2018 56th Annual Allerton Conference on Communication, Control, and Computing (Allerton)
Allerton Park and Retreat Center
Monticello, IL, USA, October 2-5, 2018

The Caching Broadcast Channel with a Wire and Cache Tapping Adversary of Type II: Multiple Library Files

Mohamed Nafea and Aylin Yener
Wireless Communications and Networking Laboratory (WCAN), Electrical Engineering Department
The Pennsylvania State University, University Park
mnafea@psu.edu *yener@engr.psu.edu*

***Abstract*—A wiretap model with two receivers equipped with fixed-size cache memories, and a type II adversary is considered. The adversary in this model chooses a subset of symbols to tap into either from cache placement, delivery transmission, or both phases. The legitimate parties do not know the fractions or the positions of the tapped symbols in either phase. For a library of size three files or more, lower and upper bounds on the strong secrecy capacity, i.e., the maximum achievable file rate while keeping the overall library strongly secure, are derived. The strong secrecy capacity is identified for the instance of large tapped subsets. Achievability is established by wiretap coding, security embedding codes, one-time pad keys, and coded caching techniques. The upper bound is constructed by three successive channel transformations.**

I. Introduction

Information theoretic security guarantees enable communication in the presence of a computationally unlimited adversary [1]. The wiretap II channel [2] models a noiseless legitimate channel and an erasure channel to the adversary, where the adversary chooses the positions of erasures. Reference [2] has shown that the secrecy capacity of the wiretap II model is identical to the secrecy capacity when the erasures are randomly chosen. This demonstrates the ability of coding to neutralize the adversary's capability of choosing where to tap. The wiretap II model addresses a scenario where the adversary can strategize where to tap and is thus a step towards modeling security scenarios in which the adversary is more powerful than a passive eavesdropper of the classical models [1]. Recently, the wiretap II model has been extended to more general and realistic channel models and various network configurations [2]–[9].

Caching is proposed to reduce network congestion by storing partial information at the end users during off-peak times. In particular, with coded caching, the server can design the cache contents in order to send delivery transmissions that are simultaneously useful for multiple users [10]–[15]. Coded caching with confidentiality concerns has recently been studied, see for example [15]–[21]. In this line of work, the cache placement phase is assumed to be secure, i.e., it is assumed that the adversary cannot tap into the cache contents or the physical communication which performs the cache placement. At the other extreme, if the cache placement were to be public, i.e., the adversary were to have perfect access to the cache contents, the presence of cache memories could not increase the secrecy capacity [22], [23].

Recently, reference [9] has introduced the notion of *cache-tapping* in which the adversary is able to overhear a fixed-size subset of symbols either from cache placement, delivery transmission, or both. In particular, in [9], we have studied the strong secrecy capacity, i.e., the maximum achievable file rate while keeping the overall library strongly secure, when the sender's library has only two files. For this case, we have shown that the strong secrecy capacity is invariant to the positions of the tapped symbols varying between cache placement or delivery. In [9], restricted adversary models, in which the adversary taps into (i) cache placement only, (ii) delivery only, and (iii) both phases with the relative fractions are known, are considered first as building blocks for the general adversary model in question, i.e., when the adversary taps into both phases and the relative fractions are *unknown*. A scheme for the general adversary model which combines wiretap coding, security embedding codes [24], [25], one-time pad keys [22], and coded placement [10] is shown to achieve the strong secrecy capacity.

In this work, we study the model in [9] where the library is larger. In particular, we derive lower and upper bounds on the strong secrecy file rate for a library of size three files or more. For achievability, we use a coding scheme that is similar to the scheme in [9]. However, the cache placement and delivery schemes when the library size is three or larger must differ from those of [9]. Specifically, while for [9] coded placement and uncoded delivery are sufficient, for the present paper, we will be using *uncoded* cache placement and a *partially coded* delivery transmission. We will comment on these design choices in the sequel.

We derive the upper bound in three steps. First, we consider an adversary who can tap into an equal fraction of symbols as in our model, but is only allowed to tap into the delivery phase. Since this adversary has a more restricted strategy space, the secrecy capacity for this adversary model is at least as large as the original model. Second, we utilize Sanov's theorem in method of types [26, Thm. 11.4.1] to upper bound the secrecy capacity for the restricted adversary model by the secrecy capacity when the adversary encounters a discrete memoryless binary erasure channel. Finally, the secrecy capacity of the

978-1-5386-6596-1/18/$31.00 ©2018 IEEE

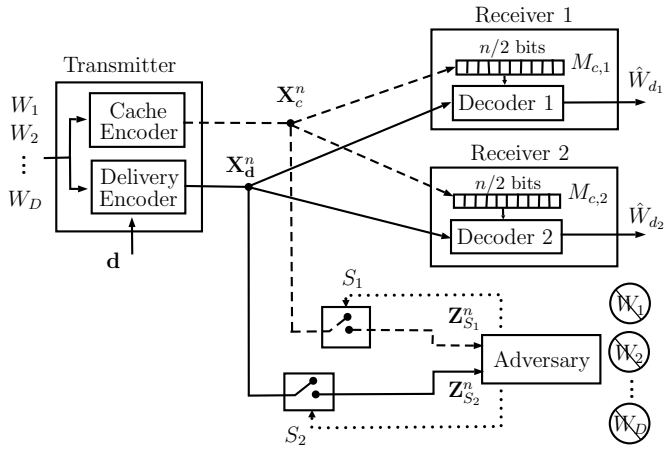

Fig. 1. The caching broadcast channel with a wire and cache tapping adversary of type II (CBC-WCT II).

discrete memoryless model is upper bounded by the secrecy capacity of a single receiver setting in which the receiver requests two files from the library.

Overall, this study shows that under the new and powerful adversarial model we have introduced in [9], and for a library with arbitrary number of files, information theoretically secure communication is possible, and quantifies the strongly secure communication rates.

Notation: For $a, b \in \mathbb{R}$, $[a:b]$ is the set of integers $\{i \in \mathbb{N} : a \leq i \leq b\}$. $A_{[1:n]}$ denotes the sequence $\{A_1, \cdots, A_n\}$. For two sets $\mathcal{A}_1, \mathcal{A}_2$, $\mathcal{A}_1 \times \mathcal{A}_2$ is their Cartesian product. $\mathcal{A}^T$ is the T-fold Cartesian product of the set $\mathcal{A}$. For $W_1, W_2 \in [1:M]$, $W_1 \oplus W_2$ is the bit-wise XOR of W_1, W_2. $\mathbb{D}(p_x||q_x)$ is the Kullback-Leibler divergence between the distributions p_x, q_x.

II. System Model

We consider the communication system in Fig. 1. The transmitter observes $D \geq 2$ independent messages, $W_1, \cdots, W_D$, each is uniformly distributed over $[1 : 2^{nR_s}]$. Each receiver has a cache memory of size $\frac{n}{2}$ bits. The communication occurs over two phases: cache placement and delivery. The broadcast channel is noiseless during both phases.

Notice that, in order to model cache placement that is tapped by an adversary, we consider a length-n communication block over a two-user broadcast channel. The sizes of the cache memories at the receivers in this model are fixed.

Cache placement: The transmitter sends the length-n binary signal $\mathbf{X}_c^n$ to both receivers. $\mathbf{X}_c^n$ is a function of the library files, i.e., $\mathbf{X}_c^n \triangleq f_c(W_{[1:D]})$. The transmitter does not know the receiver demands during placement [10]. Each receiver has an $\frac{n}{2}$ bits cache memory in which they store a function of $\mathbf{X}_c^n$, $M_{c,j} \triangleq f_{c,j}(\mathbf{X}_c^n)$; $f_{c,j} : \{0,1\}^n \mapsto [1 : 2^{\frac{n}{2}}]$, $j = 1, 2$.

Delivery: At the beginning of the delivery phase, both receivers announce their demands $\mathbf{d} \triangleq (d_1, d_2) \in [1:D]^2$ to the transmitter. In order to satisfy these demands, the transmitter encodes $W_{[1:D]}$ and $\mathbf{d}$ into the binary signal $\mathbf{X}_\mathbf{d}^n$. For each $\mathbf{d}$, the transmitter uses the encoder $f_\mathbf{d} : [1 : 2^{nR_s}]^D \mapsto \{0,1\}^n$ and sends the binary codeword $\mathbf{X}_\mathbf{d}^n \triangleq f_\mathbf{d}(W_{[1:D]})$.

Decoding: Receiver j utilizes the decoder $g_{\mathbf{d},j} : [1 : 2^{\frac{n}{2}}] \times \{0,1\}^n \mapsto [1 : 2^{nR_s}]$ and outputs the estimate $\hat{W}_{d_j} \triangleq g_{\mathbf{d},j}(f_{c,j}(\mathbf{X}_c^n), \mathbf{X}_\mathbf{d}^n)$ of its desired message W_{d_j}, $j = 1, 2$.

Adversary model: The adversary chooses $S_1, S_2 \subseteq [1:n]$, where $|S_1| = \mu_1$, $|S_2| = \mu_2$, $0 < \mu_1, \mu_2 \leq n$ and $\mu_1 + \mu_2 = \mu$. S_1, S_2 indicate the positions tapped by the adversary during cache placement and delivery. The adversary observes the length-$2n$ sequence $\mathbf{Z}_S^{2n} = [\mathbf{Z}_{S_1}^n, \mathbf{Z}_{S_2}^n]$, where $\mathbf{Z}_{S_j}^n \triangleq [Z_{S_j,1}, \cdots, Z_{S_j,n}] \in \mathcal{Z}^n$, $j = 1, 2$,

$$Z_{S_1,i} = \begin{cases} X_{c,i}, \ i \in S_1 \\ ?, \ i \notin S_1 \end{cases}, \quad Z_{S_2,i} = \begin{cases} X_{\mathbf{d},i}, \ i \in S_2 \\ ?, \ i \notin S_2. \end{cases} \tag{1}$$

The alphabet $\mathcal{Z} = \{0, 1, ?\}$, where "?" denotes an erasure.

