Secrecy Capacity-Memory Tradeoff of Erasure Broadcast Channels

Sarah Kamel, Mireille Sarkiss, Michèlè Wigger, and Ghaya Rekaya-Ben Othman

Abstract

This paper derives upper and lower bounds on the secrecy capacity-memory tradeoff of a wiretap erasure broadcast channel (BC) with \( K_w \) weak receivers and \( K_s \) strong receivers, where weak receivers, respectively strong receivers, have same erasure probabilities and cache sizes. The lower bounds are achieved by schemes that meticulously combine joint cache-channel coding with wiretap coding and key-aided one-time pads. The presented upper bound holds more generally for arbitrary degraded BCs and arbitrary cache sizes. When only weak receivers have cache memories, upper and lower bounds coincide for small and large cache memories, thus providing the exact secrecy capacity-memory tradeoff for this setup. The derived bounds allow to further conclude that the secrecy capacity is positive even when the eavesdropper is stronger than all the legitimate receivers with cache memories. Moreover, they show that the secrecy capacity-memory tradeoff can be significantly smaller than its non-secure counterpart, but it grows much faster when cache memories are small.

The paper also presents a lower bound on the global secrecy capacity-memory tradeoff where one is allowed to optimize the cache assignment subject to a total cache budget. It is close to the best known lower bound without secrecy constraint. For small total cache budget, the global secrecy capacity-memory tradeoff is achieved by assigning all the available cache memory uniformly over all receivers if the eavesdropper is stronger than all legitimate receivers, and it is achieved by assigning the cache memory uniformly only over the weak receivers if the eavesdropper is weaker than the strong receivers.

I. INTRODUCTION

Traffic load in communication systems varies tremendously during the day between busy periods where the network is highly congested causing packet loss, delivery delays and unsatisfied users and other periods where the network is barely used. Lately, caching has emerged as a promising technique to reduce the network load and latency in such dense wireless networks. In caching, the communication is divided into two phases: the caching phase and the delivery phase. The caching phase occurs during the off-peak periods of the network, where fragments of popular contents are stored in users’ cache memories or on nearby servers. The delivery phase occurs when users request specific files during the peak-traffic periods of the network and they are served partly from their cache memories and partly from the server. The technical challenge in these networks is that in the caching phase the servers do not know exactly which files the receivers will demand during the delivery phase. They are thus obliged to store information about all possibly requested files in the receivers’ cache memories.

Maddah-Ali and Niesen showed in their seminal work [1] that the delivery (high-traffic) communication can benefit from the cache memories more than the obvious local caching gain arising from locally retrieving parts of the requested files. The additional gain, termed global caching gain, is obtained through carefully designing the cached contents and applying a new coding scheme, termed coded caching, which allows the transmitter to simultaneously serve multiple receivers. In [1] and in many subsequent works, the delivery phase is modelled as an error-free broadcast channel and all receivers have equal cache sizes. Coded caching is straightforwardly extended to noisy BCs by means of a separate cache-channel coding architecture where a standard BC code that ignores the cache contents is used to transmit the delivery-message produced by the coded caching algorithm to the receivers. Improved global caching gains can be achieved by employing joint cache-channel coding where the encoder and the decoder simultaneously adapt to the cache contents and the channel statistics [2]–[5].

A different line of works has addressed secrecy issues in cache-aided BCs [6]–[8], where delivery communication takes place over a noiseless link. Different secrecy requirements have been studied. In [6], [8], the entire library of messages needs to be kept secret from an external eavesdropper that has access to the outputs of the common bit-pipe but not to the cache memories. This is achieved by means of securing the XOR packets produced by coded caching with secret keys that have been prestored at the receivers during the caching phase [6]. This approach has subsequently been extended to resolvable networks in [9] and to device-to-device communication models [10]. In [7], each legitimate receiver acts also as eavesdropper and is thus not allowed to learn anything about the files requested by the other receivers. In this case, uncoded fragments of the messages cannot be stored in the users’ caches. Instead, random keys and combinations of messages XORed with these random keys are cached. In the delivery phase, messages (or combination of messages) XORed with random keys are transmitted in a way that...
each message can be decoded only by its intended receiver. Secret communication has also been considered for cache-aided heterogeneous and multi-antenna interference networks, see for example [11], [12], and [13]. A different angle of attack on this problem is taken in [14], which presents a privacy-preserving protocol that prevents eavesdroppers from learning which users are requesting which files as well as the statistical popularities of the files.

In this paper, we follow the secrecy requirement in [5] where an external eavesdropper is not allowed to learn anything about all the files in the library, but here delivery communication takes place over an erasure BC with one transmitter and $K \geq 2$ receivers. The eavesdropper does not have access to the cache memories but overhears the delivery communication over the erasure BC. The main interest of this paper is the secrecy capacity-memory tradeoff of such a system, i.e., the largest message rate that allows to find encoding and decoding functions so that the normalized mutual information

$$\frac{1}{n} I(W_1, \ldots, W_D; Z^n)$$

between all the messages $W_1, \ldots, W_D$ of the library and the eavesdropper’s observations $Z^n$ vanishes asymptotically for increasing blocklengths $n$. In our previous work [15], we have addressed the weaker secrecy constraint where the eavesdropper is not allowed to learn any information about each of the actually demanded messages individually. Each of the $K$ mutual informations $\frac{1}{n} I(W_{d_1}; Z^n), \ldots, \frac{1}{n} I(W_{d_K}; Z^n)$ thus needs to vanish asymptotically, where $W_{d_1}, \ldots, W_{d_K}$ denoting the files requested and delivered to Receivers $1, \ldots, K$. Our conference publications [15] and [16] suggest that the ultimate performance limits under these two secrecy constraints are close.

There are two basic approaches to render cache-aided BCs secure: 1) introduce binning to the non-secure coding schemes so as to transform them into wiretap codes [17]; and 2) store secret keys into the cache memories and apply one-time pads [18] to parts of the delivery-messages which can then be sent using non-secure channel codes. As we will see, in the BC scenarios where different receivers have different cache sizes, combinations thereof should be employed. Moreover, by applying superposition coding or joint cache-channel coding, secret keys stored in caches can even be used to secure the communication to other receivers. Under secrecy constraints, further global caching gains are thus possible than the previously reported gains for non-secure communication [1], [3].

Based on the described coding ideas, we propose lower bounds on the secrecy capacity-memory tradeoff of the cache-aided erasure BC in Figure 1. The system consists of $K_w$ weak receivers $1, \ldots, K_w$ that have equal erasure probability $\delta_w \geq 0$ and cache size $M_w$, and $K_s$ strong receivers $K_w + 1, \ldots, K$ that have equal erasure probability $\delta_s \geq 0$ and cache size $M_s$. We also provide a general upper bound on the secrecy capacity-memory tradeoff of an arbitrary degraded BC with receivers having arbitrary cache sizes. Upper and lower bounds match for the setup in Figure 1 in special cases, for example, when $M_s = 0$ and $M_w$ is sufficiently large or small. The proposed bounds moreover allow to conclude the following:

- **Secrecy Capacity is Always Positive:** In particular, the secrecy capacity is positive even when the eavesdropper is stronger than all the legitimate receivers with cache memories.

- **The Secrecy Constraint Can Significantly Harm Capacity:** The secrecy capacity-memory tradeoff can be significantly smaller than its non-secure counterpart, especially when only weak receivers have cache memories. One explanation is that when only weak receivers have cache memories, the communication to the strong receivers needs to be either secured through wiretap binning or other secrecy mechanisms, which both significantly reduce the rate of communication.

- **Caching Gains are More Important under a Secrecy Constraint:** In the regime of small cache memories, the gains of caching (i.e., the slope of the capacity) are more pronounced in our system with secrecy constraint than in the standard non-secure system. Consider for example, $M_s = 0$ and $M_w$ sufficiently small. In this regime, when the eavesdropper’s erasure probability $\delta_z$ is larger than erasure probability at the strong receivers $\delta_s$, the slope $\gamma_{sec}$ of the secrecy capacity-memory tradeoff satisfies (see Corollary 2)

$$\gamma_{sec} = \frac{K_w(\delta_z - \delta_s)}{K_w(\delta_z - \delta_s) + K_s(\delta_z - \delta_w)^+},$$

The slope $\gamma$ of the standard non-secure capacity-memory tradeoff satisfies (see [2] Theorem 2)

$$\gamma \leq \frac{K_w}{D}.$$  

This latter slope $\gamma$ thus deteriorates with increasing library size $D$, which is not the case for $\gamma_{sec}$. The main reason for this behavior is that in a standard system the cache memories are filled with data, and intuitively each stored bit is useful only under some of the demands. In a secure system, a good option is to store secret keys in the cache memories of the receivers. These secret keys are helpful for all possible demands, and therefore the caching gain does not degrade with the library size $D$.

- **Optimal Cache Assignments for Small Total Cache Budgets:** For small total cache budgets, the global secrecy capacity-memory tradeoff is achieved by assigning all of the cache memory uniformly only over the weak receivers if the
eavesdropper is weaker than strong receivers, and it is achieved by assigning all the cache memory uniformly over all receivers, if the eavesdropper is stronger than all receivers.

Paper Organization: The remainder of this paper is organized as follows. Section II formally defines the problem. Section III presents a general upper bound on the secrecy capacity-memory tradeoff and specializes it to the specific model of this work. In Sections IV and V we present our results for the scenarios when only weak receivers have cache memories and when all receivers have cache memories, and we sketch the coding schemes achieving the proposed lower bounds. Section VI contains our results on the global secrecy capacity-memory tradeoff. Sections VIII and VII describe and analyze in detail all the coding schemes proposed in this paper. Finally, Section IX concludes the paper.

II. PROBLEM DEFINITION

A. Channel Model

We consider a wiretap erasure BC with a single transmitter, $K$ receivers and one eavesdropper, as shown in Figure 1. The input alphabet of the BC is

$$\mathcal{X} = \{0, 1\}$$

and all receivers and the eavesdropper have the same output alphabet

$$\mathcal{Z} = \mathcal{Y} = \mathcal{X} \cup \Delta.$$  

The output erasure symbol $\Delta$ indicates the loss of a bit at the receiver. Let $\delta_k$ be the erasure probability of Receiver $k$’s channel, for $k \in K := \{1, \ldots, K\}$, and $\delta_z$ be the erasure probability of the eavesdropper’s channel. Hence, the marginal transition laws of this BC are described by

$$P[Y_k = y_k | X = x] = \begin{cases} 1 - \delta_k & \text{if } y_k = x \\ \delta_k & \text{if } y_k = \Delta, \forall k \in K \\ 0 & \text{otherwise} \end{cases}$$

and

$$P[Z = z | X = x] = \begin{cases} 1 - \delta_z & \text{if } z = x \\ \delta_z & \text{if } z = \Delta \\ 0 & \text{otherwise} \end{cases}$$

with $0 \leq \delta_k, \delta_z \leq 1$.

The $K$ receivers are partitioned into two sets. The first set

$$K_w := \{1, \ldots, K_w\}$$

is formed by $K_w$ weak receivers which have bad channel conditions. The second set

$$K_s := \{K_w + 1, \ldots, K\}$$

is formed by $K_s = K - K_w$ strong receivers which have good channel conditions.

In other words, we assume that

$$\delta_k = \begin{cases} \delta_w & \text{if } k \in K_w \\ \delta_s & \text{if } k \in K_s \end{cases}$$

with

$$0 \leq \delta_s \leq \delta_w \leq 1.$$  

In a standard wiretap erasure BC, reliable communication with positive rates is only possible when the eavesdropper’s erasure probability $\delta_z$ is larger than the erasure probabilities at all legitimate receivers. Here, any configuration of erasure probabilities is possible, because the legitimate receivers can prestore information in local cache memories and this information is not accessible by the eavesdropper. Specifically, we assume that each weak receiver has access to a local cache memory of size $nM_w$ bits and each strong receiver has access to a local cache memory of size $nM_s$ bits.
B. Library and Receiver Demands

The transmitter can access a library of \( D > K \) independent messages
\[
W_1, \ldots, W_D
\]
(12)
of rate \( R \geq 0 \) each. So for each \( d \in \mathcal{D} \),
\[
\mathcal{D} := \{1, \ldots, D\},
\]
(13)
message \( W_d \) is uniformly distributed over the set \( \{1, \ldots, \lfloor 2^nR \rfloor\} \), where \( n \) is the transmission blocklength.

Every receiver \( k \in K \) demands exactly one message \( W_{d_k} \) from the library. We denote the demand of Receiver \( k \) by \( d_k \in \mathcal{D} \) and the demand vector of all receivers by
\[
d := (d_1, \ldots, d_K) \in \mathcal{D}^K.
\]
(14)

Communication takes place in two phases: a first caching phase where the transmitter sends caching information to be stored in the receivers’ cache memories and the subsequent delivery phase where the demanded messages \( W_{d_k} \), for \( k \in K \), are conveyed to the receivers.

C. Placement Phase

The placement phase takes place during periods of low network-traffic. The transmitter therefore has all the available resources to transmit the cached contents in an error-free and secure fashion, and this first phase is only restricted by the storage constraints on the cache memories. However, since the caching phase takes place before the receivers demand their files, the cached content cannot depend on the demand vector \( d \), but only on the library and local randomness \( \theta \) that is accessible by the transmitter. The cache content \( V_k \) stored at receiver \( k \in \{1, \ldots, K\} \) is thus of the form
\[
V_k = g_k(W_1, \ldots, W_D, \theta),
\]
(15)
for some caching function
\[
g_k : \{1, \ldots, \lfloor 2^nR \rfloor\}^D \times \Theta \to \mathcal{V}_k
\]
(16)
where for \( k \in K_w \)
\[
\mathcal{V}_k := \{1, \ldots, \lfloor 2^nM_w \rfloor\}, \quad k \in K_w
\]
(17)
and for \( k \in K_s \)
\[
\mathcal{V}_k := \{1, \ldots, \lfloor 2^nM_s \rfloor\}, \quad k \in K_s.
\]
(18)
D. Delivery Phase

Prior to the delivery phase, the demand vector \( \mathbf{d} \) is learned by the transmitter and the legitimate receivers. The communication of the demand vector requires zero communication rate since it takes only \( K \cdot \lceil \log(D) \rceil \) bits to describe \( \mathbf{d} \).

Based on the demand vector \( \mathbf{d} \), the transmitter sends

\[
X^n = f_\mathbf{d}(W_1, \ldots, W_D, \theta),
\]

for some function

\[
f_\mathbf{d}: \{1, \ldots, [2^{nR}]\}^D \times \Theta \rightarrow X^n.
\]

Each Receiver \( k \in K \), attempts to decode its demanded message \( W_{d_k} \) based on its observed outputs \( Y^n_k \) and its cache content \( V_k \):

\[
\hat{W}_k := \varphi_{k,\mathbf{d}}(Y^n_k, V_k), \quad k \in K,
\]

for some function

\[
\varphi_{k,\mathbf{d}}: \mathcal{Y}^n_k \times \mathcal{V}_k \rightarrow \{1, \ldots, [2^{nR}]\}.
\]

E. Secrecy Capacity-Memory Tradeoff

A decoding error occurs whenever \( \hat{W}_k \neq W_{d_k} \), for some \( k \in K \). We consider the worst-case probability of error over all feasible demand vectors

\[
P^\text{Worst}_e := \max_{d \in \mathcal{D}^K} P \left( \bigcup_{k=1}^K \{ \hat{W}_k \neq W_{d_k} \} \right).
\]

The communication is considered secure if the eavesdropper’s channel outputs \( Z^n \) during the delivery phase provide no information about the entire library:

\[
\lim_{n \to \infty} \frac{1}{n} I(W_1, \ldots, W_D; Z^n) < \epsilon.
\]

As mentioned previously, the caching phase is supposed to be kept secure from the eavesdropper. This latter thus eavesdrops only on the delivery communication.

Definition 1. A rate-memory triple \((R, M_w, M_s)\) is securely achievable if for every \( \epsilon > 0 \) and sufficiently large blocklength \( n \), there exist caching, encoding, and decoding functions as in (16), (20), and (22) so that

\[
P^\text{Worst}_e \leq \epsilon \quad \text{and} \quad \frac{1}{n} I(W_1, \ldots, W_D; Z^n) < \epsilon.
\]

In our previous works [15] and [16], we called this secrecy constraint a *joint secrecy constraint* to distinguish it from the individual secrecy constraint in [15] where the second inequality in (25) is replaced by \( \frac{1}{n} I(W_{d_k}; Z^n) < \epsilon, \forall k \in K \).

Definition 2. Given cache memory sizes \((M_w, M_s)\), the secrecy capacity-memory tradeoff \( C_{\text{sec}}(M_w, M_s) \) is the supremum of all rates \( R \) so that the triple \((R, M_w, M_s)\) is securely achievable:

\[
C_{\text{sec}}(M_w, M_s) := \sup \{ R : (R, M_w, M_s) \text{ securely achievable} \}.
\]

Remark 1. Without cache memories, i.e., \( M_w = M_s = 0 \), the secrecy capacity-memory tradeoff \( C_{\text{sec}}(M_w, M_s) \) was determined in [19]:

\[
C_{\text{sec}}(M_w = 0, M_s = 0) = \left( \sum_{k=1}^K \frac{1}{\delta_s - \delta_k} \right)^{-1}.
\]

For comparison, we will also be interested in the standard (non-secure) capacity-memory tradeoff \( C(M_w, M_s) \) as defined in [3, 20]. It is the largest rate \( R \) for given cache sizes \( M_w \) and \( M_s \) that allows to find caching, encoding, and decoding functions as in (16), (20), and (22) so that

\[
P^\text{Worst}_e \leq \epsilon.
\]

That means, \( C(M_w, M_s) \) differs from \( C_{\text{sec}}(M_w, M_s) \) in that no secrecy constraint is imposed.

We start with a small section on preliminaries.
Let each Receiver $k$ and all other legitimate receivers are degraded with respect to the eavesdropper. Three scenarios can be considered: then $P$ with entries drawn i.i.d. according to some distribution $\mathcal{D}$.

Otherwise, the lemma can be proved for example by following the steps in [17, Ch. 22.2], see p. 554 and Proof of Lemma 22.1.

The message $W$ sends this codeword over the channel. If the cardinalities of the subsets $S(w)$ satisfy

$$\log_2 |S(w)| \geq \min\{R', (1 - \delta_z)\}, \quad \forall w' \in \{1, \ldots, [2^{nR'}]\},$$

then

$$\frac{1}{n} I(W'; Z^n | C) \to 0 \quad \text{as} \quad n' \to \infty.$$  \hspace{1cm} (35)

**Proof:** If $\log_2 |S(w')| = R'$, then the message is encoded by means of a one-time pad [18] and $\frac{1}{n} I(W'; Z^n | C) = 0$. Otherwise, the lemma can be proved for example by following the steps in [17 Ch. 22.2], see p. 554 and Proof of Lemma 22.1.

### III. Upper Bounds on Secrecy Capacity-Memory Tradeoff

We start by presenting an upper bound on the secrecy capacity-memory tradeoff of a general degraded $K$-user BC with arbitrary cache sizes $M_1, \ldots, M_K$ at the receivers. Subsequently, we specialize this bound to the erasure BC studied in this paper where all weak receivers and all strong receivers have equal cache sizes.

Consider an arbitrary degraded $K$-user discrete memoryless BC (not necessarily an erasure BC) with channel transition law $\Gamma(y_1, \ldots, y_K|x)$. For simplicity, and because our result depends only on the conditional marginals $\Gamma_1(y_1|x), \ldots, \Gamma_K(y_K|x)$, we assume that the channel is physically degraded, so the Markov chain

$$X \to Y_K \to Y_{K-1} \to \ldots \to Y_1$$

holds. In the same spirit, we also assume that the eavesdropper is degraded with respect to some of the legitimate receivers, and all other legitimate receivers are degraded with respect to the eavesdropper. Three scenarios can be considered:

a) The eavesdropper is degraded with respect to all legitimate receivers:

$$X \to Y_K \to Y_{K-1} \to \ldots \to Y_1 \to Z.$$  \hspace{1cm} (37)

b) All legitimate receivers are degraded with respect to the eavesdropper:

$$X \to Z \to Y_K \to Y_{K-1} \to \ldots \to Y_1.$$  \hspace{1cm} (38)

c) The eavesdropper is degraded with respect to the strongest $K - \ell^*$ legitimate receivers, for some $\ell^* \in \{1, \ldots, K - 1\}$, and the remaining legitimate receivers are degraded with respect to the eavesdropper:

$$X \to Y_K \to Y_{K-1} \to \ldots \to Y_{\ell^*+1} \to Z \to Y_{\ell^*} \to \ldots \to Y_1.$$  \hspace{1cm} (39)

Let each Receiver $k \in \{1, \ldots, K\}$ have cache size $M_k$. The following lemma holds.

**F. Preliminaries: A Mapping and A Lemma**

For fixed positive real numbers $n, R', R_{\text{Key}},$ define the mapping

$$\text{sec}(w, \text{key}): [2^{nR'}] \times [2^{nR_{\text{Key}}}] \to [2^{nR'}],$$

where $\mod$ denotes the modulo operator. Notice that from $\text{sec}(w, \text{key})$ and key it is possible to recover $w$. Let $\text{sec}_{\text{key}}^{-1}()$ denote this inverse mapping so that

$$\text{sec}_{\text{key}}^{-1}(\text{sec}(w, \text{key})) = w.$$  \hspace{1cm} (31)

When $R' = R_{\text{Key}}$, we also write $\bigoplus$ instead of $\text{sec}$:

$$w_1 \bigoplus w_2 := \text{sec}(w_1, w_2).$$  \hspace{1cm} (32)

We mostly use $\text{sec}$ when one of the arguments is a secret key and we use $\bigoplus$ when both arguments refer to messages.

