Achieving Joint Secrecy with Cache-Channel Coding over Erasure Broadcast Channels

Sarah Kamel[1,2], Mireille Sarkiss[1] and Michèle Wigger[2]

[1] CEA, LIST, Communicating Systems Laboratory, BC 173, 91191 Gif-sur-Yvette, France, mireille.sarkiss@cea.fr
[2] Télécom ParisTech, 46 Rue Barrault, 75013, Paris, France, {sarah.kamel, michele.wigger}@telecom-paristech.fr

***Abstract*—We derive upper and lower bounds on the secure capacity-memory tradeoff of the K-user $(K \geq 2)$ wiretap erasure broadcast channel where K_w receivers are weak and have cache memories of equal size, and K_s receivers are strong and have no cache. The bounds coincide for small and large cache memories. The lower bound also exhibits that cache memories provide larger gains under a secrecy constraint than without such a constraint. Moreover, we show for the two-user scenario that in the regime of small cache memories, the capacity-memory tradeoff is larger when only the weaker receiver has cache memory than when this cache memory is split equally among the two receivers. The lower bound is based on a joint cache-channel coding scheme that simultaneously exploits the cache contents and the channel statistics.**

I. Introduction

Caching has lately emerged as a promising technique to reduce the network load and latency in dense wireless networks. The main idea is to have a first *caching phase* where popular content are pre-stored during off-peak periods in cache memories distributed across users, and a second *delivery phase* where specific requested files are conveyed to the users. This approach allows to reduce network load during periods of peak-traffic, because receivers can retrieve parts of their requested files locally from their cache memories. The technical challenge in this system is that during off-peak periods when the servers do pre-store contents in caches, they do not know exactly which files the receivers will demand during the peak-traffic period.

Several recent works have studied the caching problem from an information-theoretic perspective in order to improve the performance limits of cache-aided communications [1]–[6]. In [1], Maddah-Ali and Niesen assumed that the delivery phase takes place over an error-free broadcast channel (BC) and that all the receivers have equal cache sizes. Through a careful design of the cached contents and by applying their new *coded caching scheme*, they attain gains beyond the obvious local caching gains arising from locally retrieving parts of the requested files. The additional gains, which they termed global caching gains, occur because in the coded caching scheme the transmitter can simultaneously serve multiple receivers. Saeedi, Timo, and Wigger showed in [2], [3] that further global caching gains can be achieved by means of their new *piggyback coding scheme*, when the delivery phase is modeled as a packet-erasure BC and different receivers have different channel strengths. Piggyback coding is a *joint cache-channel coding scheme* where the encoder and the decoders simultaneously exploit the cache content and the channel statistics; this is in contrast to *separate cache-channel coding* as in [1] where they are divided into *cache encoder/decoders* and *channel encoder/decoders* that depend only on the channel statistics or only on the cache content.

A different line of research has addressed security issues in cache-aided BCs [4]–[6]. The works most related to ours are [4], [6], where an external eavesdropper is not allowed to learn any information about the messages. More precisely, in [4] it is not allowed to learn anything about the set of all possible messages, whereas in [6] it cannot learn anything about each of the transmitted messages individually. We refer to the former secrecy constraint as a *joint secrecy constraint* and to the latter as an *individual secrecy constraint*. In both works, the external eavesdropper does not have access to the cache memories. In [5], any legitimate receiver acts also as an eavesdropper and is not allowed to learn anything about the other files requested by the other receivers. The work in [4] assumed like [1] that delivery communication takes place over a noise-free BC, and that each legitimate receiver has the same cache memory size. Our previous work [6] modelled the delivery communication with a packet-erasure BC, and assumed that only the weaker among the two receivers has a cache memory.

In this paper, we consider the setup in [6], but under a joint secrecy constraint and with $K \geq 2$ receivers. We partition the set of receivers into K_w weak receivers and K_s strong receivers, and assume that only the weak receivers have equal cache memories of size $\mathcal{M}$. We establish upper and lower bounds on the securely achievable *capacity-memory tradeoff*, i.e., on the largest rates at which the transmitter can communicate reliably with the receivers for a given cache memory size. To obtain the lower bound, we propose four different secure coding schemes that build on sophisticatedly combining wiretap coding, superposition coding and piggyback coding with random secret keys, which are independent of all the data and stored in the receivers' caches. The necessity for secret keys stems from the joint-secrecy constraint and had already been observed in [4], [5]. In our previous work [6], we were able to use cached data as "secret keys" because only an individual secrecy-constraint had to be satisfied.

Our upper and lower bounds match for small and for large cache memories. For small cache memories, they prove optimality of only storing secret keys in the caches, but no data. The reason being that a cached secret key serves in securing any possible users' demand, whereas cached data

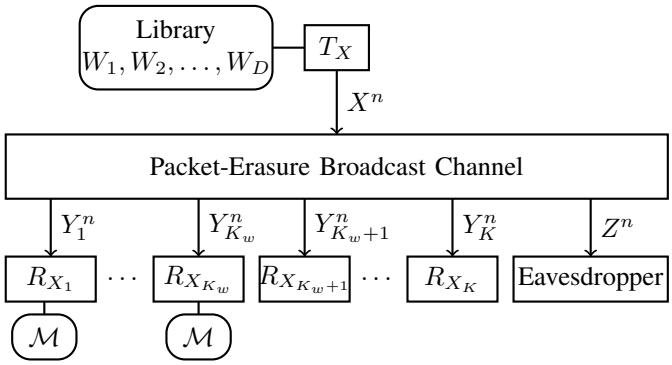

Fig. 1. Packet-erasure BC with K legitimate receivers and an eavesdropper. The K_w weaker receivers have cache memories of size $\mathcal{M}$.

serves only for a subset of demands. As a consequence, in the low cache memory regime, the capacity-memory tradeoff grows proportionally with the cache memory size, irrespective of the number of possible messages in the library.

