Secure Joint 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 two-user wiretap erasure BC with cache memory at the weaker receiver. The bounds coincide when the cache memory exceeds a given threshold. The lower bound also exhibits that cache memories provide larger gains under a secrecy constraint than without such a constraint. Moreover, for a large set of parameters the capacity-memory tradeoff is larger if 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. Such a joint design yields significant gains over a separation-based design.

I. Introduction

Traffic in communication systems varies as a function of the time of day. There are periods where network congestion is high, resulting in packet loss, delivery delays and unsatisfied users. During other periods, the network is barely used. Caching is an interesting approach that allows to lighten the burden of the network during peak-times. Its main idea is to take advantage of the low network-traffic periods to store parts of the data on users' local caches or on nearby servers. The information stored in the caches can then be used to reduce network traffic during congested periods.

In such scenarios, communication can be divided into two phases: the caching phase and the delivery phase. The main challenge is that during the caching phase, the receivers' requests are unknown. One is thus obliged to store information about *all possibly requested files* (i.e., the *library*) in the receivers' cache memories. As Maddah-Ali and Niesen showed in their seminal work [1], with a smart caching strategy it is nevertheless possible that the delivery (high-traffic) communication benefits from the cache memories more than the obvious local caching gain.

Another important aspect of these systems is secrecy. Wireless channels are extremely vulnerable against eavesdropper attacks. In this paper, we focus on a two-receiver erasure broadcast channel (BC) where the weaker receiver has a cache memory. We analyze the rates at which the transmitter can communicate with the two receivers while preventing an external eavesdropper from learning any of the two messages. The eavesdropper is assumed to be weaker (degraded) than the weaker user, and has no access to the cache memories.

Secret communication in cache-aided BCs has previously been studied in [4], [5]. In both works the BC was noiseless for all legitimate receivers as well as for the eavesdropper, and all legitimate receivers had equal cache memory size. Moreover, these previous works imposed stronger secrecy constraints than what we do in this paper. In [4] the eavesdropper is not allowed to learn any information about the entire library. In [5] any legitimate receiver acts also as an eavesdropper and is not allowed to learn anything about the entire message tuple intended for the other receivers. In contrast, in this paper, we require only that the eavesdropper cannot learn any information about any of the messages *individually*. It is allowed to learn, for example, the XOR of two messages.

We propose a new secure coding scheme and a new information-theoretic converse for the wiretap erasure BC with cache memory at only the weaker receiver. The corresponding lower and upper bounds on the *secure capacity-memory tradeoff* are close for most scenarios and coincide when the weak receiver's cache memory exceeds a certain size. We thus establish the exact secure capacity-memory tradeoff for cache memory sizes above this threshold.

For comparison, we also present upper and lower bounds on the secure capacity-memory tradeoff when both receivers have cache memories of equal size. These bounds show that for a large range of parameters, the capacity-memory tradeoff is larger when all the cache memory is allocated to the weaker receive instead of allocating half of it to both receivers. This finding confirms our choice of cache memory assignment. The lower bound further exhibits that under our secrecy constraint, cache memories provide larger gains than in the standard scenario without any secrecy constraints [3]. The reason being that the cache content cannot only help to improve the rate of communication, but also to make it more secure. In particular, as we shall see (and as proposed also in [4]), cache content can be used as a one-time pad.

Our secure coding scheme extends the piggyback coding in [2], [3] to a wiretap scenario. The so obtained *secure piggyback coding* is a *joint cache-channel coding scheme* where the design of encoder and decoders simultaneously exploits the cache content and the channel statistics. This is in contrast to *separate cache-channel coding schemes* where: the encoder consists of a *cache-encoder* that does not depend on the channel statistics followed by a *channel encoder* that does not depend on the cache content; and each decoder consists of a *channel decoder* followed by a *cache decoder* that are subject to similar restrictions. Most previous works [1], [4], [5] assume such a separation-based architecture (both under secrecy constraints and in the standard model), and focus only on the design of the cache encoder and decoders while assuming that the BC is a noise-free pipe from the transmitter to all receivers. This approach was shown to be

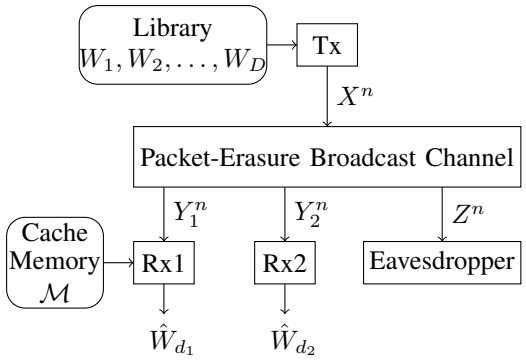

Fig. 1. Packet-erasure BC with two legitimate receivers and an eavesdropper. Receiver Rx1 has cache memory of size $\mathcal{M}$.

highly suboptimal when there is no secrecy constraint [2], [3]; the same is shown here in the presence of such a constraint.

