Key-Message Security over State-Dependent Wiretap Channels

Alexander Bunin, Technion
Ziv Goldfeld, MIT
Haim H. Permuter, Ben-Gurion University
Shlomo Shamai, Technion
Paul Cuff, Princeton University
Pablo Piantanida, CentraleSupélec

***Abstract*—The state-dependent (SD) wiretap channel (WTC) with non-causal channel state information (CSI) available at the encoder is considered. An inner bound on the trade-off region between admissible secret key (SK) and secret message (SM) rates is provided. The result is derived under the stringent semantic-security metric. Our inner bound recovers the best-known achievability results for either SK generation, SM transmission, or simultaneous execution of both. Since some of these past benchmarks were derived under weaker security metrics, our results imply that an upgrade to semantic-security is possible without inflicting any rate loss. It is shown that for certain instances of the considered SD-WTC, the derived region is strictly larger than the previously best-known SK-SM trade-off region reported by Prabhakaran et al., and that a recently reported SK rate for this setup cannot be achieved.**

I. Introduction

Two fundamental questions in Physical layer security (PLS) concern the best achievable transmission rate of a secret message (SM) over a noisy channel, and the highest attainable SK rate that distributed parties can agree upon. The base model for SM transmission is Wyner's WTC [1]. The study of SK agreement was pioneered by Maurer [2], and, independently, by Ahlswede and Csiszár [3], who studied the achievable SK rates based on correlated observations at the terminals that can communicate via a noiseless public link.

A more general framework is the state-dependent (SD) WTC with non-causal encoder channel state information (CSI). This model combines the WTC and the Gelfand and Pinsker (GP) channel [4], and is, therefore, sometimes referred to as the GP-WTC. The dependence of the channel's transition probability on the state sequence accounts for the possible availability of correlated sources at the terminals. The similarity between the SM transmission and the SK agreement tasks makes their integration in a single model natural. Adhering to the most general framework, we study the SM-SK rate pairs that are simultaneously achievable over the GP-WTC.

The scenario with a SM only was first studied in [5], where an achievable formula was established. This result was improved upon in [6] based on a novel superposition coding scheme. SK agreement over the GP-WTC was the focus of [7], and, more recently, of [8] (see also references therein). The combined model was considered by Prabhakaran *et al.* [9], who derived the best inner bound on the SM-SK capacity region known until this work. The result from [9] is optimal for several classes of GP-WTCs.

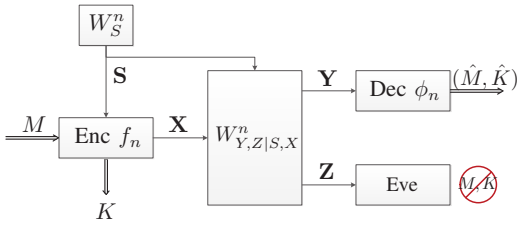

Fig. 1. Secret message transmission and secret key generation over the state-dependent WTC with non-casual encoder CSI

We extend the superposition coding scheme from [6] to generate a SK, which gives rise to a novel inner bound on the SM-SK capacity region of the GP-WTC. To the best of our knowledge, all existing inner bounds on SM transmission, SK agreement or both, for this setup, are captured by our result. Furthermore, we demonstrate our region can achieve strictly higher rates than [9], for certain instances of the GP-WTC. The key observation here is that the scheme from [9] does not allow GP coding in the inner code layer. Exploiting this fact, we propose an example for which GP coding in the inner layer is necessary to achieve capacity. For that example, the scheme from [9] is strictly sub-optimal, while our result attains optimality. In addition, we show that a recently reported achievability bound on the SK capacity for this setup [10], that seemingly achieves higher rates than the result herein, is missing a condition to be correct. The amended result (with the missing condition) is a special case of our inner bound.