For comparison, we also provide an upper bound for the two-user scenario on the secure capacity-memory tradeoff under a joint secrecy constraint when both receivers have equal cache size. We observe that in the regime of small cache memory, it is highly beneficial to allocate all the available cache to the weaker receiver compared to allocating the cache memory uniformly across receivers. In fact, in our proposed coding schemes, the data and secret keys cached at the weak receivers are also used to secure the communication to the stronger receivers and to render it more efficient. For the first goal we extend ideas from wiretap coding with secret key to include superposition coding, and for the second one we extend the piggyback coding idea.

II. Problem definition

Consider a wiretap broadcast channel (BC) with a single transmitter, K receivers and an eavesdropper, as shown in Figure 1. We model this channel by a memoryless packet-erasure BC with input alphabet $\mathcal{X} := \{0,1\}^F$ and same output alphabet $\mathcal{Y} := \mathcal{X} \cup \Delta$ at all receivers and the eavesdropper. Here, F is a fixed positive integer and Δ indicates the loss of a packet at the receiver.

The K receivers are partitioned into two sets. The first set $\mathcal{K}_w = \{1, \ldots, K_w\}$ is formed by K_w weak receivers which have bad channels. The second set $\mathcal{K}_s = \{K_w + 1, \ldots, K\}$ is formed by $K_s = K - K_w$ strong receivers which have good channels. Let δ_w, δ_s and δ_z be the erasure probabilities at weak receivers, strong receivers, and the eavesdropper, respectively, where we assume that

$$0 \leq \delta_s \leq \delta_w \leq \delta_z \leq 1. \tag{1}$$

Every weak receiver has access to a local cache memory of size $n\mathcal{M}$ bits, while the stronger receivers have no cache memory. The transmitter accesses a library of $D > 2$ independent messages $W_1, \ldots, W_D$ of rate R_s each. Every message W_d, for $d \in \{1, \ldots, D\}$, is uniformly distributed over $\{1, \ldots, \lfloor 2^{nR_s} \rfloor\}$, where n is the transmission blocklength. The transmitter has also access to a source of randomness θ which we assume over some alphabet Θ.

Every receiver k demands one message W_{d_k} from the library. We denote the demand of receiver k by $d_k \in \{1, \ldots, D\}$, and the *demand vector* by $\mathbf{d} = \{d_1, \ldots, d_K\} \in \{1, \ldots, D\}^K$.

The communication takes place in two phases: the caching phase, where information is stored in weak receivers' cache memories, and the delivery phase, where the demanded messages W_{d_k}, for $k \in \{1, \ldots, K\}$, are conveyed to the receivers.

During the caching phase, the demand vector is unknown to the transmitter and the receivers. Thus, the cache content V_k of every weak receiver $k \in \mathcal{K}_w$ will be a function of the entire library:

$$V_k := g_k(W_1, \ldots, W_D, \theta) \qquad k \in \mathcal{K}_w \tag{2}$$

for some caching function $g_k : \{1, \ldots, \lfloor 2^{nR_s} \rfloor\}^D \times \Theta \to \mathcal{V}$ and cache memory alphabet $\mathcal{V} := \{1, \ldots, \lfloor 2^{n\mathcal{M}} \rfloor\}$.

Prior to the delivery phase, the demand vector $\mathbf{d}$ is learned by the transmitter and the legitimate receivers[1]. Based on the demand vector, the transmitter produces its channel inputs as

$$X^n := f_{\mathbf{d}}(W_1, \ldots, W_D, \theta), \tag{3}$$

for some function $f_{\mathbf{d}} : \{1, \ldots, \lfloor 2^{nR_s} \rfloor\}^D \times \Theta \to \mathcal{X}^n$.

At the end of the delivery phase, receivers decode their demanded messages. Every weak receiver $k \in \mathcal{K}_w$ uses its observed vector Y_k^n and its cache content V_k to produce

$$\hat{W}_k := \varphi_{k,\mathbf{d}}(Y_k^n, V_k), \qquad k \in \mathcal{K}_w \tag{4}$$

for some function $\varphi_{k,\mathbf{d}} : \mathcal{Y}^n \times \mathcal{V} \to \{1, \ldots, \lfloor 2^{nR_s} \rfloor\}$. Every strong receiver $k' \in \mathcal{K}_s$ uses its observed vector $Y_{k'}^n$ to produce the guess

$$\hat{W}_{k'} := \varphi_{k',\mathbf{d}}(Y_{k'}^n), \qquad k' \in \mathcal{K}_s \tag{5}$$

for some function $\varphi_{k',\mathbf{d}} : \mathcal{Y}^n \to \{1, \ldots, \lfloor 2^{nR_s} \rfloor\}$.

A decoding error occurs whenever $\hat{W}_k \neq W_{d_k}$, for $k \in \{1, \ldots, K\}$. We are interested in the worst-case probability of error

$$\mathrm{P}_e^{\text{Worst}} := \max_{\mathbf{d} \in \{1,\ldots,D\}^K} \mathbb{P}\Big[\bigcup_{k=1}^{K} \{\hat{W}_k \neq W_{d_k}\} \Big]. \tag{6}$$

The communication is considered secure if the eavesdropper does not learn any information about the library messages from its outputs Z^n.

