HAL
open science

Multi-library coded caching with partial secrecy

Michèle Wigger, Mireille Sarkiss

To cite this version:

Michèle Wigger, Mireille Sarkiss. Multi-library coded caching with partial secrecy. 2019 IEEE Information Theory Workshop (ITW), Aug 2019, Visby, Sweden. 10.1109/ITW44776.2019.8989309 . hal-02440877

HAL Id: hal-02440877

https://hal.science/hal-02440877v1

Submitted on 15 Jan 2020

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Multi-library Coded Caching with Partial Secrecy

Mireille Sarkiss[1] and Michèle Wigger[2]

[1] SAMOVAR, CNRS, Télécom SudParis, Institut Polytechnique de Paris, 91011 Evry, France; mireille.sarkiss@telecom-sudparis.eu
[2] LTCI, Télécom Paris, Institut Polytechnique de Paris, 75013, Paris, France; michele.wigger@telecom-paristech.fr

***Abstract*—The paper considers a coded caching setup with two libraries and where only one of them needs to be kept secret from an external eavesdropper. We provide upper and lower bounds on the secrecy rate-memory tradeoff for systems with $\mathsf{K} = 2$ or $\mathsf{K} = 3$ receivers. Our bounds are tight in some regimes and show that the standard (non-secure) coded caching upper bound can be approached for a wide range of parameters. In some cases, the proposed upper bound on the secrecy rate-memory tradeoff is even lower than the lower bound for standard coded caching. The reason is that in our setup the ratio of receivers requesting secure files over those requesting nonsecure files is fixed and known to everyone in advance. The transmitter can thus adjust the contents stored in the cache memories to this ratio.**

I. Introduction

Coded caching [1] promises to reduce peak-traffic in networks by smartly prefetching popular contents at the receivers during periods of low network congestion so as to create coding opportunities. This method is useful for transmitting stable and popular contents such as on-demand videos. To protect these transmissions from external eavesdroppers, [2] and [3] (see also [4], [5], [6], [7] for related works) proposed to additionally prefetch shared secret keys and to secure the coded transmissions with these secret keys. A crucial assumption in these works is that the entire library needs to be kept secret from the external eavesdropper.

In this paper, we consider a modified setup with two libraries and where only one of them needs to be kept secret from the eavesdropper. In our setup, each receiver demands a file from only one of the two library. This differs from the setup in [8] (which does not impose secrecy constraints), where each receiver demands a file from each libraries. Like in the standard coded caching scenario, the transmitter ignores the receivers' demands during the placement phase. It knows however the fraction of receivers demanding secure files, which can be seen as some form of popularity information.

We derive lower and upper bounds on the secrecy rate-memory tradeoff of the described setup for systems with 2 or 3 receivers. The upper bound is achieved by schemes based on coded caching [1] and on securing some of the transmissions by XORing them with nonsecure files and prefetched secret keys. In view of this, notice that the XOR of two files from the secure library is not secure and needs to be further protected, but the XOR of a file from the secure library and a file from the nonsecure library is secure. The lower bound is obtained by noting that some (but not all) of the lower bounds [9] previously derived for the standard coded caching setup, remain valid also in our new setup.

The obtained results allow us to conclude that the secrecy rate-memory tradeoff of the present setup can be smaller than the (worst case) rate-memory tradeoff of standard coded caching. The reason is that the transmitter can exploit the knowledge of the fraction of receivers demanding a secure file when designing the cache contents.

II. Problem Definition

We consider a system with a single transmitter connected through an error-free link to K receivers and one eavesdropper, as shown in Figure 1.

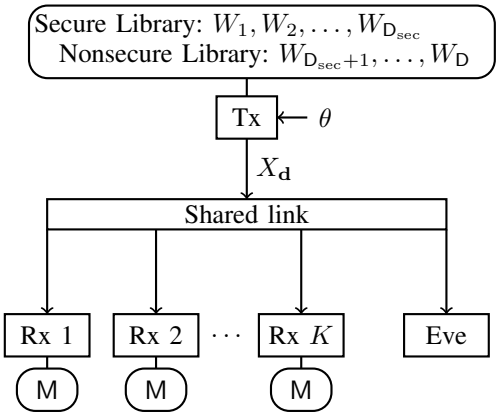

Fig. 1. Shared link with K legitimate receivers with cache memories of size M and an eavesdropper.