Our coding scheme uses an over-populated superposition codebook that encodes the entire confidential message in its outer layer. Using the redundancies in the inner and outer layers, the transmission is correlated with the state via the likelihood encoder [11]. Although the redundancy indices are chosen as part of the encoding process, their distribution turns out to be approximately uniform. Consequently, as long as a certain redundancy index is kept secret, it may be declared as a SK. The security analysis is based on constructing the inner codebook such that it is better observable by the eavesdropper, making the inner layer index decodable by him/her. This enhances the secrecy resources that the legitimate parties can extract from the outer layer, which they use to secure the SM and part of the redundancy index of the outer layer, which is

The work of A. Bunin and S. Shamai was supported by the European Union's Horizon 2020 Research and Innovation Programme, grant agreement #694630. The work of Z. Goldfeld and H. Permuter was supported by the Israel Science Foundation (grant #684/11), an ERC starting grant and the Cyber Security Research Grant at Ben-Gurion University. Z. Goldfeld was also supported by the Rothschild postdoc fellowship and by a grant from Skoltech–MIT Joint Next Generation Program (NGP). The work of P. Cuff was supported by the National Science Foundation, grant CCF-1350595, and the Air Force Office of Scientific Research, grant FA9550-15-1-0180.

declared as the SK.

Our results are derived under the strict metric of semantic-security (SS), i.e., negligible mutual information (MI) between the confidential data (in our case, the SM-SK pair) and the eavesdropper's observations, when maximized over all possible message distributions. Since many of the past secrecy results were derived under the weak secrecy metric (i.e., a vanishing *normalized* MI with respect to a *uniformly distributed* message-key pair), our achievability outperforms those schemes, not only in terms of the achievable rate pairs, but also in the upgraded sense of security.

II. Setup and Definitions

We use notations from [12, Section 2]. Let $\mathcal{S},\ \mathcal{X},\ \mathcal{Y}$ and $\mathcal{Z}$ be finite sets. The $\left(\mathcal{S},\mathcal{X},\mathcal{Y},\mathcal{Z},W_S,W_{Y,Z|S,X}\right)$ GP-WTC is shown in Fig. 1. A state sequence $\mathbf{s}\in\mathcal{S}^n$ is sampled from the product distribution W_S^n and non-causally revealed to the encoder. The sender chooses a message m from the set $\left[1:2^{nR_M}\right]$ and maps $(\mathbf{s},m)$ onto a channel input sequence $\mathbf{x}\in\mathcal{X}^n$ and a key index $k\in\left[1:2^{nR_K}\right]$ (the mapping may be random). The sequence $\mathbf{x}$ is transmitted over the SD-WTC $W_{Y,Z|S,X}$. The channel's outputs $\mathbf{y}\in\mathcal{Y}^n$ and $\mathbf{z}\in\mathcal{Z}^n$ are observed by the receiver and the eavesdropper, respectively. Based on $\mathbf{y}$, the receiver produces its estimates of (m,k). The eavesdropper tries to glean whatever it can about the message-key pair from $\mathbf{z}$.

Remark 1 *The considered model is the most general instance of a SD-WTC with non-causal CSI known at some or all of the terminals. Receiver and/or eavesdropper CSI may be incorporated in their channel outputs. Our model also supports the existence of a public (or private) bit-pipe from the transmitter to the receiver and the eavesdropper (or to the receiver only). The bit-pipe may replace or coexist with the noisy channel.*

Definition 1 (Code) *An (n,R_M,R_K)-code c_n for the GP-WTC with a message set $\mathcal{M}_n\triangleq\left[1:2^{nR_M}\right]$ and a key set $\mathcal{K}_n\triangleq\left[1:2^{nR_K}\right]$ is a pair of maps:*

1) *$f_n:\mathcal{M}_n\times\mathcal{S}^n\to\mathcal{P}(\mathcal{K}_n\times\mathcal{X}^n)$ is a stochastic encoder.*
2) *$\phi_n:\mathcal{Y}^n\to\mathcal{M}_n\times\mathcal{K}_n$ is the decoding function.*

For any message distribution p_M and an (n,R_M,R_K)-code c_n, the induced joint distribution is

$$p^{(c_n)}(\mathbf{s},m,k,\mathbf{x},\mathbf{y},\mathbf{z},\hat{m},\hat{k})=W_S^n(\mathbf{s})P_M(m)\times f_n(k,\mathbf{x}|m,\mathbf{s})W_{Y,Z|S,X}^n(\mathbf{y},\mathbf{z}|\mathbf{s},\mathbf{x})\mathbb{1}_{\left\{(\hat{m},\hat{k})=\phi_n(\mathbf{y})\right\}}.$$

The probability measure induced by $p^{(c_n)}$ is $\mathbb{P}$. MI terms taken with respect to $p^{(c_n)}$ are denoted by I_p.

