# The Gelfand-Pinsker Wiretap Channel: Higher Secrecy Rates via a Novel Superposition Code

Ziv Goldfeld
Ben Gurion University
gziv@post.bgu.ac.il

Paul Cuff
Princeton University
cuff@princeton.edu

Haim H. Permuter
Ben Gurion University
haimp@bgu.ac.il

***Abstract*—To be considered for the 2017 IEEE Jack Keil Wolf ISIT Student Paper Award. We study the state-dependent (SD) wiretap channel (WTC) with non-causal channel state information (CSI) at the encoder. This model subsumes all other instances of CSI availability as special cases, and calls for an efficient utilization of the state sequence both for reliability and security purposes. A lower bound on the secrecy-capacity, that improves upon the previously best known result by Chen and Han Vinck, is derived based on a novel superposition coding scheme. The improvement over the Chen and Han Vinck result is strict for some SD-WTCs. Specializing the lower bound to the case where CSI is also available to the decoder reveals that it is at least as good as the achievable formula by Chia and El-Gamal, which is already known to outperform the adaptation of the Chen and Han Vinck code to the encoder and decoder CSI scenario. The results are derived under the strict semantic-security metric that requires negligible information leakage for all message distributions. The proof of achievability relies on a stronger version of the soft-covering lemma for superposition codes.**

## I. Introduction

Reliably transmitting a message over a noisy state-dependent (SD) channel with non-causal encoder channel state information (CSI) is a fundamental information theoretic scenario. This problem was formulated by Gelfand and Pinsker (GP) in their celebrated paper [1], where they also derived its capacity. Not only did the result from [1] have various implication for many information-theoretic problems (such as the broadcast channel), it is also the most general instance of a SD point-to-point channel in which any or all of the terminals have non-causal access to the sequence of states. Motivated by the above as well as the indisputable importance of security in modern communication systems, we study the SD wiretap channel (WTC) with non-causal encoder CSI, which incorporates the notion of security in the presence of a wiretapper into the GP channel coding problem.

First to consider a discrete and memoryless (DM) WTC with random states were Chen and Han Vinck [2], who studied the encoder CSI scenario. They established a lower bound on the secrecy-capacity based on a combination of wiretap coding with GP coding. This work was later generalized in [3] to a WTC that is driven by a pair of states, one available to the encoder and the other one to the decoder. However, as previously mentioned, since CSI at the encoder is the most general setup, the result of [3] is a special of [2]. A more sophisticated coding scheme was constructed by Chia and El-Gamal for the SD-WTC with causal encoder CSI and full decoder CSI [4]. Their idea was to explicitly extract a cryptographic key from the random state, and encrypt part of the confidential message via a one-time-pad with that key. The remaining portion of the confidential message is protected by a wiretap code (whenever wiretap coding is possible). Although their code is restricted to utilize the state in a causal manner, the authors of [4] proved that it can strictly outperform the adaptations of the non-causal schemes from [2], [3] to the encoder and decoder CSI setup.

In this paper we study the SD-WTC with non-causal encoder CSI, for which we propose a novel superposition-based coding scheme. The scheme results in a new lower bound on the secrecy-capacity, which recovers the previously best known achievability formulas from [2] and [3] as special cases. To show that the relation to the previous schemes can be strict we fashion an example where our scheme achieves strictly higher secrecy rates than [2], [3]. The example is a specific instance of a class of SD-WTCs whose channel transition probability decomposes into a WTC that is independent of the state and another channel that generates two noisy versions of the state, each observed either by the legitimate receiver or by the eavesdropper. For this class of channels, our lower bound is tight whenever the eavesdropper's observation is less noisy than this of the legitimate user

When specializing to the case where the decoder also knows the state sequence, our achievability is at least as good as the scheme from [4]. Interestingly, while the scheme from [4] relies on generating the aforementioned cryptographic key, our code construction does not involve any explicit key generation/agreement phase. Instead, we use an over-populated superposition codebook and encode the entire confidential message at the outer layer. The transmission is correlated with the state sequence by means of the likelihood encoder [5], while security is ensured by making the eavesdropper decode the inner layer codeword that contains no confidential information. Having done so, the eavesdropper is lacking the resources to extract any information about the secret message.