The following lemma is key in the secrecy analysis of our schemes.

**Lemma 1.** Consider the rates $\tilde{R} \geq R' > 0$ and the random codebook

$$\mathcal{C} = \left\{ x^n(\ell) : \ell \in \{1, \ldots, [2^{nR'}]\} \right\}$$

with entries drawn i.i.d. according to some distribution $P_X$. Let the message $W'$ be uniform over $\{1, \ldots, [2^{nR'}]\}$. To encode the message $W' = w'$, the transmitter picks uniformly at random a codeword from a predetermined subset $S(w') \subseteq \mathcal{C}$ and sends this codeword over the channel. If the cardinalities of the subsets $\{S(w')\}$ satisfy

$$\log_2 |S(w')| \geq \min\{R', (1 - \delta_z)\}, \quad \forall w' \in \{1, \ldots, [2^{nR'}]\},$$

then

$$\frac{1}{n} I(W'; Z^n | C) \to 0 \quad \text{as} \quad n' \to \infty.$$  \hspace{1cm} (35)

**Proof:** If $\log_2 |S(w')| = R'$, then the message is encoded by means of a one-time pad [18] and $\frac{1}{n} I(W'; Z^n | C) = 0$. Otherwise, the lemma can be proved for example by following the steps in [17 Ch. 22.2], see p. 554 and Proof of Lemma 22.1.

\end{document}
Lemma 2 (Upper Bound for Arbitrary Degraded BCs and Cache Sizes). If a rate-memory tuple \((R, M_1, \ldots, M_k)\) is securely achievable, then for each receiver set \(S := \{j_1, \ldots, j_{|S|}\} \subseteq \mathcal{K}\), there exist auxiliary \((U_1, U_2, \ldots, U_{|S|}, Q)\) so that for each realization of \(Q = q\) the following Markov chain holds:

\[
U_1 \rightarrow U_2 \rightarrow \ldots \rightarrow U_{|S|} \rightarrow X \rightarrow (Y_{j_1}, \ldots, Y_{j_{|S|}}, Z);
\]

and the following \(|S|\) inequalities are satisfied:

\[
R \leq [I(U_1; Y_{j_1}|Q) - I(U_1; Z|Q)]^+ + M_{j_1},
\]

or

\[
R \leq \max_{\ell=1}^k [I(U_{\ell}; Y_{j_\ell}|U_{\ell-1}, Q) - I(U_\ell; Z|U_{\ell-1}, Q)]^+ + \sum_{\ell=1}^k M_{j_\ell}, \quad k \in \{2, \ldots, |S|\},
\]

where \(\{\cdot\}^+ := \max\{0, \cdot\}\).

Proof. See Appendix A.

Theorem 1 (Upper Bound on \(C_{\text{sec}}(M_w, M_s)\)). For each choice of \(k_w \in \{0, 1, \ldots, K_w\}\) and \(k_s \in \{0, 1, \ldots, K_s\}\), the secrecy capacity-memory tradeoff is upper bounded in the following two ways:

1) \[
C_{\text{sec}}(M_w, M_s) \leq \max_{\beta \in [0, 1]} \min \left\{ \frac{\beta (\delta_z - \delta_u)^+}{k_w} + M_w, \frac{\beta (\delta_z - \delta_u)^+}{k_w + k_s} + M_w + k_s M_s \right\};
\]

and

2) \[
C_{\text{sec}}(M_w, M_s) \leq \left\{ \min_{i=1, \ldots, k_w} \left\{ (1 - \delta_u) \beta_j + \alpha_i \right\}, \min_{j=1, \ldots, k_s} \left\{ (1 - \delta_u) \beta_{k_w+j} + \alpha_{k_w+j} \right\} \right\},
\]

for some tuple of nonnegative real numbers \(\beta_1, \ldots, \beta_{k_w+k_s} \geq 0\) summing to 1, where

\[
\alpha_i := \min \left\{ \frac{i M_w}{D - i + 1} \cdot \frac{1}{k_w + k_s - i + 1}, \frac{(k_w + k_s)(k_w M_w + k_s M_s)}{D} - \sum_{\ell=1}^{i-1} \alpha_{\ell} \right\}, \quad i = 1, \ldots, k_w,
\]

\[
\alpha_{k_w+j} := \min \left\{ \frac{k_w M_w + j M_s}{D - k_w - j + 1} \cdot \frac{1}{k_s + j - 1}, \frac{(k_w + k_s)(k_w M_w + k_s M_s)}{D} - \sum_{\ell=1}^{j-1} \alpha_{\ell} \right\}, \quad j = 1, \ldots, k_s.
\]

Proof. The first upper bound in (42a) is obtained by specializing Lemma 2 to the erasure BC in Figure 1. Based on the previous lemma and the upper bound on the standard (non-secure) capacity-memory tradeoff in [20] Theorem 5], the following Theorem 1 presents two upper bounds (Inequalities (42a) and (42b)) on the secrecy capacity-memory tradeoff for each choice of \(k_w \in \{0, 1, \ldots, K_w\}\) and \(k_s \in \{0, 1, \ldots, K_s\}\). Depending on the cache sizes \(M_w\) and \(M_s\), a different choice of the parameters and of the bounds (42a) or (42b) is tightest.
or

\[ S = \{K_w + 1, \ldots, K_w + k_s\}, \]  

and by noticing that for the subset in (45a) one can restrict to

\[ \beta_1 = \beta_2 = \ldots = \beta_{K_w} = \frac{\beta}{K_w} \]  

and

\[ \beta_{K_w+1} = \beta_{K_w+2} = \ldots = \beta_{K_w+k_s} = \frac{1 - \beta}{k_s}, \]  

for some \( \beta \in [0, 1] \). For the subset in (45b) one can restrict to

\[ \beta_1 = \beta_2 = \ldots = \beta_{K_w} = \frac{1}{K_w}, \]  

and the subset in (45c) one can restrict to

\[ \beta_{K_w+1} = \beta_{K_w+2} = \ldots = \beta_{K_w+k_s} = \frac{1}{k_s}. \]  

Constraint (42b) follows by ignoring the secrecy constraint and specializing [20, Theorem 5] to the erasure BC with weak and strong receivers considered in this paper.

We simplify this upper bound for the special cases where only weak receivers have cache memories. More specifically, we replace the upper bound in (42b), which is obtained from [20, Theorem 5], by a simpler bound that is obtained by specializing the weaker upper bound in [3].

**Corollary 1** (Upper Bound on \( C_{sec}(M_w, M_s = 0) \) ). For each choice of \( k_w \in \{0, 1, \ldots, K_w\} \), the secrecy capacity-memory tradeoff \( C_{sec}(M_w, M_s = 0) \) is upper bounded in the following two ways:

\[
C_{sec}(M_w, M_s = 0) \leq \left( \frac{k_w}{1 - \delta_w} + \frac{K_s}{1 - \delta_s} \right)^{-1} + \frac{k_w M_w}{D},  
\]

and

\[
C_{sec}(M_w, M_s = 0) \leq \max_{\beta \in [0, 1]} \min \left\{ \frac{\beta(\delta_s - \delta_w)^+}{k_w} + M_w, \frac{\beta(\delta_s - \delta_w)^+ + (1 - \beta)(\delta_s - \delta_s)^+}{k_w + K_s} + \frac{k_w M_w}{k_w + K_s} \right\}.  
\]

**Proof.** Constraint (50a) follows from [3] and by ignoring the secrecy constraint. Constraint (50b) is obtained by specializing (42a) to the case when \( M_s = 0 \). We notice that in this case the constraint that (42a) generates for \( j = K_s \) is tighter than any constraint that it generates for \( j < K_s \). Thus, we can remove all constraints for \( j < K_s \) without affecting the result and we retain only the constraint in (50b).

**IV. RESULTS WHEN ONLY WEAK RECEIVERS HAVE CACHE MEMORIES**

Consider the special case where only weak receivers have cache memories, i.e.

\[ M_s = 0. \]

(51)

In this case, a positive secrecy rate can only be achieved if

\[ \delta_s < \delta_s. \]

(52)

In the remainder of this section we assume that (52) holds.

**A. Coding Schemes**

We present four coding schemes in the order of increasing cache requirements. In the first two schemes, only random keys are placed in the cache memories. The third and fourth schemes also place parts of the messages in the cache memories and apply joint cache-channel coding for the delivery communication where the decoding operations at the receivers adapt at the same time to the channel statistics and the cache contents. For simplicity, and because on an erasure BC time-sharing is optimal to send independent messages to the various receivers, in some of our schemes communication is divided into subphases. When applied to general discrete memoryless BCs, the schemes can be improved by superposing various subphases on each other.
1) Wiretap and Cached Keys:

**Placement phase:** Store an independent secret key $K_i$ in Receiver $i$’s cache memory, for $i \in K_w$.

| Cache at Rx 1 | Cache at Rx 2 | Cache at Rx 3 | Cache at Rx $K_w$ |
|--------------|--------------|--------------|------------------|
| $K_1$        | $K_2$        | $K_3$        | $K_{K_w}$        |

**Delivery phase:** Time-sharing is applied over two subphases, where transmission in the first subphase is to all the weak receivers and transmission in the second subphase is to all strong receivers. In Subphase 1, the transmitter uses a standard (non-secure) broadcast code to send the secured message tuple

$$W_{sec} := \left\{ \sec(W_{d_1}, K_1), \sec(W_{d_2}, K_2), \sec(W_{d_3}, K_3), \ldots, \sec(W_{d_{K_w}}, K_{K_w}) \right\},$$

(53)
to weak receivers $1, \ldots, K_w$, respectively. With the secret key $K_i$ stored in its cache memory, each weak receiver $i \in K_w$ can then recover a guess of its desired message $W_{d_i}$. In Subphase 2, the transmitter uses a wiretap broadcast code [19] to send messages $W_{d_{K_w+1}}, \ldots, W_{d_k}$ to the strong receivers $K_{w+1}, \ldots, K$, respectively.

For a detailed analysis, see Section VII-A.

2) Cache-Aided Superposition Jamming:

**Placement phase:** As in the previous subsection, store an independent secret key $K_i$ in Receiver $i$’s cache memory, for $i \in K_w$.

| Cache at Rx 1 | Cache at Rx 2 | Cache at Rx 3 | Cache at Rx $K_w$ |
|--------------|--------------|--------------|------------------|
| $K_1$        | $K_2$        | $K_3$        | $K_{K_w}$        |

**Delivery phase:** The transmitter uses a superposition code to send the secured message tuple

$$W_{sec} := \left\{ \sec(W_{d_1}, K_1), \sec(W_{d_2}, K_2), \sec(W_{d_3}, K_3), \ldots, \sec(W_{d_{K_w}}, K_{K_w}) \right\},$$

(54)
in the cloud center and the non-secure message tuple

$$W_{sat} := \left( W_{d_{K_w+1}}, \ldots, W_{d_k} \right)$$

(55)
in the satellite. If the rate of the cloud messages (54) does not suffice to secure the satellite message, random binning is added to the satellite codebook. See Figure 2. Weak receivers decode only the cloud center and strong receivers the cloud center and the satellite codeword. From this decoding operation, each strong receiver $j \in K_s$ directly obtains a guess of $W_{d_j}$. Each weak receiver $i \in K_w$ uses the secret key $K_i$ stored in its cache memory to recover a guess of its intended message $W_{d_i}$. Section VII-B presents the details of the scheme and its analysis.

---

Fig. 2. Superposition codebook with random binning in the satellites.
3) Secure Cache-Aided Piggyback Coding I:

The scheme builds on the nested piggyback coding scheme in [3], which is rendered secure by applying secret keys to the produced XOR-messages and by introducing wiretap binning. During the placement phase, each of these secret keys is stored in the cache memories of the weak receivers that decode the corresponding XOR-message. We outline the scheme for $K_w = 3$ weak receivers and $K_s = 1$ strong receiver.

Divide each message $W_d$ into six submessages

$$W_d = \left\{ W_{d,(1)}^{(A)}, W_{d,(2)}^{(A)}, W_{d,(1)}^{(B)}, W_{d,(2)}^{(B)}, W_{d,(3)}^{(B)} \right\}, \quad d \in \mathcal{D},$$

where the first three are of equal rate and the latter three are of equal rate. Let $K_{1,2,3}, K_{1,2}, K_{2,3}, K_{1,3}$ be independent secret keys generated at the transmitter.

**Placement phase:** Placement is as described in the following table:

| Cache at Rx 1 | Cache at Rx 2 | Cache at Rx 3 |
|---------------|---------------|---------------|
| $\left\{ W_{d,(1)}^{(A)} \right\}_{d=1}^{D}$ | $\left\{ W_{d,(1)}^{(A)} \right\}_{d=1}^{D}$ | $\left\{ W_{d,(3)}^{(A)} \right\}_{d=1}^{D}$ |
| $\left\{ W_{d,(1,2)}^{(B)}, W_{d,(1,3)}^{(B)} \right\}_{d=1}^{D}$ | $\left\{ W_{d,(1,2)}^{(B)}, W_{d,(1,3)}^{(B)} \right\}_{d=1}^{D}$ | $\left\{ W_{d,(1,3)}^{(B)}, W_{d,(2,3)}^{(B)} \right\}_{d=1}^{D}$ |
| $K_{1,2,3}$ | $K_{1,2,3}$ | $K_{1,2,3}$ |
| $K_{1,2,3}$ | $K_{1,2,3}$ | $K_{1,2,3}$ |

**Delivery phase:** Time-sharing is applied over three subphases and Subphase 2 is further divided into 3 periods.

In Subphase 1, the secured message

$$\text{sec}\left( W_{d,(1,2)}^{(B)} \oplus W_{d,(1,3)}^{(B)} \oplus W_{d,(2,3)}^{(B)} ; K_{1,2,3} \right)$$

is sent to all three weak receivers using a standard point-to-point code. With their cache contents, each weak receiver $i$ can decode the submessage of $W_d$ sent in this subphase. Communication is secured when the key $K_{1,2,3}$ is sufficiently long. In Subphase 3, the non-secure message $W_{d,(4)}^{(A)}$ is sent to the strong receiver 4 using a standard wiretap code.

In the first period of Subphase 2, the transmitter uses the secure piggyback codebook in Figure 3 to transmit the secure message

$$W_{d,(1,2)}^{(A)} = \text{sec}\left( W_{d,(1,2)}^{(A)} \oplus W_{d,(1,1)}^{(A)} ; K_{1,2} \right)$$

to Receivers 1 and 2 and the non-secure message $W_{d,(1,2)}^{(B)}$ to Receiver 4. It randomly chooses a codeword in the wiretap bin indicated by $W_{\text{sec},(1,2)}$ and $W_{d,(1,2)}^{(B)}$ and sends the chosen codeword over the channel. Weak receivers 1 and 2 have stored $W_{d,(1,2)}^{(B)}$, in their cache memories and can decode based on a restricted codebook consisting only of the bins in the column indicated by $W_{d,(1,2)}^{(B)}$. Their decoding performance is thus the same as if this message $W_{d,(1,2)}^{(B)}$ had not been sent at all. The strong receiver 4 has no cache memory and decodes both messages based on the entire codebook. Notice that the secured message $W_{\text{sec},(1,2)}$ also acts as random wiretap binning to secure message $W_{d,(1,2)}^{(B)}$ to Receiver 4. If this binning suffices to secure $W_{d,(1,2)}^{(B)}$, then no additional random binning is needed, i.e., the magenta bin in Figure 3 can be chosen of size 1.

Similar secure piggyback codebooks are also used during the second and third periods of Subphase 2 to send messages $\text{sec}\left( W_{d,(1,3)}^{(A)} \oplus W_{d,(1,1)}^{(A)} ; K_{1,3} \right)$ and $W_{d,(1,3)}$ and messages $\text{sec}\left( W_{d,(1,2)}^{(A)} \oplus W_{d,(1,2)}^{(A)} ; K_{2,3} \right)$ and $W_{d,(2,3)}$, respectively.

At the end of the delivery phase, each Receiver $k \in \mathcal{K}$ assembles all the guesses pertaining to its desired message $W_{d,k}$ and (in case of the weak receivers) all the parts of this message stored in its cache memory to form the final guess $W_k$.

**Remark 2.** The secure piggyback codebook used in Subphase 2 is inspired by the non-secure piggyback coding and Tancev coding in [3] and [21], and by the secure coding scheme for BCs with complementary side-information in [22]. In fact, the main difference to the scheme in [22] is that here one of the receivers and the transmitter share a common secret key, which allows to reduce the size of the wiretap bins or even eliminate them completely.

Interestingly, in this construction, the secret key $K_{1,2}, K_{1,3}, K_{2,3}$ stored at the weak receivers allow to “remotely secure” the transmission from the transmitter to the strong receiver 4.
4) Secure Cache-Aided Piggyback Coding II:
This scheme is similar to the scheme in the previous section, but simpler. Divide each message $W_d$ into 2 submessages $W_d = (W_d^{(A)}, W_d^{(B)})$ and let $K_1, \ldots, K_{K_w}$ be independent secret keys.

Placement phase: Placement is as depicted in the following. In particular, each weak receiver $i \in K_w$ caches the secret key $K_i$ and all submessages $W_d^{(B)}$, for $d \in D$.

![Diagram of cache placement](image)

Delivery phase: Transmission is in two subphases. In Subphase 1, the secure piggyback codebook is used to send the secured message tuple $W_{sec,w}^{(A)} := (\sec(W_{d_1}^{(A)}, K_1), \ldots, \sec(W_{d_{K_w}}^{(A)}, K_{K_w}))$ to all weak receivers and the non-secure message tuple $W_s^{(B)} := (W_{d_{K_w+1}}^{(B)}, \ldots, W_{d_K}^{(B)})$ to the strong receivers. The codebook is depicted in Figure 3 where $W_{sec,(1,2)}^{(A)}$ needs to be replaced by $W_{sec,w}^{(A)}$ and $W_{d,(1,2)}^{(B)}$ by $W_s^{(B)}$. The weak receivers can reconstruct $W_s^{(B)}$ from their cache contents, and thus decode their desired message tuple $W_{sec,w}^{(A)}$ based on the single column of the codebook indicated by $W_s^{(B)}$. From this decoded tuple and the secret key $K_i$ stored in its cache memory, each weak receiver $i \in K_w$ can then produce a guess of its desired message part $W_d^{(B)}$. The strong receivers decode both message tuples $W_{sec,w}^{(A)}$ and $W_s^{(B)}$. Strong receiver $j \in K_s$ keeps only its guess of $W_d^{(B)}$ and discards the rest.

Communication in this first subphase is secured because messages $W_{d_1}^{(A)}, \ldots, W_{d_{K_w}}^{(A)}$ are perfectly secured by one-time pads and these one-time pads act as random bin indices to protect the messages $W_{d_{K_w+1}}^{(B)}, \ldots, W_{d_K}^{(B)}$ as in wiretap coding.

In Subphase 2, the message tuple $W_s^{(A)} = (W_{d_{K_w+1}}^{(A)}, \ldots, W_{d_K}^{(A)})$ is sent to all the strong receivers using a point-to-point wiretap code.

The choice of the rates and the lengths of the subphases are explained in Section VII-D, where the scheme is also analyzed.
B. Results on the Secrecy Capacity-Memory Tradeoff

Consider the following $K_w + 4$ rate-memory pairs:

- $R^{(0)} := \frac{\delta_2 - \delta_s}{K_w(\delta_z - \delta_s)} + K_s(\delta_z - \delta_w)^+$
- $M^{(0)} := 0$;

- $R^{(1)} := \frac{(1 - \delta_w)(\delta_z - \delta_s)}{K_s(1 - \delta_w) + K_w(\delta_z - \delta_s)}$
- $M^{(1)} := \frac{(\delta_z - \delta_s) \min \{1 - \delta_2, 1 - \delta_w\}}{K_s(1 - \delta_w) + K_w(\delta_z - \delta_s)}$;

- $R^{(2)} := \min \left\{ \frac{(1 - \delta_w)(1 - \delta_s)}{K_s(1 - \delta_w) + K_w(1 - \delta_s)}, \frac{(1 - \delta_w)(\delta_z - \delta_s)}{K_s(1 - \delta_w) + K_w(\delta_z - \delta_s)} \right\}$
- $M^{(2)} := \frac{\min \{1 - \delta_s, \delta_z - \delta_s\}}{K_w(1 - \delta_w) + K_w(\delta_z - \delta_s)}$;

- For $t \in \{1, \ldots, K_w - 1\}$
  
  \begin{align*}
  R^{(t+2)} & := \frac{(t+1)(1 - \delta_w)(\delta_z - \delta_s)}{K_w(t+1)(1 - \delta_w) + (K_w - t + 1) \min \{\delta_w - \delta_s, \delta_z - \delta_s\}} \\
  M^{(t+2)} & := \frac{D \cdot t(t+1)(1 - \delta_w)(\delta_z - \delta_s)[K_w(t+1)(1 - \delta_w) + (K_w - t + 1) \min \{\delta_w - \delta_s, \delta_z - \delta_s\}] + K_w^2 t(t+1)(1 - \delta_w) + (K_w - t + 1) \min \{\delta_w - \delta_s, \delta_z - \delta_s\}] + \frac{K_w[(K_w - t + 1)(\delta_z - \delta_s)]K_s(t+1)(1 - \delta_w) + (K_w - t + 1) \min \{\delta_w - \delta_s, \delta_z - \delta_s\}] + K_w^2 t(t+1)(1 - \delta_w)^2]}{K_w[(K_w - t + 1)(\delta_z - \delta_s)]K_s(t+1)(1 - \delta_w) + (K_w - t + 1) \min \{\delta_w - \delta_s, \delta_z - \delta_s\}] + K_w^2 t(t+1)(1 - \delta_w)^2} \\
  \end{align*}

- $R^{(K_w+2)} := \frac{\delta_z - \delta_s}{K_s}$
- $M^{(K_w+2)} := \frac{D \cdot K_w(\delta_z - \delta_s)^2 + K_w(\delta_z - \delta_s) \min \{1 - \delta_2, 1 - \delta_w\}}{K_s[K_s \min \{1 - \delta_2, 1 - \delta_w\} + K_w(\delta_z - \delta_s)]}$;

- $R^{(K_w+3)} := \frac{\delta_z - \delta_s}{K_s}$
- $M^{(K_w+3)} := \frac{D \cdot (\delta_z - \delta_s)}{K_s}$.