The transmitter can access two libraries $\mathcal{L}_{\text{sec}}$ and $\mathcal{L}_{\text{nosec}}$ containing D_{sec} and $\mathsf{D}_{\text{nosec}} := \mathsf{D} - \mathsf{D}_{\text{sec}}$ files respectively:

$$\mathcal{L}_{\text{sec}} := \{W_1, \ldots, W_{\mathsf{D}_{\text{sec}}}\} \tag{1}$$

$$\mathcal{L}_{\text{nosec}} := \{W_{\mathsf{D}_{\text{sec}}+1}, \ldots, W_{\mathsf{D}}\}. \tag{2}$$

All files are independent of each other and consist of F i.i.d. random bits. So,

$$W_d \quad \text{uniform over } \{1, \ldots, 2^{\mathsf{F}}\}, \quad \forall d \in \{1, \ldots, \mathsf{D}\}. \tag{3}$$

As described later on, the messages in the secure library $\mathcal{L}_{\text{sec}}$ have to be kept secure from an external eavesdropper.

Each receiver wishes to learn one of the D files. A fraction

$$\alpha \in \{0, 1/\mathsf{K}, 2/\mathsf{K}, \ldots, 1\} \tag{4}$$

of all demanded files belongs to the secure library and the remaining fraction $1-\alpha$ to the nonsecure library. The number of receivers asking for secure files, resp., for non-secure files, are thus given by:

$$\mathsf{K}_{\text{sec}} = \alpha \mathsf{K} \tag{5}$$

and

$$\mathsf{K}_{\text{nosec}} = (1-\alpha)\mathsf{K}. \tag{6}$$

We consider a scenario where all receivers ask for a different file and thus we require that

$$\alpha\mathsf{K} \leq \mathsf{D}_{\text{sec}} \qquad \text{and} \qquad (1-\alpha)\mathsf{K} \leq \mathsf{D}_{\text{nosec}}. \tag{7}$$

In our system, each receiver $k \in \mathcal{K} := \{1, \dots, \mathsf{K}\}$ is equipped with a local cache memory V_k of size MF bits and communication takes place in two phases. In a first *placement phase*, the transmitter can store MF bits in each of the receivers' cache memories. During this phase, the transmitter does'nt know which file each receiver wishes to learn. This information is only available in the second phase, the *delivery phase*, where the transmitter sends a signal $X_{\mathbf{d}}$ to all receivers over a shared link. We explain the two phases in more detail.

A. Placement Phase

The transmitter stores the outcome of a caching function

$$g_k \colon \left\{1, \dots, 2^{\mathsf{F}}\right\}^{\mathsf{D}} \times \Theta \to \{1, \dots, 2^{\mathsf{FM}}\} \tag{8}$$

in the cache memory for receiver k, for each $k \in \mathcal{K}$. After this phase, receiver k has cache content

$$V_k = g_k\left(W_1, \dots, W_{\mathsf{D}}, \theta\right). \tag{9}$$

We notice that the cache contents only depend on the two libraries $\mathcal{L}_{\text{sec}}$ and $\mathcal{L}_{\text{nosec}}$ and some local randomness θ.

B. Delivery Phase

Prior to the delivery phase, each receiver $k \in \mathcal{K}$ produces a demand $d_k \in \{1, \dots, \mathsf{D}\}$. It is assumed that all demands are different, so

$$d_k \neq d_{k'}, \quad k \neq k', \tag{10a}$$

and that a fraction α of the demands are between 1 and D_{sec}, whereas the remaining fraction $1-\alpha$ of demands are between $\mathsf{D}_{\text{sec}}+1$ and D:

$$\left|\{k \colon d_k \in \{1, \dots, \mathsf{D}_{\text{sec}}\}\}\right| = \alpha\mathsf{K} \tag{10b}$$

and

$$\left|\{k \colon d_k \in \{1, \dots, \mathsf{D}_{\text{nosec}}\}\}\right| = (1-\alpha)\mathsf{K} \tag{10c}$$

The demand vector

$$\mathbf{d} := (d_1, \dots d_{\mathsf{K}}) \tag{11}$$

is learned by the transmitter and all receivers.[1]

The transmitter aims at providing to each receiver k its demanded file W_{d_k}. To this end, it can send a signal $X_{\mathbf{d}}$ consisting of $R\mathsf{F}$ bits over a shared link to all receivers, where R denotes the rate of communication. The transmitted signal is of the form

$$X_{\mathbf{d}} = f_{\mathbf{d}}\left(W_1, \dots, W_{\mathsf{D}}, \theta\right), \tag{12}$$

[1]In fact, the communication of the demand vector requires zero communication rate since it takes only $\mathsf{K} \cdot \lceil \log(\mathsf{D}) \rceil$ bits to describe $\mathbf{d}$.

for some function

$$f_{\mathbf{d}} \colon \left\{1, \dots, 2^{\mathsf{F}}\right\}^{\mathsf{D}} \times \Theta \to \left\{1, \dots, 2^{R\mathsf{F}}\right\}. \tag{13}$$

