On Caching with Finite Blocklength Coding for Secrecy over the Binary Erasure Wiretap Channel

Willie K. Harrison and Morteza Shoushtari
Department of Electrical and Computer Engineering
Brigham Young University, Provo, UT, USA
Emails: {willie.harrison, morteza.shoushtari}@byu.edu

***Abstract*—Coded caching has been shown to be an effective means for enhancing efficient delivery of content over communication networks. In this paper, we show that caching can also aid in achieving secure communications by considering a wiretap scenario where the transmitter and legitimate receiver share access to a secure cache, and an eavesdropper is able to tap transmissions over a binary erasure wiretap channel during the delivery phase of a caching protocol. The scenario under consideration gives rise to a new channel model for wiretap coding that allows the transmitter to effectively choose a subset of bits to erase at the eavesdropper by caching the bits ahead of time. The eavesdropper observes the remainder of the coded bits through the wiretap channel for the general case. In the wiretap type-II scenario, the eavesdropper is able to choose a set of revealed bits only from the subset of bits not cached. We present a coding approach that allows efficient use of the cache to realize a caching gain in the network, and show how to use the cache to optimize the information theoretic security in the choice of a finite block length code and the choice of the cached bit set. To our knowledge, this is the first work on explicit algorithms for secrecy coding in any type of caching network.**

I. Introduction

The last decade has seen an unprecedented increase in the sheer volume of wireless data transmissions. Much of this increase has been brought on by the nearly ubiquitous use of personal digital devices, and the continuing deployment of the Internet of Things (IoT) assures that this trend of increasing wireless communications will continue. Content delivery and security are two major concerns that are of utmost importance in these modern networks and, hence, are both active areas of research. Caching [1], and specifically coded caching [2], are likely to play a role in increasing the efficiency of content delivery, while information theoretic security [3] through wiretap coding [4] is likely to play a role in securing these dense networks of the future.

Coded caching was first developed in [2], where it was shown that caching nodes in networks could be used to store coded data in such a way to decrease overall traffic flow in the network. Many additional contributions have been made over the last few years. For example, [5] extended coded caching to applications where there are more users than files that can be requested over the network, and the solution for solving this case was in initiating a more global encoding scheme of information. Also, sub-packetization strategies for potential future caching algorithms were explored in [6], where it was shown that the combinatorial structure of linear block codes, including rank properties of generator matrices, can be used to devise effective caching schemes. Additional works address fundamental tradeoffs between delivery rate and cache capacity [7], and the potential energy savings when coded caching is used [8]. Finally, it was shown that when preferences of users are known a priori, caching algorithms can be made to perform much more efficiently [9], and there are a host of additional results in this area.

Caching was introduced to the wiretap channel in [10], where the secrecy capacity was characterized when a secure cache was added to the legitimate receiver, and a discrete memoryless wiretap channel was assumed for the delivery of uncached content. This idea was extended to multiple receivers in [11], and cache tapping was allowed in the models studied in [12], [13]. Caching in a wiretap model is new enough that there currently exist only these few works, and coding for these new channel models has yet to be addressed in any explicit sense.

In this paper, we consider the problem of finite blocklength coding for the simplest wiretap channel model with a cache, and show how the model gives way to a new wiretap coding scheme for secure communication of sensitive data. The cache is assumed to be secure and reliable; meaning only the transmitter can write to the cache, only the legitimate receiver can read from the cache, and all access to the cache is accomplished error free. The size of the cache is fixed, and smaller than what is required to store all files that could be requested. The remainder of transmitted data must be sent over a binary erasure wiretap channel (BEWC), wherein the link to the legitimate receiver is noise-free, and the link to the eavesdropper is a binary erasure channel (BEC). We show how to adapt wiretap codes to such a channel model, and show how they can be optimized for finite blocklength to maximize the equivocation in the network.

The remainder of the paper is organized as follows. Section II gives the basic setup of the scenario under study in this work. In Section III, we show how wiretap coding and the choice of caching pattern can be optimized, and introduce tools that can help in the optimization. Two new channel models are presented in Section IV, over which wiretap codes can be explored that allow Alice to choose erasures for Eve prior to transmission using a secure cache. Section V gives examples,

This work was partially funded by the National Science Foundation (Grant Award #1910812).