Definition 1. *A rate-memory pair $(R_s, \mathcal{M})$ is* securely achievable *if for every $\epsilon > 0$ and sufficiently large blocklength n, there exist caching, encoding, and decoding functions as in* (2)–(5) *so that*

$$P_e^{\textit{Worst}} \leq \epsilon \quad \text{and} \quad \frac{1}{n} I(W_1, \ldots, W_D; Z^n) < \epsilon. \tag{7}$$

We are mainly interested in the following quantity:

Definition 2. *For a cache memory size $\mathcal{M}$, the* secure

[1]Informing all terminals of both demands requires zero communication rate.

capacity-memory tradeoff $C_s(\mathcal{M})$ *is the supremum of all rates* R_s *so that the pair* $(R_s, \mathcal{M})$ *is securely achievable:*

$$C_s(\mathcal{M}) := \sup\big\{R_s\colon \ \ (R_s, \mathcal{M}) \text{ securely achievable}\big\}. \quad (8)$$

When there is no cache, i.e., $\mathcal{M} = 0$, the secure capacity-memory tradeoff $C_s(\mathcal{M})$ was determined in [8]:

$$C_s(\mathcal{M}=0) = F\left(\sum_{k=1}^{K}\frac{1}{\delta_z-\delta_k}\right)^{-1}. \quad (9)$$

Since the strong receivers have no cache memory, the secure capacity-memory tradeoff $C_s(\mathcal{M})$ cannot exceed $F\frac{\delta_z-\delta_s}{K_s}$, see also Theorems 2 and 3. Rate $F\frac{\delta_z-\delta_s}{K_s}$ is trivially achieved for all $\mathcal{M} \geq F\frac{\delta_z-\delta_s}{K_s}D$, because then each weak receiver can store the entire library in its cache. In the following, we restrict attention to $\frac{\mathcal{M}}{D} \leq F\frac{\delta_z-\delta_s}{K_s}$.

III. Main Results for 2 Receivers

In this section, we consider only one weak and one strong receiver. Consider the six rate-memory pairs:

- $$R_0 := F\frac{(\delta_z-\delta_w)(\delta_z-\delta_s)}{2\delta_z-\delta_w-\delta_s}, \quad \mathcal{M}_0 := 0; \quad (10a)$$
- $$R_1 := F\frac{(1-\delta_w)(\delta_z-\delta_s)}{1+\delta_z-\delta_w-\delta_s}, \quad (10b)$$
  $$\mathcal{M}_1 := F\frac{(1-\delta_z)(\delta_z-\delta_s)}{1+\delta_z-\delta_w-\delta_s}; \quad (10c)$$
- $$R_2 := F(1-\delta_s)\min\left\{\frac{\delta_z-\delta_w}{1-\delta_w}, \frac{1-\delta_w}{2-\delta_w-\delta_s}\right\}, \quad (10d)$$
  $$\mathcal{M}_2 := F(1-\delta_z); \quad (10e)$$
- $$R_3 := F\frac{(1-\delta_s)(\delta_z-\delta_s)}{1+\delta_z-\delta_w-\delta_s}, \quad (10f)$$
  $$\mathcal{M}_3 := F\frac{(\delta_z-\delta_s)\big[(\delta_w-\delta_s)D+(1-\delta_z)\big]}{1+\delta_z-\delta_w-\delta_s}; \quad (10g)$$
- $$R_4 := F(\delta_z-\delta_s), \quad (10h)$$
  $$\mathcal{M}_4 := F\frac{(\delta_z-\delta_s)\big[(\delta_z-\delta_s)D+(1-\delta_z)\big]}{1-\delta_s}; \quad (10i)$$
- $$R_5 := F(\delta_z-\delta_s), \qquad \mathcal{M}_5 := F(\delta_z-\delta_s)D. \quad (10j)$$

Theorem 1 (Lower Bound 2 Users)**.** *The upper convex hull of the six rate-memory pairs* $\big\{(R_\ell, \mathcal{M}_\ell);\ \ell \in \{0,1,\ldots,5\}\big\}$ *in* (10) *lower bounds the secure capacity-memory tradeoff:*

$$C_s(\mathcal{M}) \geq \text{upper hull}\big\{(R_\ell, \mathcal{M}_\ell)\colon\ \ell = 0,\ldots,5\big\}. \quad (11)$$

Proof: It suffices to prove achievability of the six rate-memory pairs $\{(R_\ell, \mathcal{M}_\ell)\colon\ \ell = 0,\ldots,5\}$. Achievability of the upper convex hull follows by time/memory sharing arguments as in [1]. Achievability of the pair $(R_0, \mathcal{M}_0)$ is shown in [8]. We justify achievability of $(R_5, \mathcal{M}_5)$ at the end of section II. Achievability of the remaining rate-memory pairs is outlined in section IV. ■

Theorem 2 (Upper Bound 2 Users)**.** *The secure capacity-memory tradeoff* $C_s(\mathcal{M})$ *is upper bounded as:*

$$C_s(\mathcal{M}) \leq F\frac{(\delta_z-\delta_w)(\delta_z-\delta_s)}{2\delta_z-\delta_w-\delta_s} + \frac{\delta_z-\delta_s}{2\delta_z-\delta_w-\delta_s}\mathcal{M}, \quad (12a)$$
$$C_s(\mathcal{M}) \leq F\frac{(1-\delta_w)(1-\delta_s)}{2-\delta_w-\delta_s} + \frac{\mathcal{M}}{D}, \quad (12b)$$
$$C_s(\mathcal{M}) \leq F(\delta_z-\delta_s). \quad (12c)$$

Proof: Bound (12a) follows from [3] and by ignoring the secrecy constraint. Bound (12c) holds because receiver 2 has no cache, and its rate cannot be larger than in the absence of receiver 1. Bound (12b) is proved in Appendix A. ■

Upper bound (12a) is tight when the cache memory is small and upper bound (12c) is tight when the cache memory is sufficiently large.