Theorem 2 (Lower Bound on $C_{\text{sec}}(M_w, M_s = 0)$).

$$C_{\text{sec}}(M_w, M_s = 0) \geq \text{upper hull} \left\{ \left( R^{(\ell)}, M^{(\ell)} \right) : \ell \in \{0, \ldots, K_w + 3\} \right\}.$$  \hspace{1cm} (63)

Proof. It suffices to prove achievability of the $K_w + 4$ rate-memory pairs $\{(R^{(\ell)}, M^{(\ell)}) : \ell = 0, \ldots, K_w + 3\}$. Achievability of the upper convex hull follows by time/memory sharing arguments as in \[1\]. The pair $(R^{(0)}, M^{(0)})$ is achievable by Remark \[1\]. The pair $(R^{(1)}, M^{(1)})$ is achieved by the “wiretap and cached keys” scheme described and analyzed in Sections \[IV-A1\] and \[VII-A\]. The pair $(R^{(2)}, M^{(2)})$ is achieved by the “cache-aided superposition jamming” scheme described and analyzed in Sections \[IV-A2\] and \[VII-B\]. The pairs $(R^{(t+2)}, M^{(t+2)})$, for $t \in \{1, \ldots, K_w - 1\}$, are achieved by the “secure cache-aided piggyback coding I” scheme described and analyzed in Sections \[IV-A3\] and \[VII-C\]. The pair $(R^{(K_w+2)}, M^{(K_w+2)})$ is achieved by the “secure cache-aided piggyback coding II” scheme described and analyzed in Sections \[IV-A4\] and \[VII-D\]. The pair $(R^{(K_w+3)}, M^{(K_w+3)})$ is achieved by storing the entire library in the cache memory of each weak receiver and by applying a standard wiretap BC code \[19\] to send the requested messages to the strong receivers. □
Interestingly, upper and lower bounds in Corollary 1 and Theorem 2 match for small and large $M_w$ irrespective of the number of weak and strong receivers $K_w$ and $K_s$. In the absence of a secrecy constraint, the best upper and lower bounds for small $M_w$ match only when $K_w = 1$, irrespective of the value of $K_s$ [3, 5].

**Corollary 2.** When the cache memory $M_w$ is small:

\[ C_{sec}(M_w, M_s = 0) = R^{(0)} + \frac{K_w(\delta_z - \delta_s)}{K_w(\delta_z - \delta_s) + K_w(\delta_z - \delta_w)^+} M_w, \quad 0 \leq M_w \leq M^{(1)}, \]

where $R^{(0)}$ is defined in (62a) and $M^{(1)}$ is defined in (62d).

Proof: Achievability follows from the two achievable rate-memory pairs $(R^{(0)}, M^{(0)})$ and $(R^{(1)}, M^{(1)})$ in (62a)–(62d) and by time/memory-sharing arguments. The converse follows from upper bound (50b) in Corollary 1 when specialized to $k_w = K_w$. In fact, for $k_w = K_w$ and cache size $M_w \in [0, M^{(1)}]$, the maximizing $\beta$ is:

\[ \beta = \frac{(\delta_z - \delta_s) - K_s M_w}{K_w(\delta_z - \delta_s) + K_w(\delta_z - \delta_w)^+} K_w. \]

This choice of $\beta$ makes the two terms in the minimization (50b) equal.

Notice that when $\delta_z \leq \delta_w$, then (64) specializes to

\[ C_{sec}(M_w, M_s = 0) = M_w. \]

The secrecy capacity thus grows in the same way as the cache size at weak receivers. This is achieved by the scheme we termed cache-aided wiretap coding with secret keys.

Notice that in this case the secrecy capacity-memory tradeoff $C_{sec}(M_w, M_s = 0)$ grows much faster in the cache size $M_w$ than its non-secure counterpart $C(M_w, M_s = 0)$. In fact, by the upper bound in [3], the maximum slope of the standard capacity-memory tradeoff

\[ \gamma := \max_{m \geq 0} \left\{ \frac{dC(M_w, M_s = 0)}{dM_w} \bigg|_{M_w = m} \right\} \]

is at most

\[ \gamma \leq \frac{K_w M_w}{D}. \]

By the above Corollary 2 and the concavity of $C_{sec}(M_w, M_s = 0)$ in $M_w$, the maximum slope of the secrecy capacity-memory tradeoff

\[ \gamma_{sec} := \max_{m \geq 0} \left\{ \frac{dC_{sec}(M_w, M_s = 0)}{dM_w} \bigg|_{M_w = m} \right\} \]

is

\[ \gamma_{sec} = \lim_{m \to 0} \left\{ \frac{dC_{sec}(M_w, M_s = 0)}{dM_w} \bigg|_{M_w = m} \right\} = \frac{K_w(\delta_z - \delta_s)}{K_w(\delta_z - \delta_s) + K_s(\delta_z - \delta_w)^+} M_w. \]

So in contrast to the maximum slope of the standard capacity-memory tradeoff $\gamma$, the maximum slope of the secrecy capacity-memory tradeoff $\gamma_{sec}$ does not deteriorate with the size of the library $D$. The reason for this discrepancy is that in the setup with secrecy constraint an optimal strategy for small cache memories is to exclusively place secret keys in the cache memories. In this case, each bit of the cache content is useful irrespective of the specifically demanded files. In a setup without secrecy constraint, only data is placed in the cache memories. So, at least on an intuitive level, each bit of cache memory is useful only under some of the demands.

We turn to the regime of large cache memories.

**Corollary 3.** When the cache memory $M_w$ is large:

\[ C_{sec}(M_w, M_s = 0) = \frac{\delta_z - \delta_s}{K_s}, \quad M_w \geq M^{(K_w+2)}, \]

where $M^{(K_w+2)}$ is defined in (62a).

The rate-memory pairs (62a)–(62d) are attained by means of joint cache-channel coding where the decoders simultaneously adapt to the cache contents and the channel statistics. To emphasize the strength of the joint coding approach, we characterize the rates that are securely achievable under a separate cache-channel coding approach.
For $t \in \{1, \ldots, K_w - 1\}$, define the following rate-memory pairs:

\[ R_{\text{sep}}^{(t)} := \frac{(t + 1)(1 - \delta_w)(\delta_z - \delta_s)}{K_s(t + 1)(1 - \delta_w) + (K_w - t)(\delta_z - \delta_s)}, \]

\[ M_{\text{sep}}^{(t)} := \frac{D \cdot t(t + 1)(1 - \delta_w)(\delta_z - \delta_s) + (t + 1)(K_w - t)(\delta_z - \delta_s) \min\{1 - \delta_z, 1 - \delta_w\}}{K_w [K_s(t + 1)(1 - \delta_w) + (K_w - t)(\delta_z - \delta_s)]}. \]

**Proposition 1.** Any rate $R > 0$ is achievable by means of separate cache-channel coding, if it satisfies

\[ R < \text{upper hull}\{ (R^{(\ell)}, M^{(\ell)}) : R_{\text{sep}}^{(\ell)}, M_{\text{sep}}^{(\ell)} : \ell \in \{0, 1, 2, K_w + 3\} \text{ and } t \in \{1, \ldots, K_w - 1\} \}. \tag{73} \]

**Proof:** The rate-memory tuples $\{ (R^{(\ell)}, M^{(\ell)}) : \ell = 0, 1, 2, K_w + 3 \}$ in (62a)–(62f) and (62k)–(62l) are achieved by the schemes in Subsections IV-A1 and IV-A2. It can be verified that these schemes apply a separate cache-channel coding architecture. Rate-memory pairs $\{ (R_{\text{sep}}^{(t)}, M_{\text{sep}}^{(t)}) : t = 1, \ldots, K_w - 1 \}$ are achieved by a scheme that communicates to weak and strong receivers in two independent phases: in the first phase it combines the Sengupta secure coded caching scheme [5] with a standard optimal BC code to communicate to the weak receivers, and in the second phase it applies a standard wiretap BC code to communicate to the strong receivers.

C. Numerical Comparisons

In Figure 4, we compare the presented bounds at hand of an example with 5 weak and 15 strong receivers and where the eavesdropper is degraded with respect to all receivers. The figure shows the upper and lower bounds on the secrecy capacity-memory tradeoff $C_{\text{sec}}(M_w, M_s = 0)$ in Corollary 1 and Theorem 2. It also shows the rates achieved by the separate cache-channel coding scheme leading to Proposition 1. Finally, the figure presents the lower bound on the standard capacity-memory tradeoff in [3].

The presented lower bound of Theorem 2 (see the black solid line in Figure 4) is piece-wise linear with the end points of the pieces corresponding to the points in (62). The left-most point (a) corresponds to the capacity in the absence of cache memories. The second and third left-most points (b) and (c) are obtained by storing only secret keys in the cache memories. The right-most point (e) corresponds to the point where the messages can be sent at the same rate as if only strong receivers were present in the system. This performance is trivially achieved by storing all messages in each of the weak receivers’ cache memories and holding the delivery communication only to strong receivers. After this point, the capacity cannot be increased.
Further because strong receivers do not have cache memories. Through coding, the same rate can also be achieved without storing the entire library at each weak receiver, see the second right-most point \((d)\).

For small and large cache memories, our upper and lower bounds are exact. This shows that in the regime of small cache memories, it is optimal to place only secret keys in the weak receivers’ cache memories. In this regime, the slope of \(C_{\text{sec}}(M_w, M_s = 0)\) in \(M_w\) is steep (see Corollary \(\ref{corollary:small_caches}\) and Equation \((70)\)) because the secret keys stored in the cache memories are always helpful, irrespective of the specific demands \(d\). In particular, the slope is not divided by the library size \(D\) as is the case in the traditional caching setup without secrecy constraint.

In the regime of moderate or large cache memories, the proposed placement strategies also store information about the messages in the cache memories. In this regime, the slope \(C_{\text{sec}}\) is smaller and proportional to \(1/D\), because only a fraction of the cache content is effectively helpful for a specific demand \(d\).

Figure 5 shows the bounds for an example where the eavesdropper is stronger than the weak receivers but not the strong receivers:

\[ \delta_s < \delta_z < \delta_w, \]  

(74)

It shows that positive rates can be achieved even if \(\delta_z \leq \delta_w\), because messages sent to weak receivers can be specially secured by means of one-time pads using the secret keys stored in their cache memories.

V. RESULTS WHEN ALL RECEIVERS HAVE CACHE MEMORIES

We turn to the case where all receivers have cache memories, so \(M_w, M_s > 0\). In this case, we do not impose any constraint on the eavesdropper’s channel, so \(\delta_x\) can be larger or smaller than \(\delta_s, \delta_w\).

A. Coding Schemes

We present four coding schemes. The first one only stores secret keys in all the cache memories, the second one stores keys in all cache memories and data at weak receivers, and the last two schemes store keys and data at all the receivers.

1)Cached Keys:

**Placement phase:** Store independent secret keys \(K_1, \ldots, K_K\) in the cache memories of Receivers \(1, \ldots, K\):

\[
\begin{array}{cccc}
\text{Cache at Rx 1} & \text{Cache at Rx 2} & \text{Cache at Rx 3} & \text{Cache at Rx K} \\
K_1 & K_2 & K_3 & K_K \\
\end{array}
\]

**Delivery phase:** Apply a standard (non-secure) broadcast code to send the secured message tuple

\[
W_{\text{sec}} := \left( \text{sec}(W_{d_1}, K_1), \text{sec}(W_{d_2}, K_2), \text{sec}(W_{d_3}, K_3), \ldots, \text{sec}(W_{d_K}, K_K) \right),
\]

(75)

to Receivers \(1, \ldots, K\), respectively. With the secret key \(K_k\) stored in its cache memory, each Receiver \(k \in K\) recovers a guess of its desired message \(W_{d_k}\). See Section VIII-A on how to choose the parameters of the scheme.
2) Secure Cache-Aided Piggyback Coding with Keys at All Receivers:

The difference between this scheme and the secure cache-aided piggyback coding scheme of Sections [V-A3] and [VII-C] is that additional secret keys are placed in the cache memories of weak and strong receivers so that communications in Subphases 2 and 3 can entirely be secured with these keys, i.e., no wiretap binning is required.

We outline the scheme for \( K_w = 3 \) weak receivers and \( K_s = 1 \) strong receiver. For a detailed description and an analysis in the general case, see Section [VIII-C].

Divide each message \( W_d \) into six submessages

\[
W_d = (W_d^{(A)}_{d,1}, W_d^{(A)}_{d,2}, W_d^{(A)}_{d,3}, W_d^{(B)}_{d,1,2}, W_d^{(B)}_{d,1,3}, W_d^{(B)}_{d,2,3}), \quad d \in D,
\]

(76)

where the first three are of equal rate and the latter three are of equal rate.

**Placement phase:** Placement is as described in the following table, where \( K_{1,2,3}, K_{1,2}, K_{2,3}, K_{1,3}, K_{4,1,2}, K_{4,1,3}, K_{4,2,3}, K_{4,4} \) denote independent secret keys.

**Cache at Rx1**

\[
\begin{align*}
\{W_d^{(A)}\}_{d=1}^D & \quad K_{1,2}, K_{1,3}, \\
\{W_d^{(B)}\}_{d,1,2} & \quad K_{1,2,3}, \\
\{W_d^{(B)}\}_{d,1,3} & \quad K_{1,2,3}, \\
\{W_d^{(B)}\}_{d,2,3} & \quad K_{1,2,3}, \\
K_{4,1,2} & \quad K_{4,4}, \\
K_{4,1,3} & \quad K_{4,4}, \\
K_{4,2,3} & \quad K_{4,4}.
\end{align*}
\]

**Cache at Rx2**

\[
\begin{align*}
\{W_d^{(A)}\}_{d,1} & \quad K_{1,2}, K_{1,3}, \\
\{W_d^{(B)}\}_{d,1,2} & \quad K_{1,2,3}, \\
\{W_d^{(B)}\}_{d,1,3} & \quad K_{1,2,3}, \\
\{W_d^{(B)}\}_{d,2,3} & \quad K_{1,2,3}, \\
K_{4,1,2} & \quad K_{4,4}, \\
K_{4,1,3} & \quad K_{4,4}, \\
K_{4,2,3} & \quad K_{4,4}.
\end{align*}
\]

**Cache at Rx3**

\[
\begin{align*}
\{W_d^{(A)}\}_{d,1} & \quad K_{1,2}, K_{1,3}, \\
\{W_d^{(B)}\}_{d,1,3} & \quad K_{1,2,3}, \\
\{W_d^{(B)}\}_{d,2,3} & \quad K_{1,2,3}, \\
K_{4,1,2} & \quad K_{4,4}, \\
K_{4,1,3} & \quad K_{4,4}, \\
K_{4,2,3} & \quad K_{4,4}.
\end{align*}
\]

**Cache at Rx4**

\[
\begin{align*}
K_4 & \quad K_{4,1,2}, \\
K_4 & \quad K_{4,1,3}, \\
K_4 & \quad K_{4,2,3}.
\end{align*}
\]

**Delivery phase:** Time-sharing is applied over three subphases and Subphase 2 is further divided into 3 periods.

Transmission in Subphase 1 is as described in Section [V-A3]. In Subphase 3, the secured message \( \text{sec}(W_{d,4}^{(A)}, K_4) \) is sent to the strong receiver 4 using a standard point-to-point code. This transmission is secure if the key \( K_4 \) is chosen sufficiently long.

In the first period of Subphase 2, the transmitter uses the standard piggyback codebook in Figure 5 to transmit the secure message

\[
W_{sec,1,2}^{(A)} = \text{sec}(W_{d,1,2}^{(A)} \oplus W_{d,1,2}^{(A)}, K_{1,2})
\]

(77)

to Receivers 1 and 2 and the secure message

\[
W_{sec,4}^{(B)} = \text{sec}(W_{d,4,1,2}^{(B)}, K_{1,4})
\]

(78)

to Receiver 4. Receivers 1 and 2 can reconstruct \( W_{sec,1,2}^{(A)} \) from their cache contents, and thus decode message \( W_{sec,1,2}^{(A)} \) based solely on the column of the codebook that corresponds to \( W_{sec,1,2}^{(A)} \). Receiver 4 decodes both messages \( W_{sec,1,2}^{(A)} \) and \( W_{sec,4}^{(B)} \). From the decoded secured messages and the keys stored in their cache memories, Receivers 1, 2, and 4 can recover their desired message parts \( W_{d,1,2}^{(A)} \) and \( W_{d,1,2}^{(B)} \) and \( W_{d,4,1,2}^{(B)} \).

In the same way, using a standard piggyback codebook, the secured messages \( \text{sec}(W_{d,1,3}^{(A)} \oplus W_{d,1,3}^{(A)}, K_{1,3}) \) and \( \text{sec}(W_{d,3,1}^{(A)}, K_{4,1,3}) \) are transmitted in Period 2 to Receivers 1, 3, and 4, and the secured messages \( \text{sec}(W_{d,2,3}^{(A)} \oplus W_{d,2,3}^{(A)}, K_{2,3}) \) and \( \text{sec}(W_{d,4,2,3}^{(B)}, K_{4,2,3}) \) are transmitted in Period 3 to Receivers 2, 3, and 4.

3) Symmetric Secure Piggyback Coding:

Each message is split into two submessages \( W_d = (W_d^{(A)}, W_d^{(B)}) \), and communication is in three subphases. Submessages of \( \{W_d^{(A)}\} \) and corresponding secret keys are placed in weak receivers’ cache memories according to the Sengupta et al. secure coded caching placement algorithm 6. Submessages of \( \{W_d^{(B)}\} \) and corresponding secret keys are placed in strong receivers’ cache memories according to the same placement algorithm. In Subphase 1, the Sengupta et al. delivery scheme for submessages \( \{W_d^{(A)}\} \) is combined with a standard BC code to transmit only to weak receivers and in Subphase 3 it is combined with a standard BC code to transmit only to strong receivers. Transmission in Subphase 2 is divided into into \( K_w \) periods, each dedicated to a pair of weak and strong receivers \( i \in K_w \) and \( j \in K_s \). A standard piggyback codebook is used in each of these periods to send secured messages to the corresponding pair of receivers. The secret keys securing these messages have been pre-placed in the appropriate cache memories.

We now describe the scheme in more detail for the special case \( K_w = 3 \) and \( K_s = 2 \), and for parameters \( t_w = 2 \) and \( t_s = 1 \). The general scheme is described and analyzed in Section [VIII-C].
Divide each $W_d$ into six submessages

$$W_d = \left\{ W^{(A)}_{d,(1,2)}, W^{(A)}_{d,(1,3)}, W^{(A)}_{d,(2,3)}, W^{(B)}_{d,(4)}, W^{(B)}_{d,(5)} \right\}, \quad d \in D,$$

where the first three are of equal rate and the latter two are of equal rate.

**Placing phase:** Generate independent secret keys $K_{(1,2,3)}$, $K_{w,(1,4)}$, $K_{w,(1,5)}$, $K_{w,(2,4)}$, $K_{w,(2,5)}$, $K_{w,(3,4)}$, $K_{w,(3,5)}$, $K_{s,(1,4)}$, $K_{s,(1,5)}$, $K_{s,(2,4)}$, $K_{s,(2,5)}$, $K_{s,(3,4)}$, $K_{s,(3,5)}$, $K_{(4,5)}$.

Placement of information in the cache memories is as indicated in the following table:

| Cache at Rx1 | Cache at Rx2 | Cache at Rx3 |
|--------------|--------------|--------------|
| $\{ W^{(A)}_{d,(1,2)}, W^{(A)}_{d,(1,3)} \}_{d=1}^D$ | $\{ W^{(A)}_{d,(1,2)}, W^{(A)}_{d,(2,3)} \}_{d=1}^D$ | $\{ W^{(A)}_{d,(1,3)}, W^{(A)}_{d,(2,3)} \}_{d=1}^D$ |
| $K_{(1,2,3)}$ | $K_{(1,2,3)}$ | $K_{(1,2,3)}$ |
| $K_{w,(1,4)}$, $K_{w,(1,5)}$ | $K_{w,(2,4)}$, $K_{w,(2,5)}$ | $K_{w,(3,4)}$, $K_{w,(3,5)}$ |
| $K_{s,(1,4)}$, $K_{s,(1,5)}$ | $K_{s,(2,4)}$, $K_{s,(2,5)}$ | $K_{s,(3,4)}$, $K_{s,(3,5)}$ |

| Cache at Rx4 | Cache at Rx5 |
|--------------|--------------|
| $\{ W^{(B)}_{d,(4)} \}_{d=1}^D$ | $\{ W^{(B)}_{d,(5)} \}_{d=1}^D$ |
| $K_{w,(1,4)}$, $K_{w,(2,4)}$, $K_{w,(3,4)}$ | $K_{w,(1,5)}$, $K_{w,(2,5)}$, $K_{w,(3,5)}$ |
| $K_{s,(1,4)}$, $K_{s,(2,4)}$, $K_{s,(3,4)}$ | $K_{s,(1,5)}$, $K_{s,(2,5)}$, $K_{s,(3,5)}$ |
| $K_{(4,5)}$ | $K_{(4,5)}$ |

**Delivery phase:** The delivery phase is divided into three subphases, where Subphase 2 is further divided into 6 periods. Subphase 1 is intended only for weak receivers. The transmitter sends the secured message

$$W^{(A)}_{\text{sec.}(1,2,3)} = \text{sec}(W^{(A)}_{d,(1,2)} \oplus W^{(A)}_{d,(1,3)} \oplus W^{(A)}_{d,(2,3)}, K_{(1,2,3)}$$

using a capacity-achieving code to the weak receivers 1, 2, and 3. With their cache contents, each of these weak receivers can decode its desired submessage.

