Coded caching for wiretap broadcast channels

Sarah Kamel, Michèle Wigger, Mireille Sarkiss

Coded Caching for Wiretap Broadcast Channels

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

[1] LTCI, Télécom ParisTech, Université Paris-Saclay, 75013, Paris, France,
{sarah.kamel, michele.wigger}@telecom-paristech.fr

[2] CEA, LIST, Communicating Systems Laboratory, BC 173, 91191 Gif-sur-Yvette, France; mireille.sarkiss@cea.fr

***Abstract*—The paper studies the wiretap erasure broadcast channel (BC) with an external eavesdropper when the legitimate receivers have cache memories. Various secure coding schemes are proposed for a scenario where K_w weak receivers have same erasure probabilities and K_s strong receivers have same erasure probabilities. The coding schemes achieve the cache-aided secrecy capacity when only weak receivers have cache memories and this cache memory is either small or large. They also allow to conclude the following: 1) Under a total cache budget it is often beneficial to assign the cache memories unequally between strong and weak receivers. 2.) Joint cache-channel coding is necessary to attain the optimal performance. 3.) The secrecy capacity can be positive even when the eavesdropper is stronger than the legitimate receivers.**

I. Introduction

The wiretap channel was introduced by Wyner in [1], where he determined the secrecy capacity of channels with an eavesdropper that is degraded with respect to the legitimate receiver. The secrecy capacity was also established for more complicated channels [2]. Most relevant to this paper is the secrecy capacity of the degraded broadcast channel (BC) [12].

This paper studies wiretap erasure BCs with cache memories at the receivers. Cache memories close to end-users can be used to store fragments of popular contents or secret keys, with the goal to reduce and secure network traffic during peak-traffic periods. The main challenge of these systems is that the demands are unknown prior to the delivery and thus, in the placing phase, contents related to all possible demands have to be stored. A large body of works studied cache-aided systems with the purpose of decreasing network traffic during peak-traffic periods [5]–[9]. Cache-aided systems with secrecy constraints were studied in [10], [11]. In both these works, all legitimate receivers have cache memories of equal size and delivery communication takes place over a common noise free bit-pipe to all the receivers. In [10], this communication needs to be kept secret from an external eavesdropper that can access the common bit-pipe but not the cache memories. In [11], each legitimate receiver acts as an eavesdropper: it is not allowed to learn anything about the messages demanded by the other receivers.

In our previous works [3], [4], we presented upper and lower bounds on the secrecy capacity of a cache-aided wiretap erasure BC. In [3], the focus is on only two users and the external eavesdropper is not allowed to learn anything about each of the demanded messages individually. In contrast, in the more recent work [4], the external eavesdropper is not allowed to learn anything about the library of all possibly demanded messages. In both these works, the eavesdropper is degraded with respect to the legitimate receivers.

Similarly to [4], this paper imposes the stronger secrecy condition that the eavesdropper is not allowed to learn anything about the entire library of messages. However, here more general cache configurations are studied and the eavesdropper does not have to be degraded with respect to the legitimate receivers.

Specifically, this paper presents lower bounds on the secure capacity-memory tradeoff of the cache-aided wiretap BC with K_w weak receivers that all have same erasure probability δ_w and K_s strong receivers that all have same erasure probability $\delta_s \leq \delta_w$. The lower bounds are obtained by introducing secret keys and adapting generalized coded caching [5], [9] and piggyback coding [7] to the BC wiretap channel.

The new lower bound matches the existing upper bound in [4] when only weak receivers have cache memories and this cache memory is either small or large. As our numerical example shows, for this asymmetric cache-memory configuration, the imposed secrecy constraint causes a significant loss in capacity-memory tradeoff. For more balanced configurations with cache-memories also at strong receivers, the loss in capacity-memory tradeoff seems to be smaller. In particular, in a scenario where one is allowed to optimize over the cache sizes subject to a given total cache budget, numerical examples show that the secure capacity-memory tradeoff is close to its non-secure counterpart. This numerical example also reveals that allocating equal cache sizes to all receivers performs poorly for all regimes of total cache budget, whereas allocating equal cache sizes to all weak receivers and no cache sizes to strong receivers performs well for small total cache budgets but not for moderate or large cache budgets.