Corollary 1. *When the cache memory is small:*

$$C_s(\mathcal{M}) = F\frac{(\delta_z-\delta_w)(\delta_z-\delta_s)}{2\delta_z-\delta_w-\delta_s} + \frac{\delta_z-\delta_s}{2\delta_z-\delta_w-\delta_s}\mathcal{M}, \quad 0 \leq \mathcal{M} \leq \mathcal{M}_1, \quad (13)$$

where $\mathcal{M}_1$ *is defined in* (10c)*.*

When the cache memory is large:

$$C_s(\mathcal{M}) = F(\delta_z-\delta_s), \qquad \mathcal{M} \geq \mathcal{M}_4, \quad (14)$$

where $\mathcal{M}_4$ *is defined in* (10i)*.*

The following Figure 2 shows upper and lower bounds for a specific example.

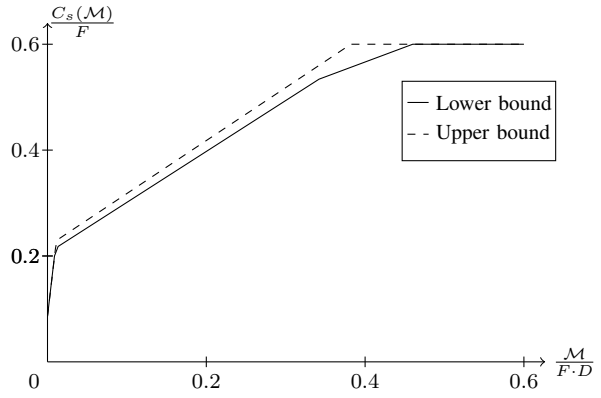

Fig. 2. Upper and lower bounds on the secure capacity-memory tradeoff $C_s(\mathcal{M})$ for $\delta_z = 0.8, \delta_w = 0.7, \delta_s = 0.2, F = 5, D = 15$.

We observe (see also Corollary 1 above) that for small cache memories, the rate-memory pairs $(R_0, \mathcal{M}_0)$, $(R_1, \mathcal{M}_1)$, and $(R_2, \mathcal{M}_2)$ determine the performance of our lower bound in Theorem 1. The first point takes no cache memories. We achieve the other two points by storing only random keys in the cache memory, but no data. We thus conclude that for

small cache memories it is not worth caching data, but only secret keys. The reason is that each piece of data will be useful for only a subset of all possible user demands, whereas a secret key serves with any demand. This also explains why in the regime of small $\mathcal{M}$, the secure capacity-memory tradeoff $C_s(\mathcal{M})$ can grow as a factor times $\mathcal{M}$, irrespective of the library size D. For larger values of $\mathcal{M}$, it grows at most like $\mathcal{M}/D$.

A. Comparison to Other Cache Sizes and Secrecy Constraints

We compare our results also to the following scenarios:

- *Symmetric Caches:* Each receiver has same cache memory size $\mathcal{M}/2$. Similarly to Theorem 2, one can prove that the secure capacity-memory tradeoff $C_{s,\text{sym}}(\mathcal{M})$ under the joint secrecy-constraint in (7) and with cache size $\mathcal{M}/2$ at both receivers is upper bounded as:

$$C_{s,\text{sym}}(\mathcal{M}) \leq F\frac{(\delta_z-\delta_w)(\delta_z-\delta_s)}{2\delta_z-\delta_w-\delta_s}+\frac{\mathcal{M}}{2}, \tag{15a}$$

$$C_{s,\text{sym}}(\mathcal{M}) \leq F(1-\delta_w)+\frac{\mathcal{M}}{2D}, \tag{15b}$$

$$C_{s,\text{sym}}(\mathcal{M}) \leq F\frac{(1-\delta_w)(1-\delta_s)}{2-\delta_w-\delta_s}+\frac{\mathcal{M}}{D}. \tag{15c}$$

- *Individual Secrecy Constraint:* We replace (7) by the weaker *individual* secrecy constraint:

$$\lim_{n\to\infty}\frac{1}{n}I(W_d;Z^n)=0, \qquad \forall d\in\{1,\dots,D\}. \tag{16}$$

  Upper and lower bounds on the secure capacity-memory tradeoff of this scenario were given in [6].
- *No Secrecy Constraint:* Remove (7). Upper and lower bounds on the capacity-memory tradeoff without any secrecy constraint were presented in [3]. For our original scenario where only the weaker receiver has cache memory, the (non-secure) capacity-memory tradeoff is upper bounded by the right-hand sides of (12b) and (12c).

