The Wiretap Channel with a Cache

Ahmed A. Zewail and Aylin Yener

Wireless Communications and Networking Laboratory (WCAN)
The School of Electrical Engineering and Computer Science
The Pennsylvania State University, University Park, PA 16802.
zewail@psu.edu *yener@engr.psu.edu*

***Abstract*—We consider the wiretap channel when a (secure) cache memory is added to the legitimate receiver. With the goal of utilizing coded caching for improving secrecy, during the cache placement phase, the receiver caches a function of the files, and the secret key shared with the transmitter subject to the memory constraint. The signals transmitted to serve the receiver's request during the delivery phase are observed by an eavesdropper over a wiretap channel. We characterize the secrecy capacity of the wiretap channel with a cache, i.e., the maximum achievable file size while keeping the overall database secure, for both the discrete memoryless and the Gaussian channels. The optimal caching scheme maximizes the utilization from the transmission over the delivery phase by sharing sufficient amount of keys between the legitimate communication nodes during the placement phase. Interestingly, we demonstrate that the existence of cache memory is an enabler of secure communication, i.e., the secrecy capacity remains positive, even when the main channel is degraded with respect to the eavesdropper channel.**

I. Introduction

The wiretap channel introduced by Wyner in [1] has provided the foundation for information theoretically secure communication in the presence of an eavesdropper. In addition to a number of extensions and generalizations in the single user setting [2]–[8], multi-terminal wiretap channels have also been investigated extensively to date, see for example [9]–[15].

In this work, we consider the single user wiretap channel when a cache memory is added to the legitimate receiver. The goal of utilizing the cache at the receiver is to improve the secrecy capacity of the channel. We demonstrate that the secrecy capacity is improved with this additional resource, and that in instances where the wiretap channel is reversely degraded where secure communication is otherwise impossible, the existence of this additional resource enables a non-zero secrecy capacity. The model is in line with the recently introduced coded caching paradigm [16], and imposes the secure delivery constraint studied for multireceiver channels in recent references [17]–[20]. Unlike the coded caching references to date where the primary objective is to provide improvement by means of multicasting in broadcast or other multireceiver set ups, in this work, the primary utilization of the cache memory at the single receiver is as a resource for secure communication, i.e., one that increases the secrecy capacity of the channel.

We establish the secrecy capacity of the discrete memoryless wiretap channel as a function of the memory constraint and as a corollary the secrecy capacity of the Gaussian wiretap channel under the same memory model.

In line with recent information theoretic models of caching, the transmitter has access to a data base of files (messages) any one of which may be requested by the receiver. The system operates over two phases: a *secure* cache placement phase and delivery phase over a *wiretap* channel. In particular, during the cache placement phase, the receiver populates its cache with a function of the database files as well as keys shared with the transmitter subject to the memory capacity constraint. When the receiver requests a file, the delivery phase occurs over a wiretap channel. All database files, i.e., all messages must be kept secret from the wiretapper.

The fundamental gains transpire in this model due to the presence of the secure cache. We characterize the optimal caching and delivery strategies which maximize the achievable file size, while satisfying the secrecy constraint. We characterize the capacity of this setting, both for discrete memoryless and Gaussian wiretap channels, by defining the optimal memory partitioning between cached data and shared keys and the optimal delivery policy. The secrecy capacity is piece-wise linear in the cache size. As long as the cache size is less than the minimum of the main channel and the wiretapper channel capacities, the linear scaling factor is unity, while after that point, the scaling factor is normalized by the number of database files. The learned insights from this study include prioritizing keys during the cache placement: for example, whenever the cache size is less than the minimum between the main channel and the wiretapper channel capacities, the cache is dedicated to storing keys only. In addition, when the main channel is degraded with respect to the wiretapper channel, the cache acts as an enabler of communication, in other words the cache facilitates non-zero secrecy rates over this channel.

II. System Model

Consider the wiretap channel with a cache memory at the legitimate receiver, shown in Fig. 1. The transmitter has a library of D files, $W_1, .., W_D$, each of which has size nR bits. The files are independent and uniformly distributed over the set $\{1, .., 2^{nR}\}$. The receiver is equipped with a cache memory of size nM bits. The system operates over two phases.