II. Problem definition

We consider a wiretap broadcast channel (BC) with one transmitter, two receivers and an eavesdropper, as shown in Figure 1. The BC is a memoryless packet-erasure BC with input alphabet $\mathcal{X} := \{0,1\}^F$ and same output alphabet $\mathcal{Y} := \mathcal{X} \cup \Delta$ at both legitimate receivers and the eavesdropper. Here, F is a fixed positive integer and Δ indicates the loss of a packet at the receiver. Let δ_1, δ_2 and δ_Z be the erasure probabilities at receiver 1, receiver 2, and the eavesdropper, respectively, where we assume that

$$0 \le \delta_2 \le \delta_1 \le \delta_Z \le 1. \tag{1}$$

The weaker receiver 1 has access to a local cache memory of size $n\mathcal{M}$ bits; the stronger receiver 2 has 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. Receiver 1 demands message W_{d_1} and receiver 2 message W_{d_2}. We denote by d_1 and d_2 in $\{1, \ldots, D\}$ the demands of receivers 1 and 2.

The communication consists of two consecutive phases: a first caching phase, where information is stored in receiver 1's cache memory, and a subsequent delivery phase, where the demanded messages W_{d_1} and W_{d_2} are conveyed to the receivers.

During the caching phase, the receivers' demands are unknown, and thus receiver 1's cache content V will be a function of the entire library:

$$V := g(W_1, \ldots, W_D), \tag{2}$$

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

Prior to the delivery phase, the transmitter and both receivers[1] learn the entire *demand vector* $\mathbf{d} := (d_1, d_2)$. The transmitter then produces its channel inputs as

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

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

At the end of the delivery phase, both receivers attempt to decode their demanded messages. After observing Y_1^n, receiver 1 uses its cache content V to produce the guess

$$\hat{W}_1 := \varphi_{1,\boldsymbol{d}}(Y_1^n, V), \tag{4}$$

for some function $\varphi_{1,\boldsymbol{d}} : \mathcal{Y}^n \times \mathcal{V} \to \{1, \ldots, \lfloor 2^{nR_s} \rfloor\}$. After observing Y_2^n, receiver 2 produces the guess

$$\hat{W}_2 := \varphi_{2,\boldsymbol{d}}(Y_2^n), \tag{5}$$

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

A decoding error occurs if $\hat{W}_k \neq W_{d_k}$, for $k \in \{1, 2\}$. We are interested in the worst-case probability of error

$$\mathrm{P}_e^{\text{Worst}} := \max_{\boldsymbol{d} \in \{1,\ldots,D\}^2} \mathbb{P}\Big[\{\hat{W}_1 \neq W_{d_1}\} \cup \{\hat{W}_2 \neq W_{d_2}\}\Big]. \tag{6}$$

The communication is considered secure if the eavesdropper's channel outputs Z^n during the delivery phase provide no information about any of the two demanded messages.

Definition 1. *We say that a rate-memory pair $(R_s, \mathcal{M})$ is* securely achievable *if for every $\epsilon > 0$, there exists a coding scheme with sufficiently large blocklength n such that,*

$$P_e^{\textit{Worst}} \le \epsilon, \tag{7}$$

and

$$\frac{1}{n} I(W_{d_k}, Z^n) < \epsilon, \quad k \in \{1, 2\}. \tag{8}$$

Our main interest in this paper is the following quantity:

Definition 2. *Given memory-size $\mathcal{M}$, the supremum of all rates R_s so that the pair $(R_s, \mathcal{M})$ is securely achievable is called the* secure capacity-memory tradeoff *$C_s(\mathcal{M})$:*

$$C_s(\mathcal{M}) := \sup\big\{R_s : \ (R_s, \mathcal{M}) \text{ securely achievable}\big\}. \tag{9}$$

The secure capacity-memory tradeoff is unknown even when $\mathcal{M} = 0$, i.e., when there is no cache.

III. Main results

Our main results are an upper and a lower bound on the secure capacity-memory tradeoff $C_s(\mathcal{M})$.

A. One-Sided Cache Assignment

Theorem 1 (Upper Bound on $C_s(\mathcal{M})$)**.** *The secure capacity-memory tradeoff $C_s(\mathcal{M})$ of the two-user wiretap erasure BC with cache memory only at the weaker receiver satisfies the following three conditions:*

$$C_s(\mathcal{M}) \le (\delta_Z - \delta_1)F + \mathcal{M} \tag{10a}$$
$$C_s(\mathcal{M}) \le (\delta_Z - \delta_2)F \tag{10b}$$
$$C_s(\mathcal{M}) \le \frac{(1-\delta_1)(1-\delta_2)}{2-\delta_1-\delta_2}F + \frac{\mathcal{M}}{D}. \tag{10c}$$

Proof: See Section IV.

Theorem 2 (Lower Bound on $C_s(\mathcal{M})$)**.** *Every rate-memory pair $(R_s, \mathcal{M})$ is securely achievable over the two-user wiretap erasure BC with cache memory $\mathcal{M}$ at only the weak receiver, if it satisfies the following six conditions:*

$$R_s \le (\delta_Z - \delta_2)F \tag{11a}$$
$$R_s \le \frac{(1-\delta_2)(\delta_Z-\delta_2)}{1-2\delta_2+\delta_Z}F + \frac{1-\delta_2}{1-2\delta_2+\delta_Z}\frac{\mathcal{M}}{D} \tag{11b}$$
$$R_s \le \frac{(1-\delta_1)(\delta_Z-\delta_2)}{1-\delta_1-\delta_2+\delta_Z}F + \frac{\mathcal{M}}{D} \tag{11c}$$
$$R_s \le \frac{(\delta_Z-\delta_1)(\delta_Z-\delta_2)}{2\delta_Z-\delta_1-\delta_2}F + \frac{\delta_Z-\delta_1+D(\delta_Z-\delta_2)}{2\delta_Z-\delta_1-\delta_2}\frac{\mathcal{M}}{D} \tag{11d}$$

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

$$R_s \le \frac{\delta_Z - \delta_2}{2} F + \frac{D}{2}\frac{\mathcal{M}}{D} \tag{11e}$$

$$R_s \le \frac{D}{D+1}\left[(\delta_Z - \delta_2)F + \frac{\mathcal{M}}{D}\right]. \tag{11f}$$

Thus, any R_s satisfying (11) *forms a lower bound on $C_s(\mathcal{M})$.*

Proof: See Section V.