Our results are derived under the strict metric of semantic-security (SS). The SS criterion is a cryptographic benchmark that was adapted to the information-theoretic framework (of computationally unbounded adversaries) in [6]. In that work, SS was shown to be equivalent to a negligible mutual information (MI) between the message and the eavesdropper's observations for all message distributions. We establish SS for our superposition code via a strong soft-covering lemma (SCL)

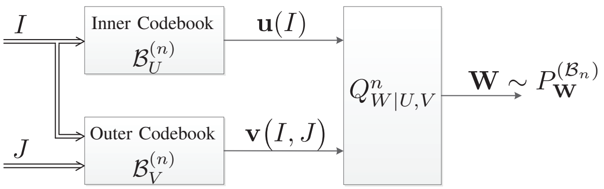

Fig. 1: Superposition SCL setup with the goal of making $P_{\mathbf{W}}^{(\mathcal{B}_n)} \approx Q_W^n$, where $\mathcal{B}_n = \left\{\mathcal{B}_U^{(n)}, \mathcal{B}_V^{(n)}\right\}$ is a fixed superposition codebook.

for superposition codebooks that produces double-exponential decay of the probability of soft-covering not happening. Since all the aforementioned secrecy results were derived under the weak-secrecy metric (i.e., a vanishing *normalized* MI with respect to a *uniformly distributed* message), our achievability outperforms the schemes from [2], [3] for the SD-WTC with non-causal encoder CSI not only in terms of the achievable secrecy rate, but also in the upgraded sense of security is provides. When CSI is also available at the decoder, our result implies that an upgrade to SS is possible, without inflicting any loss of rate compared to [4].

## II. Strong SCL for Superposition Codes

We use notation from [7, Section II]. Our derivation of SS for the SD-WTC with non-causal encoder CSI relies on a new strong SCL (in the spirit of [8], [9]) adjusted for superposition codebooks. The setup is shown in Fig. 1, where inner and outer layer codewords are uniformly chosen from the corresponding codebook and passed through a DMC. The induced output distribution should be a good approximation of a product distribution. The approximation is in terms of relative entropy, which is shown to converge to 0 exponentially quickly with high probability. The negligible probability is doubly-exponentially small with the blocklength $n$.

Let $Q_{U,V,W} \in \mathcal{P}(\mathcal{U}\times\mathcal{V}\times\mathcal{W})$, where $Q_U$ and $Q_{V|U}$ are two codebook distributions and $Q_{W|U,V}$ is a memoryless channel. Let $\mathcal{B}_U^{(n)}$ be a randomly generated collection of $\mathbf{u}(i)\in\mathcal{U}^n$ sequences, for all $i\in\mathcal{I}_n \triangleq \left[1:2^{nR_1}\right]$, each drawn independently from $Q_U^n$, and let $\mathcal{B}_V^{(n)}$ be a randomly generated collection of $\mathbf{v}(i,j)\in\mathcal{V}^n$ sequences, for all $(i,j)\in\mathcal{I}_n\times\mathcal{J}_n$, where $\mathcal{J}_n \triangleq \left[1 : 2^{nR_2}\right]$, such that for each $i\in\mathcal{I}_n$ every $\mathbf{v}(i,j)$ is drawn independently from $Q^n_{V|U=\mathbf{u}(i)}$. Setting, $\mathcal{B}_n \triangleq \left\{\mathcal{B}_U^{(n)}, \mathcal{B}_V^{(n)}\right\}$, let $P_{\mathbf{W}}^{(\mathcal{B}_n)}$ be the output distribution induced by applying the codebooks in the configuration of Fig. 1, where $I$ and $J$ are uniformly distributed over $\mathcal{I}_n$ and $\mathcal{J}_n$, respectively, and let be the desired i.i.d. output distribution be $Q_W^n$. Denoting a random superposition codebook by $\mathsf{B}_n$, the strong SCL reads as follows.

**Lemma 1 (Stronger Superposition Soft-Covering Lemma)** *For any $Q_{U,V,W} \in \mathcal{P}(\mathcal{U}\times\mathcal{V}\times\mathcal{W})$, where $|\mathcal{W}| < \infty$, and $(R_1,R_2) \in \mathbb{R}_+^2$ with $R_1 > I(U;W)$ and $R_1 + R_2 > I(U,V;W)$, there exist $\gamma_1,\gamma_2 > 0$, such that for $n$ large enough*

$$\mathbb{P}\left(D\left(P_{\mathbf{W}}^{(\mathsf{B}_n)}\middle|\middle|Q_W^n\right) > e^{-n\gamma_1}\right) \leq e^{-e^{n\gamma_2}}. \tag{1}$$

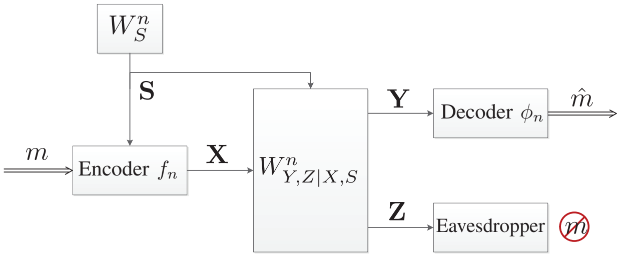

Fig. 2: The state-dependent wiretap channel with non-casual encoder channel state information.

Lemma 1 is a simplified version of the full statement from [7, Lemma 1]. The proof of Lemma 1 is omitted due to space limitations. The reader is referred to [7] for a statement that includes exact exponents of decay and its proof.