A. Cache Placement Phase

The cache placement is assumed to be error free and secure from wiretapper. The transmitter populates the receiver's cache

978-1-5386-4780-6/18/$31.00©2018 IEEE

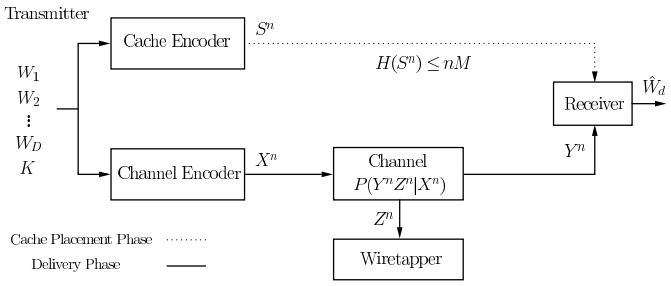

Fig. 1: The wiretap channel with receiver's cache.

with a function of the library files and a shared key. Let M_D represent the fraction of the memory dedicated to store data and M_K be fraction dedicated for the shared key. The cache at the legitimate receiver stores

$$S_D^n = \mu(W_1, .., W_D), \qquad H(S_D^n) = nM_D. \tag{1}$$

The transmitter generates a secure random key, K, that is independent from the files $\{W_1, .., W_D\}$ and uniformly distributed over the set $\{1, .., 2^{nM_K}\}$. We denote all cached contents by the receiver by S^n.The system designs the cached content subject to the memory capacity constraint. Thus, we have

$$H(S^n) = H(S_D^n, K) = nM_D + nM_K \leq nM. \tag{2}$$

B. Delivery Phase

The receiver requests one of the database files at random [16], i.e., the demand profile is assumed to be uniform. We denote the requested file by W_d. The transmitter responds to this request by sending a signal over a discrete memoryless wiretap channel [2], described by

$$P(Y^n = y^n, Z^n = z^n | X^n = x^n) = \prod_{i=1}^{n} P(Y_i = y_i, Z_i = z_i | X_i = x_i), \tag{3}$$

where n is the number of channel uses, $X_i \in \mathcal{X}$ is the channel input, $Y_i \in \mathcal{Y}$ and $Z_i \in \mathcal{Z}$ are the channel outputs at channel use i at the legitimate receiver and the wiretapper, respectively. In particular, the transmitter encodes the requested file and the shared key using stochastic encoding [1] into the signal X^n. Equivalently, we have

$$X^n = \phi(W_d, K, K'), \tag{4}$$

where K' is the local randomness at the transmitter. Using Y^n and the cached contents, the receiver must be able to decode its requested file reliably, i.e., for the decoded file $\hat{W}_d = \lambda(Y^n, S^n)$, for any $\delta > 0$, we have

$$P(\hat{W}_d \neq W_d) < \delta. \tag{5}$$

Since any file from the database can be requested in the delivery phase, all files need to be kept secret from the wiretapper [17]–[20]. Thus, for any $\epsilon > 0$, we have the following secrecy constraint.

$$H(W_1, .., W_D | Z^n) \geq H(W_1, .., W_D) - n\epsilon. \tag{6}$$

The rate-memory tuple (R, M) is said to be achievable, if for $n \to \infty$, there exist a caching function, μ, a shared key K, an encoding function, ϕ, and a decoding function, λ, such that for any $\epsilon, \delta > 0$ conditions (5) and (6) are satisfied. Furthermore, the secrecy capacity of the considered wiretap channel is defined as $\sup\{(R, M) : (R, M) \text{ is achievable}\}$.

III. Main Result

Theorem 1. *The secrecy capacity of the wiretap channel with a cache with total memory M is given by*

$$R = \max_{M_D + M_K \leq M} \max_{U - V - X - (Y,Z)} \min([I(Y;V|U) - I(V;Z|U)]^+ + M_K, I(V;Y)) + \frac{M_D}{D}, \tag{7}$$

for some random variables U and V.

We observe that the outer maximization in (7) maximizes the sum of two terms. The first term represents the capacity of wiretap channel with shared key of size nM_K bits like in [8]. The second term represents the data caching gain, i.e., the fraction of the memory dedicated to store the bits of each of the D files. For the degraded wiretap channel [1], the corollary below immediately follows; we will use it in Section V.