Each Receiver $k \in \mathcal{K}$ attempts to decode its demanded message W_{d_k} based on the received signal $X_{\mathbf{d}}$ and its cache content V_k:

$$\hat{W}_k := \varphi_{k,\mathbf{d}}(X_{\mathbf{d}}, V_k), \quad k \in \mathcal{K}, \tag{14}$$

for some function

$$\varphi_{k,\mathbf{d}} \colon \left\{1, \dots, 2^{R\mathsf{F}}\right\} \times \left\{1, \dots, 2^{\mathsf{MF}}\right\} \to \left\{1, \dots, 2^{\mathsf{F}}\right\}. \tag{15}$$

C. Secrecy Rate-Memory Tradeoff

A decoding error occurs whenever $\hat{W}_k \neq W_{d_k}$, for some $k \in \mathcal{K}$. For a given demand vector $\mathbf{d}$, the probability of error is defined as

$$\mathrm{P}_{e,\mathbf{d}} := \mathrm{P}\left[\bigcup_{k=1}^{\mathsf{K}} \left\{\hat{W}_k \neq W_{d_k}\right\}\right]. \tag{16}$$

We assume a system with an external eavesdropper that observes the shared link during the delivery phase, but has no access to the cache memories. *All files* $W_1, \dots, W_{\mathsf{D}_{\text{sec}}}$ in the secure library $\mathcal{L}_{\text{sec}}$ have to be kept secret from this eavesdropper.

Definition 1. *Given a fraction* $\alpha \in \{0, 1/\mathsf{K}, 2/\mathsf{K}, \dots, 1\}$*, a rate-memory pair* (R, M) *is* securely achievable *if for every* $\epsilon > 0$ *and sufficiently large file size* F*, there exist caching, encoding, and decoding functions as in* (8)*,* (13)*, and* (15) *so that for each demand vector* $\mathbf{d}$ *satisfying* (10)*, the following two conditions hold:*

$$\mathrm{P}_{e,\mathbf{d}} \leq \epsilon \quad \text{and} \quad I\left(W_1, \dots, W_{\mathsf{D}_{\text{sec}}}; X_{\mathbf{d}}\right) < \epsilon. \tag{17}$$

Definition 2. *Fix a fraction* $\alpha \in \{0, 1/\mathsf{K}, 2/\mathsf{K}, \dots, 1\}$*. For a given cache memory size* M*, the* secrecy rate-memory tradeoff $R^\star_\alpha(\mathsf{M})$ *is the smallest rate* R *so that the pair* (R, M) *is securely achievable:*

$$R^\star_\alpha\left(\mathsf{M}\right) := \inf\left\{R \colon \ (R, \mathsf{M}) \text{ securely achievable}\right\}. \tag{18}$$

III. $\mathsf{K} = 2$ Receivers

Throughout this section, we assume

$$\mathsf{K} = 2, \tag{19}$$

and distinguish different values for D_{sec} and $\mathsf{D}_{\text{nosec}}$.

A. Single Files

We start with the simplest model:

$$\mathsf{D}_{\text{sec}} = \mathsf{D}_{\text{nosec}} = 1 \tag{20}$$

The only possible value for α in this case is

$$\alpha = 1/2, \tag{21}$$

and its secrecy rate-memory tradeoff is easily found to be:

$$R^\star_{\frac{1}{2}}\left(\mathsf{M}\right) = 1 - \frac{\mathsf{M}}{2}, \qquad \mathsf{M} \in [1, 2]. \tag{22}$$

To see this, notice first that $\mathsf{M} < 1$ is not admissible because it does not allow any of the receivers to learn W_1 while keeping it secret from the eavesdropper. For $\mathsf{M} \geq 1$, coded caching [1] is secure because the XOR of a secure and a nonsecure message is secure. Moreover, it achieves the smallest possible delivery rate even when there is no secrecy constraint.

B. Multiple Files

Consider now the case where

$$\mathsf{D}_{\text{nosec}} \geq 2 \qquad \text{and} \qquad \mathsf{D}_{\text{sec}} \geq 2. \tag{23}$$

The admissible values for α in this case are

$$\alpha \in \{0, 1/2, 1\}. \tag{24}$$

When $\alpha = 0$, then both receivers ask for files in the nonsecure library $\mathcal{L}_{\text{nosec}}$, and we can limit attention to this library. We thus recover the standard coded caching problem [1] for files in $\mathcal{L}_{\text{nosec}}$ and the corresponding upper and lower bounds on the rate-memory tradeoff. Similarly, when $\alpha = 1$, we fall into the standard secure caching setup of [2] with library $\mathcal{L}_{\text{sec}}$ and the nonsecure library can simply be ignored.