## III. The Gelfand-Pinsker Wiretap Channel

We study the SD-WTC with non-causal encoder CSI, for which we establish a new and improved achievability formula that (in some cases) strictly outperforms the previously best known coding schemes for this scenario.

### A. Problem Setup

Let $\mathcal{S}$, $\mathcal{X}$, $\mathcal{Y}$ and $\mathcal{Z}$ be finite sets. The $\left(\mathcal{S},\mathcal{X},\mathcal{Y},\mathcal{Z},W_S,W_{Y,Z|X,S}\right)$ discrete and memoryless SD-WTC with non-causal encoder CSI is illustrated in Fig. 2. A state sequence $\mathbf{s}\in\mathcal{S}^n$ is generated in an i.i.d. manner according to $W_S$ and is revealed in a non-causal fashion to the sender, who chooses a message $m$ from the set $\left[1:2^{nR}\right]$. The sender then maps the observed state sequence $\mathbf{s}$ and the chosen message $m$ into a sequence $\mathbf{x}\in\mathcal{X}^n$ (the mapping may be random). The sequence $\mathbf{x}$ is transmitted over the SD-WTC with transition probability $W_{Y,Z|X,W}$. The output sequences $\mathbf{y}\in\mathcal{Y}^n$ and $\mathbf{z}\in\mathcal{Z}^n$ are observed by the receiver and the eavesdropper, respectively. Based on $\mathbf{y}$, the receiver produces an estimate $\hat{m}$ of $m$. The eavesdropper tries to glean whatever it can about the message from $\mathbf{z}$.

**Definition 1 (Code)** *An $(n,R)$-code $c_n$ for the SD-WTC with non-causal encoder CSI has a message set $\mathcal{M}_n \triangleq \left[1:2^{nR}\right]$, a stochastic encoder $f_n : \mathcal{M}_n\times\mathcal{S}^n \to \mathcal{P}(\mathcal{X}^n)$ and a decoder $\phi_n : \mathcal{Y}^n \to \hat{\mathcal{M}}_n$, where $\hat{\mathcal{M}}_n = \mathcal{M}_n\cup\{e\}$ and $e\notin\mathcal{M}_n$.*

For any message distribution $P_M \in \mathcal{P}(\mathcal{M}_n)$ and any $(n,R)$-code $c_n$, the induced joint PMF is:

$$\begin{aligned}P^{(c_n)}(\mathbf{s},m,\mathbf{x},\mathbf{y},\mathbf{z},\hat{m}) &= W_S^n(\mathbf{s})P_M(m)f_n(\mathbf{x}|m,\mathbf{s})\\ &\quad\times W^n_{Y,Z|X,S}(\mathbf{y},\mathbf{z}|\mathbf{x},\mathbf{s})\mathbb{1}_{\left\{\hat{m}=\phi_n(\mathbf{y})\right\}}.\end{aligned} \tag{2}$$

The performance of $c_n$ is evaluated in terms of its rate $R$, the maximal decoding error probability and the SS-metric.

**Definition 2 (Maximal Error Probability)** *The maximal error probability of an $(n,R)$-code $c_n$ is*

$$e(c_n) = \max_{m\in\mathcal{M}_n} e_m(c_n), \tag{3}$$

*where* $e_m(c_n) = \sum\limits_{(\mathbf{s},\mathbf{x})\in\mathcal{S}^n\times\mathcal{X}^n} W_S^n(\mathbf{s})f_n(\mathbf{x}|m,\mathbf{s}) \sum\limits_{\substack{\mathbf{y}\in\mathcal{Y}^n:\\ \phi_n(\mathbf{y})\neq m}} W^n_{Y|X,S}(\mathbf{y}|\mathbf{x},\mathbf{s}).$

**Definition 3 (Information Leakage and SS Metric)** *The information leakage to the eavesdropper under the $(n, R)$-code $c_n$ and the message PMF $P_M \in \mathcal{P}(\mathcal{M}_n)$ is $\ell(P_M, c_n) = I_{c_n}(M; \mathbf{Z})$, where $I_{c_n}$ denotes that the MI is taken with respect to the marginal $P^{(c_n)}_{M,\mathbf{Z}}$ of* (2)*. The SS metric with respect to $c_n$ is*

$$\ell_{\mathsf{Sem}}(c_n) = \max_{P_M \in \mathcal{P}(\mathcal{M}_n)} \ell(P_M, c_n). \tag{4}$$

With respect to the above definitions, *achievability* and the *SS-capacity* are defined in the standard manner (see [7].