The legitimate parties know neither the realizations of S_1 and S_2, nor μ_1, μ_2. Only $\mu = \mu_1 + \mu_2$ is known. Let $\alpha_1 = \frac{\mu_1}{n}$, $\alpha_2 = \frac{\mu_2}{n}$ be the fractions of tapped symbols in cache placement and delivery, and let $\alpha = \alpha_1 + \alpha_2$ be the overall tapped ratio. Notice that $\alpha_1, \alpha_2 \in [0, 1]$ and $\alpha \in (0, 2]$.

Remark 1 We consider $\alpha > 0$, i.e., the adversary exists. For $\alpha = 0$, i.e., no adversary, the problem in consideration has been extensively studied in the literature, see for example [10], [27]–[29].

A channel code $\mathcal{C}_{2n}$ for this model consists of

- D message sets; $\mathcal{W}_l \triangleq [1 : 2^{nR_s}]$, $l = 1, 2, \cdots, D$,
- Cache encoder; $f_c : [1 : 2^{nR_s}]^D \mapsto \{0,1\}^n$,
- Cache decoders; $f_{c,j} : \{0,1\}^n \mapsto [1 : 2^{\frac{n}{2}}]$, $j = 1, 2$,
- Delivery encoders; $f_\mathbf{d} : [1 : 2^{nR_s}]^D \mapsto \{0,1\}^n, \mathbf{d} \in [1:D]^2$,
- Decoders; $g_{\mathbf{d},j} : [1 : 2^{\frac{n}{2}}] \times \{0,1\}^n \mapsto [1 : 2^{nR_s}], \mathbf{d} \in [1 : D]^2, \ j = 1, 2$.

The file rate R_s is achievable with strong secrecy if there exists a sequence of channel codes $\{\mathcal{C}_{2n}\}_{n \geq 1}$ satisfying

$$\lim_{n \to \infty} \max_{\mathbf{d} \in [1:D]^2} \mathbb{P}\left(\bigcup_{j=1,2} (\hat{W}_{d_j} \neq W_{d_j}) \right) = 0, \tag{2}$$

$$\lim_{n \to \infty} \max_{\substack{S_1, S_2 \subseteq [1:n]: \\ |S_1| + |S_2| = \mu}} I(W_{[1:D]}; \mathbf{Z}_{S_1}^n, \mathbf{Z}_{S_2}^n) = 0. \tag{3}$$

That is, R_s is the symmetric secure file rate, under any demand vector and adversarial strategy. The strong secrecy capacity C_s is the the supremum of all achievable R_s.

III. Main Results

The following theorem presents an achievable strong secrecy file rate for the model in Section II when $D \geq 3$.

Theorem 1 *For $0 < \alpha \leq 2$ and $D \geq 3$, the achievable strong secrecy file rate for the caching broadcast channel with a wire and cache tapping adversary of type II (CBC-WCT II) is lower bounded as*

$$R_s(\alpha) \geq \begin{cases} \frac{1}{2} + \frac{3(1-\alpha)}{4D}, & 0 < \alpha < 1 \\ 1 - \frac{\alpha}{2}, & 1 \leq \alpha \leq 2. \end{cases} \tag{4}$$

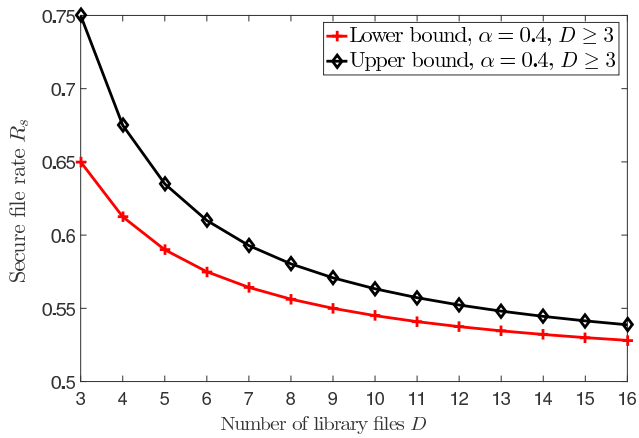

Fig. 2. Lower and upper bounds for the achievable strong secrecy file rate R_s, when $\alpha = 0.4$ and $D \geq 3$.

Proof: The proof is provided in Section IV. ■

The following theorem upper bounds the secrecy file rate when $D \geq 3$.

Theorem 2 *For $0 < \alpha \leq 2$ and $D \geq 3$, the achievable strong secrecy file rate for the CBC-WCT II is upper bounded as*

$$R_s(\alpha) \leq \begin{cases} \frac{1}{2} + \frac{2D-1}{2D(D-1)}(1-\alpha), & 0 < \alpha < 1 \\ 1 - \frac{\alpha}{2}, & 1 \leq \alpha \leq 2. \end{cases} \tag{5}$$

Proof: The proof is provided in Section V. ■

The following corollary follows directly from Theorems 1, 2, and [9].

Corollary 1 *For $1 \leq \alpha \leq 2$, i.e., when the adversary taps a subset of symbols larger than one phase of communication, the strong secrecy capacity for the CBC-WCT II is*

$$C_s(\alpha) = 1 - \frac{\alpha}{2}. \tag{6}$$

For $\alpha \in (0, 1)$, the lower and upper bounds in (4), (5), do not match. These bounds are sketched for $\alpha = 0.4$ in Fig. 2.

Remark 2 Setting $\alpha = 0$, i.e., no adversary, in (4), (5), does not result in matching bounds. However, our achievability scheme described in Section IV for $\alpha = 0$ reduces to the achievability scheme in [10], which is shown to achieve the optimal rate-memory tradeoff for the case of two users and more than two files [27], [29]. The upper bound derived in this work is to address the intricacies of the adversarial model and is useful when the adversary is present ($\alpha > 0$).

Remark 3 In [9], we have shown that the strong secrecy capacity for $D = 2$, for $0 < \alpha \leq 2$, is $C_s(\alpha) = 1 - \frac{\alpha}{2}$, which outperforms the rate in Theorem 1 for $D = 2$.

IV. Proof of Theorem 1

The achievability scheme we use for $D \geq 3$ utilizes the same channel coding structure as in the scheme proposed in [9] for $D = 2$. The difference however lies in generating the messages to be communicated over cache placement and delivery. In particular, we utilize here uncoded placement for designing the cache contents, and a partially coded delivery transmission that is simultaneously useful for both receivers, while the scheme in [9] utilized coded placement and uncoded delivery. In the following, we describe the channel code structure in detail for the sake completeness.

A. Achievability for $\alpha \in (0, 1)$

Recall that $n\alpha_1 = \mu_1$, $n\alpha_2 = \mu_2$, $n\alpha = \mu$. Let $\{\epsilon_n\}_{n \geq 1}$ denote a sequence of positive real numbers such that $\epsilon_n \to 0$ as $n \to \infty$. Define $\alpha_\epsilon = \alpha + 2\epsilon_n$, $\alpha_{1,\epsilon} = \alpha_1 + \epsilon_n$, $\alpha_{2,\epsilon} = \alpha_\epsilon - \alpha_{1,\epsilon}$. For simplicity, let $n\frac{\alpha_\epsilon}{2}$, $n\frac{\alpha_{1,\epsilon}}{2}$ be integers. A minor modification to the analysis can be adopted otherwise.

The transmitter divides each file W_l, $l \in [1 : D]$, into the independent messages $\{W_l^{(1)}, W_l^{(2)}, W_{l,t}, W_{l,s}\}$. $W_l^{(1)}$, $W_l^{(2)}$ are uniformly distributed over $[1 : 2^{n\frac{1-\alpha_\epsilon}{2D}}]$. $W_{l,t}$ is uniformly distributed over $[1 : 2^{n\frac{(2D-1)(1-\alpha_\epsilon)}{4D}}]$, and $W_{l,s}$ is uniformly distributed over $[1 : 2^{n\frac{\alpha_\epsilon}{2}}]$. The transmitter randomly, and independently from $W_{[1:D]}$, generates the two independent keys K_1, K_2, each is uniformly distributed over $[1 : 2^{n\frac{\alpha_\epsilon}{2}}]$. The main ideas of the achievability scheme are

1) The transmitter uses wiretap coding with a randomization message of size $n(\alpha_1 + \alpha_2) = n\alpha$ bits in *both cache placement and delivery* phases. As the adversary does not tap into more than $n\alpha$ bits in each phase, a secure transmission rate of $1 - \alpha$ is achievable in each phase, as long as the randomization messages in the two phases are independent. Using uncoded placement and a partially coded delivery, a secure file rate of $\frac{1-\alpha}{2} + \frac{3(1-\alpha)}{4D}$ can be achieved.
2) The randomization messages over the two phases can deliver additional secure information, of rate $\frac{\alpha}{2}$ per file, via encryption. The overall achievable file rate is thus $R_s = \frac{1}{2} + \frac{3(1-\alpha)}{4D}$. In particular, we utilize the keys K_1, K_2 as the randomization message for cache placement. Along with wiretap coding, we employ a security embedding code [24], [25], by using bits of K_1, K_2 in a manner that allows the adversary to be able to retrieve only the last $n\frac{\alpha_1}{2}$ bits from each. In the delivery phase, we encrypt additional pieces of information, $W_{d_1,s}, W_{d_2,s}$, with K_1, K_2, and utilize this encrypted information as the randomization message. We employ again a security embedding code, in the *reverse order*, such that the adversary can only retrieve the first $n\frac{\alpha_2}{2}$ bits from each of $W_{d_1,s} \oplus K_1$ and $W_{d_2,s} \oplus K_2$.
3) With the aforementioned construction, the adversary, for any values of α_1, α_2 it chooses, can only retrieve a set of key bits and/or information bits encrypted with a distinct set of key bits. In particular, due to the *reversed embedding order*, the adversary does not obtain, in the delivery phase, any message bits encrypted with key bits it has seen during cache placement. Since $\{K_1, K_2\}$, $\{W_{d_1,s} \oplus K_1, W_{d_2,s} \oplus K_2\}$ are independent, and each is an independent sequence of bits, the adversary cannot

use the revealed key bits in cache placement to obtain any information about the encrypted message bits to be securely transmitted during delivery.