Remark 1. *At $\mathcal{M} = 0$, the best lower bound on $C_s(\mathcal{M} = 0)$ that can be obtained from above theorem is*

$$C_s(\mathcal{M} = 0) \ge R_0 := \frac{(\delta_Z - \delta_1)(\delta_Z - \delta_2)}{2\delta_Z - \delta_1 - \delta_2} F. \tag{12}$$

The right-hand side R_0 coincides with the secrecy capacity of the two-user wiretap BC without caching when the secrecy constraints in (8) *are replaced by the stronger constraint [7]*

$$\lim_{n\to\infty} \frac{1}{n} I(W_{d_1}, W_{d_2}; Z^n) = 0.$$

Our lower and upper bound on $C_s(\mathcal{M})$ are close (see Figures 2 and 3 ahead) for many parameters; however, they seem to coincide only for sufficiently large cache memories.

Corollary 1. *When*

$$\mathcal{M} \ge F \cdot \max\left\{ D\frac{(\delta_z - \delta_2)^2}{1 - \delta_2}, \delta_z - \delta_2 \right\}. \tag{13}$$

the capacity-memory tradeoff $C(\mathcal{M})$ of the two-user wiretap erasure BC with cache memory $\mathcal{M}$ at the weaker receiver is

$$C(\mathcal{M}) = F(\delta_z - \delta_2). \tag{14}$$

Proof: Under condition (13), constraints (11b)–(11f) are less stringent than constraint (11a). ∎

Theorem 2 is obtained by means of a joint cache-channel coding scheme (see Section V). To demonstrate the strength of the joint cache-channel coding approach, we also characterize the rates that are securely-achievable under the equivalent separate cache-channel coding scheme.

Proposition 1. *Every rate-memory pair $(R_s, \mathcal{M})$ is securely achievable over the wiretap erasure BC with cache memory $\mathcal{M}$ only at the weak receiver using a* separate cache-channel coding scheme*, if it satisfies the following three conditions:*

$$R_s \le (\delta_Z - \delta_2)F,$$

$$R_s \le \frac{(1-\delta_1)(\delta_Z - \delta_2)}{1 - \delta_1 - \delta_2 + \delta_Z} F + \frac{\delta_Z - \delta_2}{1 - \delta_1 - \delta_2 + \delta_Z}\frac{\mathcal{M}}{D},$$

$$R_s \le \frac{(\delta_Z - \delta_2)(\delta_Z - \delta_1)}{2\delta_Z - \delta_1 - \delta_2} F + \frac{(\delta_Z - \delta_2)\big[(D-1)(1-\delta_Z) + (\delta_Z - \delta_1)\big]}{(1-\delta_1)(2\delta_Z - \delta_1 - \delta_2)}\frac{\mathcal{M}}{D}.$$

Proof: See Remark 2 at the end of Section V.

B. Symmetric Cache Assignment

For the purpose of comparison, we assume in this subsection that each receiver has a cache memory of rate $\mathcal{M}/2$. Let the secure capacity-memory tradeoff $C_{s,\text{Sym}}(\mathcal{M})$ be defined in analogy to the capacity-memory tradeoff $C_s(\mathcal{M})$ for one-sided cache memory in the previous section.

Proposition 2 (Upper Bound under Symmetric Cache Assignment)**.** *The secure capacity-memory tradeoff $C_{s,\text{Sym}}(\mathcal{M})$ of the wiretap erasure BC with symmetric cache memory $\mathcal{M}/2$ at both receivers satisfies the following three conditions:*

$$C_{s,\text{Sym}}(\mathcal{M}) \le (\delta_Z - \delta_1)F + \frac{\mathcal{M}}{2} \tag{15a}$$

$$C_{s,\text{Sym}}(\mathcal{M}) \le (1 - \delta_1)F + \frac{\mathcal{M}}{2D} \tag{15b}$$

$$C_{s,\text{Sym}}(\mathcal{M}) \le \frac{(1-\delta_1)(1-\delta_2)}{2 - \delta_1 - \delta_2} F + \frac{\mathcal{M}}{D}. \tag{15c}$$

Proof: Analogous to Theorem 1. Details omitted.