The following Figure 3 compares our upper and lower bounds in Theorems 1 and 2 to the upper and lower bounds on the secure capacity-memory tradeoff with the weaker individual secrecy constraint in (16), see [6], and to the upper bound in (15) on the secure capacity-memory tradeoff under the original joint secrecy constraint when both receivers have equal cache memory size $\frac{\mathcal{M}}{2}$. Figure 3 shows the regime of small cache memory sizes. We observe that in the regime of small cache memory, our coding scheme for cache only at the weak receiver has a much steeper slope, namely $\frac{\delta_z-\delta_s}{2\delta_z-\delta_w-\delta_s}$, than the best possible coding scheme assuming that each receiver has same cache memory size $\frac{\mathcal{M}}{2}$. (The dashed red line is an upper bound for this symmetric setup.) In fact, by (15), the latter is upper bounded by $\frac{1}{2}$. So, for small cache memory sizes, allocating all the cache memory to the weak receivers results in a significantly higher performance than allocating the available cache memory equally between the two receivers. For larger cache sizes, depending on the channel parameters, the upper bound for equal cache sizes is sometimes higher than our lower bound for cache only at receiver 1. We also observe that the capacity-memory tradeoff under an individual secrecy constraint is generally higher than under a joint constraint.

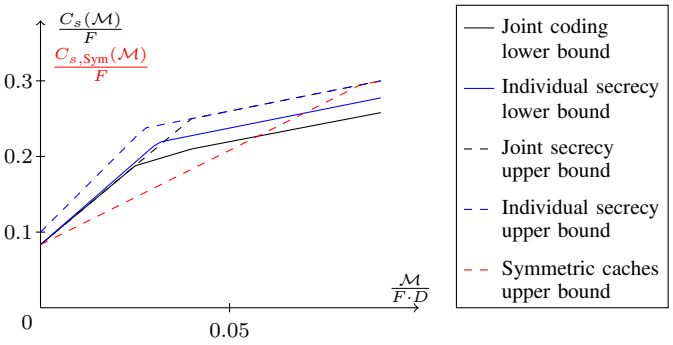

Fig. 3. Upper and lower bounds on the secure capacity-memory tradeoffs $C_s(\mathcal{M})/C_{s,\text{Sym}}(\mathcal{M})$ for $\delta_z=0.8, \delta_w=0.7, \delta_s=0.3, F=5, D=5$.

IV. Proof of Lower Bound, Theorem 1

A. Scheme Achieving Rate-Memory Pair $(R_1, \mathcal{M}_1)$

Divide the delivery phase into two periods of length αn and $(1-\alpha)n$, where $\alpha=\frac{\delta_z-\delta_s}{1+\delta_z-\delta_w-\delta_s}$. Generate a random key K_1 of rate $\alpha(1-\delta_z)F$ and store it in receiver 1's cache. In the first period, the transmitter sends W_{d_1} to receiver 1 using a wiretap code with secret key K_1 [9], [7, (22.7)]. In the second period, the transmitter sends W_{d_2} to receiver 2 using a wiretap code without secret key.

B. Scheme Achieving Rate-Memory Pair $(R_2, \mathcal{M}_2)$

Divide the delivery phase into two periods of length αn and $(1-\alpha)n$, where $\alpha=\max\left\{0,\frac{(1-\delta_s)(\delta_z-\delta_w)-(1-\delta_z)(1-\delta_w)}{(\delta_z-\delta_w)(2-\delta_w-\delta_s)}\right\}$. For $d\in\{1,\dots,D\}$, split each message W_d into two sub-messages $W_d=[W_d^{(0)},W_d^{\oplus}]$ of rates $\alpha(1-\delta_w)F$ and $(1-\alpha)(1-\delta_z)F$. Generate two random keys K_1 and K_2 of rates $\alpha(1-\delta_z)F$ and $(1-\alpha)(1-\delta_z)F$ and store them in receiver 1's cache. In the first period, the transmitter sends message $W_{d_1}^{(0)}$ to receiver 1 using a wiretap code with secret key K_1.

For the communication in the second period, generate a superposition codebook with a cloud center that contains $2^{n(1-\alpha)(1-\delta_z)F}$ codewords, and with each of the satellite codebooks containing 2^{nR_2} codewords. The transmitter encodes $W_{d_1}^{\oplus}\oplus K_2$ into the cloud center and W_{d_2} into the satellite. Receiver 1 decodes only message $W_{d_1}^{\oplus}\oplus K_2$. Receiver 2 decodes both messages. Secrecy of the proposed scheme can be proved by following the steps in [7, pp.554-555], where in the proof of Lemma 22.1 one has to use the fact that the entire superposition codebook contains $2^{n(1-\alpha)(1-\delta_z)F}$ codewords that are compatible with a given satellite message W_{d_2}.

C. Scheme achieving Rate-Memory Pair $(R_3, \mathcal{M}_3)$

Let $\alpha=\frac{\delta_z-\delta_s}{1+\delta_z-\delta_w-\delta_s}$. For $d\in\{1,\dots,D\}$, split each message W_d into three sub-messages $W_d=[W_d^{(0)},W_d^{(1)},W_d^{\oplus}]$ of rates $\alpha(\delta_z-\delta_w)F$, $\alpha(\delta_w-\delta_s)F$ and $\alpha(1-\delta_z)F$. Generate a random key K_1 of rate $\alpha(1-\delta_z)F$. Store K_1 and the D-tuple $W_1^{(1)},\dots,W_D^{(1)}$ in receiver 1's cache. Generate a piggyback