Section VI highlights the promising nature of the results and discusses future directions to be explored, and we conclude the paper in Section VII.

II. System Setup

Consider the wiretap channel model variant shown in Fig. 1. Note the presence of three players: the transmitter Alice, the legitimate receiver Bob, and an eavesdropper named Eve. Alice has a library of L files, $W^1, W^2, \ldots, W^L$, each of which is comprised of k bits, which are assumed to be uniformly distributed and independent. The size of the cache is $M = \eta \times L$ bits, where $\eta < k$. The system acts over two phases: a *secure cache placement phase* and a *delivery phase* over the BEWC.

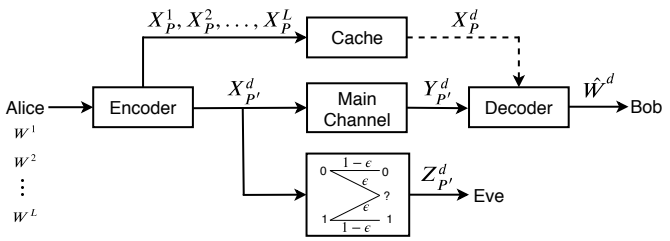

Fig. 1. Wiretap channel model with cache

A. Secure Cache Placement Phase

Prior to any request for a file transfer from Bob, the files are encoded according to an encoding function $\phi(\cdot)$, whereby file W^i is encoded into an n-bit codeword X^i, for $i = 1, 2, \ldots, L$. Then η bits from each codeword are placed in the cache memory during the secure cache placement phase. Let $P = \{i \in \{1, 2, \ldots, n\} : \text{bit } i \text{ is cached}\}$. The bits with indices in P will appear to be punctured to the eavesdropper, but not the legitimate receiver. Let $X_P^1, X_P^2, \ldots, X_P^L$ denote the cached portions of each of the respective codewords, where the exponent indicates the file index as before, and the subscript indicates the bit indices included. The cache placement phase is assumed to be secure from eavesdropping and error-free for Bob.

B. Delivery phase

The delivery phase begins when Bob requests one of the files from the library, which we call W^d. Upon receiving the request, Alice sends $X_{P'}^d$ over the BEWC, Bob receives $Y_{P'}^d$ through the main channel, and Eve receives $Z_{P'}^d$, where P' is the complement of P in the set $\{1, 2, \ldots, n\}$. Bob uses X_P^d from the cache and his channel observations $Y_{P'}^d$ as inputs to the decoding function $\psi(\cdot)$, which produces an estimate of the desired file $\hat{W}^d$. Since the BEWC contains a noise-free main channel over which Bob receives the transmission, $Y_{P'}^d = X_{P'}^d$, and Bob can reconstruct X^d error free. However, the BEWC stipulates a BEC for Eve for the transmitted data, where bits are erased independently with probability ϵ. Thus Eve receives a bit in X_P^d with probability zero, and Eve receives a bit in $X_{P'}^d$ with probability $(1 - \epsilon)$.

C. Constraints for Secure and Reliable Communication with Caching

Normally, wiretap coding algorithms operate so as to satisfy a reliability constraint and a security constraint. With the addition of the cache, however, we propose that a third constraint should be added to the problem to ensure a network reduction in traffic, or *caching gain*, although the cache may also be used to increase reliability and/or security. For this paper, the caching gain is achieved by caching η bits ahead of time for all codewords, so that only $(n - \eta)$ bits need to be transmitted in real time. We consider the caching gain calculated pertaining to real-time transmissions only, and the gain can be represented as a rate of $(n - \eta)/n$.