Proposition 3 (Lower Bound under Symmetric Cache Assignment)**.** *A rate-pair $(R_s, \mathcal{M})$ is securely achievable over the two-user wiretap erasure BC with symmetric cache assignment $\mathcal{M}/2$ at both receivers, if it satisfies the following three constraints:*

$$R_s \le 2(1 - \delta_1)F, \tag{16a}$$

$$R_s \le \frac{(1-\delta_1)(1-\delta_2)}{2 - \delta_1 - \delta_2} F + \frac{3 - 2\delta_1 - \delta_2}{2(2 - \delta_1 - \delta_2)}\frac{\mathcal{M}}{D}, \tag{16b}$$

$$R_s \le \frac{(\delta_Z - \delta_1)(\delta_Z - \delta_2)}{2\delta_Z - \delta_1 - \delta_2} F + \left[\frac{D(1-\delta_Z)\big[(1-\delta_1)(\delta_Z - \delta_1) + (1-\delta_2)(\delta_Z - \delta_2)\big]}{2(1-\delta_1)(1-\delta_2)(2\delta_Z - \delta_1 - \delta_2)} + \frac{(\delta_Z - \delta_1)(\delta_Z - \delta_2)(3 - 2\delta_1 - \delta_2)}{2(1-\delta_1)(1-\delta_2)(2\delta_Z - \delta_1 - \delta_2)}\right]\frac{\mathcal{M}}{D}. \tag{16c}$$

Proof: See Section VI.

The scheme in Section VI is a separate cache-channel coding scheme. Under a symmetric cache assignment it is unclear whether joint cache-channel coding can attain a better performance than separate cache-channel coding.

C. Examples and Comparisons

Example 1. *Let $\delta_2 = 0.2$, $\delta_1 = 0.7$ and $\delta_Z = 0.8$. Figure 2 and 3 depict upper bounds (dashed lines) and lower bounds (solid lines) on $C(\mathcal{M})$ and on $C_{\text{Sym}}(\mathcal{M})$ for library sizes $D = 5$ and $D = 30$. The black solid lines show the lower bound in Theorem 2 which is based on our joint cache-channel coding scheme in Section V; the blue solid lines show the lower bound in Proposition 1 based on separate cache-channel coding; and the red solid lines show the lower bound in Proposition 3 for symmetric cache assignment.*

We generally observe the following:

- Without cache memory, $\mathcal{M} = 0$, all three schemes achieve the same rate R_0 in (12).
- For cache memories $\mathcal{M}$ below a given threshold, our joint cache-channel coding scheme achieves rates

$$R_s = R_0 + \frac{\delta_Z - \delta_1 + D(\delta_Z - \delta_2)}{(\delta_Z - \delta_1) + (\delta_Z - \delta_2)}\frac{\mathcal{M}}{D}. \tag{17}$$

  For small cache memories, the slope of the secure capacity-memory tradeoff $C_s(\mathcal{M})$ is larger than $1/D$ and does not decrease with the library size D. This is different in a scenario without secrecy, where the slope is $\frac{\mathcal{M}}{D}$ [3]. Caching is thus more useful in a wiretap-communication scenario than in a standard scenario. The reason is that the cache memory cannot only render the transmission more efficient, but also more secure; for example by means of a one-time pad.

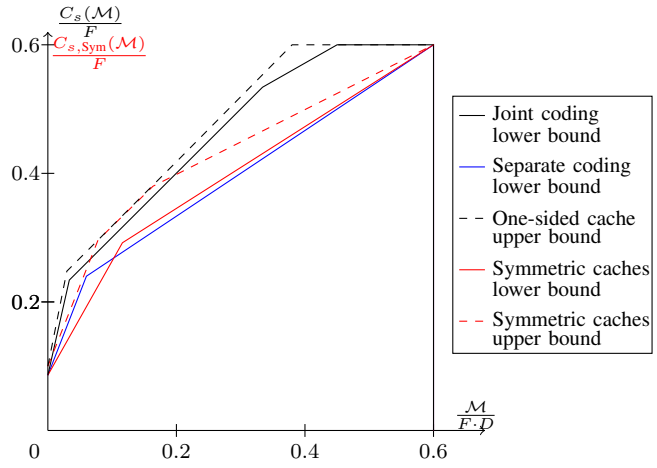

Fig. 2. Upper and lower bounds on the secure capacity-memory tradeoffs $C_s(\mathcal{M})/C_{s,\text{Sym}}(\mathcal{M})$ for the wiretap erasure BC with erasure probabilities $\delta_1 = 0.7$, $\delta_2 = 0.2$, $\delta_Z = 0.8$, and library size $D = 5$.

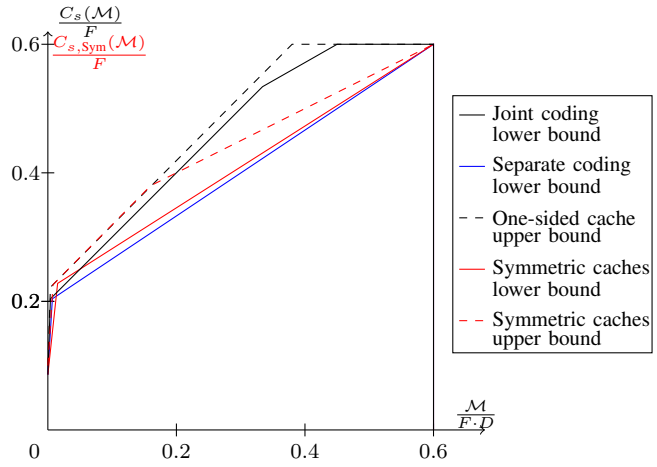

Fig. 3. Upper and lower bounds on the secure capacity-memory tradeoffs $C_s(\mathcal{M})/C_{s,\text{Sym}}(\mathcal{M})$ for the wiretap erasure BC with erasure probabilities $\delta_1 = 0.7$, $\delta_2 = 0.2$, $\delta_Z = 0.8$, and library size $D = 30$.