The first period of Subphase 2 is dedicated to Receivers 1 and 4. The transmitter sends the secured messages

$$W^{(B)}_{\text{sec.}(1,4)} = \text{sec}(W^{(B)}_{d,(1,4)}, K_{w,(1,4)})$$

and

$$W^{(A)}_{\text{sec.}(4,1)} = \text{sec}(W^{(A)}_{d,(1,2)}, K_{s,(1,4)})$$
using a standard piggyback codebook where rows encode \( W_{sec,1,4}^{(B)} \) and columns encode \( W_{sec,4,1}^{(A)} \). (This corresponds to the piggyback codebook in Figure 6 where \( W_{sec,1,2}^{(A)} \) needs to be replaced by \( W_{sec,1,4}^{(B)} \) and \( W_{sec,4,1}^{(B)} \) by \( W_{sec,4,1}^{(A)} \).) Since Receiver 1 can reconstruct \( W_{sec,4,1}^{(A)} \) from its cache content, it decodes \( W_{sec,1,4}^{(B)} \) based on the single column of the piggyback codebook indicated by \( W_{sec,4,1}^{(A)} \). Similarly, since Receiver 4 can reconstruct \( W_{sec,1,4}^{(A)} \) from its cache content, it decodes \( W_{sec,4,1}^{(A)} \) based on the single row corresponding to \( W_{sec,1,4}^{(B)} \). With their decoded secure messages and the secret keys in their cache memories, Receiver 1 can recover \( W_{d1,4}^{(A)} \) and Receiver 4 can recover \( W_{d4,1,2}^{(A)} \).

A similar scheme is used in the subsequent periods to convey the parts \( W_{d1,4}^{(B)}, W_{d2,4}^{(B)}, W_{d4,1}^{(B)}, W_{d4,1}^{(A)}, W_{d5}^{(A)} \) that are not stored in their cache memories to Receivers 1–5. Table I shows the concerned receivers, the conveyed messages and the keys used in each period of Subphase 2.

### Table I

**Messages sent and keys used in the six periods of Subphase 2 for the example with \( K_w = 3 \) weak receivers and \( K_s = 2 \) strong receivers.**

| Receivers | Period 1 | Period 2 | Period 3 | Period 4 | Period 5 | Period 6 |
|-----------|----------|----------|----------|----------|----------|----------|
| Keys      | \( K_w(1,4), K_s(1,4) \) | \( K_w(2,4), K_s(2,4) \) | \( K_w(3,4), K_s(3,4) \) | \( K_w(1,5), K_s(1,5) \) | \( K_w(2,5), K_s(2,5) \) | \( K_w(3,5), K_s(3,5) \) |
| Messages for weak receivers | \( W_{d1,4}^{(B)} \) | \( W_{d2,4}^{(B)} \) | \( W_{d3,4}^{(B)} \) | \( W_{d4,1}^{(B)} \) | \( W_{d5}^{(B)} \) | \( W_{d5}^{(B)} \) |
| Messages for strong receivers | \( W_{d4,1,2}^{(A)} \) | \( W_{d4,2,3}^{(A)} \) | \( W_{d4,1,3}^{(A)} \) | \( W_{d5,1,2}^{(A)} \) | \( W_{d5,2,3}^{(A)} \) | \( W_{d5,1,3}^{(A)} \) |

#### Subphase 3: The transmitter sends

\[
W_{sec,4,5}^{(B)} = \text{sec}(W_{sec,4,5}^{(B)} \oplus W_{sec,4,5}) \tag{83}
\]

using a capacity-achieving code to the strong receivers 4 and 5. With their cache contents, each receiver can decode its desired submessage sent in this subphase.

Choosing all keys sufficiently long ensures that the delivery communication satisfies the secrecy constraint \( (24) \).

#### 4) Secure Generalized Coded Caching:

The scheme is based on the **generalized coded caching** algorithms of \( (20) \), but where the produced zero-padded XORs are secured with independent secret keys and these keys are placed in the cache memories of the receivers that decode the XORs. Choosing the secret keys sufficient long, ensures than the secrecy constraint \( (24) \) is satisfied.

### B. Results on the Secrecy Capacity-Memory Tradeoff

Consider the following \( K + K_w + K_s \) rate-memory tuples. Let \( R^{(0)} = R^{(0)} \) and \( M^{(0)} = M^{(0)} = 0 \).

- Let

\[
\begin{align*}
\tilde{R}_w^{(1)} & := \frac{(1 - \delta_s)(1 - \delta_w)}{K_w(1 - \delta_s) + K_s(1 - \delta_w)}, \\
\tilde{M}_w^{(1)} & := (1 - \delta_s) \min \left\{ 1 - \delta_s, 1 - \delta_w \right\}, \\
\tilde{M}_s^{(1)} & := (1 - \delta_w) \min \left\{ 1 - \delta_s, 1 - \delta_w \right\},
\end{align*}
\]

- For \( t \in \{1, \ldots, K_w - 1\} \), let

\[
\begin{align*}
\tilde{R}_w^{(t+1)} & := \frac{\left( (t + 1)(1 - \delta_w)(1 - \delta_s) + (K_w - t + 1)(\delta_w - \delta_s) \right)}{(K_w - t + 1)(1 - \delta_s) + K_s(1 - \delta_w) + (K_w - t)(\delta_s - \delta_w)} \\
\tilde{M}_w^{(t+1)} & := \frac{D \cdot (t + 1)(1 - \delta_s)(1 - \delta_w) + (K_w - t)(\delta_w - \delta_s) + K_s(t + 1)(1 - \delta_w)}{K_w(1 - \delta_s) + (K_w - t + 1)(\delta_w - \delta_s) + K_s(t + 1)(1 - \delta_w)}
\end{align*}
\]
\[\tilde{S}_s^{(t+1)} := \frac{K_s(t+1)(1-\delta_s)(1-\delta_s)\min\{1-\delta_s, 1-\delta_s\}}{K_s[(K_s-t+1)(1-\delta_s)(1-\delta_s) + (K_s-t)(1-\delta_s) + K_s^2(t+1)(1-\delta_s)^2]}
\]

\[\tilde{R}_K^{(t+1)} := \frac{K_s[t+1][t+1](1-\delta_s)(1-\delta_s)\min\{1-\delta_s, 1-\delta_s\}}{K_s[(K_s-t+1)(1-\delta_s)(1-\delta_s) + (K_s-t)(1-\delta_s) + K_s^2(t+1)(1-\delta_s)^2]}
\]

**Theorem 3 (Lower bound on \(C_s(M_w, M_s)\)).**

\[C_{sec}(M_w, M_s) \geq \text{upper hull} \left\{ \left( \tilde{R}^{(t)}, \tilde{M}_w^{(t)}, \tilde{M}_s^{(t)} \right) : \ell \in \{0, 1, \ldots, K + W + K_sK_s - 1\} \right\}.
\]

**Proof.** By time/memory-sharing arguments, it suffices to prove the achievability of the rate-memory triples \(\{\tilde{R}^{(t)}, \tilde{M}_w^{(t)}, \tilde{M}_s^{(t)}\} : \ell \in \{0, 1, \ldots, K + W + K_sK_s - 1\}\). The triple \(\{\tilde{R}^{(t)}, \tilde{M}_w^{(t)}, \tilde{M}_s^{(t)}\}\) is achieved by the "cached keys" scheme, see Subsections \textbf{V-A1} and \textbf{VIII-A} The triples \(\tilde{R}^{(t)}, \tilde{M}_w^{(t)}, \tilde{M}_s^{(t)}\), for \(\ell \in \{2, \ldots, K_s\}\), are achieved by the "secure piggyback coding scheme with keys at all receivers", see Subsections \textbf{V-A2} and \textbf{VIII-B}. The triples \(\tilde{R}^{(t)}, \tilde{M}_w^{(t)}, \tilde{M}_s^{(t)}\), for \(\ell \in \{K_w + 1, \ldots, K + W + K_sK_s\}\), are achieved by the "symmetric secure piggyback coding scheme", see Subsections \textbf{V-A3}.
Corollary 4. The rate-memory tradeoff \( \left( \tilde{R}^{(1)}, \tilde{M}_{w}^{(1)}, \tilde{M}_{s}^{(1)} \right) \) is optimal, i.e.,
\[
C_{\text{sec}} \left( M_{w} = \tilde{M}_{w}^{(1)}, M_{s} = \tilde{M}_{s}^{(1)} \right) = \tilde{R}^{(1)}.
\]

Proof: Achievability follows from the two achievable rate-memory triples \((\tilde{R}^{(0)}, \tilde{M}_{w}^{(0)} = 0, \tilde{M}_{s}^{(0)})\) and \((\tilde{R}^{(1)}, \tilde{M}_{w}^{(1)}, \tilde{M}_{s}^{(1)})\) in (84a)–(84c) and by time/memory-sharing arguments. The converse follows by specializing upper bound (42a) in Theorem II to \( k_{w} = K_{w} \) and \( k_{s} = K_{s} \). In fact, for \( k_{w} = K_{w} \), \( k_{s} = K_{s} \), and cache sizes \( M_{w} = \tilde{M}_{w}^{(1)} \) and \( M_{s} = \tilde{M}_{s}^{(1)} \), the maximizing \( \beta \) equals
\[
\beta = \frac{K_{w}(1-\delta_{s})}{K_{w}(1-\delta_{s}) + K_{s}(1-\delta_{w})}
\]
when \( \delta_{z} < \delta_{w} \), and it equals \( \beta = 0 \) when \( \delta_{z} \geq \delta_{w} \).

Notice that when \( \delta_{z} \leq \delta_{s} \), then
\[
\tilde{R}^{(1)} = \tilde{M}_{w}^{(1)} = \tilde{M}_{s}^{(1)}.
\]
This rate is achieved by XORing the messages with secret keys stored in the cache memories, and by sending the resulting bits using a traditional non-secure code for the erasure BC.

VI. GLOBAL SECRECY CAPACITY-MEMORY TRADEOFF

In the preceding sections, we considered scenarios with unequal cache sizes at the receivers and showed that in these scenarios joint cache-channel coding schemes can significantly improve over the traditional separation-based schemes with their typical uniform cache assignment. In this section, we emphasize the importance of unequal cache sizes that depend on the receivers’ channel conditions by focusing on the global secrecy capacity-memory tradeoff \( C_{\text{sec,glob}} \), which is the largest secrecy capacity-memory tradeoff that is possible given a total cache budget
\[
K_{w}M_{w} + K_{s}M_{s} \leq M_{\text{tot}}.
\]
We assign the same cache memory size \( M_{w} \) to all weak receivers and the same cache memory size \( M_{s} \) to all strong receivers. Using simple time/memory-sharing arguments, it can be shown that this assumption is without loss in optimality.

So, the main quantity of interest in this section is
\[
C_{\text{sec,glob}}(M_{\text{tot}}) := \max_{\begin{array}{c}
M_{w}, M_{s} \geq 0, \\
K_{w}M_{w} + K_{s}M_{s} \leq M_{\text{tot}}
\end{array}} C_{\text{sec}}(M_{w}, M_{s})
\]

A. Results

Using the achievability results in Theorems II and III combined with an appropriate cache assignment and time/memory-sharing arguments, yields the following lower bound on \( C_{\text{sec,glob}}(M_{\text{tot}}) \).

Corollary 5. (Lower bound on \( C_{\text{sec,glob}}(M_{\text{tot}}) \)) The global secrecy capacity-memory tradeoff \( C_{\text{sec,glob}} \) is lower bounded as
\[
C_{\text{sec,glob}}(M_{\text{tot}}) \geq \text{upper hull} \left\{ \left( R^{(\ell)}, M_{\text{tot}} = K_{w}M^{(\ell)} \right), \left( \tilde{R}^{(\ell')}, M_{\text{tot}} = K_{w}M_{w}^{(\ell')} + K_{s}M_{s}^{(\ell')} \right) : \ell \in \{0, \ldots, K_{w} + 3\} \text{ and } \ell' \in \{1, \ldots, K + K_{w} + K_{w}K_{s} - 1\} \right\}.
\]

Proposition 2. If the eavesdropper is weaker than the strong receivers, i.e.,
\[
\delta_{z} > \delta_{s},
\]
then for small cache sizes:
\[
C_{\text{sec,glob}}(M_{\text{tot}}) = R^{(0)} + \frac{(\delta_{z} - \delta_{s})^{+}}{K_{w}(\delta_{z} - \delta_{s})^{+} + K_{s}(\delta_{z} - \delta_{w})^{+}} M_{\text{tot}}, \quad 0 \leq M_{\text{tot}} \leq K_{w}M_{w}^{(1)}.
\]
If the eavesdropper is at least as strong as the strong receivers, i.e.,
\[
\delta_{z} \leq \delta_{s},
\]
\[
C_{\text{sec,glob}}(M_{\text{tot}}) = R^{(0)} + \frac{\delta_{z} - \delta_{s}^{+}}{K_{w}(\delta_{z} - \delta_{s})^{+} + K_{s}(\delta_{z} - \delta_{w})^{+}} M_{\text{tot}}, \quad 0 \leq M_{\text{tot}} \leq K_{w}M_{w}^{(1)}.
\]
When the total cache budget $M$ (the total cache budget $M$ receivers)

Results under Uniform Cache Assignment

then for small cache sizes:

$$C_{\text{sec, glob}}(M_{\text{tot}}) = \frac{M_{\text{tot}}}{K}, \quad 0 \leq M_{\text{tot}} \leq K \cdot \frac{(1 - \delta_w)(1 - \delta_s)}{K_w(1 - \delta_s) + K_s(1 - \delta_w)}.$$  \hfill (95)

Proof: Achievability of (93) follows from Corollary 2 and by assigning all available cache memory uniformly across weak receivers, so $M_w = \frac{M_{\text{tot}}}{K}$ and $M_s = 0$. The converse to (93) can be proved by specializing Lemma 2 to the set of all users $\mathcal{S} = \mathcal{K}$. For a given choice of the cache assignment $M_w, M_s \geq 0$, Lemma 2 yields (amongst others) that for some $\beta \in [0, 1]$, the secrecy capacity-memory tradeoff is upper bounded as

$$K_w \cdot C_{\text{sec, glob}}(M_{\text{tot}}) \leq \beta(\delta_z - \delta_w)^+ + K_w M_w.$$  \hfill (96)

and

$$K \cdot C_{\text{sec, glob}}(M_{\text{tot}}) \leq \beta(\delta_z - \delta_w)^+ + (1 - \beta)(\delta_z - \delta_s)^+ + M_{\text{tot}}.$$  \hfill (97)

Upper bounding now $K_w M_w$ by $M_{\text{tot}}$ and combining (96) and (97) into a single bound yields:

$$C_{\text{sec, glob}}(M_{\text{tot}}) \leq \max_{\beta \in [0, 1]} \min \left\{ \frac{\beta(\delta_z - \delta_w)^+ + M_{\text{tot}}}{K_w}, \frac{\beta(\delta_z - \delta_w)^+ + (1 - \beta)(\delta_z - \delta_s)^+ + M_{\text{tot}}}{K} \right\}.$$  \hfill (98)

If $\delta_z > \delta_w$, then the maximizing $\beta$ in the above upper bound is as in (65) when $M_w$ is replaced by $M_{\text{tot}}$; otherwise the maximizing $\beta$ equals 0. Plugging these values into (98) establishes the desired upper bound.

Achievability of (95) follows from time/memory-sharing arguments and from the achievability of the rate-memory triple $(\tilde{R}^{(1)}, \tilde{M}_w^{(1)}, \tilde{M}_s^{(1)})$ in (84a)--(84c), which under (94) specializes to the rate-memory triple:

$$\tilde{R}^{(1)} = \tilde{M}_w^{(1)} = \tilde{M}_s^{(1)} = \frac{(1 - \delta_w)(1 - \delta_s)}{K_w(1 - \delta_s) + K_s(1 - \delta_w)}.$$  \hfill (99)

In fact, the rate-memory triples under consideration are achieved by storing an independent secret key at each receiver and securing the messages with these keys by means of one-time pads. This requires a uniform cache assignment across all receivers, i.e., $M_w = M_s = \frac{M_{\text{tot}}}{K}$. The converse to (95) follows from upper bound (97), which under (94) specializes to $C_{\text{sec, glob}}(M_{\text{tot}}) \leq M_{\text{tot}}/K$.

Figure 7 illustrates our choices of the cache contents when $\delta_z > \delta_s$ in the order of increasing total cache memory $M_{\text{tot}}$. When the total cache budget $M_{\text{tot}}$ is small, all of it is assigned to the weak receivers and it is solely used to store secret keys. For a slightly larger cache budget $M_{\text{tot}}$, it is assigned to all receivers and secret keys are stored in the cache memories. When the total cache budget $M_{\text{tot}}$ exceeds the size required to store the keys for securing the entire communication, the additional space is used to store data at weak receivers. Once the cached data renders the weak receivers equally powerful (in terms of their decoding performance) as the strong receivers, data is also stored in strong receivers’ cache memories. When $\delta_z \leq \delta_s$, then our choice is similar, but we start with placing secret keys directly at all the receivers.

B. Results under Uniform Cache Assignment

For comparison, we also propose a lower bound on $C_{\text{sec, glob}}(M_{\text{tot}})$ when the cache memory is uniformly assigned over all receivers, i.e.

$$M_w = M_s = \frac{M_{\text{tot}}}{K}.$$  \hfill (100)

Consider the following $K + 2$ rate-memory pairs:

- $R_{\text{sym}}^{(0)} := \frac{(\delta_z - \delta_s)^+ \cdot (\delta_z - \delta_w)^+}{K_w(\delta_z - \delta_s) + K_s(\delta_z - \delta_w)},$ \hfill (101a)

- $M_{\text{sym}}^{(0)} := 0;$ \hfill (101b)
\[ R^{(1)}_{\text{sym}} := \frac{(1 - \delta_w)(1 - \delta_s)}{K_w(1 - \delta_s) + K_s(1 - \delta_w)}, \quad M^{(1)}_{\text{sym}} := \frac{(1 - \delta_s)(1 - \delta_w)}{K_w(1 - \delta_s) + K_s(1 - \delta_w)}, \]  
(101c, 101d)

For \( t \in \{1, \ldots, K_s - 1\} \)
\[ R^{(t+1)}_{\text{sym}} := \frac{(K^t)(1 - \delta_w)(1 - \delta_s)}{(K_t)(1 - \delta_s) - (K_{t+1})(\delta_w - \delta_s)}, \quad M^{(t+1)}_{\text{sym}} := \frac{D \cdot t(K^t)(1 - \delta_w)(1 - \delta_s)}{K[(K^t)(1 - \delta_s) - (K_{t+1})(\delta_w - \delta_s)]} + \frac{(K - t)(K^t)(1 - \delta_s)(1 - \delta_w)}{K[(K^t)(1 - \delta_s) - (K_{t+1})(\delta_w - \delta_s)]}; \]  
(101e, 101f)

For \( t \in \{K_s, \ldots, K\} \)
\[ R^{(t+1)}_{\text{sym}} := \frac{(t + 1)(1 - \delta_w)}{(K - t)}, \quad M^{(t+1)}_{\text{sym}} := \frac{D \cdot t(t + 1)(1 - \delta_w)}{K(K - t)} + \frac{t + 1}{K} \min \{1 - \delta_s, 1 - \delta_w\}. \]  
(101g, 101h)

**Proposition 3** (Lower Bound on \( C_{\text{sec}}(M_w = M_{\text{sym}}, M_s = M_{\text{sym}}) \)).
\[ C_{\text{sec}}(M_w = M_{\text{sym}}, M_s = M_{\text{sym}}) \geq \text{upper hull} \left\{ \left( R^{(\ell)}_{\text{sym}}, M^{(\ell)}_{\text{sym}} \right) : \ell \in \{0, \ldots, K + 1\} \right\}. \]  
(102)

**Proof.** It suffices to prove the achievability of the \( K + 2 \) rate-memory pairs \( \left( R^{(\ell)}_{\text{sym}}, M^{(\ell)}_{\text{sym}} \right) : \ell = 0, \ldots, K + 1 \}. \) The rate-memory pair \( \left( R^{(0)}_{\text{sym}}, M^{(0)}_{\text{sym}} \right) \) is achievable by Remark 1. The rate-memory pair \( \left( R^{(1)}_{\text{sym}}, M^{(1)}_{\text{sym}} \right) \) is achievable because, by Theorem 3 rate \( R^{(1)} = R^{(1)}_{\text{sym}} \) is achievable with cache size \( M^{(1)}_{\text{sym}} \) at weak receivers and cache size \( M^{(1)}_{\text{sym}} \) at strong receivers, and because \( M^{(1)}_{\text{sym}} = \max \{M^{(1)}_w, M^{(1)}_s\} \). For each \( t \in \{1, \ldots, K\} \), the rate-memory pair \( \left( R^{(t+1)}_{\text{sym}}, M^{(t+1)}_{\text{sym}} \right) \) is achieved by a scheme that combines the Sengupta et al. secure coded caching scheme [6] with a standard BC code. Notice that when \( t = K_s \), then each of the secured XORs produced by the Sengupta et al. scheme is intended for at least one weak receiver, and communication is limited by this weak receiver. Each secured XOR, which is of rate \( \left( \frac{K^t}{t+1} \right)^{-1} R^{(t+1)}_{\text{sym}} \), thus requires slightly more than \( \frac{K^t}{t+1} - \frac{nR_{\text{sym}}}{1 - \delta_w} \) channel uses to be transmitted reliably. When \( t < K_s \), \( \frac{K^t}{t+1} \) of the secured XOR are only sent to strong receivers and can thus be sent reliably by using slightly more than \( \frac{K^t}{t+1} - \frac{nR_{\text{sym}}}{1 - \delta_w} \) channel uses. The remaining \( \frac{K^t}{t+1} - \frac{K^t}{t+1} \) secured XORs are sent to at least one weak receiver, and can thus be sent reliably by using slightly more than \( \frac{K^t}{t+1} - \frac{nR_{\text{sym}}}{1 - \delta_w} \) channel uses. \( \square \)

**C. Numerical Comparison**

Figure 8 plots the lower bound on \( C_{\text{sec, glob}}(M_{\text{tot}}) \) in Corollary 5 (black line) for an example with \( K_w = 20 \) weak receivers and \( K_s = 10 \) strong receivers. The eavesdropper is degraded with respect to all legitimate receivers. For comparison, the figure also shows our lower bound on the secrecy capacity-memory tradeoff for the scenarios where the available cache memory is uniformly assigned over all weak receivers , i.e., \( M_w = M_{\text{tot}}/K_w \) and \( M_s = 0 \), and where it is uniformly assigned over all receivers (blue line), i.e., \( M_w = M_s = M_{\text{tot}}/K \). Finally, the red line depicts the lower bound on the standard (non-secure) global capacity-memory tradeoff obtained from [20] and [5]. One observes that our lower bound on the global secrecy capacity-memory tradeoff is close to the currently best known lower bound on the non-secure capacity-memory tradeoff. Moreover, similarly to [20], for the global secrecy capacity-memory tradeoff it is suboptimal to assign the cache memories uniformly across users (unless the eavesdropper is stronger than all other receivers). In particular, as Proposition 4 shows, for small cache memories all of it should be assigned uniformly over the weak receivers only.