It is assumed that Eve knows the caching pattern P, and the index d of the file requested. The goal of this paper is to devise encoding and decoding algorithms as well as cache placement strategies so as to use the cache to reduce real-time network congestion while also satisfying the additional two traditional contraints:

- $\Pr(W^d \neq \hat{W}^d) < \delta_r$, (reliability constraint),
- $\mathbb{H}(W^d) - \mathbb{H}(W^d | Z_{P'}^d) < \delta_s$, (security constraint),

where δ_r and δ_s can be set arbitrarily by the legitimate users of the network, and are assumed to be small positive real numbers. Since Bob can reconstruct X^d without error, the reliability constraint is achieved for free as long as the decoder is a bijection. The caching gain is guaranteed by how the cache is used in the system. We, therefore, need only concern ourselves with the security constraint. Notice, that the security contraint is with respect to the exact equivocation experienced by Eve, assuming a fixed blocklength code. Our true goal, therefore, is to choose the encoder/decoder pair, along with the caching pattern P to maximize

$$E = \mathbb{H}(W^d | Z_{P'}^d). \tag{1}$$

III. Best Coset-Based Wiretap Codes with Caching

In this paper, the encoding function is a wiretap encoder based on the coset structure of linear block codes, as has been used in many works, e.g. in [4], [14], [15]. We first encode the files using these well-known wiretap codes, and then choose the caching pattern to apply to the codewords.

A. Coset Coding for the Binary Erasure Wiretap Channel

Let $\mathcal{C}$ be an $(n, n-k)$ binary linear block code, with cosets $\mathcal{C} = C_0, C_1, C_2, ..., C_{2^k-1}$. Also let G be the $(n - k) \times n$ generator matrix of $\mathcal{C}$ and H be the $k \times n$ parity-check matrix of $\mathcal{C}$. Then G^* is required for the encoder, and takes the form

$$G^* = \begin{bmatrix} G \\ G' \end{bmatrix}, \tag{2}$$

where G' is comprised of k linearly independent vectors in $\mathbb{F}_2^n$ but not in $\mathcal{C}$. The encoding is done by choosing an auxiliary file W' uniformly at random from $\mathbb{F}_2^{n-k}$, and then computing

$$\phi(w) = x = \begin{bmatrix} w' & w \end{bmatrix} G^*, \tag{3}$$

where w is the file to be encoded, and x is the corresponding codeword. Effectively, the file w chooses the coset, and the auxiliary file w' choose a specific codeword from the coset uniformly at random.

The decoder $\psi(x)$ can be accomplished by realizing that every codeword in a specific coset must have the same syndrome

$$s = xH^T, \tag{4}$$

and the syndrome can be mapped to the file w with a look-up table, or it was shown in [16] that the rows of G' can be chosen so that $s = w$. Assuming a construction such as this,

$$\psi(x) = \hat{w} = xH^T. \tag{5}$$

B. Best Codes and Best Caching Patterns

Let Z^d be the eavesdropper's observation through the wiretap channel with erasures inserted into the cached bit locations. Thus, the ith bit of Z^d is

$$Z_i^d = \begin{cases} ?, & \text{if } i \in P, \\ ?, & \text{with probability } \epsilon \text{ if } i \in P', \\ X_i^d, & \text{with probability } (1-\epsilon) \text{ if } i \in P', \end{cases} \tag{6}$$

where the symbol '?' indicates an erasure. Let

$$R = \{i \in \{1, 2, \ldots, n\} : Z_i^d = X_i^d\}. \tag{7}$$

Thus, we can deduce that

$$\mathbb{H}(W^d|Z_{P'}^d) = \mathbb{H}(W^d|Z^d). \tag{8}$$

It has been shown in [16] that

$$\mathbb{H}(W^d|Z^d = z^d) = \mathbb{H}(W^d) - |R| + \text{rank } G_R, \tag{9}$$

where G_R is a submatrix of G comprised of only the columns indexed in R. Let $\mathcal{R}$ indicate the alphabet of all possible R sets. It was discussed in [17] that

$$\mathbb{H}(W^d|Z^d) = \sum_{r \in \mathcal{R}} p(r)[\mathbb{H}(W^d) - |r| + \text{rank } G_r] \tag{10}$$

$$= \gamma + \sum_{r \in \mathcal{R}} p(r)[k - |r|]), \tag{11}$$

where

$$\gamma = \sum_{r \in \mathcal{R}} p(r) \text{rank } G_r. \tag{12}$$

If maximization of (10) is desired, then only maximization of (12) need be considered since the other pieces of (10) are all constants. In [17], we used this knowledge to prove that a code of blocklength n and dimension k is *best for its size*, in the sense that it maximizes $\mathbb{H}(W^d|Z^d)$ for all possible codes with matching parameters n and k, if

$$\sum_{r \in \mathcal{R}: |r| = \mu} \text{rank } G_r \tag{13}$$

is maximum for all $\mu \in \{0, 1, \ldots, n\}$.

