The Caching Broadcast Channel with a Wire and Cache Tapping Adversary of Type II

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*—This paper introduces the notion of cache-tapping into information theoretic models of coded caching. In particular, the wiretap II model with two receivers equipped with fixed-size cache memories is considered. The adversary chooses a set of symbols from cache placement, delivery, or both to tap into. The legitimate parties know neither whether cache placement, delivery, or both transmissions are tapped, nor the positions of tapped symbols. Only the size of overall tapped set is known. The strong secrecy capacity, i.e., the maximum achievable file rate while keeping the overall library strongly secure, is identified for the instance of two library files. Achievability is established using a code design which combines wiretap coding, security embedding codes, one-time pad keys, and coded caching. The study overall demonstrates that information theoretic security guarantees are possible against a powerful adversary which optimizes its attack over both phases of a cache-aided communication system.**

I. Introduction

Caching is a technique proposed to reduce traffic in peak time periods through storing popular contents at end users earlier during less congested times. Reference [1] has introduced an information theoretic model of the caching problem, termed *coded caching*, and showed that, in a noiseless multi-receiver setting, by carefully designing the cache contents, the server can send delivery transmissions that are simultaneously useful for multiple users. Coded caching has since been studied for various network configurations and under various modeling assumptions, see for example [2]–[4].

Coded caching with security concerns has been recently studied in [4]–[8]. These works assume secure cache placement, i.e., the adversary can neither access the placed cache contents, nor tap into the communication that performs the placement. At the other extreme, if the adversary has perfect access to cache contents, the presence of cache memories can not increase the secrecy capacity [9]. Given these two settings, one might think of an intermediate setting in which the adversary may have partial access to the placement phase.

In this work, we consider an adversary model of type II as in [10]–[15], but in a cache-aided communication system. The adversary chooses a *fixed-size* subset of symbols from either cache placement, delivery, or both transmissions, to noiselessly observe. The legitimate terminals *do not* know whether cache placement, delivery, or both are tapped, the relative fractions of tapped symbols in both, or their positions. Only the overall size of the tapped set is known.

The challenge in caching stems from the fact that the transmitter, who has access to a library of files, has no knowledge about the future demands of the end users when designing their cache contents. This remains to be the case for security concerns. Additionally, one can envision that an adversary might tap into placement or delivery phases, and where the tapping occurs would be unknown to the legitimate parties. The question then arises whether the secrecy capacity of the model is invariant to the positions of the tapped symbols varying between cache placement and delivery. In this paper, we answer this question in the positive.

In caching literature up to date, the physical communication which populates the cache memories at end users does not need to be considered in the problem formulation, since cache placement is secure. In order to model cache placement that is tapped by an adversary, we consider length-n communication over a two-user broadcast channel. Under this assumption, the sizes of cache memories at end users are fixed. We note that introducing variable memory sizes for which a rate-memory tradeoff can be characterized, as in the usual setup for caching, requires considering additional communication blocks for placement, and is of future interest.

The contributions of this work are as follows.

- We introduce the notion of *cache-tapping* in which the adversary is able to overhear a fixed-size set of symbols either from cache placement, or delivery, or both.
- We derive the strong secrecy capacity, i.e., the maximum achievable file rate, for the instance of two library files.

Notation: For $a, b \in \mathbb{R}$, $[a:b] \triangleq \{i \in \mathbb{Z} : a \leq i \leq b\}$. $A_{[1:n]}$ is the sequence $\{A_1, \cdots, A_n\}$. $\mathcal{A}^T$ is the T-fold Cartesian product of $\mathcal{A}$. For $W_1, W_2 \in [1:M]$, $W_1 \oplus W_2$ is the integer output corresponding to the bit-wise XOR of W_1, W_2. $\mathbb{D}(p_x||q_x)$ is the Kullback-Leibler divergence between p_x, q_x.

II. System Model

Consider the communication system in Fig. 1, in which the adversary taps into both the cache placement and delivery. The transmitter observes $D \geq 2$ independent files, $W_1, W_2, \cdots, W_D$, each is uniform 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 (BC) is noiseless during both phases. The communication model is described as follows:

Cache placement phase: During this phase, the transmitter sends a length-n binary signal, $\mathbf{X}_c^n$, to both receivers. The codeword $\mathbf{X}_c^n$ is a function of the library files only, i.e.,

978-1-5386-3599-5/18/$31.00©2018 IEEE

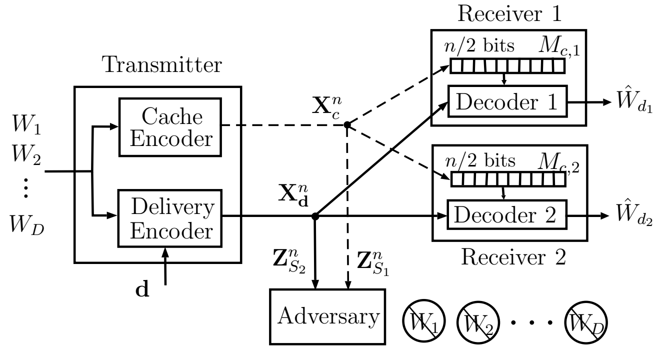

Fig. 1. The caching BC with a wire and cache tapping adversary of type II.

$\mathbf{X}_c^n \triangleq f_c(W_{[1:D]})$. The transmitter does not know the receiver demands during cache placement. Each receiver has a cache memory of size $\frac{n}{2}$ bits in which they store a function of $\mathbf{X}_c^n$, $M_{c,j} \triangleq f_{c,j}(\mathbf{X}_c^n)$; $f_{c,j} : \{0,1\}^n \mapsto [1 : 2^{\frac{n}{2}}]$ and $j = 1, 2$.