II. Problem definition

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 $\mathcal{Z} = \mathcal{Y} = \mathcal{X} \cup \Delta$ where Δ indicates the loss of a bit 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 with bad channel conditions. The second set $\mathcal{K}_s := \{K_w+1, \ldots, K\}$ is formed by $K_s = K - K_w$ strong receivers with good channel conditions. Let δ_w, δ_s, and δ_z be the erasure probabilities at weak receivers, strong receivers and the eavesdropper,

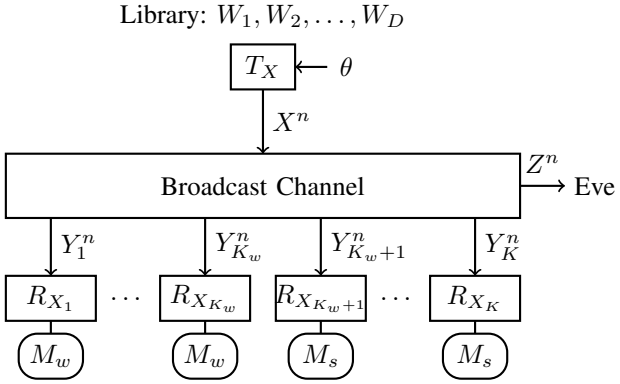

Fig. 1. BC with K legitimate receivers and an eavesdropper. The K_w weaker receivers have cache memories of size M_w and the K_s stronger receivers have cache memories of size M_s.

respectively, where we assume that

$$0 \le \delta_s \le \delta_w \le 1 \quad \text{and} \quad 0 \le \delta_z \le 1. \tag{1}$$

In a standard wiretap erasure BC, positive communication rates are achievable only if the eavesdropper has larger erasure probability than *all* legitimate receivers. This is not the case here, because receivers have access to individual cache memories. In fact, 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, where n is the blocklength of transmission.

The transmitter can access a library of $D > K$ independent messages $W_1, \ldots, W_D$ of rate $R \ge 0$ each. So for each $d \in \mathcal{D} := \{1, \ldots, D\}$, message W_d is uniformly distributed over the set $\{1, \ldots, \lfloor 2^{nR} \rfloor\}$.

Every Receiver $k \in \mathcal{K} := \{1, \ldots, K\}$ demands exactly one message W_{d_k} from the library. We denote the demand of Receiver k by $d_k \in \mathcal{D}$, and all receivers' *demand vector* by

$$\mathbf{d} := (d_1, \ldots, d_K) \in \mathcal{D}^K. \tag{2}$$

Communication takes place in two phases: the *placement phase* where the transmitter sends caching information to be stored in the receivers' cache memories and the *delivery phase* where the demanded messages $W_{d_1}, \ldots, W_{d_K}$, are conveyed to the receivers. During the placement phase, the demand vector $\mathbf{d}$ is unknown to the transmitter and the receivers. Thus, the cache content V_k of every Receiver $k \in \mathcal{K}$ depends only on the library and on the source of local randomness θ available at the transmitter:

$$V_k = g_k(W_1, \ldots, W_D, \theta), \tag{3}$$

for some placement function $g_k \colon \{1, \ldots, \lfloor 2^{nR} \rfloor\}^D \times \Theta \to \mathcal{V}_k$, where for $k \in \mathcal{K}_w$, $\mathcal{V}_k := \{1, \ldots, \lfloor 2^{nM_w} \rfloor\}$, and for $k \in \mathcal{K}_s$, $\mathcal{V}_k := \{1, \ldots, \lfloor 2^{nM_s} \rfloor\}$. Since the placement phase occurs during periods of low-network congestion, each Receiver $k \in \mathcal{K}$ perfectly receives V_k and stores it in its cache memory.