Corollary 1. *The capacity of a degraded wiretap channel with cache, i.e., $X - Y - Z$, is given by*

$$R = \max_{M_D + M_K \leq M} \max_{X - Y - Z} \min(I(X;Y) + M_K - I(X;Z), I(X;Y)) + \frac{M_D}{D}. \tag{8}$$

■

IV. Proof of Theorem 1

A. Achievability

First, we show the achievability of the file size given in Theorem 1. For a fixed choice of the parameters M_D and M_K, we show the achievability of the following file size:

$$R = \max_{U - V - X - (Y,Z)} \min([I(V;Y|U) - I(V;Z|U)]^+ + M_K, I(V;Y)) + \frac{M_D}{D}. \tag{9}$$

During the placement phase, we divide each file W_i into two subfiles, W_i^c, and W_i^t. W_i^c has length equal to $\frac{nM_D}{D}$ bits and will be cached by the receiver. W_i^t with length $n(R - \frac{M_D}{D})$ bits is only known at the transmitter during this phase. In addition, the transmitter generates random key, K, with length nM_K bits, that is uniformly distributed over the set $\{1, .., 2^{nM_K}\}$ and places it in the cache memory of the receiver. Thus, the number of bits cached by the receiver is $D|W_i^c| + |K| = \frac{nDM_D}{D} + nM_K \leq nM$, i.e., the memory constraint is satisfied.

At the beginning of the delivery phase, the receiver requests W_d. The subfile W_d^c can be retrieved from the receiver's cache, while the subfile W_d^t needs to be transmitted securely over the wiretap channel. The transmission over the wiretap channel follows the techniques for a wiretap channel with shared key of length nM_K bits [8]. The size of the key and the degradedness

of the channel determine the optimal utilization of the key: either we use it as a randomization index in the codebook, or as a one-time pad [21], to satisfy the secrecy constraint (6).

B. Converse

To prove the converse, first we fix a partitioning of the cache memory, i.e., M_D and M_K. Suppose that the receiver requests the file W_j. Then, we have the following lemma.

Lemma 1. *For a fixed choice of M_D and M_K, the achievable file size is upper bounded by*

$$R \leq \min([I(Y;V|U) - I(V;Z|U)]^+ + M_K, I(V;Y)) + \frac{1}{n} I(S_D^n; W_j), \tag{10}$$

for some random variables U and V such that $U - V - X - (Y, Z)$.

Proof. Proof is provided in the Appendix. □

By averaging over all possible file requests, we obtain

$$R \leq \min([I(Y;V|U) - I(V;Z|U)]^+ + M_K, I(V;Y)) + \frac{1}{D}\sum_{i=1}^{D} \frac{1}{n} I(S_D^n; W_i). \tag{11}$$

In addition, we have

$$\sum_{i=1}^{D} I(S_D^n; W_i) = \sum_{i=1}^{D} H(W_i) - H(W_i|S_D^n) \tag{12}$$

$$\leq \sum_{i=1}^{D} H(W_i|W_1,..,W_{i-1}) - H(W_i|S_D^n W_1,..,W_{i-1}) \tag{13}$$

$$= \sum_{i=1}^{D} I(W_i, S_D^n|W_1,..,W_{i-1}) \tag{14}$$

$$= I(W_1,...,W_D; S_D^n) \leq H(S_D^n) = nM_D. \tag{15}$$

Finally, we maximize the obtained bound over all possible memory partitions, which yields (7), concluding the converse.

V. The Gaussian Wiretap Channel with a Cache

In this section, we consider the wiretap channel with a cache, with the same placement model and the delivery phase is performed over a Gaussian wiretap channel. At the ith channel use, the legitimate receiver and the wiretapper receive

$$Y(i) = X(i) + N_1(i), \qquad Z(i) = X(i) + N_2(i), \tag{16}$$

where N_1 and N_2 are the additive white Gaussian noise with zero-mean and variances σ_1^2 and σ_2^2, respectively. The average power constraint is P. From Corollary 1, following the same arguments as in [7], and by choosing X to be Gaussian with zero-mean and variance P, we obtain the following.

Corollary 2. *The capacity of the Gaussian wiretap channel with a cache is given by*

$$R = \max_{M_D + M_K \leq M} \min([C_M - C_E]^+ + M_K, C_M) + \frac{M_D}{D}, \tag{17}$$

where $C_M = \frac{1}{2}\log_2(1 + \frac{P}{\sigma_1^2})$ and $C_E = \frac{1}{2}\log_2(1 + \frac{P}{\sigma_2^2})$. ■

Next, we present the optimal caching scheme.