Definition 2 (Achievability) *A pair $(R_M,R_K)\in\mathbb{R}_+^2$ is an achievable SS message-key rate pair for the GP-WTC, if for every $\epsilon>0$ and sufficiently large n there exists an (n,R_M,R_K)-code c_n with*

$$\max\Big\{\max_{m\in\mathcal{M}_n}\left[e_m(c_n),\delta_m(c_n)\right],\max_{p_M\in\mathcal{P}(\mathcal{M}_n)}\ell(p_M,c_n)\Big\}\le\epsilon,$$

where

$$e_m(c_n)\triangleq\mathbb{P}\Big(\left(\hat{M},\hat{K}\right)\neq(m,K)\Big|M=m\Big)$$
$$\delta_m(c_n)\triangleq\left|\left|p_{K|M=m}^{(c_n)}-p_{\mathcal{K}_n}^{(U)}\right|\right|_{\mathsf{TV}}$$
$$\ell(p_M,c_n)\triangleq I_p(M,K;\mathbf{Z})$$

are respectively, the error probability when m is transmitted, the key uniformity and independence metric for message m, and the information leakage given message distribution p_M. Here $||p-q||_{\mathsf{TV}}$ is the TV between p and q, while $p_{\mathcal{A}}^{(U)}$ is the uniform distribution over a set $\mathcal{A}$.

Remark 2 *The maximization in Definition 2 is over the message distribution only (rather than the distribution of the SM-SK pair) because, while the choice of $M\sim p_M$ is independent of the code, the distribution of K is induced by the code.*

Definition 3 (SS-Capacity) *The SS message-key capacity region $\mathcal{C}_{\mathsf{Sem}}$ of the GP-WTC is the convex closure of the set of achievable SS rate pairs.*

III. Main Result

We give a novel inner bound on the SS message-key capacity region of the GP-WTC. To the best of our knowledge, our achievable region recovers all the best-known achievability results for the considered problem (or any of its special cases).

To state the result, let $\mathcal{U}$ and $\mathcal{V}$ be finite sets with cardinalities $|\mathcal{U}|\le\left[|\mathcal{X}||\mathcal{S}|+5\right]$ and $|\mathcal{V}|\le\left[|\mathcal{X}|^2|\mathcal{S}|^2+5|\mathcal{X}||\mathcal{S}|+3\right]$. For any $q_{U,V,X|S}$ define $\mathcal{R}_{\mathsf{A}}\left(q_{U,V,X|S}\right)$ as the set of all $(R_M,R_K)\in\mathbb{R}_+^2$ satisfying

$$R_M\le I(U,V;Y)-I(U,V;S),\tag{1a}$$
$$R_M+R_K\le I(V;Y|U)-I(V;Z|U)-|I(U;S)-I(U;Y)|_+\tag{1b}$$

where $|x|_+\triangleq\max\{x,0\}$ and the MI terms are taken with respect to $W_S q_{U,V,X|S}W_{Y,Z|S,X}$, i.e., such that $(U,V)-(S,X)-(Y,Z)$ forms a Markov chain.