### B. Main Results

The main result of this work is a novel lower bound on the SS-capacity of the SD-WTC with non-causal encoder CSI. Our achievability formula strictly outperforms the best previously known coding scheme for the considered scenario. To state our main result, let $\mathcal{U}$ and $\mathcal{V}$ be finite alphabets and for any $Q_{U,V,X|S} : \mathcal{S} \to \mathcal{P}(\mathcal{U} \times \mathcal{V} \times \mathcal{X})$ define

$$R_{\mathsf{A}}\left(Q_{U,V,X|S}\right) \triangleq \min \left\{ \begin{array}{c} I(V;Y|U) - I(V;Z|U), \\ I(U,V;Y) - I(U,V;S) \end{array} \right\}, \tag{5}$$

where the MI terms are calculated with respect to the joint distribution $W_S Q_{U,V,X|S} W_{Y,Z|X,S}$.

**Theorem 2 (SD-WTC SS-Capacity Lower Bound)** *The SS-capacity of the SD-WTC with non-causal encoder CSI is lower bounded as*

$$C_{\mathsf{Sem}} \geq R_{\mathsf{A}} \triangleq \max_{\substack{Q_{U,V,X|S}: \\ I(U;Y) - I(U;S) \geq 0}} R_{\mathsf{A}}\left(Q_{U,V,X|S}\right), \tag{6}$$

*and one may restrict the cardinalities of $U$ and $V$ to $|\mathcal{U}| \leq |\mathcal{S}||\mathcal{X}| + 5$ and $|\mathcal{V}| \leq |\mathcal{S}|^2|\mathcal{X}|^2 + 5|\mathcal{S}||\mathcal{X}| + 3$.*

An extended outline of the proof of Theorem 2 is given in Section V (see [7, Section VI-B] for the full proof), and is based on a secured superposition coding scheme. We encode the entire secret message in the *outer layer* of the superposition codebook, meaning no information is carried by the inner layer. The rate of the inner layer is chosen such that it is decodable by the eavesdropper. This results in the eavesdropper 'wasting' his channel resources on decoding the inner layer (which serves as a decoy), leaving it with insufficient resources to unveil the secret message. The legitimate decoder, on the other hand, decodes both layers of the codebook. The transmission is correlated with the observed state sequence by means of the likelihood encoder [5] and SS is established using the strong SCL (both the superposition version from Lemma 1 and the heterogeneous version from [9, Lemma 1]).

**Remark 1 (Interpretation of $R_{\mathsf{A}}$)** *To get some intuition on the structure of $R_{\mathsf{A}}$ notice that $I(V;Y|U) - I(V;Z|U)$ is the total rate of secrecy resources that are produced by the outer layer of the codebook. That is, the outer layer can achieve a secure communication rate of $I(V;Y|U) - \max\big\{I(V;Z|U), I(V;S|U)\big\}$, and it can produce secret key at a rate of $\big[I(V;S|U) - I(V;Z|U)\big]^+$, where $[x]^+ = \max(0,x)$, because some of the dummy bits needed to correlate the transmission with the state are secure for the same reason that a transmission is secure.*

*Also, the total amount of reliable (secured and unsecured) communication that this codebook allows is $I(U,V;Y) - I(U,V;S)$, including both the inner and outer layer. Therefore, one interpretation of our encoding scheme is that secret key produced in the outer layer (if any) is applied to the non-secure communication in the inner layer. In total, this achieves a secure communication rate that is the minimum of the total secrecy resources $I(V;Y|U) - I(V;Z|U)$ (i.e. secure communication and secret key) and the total communication rate $I(U,V;Y) - I(U,V;S)$, corresponding to the statement of $R_{\mathsf{A}}$. Of course, this effect happens naturally by the design of the superposition code, without the need to explicitly extract a key and apply a one-time pad.*

**Remark 2 (Relation to the Causal Scheme from [4])** *If the state sequence $\mathbf{S}$ is also known at the legitimate receiver (recovered from the considered setting by replacing $Y$ with $(Y,S)$), our result is at least as good as the best known lower bound by Chia and El-Gamal from [4, Theorem 1]. The latter work studied the case where the encoder learns the channel's state in a causal manner. Due to lack of space, we refer the reader to [7, Section V-A] for a proof that $R_{\mathsf{A}}$ indeed recovers Theorem 1 of [4].*

## IV. Outperforming the Chen-Han Vinck Scheme

The result of Theorem 2 recovers the previously best known achievable formula for the SD-WTC with non-causal encoder CSI from [2, Theorem 2]. Moreover, our achievability is strictly better than [2, Theorem 2] for some SD-WTCs. In [2, Theorem 2] it is stated that the weak-secrecy capacity of the considered SD-WTC is lower bounded by

$$R_{\mathsf{CHV}} \triangleq \max_{P_{U,X|S}} R_{\mathsf{CHV}}\left(P_{U,X|S}\right), \tag{7a}$$

where for any $Q_{U,X|S} : \mathcal{S} \to \mathcal{P}(\mathcal{U} \times \mathcal{X})$,

$$R_{\mathsf{CHV}}\left(Q_{U,X|S}\right) \triangleq I(U;Y) - \max\Big\{I(U;Z), I(U;S)\Big\}, \tag{7b}$$

and the MI terms are with respect to $W_S Q_{U,X|S} W_{Y,Z|X,S}$, i.e., $U - (X,S) - (Y,Z)$ is a Markov chain.