A. $C_M \leq C_E$

Without the cache memory, the secrecy capacity of this channel is 0 [3].

1) $M \leq C_M$: Suppose the receiver is equipped with a cache memory with size $0 < nM \leq nC_M$ bits. If we dedicate the cache for storing data only, the file size that we can achieve is $\frac{nM}{D}$ bits due to the local caching gain only, as there is no possibility of secure transmission during the delivery phase. However, if the transmitter generates a random key, K, of size nM bits to be cached by the receiver during the placement phase, during the delivery phase, assuming the receiver requests W_j, the transmitter can encrypt W_j with K as one-time pad [21] and send it over the channel. Thus, we can achieve a file size equal to nM bits, which is optimal, from Corollary 2. In this scenario, caching a key is the *enabler* of secure communication over this wiretap channel during the delivery phase.

2) $M > C_M$: In this case, we choose $M_K = C_M$ to store a key, K, of size nC_M bits while the remaining memory is divided equally to cache bits from each file. In particular, each file, W_n is divided into W_n^t with size nC_M bits and W_n^c of size $n\frac{M - C_M}{D}$ bits. In addition to the cached key, the receiver caches the subfiles $\{W_n^c, \forall n\}$. During the delivery phase, the transmitter encodes $W_d^t \oplus K$ and sends it over the channel. Thus, whenever $C_M \leq C_E$, we achieve the following file size

$$R = \begin{cases} M, & \text{if } M \leq C_M, \\ C_M + \frac{M}{D} - \frac{C_M}{D}, & \text{if } M > C_M. \end{cases} \tag{18}$$

B. $C_M > C_E$

Without the cache, the secrecy capacity is $C_M - C_E$ [3].

1) $M \leq C_E$: If we cache only files, the gain we obtain is normalized by the library size D. For example, by caching a fraction $\frac{M}{D}$ from each file and transmitting the missing bits of the requested file using a wiretap code [3], we can achieve

$$R = C_M - C_E + \frac{M}{D}. \tag{19}$$

Instead, in our scheme, the receiver caches a key, K, of size nM bits, to be used as a randomization index in the codebook used to transmit the requested file to the receiver during the delivery phase. In particular, we generate 2^{nM} codebooks, each of which is indexed by a possible realization of the key and has 2^{nC_M} codewords. We partition each codebook into 2^{nR} equal-size bins each of which is indexed by a possible realization of a file. When the receiver requests the file W_d, from the codebook indexed by K, the transmitter randomly picks a codeword from the bin indexed by W_d and transmits it over the channel. Since the codebook index is cached by the receiver, we can securely achieve

$$R = C_M - C_E + M. \tag{20}$$

Clearly, (20) is larger than (19) for all $D > 1$.

2) $M > C_E$: In this case, the receiver caches a key, K, of size nC_E bits and $n\frac{M - C_E}{D}$ bits from each file. In particular, W_n is divided into W_n^t of size nC_M bits and W_n^c of size

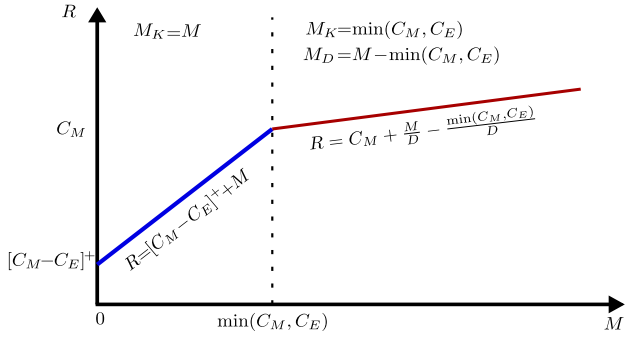

Fig. 2: File size of Gaussian wiretap channel with a cache.

$n\frac{M-C_E}{D}$ bits to be cached by the receiver. During the delivery phase, K is used as a randomization index in the codebook used to transmit W_d^t [7], [8]. Therefore, the following file size is achievable, whenever $C_M > C_E$,

$$R = \begin{cases} C_M - C_E + M, & \text{if } M \le C_E, \\ C_M + \frac{M}{D} - \frac{C_E}{D}, & \text{if } M > C_E. \end{cases} \tag{21}$$

Consequently, we get the following proposition about the optimal file size for the Gaussian wiretap channel with a cache.