- For a large range of parameters, our joint cache-channel coding scheme for one-sided cache assignment improves over the best possible coding scheme for symmetric cache assignment. Nevertheless, for some parameters, the secure capacity-memory tradeoff is larger under a symmetric cache assignment than under a one-sided cache assignment. The reason is that in the former case the cache contents can be used to secure the communication to both receivers.
- Our joint cache-channel coding scheme achieves significantly larger rate-memory tradeoff than the equivalent separate cache-channel coding scheme. In particular, the former does not allow to derive the conclusions in the preceding two bullet points.

IV. Upper Bound: Proof of Theorem 1

Constraint (10c) follows from [3, Theorem 9] and by ignoring the secrecy constraints (8). Constraint (10a) is proved as follows. By Fanos inequality and the secrecy constraint in (8), 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:

$$
\begin{aligned}
&nR_s \\
&= H(W_{d_1}) = H(W_{d_1}|Z^n) + I(W_{d_1};Z^n) \\
&\leq H(W_{d_1}|Z^n) + \frac{\epsilon_n}{2} \\
&\leq I(W_{d_1};Y_1^n,V) - I(W_{d_1};Z^n) + H(W_{d_1}|Y_1^n,V) + \frac{\epsilon_n}{2} \\
&\leq I(W_{d_1};Y_1^n,V) - I(W_{d_1};Z^n) + \epsilon_n \\
&\leq I(W_{d_1};Y_1^n|V) - I(W_{d_1};Z^n|V) + I(W_{d_1};V|Z^n) + \epsilon_n \\
&\overset{(a)}{=} \sum_{i=1}^{n} \big[I(W_{d_1};Y_{1,i}|V,Y_1^{i-1},Z_{i+1}^n) - I(W_{d_1};Z_i|V,Y_1^{i-1},Z_{i+1}^n)\big] \\
&\quad + nI(W_{d_1};V|Z^n) + \epsilon_n \\
&\overset{(b)}{\leq} \sum_{i=1}^{n} \big[I(W_{d_1};Y_{1,i}|V,Y_1^{i-1},Z_{i+1}^n) - I(W_{d_1};Z_i|V,Y_1^{i-1},Z_{i+1}^n)\big] \\
&\quad + \sum_{i=1}^{n} \big[I(V,Y_1^{i-1},Z_{i+1}^n;Y_{1,i}) - I(V,Y_1^{i-1},Z_{i+1}^n;Z_i)\big] \\
&\quad + \sum_{i=1}^{n} \big[I(X_i;Y_{1,i}|W_{d_1},V,Y_1^{i-1},Z_{i+1}^n) \\
&\qquad\qquad - I(X_i;Z_i|W_{d_1},V,Y_1^{i-1},Z_{i+1}^n)\big] + n\mathcal{M} + \epsilon_n \\
&\overset{(c)}{=} \sum_{i=1}^{n} \big[I(X_i;Y_{1,i}) - I(X_i;Z_i)\big] + n\mathcal{M} + \epsilon_n, \qquad (18)
\end{aligned}
$$

where (a) holds by Csiszar's sum-identity [6, pp. 25]; (b) because the eavesdropper is degraded with respect to receiver 1; and (c) because of the Markov chain $(V, W_{d_1}, Y_1^{i-1}, Z_{i+1}^n) \to X_i \to (Y_{1,i}, Z_i)$. Letting now $n \to \infty$ establishes constraint (10a).

Constraint (10b) can be proved along similar steps, when index 1 is replaced by index 2; cache content V by a constant, and cache memory size $\mathcal{M}$ by 0.

V. Secure Joint Cache-Channel Coding Scheme

A. Preparations

1) Message splitting: For each $d \in \{1,\dots,D\}$, split the message W_d into two sub-messages

$$W_d = \left[W_d^{(0)}, W_d^{(1)}\right] \qquad (19)$$

of rates $R^{(0)}$ and $R^{(1)}$ that sum up to $R_s = R^{(0)} + R^{(1)}$.

If $R^{(0)} > (D-2)R^{(1)}$, divide $W_d^{(0)}$ into two further parts

$$W_d^{(0)} = \left[W_{d,1}^{(0)}, W_{d,2}^{(0)}\right]$$

of rates $(D-2)R^{(1)}$ and $R^{(0)} - (D-2)R^{(1)}$. Otherwise, let $W_{d,1}^{(0)} = W_d^{(0)}$ be of rate $R^{(0)}$ and $W_{d,2}^{(0)}$ be of zero rate.