**VII. CODING SCHEMES WHEN ONLY WEAK RECEIVERS HAVE CACHE MEMORIES**

**A. Wiretap and Cachected Keys**

Let Subphase 1 comprise the first \( \beta n \) channel uses and Subphase 2 the last \( (1 - \beta)n \) channel uses, with \( \beta \) chosen as
\[ \beta = \frac{K_w(\delta_z - \delta_s)}{K_w(\delta_z - \delta_s) + K_s(1 - \delta_w)}. \]  
(103)
\[ M_{\text{tot}} = K_w M_w + K_s M_s \]

\[ C_{\text{sec}, \text{glob}}(M_{\text{tot}}) \]

\[ M_{\text{tot}} = K_w M_w + K_s M_s \]

\[ R_{\text{Key}} = \min \left\{ \frac{\beta (1 - \delta_w)}{K_w}, R \right\} \]

\[ R = \frac{(\delta_z - \delta_s)(1 - \delta_w)}{K_w (\delta_z - \delta_s) + K_s (1 - \delta_w)} - \epsilon. \]

\[ M_w = R_{\text{Key}} = \min \left\{ \frac{(\delta_z - \delta_s)(1 - \delta_z)}{K_w (\delta_z - \delta_s) + K_s (1 - \delta_w)}, \frac{(\delta_z - \delta_s)(1 - \delta_w)}{K_w (\delta_z - \delta_s) + K_s (1 - \delta_w)} - \epsilon \right\}. \]

\[ \frac{1}{n} I(W_1, \ldots, W_D; Z^n|C) = \frac{1}{n} I(W_1, \ldots, W_D; Z^n_{1n}|C) + \frac{1}{n} I(W_1, \ldots, W_D; Z^n_{\beta n+1}|C) \]

\[ = \frac{1}{n} I(W_{d_1}, \ldots, W_{d_{K_w}}; Z^n_{1n}|C) + \frac{1}{n} I(W_{d_{K_w}+1}, \ldots, W_{d_k}; Z^n_{\beta n+1}|C) \]

\[ \frac{1}{n} I(W_1, \ldots, W_D; Z^n|C) = \frac{1}{n} I(W_1, \ldots, W_D; Z^n_{1n}|C) + \frac{1}{n} I(W_1, \ldots, W_D; Z^n_{\beta n+1}|C) \]

\[ = \frac{1}{n} I(W_{d_1}, \ldots, W_{d_{K_w}}; Z^n_{1n}|C) + \frac{1}{n} I(W_{d_{K_w}+1}, \ldots, W_{d_k}; Z^n_{\beta n+1}|C) \]

Fig. 8. Lower bounds on \( C_{\text{sec}, \text{glob}}(M_{\text{tot}}) \) for \( \delta_w = 0.7, \delta_s = 0.2, \delta_x = 0.8, D = 50, K_w = 20, \) and \( K_s = 10. \)

Fix a small \( \epsilon > 0. \) Let the secret keys \( K_1, \ldots, K_{K_w} \) be independent of each other and of rate

\[ R_{\text{Key}} = \min \left\{ \frac{\beta (1 - \delta_s)}{K_w}, R \right\}, \]

where the message rate \( R \) is chosen as

\[ R = \frac{(\delta_z - \delta_s)(1 - \delta_w)}{K_w (\delta_z - \delta_s) + K_s (1 - \delta_w)} - \epsilon. \]

The scheme requires a cache size at weak receivers equal to

\[ M_w = R_{\text{Key}} = \min \left\{ \frac{(\delta_z - \delta_s)(1 - \delta_s)}{K_w (\delta_z - \delta_s) + K_s (1 - \delta_w)}, \frac{(\delta_z - \delta_s)(1 - \delta_w)}{K_w (\delta_z - \delta_s) + K_s (1 - \delta_w)} - \epsilon \right\}. \]

We analyze the scheme when averaged over the choice of the random code construction \( C. \) By the joint typicality lemma, the average probability of a decoding error at the weak receivers tends to 0 as \( n \to \infty, \) because

\[ R < \frac{\beta (1 - \delta_w)}{K_w}. \]

The probability of error of the wiretap decoding at the strong receivers tends to 0 as \( n \to \infty, \) because

\[ R < \frac{(1 - \beta)(\delta_z - \delta_s)}{K_s}. \]

Notice that by the choice of \( \beta \) in \( 103, \) the two constraints \( 107 \) and \( 108 \) coincide.

We conclude this analysis by verifying the secrecy constraint averaged over the choice of the codebooks \( C. \) For fixed blocklength \( n: \)

\[ \frac{1}{n} I(W_1, \ldots, W_D; Z^n|C) = \frac{1}{n} I(W_1, \ldots, W_D; Z^n_{1n}|C) + \frac{1}{n} I(W_1, \ldots, W_D; Z^n_{\beta n+1}|C) \]

\[ = \frac{1}{n} I(W_{d_1}, \ldots, W_{d_{K_w}}; Z^n_{1n}|C) + \frac{1}{n} I(W_{d_{K_w}+1}, \ldots, W_{d_k}; Z^n_{\beta n+1}|C) \]

The first term in \( 109 \) tends to 0 as \( n \to \infty \) by \( 104 \) and by Lemma I. The second term tends to 0 as \( n \to \infty \) because of the properties of a wiretap code.

From the analysis we conclude that the average over all choices of the codebooks satisfies the desired properties. There must thus exist at least one good codebook. Letting \( \epsilon \to 0 \) concludes the achievability proof of the rate-memory pair \( R = R^{(1)} \) and \( M_w = M^{(1)} \) in \( 62a \) and \( 62b \).
B. Cached-Aided Superposition-Jamming

Let
\[
\gamma := \left\{ \frac{K_w(\delta_2 - \delta_s)}{K_s(1 - \delta_w) + K_w(\delta_w - \delta_s)}, \frac{K_w(1 - \delta_s)}{K_s(1 - \delta_w) + K_w(1 - \delta_s)} \right\},
\]
and set the rate
\[
R = \frac{\gamma(1 - \delta_w)}{K_w} - \epsilon.
\]
Let further \( p \in [0, 1/2] \) be so that its binary entropy-function \( h_b(p) = 1 - \gamma \).

**Placement phase:** Generate independent random keys \( K_1, \ldots, K_w \) of rate
\[
R_{Key} = \min \left\{ \frac{1 - \delta_2}{K_w}, R \right\}
\]
Store each key \( K_i \) in the cache memory of Receiver \( i, \) for \( i \in K_w \).

**Delivery phase:** Fix a small \( \epsilon > 0 \), and generate a cloud center codebook
\[
C_{center} = \left\{ u^n(1), \ldots, u^n([2^nR]) \right\}
\]
by picking all entries of all codewords i.i.d. according to a Bernoulli-\( 1/2 \) distribution. Choose a wiretap binning rate of
\[
R_{bin} = \{ (1 - \delta_2) - \gamma(1 - \delta_w) \}^+.
\]
Then, superposition on each codeword \( u^n(w) \), for \( w \in \{1, \ldots, [2^nR]\} \), a satellite codebook
\[
C_{sat}(w) = \{ x^n(v, b|w) : v \in \{1, \ldots, [2^nR]\}, b \in \{1, \ldots, [2^{nR_{bin}}]\} \}
\]
by drawing all entries of all codewords i.i.d. according to a Bernoulli-\( p \) distribution.

The transmitter generates the tuples
\[
W_{sec} := \{ \text{sec}(W_{d_1}, K_1), \text{sec}(W_{d_2}, K_2), \text{sec}(W_{d_3}, K_3), \ldots, \text{sec}(W_{d_{K_w}}, K_{K_w}) \},
\]
and
\[
W_{sat} := \{ W_{d_{K_w+1}}, \ldots, W_{d_B} \},
\]
and draws \( B \) uniformly at random over \( \{1, \ldots, [2^{nR_{bin}}]\} \). It then sends the codeword
\[
x^n(W_{sat}, B|W_{sec})
\]
over the channel. Each weak receiver \( i \in K_w \) decodes the message \( W_{sec} \) in the cloud center, and with the key \( K_i \) retrieved from its cache memory, it produces a guess of its desired message \( W_{d_i} \). Each strong receiver \( j \in K_s \) decodes both messages \( W_{sec}, W_{sat} \) as well as the random binning index \( B \) and extracts the guess of its desired message \( W_{d_j} \).

**Analysis:** The scheme requires cache memories at the weak receivers of size
\[
M_w = R_{Key} = \min \left\{ \frac{1 - \delta_2}{K_w}, \frac{(\delta_2 - \delta_s)(1 - \delta_w)}{K_s(1 - \delta_w) + K_w(\delta_w - \delta_s)} - \epsilon \right\}.
\]
We analyze the scheme on average over the random choice of the codebook \( C \). The average probability of decoding error at a weak receiver tends to 0 as \( n \to \infty \), because
\[
K_w R < \gamma(1 - \delta_w).
\]
Similarly, the average probability of decoding error at a strong receiver tends to 0 as \( n \to \infty \), because
\[
R_{bin} + K_s R < (1 - \gamma)(1 - \delta_s).
\]

We turn to the secrecy analysis of the scheme. We have:
\[
\frac{1}{n} I(W_1, \ldots, W_D; Z^n|C) = \frac{1}{n} I(W_{d_1}, \ldots, W_{d_{K_w}}; Z^n|C) + \frac{1}{n} I(W_{d_{K_w+1}}, \ldots, W_{d_B}; Z^n|W_{d_1}, \ldots, W_{d_{K_w}}, C).
\]
The first term on the right-hand side of \((121)\) tends to 0 as \( n \to \infty \) because of Lemma 1, the key-rate \((112)\), and because when averaged over codebooks, the satellite codebooks can simply be considered as additional noise. That the second term in \((121)\) tends to 0 as \( n \to \infty \), can be shown following the steps in \([19]\) or by adapting the steps in \([17, \text{Chapter 22}]\). Putting these observations together proves that \( \frac{1}{n} I(W_1, \ldots, W_D; Z^n|C) \to 0 \) as \( n \to \infty \).

By standard arguments, one can then conclude that there must exist at least one deterministic codebook such that the probability of decoding error vanishes for \( n \to \infty \) and the secrecy constraint \((24)\) constraint holds.

Since \( R \to R^{(2)} \) and \( M_w \to M^{(2)} \) as \( \epsilon \to 0 \), this establishes achievability of the rate-memory pair \( (R^{(2)}, M^{(2)}_w) \) in \([62c]\) and \([62d]\).
C. Secure Cache-Aided Piggyback Coding I

Delivery transmission will be partitioned into three subphases, whose lengths are determined by the parameters:

\[
\beta_1 = \frac{1}{(K_w - t + 1)(1 - \delta_w)} \left(\frac{(K_w - t)(K_w - t + 1)(\delta_z - \delta_w)}{(K_w - t + 1)(\delta_z - \delta_w) + (K_w - t) \min\{\delta_w - \delta_s, \delta_z - \delta_s\}}\right) + K_s^2(t + 1)(1 - \delta_w)^2, \tag{122a}
\]

\[
\beta_2 = \frac{1}{(K_w - t + 1)(1 - \delta_w)} \left(\frac{K_s(K_w - t + 1)(1 - \delta_w) + (K_w - t) \min\{\delta_w - \delta_s, \delta_z - \delta_s\}}{(K_w - t + 1)(\delta_z - \delta_s)}\right) + K_s^2(t + 1)(1 - \delta_w)^2, \tag{122b}
\]

\[
\beta_3 = \frac{1}{(K_w - t + 1)(1 - \delta_w)} \left[\frac{(K_w - t)(\delta_w - \delta_s) + K_s(t + 1)(1 - \delta_w)}{(K_w - t + 1)(1 - \delta_w)^2}\right], \tag{122c}
\]

Notice that \(\beta_1 + \beta_2 + \beta_3 = 1\).

**Message splitting:** Fix a small \(\epsilon > 0\). Divide each message into two independent submessages

\[
W_d = [W_d^{(A)}, W_d^{(B)}], \quad d \in \mathcal{D}, \tag{123}
\]

that are of rates

\[
R^{(A)} = \frac{K_s(t + 1)(1 - \delta_w)\beta_1}{(K_w - t + 1)(1 - \delta_w)K_s(t + 1)(1 - \delta_w) + (K_w - t) \min\{\delta_w - \delta_s, \delta_z - \delta_s\}} + K_s^2(t + 1)(1 - \delta_w)^2 - \epsilon/2, \tag{124}
\]

and

\[
R^{(B)} = \frac{K_s(t + 1)(1 - \delta_w)\beta_2}{(K_w - t + 1)(1 - \delta_w)K_s(t + 1)(1 - \delta_w) + (K_w - t) \min\{\delta_w - \delta_s, \delta_z - \delta_s\}} + K_s^2(t + 1)(1 - \delta_w)^2 - \epsilon/2. \tag{125}
\]

Denote the \(\binom{K_w}{t-1}\) subsets of \(\{1, \ldots, K_w\}\) of size \(t-1\) by \(G_1^{(t-1)}, \ldots, G_{K_w-1}^{(t-1)}\); the \(\binom{K_w}{t}\) subsets of \(\{1, \ldots, K_w\}\) of size \(t\) by \(G_1^{(t)}, \ldots, G_{K_w}^{(t)}\); and the \(\binom{K_w}{t+1}\) subsets of \(\{1, \ldots, K_w\}\) of size \(t+1\) by \(G_1^{(t+1)}, \ldots, G_{K_w+1}^{(t+1)}\).

Divide each message \(W_d^{(A)}\) into \(\binom{K_w}{t-1}\) submessages

\[
W_d^{(A)} = \left\{ W_{d,G_\ell}^{(A)} : \quad \ell \in \left\{1, \ldots, \binom{K_w}{t-1}\right\} \right\}, \tag{126}
\]

of rate

\[
r^{(A)} = R^{(A)} \left(\binom{K_w}{t-1}\right)^{-1}, \tag{127}
\]

and divide each message \(W_d^{(B)}\) into \(\binom{K_w}{t}\) submessages

\[
W_d^{(B)} = \left\{ W_{d,G_\ell}^{(B)} : \quad \ell \in \left\{1, \ldots, \binom{K_w}{t}\right\} \right\}, \tag{128}
\]

of rate

\[
r^{(B)} = R^{(B)} \left(\binom{K_w}{t}\right)^{-1}. \tag{129}
\]

**Key generation:**

- For each \(\ell \in \left\{1, \ldots, \binom{K_w}{t-1}\right\}\), generate an independent random key \(K_{G_{\ell-1}^{(t+1)}}\) of rate

\[
R_{\text{Key,1}} = \left(\binom{K_w}{t+1}\right)^{-1} \cdot \beta_1 \cdot \min\{1 - \delta_z, 1 - \delta_w\}. \tag{130}
\]

- For each \(\ell \in \left\{1, \ldots, \binom{K_w}{t}\right\}\), generate an independent random key \(K_{G_{\ell}^{(t)}}\) of rate

\[
R_{\text{Key,2}} = \left(\binom{K_w}{t}\right)^{-1} \cdot \beta_2 \cdot \min\{1 - \delta_z, 1 - \delta_w\}. \tag{131}
\]

Define the binning rate

\[
R_{\text{bin}} = \left(\binom{K_w}{t}\right)^{-1} \cdot \beta_2 \cdot \min\{0, \delta_w - \delta_z\}, \delta_w - \delta_s\}. \tag{132}
\]
Place**ment phase:** Placement is as indicated in the following table.

| Cache at weak receiver $i$ |
|---------------------------|
| $\left\{ \{ W^{(A)}_{d,G_t^{(t)}(i)} \}_{t \in G_t^{(t-1)}}, \{ W^{(B)}_{d,G_t^{(t)}(i)} \}_{t \in G_t^{(t)}} \right\}_{d=1}^D$ |

$\{ K_G^{(t+1)} \}_{t \in G_t^{(t+1)}}, \{ K_G^{(t)} \}_{t \in G_t^{(t)}}$ |

**Delivery phase:** It is divided into three subphases of lengths $\beta_1 n$, $\beta_2 n$, and $\beta_3 n$.

**Subphase 1:** This subphase is dedicated to the transmission of the parts of $W^{(B)}_{d_1}, \ldots, W^{(B)}_{d_{K_w}}$ that are not stored in the cache memories of the respective weak receivers. For each $\ell \in \{1, \ldots, \kappa_w\}$, the transmitter first calculates the XOR-message

$$\begin{align*}
W^{(B)}_{\text{XOR}, G_t^{(t+1)}}(i) := \bigoplus_{t \in G_t^{(t+1)} \setminus \{i\}} W^{(B)}_{d_t, G_t^{(t+1)} \setminus \{i\}},
\end{align*}$$

and its secured version

$$\begin{align*}
W^{(B)}_{\text{sec}, G_t^{(t+1)}}(i) = \text{sec}(W^{(B)}_{\text{XOR}, G_t^{(t+1)}}(i), K^{(t+1)}_{G_t^{(t+1)}}).
\end{align*}$$

It then sends the secured message tuple

$$\begin{align*}
W^{(B)}_{\text{sec}, w} := (W^{(B)}_{\text{sec}, G_t^{(t+1)}}, \ldots, W^{(B)}_{\text{sec}, G_t^{(t+1)}})_{\{1, \ldots, K_w\}},
\end{align*}$$

using a capacity achieving point-to-point code to all weak receivers. After decoding the message tuple (135), each weak receiver $i$ retrieves the secret key $K^{(t+1)}_{G_t^{(t+1)}}$ from its cache memory, for $\ell \in \{1, \ldots, \kappa_w\}$ so that $i \in G_t^{(t+1)}$, and produces $W^{(B)}_{\text{XOR}, G_t^{(t+1)}}$. Then, it also retrieves the submessages

$$\begin{align*}
\left\{ W^{(B)}_{d_t, G_t^{(t+1)} \setminus \{k\}} \right\}_{k \in G_t^{(t+1)} \setminus \{i\}}
\end{align*}$$

from its cache memory, and guesses the desired submessage as:

$$\begin{align*}
W^{(B)}_{d_t, G_t^{(t+1)} \setminus \{i\}}(i) = \bigoplus_{k \in G_t^{(t+1)} \setminus \{i\}} W^{(B)}_{d_t, G_t^{(t+1)} \setminus \{k\}}.
\end{align*}$$

At the end of Subphase 1, each weak receiver $i \in \kappa_w$ assembles the guesses produced in (137) with the parts of $W^{(B)}_{d_t}$ it has stored in its cache memory to form a guess $\hat{W}^{(B)}_{d_t}$.