Although the channel model in [17] did not consider a secure cache, we note herein that the presence of the cache simply allows an extra design step to further confuse the eavesdropper. That is, the code design and caching pattern design should be completed so as to maximize (1), and maximizing (13) for all possible μ is a sufficient condition for maximizing (1). Since η bits from each codeword are cached, we only need consider $\mu \in \{\eta, \eta + 1, \ldots, n\}$ for our case.

C. Equivocation Matrices

The equivocation matrix is a tool that has been found useful in the optimization of coset-coding structures for the wiretap channel [17], [18]. It was first presented in [17], and the tool naturally extends itself to aid in finding the best codes with the best caching patterns to maximize the equivocation in (1). The (e, μ)th entry of the equivocation matrix A is equal to the number of unique sets $r \in \mathcal{R}$ such that $\mathbb{H}(W^d|Z^d = z^d) = e$, where $z_i^d \neq ?$ iff $i \in r$, and the number of bits revealed to the eavesdropper is $|r| = \mu$. Column indices range over the possible values of μ, i.e., $0, 1, \ldots, n$; while row indices range over the possible values of e, i.e., $0, 1, \ldots, k$. Note from (9) that equivocation can only result in integer values for these types of codes because all elements in the expression for (9) are themselves integers. Somewhat unconventionally, we begin indexing at the lower left corner of the matrix with the $(0, 0)$th entry so that the shape of the nonzero entries matches that of traditional equivocation curves.

We now know that maximizing (13) for all μ in the choice of a code is sufficient for a code to be the best of its size. We also know that $\mathbb{H}(W^d|Z^d = z^d)$ in (9) is only a function of constants (which are equal for all r counted in the same column of the equivocation matrix) and $\text{rank } G_R$. Putting these two facts together, sets r counted in the same column of the equivocation matrix are for a single value of μ, and $\text{rank } G_r$ increases by one for r counted in an adjacent higher row of the equivocation matrix. This is also true for the case where caching is applied as in Section II, although caching bits ensures erasures at Eve, and therefore must zero out some entries in the equivocation matrix. The matrix changes with respect to the choice of the code $\mathcal{C}$ and the choice of the caching pattern P. Comparison of different choices immediately reveals which choices are better.

IV. Channel Models

Coding over our system setup in Fig. 1 with the coding approach outlined in Section III, we identify two new combinatorial channel models based on the BEWC. We briefly outline these contributions in this section, and note that other works have presented similar models that arise from other coding schemes, e.g., as in [19], [20] and [21], [22], although our models are the first that justify Alice in choosing erasures for Eve, particularly prior to any choices that may be made by Eve herself.

A. Binary Erasure Wiretap Channel with a Secure Cache

The first model considers the system setup in Section II and the coding approach in Section III precisely. The channel model has parameters η and ϵ, and is called the binary erasure wiretap channel with a secure cache, or BEWC-SC(η, ϵ).

This model first allows Alice to choose η bits to erase at the eavesdropper (which is done by secure caching), and then allows a BEC(ϵ) to govern any remaining erasures that may occur at Eve. The cache gives a security advantage by allowing Alice to dictate a lower bound on the number of erasures experienced by Eve, regardless of the value of ϵ, and allows Alice to choose the locations for these erasures however she desires, which she will presumably do to maximize the equivocation in (1).

B. Binary Erasure Wiretap Channel with a Secure Cache of Type II

A slight variant on the BEWC-SC(η, ϵ) is the type-II scenario, where Alice first chooses η bits to erase at Eve, and then Eve is allowed to choose μ bits from those that remain. Again we see the advantage of the cache allowing Alice to erase bits prior to transmission presumably so as to maximize (1), but now Eve is allowed to choose μ revealed bits directly following Alice's choice presumably in an attempt to minimize (1) subject to the constraint of Alice's choice. We call this channel model the binary erasure wiretap channel with a secure cache of type II, or BEWC-SC-II(η,μ). Both of these new models allow coding design to be considered in a new light, where Alice chooses the code, chooses bits to be seen only by Bob, and then transmits the remaining data over the wiretap channel.