Delivery phase: The two receivers announce their demands $\mathbf{d} \triangleq (d_1, d_2) \in [1 : D]^2$ before delivery. The transmitter, in order to satisfy these demands, 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 $\mathbf{X}_{\mathbf{d}}^n \triangleq f_{\mathbf{d}}(W_{[1:D]})$.

Decoding: Receiver j uses the decoder $g_{\mathbf{d},j} : [1 : 2^{\frac{n}{2}}] \times \{0,1\}^n \mapsto [1 : 2^{nR_s}]$, in order to output the estimate $\hat{W}_{d_j} \triangleq g_{\mathbf{d},j}(f_{c,j}(\mathbf{X}_c^n), \mathbf{X}_{\mathbf{d}}^n)$ of his desired message W_{d_j}; $j = 1, 2$.

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

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

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

The legitimate parties do not know the realizations of S_1, S_2, nor the values of μ_1, μ_2. Only $\mu = \mu_1 + \mu_2$ is known. Let $\alpha_1 \triangleq \frac{\mu_1}{n}$, $\alpha_2 \triangleq \frac{\mu_2}{n}$, be the fractions of the tapped symbols in cache placement and delivery, and let $\alpha = \alpha_1 + \alpha_2$ be the overall tapped ratio. Note that $\alpha_1, \alpha_2 \in [0, 1]$ and $\alpha \in [0, 2]$.

A channel code $\mathcal{C}_{2n}$ for this model consists of (i) D message sets, (ii) cache encoder f_c, (iii) cache decoders $f_{c,j}$, $j = 1, 2$, (iv) delivery encoders $\{f_{\mathbf{d}}\}_{\mathbf{d} \in [1:D]^2}$, and (v) the decoders $\{g_{\mathbf{d},j}\}_{j=1,2,\ \mathbf{d} \in [1:D]^2}$. The file rate R_s is achievable with strong secrecy if there is a sequence $\{\mathcal{C}_{2n}\}_{n \geq 1}$ satisfying

$$\lim_{n\to\infty} \max_{\mathbf{d} \in [1:D]^2} \mathbb{P}((\hat{W}_{d_1} \neq W_{d_1}) \cup (\hat{W}_{d_2} \neq W_{d_2})) = 0, \tag{2}$$

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

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

III. Main Result

The main result of this paper is the strong secrecy capacity for the model in Section II when $D = 2$.

Theorem 1 *For $0 \leq \alpha \leq 2$ and $D = 2$, the strong secrecy capacity for the model in Section II is given by*

$$C_s(\alpha) = 1 - \frac{\alpha}{2}. \tag{4}$$

The proof for Theorem 1 is provided in Section IV.

Lower and upper bounds for the achievable strong secrecy file rate when $D > 2$ are derived in the longer version of this work [16]. The proof for the lower bound when $D > 2$ utilizes the same channel coding structure as for $D = 2$ in Section IV, but the cache placement and delivery schemes must differ. In particular, *uncoded placement and coded delivery* are utilized.

IV. Proof of Theorem 1

A. Converse

For the model in Theorem 1, when $\mathbf{d} \in \{1, 2\}^2$ is known to the transmitter during cache placement, the model reduces to a broadcast wiretap channel II over a length-$2n$ communication block, whose strong sum secrecy rate is upper bounded as

$$2R_s(\alpha) \leq 2 - \alpha, \tag{5}$$

which follows from [14, Thm. 1]. Notice that (5) holds for the worst-case demands, i.e., $d_1 \neq d_2$. Since $\mathbf{d} = (d_1, d_2)$ is unknown for the model in consideration, $1 - \frac{\alpha}{2}$ constitutes an upper bound for the strong secrecy file rate, when $D = 2$.

B. Restricted Adversary Models as Building Blocks

Before proceeding with the achievability proof for (4), it is relevant to investigate the secrecy capacity of the model when a fraction of cache placement, delivery, or both, is tapped. We thus first consider the cases where the adversary taps into (i) cache placement only, (ii) delivery only, (iii) both phases, with the relative fractions of tapped symbols in each are known. For each of these models and $\alpha \in [0, 1)$, we show that the strong secrecy capacity is identical to $1 - \frac{\alpha}{2}$. These are building blocks for the scenario in question in this paper which is when the relative fractions are *unknown*, the achievability proof of which is provided in Sections IV-C and IV-D.

1) The adversary taps into cache placement only: This setting corresponds to $\alpha_1 = \alpha$ and $\alpha_2 = 0$, i.e., $|S_1| = \mu$ and $S_2 = \varnothing$, where $\alpha \in [0, 1)$. The transmitter and receivers know the values of α_1, α_2. Let $\{\epsilon_n\}_{n \geq 1}$ denote a sequence of positive real numbers such that $\epsilon_n \to 0$ as $n \to \infty$.

The strong secrecy file rate $1 - \frac{\alpha}{2}$ is achieved as follows. The transmitter divides W_l, $l = 1, 2$, into three independent messages $\{W_l^{(1)}, W_l^{(2)}, W_{l,s}\}$. $W_l^{(1)}, W_l^{(2)}$ are uniform over $[1 : 2^{n\frac{1-\alpha-\epsilon_n}{2}}]$, and $W_{l,s}$ is uniform over $[1 : 2^{n\frac{\alpha+\epsilon_n}{2}}]$. Define $M_c \triangleq \{M_{c,1}, M_{c,2}\}$, where $M_{c,1} = W_1^{(1)} \oplus W_2^{(1)}$, $M_{c,2} = W_1^{(2)} \oplus W_2^{(2)}$, and $M_{\mathbf{d}} = \{W_{d_1}^{(2)}, W_{d_2}^{(1)}, W_{d_1,s}, W_{d_2,s}\}$.