**Subphase 2:** This subphase is dedicated to the transmission of the parts of $W^{(A)}_{d_i}$ that are not stored in weak receiver $i$’s cache memory, for $i \in \kappa_w$, and messages $W^{(B)}_{d_j}$, for $j \in \kappa_w$. Time-sharing is applied over $(K_w)$ periods, each of length

$$\begin{align*}
n_2 = \binom{K_w}{t}^{-1} \cdot \beta_2 n.
\end{align*}$$

The periods are labeled $G_1^{(t)}, \ldots, G_{K_w}^{(t)}$. For Period $G_t^{(t)}$, $\ell \in \{1, \ldots, K_w\}$, the transmitter calculates the XOR-message

$$\begin{align*}
W^{(A)}_{\text{XOR}, G_t^{(t)}}(i) := \bigoplus_{i \in G_t^{(t)}} W^{(A)}_{d_t, G_t^{(t)} \setminus \{i\}}
\end{align*}$$

and its secured version

$$\begin{align*}
W^{(A)}_{\text{sec}, G_t^{(t)}} := \text{sec}(W^{(A)}_{\text{XOR}, G_t^{(t)}}, K^{(t)}_{G_t^{(t)}})
\end{align*}$$

It also forms the tuple of non-secured messages

$$\begin{align*}
W^{(B)}_{s,G_t^{(t)}} := (W^{(B)}_{d_{k_{w+1}}, G_t^{(t)}}, \ldots, W^{(B)}_{d_{K_w}, G_t^{(t)}})
\end{align*}$$
which it sends to the strong receivers. To this end, generate for each period $G^{(t)}_t$ a secure piggyback codebook [22], see Figure 3.

$$C_{\text{spg},G^{(t)}_t} = \left\{ x_{G^{(t)}_t}^{n_2} \left( \ell_{\text{row}}; \ell_{\text{col}}; b \right) : \ell_{\text{row}} \in \{ 1, \ldots, [2^{n_{R_{\text{sec}}}}] \}, \ell_{\text{col}} \in \{ 1, \ldots, [2^{n_{R_{\text{bin}}}}] \}, b \in \{ 1, \ldots, [2^{n_{\text{R_{\text{bin}}}}}] \} \right\},$$

(139)

by drawing each entry of each codeword i.i.d. according to a Bernoulli-1/2 distribution. The rates $r^{(A)}$, $r^{(B)}$, and $R_{\text{bin}}$ are defined in (127), (129), and (132).

The transmitter draws an index $B$ uniformly at random over $\{ 1, \ldots, [2^{n_{R_{\text{R_{\text{bin}}}}}}] \}$, and sends the codeword

$$x_{G^{(t)}_t}^{n_2} \left( \text{W}^{(A)}_{\text{sec},G^{(t)}_t}; \text{W}^{(B)}_{s,G^{(t)}_t}; B \right)$$

(140)

over the channel.

We now describe the decoding, starting with the decoding at the weak receivers. For each $i \in K_w$ and each $t \in \{ 1, \ldots, K^{(t)}_w \}$, so that $i \in G^{(t)}_t$, Receiver $i$ decodes message $W^{(A)}_{d_i,G^{(t)}_t} \setminus \{ k \}$ sent in Period $G^{(t)}_t$ by performing the following steps:

1) It retrieves the secret key $K^{(t)}_i$ and the messages $W^{(B)}_{d_{w+1,i},G^{(t)}_t}, \ldots, W^{(B)}_{d_{K_i,G^{(t)}_t}}$ from its cache memory.

2) It extracts the subcodebook

$$\tilde{C}_{\text{spg},G^{(t)}_t} \left( \text{W}^{(B)}_{s,G^{(t)}_t} \right) := \left\{ x_{G^{(t)}_t}^{n_2} \left( \ell_{\text{row}}; \text{W}^{(B)}_{s,G^{(t)}_t}; b \right) : \ell_{\text{row}} \in \{ 1, \ldots, [2^{n_{2r^{(A)}}}] \}, b \in \{ 1, \ldots, [2^{n_{R_{\text{bin}}}}] \} \right\},$$

(141)

3) Based on the reduced codebook $\tilde{C}_{\text{spg},G^{(t)}_t} \left( \text{W}^{(B)}_{s,G^{(t)}_t} \right)$, it decodes the secured message $W^{(A)}_{\text{sec},G^{(t)}_t}$ from its channel outputs in this period $G^{(t)}_t$.

4) It applies the inverse mapping $\text{sec}_{K^{(t)}_i}^{-1}$ to the message decoded in step 3) to obtain the guess $\hat{W}^{(A)}_{\text{XOR},G^{(t)}_t}$.

5) Finally, it produces the guess

$$\hat{W}^{(A)}_{d_i,G^{(t)}_t} = \hat{W}^{(A)}_{\text{XOR},G^{(t)}_t} \bigoplus_{k \in G^{(t)}_t \setminus \{ k \}} W^{(A)}_{d_k,G^{(t)}_t}.$$  

(142)

Strong receivers treat the secure piggyback codebook as a simple wiretap codebook and decode all transmitted messages as well as the bin indices.

At the end of Subphase 2, each weak receiver $i \in K_w$ assembles the parts of submessage $W^{(A)}_{d_i}$ that it decoded or that are stored in its cache memory to form the guess $\hat{W}^{(A)}_{d_i}$. Similarly, each strong receiver $j \in K_s$ assembles the decoded parts of $W^{(B)}_{d_j}$ to form the guess $\hat{W}^{(B)}_{d_j}$.

**Subphase 3:** A wiretap code is used to send the message tuple

$$W^{(A)}_{d_{w+1}}, \ldots, W^{(A)}_{d_K}$$

(143)

to all the strong receivers $K_w + 1, \ldots, K$.

After the last subphase, each Receiver $k \in K$ assembles its guesses produced for the two submessages $W^{(A)}_{d_k}$ and $W^{(B)}_{d_k}$ to the final guess $\hat{W}_k$.

**Analysis:** Analysis is performed averaged over the random choice of the codebooks. We first verify that in each of the three subphases the probability of decoding error tends to 0 as $n \to \infty$. Only weak receivers decode during the first subphase.

Probability of decoding error vanishes asymptotically as $n \to \infty$, because

$$\frac{(K_w) (K_s - 1) (1 - \delta_w)}{1 - \delta_w} = \frac{K_s - 1}{1 - \delta_w} R^{(B)} < \beta_1.$$  

(144)

Only strong receivers decode during the third subphase. Probability of decoding error in Subphase 3 vanishes asymptotically, because

$$\frac{K_s R^{(A)}}{(\delta_s - \delta_a)} < \beta_3,$$

(145)

Probability of decoding error at the weak receivers in Subphase 2 vanishes asymptotically, because

$$\frac{K_{w+1} R^{(A)}}{(1 - \delta_w)} < \beta_2.$$  

(146)
Letting \( \epsilon \) and submessages receivers in Subphase 1 vanishes asymptotically as \( n \to \infty \), the key rate is chosen as

\[
\frac{K_w}{1 - \delta_s} R(A) + K_s R(B) + \frac{K_w}{1 - \delta_s} R_{\text{bin}} < \beta_2.
\]  

(147)

Whenever the decodings in all subphases are successful, all receivers correctly guess their desired messages. Since the decoding error for each subphase vanishes asymptotically, we conclude that also the average overall probability of error vanishes.

We verify the secrecy constraint averaged over the choice of the code construction. For fixed blocklength \( n \):

\[
\frac{1}{n} I(W_1, \ldots, W_D; Z^n|C) = \frac{1}{n} I(W_1^{(B)}, \ldots, W_d^{(B)}; Z^n|C) + \frac{1}{n} I(W_1^{(A)}, W_d^{(B)}; W_d^{(B)}; Z^{(\beta_1+\beta_2)n}|C) + \frac{1}{n} I(W_d^{(B)}; W_d^{(B)}; Z^{(\beta_1+\beta_2)n}|C),
\]

(148)

because of the independence of the communications in the three subphases. By Lemma 1, all of the three summands can be bounded by \( \epsilon/3 \) for sufficiently large \( n \). This holds in particular for the second summand because from the eavesdropper’s point of view, the structure of the piggyback codebook is meaningless and for each message tuple \((W_1^{(A)}; W_1^{(B)}; Z^{(\beta_1+\beta_2)n})\), the codeword to transmit is chosen uniformly at random (depending on \( B \) and \( K_{G_1}^{(n)} \)) over a set of \( 2^{nR_{\text{bin}}} \) i.i.d. random codewords where \( r_s = R_{\text{Key}} + R_{\text{bin}} = \min\{1 - \delta_s, 1 - \delta_s\} \).

Since averaged over the random codebooks, the probability of decoding error and the average mutual information \( \frac{1}{n} I(W_1, \ldots, W_D; Z^n|C) \) both vanish as \( n \to \infty \), there must exist at least one choice of the codebooks so that for this choice \( P^e_{\text{error}} \) and \( \frac{1}{n} I(W_1, \ldots, W_D; Z^n) \) both vanish asymptotically.

Notice that for each \( t \in \{1, \ldots, K_w - 1\} \), the rate of communication satisfies

\[
R = R^{(A)} + R^{(B)} = R^{(t+2)} - \epsilon,
\]

(149)

and weak receivers require a cache memory of

\[
M_w = D \frac{(t-1)}{K_w} R^{(A)} + D \frac{t}{K_w} R^{(B)} + \left(\frac{K_w - 1}{t}\right) R_{\text{Key},1} + \left(\frac{K_w - 1}{t-1}\right) R_{\text{Key},2} = M^{(t+2)} - D \frac{t - 1/2}{K_w} \epsilon.
\]

(150)

Letting \( \epsilon \to 0 \) thus concludes the achievability proof of rate-memory pairs \((R^{(t+2)}, M_w^{(t+2)})\), for \( t = 1, \ldots, K_w - 1 \), as defined in (628–629).

### D. Secure Cache-Aided Piggyback Coding II

Let

\[
\beta = \frac{K_w (\delta_z - \delta_s)}{K_s \min\{1 - \delta_z, 1 - \delta_w\} + K_w (\delta_z - \delta_s)}
\]

(151)

Subphase 1 is of length \( \beta n \) and Subphase 2 of length \((1 - \beta)n\).

Submessages \( \{W_1^{(A)}\} \) are of rate

\[
R^{(A)} = \frac{(\delta_z - \delta_s) \min\{1 - \delta_z, 1 - \delta_w\}}{K_s \min\{1 - \delta_z, 1 - \delta_w\} + K_w (\delta_z - \delta_s)} - \epsilon/2,
\]

(152)

and submessages \( \{W_d^{(B)}\} \) are of rate

\[
R^{(B)} = \frac{K_w (\delta_z - \delta_s)^2}{K_s \min\{1 - \delta_z, 1 - \delta_w\} + K_w (\delta_z - \delta_s)} - \epsilon/2.
\]

(153)

The key rate is chosen as

\[
R_{\text{Key}} = R^{(A)}.
\]

(154)

We analyze the scheme averaged over the random choice of the codebooks \( C \). Probability of decoding error at the weak receivers in Subphase 1 vanishes asymptotically as \( n \to \infty \), because

\[
\frac{K_w R^{(A)}}{1 - \delta_w} < \beta.
\]

(155)

Probability of decoding error at the strong receivers in Subphase 1 vanishes asymptotically, because

\[
\frac{K_w R^{(A)} + K_s R^{(B)}}{1 - \delta_s} < \beta.
\]

(156)
Probability of decoding error in Subphase 2 vanishes asymptotically, because
\[
\frac{K_s R^{(A)}}{(\delta_z - \delta_s)} < (1 - \beta).
\] (157)

As a consequence, also the overall probability of error (averaged over the random choice of the codebooks \(C\)) vanishes as \(n \to \infty\). Following a similar secrecy analysis as in the previous Subsection VII.C, it can be shown that also the averaged mutual information \(\frac{1}{n} I(W_1, \ldots, W_D; Z^n|C)\) vanishes as \(n \to \infty\). This implies that there must exist at least one choice of the codebooks so that for this choice \(P_{\text{e, Worst}} \to 0\) and \(\frac{1}{n} I(W_1, \ldots, W_D; Z^n) \to 0\) as \(n \to \infty\).

Notice now that
\[
R = R^{(A)} + R^{(B)} = \frac{\delta_z - \delta_s}{K_s} - \epsilon.
\] (158)

Moreover, the required cache size at each weak receiver is
\[
M_w = D R^{(B)} + R_{\text{Key}} = M_w^{(K_w+2)} - D \epsilon/2.
\] (159)

Taking \(\epsilon \to 0\), this concludes the proof of achievability of the rate-memory pair \(R^{(K_w+2)}, M_w^{(K_w+2)}\) in (62i) and (62j).

VIII. CODING SCHEMES WHEN ALL RECEIVERS HAVE CACHE MEMORIES

A. Cached Keys

Fix a small \(\epsilon > 0\) and let
\[
\beta = \frac{K_w (1 - \delta_s)}{K_w (1 - \delta_s) + K_s (1 - \delta_w)}.
\] (160)

and the message rate be
\[
R = \frac{\beta (1 - \delta_w)}{K_w} - \epsilon.
\] (161)

Notice that by the choice of the parameter \(\beta\), also
\[
R = \frac{(1 - \beta)(1 - \delta_s)}{K_s} - \epsilon.
\] (162)

Choose key rates
\[
R_{\text{Key}, w} = \frac{\beta}{K_w} \cdot \min \{1 - \delta_z, 1 - \delta_w\},
\] (163)

\[
R_{\text{Key}, s} = \frac{1 - \beta}{K_s} \cdot \min \{1 - \delta_z, 1 - \delta_s\},
\] (164)

and let secret keys \(K_1, \ldots, K_{K_w}\) be of rate \(R_{\text{Key}, w}\) and secret keys \(K_{K_w+1}, \ldots, K_K\) be of rate \(R_{\text{Key}, s}\).

The cache requirement at weak receivers is
\[
M_w = R_{\text{Key}, w} = \frac{(1 - \delta_s)}{K_w (1 - \delta_s) + K_s (1 - \delta_w)} \min \{1 - \delta_z, 1 - \delta_w\}
\] (165)

and the cache requirement at strong receivers is
\[
M_s = R_{\text{Key}, s} = \frac{(1 - \delta_w)}{K_w (1 - \delta_s) + K_s (1 - \delta_w)} \min \{1 - \delta_z, 1 - \delta_s\}
\] (166)

Analysis of the probability of error and of the secrecy constraint (24) are standard and omitted. Letting \(\epsilon \to 0\) proves achievability of the rate-memory pair \((\tilde{R}^{(1)}, \tilde{M}_w^{(1)}, \tilde{M}_s^{(1)})\).
B. Secure Cache-Aided Piggyback Coding with Keys at All Receivers

The scheme follows closely the secure cache-aided piggyback coding I in Subsection VII-C, but for a different choice of rates and time-sharings and with additional secret keys for Subphases 2 and 3 which render wiretap binning useless.

The time-sharing parameters used here are:
\[
\beta_1 = \frac{(K_w - t + 1)(K_w - t)(1 - \delta_s)(\delta_w - \delta_s)}{(K_w - t + 1)(1 - \delta_s)[(K_w - t)(\delta_w - \delta_s) + K_s(t + 1)(1 - \delta_w)] + K_s^2(t + 1)(1 - \delta_w)^2} \tag{167a}
\]
\[
\beta_2 = \frac{K_s(K_w - t + 1)(t + 1)(1 - \delta_w)(1 - \delta_s)}{(K_w - t + 1)(1 - \delta_s)[(K_w - t)(\delta_w - \delta_s) + K_s(t + 1)(1 - \delta_w)] + K_s^2(t + 1)(1 - \delta_w)^2} \tag{167b}
\]
\[
\beta_3 = \frac{K_s^2(t + 1)(1 - \delta_w)^2}{(K_w - t + 1)(1 - \delta_s)[(K_w - t)(\delta_w - \delta_s) + K_s(t + 1)(1 - \delta_w)] + K_s^2(t + 1)(1 - \delta_w)^2} \tag{167c}
\]
and the rates are
\[
R^{(A)} = \frac{K_s(t + 1)(1 - \delta_w)^2(1 - \delta_s)}{(K_w - t + 1)(1 - \delta_s)[(K_w - t)(\delta_w - \delta_s) + K_s(t + 1)(1 - \delta_w)] + K_s^2(t + 1)(1 - \delta_w)^2 - \epsilon/2} \tag{168}
\]
and
\[
R^{(B)} = \frac{(K_w - t + 1)(1 + 1)(1 - \delta_w)(1 - \delta_s)(\delta_w - \delta_s)}{(K_w - t + 1)(1 - \delta_s)[(K_w - t)(\delta_w - \delta_s) + K_s(t + 1)(1 - \delta_w)] + K_s^2(t + 1)(1 - \delta_w)^2 - \epsilon/2}. \tag{169}
\]

The following keys are generated:

- For each \( \ell \in \{1, \ldots, (K_w)\} \), generate an independent secret key \( K_{G^{(t+1)}_{\ell}} \) of rate
  \[
  R_{\text{Key},1} = \left(\frac{K_w}{t + 1}\right)^{-1} \cdot \beta_1 \cdot \min\{1 - \delta_s, 1 - \delta_w\}. \tag{170}
  \]
- For each \( \ell \in \{1, \ldots, (K_w)\} \), generate an independent secret key \( K_{G^{(t)}_{\ell}} \) of rate
  \[
  R_{\text{Key},2} = \left(\frac{K_w}{t}\right)^{-1} \cdot \beta_2 \cdot \min\{1 - \delta_s, 1 - \delta_w\}. \tag{171}
  \]
and \( K_s \) independent secret keys \( K_{K_w+1,G^{(t)}_{\ell}}, \ldots, K_{K_s,G^{(t)}_{\ell}} \) of rate
\[
R_{\text{Key},3} = \left(\frac{K_w}{t}\right)^{-1} \cdot \frac{\beta_3}{K_s} \cdot \min\{\max\{0, \delta_w - \delta_s\}, \delta_w - \delta_s\}. \tag{172}
\]
- For \( j \in K_s \), generate an independent secret key \( K_j \) of rate
  \[
  R_{\text{Key},4} = \frac{\beta_3}{K_s} \cdot \min\{1 - \delta_s, 1 - \delta_s\}. \tag{173}
  \]

**Placement phase:** For each weak receiver \( i \in K_w \), cache
\[
V_i = \left\{ W^{(A)}_{d,G^{(t-1)}_{\ell}} : d \in D \text{ and } i \in G^{(t-1)}_{\ell} \right\} \cup \left\{ W^{(B)}_{d,G^{(t)}_{\ell}} : d \in D \text{ and } i \in G^{(t)}_{\ell} \right\} \cup \left\{ K_{G^{(t+1)}_{\ell}} : i \in G^{(t+1)}_{\ell} \right\} \nonumber \cup \left\{ K_{j,G^{(t)}_{\ell}} : i \in G^{(t)}_{\ell} \text{ and } j \in K_s \right\}. \tag{174}
\]
For each strong receiver \( j \in K_s \), cache
\[
V_j = K_j \cup \left\{ K_{j,G^{(t)}_{\ell}} : \ell \in \{1, \ldots, (K_w)\} \right\}. \tag{175}
\]

**Delivery phase:** Is divided into three subphases of lengths \( n_1 = \beta_1 n, n_2 = \beta_2 n, \) and \( n_3 = \beta_3 n \), where \( \beta_1, \beta_2, \) and \( \beta_3 \) are defined in (167).

Subphase 1: As described in Subsection VII-C.

Subphase 2: Similar to Subsection VII-C but with extra keys. As in Subsection VII-C, this subphase is split into \( (K_w) \) equally-long periods that we label by all \( t \)-user subsets of \( K_w \), i.e., \( G^{(t)}_{\ell}, \ldots, G^{(t)}_{(K_w)_{t}} \). For the transmission in Period \( G^{(t)}_{\ell} \), for \( \ell \in \{1, \ldots, (K_w)\} \), a standard piggyback codebook
\[
C_{\text{pp},G^{(t)}_{\ell}} = \left\{ x_{G^{(t)}_{\ell}}^{e_{\text{row}}(A)}(\ell_{\text{row}}; \ell_{\text{col}}) : \ell_{\text{row}} \in \{1, \ldots, 2^{n(\ell_{\text{row}})}\}, \ell_{\text{col}} \in \{1, \ldots, 2^{n(\ell_{\text{col}})}\} \right\}. \tag{176}
\]
is generated by drawing all entries i.i.d. Bernoulli-1/2. The codebooks are revealed to the transmitter and all receivers, and the rates $r^{(A)}$ and $r^{(B)}$ are chosen as

$$r^{(A)} = R^{(A)} \left( \frac{K_w}{t-1} \right),$$

$$r^{(B)} = R^{(B)} \left( \frac{K_w}{t} \right).$$

At the beginning of Period $G^{(t)}_t$, the transmitter computes

$$W^{(A)}_{sec,w,G^{(t)}_t} = sec( \bigoplus_{i \in G^{(t)}_t} W^{(A)}_{d_i,G^{(t)}_t \setminus \{i\}, K^{(t)}_{G^{(t)}_t}}).$$

and

$$W^{(B)}_{sec,s,G^{(t)}_t} := \left( sec(W^{(B)}_{d_{w+1},G^{(t)}_t}, K_{K_{w+1},G^{(t)}_t}), \ldots, sec(W^{(B)}_{d_k,G^{(t)}_t}, K_{K_{G^{(t)}_t}}) \right),$$

and sends the codeword

$$x^{n_2}_{G^{(t)}_t} W^{(A)}_{sec,w,G^{(t)}_t}, W^{(B)}_{sec,s,G^{(t)}_t}$$

over the channel. Decoding of Period $G^{(t)}_t$ is performed as follows. All weak receivers $i \in G^{(t)}_t$ compute the message tuple to the strong receivers $W^{(B)}_{sec,s,G^{(t)}_t}$ and perform their decoding steps as described in Subsection VII-C. Strong receivers decode both secured message tuples transmitted in this period. Any given strong receiver $j \in K_s$ can then recover its desired message

$$W^{(B)}_{d_j,G^{(t)}_t}$$

using the secret key $K_{j,G^{(t)}_t}$ stored in its cache memory.