V. Best Coding and Caching Examples

Let us consider a specific instantiation of our approach to coding over the two channel models from the previous section. We would like to find a code $\mathcal{C}$ with generator matrix G and caching pattern P to maximize (1) when $n = 8$, $k = 5$, and $\eta = 2$. We first choose the best code of this size by considering all possible codes and examining their equivocation matrices. It is only possible to do this for very small n, but shortcuts for finding such codes may exist for some size parameters (see [17], [18]).

In this case, there are a few different codes that maximize (13) for all choices of $\mu \in \{0, 1, \ldots, n\}$. One such code $\mathcal{C}$ has generator matrix

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 \end{bmatrix}. \tag{14}$$

The code's equivocation matrix is

$$A = \begin{bmatrix} 1 & 8 & 27 & 40 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 16 & 67 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 3 & 56 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 28 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 8 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}. \tag{15}$$

Recall that the left-bottom corner of the matrix is the $(0, 0)$th entry of the matrix, and notice that the $\mu = 2$ column has a 1 in the $e = 4$ row. This indicates that there is exactly one way to leak a bit of information to an eavesdropper (four bits of equivocation, rather than five) using this code when the eavesdropper observes only two bits. This revealed-bit pattern of size two is the only collection of indices of size two, wherein the submatrix of G comprised of the indexed columns has rank 1 in GF(2). This pattern is $r = \{7, 8\}$, which can be deduced by observation of (14).

Let us consider all possible ways to cache $\eta = 2$ bits, and examine the equivocation matrices that follow. There are only three unique matrices, although there are $\binom{8}{2} = 28$ unique caching patterns. The unique equivocation matrices are

$$A_1 = \begin{bmatrix} 1 & 6 & 15 & 16 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 4 & 15 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 6 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}, \tag{16}$$

$$A_2 = \begin{bmatrix} 1 & 6 & 14 & 13 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 7 & 14 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 6 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}, \tag{17}$$

$$A_3 = \begin{bmatrix} 1 & 6 & 14 & 12 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 8 & 13 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 2 & 6 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}, \tag{18}$$

where A_1 is superior to A_2, which is in turn superior to A_3 in terms of maximizing (13) for all μ. There are 13 unique caching patterns that return A_1 for an equivocation matrix, and each of these patterns caches at least one of bits 7 or 8. Since the revealed-bit pattern $r = \{7, 8\}$ is the only length-two pattern that leaks information about the file, perhaps this is easily deduced, although choosing the optimal caching pattern for larger codes is not generally this straightforward. There are 12 unique caching patterns that return A_2 as their equivocation matrix, and only 3 unique caching patterns that return A_3.

For both the BEWC-SC(η, ϵ) and the BEWC-SC-II(η,μ), the choice of $\mathcal{C}$ combined with caching at least one of bits 7 or 8 in the two-bit caching pattern is optimum when $n = 8$, $k = 5$, and $\eta = 2$. The matrices A_1, A_2, and A_3 are sufficient to deduce that (13) is maximum for all μ when A_1 is the equivocation matrix, rather than either A_2 or A_3. For the wiretap-II case, Eve presumably chooses the revealed bits that leak the most information. This amounts to the patterns that cause nonzero entries as low as possible in the equivocation matrix. Notice that A_1 wins here as well, where A_2 and A_3 give additional leakage opportunities for the eavesdropper over A_1 when $\mu = 2$ and $\mu = 4$. We studied the $\eta = 3$ case and found similar results. There was a clear advantage to choosing specific caching patterns over others within the choice of the optimal wiretap code. Average equivocation curves for the $\eta = 0$, $\eta = 2$, and $\eta = 3$ cases are shown in Fig. 2, where we

see the biggest gain in secrecy is to be had by growing the cache size, but significant gains can be achieved by optimizing caching patterns as well.