First note that Theorem 2 recovers $R_{\mathsf{CHV}}$ by setting $U = 0$ in $R_{\mathsf{A}}$ (while relabeling $V$ as $U$), thus $R_{\mathsf{A}} \geq R_{\mathsf{CHV}}$. On top of this observation, the following example shows that there exist SD-WTCs for which the previous inequality is strict.

**Example:** Let $\mathcal{S} = \mathcal{X} = \mathcal{Y} = \mathcal{Z} = \{0,1\}$ and $\mathcal{S}_1 = \{0,1,?\}$, where $? \notin \{0,1\}$. Consider a SD-WTC that factors as $W_{S_1|S} W_{Y,Z|X}$ and is defined by two parameters $\alpha \in \left(0, \frac{1}{2}\right)$ and $\sigma \in (0,1)$ as follows:

- $S \sim \text{Ber}(p_\alpha)$, where $p_\alpha = h^{-1}\Big(1 - h(\alpha)\Big) \in \left(0, \frac{1}{2}\right)$, $h$ is the binary entropy function and $h^{-1}$ is the inverse of the restriction of $h$ to $\left[0, \frac{1}{2}\right]$.
- $Z = X$, i.e., the eavesdropper noiselessly observes the transmitted symbol $X$.

- $W_{Y|X}$ is a BSC with crossover probability $\alpha \in \big(0, \frac{1}{2}\big)$ (abbreviated as a BSC($\alpha$)).
- $W_{S_1|S}$ is a binary erasure channel with erasure probability $\sigma \in (0,1)$ (abbreviated as a BEC($\sigma$)).

It can be readily verified that setting $V = S$ and $U = X \sim \text{Ber}\big(\frac{1}{2}\big)$ independent of $S$ into $R_{\mathsf{A}}$ from Theorem 2 with $(Y, S_1)$ instead of $Y$, gives $R_{\mathsf{A}} \geq \bar{\sigma}\big[1 - h(\alpha)\big]$, where $\bar{\sigma} \triangleq 1 - \sigma$. [1] To show that the above rate cannot be achieved by $R_{\mathsf{CHV}}$ from (7a), first note that for the considered SD-WTC

$$R_{\mathsf{CHV}}\left(Q_{U,X|S}\right) = I(U;Y,S_1) - \max\Big\{I(U;X), I(U;S)\Big\}, \tag{8}$$

and the corresponding joint distribution is $W_S Q_{U,X|S} W_{S_1|S} W_{Y|X}$. Assume by contradiction that $R_{\mathsf{CHV}} \geq \bar{\sigma}\big[1 - h(\alpha)\big]$ and consider the two following cases:

**Case 1:** For any $Q_{U,X|S}$ with $I(U;Y) \leq I(U;S)$, we have

$$\begin{aligned}
&I(U;Y,S_1) - I(U;S)\\
&\overset{(a)}{=} I(U;Y|S_1) - I(U;S|S_1)\\
&\overset{(b)}{=} \bar{\sigma}\Big[I(U;Y|S) - I(U;S|S)\Big] + \sigma\Big[I(U;Y) - I(U;S)\Big]\\
&\overset{(c)}{\leq} \bar{\sigma} I(U;Y|S)\\
&\overset{(d)}{=} \bar{\sigma}\big[1 - h(\alpha)\big]
\end{aligned} \tag{9}$$

where (a) is because $U - S - S_1$ forms a Markov chain; (b) is since $S_1$ is the output of a BEC($\sigma$) with input $S$; (c) uses the assumption in Case 1 that $I(U;Y) \leq I(U;S)$; (d) is because $(U,S) - X - Y$ forms a Markov chain and since $I(X;Y)$ is upper bounded by the capacity of the BSC($\alpha$).

Thus, to satisfy $R_{\mathsf{CHV}} \geq \bar{\sigma}\big[1 - h(\alpha)\big]$, it must be true that $I(U;Y,S_1) - I(U;S) = \bar{\sigma}\big[1 - h(\alpha)\big]$, for all $Q_{U,X|S}$ with $I(U;Y) \leq I(U;S)$. Thus, an end-to-end equality holds in the chain of inequalities from (9). In particular, we see that

- (d) holds with equality if and only if (iff) $S$ and $Y$ are independent.
- (e) holds with equality iff $I(X;Y|U,S) = 0$, which is equivalent to $X - (U,S) - Y$ forming a Markov chain.
- (f) holds with equality iff $X \sim \text{Ber}\big(\frac{1}{2}\big)$.

The following simple lemma (which we state without proof; see [7, Appendix F]) specifies some properties that are implied by the above relations.