The most interesting case is

$$\alpha = 1/2, \tag{25}$$

and in the following we restrict attention to this value.

Depending on the available cache memory, we propose to use either of the following schemes: the coded caching scheme [1] for the combined library $\mathcal{L}_{\text{nosec}} \cup \mathcal{L}_{\text{sec}}$ with parameters $t = 1$ or $t = 2$; one of the two schemes that we describe in the following; or linear combinations of these four schemes. The coded caching schemes with parameters $t = 1$ or $t = 2$ are secure because either nothing is transmitted at all or because only the XOR of a secure message with a nonsecure message is transmitted. These two schemes achieve the rate-memory pairs (recall that here $\mathsf{K} = 2$, see (19)):

$$R_1 = \frac{1}{\mathsf{K}} \qquad \text{and} \qquad \mathsf{M}_1 = \mathsf{D}\frac{\mathsf{K}-1}{\mathsf{K}} \tag{26}$$

$$R_2 = 0 \qquad \text{and} \qquad \mathsf{M}_2 = \mathsf{D}. \tag{27}$$

We now describe a new scheme tailored to our scenario. Split each file into two subfiles

$$W_d = (W_d^{(A)}, W_d^{(B)}), \qquad d \in \{1, \dots, \mathsf{D}\} \tag{28}$$

of $\mathsf{F}/2$ bits each. Split further each of these subfiles as

$$W_d^{(A)} = (W_d^{(A_1)}, W_d^{(A_2)}) \tag{29}$$

$$W_d^{(B)} = (W_d^{(B_1)}, W_d^{(B_2)}) \tag{30}$$

of sizes $(\mathsf{F}/2)/\mathsf{D}_{\text{nosec}}$ bits and $\mathsf{F}/2(1 - 1/\mathsf{D}_{\text{nosec}})$ bits. Placement is performed as indicated below.

Cache at Rx 1	Cache at Rx 2
$\left\{W_d^{(A)}\right\}_{d=1}^{\mathsf{D}_{\text{sec}}}$ $\left\{W_d^{(A_1)}\right\}_{d=\mathsf{D}_{\text{sec}}+1}^{\mathsf{D}}$	$\left\{W_d^{(B)}\right\}_{d=1}^{\mathsf{D}_{\text{sec}}}$ $\left\{W_d^{(B_1)}\right\}_{d=\mathsf{D}_{\text{sec}}+1}^{\mathsf{D}}$

To describe the delivery communication, we assume that Receiver 1 demands a secure file and Receiver 2 a nonsecure file. For this demand vector $\mathbf{d} = (d_1, d_2)$, with $d_1 \in \{1, \dots, \mathsf{D}_{\text{sec}}\}$ and $d_2 \in \{\mathsf{D}_{\text{sec}} + 1, \dots, \mathsf{D}_{\text{nosec}}\}$, the transmitter sends

$$X_{\mathbf{d}} = [(W_{d_1}^{(B)} \oplus W_{\text{nosec}}^{(A_1)}),\ W_{d_2}^{(A_2)},\ W_{d_2}^{(B_2)}] \tag{31}$$

where $\oplus$ denotes the componentwise XOR operation and

$$W_{\text{nosec}}^{(A_1)} := (W_{\mathsf{D}_{\text{sec}}+1}^{(A_1)}, \dots, W_{\mathsf{D}}^{(A_1)}). \tag{32}$$

It is not hard to verify that with this signal and its own cache content, each receiver can reconstruct its demanded file. Moreover, an eavesdropper cannot learn anything about the secure files $W_1, \dots, W_{\mathsf{D}_{\text{sec}}}$ because the part of it that is transmitted is secured by an XOR with a nonsecure file.

The proposed scheme achieves the rate-memory pair

$$R_3 = \frac{3}{2} - \frac{1}{\mathsf{D}_{\text{nosec}}} \qquad \text{and} \qquad \mathsf{M}_3 = (\mathsf{D}_{\text{sec}} + 1)/2. \tag{33}$$

The last scheme, stores individual secret keys in the cache memories of the receivers, and communicates with each receiver separately using this key. This scheme achieves

$$R_4 := \mathsf{K} \qquad \text{and} \qquad \mathsf{M}_4 := 1. \tag{34}$$

Time- and memory-sharing these schemes yields the upper bound in the following theorem. The lower bound in the theorem is obtained from the existing lower bounds for the standard coded caching setup, see for example in [1], [9], that are derived by restricting to a single receiver. In fact, when considering a single receiver, the additional constraints (10b) and (10c) in our setup are meaningless. In this case, the lower bounds for standard coded caching apply. In contrast, when considering two receivers, constraints (10b) and (10c) become active and the lower bounds derived in [1], [9] by considering both users do not apply.