During cache placement, the transmitter encodes M_c into $\mathbf{X}_c^n$ using wiretap coding. Since the rate of M_c is less than $1 - \alpha$, M_c is strongly secure from the adversary who observes $n\alpha$

symbols of $\mathbf{X}_c^n$ [12], [13]. During the delivery, the transmitter sends $\mathbf{X}_{\mathbf{d}}^n$ as the binary representation of $M_{\mathbf{d}}$, whose length is n bits, since the delivery phase is noiseless and secure.

Using $\mathbf{X}_c^n$, receiver $j = 1,2$, recovers $M_{c,j}$ and stores it in its cache; the size of $M_{c,j}$ is smaller than $\frac{n}{2}$ bits, i.e., the cache size at each receiver. Using $\mathbf{X}_{\mathbf{d}}^n$, both receivers recover $M_{\mathbf{d}}$. Using $M_{\mathbf{d}}$ and $M_{c,j}$, and for n large enough, receiver j correctly decodes W_{d_j}. Since $\epsilon_n \to 0$ as $n \to \infty$, the achievable strong secrecy file rate is $R_s = 2 \times \frac{1-\alpha}{2} + \frac{\alpha}{2} = 1 - \frac{\alpha}{2}$.

2) The adversary taps into delivery only: This setting corresponds to $\alpha_1 = 0$, $\alpha_2 = \alpha$; $\alpha \in [0,1)$. The transmitter and receivers know the values of α_1, α_2. The strong secrecy rate $1 - \frac{\alpha}{2}$ is achievable as follows. The transmitter performs the same division of W_1, W_2, as in Setting 1, and randomly, and independently from W_1, W_2, generates the independent keys K_1, K_2, each is uniform over $[1 : 2^{n\frac{\alpha+\epsilon_n}{2}}]$. Let us define $M_{c,1} = \{W_1^{(1)} \oplus W_2^{(1)}, K_1\}$, $M_{c,2} = \{W_1^{(2)} \oplus W_2^{(2)}, K_2\}$, $M_{\mathbf{d}} = \{W_{d_1}^{(2)}, W_{d_2}^{(1)}\}$, and $\tilde{M}_{\mathbf{d}} = \{W_{d_1,s} \oplus K_1, W_{d_2,s} \oplus K_2\}$.

During placement, the transmitter sends $\mathbf{X}_c^n$ as the binary representation of M_c. During delivery, the transmitter encodes $M_{\mathbf{d}}$ into $\mathbf{X}_{\mathbf{d}}^n$ using wiretap coding and uses $\tilde{M}_{\mathbf{d}}$ as the randomization message. Using $\mathbf{X}_c^n$, receiver $j = 1,2$, recovers $M_{c,j}$ and stores it in its cache. From $\mathbf{X}_{\mathbf{d}}^n$, both receivers recover $M_{\mathbf{d}}$, $\tilde{M}_{\mathbf{d}}$. Using $M_{\mathbf{d}}$, $\tilde{M}_{\mathbf{d}}$, $M_{c,j}$, and for large n, receiver j correctly decodes W_{d_j}. The adversary can only retrieve $\tilde{M}_{\mathbf{d}}$ using which it gains no information about W_1, W_2.

3) The legitimate terminals know α_1,α_2: Here, neither $\alpha_1 = 0$ nor $\alpha_2 = 0$, but the legitimate terminals know α_1, α_2. To achieve a strong secrecy file rate of $1 - \frac{\alpha}{2}$, we use an achievability scheme similar to Setting 1 when $\alpha_1 \geq \alpha_2$, and a scheme similar to Setting 2 when $\alpha_1 < \alpha_2$; along with utilizing wiretap coding in both phases. The next question then is whether the lack of assumed knowledge about α_1, α_2 decreases the strong secrecy capacity of the model. The following setting provides a hint on the answer.

4) Either $\alpha_1 = 0$ or $\alpha_2 = 0$, the legitimate parties do not know which is zero: The adversary taps into either cache placement or delivery but not both. The legitimate parties do not know which phase is tapped. Let $\alpha \in [0,1)$. The strong secrecy capacity is again $1 - \frac{\alpha}{2}$. The transmitter performs the same division of W_1, W_2 as in Settings $1, 2$, and generates K_1, K_2 as in Setting 2. Let $M_c \triangleq \{M_{c,1}, M_{c,2}\}$, where

$$M_{c,1} = W_1^{(1)} \oplus W_2^{(1)}, \qquad M_{c,2} = W_1^{(2)} \oplus W_2^{(2)},$$
$$\tilde{M}_c \triangleq \{\tilde{M}_{c,1}, \tilde{M}_{c,2}\},\ \tilde{M}_{c,1} = K_1,\ \tilde{M}_{c,2} = K_2, \text{ and} \tag{6}$$
$$M_{\mathbf{d}} = \{W_{d_1}^{(2)}, W_{d_2}^{(1)}\},\ \ \tilde{M}_{\mathbf{d}} = \{W_{d_1,s} \oplus K_1, W_{d_2,s} \oplus K_2\}. \tag{7}$$

During placement, the transmitter encodes M_c into $\mathbf{X}_c^n$ using wiretap coding and uses $\tilde{M}_c$ as the randomization message. During delivery, the transmitter encodes $M_{\mathbf{d}}$ into $\mathbf{X}_{\mathbf{d}}^n$ using wiretap coding and uses $\tilde{M}_{\mathbf{d}}$ as the randomization message. Receiver j stores $M_{c,j}, \tilde{M}_{c,j}$ in its cache, and uses them, with $M_{\mathbf{d}}, \tilde{M}_{\mathbf{d}}$, to decode W_{d_j}. The adversary can only retrieve either $\{K_1, K_2\}$ or $\{W_{d_1,s} \oplus K_1, W_{d_2,s} \oplus K_2\}$, using which it gains no information about W_1, W_2.