Theorem 1 (Inner Bound) *The following inclusion holds:*

$$\mathcal{C}_{\mathsf{Sem}}\supseteq\mathcal{R}_{\mathsf{A}}\triangleq\bigcup_{q_{U,V,X|S}}\mathcal{R}_{\mathsf{A}}\left(q_{U,V,X|S}\right).\tag{2}$$

Due to space limitation, the proof of Theorem 1 is omitted (see [13]). A high-level description of the code construction is as follows. We use secured superposition coding scheme. An over-populated two-layered superposition codebook is constructed (independently of the state sequence), in which the entire secret message is encoded in the *outer layer*. The likelihood encoder [11] uses the redundancies in the inner and outer codebooks to correlate the transmission with the state. Upon doing so, part of the correlation index from the outer layer is declared by the encoder as the key. The inner layer is designed to utilize the part of the channel which is better observable by the eavesdropper. This saturates the eavesdropper with redundant information, leaving him/her with insufficient

resources to extract any information on the SM-SK pair from the outer layer. The legitimate decoder, on the other hand, decodes both layers and declares the appropriate indices as the decoded message-key pair.

Remark 3 (Interpretation of Theorem 1) *We interpret the terms in* (1) *as follows. The right-hand side (RHS) of* (1a) *is the total rate of reliable (secured and unsecured) communication that our superposition codebook supports, which restricts R_M. For* (1b)*, the term $I(V;Y|U)-I(V;Z|U)$ is the total rate of secrecy resources that are produced by the outer layer of the codebook. Since the security of the SM-SK pair comes entirely from the outer layer, this MI difference is an upper bound on the sum of rates. To interpret the penalty term $|I(U;S)-I(U;Y)|_+$, we note that $I(U;S)$ is approximately the rate of the inner codebook. Thus, $I(U;Y) < I(U;S)$ means that looking solely at the inner layer, the decoder lacks the resolution to decode it. However, the success of our communication protocol relies on the decoder reliably decoding both layers. Therefore, in this case, some of the rate from the outer layer is allocated to convey the inner layer index. As our security analysis is based on revealing the inner layer to the eavesdropper, this rate allocation effectively results in a loss of $|I(U;S)-I(U;Y)|_+$ in the secrecy rate.*

IV. Tight Secrecy Capacity Results

An interesting special case of the considered GP-WTC is as follows. Assume that $W_{Y,Z|S,X}$ is such that the eavesdropper's channel is less noisy than the main channel, but that the legitimate parties share noiseless observations of a source $\mathbf{L} \sim W_L^n$, independent of the channel and its state sequence $\mathbf{S} \sim W_S^n$. Using $\mathbf{L}$ the legitimate parties may extract a SK and secure the confidential data.

Formally, let $\mathcal{L}$, $\mathcal{S}$, $\mathcal{X}$, $\mathcal{Y}$ and $\mathcal{Z}$ be the corresponding alphabets. The considered instance is the $\left(\tilde{\mathcal{S}}, \mathcal{X}, \tilde{\mathcal{Y}}, \mathcal{Z}, W_{\tilde{S}}, W_{\tilde{Y},Z|\tilde{S},X}\right)$ GP-WTC with $\tilde{\mathcal{S}} = \mathcal{L}\times\mathcal{S}$, $\tilde{\mathcal{Y}} = \mathcal{L}\times\mathcal{Y}$, $W_{\tilde{S}} = W_L \times W_S$, $\tilde{S} = (L,S)$, $\tilde{Y} = (L',Y)$, and

$$W_{\tilde{Y},Z|\tilde{S},X} = W_{(L',Y),Z|(L,S),X} = \mathbb{1}_{\{L'=L\}} W_{Y,Z|S,X},$$

where $W_{Y,Z|S,X}$ satisfies the less-noisy eavesdropper property: $I(U;Y) \le I(U;Z)$, for any U for which $U-(S,X)-(Y,Z)$ forms a Markov chain. We refer to this instance as the *SD less-noisy-eavesdropper WTC with a key*.

Corollary 1 (SM-SK Capacity Region) *The SS message-key capacity region of the SD less-noisy-eavesdropper WTC with a key is the set of all $(R_M, R_K) \in \mathbb{R}_+^2$ satisfying*

$$R_M \le \max_{q_{U,X|S}} \left[I(U;Y) - I(U;S)\right], \tag{3a}$$

$$R_K + R_M \le H(L), \tag{3b}$$

where the joint distribution in (3a) *is $W_S q_{U,X|S} W_{Y|S,X}$.*

The achievability of (3) follows by setting $V = (L,U)$ into Theorem 1, with (U,X) that are independent of L. The converse relies on two observations. First, the SM rate of the channel cannot exceed the total reliable rate for this channel. Second, since the channel is less noisy in favor of the eavesdropper, all the secrecy comes from the external source L. For the full proof see [13, Appendix A].