We now explain the proof in detail. Define

$$M_c = \{M_{c,1}, M_{c,2}\}; \quad M_{c,1} = \{W_1^{(1)}, W_2^{(1)}, \cdots, W_D^{(1)}\},$$
$$M_{c,2} = \{W_1^{(2)}, W_2^{(2)}, \cdots, W_D^{(2)}\} \tag{7}$$
$$\tilde{M}_c = \{\tilde{M}_{c,1}, \tilde{M}_{c,2}\}; \quad \tilde{M}_{c,1} = K_1, \qquad \tilde{M}_{c,2} = K_2. \tag{8}$$

$M_{c,1}$, $M_{c,2}$ represent the messages to be securely transmitted during cache placement regardless the adversary's choice of α_1, and stored in the receivers caches; $M_{c,j}$ is stored in receiver j's cache. $\tilde{M}_c = \{\tilde{M}_{c,1}, \tilde{M}_{c,2}\}$ is the randomization message utilized for wiretap coding in cache placement. $\tilde{M}_{c,j}$ is stored as well in receiver j's cache. Notice that the size of M_c is $2D \times n\frac{1-\alpha_\epsilon}{2D} = n(1-\alpha_\epsilon)$ bits and the size of $\tilde{M}_c$ is $n\alpha_\epsilon$ bits. In addition, the combined size of $M_{c,j}, \tilde{M}_{c,j}$ is $\frac{n}{2}$ bits, i.e., equal to the cache size at receiver j.

The transmitter further divides $\tilde{M}_{c,1}, \tilde{M}_{c,2}$, into sequences of independent bits $\{\tilde{M}_{c,1}^{(1)} \cdots \tilde{M}_{c,1}^{(n\frac{\alpha_\epsilon}{2})}\}$, $\{\tilde{M}_{c,2}^{(1)} \cdots \tilde{M}_{c,2}^{(n\frac{\alpha_\epsilon}{2})}\}$. The transmitter generates the binary codeword $\mathbf{X}_c^n$ as follows:

Cache Placement Code Generation, $\mathcal{C}_{c,n}$: Let m_c, $\tilde{m}_{c,1} = \{\tilde{m}_{c,1}^{(1)}, \cdots, \tilde{m}_{c,1}^{(n\frac{\alpha_\epsilon}{2})}\}$, $\tilde{m}_{c,2} = \{\tilde{m}_{c,2}^{(1)}, \cdots, \tilde{m}_{c,2}^{(n\frac{\alpha_\epsilon}{2})}\}$ be the realizations of M_c, $\tilde{M}_{c,1}$, $\tilde{M}_{c,2}$ in (7) and (8). We construct the code $\mathcal{C}_{c,n}$, from which $\mathbf{X}_c^n$ is drawn, as follows. Randomly and independently divide all the possible 2^n length-n binary sequences into $2^{n(1-\alpha_\epsilon)}$ bins, indexed by $m_c \in [1 : 2^{n\frac{1-\alpha_\epsilon}{2}}]^2$, and each contains $2^{n\alpha_\epsilon}$ binary codewords. Further, randomly and independently divide each bin m_c into two sub-bins, indexed by $\tilde{m}_{c,1}^{(1)}$, and each contains $2^{n\alpha_\epsilon - 1}$ binary codewords. The two sub-bins $\tilde{m}_{c,1}^{(1)}$ are further randomly and independently divided into two smaller bins, indexed by $\tilde{m}_{c,2}^{(1)}$, and each contains $2^{n\alpha_\epsilon - 2}$ binary codewords. The process continues, going over $\tilde{m}_{c,1}^{(2)}$, $\tilde{m}_{c,2}^{(2)}$, $\cdots$, $\tilde{m}_{c,1}^{(n\frac{\alpha_\epsilon}{2}-1)}$, $\tilde{m}_{c,2}^{(n\frac{\alpha_\epsilon}{2}-1)}$, $\tilde{m}_{c,1}^{(n\frac{\alpha_\epsilon}{2})}$, until the remaining two codewords, after each sequence of divisions, are indexed by $\tilde{m}_{c,2}^{(n\frac{\alpha_\epsilon}{2})}$.

Cache Encoder: Given $w_{[1:D]}$, i.e., $\{w_l^{(1)}, w_l^{(2)}, w_{l,t}, w_{l,s}\}$, $l \in [1 : D]$, the transmitter generates m_c, $\tilde{m}_c$ as in (7), (8). Using $\mathcal{C}_{c,n}$, the transmitter sends $\mathbf{x}_c^n$ which corresponds to m_c, $\tilde{m}_{c,1}$, $\tilde{m}_{c,2}$, i.e., $\mathbf{x}_c^n(m_c, \tilde{m}_{c,1}^{(1)}, \tilde{m}_{c,2}^{(1)}, \cdots, \tilde{m}_{c,1}^{(n\frac{\alpha_\epsilon}{2})}, \tilde{m}_{c,2}^{(n\frac{\alpha_\epsilon}{2})})$.

For the demand vector $\mathbf{d} = (d_1, d_2)$, $d_1, d_2 \in [1 : D]$, define

$$M_{\mathbf{d}} = \{W_{d_2}^{(1)} \oplus W_{d_1}^{(2)}, W_{d_1,t}, W_{d_2,t}\} \tag{9}$$
$$\tilde{M}_{\mathbf{d}} = \{\tilde{M}_{\mathbf{d},1}, \tilde{M}_{\mathbf{d},2}\};$$
$$\tilde{M}_{\mathbf{d},1} = W_{d_1,s} \oplus K_1, \ \tilde{M}_{\mathbf{d},2} = W_{d_2,s} \oplus K_2. \tag{10}$$

$M_{\mathbf{d}}$ is the message to be securely transmitted during delivery regardless the adversary's choice of α_2. $\tilde{M}_{\mathbf{d}}$ is the randomization message. The size of $M_{\mathbf{d}}$ is $n\frac{1-\alpha_\epsilon}{2D} + 2 \times n\frac{(2D-1)(1-\alpha_\epsilon)}{4D} = n(1-\alpha_\epsilon)$ bits, and the size of $\tilde{M}_{\mathbf{d}}$ is $n\alpha_\epsilon$ bits.

Similar to cache placement, the transmitter further divides $\tilde{M}_{\mathbf{d},1}, \tilde{M}_{\mathbf{d},2}$ into sequences of independent binary messages, $\{\tilde{M}_{\mathbf{d},1}^{(1)} \cdots \tilde{M}_{\mathbf{d},1}^{(n\frac{\alpha_\epsilon}{2})}\}$, $\{\tilde{M}_{\mathbf{d},2}^{(1)} \cdots \tilde{M}_{\mathbf{d},2}^{(n\frac{\alpha_\epsilon}{2})}\}$. The transmitter generates the binary codeword $\mathbf{X}_{\mathbf{d}}^n$ as follows.

Delivery Code Generation, $\mathcal{C}_{\mathbf{d},n}$: Let $m_{\mathbf{d}}$, $\tilde{m}_{\mathbf{d},1} = \{\tilde{m}_{\mathbf{d},1}^{(1)}, \cdots, \tilde{m}_{\mathbf{d},1}^{(n\frac{\alpha_\epsilon}{2})}\}$, $\tilde{m}_{\mathbf{d},2} = \{\tilde{m}_{\mathbf{d},2}^{(1)}, \cdots, \tilde{m}_{\mathbf{d},2}^{(n\frac{\alpha_\epsilon}{2})}\}$ be the realizations of $M_{\mathbf{d}}$, $\tilde{M}_{\mathbf{d},1}$, $\tilde{M}_{\mathbf{d},2}$ in (9), (10). We construct $\mathcal{C}_{\mathbf{d},n}$, from which $\mathbf{X}_{\mathbf{d}}^n$ is drawn, in a similar fashion as $\mathcal{C}_{c,n}$, but with a reversed indexing of the sub-bins. In particular, randomly and independently divide all the 2^n binary sequences into $2^{n(1-\alpha_\epsilon)}$ bins, indexed by $m_{\mathbf{d}} \in [1 : 2^{n\frac{1-\alpha_\epsilon}{2}}]^2$, and each contains $2^{n\alpha_\epsilon}$ binary codewords. Further randomly and independently divide each bin $m_{\mathbf{d}}$ into two sub-bins, indexed by $\tilde{m}_{\mathbf{d},1}^{(n\frac{\alpha_\epsilon}{2})}$, and each contains $2^{n\alpha_\epsilon - 1}$ binary codewords. The process continues, going in reverse order over $\tilde{m}_{\mathbf{d},2}^{(n\frac{\alpha_\epsilon}{2})}, \tilde{m}_{\mathbf{d},1}^{(n\frac{\alpha_\epsilon}{2}-1)}$, $\tilde{m}_{\mathbf{d},2}^{(n\frac{\alpha_\epsilon}{2}-1)}$, $\cdots$, $\tilde{m}_{\mathbf{d},1}^{(1)}$, until the remaining two codewords, after each sequence of divisions, are indexed by $\tilde{m}_{\mathbf{d},2}^{(1)}$.