Prior to the delivery phase, the demand vector $\mathbf{d}$ is learned by all terminals. The transmitter can thus send

$$X^n := f_{\mathbf{d}}(W_1, \ldots, W_D, \theta), \tag{4}$$

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

Each Receiver $k \in \mathcal{K}$ attempts to decode its demanded message W_{d_k} based on its outputs Y_k^n and cache content V_k:

$$\hat{W}_k := \varphi_{k,\mathbf{d}}(Y_k^n, V_k), \qquad k \in \mathcal{K}, \tag{5}$$

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

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

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

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

$$\lim_{n \to \infty} \frac{1}{n} I(W_1, \ldots, W_D; Z^n) < \epsilon. \tag{7}$$

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

$$P_e^{\textit{Worst}} \le \epsilon \qquad \textit{and} \qquad \frac{1}{n} I(W_1, \ldots, W_D; Z^n) < \epsilon. \tag{8}$$

Definition 2. *The* secure 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:*

$$C_{sec}(M_w, M_s) := \sup \big\{ R : (R, M_w, M_s) \text{ securely achievable} \big\}. \tag{9}$$

III. Results: Caches only at Weak Receivers

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

$$M_s = 0. \tag{10}$$

In this case, no positive rate is securely achievable unless

$$\delta_z < \delta_s, \tag{11}$$

which is assumed in the following. A first main result of this paper is a lower bound on the secure capacity-memory tradeoff, which extends and improves pour previous lower bound [4], which assumed that the eavesdropper is weaker than all receivers. Consider the following 5 rate-memory pairs as well as the rate-memory pairs $\{(R_{2+t}, M_{2+t})\}_{t=1}^{K_w-1}$ in (12f) and (12g):

- $R_0 := \dfrac{(\delta_z - \delta_s) \cdot (\delta_z - \delta_w)^+}{K_w(\delta_z - \delta_s) + K_s(\delta_z - \delta_w)^+}$, $M_0 := 0$; (12a)
- $R_1 := \dfrac{(1 - \delta_w)(\delta_z - \delta_s)}{K_s(1 - \delta_w) + K_w(\delta_z - \delta_s)}$, (12b)

  $M_1 := \dfrac{(\delta_z - \delta_s) \min\{1 - \delta_z, 1 - \delta_w\}}{K_s(1 - \delta_w) + K_w(\delta_z - \delta_s)}$; (12c)
- $R_2 := \min \left\{ \dfrac{(1 - \delta_w)(1 - \delta_s)}{K_s(1 - \delta_w) + K_w(1 - \delta_s)} \right.$,

$$\frac{(1-\delta_w)(\delta_z-\delta_s)}{K_s(1-\delta_w)+K_w(\delta_w-\delta_s)}\Bigg\}, \quad (12d)$$

$$M_2 := \min\Bigg\{\frac{(1-\delta_z)}{K_w}, \frac{(1-\delta_w)(\delta_z-\delta_s)}{K_s(1-\delta_w)+K_w(\delta_w-\delta_s)}\Bigg\}; \quad (12e)$$

- $$R_{K_w+2} := \frac{(\delta_z-\delta_s)}{K_s}, \quad (12h)$$

$$M_{K_w+2} := \frac{(\delta_z-\delta_s)\min\{1-\delta_z, 1-\delta_w\}}{K_s(1-\delta_z)+K_w(\delta_z-\delta_s)} + \frac{DK_w(\delta_z-\delta_s)^2}{K_s\big[K_s(1-\delta_z)+K_w(\delta_z-\delta_s)\big]}; \quad (12i)$$

- $$R_{K_w+3} := \frac{(\delta_z-\delta_s)}{K_s}, \quad M_{K_w+3} := \frac{D(\delta_z-\delta_s)}{K_s}. \quad (12j)$$