Define

$$\iota := \min\left\{\left\lceil \frac{R^{(0)}}{R^{(1)}} \right\rceil, D-2\right\}. \qquad (20)$$

2) Codebook generation: Generate a codebook $\mathcal{C}_1$ with $\Gamma_1 := \lfloor 2^{nR^{(0)}} \rfloor \cdot \lfloor 2^{nR^{(1)}} \rfloor \cdot \lfloor 2^{nR'} \rfloor$ codewords of length αn,

$$\mathcal{C}_1 := \left\{X_1^{(\alpha n)}(l_1)\right\}_{l_1=1}^{\Gamma_1}, \qquad (21)$$

by drawing each entry of each codeword at random according to a Bernoulli-$1/2$ distribution independently of all other

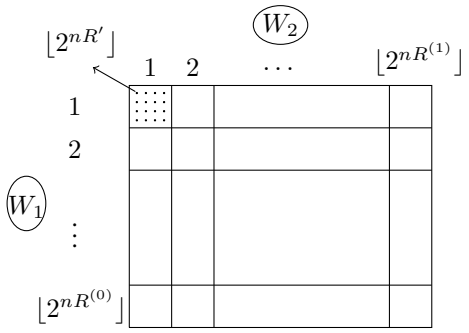

Fig. 4. *Secure piggyback codebook* $\mathcal{C}_1$ with each dot symbolizing a codeword. Subcodebooks (bins) $\mathcal{C}_1(w_1, w_2)$ are depicted by the squares, each containing $\lfloor 2^{nR'} \rfloor$ codewords.

entries. The codebook is partitioned into $\lfloor 2^{nR^{(0)}} \rfloor \cdot \lfloor 2^{nR^{(1)}} \rfloor$ subcodebooks (bins) each with $\lfloor 2^{nR'} \rfloor$ codewords. We arrange the subcodebooks into an array with $\lfloor 2^{nR^{(0)}} \rfloor$ rows and $\lfloor 2^{nR^{(1)}} \rfloor$ columns, as depicted in Figure 4 where each square depicts a subcodebook. The subcodebook in row w_1 and column w_2 is denoted $\mathcal{C}_1(w_1, w_2)$.

Generate a codebook $\mathcal{C}_2$ with $\Gamma_2 := \lfloor 2^{nR^{(1)}} \rfloor \cdot \lfloor 2^{nR''} \rfloor$ codewords of length $(1-\alpha)n$,

$$\mathcal{C}_2 := \Big\{ X_2^{((1-\alpha)n)}(l_2) \Big\}_{l_2=1}^{\Gamma_2}, \tag{22}$$

by randomly drawing each entry of each codeword according to a Bernoulli-$1/2$ distribution independently of all other entries. The codebook is partitioned into $\lfloor 2^{nR^{(1)}} \rfloor$ subcodebooks each with $\lfloor 2^{nR''} \rfloor$ codewords. Denote the w-th subcodebook by $\mathcal{C}_2(w)$, for $w \in \big[1 : \lfloor 2^{nR^{(1)}} \rfloor\big]$.

Codebooks $\mathcal{C}_1$ and $\mathcal{C}_2$ are revealed to all parties (including the eavesdropper).

B. Caching phase

For each $d \in \{1, \dots, D\}$, store $W_d^{(1)}$ in the cache memory of receiver 1. This is possible whenever

$$R^{(1)} \le \frac{\mathcal{M}}{D}. \tag{23}$$

C. Delivery phase

The delivery phase is divided into two periods of length αn and $(1-\alpha)n$, for some $\alpha \in [0, 1]$.

During the first period, the transmitter conveys message $W_{d_1}^{(0)}$ to receiver 1 and message $W_{d_2}^{(1)}$ to receiver 2. It randomly chooses a set of ι indexes

$$\{j_1, j_2, \dots, j_\iota\} \in \big(\{1, \dots, D\} \setminus \{d_1, d_2\}\big)$$

(where ι is defined in (20)) and forms

$$W_{\text{XOR},1}^{(0)} := W_{d_1,1}^{(0)} \oplus \Big[W_{j_1}^{(1)}, W_{j_2}^{(1)}, \dots, W_{j_\iota}^{(1)}\Big]. \tag{24}$$

It then uses the secure piggyback-codebook $\mathcal{C}_1$ in Figure 4. Specifically, it picks an index J_1 uniformly at random from $\big[1 : \lfloor 2^{nR'} \rfloor\big]$ and transmits the

$$J_1\text{-th codeword of subcodebook } \mathcal{C}_1\Big(W_{\text{XOR}}^{(0)}, W_{d_2}^{(1)}\Big)$$

where

$$W_{\text{XOR}}^{(0)} := \Big(W_{\text{XOR},1}^{(0)}, W_{d_1,2}^{(0)}\Big).$$

During the second period, the transmitter conveys $W_{d_2}^{(0)}$ to receiver 2. Specifically, it picks an index J_2 uniformly at random over $\big[1 : \lfloor 2^{nR''} \rfloor\big]$, and transmits the

$$J_2\text{-th codeword of subcodebook } \mathcal{C}_2\big(W_{d_2}^{(0)}\big).$$

D. 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. Given that it observes outputs $y_1^{\alpha n}$, it looks for a unique index-pair $(\hat{w}_1, j) \in \big[1 : \lfloor 2^{nR^{(0)}} \rfloor\big] \times \big[1 : \lfloor 2^{nR'} \rfloor\big]$ so that the j-th codeword in subcodebook $\mathcal{C}_1(\hat{w}_1, W_{d_2}^{(1)})$, which we denote $x_1^{(\alpha n)}\big(\hat{w}_1, W_{d_2}^{(1)}, j\big)$, is jointly typical with its observed outputs:

$$\Big(x_1^{(\alpha n)}\big(\hat{w}_1, W_{d_2}^{(1)}, j\big),\ y_1^{\alpha n}\Big) \in \mathcal{T}_\epsilon^{(\alpha n)}\big(p_X \cdot p_{Y_1|X}\big), \tag{25}$$

where p_X stands for the Bernoulli-$1/2$ distribution, $P_{Y_1|X}$ the channel law to receiver 1, and $\mathcal{T}_\epsilon^{(\alpha n)}$ for the typical set [6].