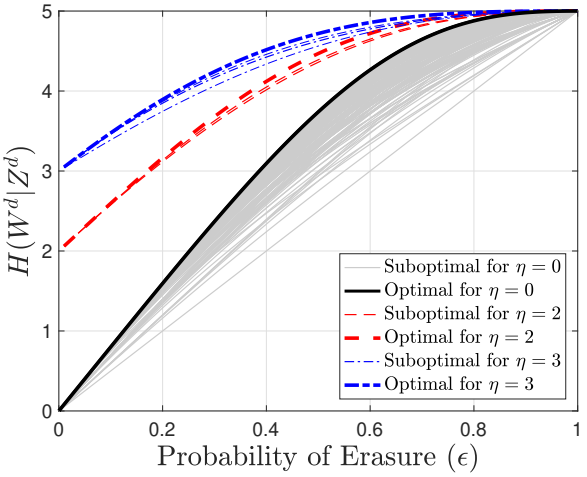

Fig. 2. Exact equivocation for suboptimal and optimal selections of codes and caching patterns. For $\eta = 2$ and $\eta = 3$, only curves for caching patterns relating to the optimal code are plotted.

We further studied the $n = 8$, $k = 4$ case, and found the best code to be the RM(1,3) code, i.e., the rate-1/2 length-8 Reed-Muller code [23]. For this case, the symmetry invoked in the code construction made all caching patterns of size $\eta = 2$ and $\eta = 3$ identical in terms of their equivocation matrices, but this is usually not the case for codes with other size parameters.

VI. Discussion and Future Directions

The outcome of this work demonstrates the promising result that caching techniques can be used to increase the equivocation at the eavesdropper with finite blocklength wiretap coding. We show how some tools may be used for small finite blocklength codes to find optimal coding and caching solutions, but this approach also has limitations.

For this initial work, we focused on arguably the simplest wiretap channel model with caching, where the main channel and caching channel are error-free to Bob, Eve does not have access to the cache, and the eavesdropping channel is a BEC. Due to the error-free reception of all coded bits at Bob, basic coset codes with no error correction can be used (see, e.g., [14], [15]. However, this approach can be extended to noisy main channels, various types of main and eavesdropping channels (including binary symmetric channels, and even Gaussian channels), as well as cases where Eve is able to tap the cache, and Bob's reliable use of the cache may be less certain. Each of these future directions brings its own set of challenges, but also makes the concepts more adaptable to real-world scenarios.

Expanding the optimization results, regarding the choice of code and caching pattern, to larger blocklength coding cases will require optimality proofs for specific constructions of codes, as searching through the space of all codes and all caching patterns becomes infeasible even at blocklengths as small as $n = 15$.

The caching gain could also be improved, along with coded caching techniques, although this will likely require the use of a key, whereas the results of the paper can be attained without the need for sharing secret keys. Coded caching may allow us to shrink the size of the cache, and still enjoy gains in equivocation at the eavesdropper. In addition, multiple receivers should be considered, and different caching architectures should be studied so as to expand the benefits of wiretap coding with a cache.

VII. Conclusion

In this paper, we presented a concept to increase the exact equivocation at the eavesdropper over a binary erasure wiretap channel when a secure cache is available to Alice and Bob. We showed how to optimize the choice of a code and a caching pattern for small blocklength codes, and derived two new channel models from the scenario. These channel models allow Alice the benefit of puncturing bits at the eavesdropper without puncturing them at the legitimate receiver using the secure cache. An approach to optimal coding over the new channel models was presented, and exhaustive techniques were shown to be effective in finding optimal structures to maximize the equivocation at Eve for a small blocklength example. In another case, it was shown that some codes may be provably optimal, even to the extent that all caching patterns may be equally optimal when the code is deployed.

References

[1] G. S. Paschos, G. Iosifidis, M. Tao, D. Towsley, and G. Caire, "The role of caching in future communication systems and networks," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 6, pp. 1111–1125, June 2018.

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

[3] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*. Cambridge, UK: Cambridge University Press, 2011.