Theorem 1. *Fix $\alpha = 1/2$. For all $\mathsf{M} \in [1, \mathsf{D}]$:*

$$R_\alpha^\star(\mathsf{M}) \leq \text{lower hull}\Big(\{(R_i, \mathsf{M}_i)\}_{i=1}^4\Big) \tag{35}$$

$$R_\alpha^\star(\mathsf{M}) \geq 1 - \frac{\mathsf{M}}{\mathsf{D}}. \tag{36}$$

Figure 2 shows the derived upper and lower bounds for a total library of $\mathsf{D} = 20$ files, and either $\mathsf{D}_{\text{sec}} = 6$ or $\mathsf{D}_{\text{sec}} = 4$, consequently, either $\mathsf{D}_{\text{nosec}} = 14$ or $\mathsf{D}_{\text{nosec}} = 16$. on the standard coded caching problem with only a single, nonsecure library of size $\mathsf{D} = 20$.

Remark 1. *From Figure 2, we observe that the rate-memory tradeoff can be smaller in this partially secure model than in the original coded caching setup. The reason is that here we have a restricted demands model. For example, for $\alpha = 1/2$ we know exactly that one of the receivers will demand a secure message. A demand vector $\mathbf{d} = (1, 2)$ is thus not possible. In fact, in the proposed scheme leading to (R_1, M_1), we take advantage of this knowledge during the placement phase.*

The placement should be adapted to the value of α. This can easily be inferred from the discussion in the previous

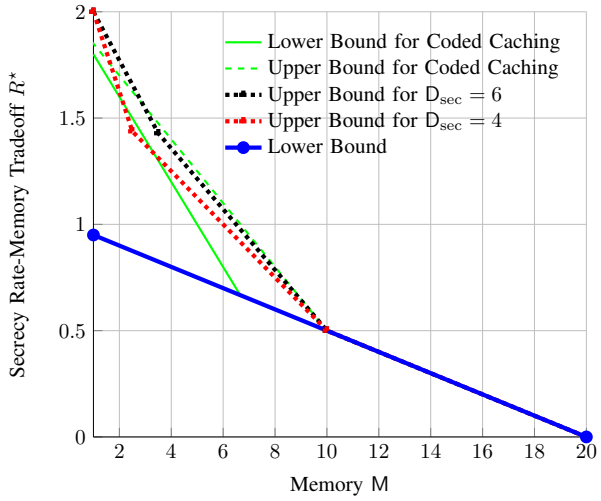

Fig. 2. Upper and lower bounds on the secrecy rate-memory tradeoff for $\mathsf{K} = 2$, $\mathsf{D}_{\text{sec}} + \mathsf{D}_{\text{nosec}} = 20$, $\mathsf{D}_{\text{sec}} = 6$ or $\mathsf{D}_{\text{sec}} = 4$. The dashed red (resp. black) line is given by connecting the rate-memory pairs (R_4, M_4), (R_3, M_3), (R_1, M_1) and (R_2, M_2) given in order from left to right.

paragraph or from the proposed placement strategies for $\alpha = 0$ or $\alpha = 1$. In fact, in these cases, the optimal strategy was simply to ignore one of the libraries depending on the value of α and to restrict to the other.

IV. $\mathsf{K} = 3$ RECEIVERS

In this section, we consider $\mathsf{K} = 3$ receivers and focus on

$$\mathsf{D}_{\text{nosec}} \geq 3 \qquad \text{and} \qquad \mathsf{D}_{\text{sec}} \geq 3. \tag{37}$$

The admissible values for α are

$$\alpha \in \{0, 1/3, 2/3, 1\}. \tag{38}$$

As before, the cases $\alpha = 0$ and $\alpha = 1$ are equivalent to the standard coded caching setup or to the secure coded caching setup with reduced libraries. We therefore focus on the cases $\alpha = 1/3$ and $\alpha = 2/3$.

A. Ratio $\alpha = 2/3$

Consider first the case $\alpha = 2/3$. The rate-memory pairs (R_1, M_1), (R_2, M_2), and (R_4, M_4) defined in (26), (27), and (34) specialized to $\mathsf{K} = 3$ are achievable using similar schemes as described for $\mathsf{K} = 2$ receivers.

