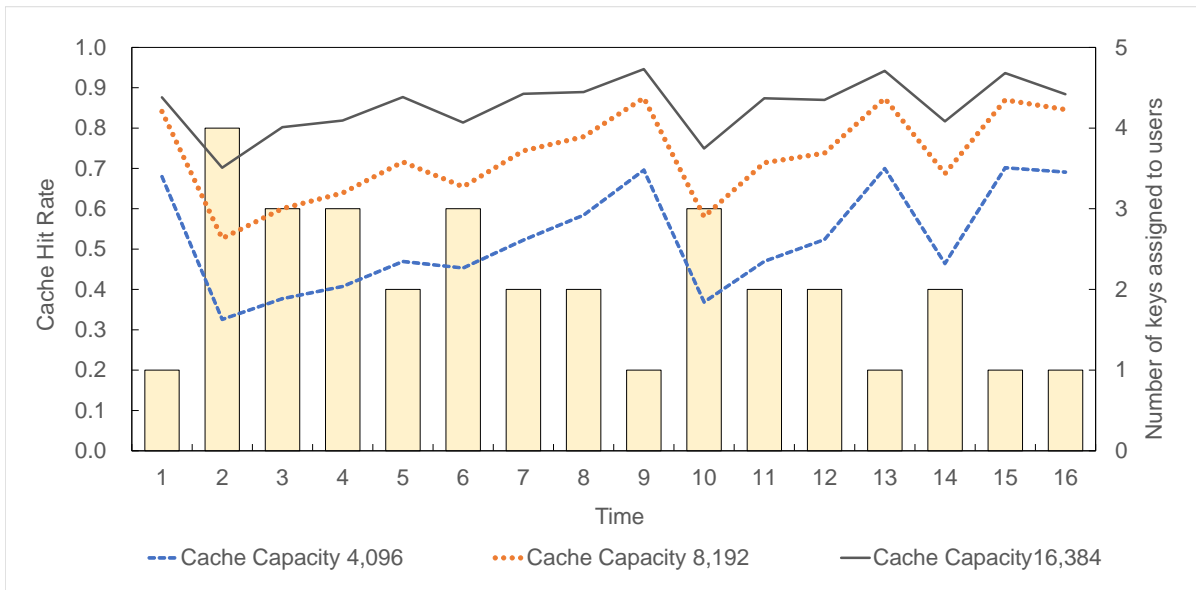


Figure 3: Time Series of Cache Hit Ratio for Three Cache Capacities in CS.

lows a characteristic trend, such as Zipf’s law and gamma distribution, especially in the case of video-on-demand services (Cheng et al., 2013). Although all components were parameterized to adapt to various situations, we set up the experimental conditions as presented in Table 3 for reasonable discussion.

As the underlying cache system, we employed the Least Recently Used (LRU) cache system. That is, ciphertexts generated in the past were unavailable at the current time and were erased from the cache table CacheTbl.

We set up several virtual machines on Amazon Elastic Compute Cloud (EC2) with a uniform configuration, as displayed in Table 2. Each host ran SP and CS processes. Many user processes were also run on EC2 with the same configuration to emulate multiple users sending requests to obtain contents from the CS.

### 4.3 Change in Network Traffic by Introducing Time-Dependent Access Control

A cache system is helpful to reduce traffic in a more upstream network, such as that between the CS and SP. There were two evaluation perspectives: (i) reduction in network traffic due to the cache system and (ii) increase in network traffic due to the time-dependent access control protocol. Figure 3 presents the time series of the cache hit ratio for each cache capacity. The three lines demonstrate that the cache capacity explicitly contributed to the reduction in network traffic. The condition of the popularity distribution in the

experiment is presented in Table 3.

At  $t_1$ , all users had  $k_1$  (which was assigned to the root node) and could obtain all contents encrypted by  $k_1$ . This signifies that a user could always decrypt a ciphertext that was stored due to a previous request by another user. The cache hit ratio in this situation was that same as that in a cache system without time-dependent access control. The cache hit ratio was greater than 70% in all cases, which demonstrates that the network traffic was reduced due to the cache system. The reduction in network traffic was approximately 50% when the cache capacity was 4,096 MB (since the size of each content is 1 MB in our experiment) which contained 6.25% of all contents. It could be increased to over 70% when the cache capacity was increased, such as to 8,192 MB and 16,384 MB, which contained 12.5% and 25% of all contents, respectively. This indicates that the network traffic can be further reduced when time-dependent access control is employed.

Next, we discuss how the cache capacity affects the hit ratio when employing time-dependent access control. Due to time-dependent access control, for every content, multiple encrypted data are generated with different encryption keys. The number of keys assigned to each content increases the number of duplicated contents. This situation may reduce the cache hit ratio because a user may not be able to decrypt a ciphertext that was stored due to a previous request by another user. The cache hit ratio is increased when the probability that the corresponding ciphertext is stored on the CS increases. Thus, when a relatively large number of keys are used for encryption, the low cache

capacity of the CS may cause an increase in the cache miss rate, which increases the amount of traffic. The cache capacity represents the effectiveness when employing time-dependent access control. This prompts us to carefully select  $T_{\max}$  because it depends on the depth of the binary tree and the number of keys used for encryption, although it provides more fine-grained access control.