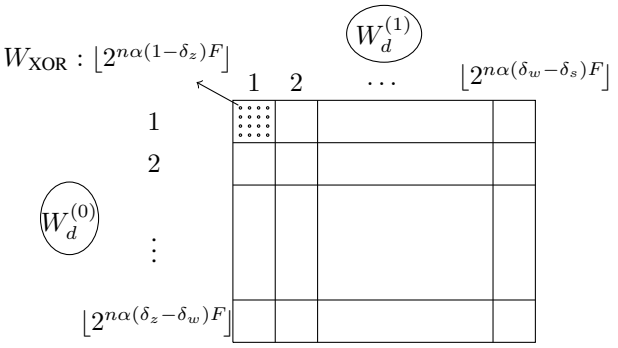

Fig. 4. *Secure piggyback codebook* $\mathcal{C}_1$ with each square depicting a subcodebook $\mathcal{C}_1(W_d^{(0)}, W_d^{(1)})$ and each dot symbolizing a codeword.

codebook [3] $\mathcal{C}_1$ with $\Gamma_1 := \lfloor 2^{n\alpha(1-\delta_z)F} \rfloor \cdot \lfloor 2^{n\alpha(\delta_z-\delta_w)F} \rfloor \cdot \lfloor 2^{n\alpha(\delta_w-\delta_s)F} \rfloor$ codewords of length αn,

$$\mathcal{C}_1 := \Big\{ X_1^{(\alpha n)}(l_1) \Big\}_{l_1=1}^{\Gamma_1}, \tag{17}$$

by drawing each entry of each codeword at random according to a Bernoulli-$1/2$ distribution independently of all other entries. The codebook is partitioned into $\lfloor 2^{n\alpha(\delta_z-\delta_w)F} \rfloor \cdot \lfloor 2^{n\alpha(\delta_w-\delta_s)F} \rfloor$ subcodebooks (bins) each with $\lfloor 2^{n\alpha(1-\delta_z)F} \rfloor$ codewords. We arrange the subcodebooks into an array with $\lfloor 2^{n\alpha(\delta_z-\delta_w)F} \rfloor$ rows and $\lfloor 2^{n\alpha(\delta_w-\delta_s)F} \rfloor$ columns, as depicted in Figure 4 where each square represents a subcodebook.

Divide the delivery phase into two periods of length αn and $(1-\alpha)n$. In the first period, the transmitter conveys messages $W_{d_1}^{(0)}$ and $W_{d_1}^{\oplus}$ to receiver 1 and $W_{d_2}^{(1)}$ to receiver 2. It generates $W_{\text{XOR}} = W_{d_1}^{\oplus} \oplus K_1$ and transmits the W_{XOR}-th codeword of the subcodebook $\mathcal{C}_1(W_{d_1}^{(0)}, W_{d_2}^{(1)})$ over the channel. In the second period, it sends message $W_{d_2}^{(0),\oplus} = [W_{d_2}^{(0)}, W_{d_2}^{\oplus}]$ to receiver 2 using a wiretap code without secret key.

Decoding at receiver 1: Receiver 1 retrieves message $W_{d_2}^{(1)}$ from its cache memory, and considers its outputs $y_1^{\alpha n}$ from the first period. It looks for a unique index-pair $(\hat{w}_{\text{XOR}}, \hat{w}_{d_1}^{(0)}) \in \big[1 : \lfloor 2^{n\alpha(1-\delta_z)F} \rfloor\big] \times \big[1 : \lfloor 2^{n\alpha(\delta_z-\delta_w)F} \rfloor\big]$ so that the $\hat{w}_{\text{XOR}}$-th codeword in subcodebook $\mathcal{C}_1(\hat{w}_{d_1}^{(0)}, W_{d_2}^{(1)})$, which we denote by $x_1^{(\alpha n)}\big(\hat{w}_{\text{XOR}}, \hat{w}_{d_1}^{(0)}, W_{d_2}^{(1)}\big)$, is jointly typical with its observed outputs:

$$\Big(x_1^{(\alpha n)}\big(\hat{w}_{\text{XOR}}, \hat{w}_{d_1}^{(0)}, W_{d_2}^{(1)}\big),\ y_1^{\alpha n} \Big) \in \mathcal{T}_\epsilon^{(\alpha n)}\big(p_X \cdot p_{Y_1|X}\big), \tag{18}$$

where p_X stands for the Bernoulli-$1/2$ distribution, $p_{Y_1|X}$ the channel law to receiver 1, and $\mathcal{T}_\epsilon^{(\alpha n)}$ the typical set [7].

If the desired unique pair of indexes $(\hat{w}_{\text{XOR}}, \hat{w}_{d_1}^{(0)})$ does not exist, receiver 1 declares an error.

Otherwise, if the pair exists, receiver 1 retrieves the key K_1 from its cache memory and generates

$$\hat{w}_{d_1}^{\oplus} = \hat{w}_{\text{XOR}} \oplus K_1. \tag{19}$$

It finally retrieves $W_{d_1}^{(1)}$ from its cache memory and declares the tuple $\hat{W}_1 = \big(\hat{w}_{d_1}^{\oplus}, \hat{w}_{d_1}^{(0)}, W_{d_1}^{(1)}\big)$.

Decoding at receiver 2: Receiver 2 decodes the entire transmitted message tuple $(W_{\text{XOR}}, W_{d_1}^{(0)}, W_{d_2}^{(0)}, W_{d_2}^{(1)}, W_{d_2}^{\oplus})$.

D. Scheme achieving Rate-Memory Pair $(R_4, \mathcal{M}_4)$

Apply the same coding scheme described for $(R_3, \mathcal{M}_3)$ with the following changes: choose $\alpha = \frac{\delta_z - \delta_s}{1-\delta_s}$, cancel $W_d^{(0)}$ rate and change $W_d^{(1)}$ rate to $\alpha(\delta_z - \delta_w)F$.