We now present two new coding schemes and their corresponding rate-memory pairs. Define the parameters

$$\delta_0 := \frac{(\mathsf{D}_{\text{nosec}} - 1)^2}{3\mathsf{D}_{\text{nosec}} + (\mathsf{D}_{\text{nosec}} - 1)^2} \tag{39a}$$

$$\delta_1 := \frac{3(\mathsf{D}_{\text{nosec}} - 1)}{3\mathsf{D}_{\text{nosec}} + (\mathsf{D}_{\text{nosec}} - 1)^2} \tag{39b}$$

$$\delta_2 := \frac{3}{3\mathsf{D}_{\text{nosec}} + (\mathsf{D}_{\text{nosec}} - 1)^2} \tag{39c}$$

and split each file W_d into three independent subfiles

$$W_d = \left(W_d^{(A)}, W_d^{(B)}, W_d^{(C)}\right), \qquad d \in \{1, \dots, \mathsf{D}\}. \tag{40}$$

of sizes $\delta_0\mathsf{F}$, $\delta_1\mathsf{F}$ and $\delta_2\mathsf{F}$ bits. (Notice that $(\delta_0 + \delta_1 + \delta_2) = 1$.) Further split each subfile $W_d^{(B)}$ and each subfile $W_d^{(C)}$ into three parts:

$$W_d^{(B)} := \left(W_d^{(B_1)}, W_d^{(B_2)}, W_d^{(B_3)}\right), \tag{41}$$

$$W_d^{(C)} := \left(W_d^{(C_{12})}, W_d^{(C_{23})}, W_d^{(C_{13})}\right), \tag{42}$$

where the first three parts are of $(\delta_1/3)\mathsf{F}$ bits and the latter three parts of $(\delta_2/3)\mathsf{F}$ bits.

The placement phase is as described in the following table:

Cache at Rx 1	Cache at Rx 2	Cache at Rx 3
$\left\{W_d^{(B_1)}\right\}_{d=1}^{\mathsf{D}}$	$\left\{W_d^{(B_2)}\right\}_{d=1}^{\mathsf{D}}$	$\left\{W_d^{(B_3)}\right\}_{d=1}^{\mathsf{D}}$
$\left\{W_d^{(C_{12})}, W_d^{(C_{13})}\right\}_{d=1}^{\mathsf{D}}$	$\left\{W_d^{(C_{12})}, W_d^{(C_{23})}\right\}_{d=1}^{\mathsf{D}}$	$\left\{W_d^{(C_{13})}, W_d^{(C_{23})}\right\}_{d=1}^{\mathsf{D}}$

We describe the delivery phase, where for ease of exposition we assume that receivers 1 and 2 demand messages from the secure library and receiver 3 demands a message from the nonsecure library. So:

$$d_1, d_2 \in \{1, \dots, \mathsf{D}_{\text{sec}}\} \qquad \text{and} \qquad d_3 \in \{\mathsf{D}_{\text{sec}} + 1, \dots, \mathsf{D}\}. \tag{43}$$

For the delivery phase, time-sharing is applied over three subphases. In Subphase 1 we apply the standard coded caching delivery scheme of parameter $t = 2$ for the files $\{W_d^{(C)}\}$. Specifically, the transmitter sends

$$W_{d_1}^{(C_{23})} \oplus W_{d_2}^{(C_{13})} \oplus W_{d_3}^{(C_{12})}. \tag{44}$$

This transmission is secured because the nonsecure subfile $W_{d_3}^{(C_{12})}$ acts as a one-time pad on the other two subfiles.

In Subphase 2 we apply the coded caching delivery scheme for parameter $t = 1$ for the files $\{W_d^{(B)}\}$. Since in standard coded caching for $t = 1$ one XOR message is composed only of secure messages, a secret key is required to secure this transmission. We propose to use fragments of $\{W_d^{(C_{12})} \colon d \in \{\mathsf{D}_{\text{sec}} + 1, \dots, \mathsf{D}\} \backslash \{d_3\}\}$ to act as a secret key for both receivers. So, the transmitter first creates

$$W_{\text{key1}} := [W_d^{(C_{12})} \colon d \in \{\mathsf{D}_{\text{sec}} + 1, \dots, \mathsf{D}\} \backslash \{d_3\}] \tag{45}$$

and then sends the three XORs

$$W_{d_2}^{(B_3)} \oplus W_{d_3}^{(B_2)}, \quad W_{d_1}^{(B_3)} \oplus W_{d_3}^{(B_1)}, \quad W_{d_1}^{(B_2)} \oplus W_{d_2}^{(B_1)} \oplus W_{\text{key1}}. \tag{46}$$