Formal proofs for the aforementioned models satisfying (3) are provided in [16, Appendix A-E]. The lack of knowledge about which phase is tapped is tackled by encrypting $W_{d_1,s}, W_{d_2,s}$, with the keys K_1, K_2, while ensuring the adversary only retrieves either the keys or the encrypted bits but not both, using which it gains no information about W_1, W_2. Next, we generalize this idea to tackle the case when the adversary taps into both phases with no knowledge of α_1, α_2, i.e., the genenral model in consideration. In each phase, we construct a security embedding code [17] in which $n\alpha$ single-bit layers are embedded into one another. Doing so, we ensure that, regardless the values for α_1, α_2, the adversary can retrieve no more than $n\alpha_1$ bits from cache placement and $n\alpha_2$ bits from delivery. By designing what the adversary retrieves to be either a set of key bits and/or information bits encrypted with distinct key bits, we guarantee no information is leaked.

C. Achievability for $\alpha \in [0,1)$:

We now prove the achievability of (4) for $\alpha \in [0,1)$. Recall that $n\alpha_1 = \mu_1$, $n\alpha_2 = \mu_2$, $n\alpha = \mu$. For simplicity, let $n\frac{\alpha}{2}$, $n\frac{\alpha_1}{2}$ be integers; minor modifications to the analysis can be adopted otherwise. The transmitter (i) divides W_l, $l = 1,2$, into the independent messages $W_l^{(1)}, W_l^{(2)}, W_{l,s}$; $W_l^{(1)}, W_l^{(2)}$ are uniform over $[1 : 2^{n\frac{1-\alpha}{2}}]$, $W_{l,s}$ is uniform over $[1 : 2^{n\frac{\alpha}{2}}]$, and (ii) randomly and independently from W_1, W_2, generates the independent keys K_1, K_2, each is uniform over $[1 : 2^{n\frac{\alpha}{2}}]$. We ignored the small rate reduction ϵ_n, and will introduce it later to the security analysis. The main ideas of the proof are

1) The transmitter uses wiretap coding with a randomization message of size $n\alpha$ bits in *both* placement and delivery. As the adversary taps into no more than $n\alpha$ bits in each phase, a secure transmission rate of $1 - \alpha$ is achievable in each, as long as the randomization messages in the two phases are independent. Using coded placement [1, Appendix], a secure file rate of $1 - \alpha$ 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 $R_s = 1 - \frac{\alpha}{2}$. We use K_1, K_2 as the randomization message for cache placement. Along with wiretap coding, we employ a security embedding code [17], 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, we encrypt $W_{d_1,s}, W_{d_2,s}$, with K_1, K_2, and use this encrypted information as the randomization message. We employ again a security embedding code, in the *reverse order*, so that the adversary can only retrieve the first $n\frac{\alpha_2}{2}$ bits from each of $W_{d_1,s} \oplus K_1, W_{d_2,s} \oplus K_2$.
3) Due to the reversed embedding order, the adversary in the delivery phase does not obtain 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, the adversary can not 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 describe the scheme in more detail. Let M_c, $\tilde{M}_c$ be defined as in (6). M_c represents the message to be securely transmitted during cache placement regardless the value of α_1, and $\tilde{M}_c$ is the randomization message. The transmitter further divides $\tilde{M}_{c,1}, \tilde{M}_{c,2}$, into sequences of independent binary bits, $\{\tilde{M}_{c,1}^{(1)}, \cdots, \tilde{M}_{c,1}^{(n\frac{\alpha}{2})}\}$, $\{\tilde{M}_{c,2}^{(1)}, \cdots, \tilde{M}_{c,2}^{(n\frac{\alpha}{2})}\}$.

Cache Placement Codebook Generation: Let m_c, $\tilde{m}_{c,1} = \{\tilde{m}_{c,1}^{(1)}, \cdots, \tilde{m}_{c,1}^{(n\frac{\alpha}{2})}\}$, $\tilde{m}_{c,2} = \{\tilde{m}_{c,2}^{(1)}, \cdots, \tilde{m}_{c,2}^{(n\frac{\alpha}{2})}\}$ be the realizations of M_c, $\tilde{M}_{c,1}$, $\tilde{M}_{c,2}$ in (6). We construct the placement 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 $2^{n(1-\alpha)}$ bins, indexed by $m_c \in [1 : 2^{n\frac{1-\alpha}{2}}]^2$ and each contains $2^{n\alpha}$ binary codewords. Further, randomly and independently divide each bin m_c into two sub-bins, indexed by $\tilde{m}_{c,1}^{(1)} \in \{0, 1\}$ and each contains $2^{n\alpha-1}$ codewords. The sub-bins $\tilde{m}_{c,1}^{(1)}$ are randomly and independently divided into two smaller bins, indexed by $\tilde{m}_{c,2}^{(1)}$ and each contains $2^{n\alpha-2}$ codewords. The process continues, going over $\tilde{m}_{c,1}^{(2)}$, $\tilde{m}_{c,2}^{(2)}, \cdots$, $\tilde{m}_{c,2}^{(n\frac{\alpha}{2}-1)}$, $\tilde{m}_{c,1}^{(n\frac{\alpha}{2})}$, until the remaining two codewords, after each sequence of divisions, are indexed by $\tilde{m}_{c,2}^{(n\frac{\alpha}{2})} \in \{0, 1\}$.