Theorem 1. *The secure capacity-memory tradeoff with cache memories only at weak receivers is lower bounded as:*

$$C_{\text{sec}}(M_w, M_s=0) \geq \text{upper hull}\big\{(R_\ell, M_\ell): \ell \in \{0,\dots,K_w+3\}\big\}. \quad (13)$$

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

$$C_{\text{sec}}(M_w, M_s=0) = R_0 + \frac{K_w(\delta_z-\delta_s)M_w}{K_w(\delta_z-\delta_s)+K_s(\delta_z-\delta_w)^+}, \quad 0 \leq M_w \leq M_1,$$

where R_0 is defined in (12a) *and M_1 is defined in* (12c)*.*

For

$$\delta_z \leq \delta_w, \quad (14)$$

Corollary 1 specializes to $C_{\text{sec}}(M_w, M_s=0) = M_w$, for $M_w \leq M_1$. So, with cache memories, it is possible to securely achieve positive rates even if some receivers are degraded with respect to the eavesdropper. For (14), the performance of Corollary 1 is achieved by XORing the weak receivers' messages with the secret keys stored in the caches.

Corollary 2. *When the cache memory M_w is large:*

$$C_{\text{sec}}(M_w, M_s=0) = \frac{\delta_z-\delta_s}{K_s}, \quad M_w \geq M_{K_w+2}, \quad (15)$$

where M_{K_w+2} is defined in (12i)*.*

Proof Outline for Theorem 1: Rate-memory pair $(R_0, M_0=0)$ follows from [12].

Rate-memory pairs (R_1, M_1) and (R_2, M_2) are both achieved by placing secret keys at the weak receivers' cache memories. For pair (R_1, M_1), the delivery phase time-shares the communications to the weak and to the strong receivers, and it applies a wiretap BC code either with or without using the stored secret keys. For pair (R_2, M_2), the delivery employs a superposition code that secures the cloud center with the stored secret keys. Securing the cloud center with a secret key, secures the communication to the weak receivers (whose messages are encoded in this cloud center) and jams the transmission to the strong receivers (whose messages are encoded in the satellites).

Rate-memory pairs $(R_3, M_3), \dots, (R_{K_w+1}, M_{K_w+1})$ are achieved by placing secret keys as well as uncoded contents as in [5] in the weak receivers' cache memories. Delivery applies *joint cache-channel coding*, where weak receivers' decoding operations simultaneously exploit their channel outputs, the channel statistics, and their cache contents. More specifically, the piggyback coding scheme of [7] is secured with the stored secret keys.

Rate-memory pair (R_{K_w+2}, M_{K_w+2}) is again achieved by placing secret keys and uncoded contents in the cache memories and by applying a piggyback code that is secured with a secret key. For this rate-memory pair, the rate of the data to be conveyed to the weak receivers equals the wiretap-binning rate of the communication to the strong receivers, and does thus not degrade the strong receivers' performance.

Finally, rate-memory pair (R_{K_w+3}, M_{K_w+3}) is achieved by placing the entire library in the cache memory of each weak receiver and communicating only to the strong receivers. ■

A. Numerical Comparison

At hand of a specific example, Figure 2 compares the new lower bound in Theorem 1 with the upper bound in [4]. To illustrate the benefit attained by joint cache-channel coding, the best known lower bound that uses a separation-based architecture is also shown. Finally, the figure also shows a lower bound on the capacity-memory tradeoff when no secrecy constraint is imposed [7].

For small and large cache memories our lower and upper 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 large (see also Corollary 1) because the secret keys stored in the cache memories are always helpful, irrespective of the specific demands $\mathbf{d}$. In particular, the slope is not divided by the library size D as is the case in the traditional caching setup without secrecy.

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 is approximately divided by D, because only a fraction of the cache content is effectively helpful for a specific demand $\mathbf{d}$.