At the end of the subphase, each weak receiver $i \in K_w$ assembles the parts of submessage $W^{(A)}_{d_i}$ that it decoded or it has stored in its cache memory, and forms the guess $\hat{W}^{(A)}_{d_i}$. Similarly, each strong receiver $j \in K_s$ assembles the decoded parts and forms $\hat{W}^{(B)}_{d_j}$. 

**Subphase 3:** A capacity-achieving code is used to send the secured message tuple

$$sec(W^{(A)}_{d_{Kw+1}}, K_{K_{w+1}}), \ldots, sec(W^{(A)}_{d_k}, K_K)$$

to the strong receivers $K_{w+1}, \ldots, K$. Each strong receiver $j \in K_s$ obtains its desired guess $\hat{W}^{(A)}_{d_j}$ with the help of the secret key $K_j$ stored in its cache memory.

At the end of the entire delivery phase, each Receiver $k \in C$ assembles its guesses of $W^{(A)}_{d_k}$ and $W^{(B)}_{d_k}$ to produce the final guess $W_k$.

**Analysis:** The scheme is analyzed by averaging over the random code constructions $C$. We first verify that in each of the three subphases the average probability of decoding error tends to 0 as $n \to \infty$. Only weak receivers decode during the first subphase. Probability of decoding error in Subphase 1 vanishes asymptotically as $n \to \infty$, because

$$\frac{(K_w-1)(K_w)}{(1-\delta_w)} R^{(B)} = \frac{K_w t R^{(B)}}{(1-\delta_w)} < \beta_1.$$  

Only strong receivers decode during the third subphase. Probability of decoding error in Subphase 3 vanishes asymptotically, because

$$\frac{K_j R^{(A)}}{(1-\delta_s)} < \beta_3.$$  

In Subphase 2, probability of decoding error at weak receivers vanishes asymptotically, because

$$\frac{K_{w-t+1} R^{(A)}}{(1-\delta_w)} < \beta_2.$$  

Probability of decoding error at strong receivers in Subphase 2 vanishes asymptotically, because

$$\frac{K_{w-t+1} R^{(A)} + K_s R^{(B)}}{(1-\delta_s)} < \beta_2.$$
Whenever the decodings in all subphases are successful, all receivers guess their desired messages correctly. As a consequence, also the average of the overall probability of error vanishes as \( n \to \infty \).

We analyze the secrecy constraint. For fixed blocklength \( n \):

\[
\frac{1}{n} I(W_1, \ldots, W_D; Z^n | C) = \frac{1}{n} I(W^{(B)}_{d_1}, \ldots, W^{(B)}_{d_{\alpha_1}}; Z^{(\beta_1+\beta_3)n} | C) + \frac{1}{n} I(W^{(A)}_{d_{\alpha_1+1}}, W^{(B)}_{d_{\alpha_1+1}}, \ldots, W^{(B)}_{d_{\alpha_2+1}}; Z^{(\beta_1+\beta_3)n+1} | C) + \frac{1}{n} I(W^{(A)}_{d_{\alpha_2+1}}, \ldots, W^{(A)}_{d_{\alpha_3}}; Z^{(\beta_1+\beta_3)n+1} | C),
\]

because of the independence of the communications in the three subphases. The sizes of the secret keys have been chosen so that the codewords to be sent in each of the three subphases are chosen uniformly at random over a subset of the random codebooks that are equal to the minimum between \((1 - \delta_z)\) and the rates of communication. By Lemma \( \text{[1]} \) this proves that

\[
\frac{1}{n} I(W_1, \ldots, W_D; Z^n | C) \to 0 \text{ as } n \to \infty.
\]

We can conclude that there must exist at least one choice of the codebooks so that for this choice both \( P^{\text{Worst}} \to 0 \) and \( \frac{1}{n} I(W_1, \ldots, W_D; Z^n) \) vanish asymptotically.

For each choice of the parameter \( t \in \{1, \ldots, K_w - 1\} \):

\[
R = R^{(A)} + R^{(B)} = \bar{R}^{(t+1)} - \epsilon.
\]

Moreover, each weak receiver requires a cache size of

\[
M_w = \frac{D[R^{(A)} + (t-1)R^{(B)}]}{K_w} + \left( K_w - 1 \right) R_{\text{Key},1} + \left( K_w - 1 \right) R_{\text{Key},2} + \left( K_w - 1 \right) R_{\text{Key},3} = M^{(t+1)}_w - \frac{D(t-1)/2}{K_w} \epsilon,
\]

and each strong receiver a cache size of

\[
M_s = R_{\text{Key},4} + \left( K_w \right) R_{\text{Key},3} = \bar{M}^{(t+1)}_s.
\]

Taking \( \epsilon \to 0 \) thus proves achievability of the rate-memory triples \((\bar{R}^{(t+1)}, \bar{M}^{(t+1)}_w, \bar{M}^{(t+1)}_s)\), for \( t \in \{1, \ldots, K_w - 1\} \), in \( \text{[84]} - \text{[85]} \).

### C. Symmetric Secure Cache-Aided Piggyback Coding

Fix \( \epsilon > 0 \) and define the time-sharing parameters

\[
\beta_1 := \frac{K_w(K_w - t_w)(t_s + 1)(1 - \delta_s)^2}{K_w(K_w - t_w)(t_s + 1)(1 - \delta_s)^2 + K_s(t_w + 1)(1 - \delta_w)\left([K_s - t_s](1 - \delta_w) + K_w(t_s + 1)(1 - \delta_s)\right)},
\]

\[
\beta_2 := \frac{K_w(K_w - t_w)(t_s + 1)(1 - \delta_s)^2}{K_w(K_w - t_w)(t_s + 1)(1 - \delta_s)^2 + K_s(t_w + 1)(1 - \delta_w)\left([K_s - t_s](1 - \delta_w) + K_w(t_s + 1)(1 - \delta_s)\right)},
\]

\[
\beta_3 := \frac{K_s(K_s - t_s)(t_w + 1)(1 - \delta_w)^2}{K_s(K_s - t_s)(t_w + 1)(1 - \delta_w)^2 + K_s(t_w + 1)(1 - \delta_w)\left([K_s - t_s](1 - \delta_w) + K_w(t_s + 1)(1 - \delta_s)\right)}.
\]

Notice that \( \beta_1 + \beta_2 + \beta_3 = 1 \).

Choose two positive integers \( t_w \in \{1, \ldots, K_w\} \) and \( t_s \in \{1, \ldots, K_s\} \).

**Message splitting:** Divide each message into two submessages,

\[
W_d = [W^{(A)}_d, W^{(B)}_d], \quad d \in \mathcal{D},
\]

so that the submessages are of rates

\[
R^{(A)}_d = \frac{K_w(t_w + 1)(t_s + 1)(1 - \delta_w)(1 - \delta_s)^2}{K_w(K_w - t_w)(t_s + 1)(1 - \delta_s)^2 + K_s(t_w + 1)(1 - \delta_w)\left([K_s - t_s](1 - \delta_w) + K_w(t_s + 1)(1 - \delta_s)\right)} - \epsilon/2
\]

and

\[
R^{(B)}_d = \frac{K_s(t_w + 1)(t_s + 1)(1 - \delta_w)^2(1 - \delta_s)}{K_w(K_w - t_w)(t_s + 1)(1 - \delta_s)^2 + K_s(t_w + 1)(1 - \delta_w)\left([K_s - t_s](1 - \delta_w) + K_w(t_s + 1)(1 - \delta_s)\right)} - \epsilon/2.
\]
Denote the $\binom{K_w}{t_w}$ subsets of $\{1, \ldots, K_w\}$ of size $t_w$ by $G_{1}^{(t_w)}, \ldots, G_{K_w}^{(t_w)}$ and the $\binom{K_s}{t_s}$ subsets of $\{1, \ldots, K_s\}$ of size $t_s$ by $G_{1}^{(t_s)}, \ldots, G_{K_s}^{(t_s)}$. Divide every message $W_{d}^{(A)}$ into $\binom{K_w}{t_w}$ submessages and every message $W_{d}^{(B)}$ into $\binom{K_s}{t_s}$ submessages:

$$
W_{d}^{(A)} = \left\{ W_{d,G_{i}^{(t_w)}}^{(A)} : \ell \in \left\{ 1, \ldots, \binom{K_w}{t_w} \right\} \right\},
$$

$$
W_{d}^{(B)} = \left\{ W_{d,G_{i}^{(t_s)}}^{(B)} : \ell \in \left\{ 1, \ldots, \binom{K_s}{t_s} \right\} \right\}.
$$

**Key generation:**

- For each $\ell \in \left\{ 1, \ldots, \binom{K_w}{t_w+1} \right\}$, generate an independent random key $K_{G_{i}^{(t_w+1)}}$ of rate

$$
R_{\text{Key},1} = \left( \frac{K_w}{t_w + 1} \right)^{-1} \cdot \beta_1 \min \left\{ 1 - \delta_z, 1 - \delta_w \right\}.
$$

- For each $\ell \in \left\{ 1, \ldots, \binom{K_s}{t_s+1} \right\}$, generate an independent random key $K_{G_{i}^{(t_s+1)}}$ of rate

$$
R_{\text{Key},2} = \left( \frac{K_s}{t_s + 1} \right)^{-1} \cdot \beta_3 \min \left\{ 1 - \delta_z, 1 - \delta_s \right\}.
$$

- For each $i \in K_w$ and $j \in K_s$, generate an independent random key $K_{w,i,j}$ of rate

$$
R_{\text{Key},3} = \frac{\beta_2}{K_wK_s} \min \left\{ 1 - \delta_z, 1 - \delta_w \right\},
$$

and an independent random key $K_{s,i,j}$ of rate

$$
R_{\text{Key},4} = \frac{\beta_2}{K_wK_s} \min \left\{ (\delta_w - \delta_z)^+, 1 - \delta_s \right\}.
$$

**Placement phase:** Place the cache contents as shown in the following table.

| Cache at weak receiver $i$ | Cache at strong receiver $j$ |
|---------------------------|-----------------------------|
| $\left\{ W_{d,G_{i}^{(t_w)}}^{(A)} \right\}_{d=1}^{D}$ | $\left\{ W_{d,G_{j}^{(t_s)}}^{(B)} \right\}_{d=1}^{D}$ |
| $\left\{ K_{G_{i}^{(t_w+1)}} \right\}_{i \in G_{i}^{(t_w+1)}}$ | $\left\{ K_{G_{j}^{(t_s+1)}} \right\}_{j \in G_{j}^{(t_s+1)}}$ |
| $K_{w,i,K_w+1}, \ldots, K_{w,i,K}$ | $K_{w,j}, K_{w,i,K}$ |
| $K_{s,i,K_s+1}, \ldots, K_{s,i,K}$ | $K_{s,j}, K_{s,i,K}$ |

**Delivery phase:** The delivery phase is divided into three subphases of lengths $\beta_1 n$, $\beta_2 n$ and $\beta_3 n$.

**Subphase 1:** This phase conveys to each weak receiver $i \in K_w$, the parts of $W_{d}^{(A)}$ that are not stored in its cache memory. Time-sharing is applied over $\binom{K_w}{t_w+1}$ equally-long periods of length $n_1 = \beta_1 n \left( \frac{K_w}{t_w + 1} \right)^{-1}$. Label the periods $G_{1}^{(t_1+1)}, \ldots, G_{K_w}^{(t_1+1)}$.

In Period $G_{i}^{(t_1+1)}$, for $\ell \in \left\{ 1, \ldots, \binom{K_w}{t_w+1} \right\}$, the secured XOR-message

$$
\text{sec} \left( \bigoplus_{i \in G_{i}^{(t_w+1)}} W_{d,G_{i}^{(t_w+1)}}^{(A)} \cdot K_{G_{i}^{(t_w+1)}} \right)
$$

is sent to the subset of receivers $G_{i}^{(t_w+1)}$. Each receiver $i \in G_{i}^{(t_w+1)}$ retrieves the content

$$
K_{G_{i}^{(t_w+1)}} \text{ and } \left\{ W_{d,G_{i}^{(t_w+1)}}^{(A)} \right\}_{k \in G_{i}^{(t_w+1)}}
$$

from its cache memory. It then decodes the secured message in (197), and with the retrieved cache content it recovers the desired message $W_{d,G_{i}^{(t_w+1)}}^{(A)}$. 

$$
\text{sec} \left( \bigoplus_{i \in G_{i}^{(t_w+1)}} W_{d,G_{i}^{(t_w+1)}}^{(A)} \cdot K_{G_{i}^{(t_w+1)}} \right)
$$

33
Subphase 2: Submessages \( W_{d_1}^{(B)}, \ldots, W_{d_K}^{(B)} \) are sent to weak receivers \( 1, \ldots, K_w \) and submessages \( W_{d_{w+1}}^{(A)}, \ldots, W_{d_K}^{(A)} \) to strong receivers \( K_w + 1, \ldots, K \).

Time-sharing is applied over \( K_w \cdot K_s \) periods, each of length \( n_2 = \frac{\theta_{n_2}}{K_w K_s} \). The periods are labeled \( \{i, j\} \), for \( i \in K_w \) and \( j \in K_s \). Divide each submessage \( W_d^{(B)} \) into \( K_s \) parts

\[
W_d^{(B)} = \left( W_{d_{K_s i + 1}}^{(B)}, \ldots, W_{d_{K_s K}}^{(B)} \right)
\]

so that each part is of equal rate \( r^{(B)} = R^{(B)}/K_s \) and for all \( j \in K_s \) and \( d \in D \), part \( W_{d,j}^{(B)} \) is stored in strong receiver \( j \)'s cache memory. Similarly, divide each submessage \( W_d^{(A)} \) into \( K_w \) parts

\[
W_d^{(A)} = \left( W_{d_{K_s i}, \ldots, W_{d_{K_s K}}}^{(A)} \right)
\]

of equal rate \( r^{(A)} = R^{(A)}/K_w \) so that for each \( i \in K_w \) and \( d \in D \), part \( W_{d,i}^{(A)} \) is stored in weak receiver \( i \)'s cache memory.

We describe the encoding and decoding operations in a period \( \{i, j\} \), for \( i \in K_w \) and \( j \in K_s \). In this period, the transmitter sends the codeword

\[
x_{n_2}^{i,j} \left( \sec(W_{d_{i,j}}, K_{w,(i,j)}); \sec(W_{d_{i,s}}, K_{s,(i,j)}) \right)
\]

over the channel. At the end of the period, Receiver \( i \) first retrieves the cache content

\[
K_{s,(i,j)}; W_{d_{i,s}},
\]

and forms the subcodebook

\[
C^{\text{row}}_{i,j} \left( \sec(W_{d_{i,j}}, K_{w,(i,j)}); \sec(W_{d_{i,s}}, K_{s,(i,j)}) \right) = \left\{ x_{n_2}^{i,j}; \sec(W_{d_{i,j}}, K_{w,(i,j)}); x_{\ell_{\text{row}}} ; \sec(W_{d_{i,s}}, K_{s,(i,j)}) : \ell_{\text{row}} \in \{1, \ldots, 2^{nr^{(B)}}\} \right\}.
\]

Based on this subcodebook, it then decodes the secured message \( \sec(W_{d_{i,j}}, K_{w,(i,j)}) \), and recovers its desired message \( W_{d_{i,j}}^{(B)} \) with the secret key \( K_{w,(i,j)} \) stored in its cache memory. Receiver \( j \) proceeds analogously, except that it retrieves the cache content

\[
K_{w,(i,j)}; W_{d_{i,j}},
\]

and forms the subcodebook

\[
C^{\text{col}}_{i,j} \left( \sec(W_{d_{i,j}}, K_{w,(i,j)}) \right) = \left\{ x_{n_2}^{i,j}; \sec(W_{d_{i,j}}, K_{w,(i,j)}); x_{\ell_{\text{col}}} ; \col \in \{1, \ldots, 2^{nr^{(B)}}\} \right\}.
\]

It then decodes the secured message \( \sec(W_{d_{i,j}}, K_{s,(i,j)}) \), and recovers \( W_{d_{i,j}}^{(A)} \) using the secret key \( K_{s,(i,j)} \) from its cache memory.

Subphase 3: This subphase conveys to each strong receiver \( j \in K_s \), the parts of submessage \( W_{d_{i,j}}^{(B)} \) that are not stored in its cache memory. Encoding/decoding operations are obtained from the encoding/decoding operations for Subphase 1 if in the latter the subscript \( w \) is replaced by the subscript \( s \) and the superscript \( (A) \) is replaced by the superscript \( (B) \).

Analysis: We analyze the average (over the random choice of the codebooks) probability of decoding error and the average leakage \( \frac{1}{n} I(W_1, \ldots, W_D; Z^n) \).

We start by showing that the probability of decoding error vanishes in each of the three subphases. Only weak receivers perform decoding operations in the first subphase. Probability of error in this subphase thus tends to 0 as \( n \to \infty \), because

\[
\frac{K_w - t_w}{t_w + 1} R^{(A)} < \beta_1
\]

In the second subphase, both weak and strong receivers perform decoding operations. The probability of decoding error at weak receivers tends to 0 as \( n \to \infty \), because

\[
\frac{K_w R^{(B)}}{1 - \delta_w} < \beta_2
\]

The probability of decoding error at strong receivers tends to 0 as \( n \to \infty \), because

\[
\frac{K_s R^{(A)}}{1 - \delta_s} < \beta_2.
\]

(Notice that by our choice of the subrates \( R^{(A)} \) and \( R^{(B)} \), the two decoding constraints of Subphase 2, \( \beta_2 \) and \( \beta_2 \) are equally strong.) Only strong receivers perform decoding operations in the third subphase. The probability of error of these decoding operations tends to 0 as \( n \to \infty \), because

\[
\frac{K_s - t_s}{t_s + 1} R^{(B)} < \beta_3
\]

34
Since all receivers correctly recover their demanded messages when all decoding operations tend to 0, when averaged over the random code construction, the total probability of error tends to 0 as \( n \to \infty \).

Communication is secured because the secret keys have been chosen sufficiently long. In fact, following the arguments given in the previous Subsection VIII-B, it can be shown that the average leakage term \( \frac{1}{n} I(W_1, \ldots, W_D; Z^n | C) \) tends to 0 as \( n \to \infty \). By standard arguments, it can then be concluded that there must exist a choice of the codebooks so that for this choice the probability of error \( p_e^{\text{Worst}} \) and the leakage \( \frac{1}{n} I(W_1, \ldots, W_D; Z^n) \) both vanish asymptotically as \( n \to \infty \).

The presented scheme requires weak receivers to have a cache of size

\[
M_w = \frac{D t_w}{K_w} R(A) + \frac{(t_w + 1) \beta_1 \min \{1 - \delta_z, 1 - \delta_w\}}{K_w} + \frac{\beta_2 \min \{1 - \delta_z, 2 - \delta_w - \delta_s\}}{K_w}
\]

and strong receivers a cache of size

\[
M_s = \frac{D t_s}{K_s} R(B) + \frac{(t_s + 1) \beta_3 \min \{1 - \delta_z, 1 - \delta_s\}}{K_s} + \frac{\beta_2 \min \{1 - \delta_z, 2 - \delta_w - \delta_s\}}{K_s}
\]

Thus, letting \( \epsilon \to 0 \) establishes achievability of the desired rate-memory triples in (84g)–(84i):

\[
\left( \tilde{R}^{(W)}(K_w + t_w | K_s + t_s), \tilde{M}^{(W)}(K_w + t_w | K_s + t_s), \tilde{M}^{(S)}(K_w + t_w | K_s + t_s) \right).
\]

IX. SUMMARY

We have studied secrecy of cache-aided wiretap erasure BCs with \( K_w \) weak receivers, \( K_s \) strong receivers and one eavesdropper. We have provided a general upper bound on the secrecy capacity-memory tradeoff for the case when receivers have arbitrary erasure probabilities and arbitrary cache sizes. We have also proposed lower bounds on the secrecy capacity-memory tradeoff for different cache sizes. For some cache arrangements, e.g., for zero cache sizes at strong receivers \( M_s = 0 \), our upper and lower bounds coincide for small cache sizes. For \( M_s = 0 \), they also match for large cache sizes. These bounds show that the secrecy constraint can induce a significant loss in capacity compared to the standard non-secure system, especially when \( M_s = 0 \). They also exhibit that in a secure system, the caching gain with small cache memories is much more important than its non-secure counterpart. This is due to the fact that secret keys can be stored in the caches, which are more useful than cached data. For larger cache sizes, data has to be stored as well and the caching gains of the secure system are similar to the gains in a standard system. We also present a lower bound on the capacity of a scenario where the cache assignment across receivers can be optimized subject to a total cache budget \( M_{\text{tot}} \). The lower bound is exact for small cache budgets \( M_{\text{tot}} \).

APPENDIX A

PROOF OF LEMMA 2

For each blocklength \( n \), we fix caching, encoding and decoding functions as in (16), (20) and (22) so that both the probability of worst-case error and the secrecy leakage satisfy:

\[
p_e^{\text{Worst}} \xrightarrow{n \to \infty} 0 \quad \text{and} \quad \frac{1}{n} I(W_1, \ldots, W_D; Z^n) \xrightarrow{n \to \infty} 0.
\]

We only prove the lemma for the set \( S = \{1, \ldots, k\} \). For other sets \( S \subseteq \{1, \ldots, K\} \) the proof is similar.