Cache Encoder: Given w_1, w_2, i.e., $\{w_l^{(1)}, w_l^{(2)}, w_{l,s}\}_{l=1,2}$, the transmitter generates m_c and $\tilde{m}_c = \{\tilde{m}_{c,1}, \tilde{m}_{c,2}\}$ as in (6). 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., $\mathbf{x}_c^n(m_c, \tilde{m}_{c,1}^{(1)}, \tilde{m}_{c,2}^{(1)}, \cdots, \tilde{m}_{c,1}^{(n\frac{\alpha}{2})}, \tilde{m}_{c,2}^{(n\frac{\alpha}{2})})$.

Let $M_{\mathbf{d}}$, $\tilde{M}_{\mathbf{d}} = \{\tilde{M}_{\mathbf{d},1}, \tilde{M}_{\mathbf{d},2}\}$ be as in (7); $\tilde{M}_{\mathbf{d},1} = W_{d_1,s} \oplus K_1$, $\tilde{M}_{\mathbf{d},2} = W_{d_2,s} \oplus K_2$. $M_{\mathbf{d}}$ is the message to be securely transmitted during delivery regardless the value of α_2, and $\tilde{M}_{\mathbf{d}}$ is the randomization message. Similar to cache placement, the transmitter further divides $\tilde{M}_{\mathbf{d},1}$, $\tilde{M}_{\mathbf{d},2}$, into sequences of independent binary bits, $\{\tilde{M}_{\mathbf{d},1}^{(1)} \cdots \tilde{M}_{\mathbf{d},1}^{(n\frac{\alpha}{2})}\}$, $\{\tilde{M}_{\mathbf{d},2}^{(1)} \cdots \tilde{M}_{\mathbf{d},2}^{(n\frac{\alpha}{2})}\}$.

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

Delivery Encoder: Given w_1, w_2, $\mathbf{d} = (d_1, d_2)$, the transmitter (i) generates $m_{\mathbf{d}}, \tilde{m}_{\mathbf{d}} = \{\tilde{m}_{\mathbf{d},1}, \tilde{m}_{\mathbf{d},2}\}$ as in (7), (ii) uses $\mathcal{C}_{\mathbf{d},n}$ to send $\mathbf{x}_{\mathbf{d}}^n$ which corresponds to $m_{\mathbf{d}}$, $\tilde{m}_{\mathbf{d},1}$, $\tilde{m}_{\mathbf{d},2}$, i.e., $\mathbf{x}_{\mathbf{d}}^n(m_{\mathbf{d}}, \tilde{m}_{\mathbf{d},1}^{(n\frac{\alpha}{2})}, \tilde{m}_{\mathbf{d},2}^{(n\frac{\alpha}{2})}, \tilde{m}_{\mathbf{d},1}^{(n\frac{\alpha}{2}-1)}, \tilde{m}_{\mathbf{d},2}^{(n\frac{\alpha}{2}-1)}, \cdots, \tilde{m}_{\mathbf{d},1}^{(1)}, \tilde{m}_{\mathbf{d},2}^{(1)})$.

Decoding: Using $\mathbf{X}_c^n$, receiver j recovers $M_{c,j}, \tilde{M}_{c,j}$, and stores them in its cache, $j = 1, 2$. The combined size of $M_{c,j}, \tilde{M}_{c,j}$ does not exceed $\frac{n}{2}$ bits. Using $\mathbf{X}_{\mathbf{d}}^n$, both receivers recover $M_{\mathbf{d}}, \tilde{M}_{\mathbf{d}}$. Using $M_{\mathbf{d}}$, $\tilde{M}_{\mathbf{d}}$, $M_{c,j}$, $\tilde{M}_{c,j}$, and for large n, receiver j correctly decodes its desired message W_{d_j}.

Security Analysis: We slightly modify the scheme above as follows. Let $\alpha_\epsilon = \alpha + 2\epsilon_n$, $\alpha_{1,\epsilon} = \alpha_1 + \epsilon_n$, $\alpha_{2,\epsilon} = \alpha_\epsilon - \alpha_{1,\epsilon}$. We (i) increase the sizes of K_1, K_2 to $\frac{n\alpha_\epsilon}{2}$ bits, instead of $n\frac{\alpha}{2}$, and zero-pad the bit strings of $W_{d_1,s}, W_{d_2,s}$ accordingly, (ii) decrease the sizes of $W_l^{(1)}$, $W_l^{(2)}$, $l = 1, 2$, to $n\frac{1-\alpha_\epsilon}{2}$ bits. Fix $S_1, S_2 \subseteq [1 : n]$. For fixed values of α_1, α_2, $\mathcal{C}_{c,n}$ can be seen as a wiretap code with $2^{n(1-\alpha_{1,\epsilon})}$ bins, indexed by

$$w_c = (m_c, \tilde{m}_{c,1}^{(1)}, \tilde{m}_{c,2}^{(1)}, \cdots, \tilde{m}_{c,1}^{(n\frac{\alpha_{2,\epsilon}}{2})}, \tilde{m}_{c,2}^{(n\frac{\alpha_{2,\epsilon}}{2})}). \quad (8)$$

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

$$\tilde{w}_c = (\tilde{m}_{c,1}^{(n\frac{\alpha_{2,\epsilon}}{2}+1)}, \tilde{m}_{c,2}^{(n\frac{\alpha_{2,\epsilon}}{2}+1)}, \cdots, \tilde{m}_{c,1}^{(n\frac{\alpha_\epsilon}{2})}, \tilde{m}_{c,2}^{(n\frac{\alpha_\epsilon}{2})}). \quad (9)$$