IV. Results: Caches at all Receivers

Let now all receivers have cache memories: $M_w, M_s > 0$. No constraint is imposed on δ_z except that $\delta_z \in [0,1]$. So the eavesdropper can be stronger or weaker than the legitimate receivers. The following lower bound on the secure capacity-memory tradeoff is the second main result of this paper.

Consider the following rate-memory triple as well as the $3K + K_wK_s - 2$ rate-memory triples in (16d)–(16l):

- $$R_1 := \frac{(1-\delta_s)(1-\delta_w)}{K_w(1-\delta_s)+K_s(1-\delta_w)}, \quad (16a)$$

$$R_{t+2} := \frac{(t+1)(1-\delta_w)(\delta_z-\delta_s)\big[K_s t(1-\delta_w)+(K_w-t+1)\min\{\delta_w-\delta_s,\delta_z-\delta_s\}\big]}{(K_w-t+1)(\delta_z-\delta_s)\big[K_s(t+1)(1-\delta_w)+(K_w-t)\min\{\delta_w-\delta_s,\delta_z-\delta_s\}\big]+K_s^2 t(t+1)(1-\delta_w)^2}, \tag{12f}$$

$$M_{t+2} := \frac{Dt(t+1)(1-\delta_w)(\delta_z-\delta_s)\big[K_s(t-1)(1-\delta_w)+(K_w-t+1)\min\{\delta_w-\delta_s,\delta_z-\delta_s\}\big]}{K_w(K_w-t+1)(\delta_z-\delta_s)\big[K_s(t+1)(1-\delta_w)+(K_w-t)\min\{\delta_w-\delta_s,\delta_z-\delta_s\}\big]+K_wK_s^2 t(t+1)(1-\delta_w)^2}$$
$$+\frac{(t+1)(K_w-t+1)(\delta_z-\delta_s)\big[K_s t(1-\delta_w)+(K_w-t)\min\{\delta_w-\delta_s,\delta_z-\delta_s\}\big]\min\{1-\delta_z,1-\delta_w\}}{K_w(K_w-t+1)(\delta_z-\delta_s)\big[K_s(t+1)(1-\delta_w)+(K_w-t)\min\{\delta_w-\delta_s,\delta_z-\delta_s\}\big]+K_wK_s^2 t(t+1)(1-\delta_w)^2}; \tag{12g}$$

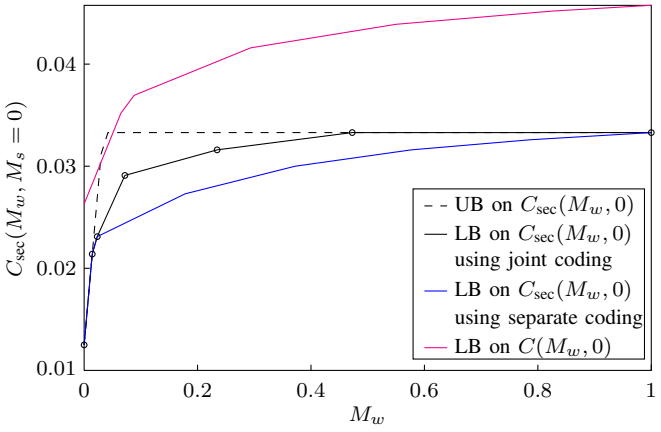

Fig. 2. Upper and lower bounds on $C_{\text{sec}}(M_w, M_s = 0)$ for $\delta_w = 0.7$, $\delta_s = 0.3$, $\delta_z = 0.8$, $D = 30$, $K_w = 5$ and $K_s = 15$.

$$M_{w,1} := \frac{(1-\delta_s)\min\{1-\delta_z, 1-\delta_w\}}{K_w(1-\delta_s)+K_s(1-\delta_w)}, \tag{16b}$$

$$M_{s,1} := \frac{(1-\delta_w)\min\{1-\delta_z, 1-\delta_s\}}{K_w(1-\delta_s)+K_s(1-\delta_w)}; \tag{16c}$$