If the desired unique pair of indexes $(\hat{w}_1, j)$ does not exit, receiver 1 declares an error.

Otherwise, if the pair exists, receiver 1 splits $\hat{w}_1 = \big[\hat{w}_{11}, \hat{w}_{d_1,2}^{(0)}\big]$, and using the messages $W_{j_1}^{(1)}, W_{j_2}^{(1)}, \dots, W_{j_\iota}^{(1)}$ from its cache memory it forms

$$\hat{w}_{d_1,1}^{(0)} = \hat{w}_{11} \oplus \Big[W_{j_1}^{(1)}, W_{j_2}^{(1)}, \dots, W_{j_\iota}^{(1)}\Big]. \tag{26}$$

It finally retrieves $W_{d_1,2}^{(1)}$ from its cache memory and declares the tuple $\big(\hat{w}_{d_1,1}^{(0)}, \hat{w}_{d_1,2}^{(0)}, W_{d_1,2}^{(1)}\big)$.

E. Decoding at Receiver 2

Receiver 2 decodes $W_{d_2}^{(1)}$ based on its outputs $y_2^{\alpha n}$ in the first period, and it decodes $W_{d_2}^{(0)}$ based on its outputs $y_2^{(1-\alpha)n}$ in the second period.

It first looks for a unique triple $(\hat{w}_1, \hat{w}_2^{(1)}, j_1)$ such that

$$\big(x_1^{(\alpha n)}\big(\hat{w}_1, \hat{w}_2^{(1)}, j_1\big), y_2^{\alpha n}\big) \in \mathcal{T}_\epsilon^{(\alpha n)}\big(p_X \cdot p_{Y_2|X}\big). \tag{27}$$

Then, it looks for unique pair $(\hat{w}_2^{(0)}, j_2)$ such that

$$\big(x_2^{((1-\alpha)n)}\big(\hat{w}_2^{(0)}, j_2\big), y_2^{(1-\alpha)n}\big) \in \mathcal{T}_\epsilon^{((1-\alpha)n)}\big(p_X \cdot p_{Y_2|X}\big). \tag{28}$$

If the desired triple and pair exist, receiver 2 declares

$$\hat{W}_{d_2} = \big(\hat{w}_2^{(0)}, \hat{w}_2^{(1)}\big). \tag{29}$$

Otherwise it declares a decoding error.

F. Analysis

By standard arguments, the average probability of error at receivers 1 and 2 (averaged over the codebooks $\mathcal{C}_1, \mathcal{C}_2$, channel realizations, and messages) tend to 0 as $n \to \infty$ if

$$R^{(0)} + R' \le \alpha F(1-\delta_1), \tag{30a}$$
$$R_s + R' \le \alpha F(1-\delta_2), \tag{30b}$$
$$R^{(0)} + R'' \le (1-\alpha) F(1-\delta_2). \tag{30c}$$

We now analyze the information leakage. Notice first that:

$$\begin{aligned} I(W_{d_1}; Z^n | \mathcal{C}_1, \mathcal{C}_2) &= I\big(W_{d_1}^{(1)}, W_{d_1,1}^{(0)}, W_{d_1,2}^{(0)}; Z^n | \mathcal{C}_1, \mathcal{C}_2\big) \\ &= I\big(W_{d_1,1}^{(0)}; Z^{\alpha n} | W_{d_1,2}^{(0)}, \mathcal{C}_1, \mathcal{C}_2\big) + I\big(W_{d_1,2}^{(0)}; Z^{\alpha n} | \mathcal{C}_1, \mathcal{C}_2\big), \end{aligned}$$

because $W_{d_1}^{(1)}$ is not sent over the channel. Furthermore,

$$\begin{aligned} I(W_{d_1,1}^{(0)}; Z^{\alpha n}|W_{d_1,2}^{(0)}, \mathcal{C}_1, \mathcal{C}_2) \\ \leq I\big(W_{d_1,1}^{(0)}; Z^{\alpha n}, W_{\text{XOR},1}^{(0)}, W_{d_1,2}^{(0)}|\mathcal{C}_1, \mathcal{C}_2\big) \\ \overset{(a)}{=} I\big(W_{d_1,1}^{(0)}; W_{\text{XOR},1}^{(0)}, W_{d_1,2}^{(0)}|\mathcal{C}_1, \mathcal{C}_2\big) \overset{(b)}{=} 0, \end{aligned}$$

where (a) holds because of the Markov chain $W_{d_1,1}^{(0)} \to (W_{\text{XOR},1}^{(0)}, W_{d_1,2}^{(0)}) \to Z^n$; and (b) holds because $W_{d_1,1}^{(0)}$ is independent of the pair $\big(W_{\text{XOR},1}^{(0)}, W_{d_1,2}^{(0)}\big)$.