Proposition 1. *For a Gaussian wiretap channel with a cache of size M, the optimal file size is given by*

$$R = \begin{cases} [C_M - C_E]^+ + M, & \text{if } M \le \min(C_M, C_E), \\ C_M + \frac{M}{D} - \frac{\min(C_M, C_E)}{D}, & \text{if } M > \min(C_M, C_E). \end{cases} \tag{22}$$

□

VI. Discussion

In this section, we discuss the learned insights from this study. For simplicity, we focus on the Gaussian setting, noting that the insights are valid for the discrete memoryless channel.

A. Caching Gain

Observe from (22), illustrated in Fig. 2, that the file size, R, is a piece-wise linear function of the cache memory size, M. In particular, R scales with factor 1 in the small memory regime, i.e., $M \le \min(C_M, C_E)$, where the cache is exclusively dedicated for storing keys. On the other hand, in the large memory regime, whenever $M > \min(C_M, C_E)$, the gain from the memory is scaled by $\frac{1}{D}$, where the memory is divided between storing keys and the data files.

B. Secrecy Cost

Without the secrecy requirement, the capacity of a point-to-point channel with a cache of size M is $C_M + \frac{M}{D}$. Under the secrecy requirement and as long as $M > \min(C_M, C_E)$, the capacity of the channel is $C_M + \frac{M}{D} - \frac{\min(C_M, C_E)}{D}$. Thus, we can consider the term $\frac{\min(C_M, C_E)}{D}$ as the cost due to imposing the secrecy requirement on the system. In this case, we dedicate $n\min(C_M, C_E)$ bits from the cache to store a key to facilitate the secure transmission with the main channel capacity, C_M during the delivery phase.

When $C_E < C_M$, without the cache, the secrecy cost is C_E [3]. As evident from (21), the presence of the cache helps on reducing the secrecy cost to $\frac{C_E}{D}$. Therefore, caching not only aids the system in satisfying the secrecy constraint but also allows reducing the cost due to the secrecy requirement.

When $C_M \le C_E$, the cache is the enabler of communication as without it the secrecy capacity is 0 [3].

C. Intuition Behind the Optimal Scheme

For the small memory regime, the optimal scheme dedicates all the cache memory to storing secure shared keys. In other words, the optimal scheme prioritizes keys over files, subject to the memory constraint, until the transmitter is able to fully utilize the channel during the delivery phase. After that we start caching from the database files. That is, the gain from transmitting during the delivery phase contributes to the number of retrieved bits from the requested file only, while the partition of the memory dedicated for caching data is distributed among all the database files.

VII. Conclusion and Future Directions

In this paper, we have introduced the wiretap channel with a cache and derived its secrecy capacity. During the cache placement phase, in addition to caching data, the transmitter can share a secure key with the receiver subject to the memory capacity constraint. The delivery phase takes place over a wiretap channel. We have characterized the maximum achievable file size by defining the optimal caching strategy and transmission technique. In the small cache region, the cache is dedicated to storing keys. In the large cache regime, caching helps in reducing the secrecy rate cost of the system by normalizing it by the number of files. In addition, the utilization of the cache renders secure communication possible even when the legitimate channel is degraded with respect to the wiretapper.

This work takes the position of utilizing receiver cache memory as a resource to improve secrecy. Natural next steps include multi-transmitter settings where channel based techniques can be synergistically utilized with caching.

Appendix
Proof of Lemma 1

The proof of Lemma 1 generalizes the converse proof in [8]. First, from reference [22], we have the following

$$H(Y^n) - H(Z^n) = \sum_{i=1}^{n} H(Y_i|Y^{i-1}Z_{i+1}^n) - H(Z_i|Y^{i-1}Z_{i+1}^n), \tag{23}$$

$$H(Y^n|W_jS^n) - H(Z^n|W_jS^n) = \sum_{i=1}^{n} H(Y_i|Y^{i-1}Z_{i+1}^n W_jS^n) - H(Z_i|Y^{i-1}Z_{i+1}^n W_jS^n). \tag{24}$$