Theorem 2. *When all receivers have cache memories:*

$$C_{\text{sec}}(M_w, M_s) \geq \text{upper hull}\big\{(R_\ell, M_{w,\ell}, M_{s,\ell}), \ell \in \{1, \ldots, 3K + K_w K_s - 1\}\big\}. \tag{17}$$

Note on Proof of Theorem 2: The coding strategies used to achieve these rate-memory triples are similar to the strategies that achieve the lower bound in Theorem 1. The main difference is that now also the strong receivers can store secret keys and data. The latter makes in particular that the secure piggyback coding scheme used for Theorem 1, here should be replaced by a secure version of the generalized coded caching scheme in [9]. ■

When $\delta_z \leq \delta_s$, then $R_1 = M_{w,1} = M_{s,1}$. This rate is achieved by XORing all messages with stored secret keys.

V. Secure Global 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 *secure global capacity-memory tradeoff* $C_{\text{sec,glob}}$, which is the largest secure capacity-memory tradeoff that is possible given a total cache budget

$$M_{\text{tot}} \geq K_w M_w + K_s M_s.$$

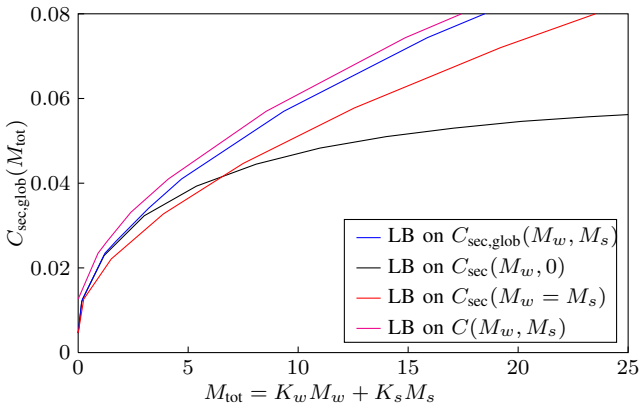

Fig. 3. Lower bounds on $C_{\text{sec,glob.}}(M_{\text{tot}})$ for $\delta_w = 0.7$, $\delta_s = 0.2$, $\delta_z = 0.8$, $D = 50$, $K_w = 20$ and $K_s = 10$.

Using the achievability results in Theorems 1 and 2 combined with time- and memory-sharing arguments, yields a lower bound on $C_{\text{sec,opt}}(M_{\text{tot}})$. This lower bound is plotted in Figure 3 for $K_w = 20$, $K_s = 10$, $D = 50$, $\delta_w = 0.7$ and $\delta_s = 0.2$, and $\delta_z = 0.8$. For comparison, the figure also shows the lower bounds obtained when the available cache memory is uniformly assigned over *all weak receivers*, $M_w = M_{\text{tot}}/K_w$ and $M_s = 0$, and when it is uniformly assigned over *all receivers*, $M_w = M_s = M_{\text{tot}}/(K_w + K_s)$. Finally, the fourth line depicts the lower bound on the global capacity-memory tradeoff without secrecy constraint obtained from [9] and [8]. The figure shows that under an optimized cache assignment, the secure capacity-memory tradeoff is close to its non-secure counterpart. Moreover, similarly to [9], also for the secure capacity-memory tradeoff it is suboptimal to assign the cache memories uniformly across users; in particular, for low cache memories all of it should be assigned to the weakest receivers.

References

[1] A. D. Wyner, "The Wire-tap channel," *The Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[2] A. Mukherjee, S. A. A. Fakoorian, J. Huang and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Communications Surveys and Tutorials*, vol. 16, no. 3, pp. 1550–1573, Third Quarter 2014.