Following the steps in [6, Ch. 22], one can show that

$$\begin{aligned} \lim_{n\to\infty} \frac{1}{n} I(W_{d_1,2}^{(0)}; Z^n|\mathcal{C}_1, \mathcal{C}_2) = 0 \\ \lim_{n\to\infty} \frac{1}{n} I(W_{d_2}^{(0)}; Z^n|\mathcal{C}_1, \mathcal{C}_2) = 0 \\ \lim_{n\to\infty} \frac{1}{n} I(W_{d_2}^{(1)}; Z^n|\mathcal{C}_1, \mathcal{C}_2) = 0 \end{aligned}$$

when

$$(D-1)R^{(1)} + R' \geq \alpha F(1-\delta_Z) \tag{31a}$$

$$R^{(0)} + R' \geq \alpha F(1-\delta_Z) \tag{31b}$$

$$R'' \geq (1-\alpha)F(1-\delta_Z). \tag{31c}$$

To summarize, under constraints (23) and (30a)–(31c), when averaged over the random choice of the codebooks $\mathcal{C}_1$ and $\mathcal{C}_2$, the probabilities of error tend to 0 and the information leakage constraints are satisfied. There must thus exist at least one choice of $\mathcal{C}_1$ and $\mathcal{C}_2$ with these properties. Theorem 2 now follows by eliminating R', R'', α from (23) and (30a)–(31c).

Remark 2. *If one replaces the secure piggyback codebook $\mathcal{C}_1$ by two independent wiretap codebooks, one for message $W_{\text{XOR}}^{(0)}$ and the other for message $W_{d_2}^{(1)}$, one obtains a separate cache-channel coding scheme that achieves the rates in Proposition 1.*

VI. Coded Caching under Symmetric Caches

A. Preparations

Split every message W_d, $d \in [1:D]$, into 3 sub-messages

$$W_d = \Big[W_d^{(0)}, W_d^{(1)}, W_d^{(2)}\Big], \tag{32}$$

of rates $R^{(0)}$, $R^{(1)}/2$, and $R^{(1)}/2$, respectively.

If $R^{(0)} > (D-2)\frac{R^{(1)}}{2}$, divide $W_d^{(0)}$ into two further parts

$$W_d^{(0)} = \Big[W_{d,1}^{(0)}, W_{d,2}^{(0)}\Big]$$

of rates $(D-2)\frac{R^{(1)}}{2}$ and $R^{(0)} - (D-2)\frac{R^{(1)}}{2}$. Otherwise, let $W_{d,1}^{(0)} = W_d^{(0)}$ be of rate $R^{(0)}$ and $W_{d,2}^{(0)}$ of zero rate.

B. Caching phase

Store $\{W_d^{(k)}\}_{d=1}^D$ in cache memory V_k, $k \in \{1,2\}$.

C. Delivery phase

If $R^{(0)} > (D-2)\frac{R^{(1)}}{2}$, transmission takes place in five periods, otherwise in three periods.

For $k \in \{1,2\}$, the transmitter randomly chooses a set of $i := \min\Big\{\lceil\frac{2R^{(0)}}{R^{(1)}}\rceil, \frac{D-2}{2}\Big\}$ indexes $\{j_1, j_2, \ldots, j_i\} \in (\{1,\ldots,D\} \setminus \{d_1, d_2\})$ and forms

$$W_{k,\text{XOR}} := W_{d_k,1}^{(0)} \oplus [W_{j_1}^{(k)}, W_{j_2}^{(k)}, \ldots, W_{j_i}^{(k)}]. \tag{33}$$

It uses a regular (non-wiretap) code to send $W_{k,\text{XOR}}$ to receiver k in period k. Receiver k first decodes the XOR message $W_{k,\text{XOR}}$ and, with its cache content, reconstructs the desired $W_{d_k,1}^{(0)}$.

In period 3, the transmitter sends the common message

$$W_{\text{XOR}} = W_{d_1}^{(2)} \oplus W_{d_2}^{(1)}, \tag{34}$$

to both receivers using an optimal regular code. Each receiver $k \in \{1,2\}$ decodes the XOR message W_{XOR} and, with its cache content, reconstructs its desired sub-message $W_{d_k}^{(3-k)}$.

If $R^{(0)} > (D-2)\frac{R^{(1)}}{2}$, there are also periods 4 and 5. In period $3+k$, $k \in \{1,2\}$, the transmitter sends message $W_{d_k,2}^{(0)}$ to Receiver k using an optimal wiretap code.

VII. Summary

We derived upper and lower bounds on the securely achievable capacity-memory tradeoff of the two-user wiretap packet-erasure BC where the weaker receiver has a cache memory and where the eavesdropper is not allowed to learn any information about each of the delivered messages individually. Upper and lower bounds are generally very close and coincide for large cache memories. They show that caching is much more beneficial under a secrecy constraint than in its' absence.

We also derived upper and lower bounds on the securely achievable capacity-memory tradeoff when both receivers have equal cache memory. These bounds show that when one of the two receivers is much weaker than the other, then in most cases it is highly beneficial to allocate all available cache memory to this weaker receiver instead of allocating half of the memory to each receiver. The benefits are even more important when applying a joint cache-channel coding scheme that simultaneously exploits the cache contents and the channel statistics.

In contrast to the scenario without secrecy constraint, there exist however situations where one receiver is much weaker, but it is still better to the cache memory symmetrically. The reason seems to be that a receiver can benefit from the cache memory at another receiver to increase its transmission rate, but it can only exploit its own cache memory to make it secure.

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

[7] E. Ekrem and S. Ulukus, "Multi-receiver wiretap channel with public and confidential messages," *IEEE Trans. Inf. Theory*, vol. 59, no. 4, Apr. 2013.