Delivery Encoder: Given $w_{[1:D]}$, $\mathbf{d} = (d_1, d_2)$, the transmitter generates $m_{\mathbf{d}}, \tilde{m}_{\mathbf{d},1}, \tilde{m}_{\mathbf{d},2}$ as in (9), (10). The transmitter then sends $\mathbf{x}_{\mathbf{d}}^n$, from $\mathcal{C}_{\mathbf{d},n}$, which corresponds to $m_{\mathbf{d}}$, $\tilde{m}_{\mathbf{d},1}$, $\tilde{m}_{\mathbf{d},2}$, i.e., $\mathbf{x}_{\mathbf{d}}^n(m_{\mathbf{d}}, \tilde{m}_{\mathbf{d},1}^{(n\frac{\alpha_\epsilon}{2})}, \tilde{m}_{\mathbf{d},2}^{(n\frac{\alpha_\epsilon}{2})}, \cdots, \tilde{m}_{\mathbf{d},1}^{(1)}, \tilde{m}_{\mathbf{d},2}^{(1)})$.

Decoding: Receiver j, $j = 1, 2$, noiselessly receives $\mathbf{X}_c^n$ using which it recovers $M_{c,j}$, $\tilde{M}_{c,j}$ and stores them in its cache. During delivery, both receivers noiselessly receive $\mathbf{X}_{\mathbf{d}}^n$ and recover $M_{\mathbf{d}}$, $\tilde{M}_{\mathbf{d}}$. Using $M_{\mathbf{d}}$, $\tilde{M}_{\mathbf{d}}$, and its cache contents, i.e., $M_{c,j}$, $\tilde{M}_{c,j}$, and for n sufficiently large, receiver j correctly recovers its desired message W_{d_j}.

Security analysis: Let us fix $S_1, S_2 \subseteq [1 : n]$. For the corresponding (fixed) values of α_1, α_2, the code $\mathcal{C}_{c,n}$ is a wiretap code with $2^{n(1-\alpha_{1,\epsilon})}$ bins. Each bin is indexed by

$$w_c = (m_c, \tilde{m}_{c,1}^{(1)}, \tilde{m}_{c,2}^{(1)}, \cdots, \tilde{m}_{c,1}^{(n\frac{\alpha_{2,\epsilon}}{2})}, \tilde{m}_{c,2}^{(n\frac{\alpha_{2,\epsilon}}{2})}), \tag{11}$$

Each bin w_c contains $2^{n\alpha_{1,\epsilon}}$ binary codewords indexed by

$$\tilde{w}_c = (\tilde{m}_{c,1}^{(n\frac{\alpha_{2,\epsilon}}{2}+1)}, \tilde{m}_{c,2}^{(n\frac{\alpha_{2,\epsilon}}{2}+1)}, \cdots, \tilde{m}_{c,1}^{(n\frac{\alpha_\epsilon}{2})}, \tilde{m}_{c,2}^{(n\frac{\alpha_\epsilon}{2})}). \tag{12}$$

Similarly, the code $\mathcal{C}_{\mathbf{d},n}$ is a wiretap code with $2^{n(1-\alpha_{2,\epsilon})}$ bins, each is indexed by

$$w_{\mathbf{d}} = (m_{\mathbf{d}}, \tilde{m}_{\mathbf{d},1}^{(n\frac{\alpha_\epsilon}{2})} \tilde{m}_{\mathbf{d},2}^{(n\frac{\alpha_\epsilon}{2})} \cdots \tilde{m}_{\mathbf{d},1}^{(n\frac{\alpha_{2,\epsilon}}{2}+1)} \tilde{m}_{\mathbf{d},2}^{(n\frac{\alpha_{2,\epsilon}}{2}+1)}) \tag{13}$$

Each bin $w_{\mathbf{d}}$ contains $2^{n\alpha_{2,\epsilon}}$ binary codewords, indexed by

$$\tilde{w}_{\mathbf{d}} = (\tilde{m}_{\mathbf{d},1}^{(n\frac{\alpha_{2,\epsilon}}{2})}, \tilde{m}_{\mathbf{d},2}^{(n\frac{\alpha_{2,\epsilon}}{2})}, \cdots, \tilde{m}_{\mathbf{d},1}^{(1)}, \tilde{m}_{\mathbf{d},2}^{(1)}). \tag{14}$$

Let $\{\mathcal{B}_{w_c}\}_{w_c=1}^{2^{n(1-\alpha_{1,\epsilon})}}$, $\{\mathcal{B}_{w_{\mathbf{d}}}\}_{w_{\mathbf{d}}=1}^{2^{n(1-\alpha_{2,\epsilon})}}$ be the partition (bins) of $\mathcal{C}_{c,n}$, $\mathcal{C}_{\mathbf{d},n}$, which correspond to w_c, $w_{\mathbf{d}}$, in (11), (13). Let $\mathbf{x}^{2n} \triangleq (\mathbf{x}_c^n, \mathbf{x}_{\mathbf{d}}^n)$ be the concatenation of $\mathbf{x}_c^n$, $\mathbf{x}_{\mathbf{d}}^n$. Define

$$\mathcal{B}_{w_c, w_{\mathbf{d}}} \triangleq \{\mathbf{x}^{2n} = (\mathbf{x}_c^n, \mathbf{x}_{\mathbf{d}}^n) : \mathbf{x}_c^n \in \mathcal{B}_{w_c}, \mathbf{x}_{\mathbf{d}}^n \in \mathcal{B}_{w_{\mathbf{d}}}\}. \tag{15}$$

Since the partitioning of $\mathcal{C}_{c,n}$, $\mathcal{C}_{\mathbf{d},n}$, is random, each $\mathcal{B}_{w_c, w_{\mathbf{d}}}$ is a random code resulting from the Cartesian product of the random bins $\mathcal{B}_{w_c}, \mathcal{B}_{w_{\mathbf{d}}}$ and contains $2^{n\alpha_\epsilon}$ length-$2n$ codewords.

Let W_c, $\tilde{W}_c$, $W_{\mathbf{d}}$, $\tilde{W}_{\mathbf{d}}$, be the random variables corresponding to the realizations in (11)-(14). $\tilde{W}_c$ and $\tilde{W}_{\mathbf{d}}$ are independent and uniformly distributed, and hence $\{\tilde{W}_c, \tilde{W}_{\mathbf{d}}\}$ is jointly uniform. In addition, $\{W_c, W_{\mathbf{d}}\}$ are independent from $\{\tilde{W}_c, \tilde{W}_{\mathbf{d}}\}$. We thus can apply [4, (94)-(103)] to show that,

for every S_1, S_2, $w_c, w_{\mathbf{d}}$, $\epsilon > 0$, and some $\gamma > 0$,

$$\mathbb{P}_{\mathcal{B}_{w_c,w_{\mathbf{d}}}}(\mathbb{D}(P_{\mathbf{Z}^n_{S_1}\mathbf{Z}^n_{S_2}|W_c=w_c,W_{\mathbf{d}}=w_{\mathbf{d}}}||P_{\mathbf{Z}^n_{S_1}\mathbf{Z}^n_{S_2}}) > \epsilon) \leq e^{-e^{n\gamma}} \tag{16}$$

$P_{\mathbf{Z}^n_{S_1}\mathbf{Z}^n_{S_2}|W_c=w_c,W_{\mathbf{d}}=w_{\mathbf{d}}}$ is the induced distribution at the adversary when $\mathbf{x}^n_c(w_c,\tilde{w}_c)$, $\mathbf{x}^n_{\mathbf{d}}(w_{\mathbf{d}},\tilde{w}_{\mathbf{d}})$ are the transmitted signals and $P_{\mathbf{Z}^n_{S_1}\mathbf{Z}^n_{S_2}}$ is the output distribution at the adversary. The number of messages $w_c, w_{\mathbf{d}}$ is $2^{n(2-\alpha_\epsilon)}$ and the number of subsets S_1, S_2 is $\binom{2n}{\alpha n} < 2^{2n}$; their combined number is at most exponential in n. Using (16) and the union bound [5],

$$\lim_{n\to\infty} \max_{S_1,S_2} I(W_c, W_{\mathbf{d}}; \mathbf{Z}^n_{S_1}, \mathbf{Z}^n_{S_2}) = 0. \tag{17}$$

Let $\{W^{(1)}_{d_j,s} \cdots W^{(n\frac{\alpha_\epsilon}{2})}_{d_j,s}\}$, $\{K^{(1)}_j \cdots K^{(n\frac{\alpha_\epsilon}{2})}_j\}$ denote the bit strings of $W_{d_j,s}$, K_j, $j = 1, 2$. For simplicity, define

$$\mathbf{W}^{(1)}_s = \{W^{(i)}_{d_1,s}, W^{(i)}_{d_2,s}\}_{i=1}^{n\frac{\alpha_{2,\epsilon}}{2}},$$
$$\mathbf{W}^{(2)}_s = \{W^{(i)}_{d_1,s}, W^{(i)}_{d_2,s}\}_{i=n\frac{\alpha_{2,\epsilon}}{2}+1}^{n\frac{\alpha_\epsilon}{2}}$$
$$\mathbf{K}^{(1)} = \{K^{(i)}_1, K^{(i)}_2\}_{i=1}^{n\frac{\alpha_{2,\epsilon}}{2}},\ \mathbf{K}^{(2)} = \{K^{(i)}_1, K^{(i)}_2\}_{i=n\frac{\alpha_{2,\epsilon}}{2}+1}^{n\frac{\alpha_\epsilon}{2}}$$
$$\mathbf{W}^{(1)}_{\oplus\mathbf{K}} = \{W^{(i)}_{d_1,s} \oplus K^{(i)}_1, W^{(i)}_{d_2,s} \oplus K^{(i)}_2\}_{i=1}^{n\frac{\alpha_{2,\epsilon}}{2}}$$
$$\mathbf{W}^{(2)}_{\oplus\mathbf{K}} = \{W^{(i)}_{d_1,s} \oplus K^{(i)}_1, W^{(i)}_{d_2,s} \oplus K^{(i)}_2\}_{i=n\frac{\alpha_{2,\epsilon}}{2}+1}^{n\frac{\alpha_\epsilon}{2}}.$$