- For $t \in \{1, \ldots, K-1\}$

$$R_{t+1} := \frac{(t+1)(1-\delta_w)(1-\delta_s)\big[K_s t(1-\delta_w) + (K_w - t + 1)(\delta_w - \delta_s)\big]}{(K_w - t + 1)(1-\delta_s)\big[K_s(t+1)(1-\delta_w) + (K_w - t)(\delta_w - \delta_s)\big] + K_s^2 t(t+1)(1-\delta_w)^2}, \tag{16d}$$

$$M_{w,t+1} := \frac{Dt(t+1)(1-\delta_w)(1-\delta_s)\big[K_s(t-1)(1-\delta_w) + (K_w - t + 1)(\delta_w - \delta_s)\big]}{K_w(K_w - t + 1)(1-\delta_s)\big[K_s(t+1)(1-\delta_w) + (K_w - t)(\delta_w - \delta_s)\big] + K_w K_s^2 t(t+1)(1-\delta_w)^2}$$
$$+ \frac{(t+1)(K_w - t + 1)(1-\delta_s)\big[K_s t(1-\delta_w)(1-\delta_z) + (K_w - t)(\delta_w - \delta_s)\min\{1-\delta_z, 1-\delta_w\}\big]}{K_w(K_w - t + 1)(1-\delta_s)\big[K_s(t+1)(1-\delta_w) + (K_w - t)(\delta_w - \delta_s)\big] + K_w K_s^2 t(t+1)(1-\delta_w)^2}, \tag{16e}$$

$$M_{s,t+1} := \frac{(t+1)(1-\delta_w)\big[K_s t(1-\delta_w)\min\{1-\delta_z, 1-\delta_s\} + (K_w - t + 1)(1-\delta_s)\max\{0, \delta_w - \delta_z\}\big]}{(K_w - t + 1)(1-\delta_s)\big[K_s(t+1)(1-\delta_w) + (K_w - t)(\delta_w - \delta_s)\big] + K_s^2 t(t+1)(1-\delta_w)^2}; \tag{16f}$$

- For $t_w \in \{0, \ldots, K_w\}$, $t_s \in \{0, \ldots, K_s\}$ such that $t = t_w + t_s$ and $t \in \{1, \ldots, K\}$

$$R_{K+t_w K_s + t} := \frac{(t_w+1)(t_s+1)(1-\delta_w)(1-\delta_s)\big[K_s(1-\delta_w) + K_w(1-\delta_s)\big]}{K_w(K_w - t_w)(t_s+1)(1-\delta_s)^2 + K_s(t_w+1)(1-\delta_w)\big[(K_s - t_s)(1-\delta_w) + K_w(t_s+1)(1-\delta_s)\big]}, \tag{16g}$$

$$M_{w,K+t_w K_s + t} := \frac{(t_w+1)(t_s+1)(1-\delta_s)^2\big[Dt_w(1-\delta_w) + (K_w - t_w)\min\{1-\delta_z, 1-\delta_w\}\big]}{K_w(K_w - t_w)(t_s+1)(1-\delta_s)^2 + K_s(t_w+1)(1-\delta_w)\big[(K_s - t_s)(1-\delta_w) + K_w(t_s+1)(1-\delta_s)\big]}$$
$$+ \frac{K_s(t_w+1)(t_s+1)(1-\delta_w)(1-\delta_s)\min\{1-\delta_z, 2-\delta_w-\delta_s\}}{K_w(K_w - t_w)(t_s+1)(1-\delta_s)^2 + K_s(t_w+1)(1-\delta_w)\big[(K_s - t_s)(1-\delta_w) + K_w(t_s+1)(1-\delta_s)\big]}, \tag{16h}$$

$$M_{s,K+t_w K_s + t} := \frac{(t_w+1)(t_s+1)(1-\delta_w)^2\big[Dt_s(1-\delta_s) + (K_s - t_s)\min\{1-\delta_z, 1-\delta_s\}\big]}{K_w(K_w - t_w)(t_s+1)(1-\delta_s)^2 + K_s(t_w+1)(1-\delta_w)\big[(K_s - t_s)(1-\delta_w) + K_w(t_s+1)(1-\delta_s)\big]}$$
$$+ \frac{K_w(t_w+1)(t_s+1)(1-\delta_w)(1-\delta_s)\min\{1-\delta_z, 2-\delta_w-\delta_s\}}{K_w(K_w - t_w)(t_s+1)(1-\delta_s)^2 + K_s(t_w+1)(1-\delta_w)\big[(K_s - t_s)(1-\delta_w) + K_w(t_s+1)(1-\delta_s)\big]}; \tag{16i}$$