Define $U_i = (Y^{i-1}, Z_{i+1}^n)$, and Q as a time sharing random variable that is uniform over $\{1, ..n\}$ that is independent from all other random variables. In addition, let $U = (U_i, Q)$, $V = (U, W_j, S^n)$, $X = X_Q$, $Y = Y_Q$ and $Z = Z_Q$. Observe that

$U-V-X-(Y,Z)$. From reference [22], we know that there exist real numbers t_1 and t_2 such that

$$\frac{1}{n}H(Y^n) = H(Y|U) + t_1, \tag{25}$$
$$\frac{1}{n}H(Z^n) = H(Z|U) + t_1, \tag{26}$$
$$\frac{1}{n}H(Y^n|W_j, S^n) = H(Y|V) + t_2, \tag{27}$$
$$\frac{1}{n}H(Z^n|W_j, S^n) = H(Z|V) + t_2, \tag{28}$$
$$\text{where} \quad 0 \le t_1 \le \min(I(U;Y), I(U;Z)), \tag{29}$$
$$0 \le t_2 \le \min(I(V;Y), I(V;Z)). \tag{30}$$

From the secrecy constraint, (6), we have

$$\begin{aligned}
n\epsilon &\ge I(W_1, .., W_D; Z^n) \ge I(W_j; Z^n) \\
&= I(W_j S^n; Z^n) - I(S^n; Z^n|W_j) && (31)\\
&= I(W_j S^n; Z^n) - I(K; Z^n|W_j) - I(S_D^n; Z^n|W_j K) && (32)\\
&= H(Z^n) - H(Z^n|W_j S^n) - H(K|W_j) + H(K|W_j Z^n) \\
&\quad - H(S_D^n|W_j K) + H(S_D^n|W_j K Z^n) && (33)\\
&\ge H(Z^n) - H(Z^n|W_j S^n) - H(K) \\
&\quad - H(S_D^n|W_j K) + H(S_D^n|W_j K Z^n) && (34)\\
&= H(Z^n) - H(Z^n|W_j S^n) - H(K) \\
&\quad - H(S_D^n|W_j K K') + H(S_D^n|W_j K Z^n) && (35)\\
&\ge H(Z^n) - H(Z^n|W_j S^n) - H(K) \\
&\quad - H(S_D^n|W_j K K') + H(S_D^n|W_j K K' Z^n) && (36)\\
&= H(Z^n) - H(Z^n|W_j S^n) - H(K) \\
&\quad - H(S_D^n|W_j K K' X^n) + H(S_D^n|W_j K K' Z^n) && (37)\\
&\ge H(Z^n) - H(Z^n|W_j S^n) - H(K) \\
&\quad - H(S_D^n|W_j K K' X^n) + H(S_D^n|W_j K K' X^n Z^n) && (38)\\
&= H(Z^n) - H(Z^n|W_j S^n) - H(K) \\
&\quad - I(S_D^n; Z^n|W_j K K' X^n) && (39)\\
&= H(Z^n) - H(Z^n|W_j S^n) - H(K). && (40)
\end{aligned}$$

Step (35) follows from the independence between S_D^n and K'. Steps (36) and (38) are due to the fact that conditioning cannot increase the entropy. (37) follows from (4). Finally, (40) follows from the fact that $(W_j, K, K', S_D^n) - X^n - Z^n$. Thus, we have

$$n\epsilon \ge nH(Z|U) + nt_1 - nH(Z|V) - nt_2 - nM_K, \tag{41}$$
$$t_1 - t_2 \le M_K - I(Z;V|U) + \epsilon, \tag{42}$$
$$t_1 - t_2 \le t_1 \le \min(I(U;Y), I(U;Z)). \tag{43}$$