**Lemma 3** *The following implications hold:*

1) *$(S,Y)$ are independent $\implies$ $(S,X)$ are independent.*
2) *$X - (U,S) - Y$ and $(U,S) - X - Y$ form Markov chains $\implies$ $\exists\ g : \mathcal{U} \times \mathcal{S} \to \mathcal{X}$ such that $X = f(U,S)$.*

We now bound the second expression from $R_{\mathsf{CHV}}$ as

$$\begin{aligned}
I(U;Y,S_1) - I(U;X) &\overset{(a)}{=} \bar{\sigma}\big[1 - h(\alpha)\big] + I(U;S) - I(U;X)\\
&\overset{(b)}{\leq} \bar{\sigma}\big[1 - h(\alpha)\big] + H(S) - I(U;X|S)\\
&\overset{(c)}{=} \bar{\sigma}\big[1 - h(\alpha)\big] + H(S) - H(X)\\
&\overset{(d)}{=} \bar{\sigma}\big[1 - h(\alpha)\big] + 1 - h(\alpha) - 1\\
&< \bar{\sigma}\big[1 - h(\alpha)\big]
\end{aligned} \tag{10}$$

where (a) adds and subtracts $I(U;S)$ and uses the end-to-end equality in (9); (b) uses the independence of $S$ and $X$ and the non-negativity of entropy; (c) again relies on $X$ and $S$ being independent and on $X = f(U,S)$; (d) is because $H(S) = 1 - h(\alpha)$ and $X \sim \text{Ber}\big(\frac{1}{2}\big)$.

The strict inequality in (10) is in contradiction to $R_{\mathsf{CHV}}^{\mathsf{Enc-CSI}} \geq \bar{\sigma}\big[1 - h(\alpha)\big]$ as $h(\alpha) > 0$ for all $\alpha \in \big(0, \frac{1}{2}\big)$.

**Case 2:** For any $Q_{U,X|S}$ with $I(U;Y) > I(U;S)$, observe that

$$\begin{aligned}
I(U;Y,S_1) - I(U;X) &\overset{(a)}{=} I(U;S_1|Y) - I(U;X|Y)\\
&\leq I(U,Y;S_1)\\
&\overset{(b)}{\leq} I(S;S_1)\\
&\overset{(c)}{=} \bar{\sigma}\big[1 - h(\alpha)\big]
\end{aligned} \tag{11}$$

where (a) is because $U - X - Y$ forms a Markov chain; (b) uses the Markov chain $(U,Y) - S - S_1$; (c) is since $I(S;S_1) = \bar{\sigma}H(S)$ and $H(S) = 1 - h(\alpha)$.

As before, for $R_{\mathsf{CHV}} \geq \bar{\sigma}\big[1 - h(\alpha)\big]$ and (11) both to hold, it must be the case that $I(U;Y,S_1) - I(U;X) = \bar{\sigma}\big[1 - h(\alpha)\big]$, for any $Q_{U,X|S}$ with $I(U;Y) > I(U;S)$. An end-to-end equality in (9) is equivalent to the following:

- The inequality between (a) and (b) holds with equality iff $I(U;X|Y) = 0$ and $S_1$ and $Y$ are independent.
- (b) holds with equality iff $I(S;S_1|U,Y) = 0$.

Lemma 4 (proven in [7, Appendix F]) produces additional properties that are implied by the above relations.

**Lemma 4** *The following implications hold:*

1) *$X - U - Y$ and $U - X - Y$ form Markov chains $\implies$ $\exists\ g_1 : \mathcal{U} \to \mathcal{X}$ such that $X = g_1(U)$.*
2) *$(S_1, Y)$ are independent $\implies$ $(S, Y)$ are independent.*
3) *$S - (U,Y) - S_1$ and $(U,Y) - S - S_1$ form Markov chains $\implies$ $\exists\ g_2 : \mathcal{U} \times \mathcal{Y} \to \mathcal{S}$ such that $S = g_2(U,Y)$.*

Using Lemma 4, we upper bound $I(U;Y)$ as

$$\begin{aligned}
I(U;Y) &\overset{(a)}{=} H(U) - H(U,S|Y)\\
&= I(U;S,Y) - H(S|Y)\\
&\overset{(b)}{=} I(U;S) + I(U;Y|S) - H(S)\\
&\overset{(c)}{=} I(U;S) + I(U,S;Y) - H(S)\\
&\overset{(d)}{\leq} I(U;S) + I(X;Y) - H(S)\\
&\overset{(e)}{\leq} I(U;S)
\end{aligned} \tag{12}$$

where (a) is because $S = g_2(U,Y)$; (b) and (c) use the independence of $S$ and $Y$; (d) follows because $(U,S) - X - Y$ forms a Markov chain; (e) is since $I(X;Y) \leq 1 - h(\alpha)$ and $H(S) = 1 - h(\alpha)$.

[1] In fact, $\bar{\sigma}\big[1 - h(\alpha)\big]$ is the capacity of the considered example, which itself is a special case of a class of SD-WTC for which our achievability formula is tight [7, Section V-B-2].