[4] W. K. Harrison, J. Almeida, M. R. Bloch, S. W. McLaughlin, and J. Barros, "Coding for secrecy: An overview of error-control coding techniques for physical-layer security," *IEEE Signal Processing Magazine*, vol. 30, no. 5, pp. 41–50, Sept. 2013.

[5] M. Mohammadi Amiri, Q. Yang, and D. Gündüz, "Coded caching for a large number of users," in *Proc. IEEE Information Theory Workshop (ITW)*, Sep. 2016, pp. 171–175.

[6] L. Tang and A. Ramamoorthy, "Coded caching schemes with reduced subpacketization from linear block codes," *IEEE Trans. Inf. Theory*, vol. 64, no. 4, pp. 3099–3120, Apr. 2018.

[7] M. Mohammadi Amiri and D. Gündüz, "Fundamental limits of coded caching: Improved delivery rate-cache capacity tradeoff," *IEEE Trans. Commun.*, vol. 65, no. 2, pp. 806–815, Feb. 2017.

[8] ——, "Caching and coded delivery over gaussian broadcast channels for energy efficiency," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 8, pp. 1706–1720, Aug. 2018.

[9] H. Al-Lawati, N. Ferdinandy, and S. C. Draperz, "Coded caching with non-identical user demands," in *Proc. Canadian Workshop Information Theory (CWIT)*, June 2017, pp. 1–5.

[10] A. A. Zewail and A. Yener, "The wiretap channel with a cache," in *Proc. IEEE Int. Symp. Information Theory (ISIT)*, June 2018, pp. 1720–1724.

[11] S. Kamel, M. Wigger, and M. Sarkiss, "Coded caching for wiretap broadcast channels," in *Proc. IEEE Information Theory Workshop (ITW)*, Nov. 2017, pp. 11–15.

[12] M. Nafea and A. Yener, "The caching broadcast channel with a wire and cache tapping adversary of type II," in *Proc. IEEE Information Theory Workshop (ITW)*, Nov. 2018, pp. 1–5.

[13] ——, "The caching broadcast channel with a wire and cache tapping adversary of type II: Multiple library files," in *Proc. Allerton Conference on Communication, Control, and Computing*, Oct. 2018, pp. 989–996.
[14] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.
[15] A. Thangaraj, S. Dihidar, A. R. Calderbank, S. W. McLaughlin, and J. Merolla, "Applications of LDPC codes to the wiretap channel," *IEEE Trans. Inf. Theory*, vol. 53, no. 8, pp. 2933–2945, Aug. 2007.
[16] J. Pfister, M. A. C. Gomes, J. P. Vilela, and W. K. Harrison, "Quantifying equivocation for finite blocklength wiretap codes," in *Proc. IEEE Int. Conf. Communications (ICC)*, May 2017, pp. 1–6.
[17] W. K. Harrison and M. R. Bloch, "On dual relationships of secrecy codes," in *Proc. Allerton Conference on Communication, Control, and Computing*, Oct. 2018, pp. 366–372.
[18] W. K. Harrison and M. R. Bloch, "Attributes of generators for best finite blocklength coset wiretap codes over erasure channels," in *Proc. IEEE Int. Symp. Information Theory (ISIT)*, July 2019, pp. 827–831.
[19] M. Nafea and A. Yener, "Wiretap channel II with a noisy main channel," in *Proc. IEEE Int. Symp. Information Theory (ISIT)*, June 2015, pp. 1159–1163.
[20] ——, "A new wiretap channel model and its strong secrecy capacity," *IEEE Trans. Inf. Theory*, vol. 64, no. 3, pp. 2077–2092, Mar. 2018.
[21] A. Frank, H. Aydinian, and H. Boche, "Type II wiretap channel with an active eavesdropper in finite blocklength regime," in *Proc. IEEE Wireless Communications and Networking Conference Workshops (WCNCW)*, Apr. 2016, pp. 258–263.
[22] P. Wang and R. Safavi-Naini, "A model for adversarial wiretap channels," *IEEE Trans. Inf. Theory*, vol. 62, no. 2, pp. 970–983, Feb. 2016.
[23] T. K. Moon, *Error Correction Coding: Mathematical Methods and Algorithms*. Hoboken, New Jersey: John Wiley & Sons, Inc., 2005.