Subphase 3 is dedicated to the transmission of the subfiles $\{W_d^{(A)}\}$ that are not stored in any cache memory. Thus, secret keys are required to secure the transmission to both

receivers. We propose to use fragments of $\{W_d^{(B)}: d \in \{\mathsf{D}_{\text{sec}}+1,\dots,\mathsf{D}\}\backslash\{d_3\}\}$ so that the transmitter first creates

$$W_{\text{key2}} := [W_d^{(B_1)}: d \in \{\mathsf{D}_{\text{sec}}+1,\dots,\mathsf{D}\}\backslash\{d_3\}] \quad (47)$$

$$W_{\text{key3}} := [W_d^{(B_2)}: d \in \{\mathsf{D}_{\text{sec}}+1,\dots,\mathsf{D}\}\backslash\{d_3\}] \quad (48)$$

and then sends

$$W_{d_1}^{(A)} \oplus W_{\text{key1}}, \quad W_{d_2}^{(A)} \oplus W_{\text{key2}}, \quad W_{d_3}^{(A)}. \quad (49)$$

With their cache contents, the receivers can decode their respective subfiles. At the end of the entire delivery phase, each Receiver k assembles its guesses of $W_{d_k}^{(A)}, W_{d_k}^{(B)}$ and $W_{d_k}^{(C)}$ to produce the desired message W_{d_k}.

The scheme achieves the rate-memory pair

$$R_5 := 3\delta_0 + \delta_1 + \frac{1}{3}\delta_2 \quad \text{and} \quad \mathsf{M}_5 := \frac{1}{3}\delta_1\mathsf{D} + \frac{2}{3}\delta_2\mathsf{D}. \quad (50)$$

If in the above coding scheme one eliminates subfiles $W_d^{(A)}$ and changes the size of subfiles $W_d^{(B)}$ to $\frac{\delta_1}{\delta_1+\delta_2}\mathsf{F}$ bits and the size of subfiles $W_d^{(C)}$ to $\frac{\delta_2}{\delta_1+\delta_2}\mathsf{F}$ bits, one obtains a coding scheme achieving the rate-memory pair

$$R_6 := \frac{1}{3} + \frac{2}{3}\frac{\delta_1}{\delta_1+\delta_2} \quad \text{and} \quad \mathsf{M}_6 := \frac{2}{3}\mathsf{D} - \frac{1}{3}\frac{\delta_1}{\delta_1+\delta_2}\mathsf{D}. \quad (51)$$

B. Ratio $\alpha = 1/3$

Consider now $\alpha = 1/3$. The rate-memory pairs (R_1, M_1), (R_2, M_2), and (R_4, M_4) defined in (26), (27), and (34), are achievable for $\mathsf{K} = 3$. Moreover, when $\alpha = 1/3$ then also the standard coded caching scheme with parameter $t = 1$ is secure and thus the following rate-memory pair is achievable:

$$R_7 := 1 \quad \text{and} \quad \mathsf{M}_7 := \frac{\mathsf{D}}{3}. \quad (52)$$

For $\alpha = 1/3$, the coding scheme leading to (R_5, M_5) is also secure when specialized to the parameters $\delta_2 = 0$, $\delta_1 = \frac{3}{\mathsf{D}_{\text{nosec}}+2} =: \tilde{\delta}_1$, and $\delta_0 = \frac{\mathsf{D}_{\text{nosec}}-1}{\mathsf{D}_{\text{nosec}}+2} =: \tilde{\delta}_0$ and when in the key constructions (45), (47), (48) not only demand d_3 but also demand d_2 is excluded. It then achieves the rate-memory pair

$$R_9 := 3\tilde{\delta}_0 + \tilde{\delta}_1 \quad \text{and} \quad \mathsf{M}_9 := \frac{1}{3}\tilde{\delta}_1\mathsf{D}. \quad (53)$$

Finally, generalizing the coding scheme leading to (R_3, M_3) to $\mathsf{K} = 3$ receivers, one can show (details omitted due to page limitation) that the following rate-memory pair is achievable:

$$R_8 = \frac{2}{3}\left(4 - \frac{5}{\mathsf{D}_{\text{nosec}}}\right), \qquad \mathsf{M}_8 = \frac{\mathsf{D}_{\text{sec}}+2}{3}. \quad (54)$$

Theorem 2. *Let $\mathsf{D}_{\text{sec}}, \mathsf{D}_{\text{nosec}} \geq 3$. Then,*

$$R^\star_{\frac{2}{3}}(\mathsf{M}) \leq \text{lower hull}\{(R_\ell, \mathsf{M}_\ell): \ell \in \{1,2,4,5,6\}\} \quad (55)$$

$$R^\star_{\frac{1}{3}}(\mathsf{M}) \leq \text{lower hull}\{(R_\ell, \mathsf{M}_\ell): \ell \in \{1,2,4,7,8,9\}\} \quad (56)$$

and irrespective of the value of α:

$$R^\star_\alpha(\mathsf{M}) \geq 1 - \frac{\mathsf{M}}{\mathsf{D}}. \quad (57)$$