## 5 CONCLUSION

In this paper, we add a time-dependent access control protocol to the Cache-22 system and provide experimental results. Due to the proposed time-dependent access control, the number of duplicated contents is higher than that in the original Cache-22 system. That is, the proposed protocol is not only effective for controlling access rights, but it also affects the relationship between the cache capacity and network traffic.

The prototype implementation of the original Cache-22 system considered multiple CSs and employed the color-based cooperative cache system (Nakajima et al., 2017), which associates servers and caches through a color tag. In the Cache-22 system with time-dependent access control, a key associated with a higher node (i.e., a node closer to the root) is assigned to more users than a key associated with a lower node (i.e., a node closer to a leaf). That is, it should be effective to introduce multiple CSs that store ciphertexts encrypted by keys associated with a higher node. Confirming the effectiveness of introducing multiple CSs is left for future work.

## ACKNOWLEDGEMENTS

This work was partially supported by JSPS KAKENHI Grant Number JP21K11897.

## REFERENCES

- Alkim, E., Ducas, L., Pöppelmann, T., and Schwabe, P. (2016). Post-quantum key exchange - A new hope. In *USENIX Security*, pages 327–343.
- Aragon, N., Barreto, P. S. L. M., Bettaieb, S., Bidoux, L., Blazy, O., Deneuville, J.-C., Gaborit, P., Gueron, S., Güneysu, T., Melchor, C. A., Misoczki, R., Persichetti, E., Sendrier, N., Tillich, J.-P., and Zémor, G. (2018). BIKE: Bit flipping key encapsulation. <https://bikesuite.org/files/BIKE.pdf>.
- Attrapadung, N., Hanaoka, G., Ogawa, K., Ohtake, G., Watanabe, H., and Yamada, S. (2016). Attribute-based encryption for range attributes. In *Security and Cryptography for Networks*, pages 42–61.
- Bellare, M. (2015). New proofs for NMAC and HMAC: security without collision resistance. *J. Cryptology*, 28(4):844–878.
- Bos, J. W., Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schanck, J. M., Schwabe, P., Seiler, G., and Stehlé, D. (2018). CRYSTALS - kyber: A CCA-secure module-lattice-based KEM. In *IEEE EuroS&P*, pages 353–367. IEEE.
- Chen, C., Danba, O., Hoffstein, J., Hulsing, A., Rijneveld, J., Schanck, J. M., Schwabe, P., Whyte, W., Zhang, Z., Saito, T., Yamakawa, T., and Xagawa, K. NTRU. <https://ntru.org/>.
- Cheng, X., Liu, J., and Dale, C. (2013). Understanding the characteristics of internet short video sharing: A youtube-based measurement study. *IEEE Transactions on Multimedia*, 15(5):1184–1194.
- D’Anvers, J.-P., Karmakar, A., Roy, S. S., and Vercauteren, F. SABER. <https://www.esat.kuleuven.be/cosic/pqcrypto/saber/>.
- Emura, K., Hayashi, T., and Ishida, A. (2020a). Group signatures with time-bound keys revisited: A new model, an efficient construction, and its implementation. *IEEE Transactions on Dependable and Secure Computing*, 17(2):292–305.
- Emura, K., Moriai, S., Nakajima, T., and Yoshimi, M. (2020b). Cache-22: A highly deployable encrypted cache system. In *ISITA*, pages 465–469. IEEE.
- Emura, K., Moriai, S., Nakajima, T., and Yoshimi, M. (2022). Cache-22: A highly deployable end-to-end encrypted cache system with post-quantum security. *IACR Cryptology ePrint Archive*, 220.
- Faz-Hernández, A. and Kwiatkowski, K. (2019). *Introducing CIRCL: An Advanced Cryptographic Library*. Cloudflare. Available at <https://github.com/cloudflare/circl>. v1.2.0 Accessed Jun 2022.
- [github.com/cloudflare/go](https://github.com/cloudflare/go) (2022). <https://github.com/cloudflare/go>.
- Grover, L. K. (1998). A framework for fast quantum mechanical algorithms. In *ACM STOC*, pages 53–62.
- Iwata, T. and Seurin, Y. (2017). Reconsidering the security bound of AES-GCM-SIV. *IACR Trans. Symmetric Cryptol.*, 2017(4):240–267.
- Leguay, J., Paschos, G. S., Quaglia, E. A., and Smyth, B. (2017). CryptoCache: Network caching with confidentiality. In *IEEE ICC*, pages 1–6.
- Nakajima, T., Yoshimi, M., Wu, C., and Yoshinaga, T. (2017). Color-based cooperative cache and its routing scheme for telco-CDNs. *IEICE Transactions on Information and Systems*, 100-D(12):2847–2856.
- Naor, D., Naor, M., and Lotspiech, J. (2001). Revocation and tracing schemes for stateless receivers. In *CRYPTO*, pages 41–62.