V. K_w WEAK AND K_s STRONG RECEIVERS

We extend the results in the previous two sections to our more general setup with K_w weak receivers and K_s strong receivers. (Proofs are omitted due to space limitations.)

Theorem 3 (Upper Bound K users)**.** *The secure capacity-memory tradeoff $C_s(\mathcal{M})$ of the scenario with K_w weak receivers and K_s strong receivers is upper bounded by the following $K_w + 1$ conditions:*

$$C_s(\mathcal{M}) \le F\frac{\delta_z - \delta_s}{K_s}, \tag{20a}$$

$$C_s(\mathcal{M}) \le F\left(\frac{j}{1-\delta_w} + \frac{K_s}{1-\delta_s}\right)^{-1} + \frac{j\mathcal{M}}{D},\ \ j \in \{1, \dots, K_w\}, \tag{20b}$$

and by the K_w conditions in (20c) *on top of the next page.*

Consider the rate-memory pair in (21g) on top of the next page and the following five rate-memory pairs

- $$R_0^{(K)} := F\Big(\frac{K_w}{\delta_z - \delta_w} + \frac{K_s}{\delta_z - \delta_s}\Big)^{-1}, \tag{21a}$$
  $$\mathcal{M}_0^{(K)} := 0; \tag{21b}$$
- $$R_1^{(K)} := F\frac{(1-\delta_w)(\delta_z - \delta_s)}{K_w(\delta_z - \delta_s) + K_s(1-\delta_w)}, \tag{21c}$$
  $$\mathcal{M}_1^{(K)} := F\frac{(1-\delta_z)(\delta_z - \delta_s)}{K_w(\delta_z - \delta_s) + K_s(1-\delta_w)}; \tag{21d}$$
- $$R_2^{(K)} := F\min\Big\{\frac{(1-\delta_s)(\delta_z - \delta_w)}{K_s(1-\delta_w)}, \frac{(1-\delta_s)(1-\delta_w)}{K_w(1-\delta_s) + K_s(1-\delta_w)}\Big\}, \tag{21e}$$
  $$\mathcal{M}_2^{(K)} := F\frac{(1-\delta_z)}{K_w}; \tag{21f}$$
- $$R_4^{(K)} := F\frac{\delta_z - \delta_s}{K_s}, \tag{21i}$$
  $$\mathcal{M}_4^{(K)} := \frac{F}{K_s}\Big[\frac{K_s(\delta_z - \delta_s)(1-\delta_z)}{K_s(1-\delta_z) + K_w(\delta_z - \delta_s)} + \frac{DK_w(\delta_z - \delta_s)^2}{K_s(1-\delta_z) + K_w(\delta_z - \delta_s)}\Big]; \tag{21j}$$
- $$R_5^{(K)} := F\frac{\delta_z - \delta_s}{K_s}, \tag{21k}$$
  $$\mathcal{M}_5^{(K)} := F\frac{\delta_z - \delta_s}{K_s}D. \tag{21l}$$

Theorem 4 (Lower Bound K Users)**.** *The upper convex hull of the six rate-memory pairs $\big\{(R_\ell^{(K)}, \mathcal{M}_\ell^{(K)}) :\ \ell \in \{0, \dots, 5\}\big\}$*

$$C_s(\mathcal{M}) \leq \max_{\alpha_j \in [0,1]} \min \left\{ \alpha_j \frac{\delta_z - \delta_w}{j} F + \mathcal{M},\ \frac{\alpha_j(\delta_z - \delta_w) + (1-\alpha_j)(\delta_z - \delta_s)}{j + K_s} F + \frac{j}{j+K_s}\mathcal{M} \right\}, \quad j \in \{1, \ldots, K_w\}. \tag{20c}$$

$$R_3^{(K)} := F \frac{2(1-\delta_w)(\delta_z - \delta_s)\big[K_s(1-\delta_w) + K_w(\delta_w - \delta_s)\big]}{K_w(\delta_z - \delta_s)\big[(K_w - 1)(\delta_w - \delta_s) + 2K_s(1-\delta_w)\big] + 2K_s^2(1-\delta_w)^2}, \tag{21g}$$

$$\mathcal{M}_3^{(K)} := 2F(\delta_z - \delta_s) \frac{D(1-\delta_w)(\delta_w - \delta_s) + (1-\delta_z)\big[(K_w - 1)(\delta_w - \delta_s) + K_s(1-\delta_w)\big]}{K_w(\delta_z - \delta_s)\big[(K_w - 1)(\delta_w - \delta_s) + 2K_s(1-\delta_w)\big] + 2K_s^2(1-\delta_w)^2}. \tag{21h}$$

in (21) *forms a lower bound on the secure capacity-memory tradeoff:*

$$C_s(\mathcal{M}) \geq \text{upper hull}\big\{(R_\ell^{(K)}, \mathcal{M}_\ell^{(K)}), \ell \in \{0, \ldots, 5\}\big\}. \tag{22}$$

Upper and lower bounds are illustrated in Figure 5 assuming there are two weak and four strong receivers.