Proof: The upper bounds follow by taking convex combinations of the presented rate-memory pairs. The lower bound is obtained by repeating the steps in the proof of [9, Theorem 1] for a single receiver. ■

Figure 3 shows the derived upper and lower bounds for $\mathsf{D}_{\text{sec}} = 10$ and $\mathsf{D}_{\text{nosec}} = 20$ and $\alpha = \frac{1}{3}$ or $\alpha = \frac{2}{3}$.

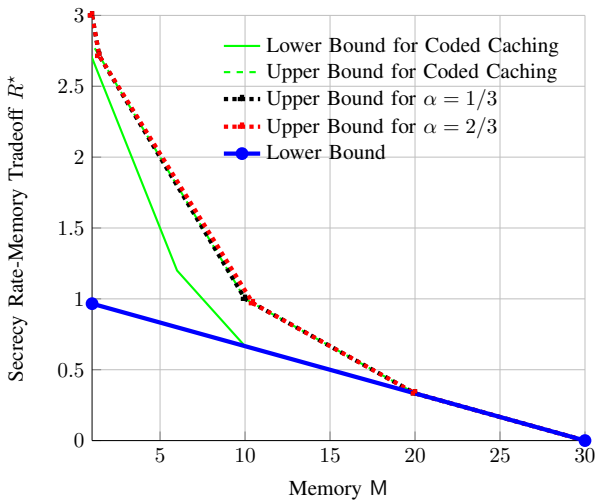

Fig. 3. Upper and lower bounds on the secrecy rate-memory tradeoff for $\mathsf{K} = 3$, $\mathsf{D}_{\text{sec}} = 10$ and $\mathsf{D}_{\text{nosec}} = 20$ for ratios $\alpha = 1/3$ and $\alpha = 2/3$. The black line is given by connecting the rate-memory pairs (R_4, M_4), (R_9, M_9), (R_8, M_8), (R_7, M_7), (R_1, M_1), (R_2, M_2) and the red line is given by connecting the rate-memory pairs (R_4, M_4), (R_5, M_5), (R_6, M_6), (R_1, M_1), (R_2, M_2), given in order from left to right.

Remark 2. *We observe from Figure 3 that for large values of $\mathsf{D}_{\text{nosec}}$ the standard coded caching lower bound can closely be approached in our secrecy setup both for $\alpha = 2/3$ and for $\alpha = 1/3$. In fact, by nesting coded caching schemes for multiple parameters, we can use the non-secure library to secure the "a priori non-secure" transmissions.*

References

[1] M. A. Maddah-Ali and U. Niesen, "Fundamental limits of caching," *IEEE Trans. Inf. Theory*, vol. 60, no. 5, pp. 2856–2867, May 2014.

[2] A. Sengupta, R. Tandon, and T. C. Clancy, "Fundamental limits of caching with secure delivery," *IEEE Trans. on Inf. Forensics and Security,* vol. 10, no. 2, pp. 355–370, Feb. 2015.

[3] H. H. Suthan C, I. Chugh, and P. Krishnan, "An improved secretive coded caching scheme exploiting common demands." *ArXiv:1705.08092*, Aug. 2017.

[4] V. Ravindrakumar, P. Panda, N. Karamchandani, and V. Prabhakarany, "Fundamental limits of secretive coded caching," *Proc. of ISIT*, Barcelona, Spain, Jul. 2016, pp. 425–429.

[5] A. A. Zewail and A. Yener, "Coded caching for resolvable networks with security requirements," *Proc. of IEEE Conf. on CNS*, Philadelphia, PA USA, Oct. 2016, pp. 621–625.

[6] Z. H. Awan and A. Sezgin, "Fundamental limits of caching in D2D networks with secure delivery," *Proc. of ICCW*, London, UK, Jun. 2015, pp. 464–469.

[7] F. Gabry, V. Bioglio and I. Land, "On edge caching with secrecy constraints," *Proc. of ICC*, Kuala Lumpur, Malaysia, May 2016.

[8] S. Sahraei and M. Gastpar, "Multi-Library Coded Caching," *ArXiv:1601.06016*, Jan 2016.

[9] C.-Y. Wang, S. Saeedi Bidokhti and M. Wigger, "Improved Converses and Gap Results for Coded Caching," *IEEE Trans. Inf. Theory*, vol. 64, no. 1, pp. 7051–7062, Jul. 2018.