- For $t \in \{1, \ldots, K-1\}$

$$R_{2K+K_w K_s + t} := \frac{\sum_{t_w=\max\{0,t-K_s\}}^{\min\{t,K_w\}} \binom{K_w}{t_w}\binom{K_s}{t-tw}(1-\delta_w)^{-t_w}(1-\delta_s)^{t_w}}{\sum_{t_w=\max\{0,t+1-K_s\}}^{\min\{t+1,K_w\}} \binom{K_w}{t_w}\binom{K_s}{t+1-t_w}(1-\delta_w)^{-t_w}(1-\delta_s)^{t_w-1}}, \tag{16j}$$

$$M_{w,2K+K_w K_s + t} := \frac{D\sum_{t_w=\max\{1,t-K_s\}}^{\min\{t,K_w\}} \binom{K_w-1}{t_w-1}\binom{K_s}{t-t_w}(1-\delta_w)^{-t_w}(1-\delta_s)^{t_w}}{\sum_{t_w=\max\{0,t+1-K_s\}}^{\min\{t+1,K_w\}} \binom{K_w}{t_w}\binom{K_s}{t+1-t_w}(1-\delta_w)^{-t_w}(1-\delta_s)^{t_w-1}}$$
$$+ \min\left\{\frac{(t+1)(1-\delta_z)}{K}, \frac{(1-\delta_w)^{-t_w}(1-\delta_s)^{t_w}\left[\binom{K-1}{t}(1-\delta_s) - \binom{K_w-1}{t}(\delta_w - \delta_s)\right]}{\sum_{t_w=\max\{0,t+1-K_s\}}^{\min\{t+1,K_w\}} \binom{K_w}{t_w}\binom{K_s}{t+1-t_w}(1-\delta_w)^{-t_w}(1-\delta_s)^{t_w}}\right\}, \tag{16k}$$

$$M_{s,2K+K_w K_s + t} := \frac{D\sum_{t_w=\max\{0,t-K_s\}}^{\min\{t-1,K_w\}} \binom{K_w}{t_w}\binom{K_s-1}{t-t_w-1}(1-\delta_w)^{-t_w}(1-\delta_s)^{t_w}}{\sum_{t_w=\max\{0,t+1-K_s\}}^{\min\{t+1,K_w\}} \binom{K_w}{t_w}\binom{K_s}{t+1-t_w}(1-\delta_w)^{-t_w}(1-\delta_s)^{t_w-1}}$$
$$+ \min\left\{\frac{(t+1)(1-\delta_z)}{K}, \frac{\binom{K-1}{t}(1-\delta_w)^{-t_w}(1-\delta_s)^{t_w+1}}{\sum_{t_w=\max\{0,t+1-K_s\}}^{\min\{t+1,K_w\}} \binom{K_w}{t_w}\binom{K_s}{t+1-t_w}(1-\delta_w)^{-t_w}(1-\delta_s)^{t_w}}\right\}; \tag{16l}$$

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

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

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

[6] 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.

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

[8] M. M. Amiri, D. Gunduz, "Cache-aided content delivery over erasure broadcast channels." ArXiv:1702.05454.

[9] S. Saeedi Bidokhti, M. Wigger and A. Yener, "Benefits of cache assignment on degraded broadcast channels." ArXiv: 1702.08044.

[10] 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.

[11] 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.

[12] 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.