Similarly, for fixed α_1, α_2, the code $\mathcal{C}_{\mathbf{d},n}$ is a wiretap code with $2^{n(1-\alpha_{2,\epsilon})}$ bins, each of which is indexed by the message

$$w_{\mathbf{d}} = (m_{\mathbf{d}}, \tilde{m}_{\mathbf{d},1}^{(n\frac{\alpha_\epsilon}{2})} \tilde{m}_{\mathbf{d},2}^{(n\frac{\alpha_\epsilon}{2})} \cdots \tilde{m}_{\mathbf{d},1}^{(n\frac{\alpha_{2,\epsilon}}{2}+1)} \tilde{m}_{\mathbf{d},2}^{(n\frac{\alpha_{2,\epsilon}}{2}+1)}) \quad (10)$$

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

$$\tilde{w}_{\mathbf{d}} = (\tilde{m}_{\mathbf{d},1}^{(n\frac{\alpha_{2,\epsilon}}{2})}, \tilde{m}_{\mathbf{d},2}^{(n\frac{\alpha_{2,\epsilon}}{2})}, \cdots, \tilde{m}_{\mathbf{d},1}^{(1)}, \tilde{m}_{\mathbf{d},2}^{(1)}). \quad (11)$$

Let $\{\mathcal{B}_{w_c}\}_{w_c=1}^{2^{n(1-\alpha_{1,\epsilon})}}$, $\{\mathcal{B}_{w_{\mathbf{d}}}\}_{w_{\mathbf{d}}=1}^{2^{n(1-\alpha_{2,\epsilon})}}$ denote the partition (bins) of $\mathcal{C}_{c,n}$, $\mathcal{C}_{\mathbf{d},n}$, which correspond to w_c, $w_{\mathbf{d}}$, in (8), (10). 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

$$\mathcal{B}_{w_c,w_{\mathbf{d}}} \triangleq \{\mathbf{x}^{2n} = (\mathbf{x}_c^n, \mathbf{x}_{\mathbf{d}}^n) : \mathbf{x}_c^n \in \mathcal{B}_{w_c}, \mathbf{x}_{\mathbf{d}}^n \in \mathcal{B}_{w_{\mathbf{d}}}\}. \quad (12)$$

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. $\tilde{W}_c$, $\tilde{W}_{\mathbf{d}}$, are independent, and so are $\{\tilde{W}_c, \tilde{W}_{\mathbf{d}}\}$, $\{W_c, W_{\mathbf{d}}\}$; $W_c, \tilde{W}_c, W_{\mathbf{d}}, \tilde{W}_{\mathbf{d}}$ are the random variables corresponding to the realizations in (8)-(11). We thus can apply [12, (94)-(103)] to show that, for every S_1, S_2, $w_c, w_{\mathbf{d}}$, $\epsilon > 0$, and some $\gamma > 0$,

$$\mathbb{P}_{\mathcal{B}_{w_c,w_{\mathbf{d}}}}(\mathbb{D}(P_{\mathbf{Z}_{S_1}^n \mathbf{Z}_{S_2}^n | W_c=w_c, W_{\mathbf{d}}=w_{\mathbf{d}}} || P_{\mathbf{Z}_{S_1}^n \mathbf{Z}_{S_2}^n}) > \epsilon) \leq e^{-e^{n\gamma}} \quad (13)$$

$P_{\mathbf{Z}_{S_1}^n \mathbf{Z}_{S_2}^n | W_c=w_c, W_{\mathbf{d}}=w_{\mathbf{d}}}$ is the induced distribution at the adversary when $\mathbf{x}_c^n(w_c, \tilde{w}_c)$, $\mathbf{x}_{\mathbf{d}}^n(w_{\mathbf{d}}, \tilde{w}_{\mathbf{d}})$ are the transmitted signals and $P_{\mathbf{Z}_{S_1}^n \mathbf{Z}_{S_2}^n}$ 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 (13) and the union bound [13],

$$\lim_{n\to\infty} \max_{S_1,S_2} I(W_c, W_{\mathbf{d}}; \mathbf{Z}_{S_1}^n, \mathbf{Z}_{S_2}^n) = 0. \quad (14)$$

Let $\{W_{d_l,s}^{(1)} \cdots W_{d_l,s}^{(n\frac{\alpha_\epsilon}{2})}\}$, $\{K_l^{(1)} \cdots K_l^{(n\frac{\alpha_\epsilon}{2})}\}$ denote the bit strings of $W_{d_l,s}, K_l$, $l = 1, 2$. For notational simplicity, define

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

$$\mathbf{K}^{(1)} = \{K_1^{(i)}, K_2^{(i)}\}_{i=1}^{n\frac{\alpha_{2,\epsilon}}{2}}, \ \mathbf{K}^{(2)} = \{K_1^{(i)}, K_2^{(i)}\}_{i=n\frac{\alpha_{2,\epsilon}}{2}+1}^{n\frac{\alpha_\epsilon}{2}}$$

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

$\mathbf{W}_s^{(2)} - \{M_c, M_{\mathbf{d}}, \mathbf{W}_s^{(1)}, \mathbf{W}_{\oplus\mathbf{K}}^{(2)}\} - \{\mathbf{Z}_{S_1}^n, \mathbf{Z}_{S_2}^n\}$ is a Markov chain, since $\{M_c, M_{\mathbf{d}}, \mathbf{W}_s^{(1)}\}$, $\{\mathbf{W}_s^{(2)}, \mathbf{K}^{(2)}\}$, are independent and only $\mathbf{W}_{\oplus\mathbf{K}}^{(2)}$ is transmitted. Using (6)-(11), we have [16]