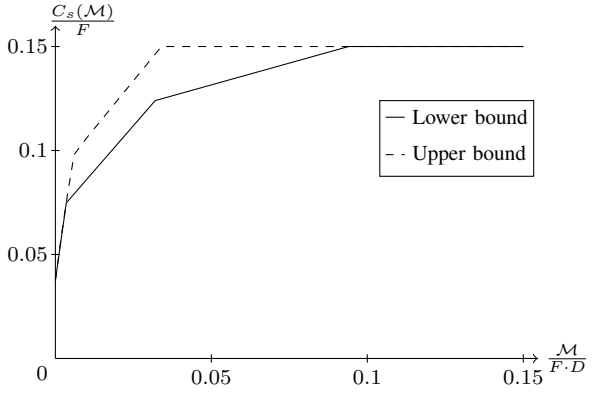

Fig. 5. Generalized upper and lower bounds on the secure capacity-memory tradeoff $C_s(\mathcal{M})$ for $\delta_z = 0.8, \delta_w = 0.7, \delta_s = 0.2, K_s = 4, K_w = 2$, $F = 5, D = 15$.

APPENDIX A
PROOF OF (12b)

By Fano's inequality and the secrecy constraint in (7), there exists a sequence of real numbers $\{\epsilon_n\}_{n=1}^{\infty}$ with $\frac{\epsilon_n}{n}$ tending to 0 as $n \to \infty$ and so that the following inequalities hold:

$$\begin{aligned}
n\,R_s &= H(W_{d_1}) \leq H(W_{d_1}|Z^n) + \frac{\epsilon_n}{2} \\
&\leq I(W_{d_1}; Y_1^n, V_1) - I(W_{d_1}; Z^n) + \epsilon_n \\
&\leq I(W_{d_1}; Y_1^n|V_1) - I(W_{d_1}; Z^n|V_1) + I(W_{d_1}; V_1|Z^n) + \epsilon_n \\
&\overset{(a)}{\leq} \sum_{i=1}^{n} \big[I(W_{d_1}, V_1, Y_2^{i-1}, Z_{i+1}^n; Y_{1,i}) \\
&\qquad - I(W_{d_1}, V_1, Y_2^{i-1}, Z_{i+1}^n; Z_i)\big] + n\mathcal{M} + \epsilon_n \\
&\overset{(b)}{\leq} nI(U_1; Y_1|Q) - nI(U_1; Z|Q) + n\mathcal{M} + \epsilon_n.
\end{aligned} \tag{23}$$

where (a) can be proved following similar steps as in [8, Appendix C] and by using $I(W_{d_1}; V_1|Z^n) \leq n\mathcal{M}$, and (b) follows by defining random variable Q to be uniform over $\{1, \ldots, n\}$ and independent of all other random variables, and $X := X_Q$, $Y_1 := Y_{1,Q}$, $Y_2 := Y_{2,Q}$, $Z := Z_Q$ and $U_1 := (W_{d_1}, V_1, Y_2^{Q-1}, Z_{Q+1}^n)$.

In a similar spirit, but also accounting for receiver 2:

$$\begin{aligned}
2nR_s &= H(W_{d_1}, W_{d_2}) \\
&\leq I(W_{d_1}; Y_1^n, V_1) + I(W_{d_2}; Y_2^n, V_1|W_{d_1}) \\
&\quad - I(W_{d_1}; Z^n) - I(W_{d_2}; Z^n|W_{d_1}) + \epsilon_n \\
&\leq nI(U_1; Y_1, Q) - nI(U_1; Z|Q) + nI(X; Y_2|U, Q) \\
&\quad - nI(X; Z|U, Q) + n\mathcal{M} + \epsilon_n.
\end{aligned} \tag{24}$$

Letting $n \to \infty$ and specializing the constraints (23) and (24) to the erasure BC, we conclude the following: Given cache memory $\mathcal{M}$, the secure capacity-memory tradeoff is upper bounded as:

$$C_s(\mathcal{M}) \leq (\delta_z - \delta_w)\,[H(X|Q) - H(X|U, Q)] + \mathcal{M}, \tag{25a}$$

$$C_s(\mathcal{M}) \leq \frac{1}{2}\,[(\delta_z - \delta_z)H(X|U, Q) + \mathcal{M}], \tag{25b}$$

for some choice of random variables (Q, U, X).

Constraints (25a) and (25b) are jointly optimized by choosing $Q = \emptyset$ and X uniform over $\{1, \ldots, 2^F\}$. Optimizing the minimum of bounds (25a) and (25b) over $H(X|U) \in [0, 2^F]$, results in the desired bound (12c) in Theorem 2.

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," *IEEE Intern, Symp. on Wireless Comm. Systems (ISWCS),* Bruxelles, Belgium, Aug. 2015.

[3] S. Saeedi Bidokhti, R. Timo and M. Wigger, "Noisy broadcast networks with receiver caching." Online: stanford.edu/saeedi/jrnlcache.pdf.

[4] 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.

[5] V. Ravindrakumar, P. Panda, N. Karamchandani, and V. Prabhakarany, "Fundamental limits of secretive coded caching," *IEEE Intern. Symp.on Inf. Theory (ISIT),*, Barcelona, Spain, Jul. 2016.

[6] Sarah Kamel, Mireille Sarkiss and Michèle Wigger, "Secure joint cache-channel coding over erasure broadcast channels," submitted to WCNC 2017.

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

[8] 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.

[9] H. Yamamoto, "Rate-distortion theory for the Shannon cipher system," *IEEE Trans. Inf. Theory,*, vol. 43, no. 3, pp. 827-835, May 1997.

[10] Y.-K. Chia and A. El Gamal, "3-receiver broadcast channels with common and confidential messages," *Proc. IEEE Int. Symp. Inf. Theory,*, Seoul, Korea, pp. 1849-1853, Jun 2009.