For any demand vector $\mathbf{d} = (d_1, d_2)$, we have

$$I(W_{[1:D]}; \mathbf{Z}^n_{S_1}, \mathbf{Z}^n_{S_2})$$
$$= I(\{W^{(1)}_l, W^{(2)}_l, W_{l,t}, W_{l,s}\}_{l=1}^D; \mathbf{Z}^n_{S_1}, \mathbf{Z}^n_{S_2}) \tag{18}$$
$$\leq I(M_c, \{W^{(1)}_l, W^{(2)}_l, W_{l,t}, W_{l,s}\}_{l=1}^D; \mathbf{Z}^n_{S_1}, \mathbf{Z}^n_{S_2}) \tag{19}$$
$$\leq I(M_c, W^{(1)}_{d_2} \oplus W^{(2)}_{d_1}, W_{d_1,t}, W_{d_2,t}, W_{d_1,s}, W_{d_2,s}; \mathbf{Z}^n_{S_1}, \mathbf{Z}^n_{S_2}) \tag{20}$$
$$= I(M_c, M_{\mathbf{d}}, W_{d_1,s}, W_{d_2,s}; \mathbf{Z}^n_{S_1}, \mathbf{Z}^n_{S_2}) \tag{21}$$
$$= I(M_c, M_{\mathbf{d}}, \mathbf{W}^{(1)}_s, \mathbf{W}^{(2)}_s; \mathbf{Z}^n_{S_1}, \mathbf{Z}^n_{S_2}) \tag{22}$$
$$\leq I(M_c, M_{\mathbf{d}}, \mathbf{W}^{(1)}_s, \mathbf{W}^{(2)}_{\oplus\mathbf{K}}; \mathbf{Z}^n_{S_1}, \mathbf{Z}^n_{S_2}) \tag{23}$$
$$= I(M_c, \mathbf{W}^{(1)}_s, W_{\mathbf{d}}; \mathbf{Z}^n_{S_1}, \mathbf{Z}^n_{S_2}) \tag{24}$$
$$= H(\mathbf{Z}^n_{S_1}, \mathbf{Z}^n_{S_2}) - H(\mathbf{Z}^n_{S_1}, \mathbf{Z}^n_{S_2}|M_c, \mathbf{W}^{(1)}_s, W_{\mathbf{d}}), \tag{25}$$

where (20) follows from the Markov chain $W_{[1:D]} - (M_c, W^{(1)}_{d_2} \oplus W^{(2)}_{d_1}, W_{d_1,t}, W_{d_2,t}, W_{d_1,s}, W_{d_2,s}) - (\mathbf{Z}^n_{S_1}, \mathbf{Z}^n_{S_2})$; (21) follows from (9); (23) follows due to the Markov chain $\mathbf{W}^{(2)}_s - (M_c, M_{\mathbf{d}}, \mathbf{W}^{(1)}_s, \mathbf{W}^{(2)}_{\oplus\mathbf{K}}) - (\mathbf{Z}^n_{S_1}, \mathbf{Z}^n_{S_2})$, which holds because $\{M_c, M_{\mathbf{d}}, \mathbf{W}^{(1)}_s\}$, $\{\mathbf{W}^{(2)}_s, \mathbf{K}^{(2)}\}$ are independent and only the encrypted information $\mathbf{W}^{(2)}_{\oplus\mathbf{K}}$ is transmitted.

The second term on the RHS of (25) is lower bounded as

$$H(\mathbf{Z}^n_{S_1}, \mathbf{Z}^n_{S_2}|M_c, \mathbf{W}^{(1)}_s, W_{\mathbf{d}})$$
$$= H(\mathbf{Z}^n_{S_1}, \mathbf{Z}^n_{S_2}, \mathbf{W}^{(1)}_s|M_c, W_{\mathbf{d}}) - H(\mathbf{W}^{(1)}_s|M_c, W_{\mathbf{d}}) \tag{26}$$
$$= H(\mathbf{Z}^n_{S_1}, \mathbf{Z}^n_{S_2}, \mathbf{W}^{(1)}_s, \mathbf{W}^{(1)}_{\oplus K}|M_c, W_{\mathbf{d}}) - H(\mathbf{W}^{(1)}_{\oplus K}|M_c, W_{\mathbf{d}}, \mathbf{W}^{(1)}_s, \mathbf{Z}^n_{S_1}, \mathbf{Z}^n_{S_2}) - H(\mathbf{W}^{(1)}_s) \tag{27}$$
$$= H(\mathbf{Z}^n_{S_1}, \mathbf{Z}^n_{S_2}, \mathbf{K}^{(1)}, \mathbf{W}^{(1)}_{\oplus K}|M_c, W_{\mathbf{d}}) - H(\mathbf{K}^{(1)}|M_c, W_{\mathbf{d}}, \mathbf{W}^{(1)}_s, \mathbf{Z}^n_{S_1}, \mathbf{Z}^n_{S_2}) - H(\mathbf{W}^{(1)}_s) \tag{28}$$
$$\geq H(\mathbf{Z}^n_{S_1}, \mathbf{Z}^n_{S_2}, \mathbf{K}^{(1)}, \mathbf{W}^{(1)}_{\oplus K}|M_c, W_{\mathbf{d}}) - H(\mathbf{W}^{(1)}_s) - \epsilon'_n \tag{29}$$
$$\geq H(\mathbf{K}^{(1)}|M_c, W_{\mathbf{d}}) + H(\mathbf{Z}^n_{S_1}, \mathbf{Z}^n_{S_2}, |M_c, \mathbf{K}^{(1)}, W_{\mathbf{d}}) - H(\mathbf{W}^{(1)}_s) - \epsilon'_n \tag{30}$$
$$= H(\mathbf{Z}^n_{S_1}, \mathbf{Z}^n_{S_2}|W_c, W_{\mathbf{d}}) + H(\mathbf{K}^{(1)}) - H(\mathbf{W}^{(1)}_s) - \epsilon'_n \tag{31}$$
$$= H(\mathbf{Z}^n_{S_1}, \mathbf{Z}^n_{S_2}, |W_c, W_{\mathbf{d}}) - \epsilon'_n, \tag{32}$$

(27) follows since $\mathbf{W}^{(1)}_s$, $\{M_c, W_{\mathbf{d}}\}$ are independent; (28) follows because there is a bijection between $\{\mathbf{W}^{(1)}_s, \mathbf{W}^{(1)}_{\oplus K}\}$ and $\{\mathbf{K}^{(1)}, \mathbf{W}^{(1)}_{\oplus K}\}$; (31) follows since $\mathbf{K}^{(1)}$, $\{M_c, W_{\mathbf{d}}\}$, are independent; (32) follows since $\mathbf{K}^{(1)}$ and $\mathbf{W}^{(1)}_s$ are independent and identically distributed. The inequality in (28) follows because, given $\{M_c, \mathbf{W}^{(1)}_s, W_{\mathbf{d}}\}$, and for sufficiently large n, the adversary can decode $\mathbf{K}^{(1)}$ using $\mathbf{Z}^n_{S_1}, \mathbf{Z}^n_{S_2}$. In particular, $\{M_c, \mathbf{W}^{(1)}_s, W_{\mathbf{d}}\}$ determine a partition of the code into bins, each of which contains $2^{n\alpha_\epsilon}$ binary codewords. For n sufficiently large, and given the values of M_c, $\mathbf{W}^{(1)}_s$, and $W_{\mathbf{d}}$, i.e., the bin index, the adversary can determine the codeword index inside the bin, and hence decode $\mathbf{K}^{(1)}$. Thus, $H(\mathbf{K}^{(1)}|M_c, W_{\mathbf{d}}, \mathbf{W}^{(1)}_s, \mathbf{Z}^n_{S_1}, \mathbf{Z}^n_{S_2}) \leq \epsilon'_n$; $\epsilon'_n \to 0$ as $n \to \infty$.

By substituting (32) in (25), and using (17), the secrecy constraint in (3) is satisfied. With $\epsilon_n \to 0$ as $n \to \infty$, the achievable strong secrecy file rate is given by

$$R_s(\alpha) = 2 \times \frac{1-\alpha}{2D} + \frac{(2D-1)(1-\alpha)}{4D} + \frac{\alpha}{2}$$
$$= \frac{1}{2} + \frac{3(1-\alpha)}{4D}. \tag{33}$$

Remark 4 Utilizing coded placement and uncoded delivery for $D \geq 3$, as we did in [9] for $D = 2$, can be shown to achieve a strong secrecy file rate of $\frac{1}{2} + \frac{1-\alpha}{2(D-1)}$. This secrecy rate is equal to (33) when $D = 3$, but it is strictly smaller than (33) for $D \geq 4$.