A direct consequence of Corollary 1 is that when no SK is to be established (i.e., $R_K = 0$) the best attainable SM rate is

$$\mathcal{C}_{\mathsf{SM}} = \min\left\{\max_{q_{U,X|S}} \left[I(U;Y) - I(U;S)\right], H(L)\right\}. \tag{4}$$

Instead of employing Theorem 1, (4) can be achieved via a simple separation-based coding scheme. Roughly speaking, a capacity achieving error correction code transforms the channel into a noiseless bit-pipe. The legitimate parties then compresses $\mathbf{L}$ to produce a shared uniformly distributed key of entropy $H(L)$. The key is used to encrypt the SM via a one-time pad and the encrypted message is transmitted. The achievable SM rate equals the minimum between the channel's capacity and the key's rate. While this scheme is very natural, to the best of our knowledge, none of the past achievability results for the GP-WTC prior to [6] attain its performance.

In Section V-B, a special case of this setup is used to demonstrate the improvement of our result over the previous benchmark achievable SM-SK region for the GP-WTC [9].

V. Comparison to SM-SK Trade-off Benchmark

We show $\mathcal{R}_{\mathsf{A}}$ contains the previously best-known achievable SK-SM trade-off region from [9]. Then, it is demonstrated that, for certain GP-WTCs, Theorem 1 strictly outperforms [9].

A. SM-SK Trade-off Region

In [9, Theorem 1] the following region was established:

$$\mathcal{R}_{\mathsf{PER}} \triangleq \bigcup_{q_U q_{V,X|U,S}} \mathcal{R}_{\mathsf{PER}}\left(q_U q_{V,X|U,S}\right), \tag{5}$$

where, for any q_U and $q_{V,X|U,S}$, $\mathcal{R}_{\mathsf{PER}}\left(q_U q_{V,X|U,S}\right)$ is the set of all $(R_M, R_K) \in \mathbb{R}_+^2$ satisfying,

$$R_M \le I(U,V;Y) - I(U,V;S) \tag{6a}$$

$$R_M + R_K \le I(V;Y|U) - I(V;Z|U), \tag{6b}$$

with the MI terms taken with respect to $W_S q_U q_{V,X|U,S} W_{Y,Z|S,X}$, i.e., U and S are independent and $(U,V)-(S,X)-(Y,Z)$ forms a Markov chain. Theorem 1 recovers $\mathcal{R}_{\mathsf{PER}}$ by restricting U and S to be independent.

B. Achieving Strictly Higher Rates

Since [9, Theorem 1] restricts the inner layer coding random variables U to be independent of S, *Gelfand-Pinsker* coding [4] (which generally requires correlating U with S), is not supported in the inner layer. Instead, only *Shannon's Strategies* coding [14], that operates with independent U and S, is allowed. The latter is optimal if the encoder observes the state *causally*, but is generally sub-optimal when non-causal encoder CSI is available.

To show that Theorem 1 can improve upon [9], we exploit the aforementioned limitation of the scheme therein, along with the observation that it is beneficial to exploit any part

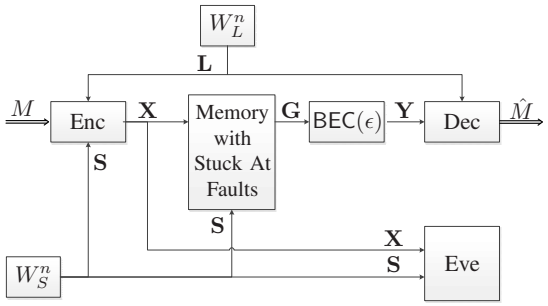

Fig. 2. Section V-B example setup.

of a considered SD-WTC that is better observable by the eavesdropper to transmit the inner layer of the code.