The inequality in (12) is in contradiction to $Q_{U,X|S}$ in Case 2 being such that $I(U;Y) > I(U;S)$. The contradictions in both cases imply that $R_{\mathsf{CHV}}^{\mathsf{Enc-CSI}} < \bar{\sigma}\big[1 - h(\alpha)\big]$, i.e., that $R_{\mathsf{CHV}}^{\mathsf{Enc-CSI}}$ is sub-optimal for the considered example.

## V. Outline of Proof of Theorem 2

We give a detailed description of the codebook construction and of the encoding and decoding processes. Due to space limitation, the analysis of reliability and SS is omitted and only the required rate bounds accompanied by broad explenations are provided (see [7, Section VI-B] for the full details). Fix $\epsilon > 0$ and a conditional PMF $Q_{U,V,X|S}$ with $I(U;Y) \geq I(U;S)$.

**Codebook $\boldsymbol{\mathcal{B}_n}$:** We use a superposition codebook where the outer layer also encodes the confidential message. The codebook is constructed independently of $\mathbf{S}$, but with sufficient redundancy to correlate the transmission with $\mathbf{S}$.

Let $I$ and $J$ be two independent random variables uniformly distributed over $\mathcal{I}_n \triangleq \big[1 : 2^{nR_1}\big]$ and $\mathcal{J}_n \triangleq \big[1 : 2^{nR_2}\big]$, respectively. Let $\mathcal{B}_U^{(n)} \triangleq \big\{\mathbf{u}(i)\big\}_{i\in\mathcal{I}_n}$ be an inner layer codebook generated as i.i.d. samples of $Q_U^n$. For every $i \in \mathcal{I}_n$, let $\mathcal{B}_V^{(n)}(i) \triangleq \big\{\mathbf{v}(i,j,m)\big\}_{(j,m)\in\mathcal{J}_n\times\mathcal{M}_n}$ be a collection of $2^{n(R_2+R)}$ vectors of length $n$ drawn according to the distribution $Q^n_{V|U=\mathbf{u}(i)}$. We use $\mathcal{B}_n$ to denote our superposition codebook, i.e., the collection of the inner and all the outer layer codebooks. The encoder and decoder are described next for a fixed superposition codebook $\mathcal{B}_n$.

**Encoder $\boldsymbol{f_n^{(\mathcal{B}_n)}}$:** The encoding phase is based on the likelihood-encoder [5], which, in turn, allows us to approximate the (rather cumbersome) induced joint distribution by a much simpler distribution which we use for the analysis.

Given $m \in \mathcal{M}_n$ and $\mathbf{s} \in \mathcal{S}^n$, the encoder randomly chooses $(i,j) \in \mathcal{I}_n \times \mathcal{J}_n$ according to

$$P_{\mathsf{LE}}^{(\mathcal{B}_n)}(i,j|m,\mathbf{s}) = \frac{Q^n_{S|U,V}\big(\mathbf{s}\big|\mathbf{u}(i),\mathbf{v}(i,j,m)\big)}{\sum\limits_{(i',j')} Q^n_{S|U,V}\big(\mathbf{s}\big|\mathbf{u}(i'),\mathbf{v}(i',j',m)\big)}, \tag{13}$$

where $Q_{S|U,V}$ is the conditional marginal of $Q_{S,U,V}$ defined by $Q_{S,U,V}(s,u,v) = \sum_{x\in\mathcal{X}} W_S(s) Q_{U,V,X|S}(u,v,x|s)$, for every $(s,u,v) \in \mathcal{S} \times \mathcal{U} \times \mathcal{V}$. The channel input sequence is then generated by feeding the chosen $u$- and $v$-codewords along with the state sequence into the DMC $Q^n_{X|U,V,S}$.

**Decoder $\boldsymbol{\phi_n^{(\mathcal{B}_n)}}$:** Upon observing $\mathbf{y} \in \mathcal{Y}^n$, the decoder searches for a unique triple $(\hat{i},\hat{j},\hat{m}) \in \mathcal{I}_n \times \mathcal{J}_n \times \mathcal{M}_n$ such that $\Big(\mathbf{u}(\hat{i}), \mathbf{v}(\hat{i},\hat{j},\hat{m}), \mathbf{y}\Big) \in \mathcal{T}_\epsilon^n(Q_{U,V,Y})$. If such a unique triple is found, then set $\phi_n^{(\mathcal{B}_n)}(\mathbf{y}) = \hat{m}$; otherwise, $\phi_n^{(\mathcal{B}_n)}(\mathbf{y}) = e$.

The triple $(\mathcal{M}_n, f_n^{(\mathcal{B}_n)}, \phi_n^{(\mathcal{B}_n)})$ defined with respect to the codebook $\mathcal{B}_n$ constitutes an $(n,R)$-code $c_n$.