Therefore, we get

$$t_1 - t_2 \le \min(M_K - I(Z;V|U) + \epsilon, I(U;Y), I(U;Z)). \tag{44}$$

Now, from the reliability requirement in (5), we have

$$\begin{aligned}
H(W_j) &= H(W_j|K) && (45)\\
&\le H(W_j|K) - H(W_j|Y^n, S_D^n K) + n\delta && (46)\\
&= I(W_j; S_D^n Y^n|K) + n\delta && (47)\\
&\le I(W_j K; S^n Y^n) + n\delta && (48)\\
&= I(W_j K; S_D^n) + I(W_j K; Y^n|S_D^n) + n\delta && (49)\\
&= H(S_D^n) - H(S_D^n|W_j K) + H(Y^n|S_D^n) \\
&\quad - H(Y^n|S_D^n W_j K) + n\delta && (50)\\
&\le H(S_D^n) - H(S_D^n|W_j) + H(Y^n) - H(Y^n|S_D^n W_j K) + n\delta && (51)\\
&= I(S_D^n; W_j) + n(H(Y|U) + t_1 - H(Y|V) - t_2) + n\delta && (52)\\
&\le I(S_D^n; W_j) + n(I(Y;V|U) + t_1 - t_2) + n\delta. && (53)
\end{aligned}$$

Putting these all together, we get (11).

REFERENCES

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

[2] I. Csiszár and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. Info. Theory*, vol. 24, no. 3, pp. 339–348, 1978.

[3] S. Leung-Yan-Cheong and M. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Info. Theory*, vol. 24, no. 4, pp. 451–456, 1978.

[4] Y. Liang, H. V. Poor, and S. Shamai, "Secure communication over fading channels," *IEEE Trans. Info. Theory*, vol. 54, no. 6, pp. 2470–2492, 2008.

[5] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas-Part II: The MIMOME wiretap channel," *IEEE Trans. Info. Theory*, vol. 56, no. 11, pp. 5515–5532, 2010.

[6] H. Yamamoto, "Rate-distortion theory for the shannon cipher system," *IEEE Trans. Info. Theory*, vol. 43, no. 3, pp. 827–835, 1997.

[7] E. Ardestanizadeh, M. Franceschetti, T. Javidi, and Y.-H. Kim, "Wiretap channel with secure rate-limited feedback," *IEEE Trans. Info. Theory*, vol. 55, no. 12, pp. 5353–5361, 2009.

[8] W. Kang and N. Liu, "Wiretap channel with shared key," in *IEEE Information Theory Workshop (ITW)*, 2010.

[9] E. Tekin and A. Yener, "The general Gaussian multiple-access and two-way wiretap channels: Achievable rates and cooperative jamming," *IEEE Trans. Info. Theory*, vol. 54, no. 6, pp. 2735–2751, 2008.

[10] ——, "The Gaussian multiple access wire-tap channel," *IEEE Trans. Info. Theory*, vol. 54, no. 12, pp. 5747–5755, 2008.

[11] X. He and A. Yener, "The role of feedback in two-way secure communications," *IEEE Trans. Info. Theory*, vol. 59, no. 12, pp. 8115–8130, 2013.

[12] ——, "Providing secrecy with structured codes: Two-user Gaussian channels," *IEEE Trans. Info. Theory*, vol. 60, no. 4, pp. 2121–2138, 2014.

[13] R. Liu, I. Maric, P. Spasojevic, and R. D. Yates, "Discrete memoryless interference and broadcast channels with confidential messages: Secrecy rate regions," *IEEE Trans. Info. Theory*, vol. 54, no. 6, pp. 2493–2507, 2008.

[14] E. Ekrem and S. Ulukus, "Secrecy capacity of a class of broadcast channels with an eavesdropper," *EURASIP Journal on Wireless Communications and Networking*, vol. 2009, no. 1, 2009.

[15] ——, "The secrecy capacity region of the Gaussian MIMO multi-receiver wiretap channel," *IEEE Trans. Info. Theory*, vol. 57, no. 4, pp. 2083–2114, 2011.

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

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

[18] A. A. Zewail and A. Yener, "Coded caching for resolvable networks with security requirements," in *IEEE Conference on Communications and Network Security (CNS)*, 2016.

[19] S. Kamel, M. Sarkiss, and M. Wigger, "Secure joint cache-channel coding over erasure broadcast channels," in *IEEE Wireless Communications and Networking Conference (WCNC)*, 2017.

[20] ——, "Coded caching for wiretap broadcast channels," in *IEEE Information Theory Workshop (ITW)*, 2017.

[21] C. E. Shannon, "Communication theory of secrecy systems," *Bell system technical journal*, vol. 28, no. 4, pp. 656–715, 1949.

[22] I. Csiszar and J. Korner, "Information theory: Coding theorems for discrete memoryless systems," in *Academic Press*, 1981.