By Fano’s inequality and because conditioning can only reduce entropy, there exists a sequence of real numbers \( \{\epsilon_n\}_{n=1}^{\infty} \) with

\[
\frac{\epsilon_n}{n} \xrightarrow{n \to \infty} 0,
\]

such that

\[
\begin{align*}
H(W_{d_1} | Y_1^n, V_1) & \leq \frac{\epsilon_n}{2K}, \\
H(W_{d_2} | Y_2^n, V_1, V_2, W_{d_1}) & \leq \frac{\epsilon_n}{2K}, \\
& \vdots \\
H(W_{d_k} | Y_k^n, V_1, \ldots, V_k, W_{d_1}, \ldots, W_{d_{k-1}}) & \leq \frac{\epsilon_n}{2K}.
\end{align*}
\]
Thus,

\[ nR = H(W_{d_1}) \]
\[ = H(W_{d_1}|Z^n) + I(W_{d_1}; Z^n) \]
\[ \leq H(W_{d_1}|Z^n) + \frac{\epsilon_n}{2} \]
\[ \leq I(W_{d_1}; Y^n_1, V_1) - I(W_{d_1}; Z^n) + H(W_{d_1}|Y^n_1, V_1) + \frac{\epsilon_n}{2} \]
\[ \leq I(W_{d_1}; Y^n_1, V_1) - I(W_{d_1}; Z^n) + \epsilon_n \]
\[ \leq I(W_{d_1}; Y^n_1|V_1) - I(W_{d_1}; Z^n|V_1) + I(W_{d_1}; V_1|Z^n) + \epsilon_n \]

\[
\begin{align*}
(a) \quad & \sum_{i=1}^{n} \left[ I(W_{d_1}; Y_{1,i}|V_1, Y_{i}^{i-1}) - I(W_{d_1}; Z_i|V_1, Z_{i+1}^n) \right] + nM_1 + \epsilon_n \\
(b) \quad & \sum_{i=1}^{n} \left[ I(W_{d_1}; Y_{1,i}|V_1, Y_{i}^{i-1}) - I(W_{d_1}; Z_i|V_1, Z_{i+1}^n) \right] + nM_1 + \epsilon_n \\
\end{align*}
\]

\[
\begin{align*}
&= \sum_{i=1}^{n} \left[ I(W_{d_1}, Z_{i+1}^n; Y_{1,i}|V_1, Y_{i}^{i-1}) - I(W_{d_1}, Y_{i}^{i-1}; Z_i|V_1, Z_{i+1}^n) \right] + nM_1 + \epsilon_n \\
&= \sum_{i=1}^{n} \left[ I(W_{d_1}, Z_{i+1}^n; Y_{1,i}|V_1, Y_{i}^{i-1}) - I(W_{d_1}, Y_{i}^{i-1}; Z_i|V_1, Z_{i+1}^n) \right] + nM_1 + \epsilon_n \\
&- \sum_{i=1}^{n} \left[ I(Z_{i+1}^n; Y_{i}, Y_{i}^{i-1}, V_1) - I(Y_{i}^{i-1}; Z_i|V_1) \right] + nM_1 + \epsilon_n \\
&= \sum_{i=1}^{n} \left[ I(W_{d_1}; Y_{1,i}|V_1, Y_{i}^{i-1}, Z_{i+1}^n) - I(W_{d_1}; Z_i|V_1, Y_{i}^{i-1}, Z_{i+1}^n) \right] + nM_1 + \epsilon_n \\
&\leq \sum_{i=1}^{n} \left[ I(W_{d_1}; Y_{1,i}|V_1, Y_{i}^{i-1}, Z_{i+1}^n) - I(W_{d_1}; Z_i|V_1, Y_{i}^{i-1}, Z_{i+1}^n) \right]^+ + nM_1 + \epsilon_n \\
&+ \sum_{i=1}^{n} \left[ I(W_{d_1}, Y_{1,i}|V_1, Y_{i}^{i-1}, Z_{i+1}^n) - I(W_{d_1}; Z_i|V_1, Y_{i}^{i-1}, Z_{i+1}^n) \right]^+ \\
&\leq \sum_{i=1}^{n} \left[ I(W_{d_1}; V_1, Y_{1,i}^{i-1}, Z_{i+1}^n; Y_{i}, Z_i) - I(W_{d_1}; V_1, Y_{1,i}^{i-1}, Z_{i+1}^n; Z_i) \right]^+ + nM_1 + \epsilon_n \\
&+ \sum_{i=1}^{n} \left[ I(Y_{i}^{i-1}; Y_{1,i}|W_{d_1}, V_1, Y_{i}^{i-1}, Z_{i+1}^n) - I(Y_{i}^{i-1}; Z_i|W_{d_1}, V_1, Y_{i}^{i-1}, Z_{i+1}^n) \right]^+ + nM_1 + \epsilon_n \\
&= \sum_{i=1}^{n} \left[ I(W_{d_1}; V_1, Y_{1,i}^{i-1}, Z_{i+1}^n; Y_{i}, Z_i) - I(W_{d_1}; V_1, Y_{1,i}^{i-1}, Y_{i}^{i-1}, Z_{i+1}^n; Z_i) \right]^+ + nM_1 + \epsilon_n \\
&\geq \sum_{i=1}^{n} \left[ I(W_{d_1}; V_1, Y_{1,i}^{i-1}, Y_{i}^{i-1}, Z_{i+1}^n; Y_{i}, Z_i) - I(W_{d_1}; V_1, Y_{1,i}^{i-1}, Y_{i}^{i-1}, Z_{i+1}^n; Z_i) \right]^+ + nM_1 + \epsilon_n \\
&\geq \sum_{i=1}^{n} \left[ I(W_{d_1}; V_1, Y_{1,i}^{i-1}, Y_{i}^{i-1}, Z_{i+1}^n; Y_{i}, Z_i) - I(W_{d_1}; V_1, Y_{1,i}^{i-1}, Y_{i}^{i-1}, Z_{i+1}^n; Z_i) \right]^+ + nM_1 + \epsilon_n \\
&\geq \sum_{i=1}^{n} \left[ I(W_{d_1}; V_1, Y_{1,i}^{i-1}, Y_{i}^{i-1}, Z_{i+1}^n; Y_{i}, Z_i) - I(W_{d_1}; V_1, Y_{1,i}^{i-1}, Y_{i}^{i-1}, Z_{i+1}^n; Z_i) \right]^+ + nM_1 + \epsilon_n,
\end{align*}
\]

where (a) holds because \( I(W_{d_1}; V_1|Z^n) \) is limited by the entropy of \( V_1 \) which cannot exceed \( nM_1 \); (b) and (c) follow by the chain rule of mutual information and by applying Csiszar’s sum-identity \[17\] pp. 25; (d) holds because for all values of \( x \) we have: \( x \leq x^+ \) and \( 0 \leq x^+ \); (e) and (g) hold because if the eavesdropper is degraded with respect to Receiver 1, then all \([\cdot]^+ \) terms are positive and if Receiver 1 is degraded with respect to the eavesdropper then all these terms are zero; (f) holds because \( 0 \leq x^+ \) for all values of \( x \) and (g) holds because Receiver 1 is degraded with respect to Receiver 2 and thus the following Markov chain holds:

\[ (V_1, W_{d_1}, Z_{i+1}^n, Y_{1,i}, Z_i) \rightarrow Y_{i}^{i-1} \rightarrow Y_{1}^{i-1} \].

Let \( Q \) be a random variable uniform over \( \{1, \ldots, n\} \) and independent of all the previously defined random variables. We define
Then, we prove that for each chain rule of mutual information.

\[
U_1 := \left( W_{d_1}, V_1, Y_2^{Q-1}, Z_{Q+1}^{n} \right),
\]

\[
Y_1 := Y_{i,q},
\]

\[
Z := Z_Q.
\]

Dividing by \( n \), we can now rewrite the above inequality as

\[
R \leq \frac{1}{n} \Pr \{ Q = q \} \left[ I( W_{d_1}, V_1, Y_2^{Q-1}, Z_{Q+1}^{n}; Y_{i,q} | Q = q ) - I( W_{d_1}, V_1, Y_2^{Q-1}, Z_{Q+1}^{n}; Z_Q | Q = q ) \right]^+ + M_1 + \frac{\epsilon_n}{n}.
\]

We now derive a similar bound as before, but involving Receivers \( 1, \ldots, k \). Consider

\[
kR \leq \frac{1}{n} H( W_{d_1}, \ldots, W_{d_k} ) = \frac{1}{n} H( W_{d_1}, \ldots, W_{d_k} | Z^n ) + \frac{1}{n} I( W_{d_1}, \ldots, W_{d_k}; Z^n ) \leq \frac{1}{n} H( W_{d_1}, \ldots, W_{d_k}; Z^n ) + \frac{\epsilon_n}{n},
\]

\[
\leq \frac{1}{n} \left[ H( W_{d_1} ) + H( W_{d_2} | W_{d_1} ) + \ldots + H( W_{d_k} | W_{d_{k-1}}, \ldots, W_{d_1} ) - I( W_{d_1}, \ldots, W_{d_k}; Z^n ) \right] + \frac{\epsilon_n}{2n},
\]

\[
\leq \frac{1}{n} \left[ I( W_{d_1}; Y_2^{Q-1}, V_1 ) + I( W_{d_2}; Y_2^{Q-1}, V_1, V_2 | W_{d_1} ) + \ldots + I( W_{d_k}; Y_2^{Q-1}, V_1, \ldots, V_k | W_{d_1}, \ldots, W_{d_{k-1}} ) - I( W_{d_1}, \ldots, W_{d_k}; Z^n ) \right] + \frac{\epsilon_n}{n},
\]

\[
= \frac{1}{n} \left[ I( W_{d_1}; Y_2^{Q-1}, V_1 | V_2 ) - I( W_{d_1}; Z^n | V_2 ) + I( W_{d_1}; V_1 | Z^n ) \right] + \frac{1}{n} \sum_{\ell=2}^{k} \left[ I( W_{d_{\ell-1}}; Y_{2}^{Q-1}, V_{\ell}, W_{d_{\ell-1}}; W_{d_{\ell}}, \ldots, W_{d_{k-1}} ) - I( W_{d_{\ell-1}}; Z^n | V_{\ell}, W_{d_{\ell}}, \ldots, W_{d_{k-1}} ) \right] + \frac{\epsilon_n}{n},
\]

where (a) follows from the chain rule of mutual information; (b) follows from Fano’s inequality; and (c) follows from the chain rule of mutual information.

In a similar way to (17), we can prove that

\[
\frac{1}{n} \left[ I( W_{d_1}; Y_2^{Q-1}, V_1 | V_2 ) - I( W_{d_1}; Z^n | V_2 ) \right] \leq \left[ I( U_1; Y_1 | Q ) - I( U_1; Z | Q ) \right]^+.
\]

Then, we prove that for each \( \ell \in \{ 2, \ldots, k \} \), the following set of inequalities holds:

\[
I( W_{d_1}; Y_2^{Q-1}, V_1, \ldots, V_\ell, W_{d_{\ell}}, \ldots, W_{d_{k-1}} ) - I( W_{d_1}; Z^n | V_1, \ldots, V_\ell, W_{d_{\ell}}, \ldots, W_{d_{k-1}} )
\]

\[
\leq \frac{1}{n} \sum_{i=1}^{n} \left[ I( W_{d_{i}}; Y_{\ell,2}^{Q-1}, V_{i}, \ldots, V_\ell, W_{d_{i}}; W_{d_{i-1}}, Y_{\ell,2}^{i-1}, Z_{i+1}^{n} ) - I( W_{d_{i}}; Z_{i} | V_{i}, \ldots, V_\ell, W_{d_{i}}; W_{d_{i-1}}, Y_{\ell,2}^{i-1}, Z_{i+1}^{n} ) \right]
\]

\[
\leq \frac{1}{n} \sum_{i=1}^{n} \left[ I( W_{d_{i}}; Y_{\ell,2}^{Q-1}, V_{i}, \ldots, V_\ell, W_{d_{i}}; W_{d_{i-1}}, Y_{2}^{i-1}, \ldots, Y_{\ell-1}^{i-1}, Z_{i+1}^{n} ) - I( W_{d_{i}}; Z_{i} | V_{i}, \ldots, V_\ell, W_{d_{i}}; W_{d_{i-1}}, Y_{2}^{i-1}, \ldots, Y_{\ell-1}^{i-1}, Z_{i+1}^{n} ) \right]
\]

\[
\leq \frac{1}{n} \sum_{i=1}^{n} \left[ I( W_{d_{i}}; Z_{i} | V_{i}, \ldots, V_\ell, W_{d_{i}}; W_{d_{i-1}}, Y_{2}^{i-1}, \ldots, Y_{\ell-1}^{i-1}, Z_{i+1}^{n} ) \right] + \frac{\epsilon_n}{n}.
\]
Finally, we bound the following sum:

\[
\sum_{i=1}^{n} [I(V_i; Y_{\ell}; V_1, \ldots, V_{\ell-1}, W_{d_{\ell-1}}, Y_2^{i-1}, \ldots, Y_1^{i-1}, Z_{i+1}^n) \\
- I(V_i; Z_i | V_1, \ldots, V_{\ell-1}, W_{d_{\ell-1}}, Y_2^{i-1}, \ldots, Y_1^{i-1}, Z_{i+1}^n)]^+
\]

\[
\leq \sum_{i=1}^{n} [I(W_{d_{\ell}}, V_i; Y_{\ell}; V_1, \ldots, V_{\ell-1}, W_{d_{\ell-1}}, Y_2^{i-1}, \ldots, Y_1^{i-1}, Z_{i+1}^n) \\
- I(W_{d_{\ell}}, V_i; Z_i | V_1, \ldots, V_{\ell-1}, W_{d_{\ell-1}}, Y_2^{i-1}, \ldots, Y_1^{i-1}, Z_{i+1}^n)]^+
\]

\[
+ \sum_{i=1}^{n} [I(Y_{\ell+1}^{i-1}; Y_{\ell}; V_1, \ldots, V_{\ell-1}, W_{d_{\ell}}, Y_2^{i-1}, \ldots, Y_1^{i-1}, Z_{i+1}^n) \\
- I(Y_{\ell+1}^{i-1}; Z_i | V_1, \ldots, V_{\ell}, W_{d_{\ell}}) Y_2^{i-1}, \ldots, Y_1^{i-1}, Z_{i+1}^n)]^+
\]

\[
= \sum_{i=1}^{n} [I(W_{d_{\ell}}, V_i; Y_{\ell}^{i-1}, V_{\ell}; V_1, \ldots, V_{\ell-1}, W_{d_{\ell-1}}, Y_2^{i-1}, \ldots, Y_1^{i-1}, Z_{i+1}^n) \\
- I(W_{d_{\ell}}, V_i; Y_{\ell}^{i-1}, Z_i | V_1, \ldots, V_{\ell-1}, W_{d_{\ell-1}}, Y_2^{i-1}, \ldots, Y_1^{i-1}, Z_{i+1}^n)]^+,
\]  

(220)

where (a) follows from the chain rule of mutual information and by applying Csiszar’s sum-identity; (b) because Receivers 1, \ldots, \ell - 1 are degraded with respect to Receiver \ell, and so the following Markov chain holds:

\[
(W_{d_{\ell}}, Y_{\ell+1}, V_1, \ldots, V_{\ell}, W_{d_{\ell-1}}, Z_{i+1}^n) \rightarrow Y_\ell^{i-1} \rightarrow (Y_1^{i-1}, \ldots, Y_{\ell-1}^n);
\]  

(221)

(c) holds because for all values of x we have: \( x \leq x^+ \) and \( 0 \leq x^+ \); (d) holds because if the eavesdropper is degraded with respect to Receiver \ell, then all \([\cdot]^+\) terms are positive and if Receiver \ell is degraded with respect to the eavesdropper than all these terms are zero.

We define for each \( k \in \{2, \ldots, K\} \) the random variables

\[
Y_k := Y_{k; Q} \\
U_k := (W_{d_k}, V_k, Y_{k+1}^{Q-1}, U_{k-1}).
\]

(222)

(223)

Dividing by \( n \), we can rewrite constraint (220) as

\[
\frac{1}{n} [I(W_i; Y_\ell^n | V_1, \ldots, V_{\ell}, W_{d_{\ell-1}}, \ldots, W_{d_{\ell-1}}) - I(W_i; Z^n | V_1, \ldots, V_{\ell}, W_{d_{\ell-1}}, \ldots, W_{d_{\ell-1}})]^+
\]

\[
\leq \sum_{\ell=1}^{k} [I(U_{\ell}; Y_{\ell}|U_{\ell-1}, Q) - I(U_{\ell}; Z|U_{\ell-1}, Q)]^+.
\]

(224)

Finally, we bound the following sum:

\[
I(W_{d_1}; V_1 | Z^n) + \sum_{\ell=2}^{k} I(W_{d_1}; V_1, \ldots, V_{\ell}|W_{d_1}, \ldots, W_{d_{\ell-1}}, Z^n)
\]

\[
\leq I(W_{d_1}; V_1, \ldots, V_k | Z^n) + \sum_{\ell=2}^{k} I(W_{d_{\ell}}; V_1, \ldots, V_k|W_{d_1}, \ldots, W_{d_{\ell-1}}, Z^n)
\]

\[
= I(W_{d_1}, \ldots, W_{d_k}; V_1, \ldots, V_k | Z^n)
\]

\[
\leq n \sum_{\ell=1}^{k} M_\ell.
\]

(225)

Finally, we bound the following sum:

\[
kR \leq \sum_{\ell=1}^{k} [I(U_{\ell}; Y_{\ell}|U_{\ell-1}, Q) - I(U_{\ell}; Z|U_{\ell-1}, Q)]^+ + \sum_{\ell=1}^{k} M_\ell + \epsilon_n/n,
\]

(226)

where \( U_0 \) is a constant.

Letting \( n \to \infty \), from constraints (217) and (226), we conclude that Lemma 2 holds.
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] R. Timo and M. Wigger, “Joint cache-channel coding over erasure broadcast channels,” *Proc. of IEEE Intern. Symp. on Wireless Comm. Systems (ISWCS)*, Bruxelles, Belgium, Aug. 2015, pp. 201–205.

[3] S. Saeedi Bidokhti, M. Wigger, and R. Timo, “Noisy broadcast networks with receiver caching,” *ArXiv:1605.02317v1*, May 2016.

[4] A. S. Cacciauputo, M. Caleffi, M. J. J. Llorca, and A. M. Talino, “Speeding up future video distribution via channel-aware caching-aided coded multicast,” *IEEE JSAC in Comm.*, vol. 34, no. 8, pp. 2207–2218, Aug. 2016.

[5] M. M. Amiri and D. Giinduz, “Cache-aided content delivery over erasure broadcast channels,” *ArXiv:1702.05454*, Feb. 2017.

[6] 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.

[7] V. Ravindrakumar, P. Panda, N. Karamchandani, and V. Prabhakaran, “Fundamental limits of secretive coded caching,” *Proc. of IEEE Intern. Symp. on Inf. Theory (ISIT)*, Barcelona, Spain, Jul. 2016, pp. 425–429.

[8] H. H. Suthan C. I. Chugh, and P. K. Krishnan, “An improved secretive coded caching scheme exploiting common demands,” *ArXiv:1705.08902*, May 2017.

[9] A. A. Zewail and A. Yener, “Coded caching for resolvable networks with security requirements,” *Proc. of IEEE Conference on Communications and Network Security (CNS)*, Philadelphia, PA USA, Oct. 2016, pp. 621–625.

[10] Z. H. Awan and A. S. Cacciapuoti, M. Caleffi, M. J. J. Llorca, and A. M. Talino, “Speeding up future video distribution via channel-aware caching-aided coded multicast,” *IEEE JSAC in Comm.*, vol. 34, no. 8, pp. 2207–2218, Aug. 2016.

[11] M. Kiskan, H. R. Sadjadpoury, “A secure approach for caching contents in wireless ad hoc networks,” *ArXiv:1709.00112*, Sep. 2017.

[12] L. Xiang, D. W. Kwan Ng, R. Schober, and V. Wong, “Cache-enabled physical layer security for video streaming in backhaul-limited cellular networks,” *ArXiv:1711.02412*, Nov. 2017.

[13] F. Engelmann and P. Elia, “A content-delivery protocol, exploiting the privacy benefits of coded caching,” *Proc. of 15th International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks (WiOpt)*, Paris, France, May 2017.

[14] S. Kamel, M. Sarkiss and M. Wigger, “Secure joint cache-channel coding over erasure broadcast channels,” *Proc. of IEEE Wireless Communications and Networking Conf. (WCNC)*, San Francisco, CA, Mar. 2017.

[15] S. Kamel, M. Sarkiss, and M. Wigger, “Achieving joint secrecy with cache-channel coding over erasure broadcast channels,” *Proc. of IEEE International Conference on Communications (ICC)*, Paris, France, May 2017.

[16] A. El Gamal and Y. H. Kim, Network Information Theory, 2011, Cambridge Univ. Press.

[17] C. E. Shannon, “Communication theory of secrecy systems,” *Bell system technical journal*, vol. 28, no. 4, pp. 656–715, 1949.

[18] E. Ekrem and S. Ulukus, “Multi-receiver wiretap channel with public and confidential messages,” *IEEE Trans. Inf. Theory*, vol. 59, no. 4, pp. 2165–2177, Apr. 2013.

[19] S. Saeedi Bidokhti, M. Wigger and A. Yener, “Benefits of cache assignment on degraded broadcast channels,” *ArXiv:1702.08044*, Feb. 2017.

[20] E. Tuncel, “Slepian-Wolf coding over broadcast channels,” *IEEE Trans. Inf. Theory*, vol. 52, no. 4, pp. 1469–1482, Apr. 2006.

[21] A. Mansour, R. Schaefer, and H. Boche, “On the capacity of broadcast channels with degraded message sets and message cognition under different secrecy constraints.” *ArXiv:1501.04490*, Jan. 2015.