**Main Idea Behind Analysis:** The key step is to approximate (in total variation) the joint PMF induced by the above encoding and decoding scheme, say $P^{(\mathcal{B}_n)}$, by a new distribution $\Gamma^{(\mathcal{B}_n)}$, which lands itself easier for the reliability and security analyses. For any $P_M \in \mathcal{P}(\mathcal{M}_n)$, $\Gamma^{(\mathcal{B}_n)}$ is

$$\begin{aligned}\Gamma^{(\mathcal{B}_n)}(m,i,j,\mathbf{u},\mathbf{v},\mathbf{s},\mathbf{x},\mathbf{y},\mathbf{z},\hat{m}) = P_M(m)\frac{1}{|\mathcal{I}_n||\mathcal{J}_n|}\mathbb{1}_{\{\mathbf{u}=\mathbf{u}(i)\}}\\ \times \mathbb{1}_{\big\{\mathbf{v}=\mathbf{v}(i,j,m)\big\}} Q^n_{S|U,V}(\mathbf{s}|\mathbf{u},\mathbf{v}) Q^n_{X|U,V,S}(\mathbf{x}|\mathbf{u},\mathbf{v},\mathbf{s})\\ \times W^n_{Y,Z|X,S}(\mathbf{y},\mathbf{z}|\mathbf{x},\mathbf{s}) \mathbb{1}_{\big\{\phi_n^{(\mathcal{B}_n)}(\mathbf{y})=\hat{m}\big\}},\end{aligned} \tag{14}$$

Namely, with respect to $\Gamma^{(\mathcal{B}_n)}$, the indices $(i,j) \in \mathcal{I}_n \times \mathcal{J}_n$ are uniformly drawn from their respective ranges. Then, the sequence $\mathbf{s}$ is generated by feeding the corresponding $u$- and $v$-codewords into the DMC $Q^n_{S|U,V}$. Based on Lemma 1, it can be shown the with respect to a random superposition codebook $\mathsf{B}_n$, $P^{(\mathsf{B}_n)}$ and $\Gamma^{(\mathsf{B}_n)}$ are close in total variation in several senses (both in expectation and with high probability), if

$$R_1 > I(U;S) \tag{15a}$$

$$R_1 + R_2 > I(U,V;S). \tag{15b}$$

Having this, both the reliability and the security analysis are preformed with respect to $\Gamma^{(\mathcal{B}_n)}$ instead of $P^{(\mathcal{B}_n)}$. Standard joint-typicality decoding arguments for superposition codes show that reliability follows provided that

$$R + R_2 < I(V;Y|U), \tag{16a}$$

$$R + R_1 + R_2 < I(U,V;Y). \tag{16b}$$

With the help of the heterogeneous strong SCL from [9, Lemma 1], SS is ensured if

$$R_2 > I(V;W|U). \tag{17}$$

This rate bound essentially means that the rates of the codebooks are chosen so that the eavesdropper can decode the inner layer codeword. This makes him waste channel resources on decoding a codeword that carries no confidential information. The remaining resources are insufficient for extracting any information on the outer layer codeword, which, in turn, results in our code being semantically-secure. Finally, applying the Fourier-Motzkin Elimination on (15), (16) and (17) shows that $R_{\mathsf{A}}\left(Q_{U,V,X|S}\right)$ is achievable.

## References

[1] S. I. Gelfand and M. S. Pinsker. Coding for channel with random parameters. *Problemy Pered. Inform. (Problems of Inf. Trans.)*, 9(1):19–31, 1980.

[2] Y. Chen and A. J. Han Vinck. Wiretap channel with side information. *IEEE Trans. Inf. Theory*, 54(1):395–402, Jan. 2008.

[3] W. Liu and B. Chen. Wiretap channel with two-sided state information. In *Proc. 41st Asilomar Conf. Signals, Syst. Comp*, page 893897, Pacific Grove, CA, US, Nov. 2007.

[4] Y.-K. Chia and A. El Gamal. Wiretap channel with causal state information. *IEEE Trans. Inf. Theory*, 58(5):2838–2849, May 2012.

[5] E. Song, P. Cuff, and V. Poor. The likelihood encoder for lossy compression. *IEEE Trans. Inf. Theory*, 62(4):1836–1849, Apr. 2016.

[6] M. Bellare, S. Tessaro, and A. Vardy. A cryptographic treatment of the wiretap channe. In *Proc. Adv. Crypto. (CRYPTO 2012)*, Santa Barbara, CA, USA, Aug. 2012.

[7] Z. Goldfeld, P. Cuff, and H. H. Permuter. Wiretap channel with random states non-causally available at the encoder. *Submitted to IEEE Trans. Inf. Theory*, 2016.

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

[9] Z. Goldfeld, P. Cuff, and H. H. Permuter. Arbitrarily varying wiretap channels with type constrained states. *IEEE Trans. Inf. Theory*, 62(12):7216–7244, Dec. 2016.