B. Achievability for $\alpha \in [1, 2]$:

For $\alpha \in [1, 2]$, we adapt the achievability scheme in Section IV-A as follows. The messages $W_1, W_2, \cdots, W_D$ are uniformly distributed over $[1 : 2^{n\frac{2-\alpha_\epsilon}{2}}]$; α_ϵ is defined as in Section IV-A. The transmitter randomly, and independently from $W_{[1:D]}$, generates the independent keys K_1, K_2, each is uniformly distributed over $[1 : 2^{n\frac{2-\alpha_\epsilon}{2}}]$. In addition, the transmitter randomly, and independently from $W_{[1:D]}$, K_1, K_2, generates the independent randomization messages $\tilde{W}, \tilde{W}_K$, each is uniformly distributed over $[1 : 2^{n(\alpha_\epsilon - 1)}]$.

The messages to be transmitted during placement and stored in the caches of the receivers are $M_{c,1} = K_1$, $M_{c,2} = K_2$; receiver j, $j = 1, 2$, stores K_j in its cache. For $\mathbf{d} = (d_1, d_2)$, the message to be transmitted during the delivery is

$$M_{\mathbf{d}} = \{M_{\mathbf{d},1}, M_{\mathbf{d},2}\};$$
$$M_{\mathbf{d},1} = W_{d_1} \oplus K_1, \qquad M_{\mathbf{d},2} = W_{d_2} \oplus K_2. \tag{34}$$

Let $\{W_{d_j}^{(1)},\cdots,W_{d_j}^{(n\frac{2-\alpha_\epsilon}{2})}\}$, $\{K_j^{(1)},\cdots,K_j^{(n\frac{2-\alpha_\epsilon}{2})}\}$, and $\{M_{\mathbf{d},j}^{(1)},\cdots,M_{\mathbf{d},j}^{(n\frac{2-\alpha_\epsilon}{2})}\}$ denote the bit strings of W_{d_j}, K_j, $M_{\mathbf{d},j}$; $j=1,2$.

Notice that, for $\alpha\in[1,2]$, the adversary can see either all transmitted symbols in cache placement, or all transmitted symbols in delivery. Thus, unlike Section IV-A, for this case, the randomization messages in both phases, $\tilde{W},\tilde{W}_K$, are not utilized to carry any information, and only key bits are stored in the cache memories. Additionally, the cache placement and delivery codebooks for this case have a different embedding structure than for $\alpha\in(0,1)$ in Section IV-A. In particular, the embedding here is performed on the bits of the messages $M_c, M_{\mathbf{d}}$, while the embedding in Section IV-A is performed on the bits of the randomization messages $\tilde{M}_c$, $\tilde{M}_{\mathbf{d}}$.

Cache Code Generation: The transmitter generates the code $\mathcal{C}_{c,n}$ as follows. The transmitter randomly and independently divide all the possible 2^n length-n binary sequences into 2 bins, indexed by $K_1^{(1)}$, and each contains 2^{n-1} binary codewords. These two bins are further randomly and independently divided into two sub-bins, indexed by $K_2^{(1)}$, and each contains 2^{n-2} binary codewords. The process continues, going over $K_1^{(2)}$, $K_2^{(2)}$, $\cdots$, $K_1^{(n\frac{2-\alpha_\epsilon}{2})}$, $K_2^{(n\frac{2-\alpha_\epsilon}{2})}$, until the remaining $2^{n(\alpha_\epsilon-1)}$ codewords, after each sequence of divisions, are indexed by the randomization message $\tilde{W}_K$.

Cache Encoder: The transmitter sends the binary codeword $\mathbf{X}_c^n$ which corresponds to the keys K_1,K_2, and the message $\tilde{W}_K$, i.e., $\mathbf{X}_c^n(K_1^{(1)},K_2^{(1)},\cdots,K_1^{(n\frac{2-\alpha_\epsilon}{2})},K_2^{(n\frac{2-\alpha_\epsilon}{2})},\tilde{W}_K)$.

Delivery Code Generation: For $\mathbf{d}=(d_1,d_2)$, the transmitter generates the code $\mathcal{C}_{\mathbf{d},n}$ as follows. The transmitter randomly and independently divides all the 2^n length-n binary sequences into 2 bins, indexed by $M_{\mathbf{d},1}^{(n\frac{2-\alpha_\epsilon}{2})}$, and each contains 2^{n-1} codewords. These two bins are further randomly and independently divided into two sub-bins, indexed by $M_{\mathbf{d},2}^{(n\frac{2-\alpha_\epsilon}{2})}$, and each contains 2^{n-2} codewords. The process continues, going in reverse order over $M_{\mathbf{d},1}^{(n\frac{2-\alpha_\epsilon}{2}-1)}$, $M_{\mathbf{d},2}^{(n\frac{2-\alpha_\epsilon}{2}-1)}$, $\cdots$, $M_{\mathbf{d},1}^{(1)}$, $M_{\mathbf{d},2}^{(1)}$, until the remaining $2^{n(\alpha_\epsilon-1)}$ codewords, after each sequence of divisions, are indexed by the message $\tilde{W}$.

Delivery Encoder: Given $W_{[1:D]}$, $\mathbf{d}=(d_1,d_2)$, K_1, K_2, and $\tilde{W}$, the transmitter forms $M_{\mathbf{d},1}$, $M_{\mathbf{d},2}$ as in (34), and sends the binary codeword $\mathbf{X}_{\mathbf{d}}^n$ which corresponds to $M_{\mathbf{d},1}$, $M_{\mathbf{d},2}$, $\tilde{W}$, i.e., $\mathbf{X}_{\mathbf{d}}^n(M_{\mathbf{d},1}^{(n\frac{2-\alpha_\epsilon}{2})},M_{\mathbf{d},2}^{(n\frac{2-\alpha_\epsilon}{2})},\cdots,M_{\mathbf{d},1}^{(1)},M_{\mathbf{d},2}^{(1)},\tilde{W})$.

Decoding: Using $\mathbf{X}_c^n$, receiver j recovers $M_{c,j}=K_j$ and stores it in its cache memory. The size of K_j is less than $\frac{n}{2}$ bits. Using $\mathbf{X}_{\mathbf{d}}^n$, both receivers recover $M_{\mathbf{d}}=\{M_{\mathbf{d},1},M_{\mathbf{d},2}\}$. Using $M_{\mathbf{d},j}$ and K_j, and for n sufficiently large, receiver j correctly decodes its desired message, W_{d_j}.

Security Analysis: Fix S_1,S_2. Recall that $\alpha_1,\alpha_2\le 1$. Since $\alpha\ge 1$, we have $\alpha_1,\alpha_2\ge\alpha-1$. If $\alpha_1=1$, then $\alpha_2=\alpha-1$, and vice versa. In addition, notice that $1-\alpha_1,1-\alpha_2\le 2-\alpha$.

As in Section IV-A, for a fixed value of α_1, the code $\mathcal{C}_{c,n}$ is a wiretap code with $2^{n(1-\alpha_{1,\epsilon})}$ bins, indexed by

$$W_c=(K_1^{(1)},K_2^{(1)},\cdots,K_1^{(n\frac{1-\alpha_{1,\epsilon}}{2})},K_2^{(n\frac{1-\alpha_{1,\epsilon}}{2})}). \tag{35}$$

Each bin W_c contains $2^{n\alpha_{1,\epsilon}}$ binary codewords, indexed by

$$\tilde{W}_c=(K_1^{(n\frac{1-\alpha_{1,\epsilon}}{2}+1)},K_2^{(n\frac{1-\alpha_{1,\epsilon}}{2}+1)},\cdots,K_1^{(n\frac{2-\alpha_\epsilon}{2})},K_2^{(n\frac{2-\alpha_\epsilon}{2})},\tilde{W}_K). \tag{36}$$

Similarly, for a fixed value of α_2, the delivery code $\mathcal{C}_{\mathbf{d},n}$ is a wiretap code with $2^{n(1-\alpha_{2,\epsilon})}$ bins, each is indexed by

$$W_{\mathbf{d}}=(\tilde{M}_{\mathbf{d},1}^{(n\frac{2-\alpha_\epsilon}{2})},\tilde{M}_{\mathbf{d},2}^{(n\frac{2-\alpha_\epsilon}{2})},\cdots,\tilde{M}_{\mathbf{d},1}^{(n\frac{1-\alpha_{1,\epsilon}}{2}+1)},\tilde{M}_{\mathbf{d},2}^{(n\frac{1-\alpha_{1,\epsilon}}{2}+1)}). \tag{37}$$

Each bin $W_{\mathbf{d}}$ contains $2^{n\alpha_{2,\epsilon}}$ codewords, indexed by

$$\tilde{W}_{\mathbf{d}}=(\tilde{M}_{\mathbf{d},1}^{(n\frac{1-\alpha_{1,\epsilon}}{2})},\tilde{M}_{\mathbf{d},2}^{(n\frac{1-\alpha_{1,\epsilon}}{2})},\cdots,\tilde{M}_{\mathbf{d},1}^{(1)},\tilde{M}_{\mathbf{d},2}^{(1)},\tilde{W}). \tag{38}$$

For notational simplicity, let us define

$$\mathbf{W}^{(1)}=\{W_{d_1}^{(i)},W_{d_2}^{(i)}\}_{i=1}^{n\frac{1-\alpha_{1,\epsilon}}{2}},$$
$$\mathbf{W}^{(2)}=\{W_{d_1}^{(i)},W_{d_2}^{(i)}\}_{i=n\frac{1-\alpha_{1,\epsilon}}{2}+1}^{n\frac{2-\alpha_\epsilon}{2}}$$
$$\mathbf{K}^{(1)}=\{K_1^{(i)},K_2^{(i)}\}_{i=1}^{n\frac{1-\alpha_{1,\epsilon}}{2}},\mathbf{K}^{(2)}=\{K_1^{(i)},K_2^{(i)}\}_{i=n\frac{1-\alpha_{1,\epsilon}}{2}+1}^{n\frac{2-\alpha_\epsilon}{2}}$$
$$\mathbf{W}_{\oplus\mathbf{K}}^{(1)}=\{W_{d_1}^{(i)}\oplus K_1^{(i)},W_{d_2}^{(i)}\oplus K_2^{(i)}\}_{i=1}^{n\frac{1-\alpha_{1,\epsilon}}{2}},$$
$$\mathbf{W}_{\oplus\mathbf{K}}^{(2)}=\{W_{d_1}^{(i)}\oplus K_1^{(i)},W_{d_2}^{(i)}\oplus K_2^{(i)}\}_{i=n\frac{1-\alpha_{1,\epsilon}}{2}+1}^{n\frac{2-\alpha_\epsilon}{2}}.$$