$$\begin{aligned}
&I(W_1, W_2; \mathbf{Z}_{S_1}^n, \mathbf{Z}_{S_2}^n) \\
&= I(W_1^{(1)}, W_1^{(2)}, W_2^{(1)}, W_2^{(2)}, W_{1,s}, W_{2,s}; \mathbf{Z}_{S_1}^n, \mathbf{Z}_{S_2}^n) && (15)\\
&= I(W_1^{(1)} \oplus W_2^{(1)}, W_1^{(2)} \oplus W_2^{(2)}, W_{d_1}^{(2)}, W_{d_2}^{(1)}, \\
&\qquad\qquad W_{d_1,s}, W_{d_2,s}; \mathbf{Z}_{S_1}^n, \mathbf{Z}_{S_2}^n) && (16)\\
&= I(M_c, M_{\mathbf{d}}, \mathbf{W}_s^{(1)}, \mathbf{W}_s^{(2)}; \mathbf{Z}_{S_1}^n, \mathbf{Z}_{S_2}^n) && (17)\\
&\leq I(M_c, M_{\mathbf{d}}, \mathbf{W}_s^{(1)}, \mathbf{W}_{\oplus\mathbf{K}}^{(2)}; \mathbf{Z}_{S_1}^n, \mathbf{Z}_{S_2}^n) && (18)\\
&= I(M_c, \mathbf{W}_s^{(1)}, W_{\mathbf{d}}; \mathbf{Z}_{S_1}^n, \mathbf{Z}_{S_2}^n) && (19)\\
&= H(\mathbf{Z}_{S_1}^n, \mathbf{Z}_{S_2}^n) - H(\mathbf{Z}_{S_1}^n, \mathbf{Z}_{S_2}^n, \mathbf{W}_s^{(1)}, \mathbf{W}_{\oplus K}^{(1)} | M_c, W_{\mathbf{d}}) \\
&\quad + H(\mathbf{W}_{\oplus K}^{(1)} | M_c, W_{\mathbf{d}}, \mathbf{W}_s^{(1)}, \mathbf{Z}_{S_1}^n, \mathbf{Z}_{S_2}^n) + H(\mathbf{W}_s^{(1)}) && (20)\\
&\leq H(\mathbf{Z}_{S_1}^n, \mathbf{Z}_{S_2}^n) - H(\mathbf{Z}_{S_1}^n, \mathbf{Z}_{S_2}^n, \mathbf{K}^{(1)}, \mathbf{W}_{\oplus K}^{(1)} | M_c, W_{\mathbf{d}}) \\
&\qquad\qquad + H(\mathbf{W}_s^{(1)}) + \epsilon_n' && (21)\\
&\leq H(\mathbf{Z}_{S_1}^n, \mathbf{Z}_{S_2}^n) - H(\mathbf{K}^{(1)} | M_c, W_{\mathbf{d}}) \\
&\quad - H(\mathbf{Z}_{S_1}^n, \mathbf{Z}_{S_2}^n, | M_c, \mathbf{K}^{(1)}, W_{\mathbf{d}}) + H(\mathbf{W}_s^{(1)}) + \epsilon_n' && (22)\\
&= H(\mathbf{Z}_{S_1}^n, \mathbf{Z}_{S_2}^n) - H(\mathbf{Z}_{S_1}^n, \mathbf{Z}_{S_2}^n, | W_c, W_{\mathbf{d}}) \\
&\qquad\qquad - H(\mathbf{K}^{(1)}) + H(\mathbf{W}_s^{(1)}) + \epsilon_n' && (23)\\
&= I(W_c, W_{\mathbf{d}}; \mathbf{Z}_{S_1}^n, \mathbf{Z}_{S_2}^n) + \epsilon_n', && (24)
\end{aligned}$$

$\epsilon_n' \to 0$ as $n \to \infty$. (21) follows since, given $\{M_c, \mathbf{W}_s^{(1)}, W_{\mathbf{d}}\}$ and for large n, the adversary can decode $\mathbf{K}^{(1)}$ using $\mathbf{Z}_{S_1}^n, \mathbf{Z}_{S_2}^n$, and (24) follows since $\mathbf{K}^{(1)}$, $\mathbf{W}_s^{(1)}$, are identically distributed. Using (14) and (24), (3) is satisfied. The achievable strong secrecy file rate is $R_s = 2 \times \frac{1-\alpha}{2} + \frac{\alpha}{2} = 1 - \frac{\alpha}{2}$.

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

We adapt the scheme in Section IV-C as follows. The messages W_1, W_2, are uniform over $[1 : 2^{n\frac{2-\alpha}{2}}]$. The transmitter randomly and independently from W_1, W_2, generates (i) the independent keys K_1, K_2, each is uniform over $[1 : 2^{n\frac{2-\alpha}{2}}]$, and (ii) the independent dummy messages $\tilde{W}, \tilde{W}_K$, each is uniform over $[1 : 2^{n(\alpha-1)}]$; $\{K_1, K_2\}$ and $\{\tilde{W}, \tilde{W}_K\}$ are independent. Let $M_{\mathbf{d},1} = W_{d_1} \oplus K_1$, $M_{\mathbf{d},2} = W_{d_2} \oplus K_2$. Let $\{W_{d_l}^{(1)} \cdots W_{d_l}^{(n\frac{2-\alpha}{2})}\}$, $\{K_l^{(1)} \cdots K_l^{(n\frac{2-\alpha}{2})}\}$, $\{M_{\mathbf{d},l}^{(1)} \cdots M_{\mathbf{d},l}^{(n\frac{2-\alpha}{2})}\}$, be the bit strings of $W_{d_l}, K_l, M_{\mathbf{d},l}$.