Similar to Section IV-A, $\tilde{W}_c$ and $\tilde{W}_{\mathbf{d}}$ are independent and uniform, and hence, $\{\tilde{W}_c,\tilde{W}_{\mathbf{d}}\}$ is jointly uniform. In addition, $\{\tilde{W}_c,\tilde{W}_{\mathbf{d}}\}$ is independent from $\{W_c,W_{\mathbf{d}}\}$. Thus, (17) holds for this case as well. We also have

$$\begin{aligned}
I(W_{[1:D]};\mathbf{Z}_{S_1}^n,\mathbf{Z}_{S_2}^n)&=I(W_{d_1},W_{d_2};\mathbf{Z}_{S_1}^n,\mathbf{Z}_{S_2}^n) &(39)\\
&=I(\mathbf{W}^{(1)},\mathbf{W}^{(2)};\mathbf{Z}_{S_1}^n,\mathbf{Z}_{S_2}^n) &(40)\\
&\le I(\mathbf{W}^{(1)},\mathbf{W}_{\oplus\mathbf{K}}^{(2)};\mathbf{Z}_{S_1}^n,\mathbf{Z}_{S_2}^n) &(41)\\
&=I(\mathbf{W}^{(1)},W_{\mathbf{d}};\mathbf{Z}_{S_1}^n,\mathbf{Z}_{S_2}^n) &(42)\\
&=H(\mathbf{Z}_{S_1}^n,\mathbf{Z}_{S_2}^n)-H(\mathbf{Z}_{S_1}^n,\mathbf{Z}_{S_2}^n|\mathbf{W}^{(1)},W_{\mathbf{d}}) &(43)\\
&\le H(\mathbf{Z}_{S_1}^n,\mathbf{Z}_{S_2}^n)-H(\mathbf{Z}_{S_1}^n,\mathbf{Z}_{S_2}^n|\mathbf{K}^{(1)},W_{\mathbf{d}})+\epsilon_n' &(44)\\
&=I(W_c,W_{\mathbf{d}};\mathbf{Z}_{S_1}^n,\mathbf{Z}_{S_2}^n)+\epsilon_n', &(45)
\end{aligned}$$

where (41) follows due to the Markov chain $\mathbf{W}^{(2)}-\{\mathbf{W}^{(1)},\mathbf{W}_{\oplus\mathbf{K}}^{(2)}\}-\{\mathbf{Z}_{S_1}^n,\mathbf{Z}_{S_2}^n\}$ and (44) follows using similar steps as in (26)-(32). Using (17) and (45), the secrecy constraint in (3) is satisfied. Since $\epsilon_n\to 0$ as $n\to\infty$, the achievable strong secrecy file rate is given by

$$R_s(\alpha)=\frac{2-\alpha}{2}=1-\frac{\alpha}{2}, \tag{46}$$

which completes the proof for Theorem 1.

V. Proof of Theorem 2

When $\alpha\in[1,2]$, the upper bound on $R_s(\alpha)$ in (5) is derived as follows. When the demand vector $\mathbf{d}\in[1:D]^2$ is known to the transmitter during cache placement, the model in Fig. 1 reduces to a broadcast wiretap II channel over a length-$2n$ communication block, whose sum secrecy capacity is given

by $C_{s,\text{sum}}(\alpha) = 2-\alpha$, which follows from [7, Thm. 1]. Since the demand vector is unknown for the model in consideration, and by considering the worst case demands, i.e., $\mathbf{d} = (d_1, d_2)$ where $d_1 \neq d_2$, $1-\frac{\alpha}{2}$ is an upper bound for the model in Fig. 1. Thus, it remains to prove the upper bound for $\alpha \in (0,1)$. The proof is divided into the three following steps.

Step 1: We first upper bound R_s by the strong secrecy capacity when the adversary is restricted to tap into the delivery transmission only, denoted as C_s^{Res}. That is, C_s^{Res} is the strong secrecy capacity when $\alpha_1 = 0$ and $\alpha_2 = \alpha$. Restricting the adversary to only tap into the delivery phase cannot decrease the strong secrecy capacity of the model, i.e., $R_s \leq C_s^{\text{Res}}$, since this setting is included in the feasible strategy space for the adversary. The cache placement transmission is thus secure, and each receiver has a secure cache of size $\frac{n}{2}$ bits.

Step 2: The secrecy capacity of the restricted adversary model, C_s^{Res}, is upper bounded by the secrecy capacity when the delivery channel to the adversary is replaced by a discrete memoryless binary erasure channel with erasure probability $1-\alpha$, denoted as C_s^{DM}. The proof for this step follows the same lines as in [5, Sec. V]. The idea is when the binary erasure channel produces a number of erasures greater than or equal to $(1-\alpha)n$, the adversary's channel in this discrete memoryless setup is worse than its channel in the former model, i.e., when it encounters exactly $(1-\alpha)n$ erasures and is able to select their positions. Hence, we have $C_s^{\text{Res}} \leq C_s^{\text{DM}}$ for this case. The result follows by using Sanov's theorem in method of types [26, Thm. 11.4.1] to show that the probability of the binary erasure channel causing a number of erasures less than $(1-\alpha)n$ goes to zero as $n \to \infty$.

Step 3: The receivers in the original model have cache memories of size $\frac{n}{2}$ bits each. Since increasing the cache sizes cannot decrease the secrecy capacity, we further upper bound C_s^{DM} with the secrecy capacity when each receiver has a cache memory of size n bits, in which it stores the transmitted codeword during cache placement, $\mathbf{X}_c^n$. That is, receiver j, $j = 1, 2$, utilizes both $\mathbf{X}_c^n$ and $\mathbf{X}_{\mathbf{d}}^n$ in order to decode its desired message W_{d_j}; $\hat{W}_{d_j} = g_{\mathbf{d},j}(\mathbf{X}_c^n, \mathbf{X}_{\mathbf{d}}^n)$, where $\mathbf{d} = (d_1, d_2)$. This setup is thus equivalent to a single receiver, with a cache memory of size n bits, who demands two files W_{d_1} and W_{d_2} and utilizes the decoder $g_{\mathbf{d}} \triangleq \{g_{\mathbf{d},1}, g_{\mathbf{d},2}\}$. Let us denote the secrecy capacity for this single receiver model as C_s^{SR}. We have $C_s^{\text{DM}} \leq C_s^{\text{SR}}$. In the following, we upper bound the secrecy capacity for the single receiver model, C_s^{SR}.

Let M_D denote the fraction of the size-n bits cache memory dedicated to store (coded or uncoded) information bits, and let M_K denote the fraction dedicated to store key bits. That is, $M_D + M_K = 1$. Let S_D denote the information bits stored in this memory, i.e., $S_D = f(W_{[1:D]})$ and $H(S_D) = nM_D$. We utilize the following lemma in order to upper bound C_s^{SR}.

Lemma 1 *[20, Lemma 1] For a fixed allocation of M_{D}, M_{K}, and a receiver which demands W_{d_1}, W_{d_2}, the secrecy rate for the single receiver model is upper bounded as*

$$2R_s^{\text{SR}} \leq \min\{1, 1-\alpha+M_{\text{K}}\} + \frac{1}{n} I(W_{d_1}, W_{d_2}; S_{\text{D}}). \quad (47)$$

Notice that (47) holds for any $\mathbf{d} = (d_1, d_2)$ such that $d_1 \neq d_2$, i.e., the worst-case demands. Summing over all such demands, we have

$$2R_s^{\text{SR}} \leq \min\{1, 1-\alpha+M_{\text{K}}\} + \frac{1}{nD(D-1)} \sum_{d_1,d_2\in[1:D],\ d_1\neq d_2} I(W_{d_1}, W_{d_2}; S_{\text{D}}). \quad (48)$$

The second term on the right hand side of (48) can be written as

$$\frac{1}{nD} \sum_{d_1\in[1:D]} I(W_{d_1}; S_{\text{D}}) + \frac{1}{nD(D-1)} \sum_{d_1,d_2\in[1:D],\ d_1\neq d_2} I(W_{d_2}; S_{\text{D}}|W_{d_1}) \quad (49)$$

$$\leq \frac{1}{nD} \sum_{d_1\in[1:D]} I(W_{d_1}; S_{\text{D}}) + \frac{1}{nD(D-1)} \sum_{d_1\in[1:D]} \Big(\sum_{d_2\in[1:D]} I(W_{d_2}; S_{\text{D}}|W_{d_1}) \Big). \quad (50)$$

For any $d_1 \in [1:D]$, we have

$$\sum_{d_2\in[1:D]} I(W_{d_2}; S_D|W_{d_1}) = \sum_{d_2=1}^{D} \big[H(W_{d_2}|W_{d_1}) - H(W_{d_2}|W_{d_1}, S_D)\big] \quad (51)$$

$$\leq \sum_{d_2=1}^{D} \big[H(W_{d_2}|W_1, W_2, \cdots, W_{d_2-1}, W_{d_1}) - H(W_{d_2}|W_1, W_2, \cdots, W_{d_2-1}, W_{d_1}, S_D)\big] \quad (52)$$

$$= I(W_1, W_2, \cdots, W_D; S_D|W_{d_1}) \quad (53)$$

$$\leq H(S_D) = nM_D, \quad (54)$$

where (52) follows because when $d_2 = d_1$, $H(W_{d_2}|W_{d_1}) = H(W_{d_2}|W_1, \cdots, W_{d_2-1}, W_{d_1}) = 0$, and when $d_2 \neq d_1$, $H(W_{d_2}|W_{d_1}) = H(W_{d_2}|W_1, \cdots, W_{d_2-1}, W_{d_1}) = H(W_{d_2})$.