During cache placement, the transmitter generates $\mathcal{C}_{c,n}$ as follows. Randomly and independently divide all the 2^n length-n binary sequences into 2 bins, indexed by $K_1^{(1)} \in \{0, 1\}$, and each contains 2^{n-1} codewords. The two bins are further randomly and independently divided into two sub-bins, indexed by $K_2^{(1)} \in \{0, 1\}$, and each contains 2^{n-2} codewords. The process continues, going over $K_1^{(2)}, K_2^{(2)} \cdots K_2^{(n\frac{2-\alpha}{2})}$, until the remaining $2^{n(\alpha-1)}$ codewords, after each sequence of divisions, are indexed by $\tilde{W}_K$. The transmitter sends the codeword $\mathbf{X}_c^n(K_1^{(1)}, K_2^{(1)}, \cdots, K_1^{(n\frac{2-\alpha}{2})}, K_2^{(n\frac{2-\alpha}{2})}, \tilde{W}_K)$.

In the delivery phase, the transmitter generates the codebook $\mathcal{C}_{\mathbf{d},n}$ as follows. The transmitter randomly and independently divide the 2^n length-n binary sequences into 2 bins, indexed by $M_{\mathbf{d},1}^{(n\frac{2-\alpha}{2})} \in \{0, 1\}$, and each contains 2^{n-1} codewords. The two bins are further randomly and independently divided into two sub-bins, indexed by $M_{\mathbf{d},2}^{(n\frac{2-\alpha}{2})} \in \{0, 1\}$, and each contains 2^{n-2} codewords. The process continues, going in a reverse order over $M_{\mathbf{d},1}^{(n\frac{2-\alpha}{2}-1)}, M_{\mathbf{d},2}^{(n\frac{2-\alpha}{2}-1)}, \cdots, M_{\mathbf{d},1}^{(1)}, M_{\mathbf{d},2}^{(1)}$, until the remaining $2^{n(\alpha-1)}$ codewords, after each sequence of divisions, are indexed by $\tilde{W}$. The transmitter sends the codeword $\mathbf{X}_{\mathbf{d}}^n(M_{\mathbf{d},1}^{(n\frac{2-\alpha}{2})}, M_{\mathbf{d},2}^{(n\frac{2-\alpha}{2})}, \cdots, M_{\mathbf{d},1}^{(1)}, M_{\mathbf{d},2}^{(1)}, \tilde{W})$.

The remainder of the analysis follows similar steps as when $\alpha \in [0, 1)$. The achievable secrecy file rate is $R_s = 1 - \frac{\alpha}{2}$.

V. Conclusion

We have introduced the caching broadcast channel with a *a wire and cache* tapping adversary of type II. In this 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 only know the size of the overall tapped subset. The strong secrecy capacity is identified when the transmitter's library has two files. The achievability scheme highlights the robustness of *wiretap coding* against a clever adversary who jointly optimizes its chosen attack over both phases of communication in a cache-aided system.

References

[1] M. A. Maddah-Ali and U. Niesen. Fundamental limits of caching. *IEEE Tran. Info. Theory*, 60(5):2856–2867, 2014.

[2] K. Wan, D. Tuninetti, and P. Piantanida. On caching with more users than files. In *IEEE Int. Symp. Info. Theory*, Jul. 2016.

[3] U. Niesen and M. A. Maddah-Ali. Coded caching with nonuniform demands. *IEEE Tran. Info. Theory*, 63(2):1146–1158, 2017.

[4] A. Zewail and A. Yener. Combination networks with or without secrecy constraints: The impact of caching relays. *IEEE Journal in Selected Areas in Comm.*, 36(7):1–13, 2018.

[5] A. Sengupta, R. Tandon, and T. Clancy. Fundamental limits of caching with secure delivery. *IEEE Tran. Info. Forensics and Security*, 10(2):355–370, 2015.

[6] A. Zewail and A. Yener. Fundamental limits of secure device-to-device coded caching. In *Asilomar Conf. on Sig., Sys., and Comp.*, Nov. 2016.

[7] V. Ravindrakumar, P. Panda, N. Karamchandani, and V. M. Prabhakaran. Private coded caching. *IEEE Tran. Info. Forensics and Security*, 13(3):685–694, 2018.

[8] S. Kamel, M. Wigger, and M. Sarkiss. Coded caching for wiretap broadcast channels. In *IEEE Info. Theory Workshop*, Nov. 2017.

[9] R. Ahlswede and I. Csiszár. Common randomness in information theory and cryptography–Part I: Secret sharing. *IEEE Tran. Info. Theory*, 39(4):1121–1132, 1993.

[10] L. H. Ozarow and A. D. Wyner. Wire-tap channel II. *Bell Sys. Tech. Jour.*, 63(10):2135—2157, 1984.

[11] M. Nafea and A. Yener. Wiretap channel II with a noisy main channel. In *IEEE Int. Symp. Info. Theory*, June 2015.

[12] Z. Goldfeld, P. Cuff, and H. Permuter. Semantic-security capacity for wiretap channels of type II. *IEEE Tran. Info. Theory*, 62(7):3863–3879, 2016.

[13] M. Nafea and A. Yener. A new wiretap channel model and its strong secrecy capacity. *IEEE Tran. Info. Theory*, 64(3):2077–2092, 2018.

[14] M. Nafea and A. Yener. A new broadcast wiretap channel model. In *IEEE Int. Symp. Info. Theory*, June 2017.

[15] M. Nafea and A. Yener. Generalizing multiple access wiretap and wiretap II channel models: Achievable rates and cost of strong secrecy. *Submitted to IEEE Tran. Info. Theory*, Jan. 2018. arXiv preprint arXiv:1802.02131.

[16] M. Nafea and A. Yener. The caching broadcast channel with a wire and cache tapping adversary of type II. *Submitted to IEEE Tran. Info. Theory*, Aug. 2018. arXiv preprint arXiv:1808.02477.

[17] Y. Liang, L. Lai, H. V. Poor, and S. Shamai. A broadcast approach for fading wiretap channels. *IEEE Tran. Info. Theory*, 60(2):842–858, 2014.