Similarly, we have

$$\sum_{d_1\in[1:D]} I(W_{d_1}; S_{\text{D}}) \leq H(S_{\text{D}}) = nM_{\text{D}}. \quad (55)$$

By substituting (54) and (55) in (50), the second term on the right hand side of (48) is upper bounded by $\frac{2D-1}{D(D-1)} M_{\text{D}}$. Thus, using (48), R_s^{SR} is further upper bounded as

$$R_s^{\text{SR}} \leq \frac{1}{2} \left[\min\{1, 1-\alpha+M_{\text{K}}\} + \frac{2D-1}{D(D-1)} M_{\text{D}} \right]. \quad (56)$$

Finally, by maximizing over all possible allocations for M_{D} and M_{K} such that $M_{\text{D}} + M_{\text{K}} = 1$, we obtain

$$C_s^{\text{SR}} \leq \frac{1}{2} \max_{\substack{M_{\text{D}}, M_{\text{K}}: \\ M_{\text{D}}+M_{\text{K}}=1}} \Big\{ \min\{1, 1-\alpha+M_{\text{K}}\} + \frac{2D-1}{D(D-1)} M_{\text{D}} \Big\} \quad (57)$$

$$= \frac{1}{2}\left[1 + \frac{2D-1}{D(D-1)}(1-\alpha)\right]. \quad (58)$$

Equation (58) follows because, for $D \geq 3$, the maximum occurs at $M_{\rm K} = \alpha$ and $M_{\rm D} = 1 - \alpha$. This completes the proof for Theorem 2.

VI. Conclusion and Discussion

We have considered the caching broadcast channel with a *wire and cache* tapping adversary of type II introduced in [9] and extended its analysis to a library of size $D \geq 3$ files. In this broadcast model, each receiver is equipped with a fixed-size cache memory, and the adversary is able to tap into a subset of its choosing of the transmitted symbols during cache placement, delivery, or both. The legitimate terminals have no knowledge about the fractions of the tapped symbols in either phase, or their positions. Only the size of the overall tapped set is known. We have derived lower and upper bounds on the strong secrecy file rate for $D \geq 3$. We have utilized an achievability scheme which combines uncoded placement, coded delivery, wiretap coding, security embedding codes, and one-time pad keys. Future directions of this work include investigating a tighter upper bound for $D \geq 3$, and exploring the extensions of this work to more than two users and to a noisy legitimate channel.

While the fixed-size cache memory setup considered in this paper can be viewed as a clean basic model for the intricate problem in consideration, it also allows us to obtain results and insights that are generalizable to more involved cache memory models. In particular, the extension to variable memory sizes can be done by considering multiple communication blocks for cache placement. Our results and coding scheme readily apply to an adversary model whose tapping capability during the delivery is normalized with respect to tapping during cache placement, i.e., $\mu_1 + B\mu_2 \leq \mu$; B is the number of communication blocks for cache placement. This is a reasonable assumption given that cache placement generally takes place a longer period than delivery. The problem turns to be more challenging when the adversary optimizes its tapping uniformly over the multiple blocks for cache placement as well as the delivery phase. This is left for future investigation.

Corollary 1 shows that for the model in consideration, when $\alpha \in [1, 2]$, the strong secrecy capacity is equal to $1 - \frac{\alpha}{2}$ for any library size. For $\alpha \in [1, 2]$, $\{S_1 = [1 : n], S_2 \subset [1 : n]\}$, $\{S_1 \subset [1 : n], S_2 = [1 : n]\}$, are two possible strategies for the adversary, i.e., the adversary can tap into either all transmitted symbols in placement and a subset of symbols in delivery, or all transmitted symbols in delivery and a subset of symbols in placement. Such an adversary limits the the use of cache memories to exchanging additional randomness (key bits) that allows for communicating a positive secure rate over the two phases. That is, the cache memories are not utilized to store any data bits, and hence the lack of knowledge of user demands during cache placement is immaterial.

References

[1] A. D. Wyner, "The wire-tap channel," *Bell Sys. Tech. Jour.*, vol. 54, no. 8, pp. 1355–1387, 1975.

[2] L. Ozarow and A. D. Wyner, "Wire-tap channel II," *Bell Sys. Tech. Jour.*, vol. 63, no. 10, pp. 2135–2157, 1984.

[3] M. Nafea and A. Yener, "Wiretap channel II with a noisy main channel," in *IEEE Inter. Symp. Info. Theory*, June 2015.

[4] Z. Goldfeld, P. Cuff, and H. H. Permuter, "Semantic-security capacity for wiretap channels of type II," *IEEE Trans. Info. Theory*, vol. 62, no. 7, pp. 3863–3879, 2016.

[5] M. Nafea and A. Yener, "A new wiretap channel model and its strong secrecy capacity," *IEEE Trans. Info. Theory*, vol. 64, no. 3, pp. 2077–2092, 2018.

[6] ——, "Generalizing multiple access wiretap and wiretap II channel models: Achievable rates and cost of strong secrecy," *Submitted to IEEE Transactions on Information Theory*, January 2018, arXiv preprint arXiv:1802.02131.

[7] ——, "A new broadcast wiretap channel model," in *IEEE Inter. Symp. Info. Theory*, June 2017.

[8] ——, "New models for the interference and broadcast channels with confidential messages," in *IEEE Inter. Symp. Info. Theory*, June 2017.

[9] ——, "The caching broadcast channel with a wire and cache tapping adversary of type II," in *IEEE Info. Theory Workshop*, Nov. 2018.

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

[11] R. Pedarsani, M. A. Maddah-Ali, and U. Niesen, "Online coded caching," *IEEE/ACM Trans. Netw.*, vol. 24, no. 2, pp. 836–845, 2016.

[12] K. Wan, D. Tuninetti, and P. Piantanida, "On caching with more users than files," in *IEEE Inter. Symp. Info. Theory*, July 2016.

[13] M. Amiri and D. Gündüz, "Cache-aided content delivery over erasure broadcast channels," *IEEE Trans. Comm.*, vol. 66, no. 1, pp. 370–381, 2018.

[14] S. S. Bidokhti, M. Wigger, and A. Yener, "Benefits of cache assignment on degraded broadcast channels," *Submitted to IEEE Trans. Info. Theory*, 2017, arXiv preprint arXiv:1702.08044.

[15] A. A. Zewail and A. Yener, "Combination networks with or without secrecy constraints: The impact of caching relays," *IEEE Jour. Selec. Areas in Commun.*, vol. 36, no. 6, pp. 1–13, 2018.

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

[17] A. A. Zewail and A. Yener, "Fundamental limits of secure device-to-device coded caching," in *Asilomar Conf. on Signals, Systems, Computers*, Nov. 2016.

[18] V. Ravindrakumar, P. Panda, N. Karamchandani, and V. M. Prabhakaran, "Private coded caching," *IEEE Trans. Info. Forensics, Security*, vol. 13, no. 3, pp. 685–694, 2018.

[19] S. Kamel, M. Sarkiss, M. Wigger, and G. R.-B. Othman, "Secrecy capacity-memory tradeoff of erasure broadcast channels," *arXiv preprint arXiv:1801.00606*, 2018.

[20] A. A. Zewail and A. Yener, "The wiretap channel with a cache," in *IEEE Inter. Symp. Info. Theory*, June 2018.

[21] ——, "Device-to-Device secure coded caching," *Submitted to IEEE Trans. Info. Forensics, Security*, Aug. 2018, arXiv preprint arXiv:1809.06844.

[22] C. E. Shannon, "Communication theory of secrecy systems," *Bell Labs Tech. Jour.*, vol. 28, no. 4, pp. 656–715, 1949.

[23] R. Ahlswede and I. Csiszár, "Common randomness in information theory and cryptography–Part I: Secret sharing," *IEEE Trans. Info. Theory*, vol. 39, no. 4, pp. 1121–1132, 1993.

[24] H. D. Ly, T. Liu, and Y. Blankenship, "Security embedding codes," *IEEE Trans. Info. Forensics, Security*, vol. 7, no. 1, pp. 148–159, 2012.

[25] Y. Liang, L. Lai, H. V. Poor, and S. Shamai, "A broadcast approach for fading wiretap channels," *IEEE Trans. Info. Theory*, vol. 60, no. 2, pp. 842–858, 2014.

[26] T. M. Cover and J. A. Thomas, *Elements of information theory 2nd edition*. New York, NY, USA: Wiley, 2006.

[27] C. Tian, "Symmetry, demand types and outer bounds in caching systems," in *IEEE Inter. Symp. Info. Theory*, Jul. 2016.

[28] A. M. Ibrahim, A. A. Zewail, and A. Yener, "Optimization of heterogeneous caching systems with rate limited links," in *IEEE Inter. Conf. Commun.*, May 2017.

[29] D. Cao, D. Zhang, P. Chen, N. Liu, W. Kang, and D. Gündüz, "Coded caching with heterogeneous cache sizes and link qualities: The two-user case," in *IEEE Inter. Symp. Info. Theory*, Jun. 2018.