Let $\mathcal{X} = \mathcal{G} = \mathcal{L} = \mathcal{E} = \{0,1\}$, $\mathcal{S} = \{0,1,2\}$, $\mathcal{Y} = \{0,1,?\}$, where $? \notin \{0,1\}$ and $\mathcal{Z} = \mathcal{X} \times \mathcal{S}$. Consider the SD less-noisy-eavesdropper WTC with a key (defined in Section IV) shown in Fig. 2, whose transition probability $W_{Y,Z|S,X}$, key $L \sim W_L$ and state $S \sim W_S$ are defined by the three parameters $\lambda, \epsilon, \sigma \in (0, 0.5)$ as follows:

- Let $(L, S, E) \sim W_L W_S W_E$ be independent random variables with $W_L = \mathsf{Ber}(\lambda)$, $W_E = \mathsf{Ber}(\epsilon)$, $W_S(0) = W_S(1) = \frac{\sigma}{2}$ and $W_S(2) = 1 - \sigma$.
- Let X and G be, respectively, the input and the output of the *Memory with Stuck-at-Faults* (MSAF) [15] channel, driven by a ternary state S. The relation between G and (X, S) is described through the deterministic function

$$g(s,x) = \begin{cases} s, & s \in \{0,1\} \\ x, & s = 2 \end{cases} .$$

- The output G of the MSAF channel is fed into a *Binary Erasure Channel* with erasure probability ϵ (abbreviated as a $\mathsf{BEC}(\epsilon)$). Thus, G and Y are related by means of the erasure random variable E through the function:

$$y(e,g) = \begin{cases} g, & e = 0 \\ ?, & e = 1 \end{cases} .$$

- Set $Z = (S, X)$ as the eavesdropper's observation.

With respect to the above definitions, we have

$$W_{Y,Z|S,X}(y', z|x, s) = \sum_{g' \in \{0,1\}} \sum_{e \in \{0,1\}} W_E(e) W_{G,Y,Z|S,X,E}(g', y', z|s, x, e),$$

where $W_{G,Y,Z|S,X,E} = \mathbb{1}_{\{G=g(S,X)\} \cap \{Y=y(E,G)\} \cap \{Z=(S,X)\}}$.

For any $\lambda, \epsilon, \sigma \in (0, 0.5)$, let $C(\lambda, \epsilon, \sigma)$ denote the secrecy-capacity of the channel. Let $R_{\mathsf{A}}(\lambda, \epsilon, \sigma)$ and $R_{\mathsf{PER}}(\lambda, \epsilon, \sigma)$ denote the maximal achievable secrecy rates attained by (2) from Theorem 1 and (5) from [9, Theorem 1], respectively. Corollary 1 (more specifically, (4)) implies that

$$C(\lambda, \epsilon, \sigma) = R_{\mathsf{A}}(\lambda, \epsilon, \sigma), \quad \forall \lambda, \epsilon, \sigma \in (0, 0.5).$$

As stated next, $R_{\mathsf{PER}}(\lambda, \epsilon, \sigma)$ is strictly below capacity.

Proposition 1 *There exist* $\lambda, \epsilon, \sigma \in (0, 0.5)$ *such that* $R_{\mathsf{A}}(\lambda, \epsilon, \sigma) > R_{\mathsf{PER}}(\lambda, \epsilon, \sigma)$.

We next outline the proof of Proposition 1 (see [13, Appendix C] for details).

Proof Outline: For the considered example, Theorem 1 attains (4). Fix $\sigma \in (0, 0.5)$ and set $\epsilon = \frac{1}{2}\left[h\left(\frac{\sigma}{2}\right) - \sigma\right]$ and $\lambda = h^{-1}(1-\sigma-\epsilon)$, where $h : [0,1] \to [0,1]$ and $h^{-1} : [0,1] \to [0, 0.5]$ are the binary entropy function and the inverse of its restriction to $[0, 0.5]$, respectively. It is readily verified that, with the these parameters, $H(L)$ attains the minimum in (4). Assuming, by contradiction, that $R_{\mathsf{PER}}(\lambda, \epsilon, \sigma)$ is no worse than (4), in particular, we must have

$$I(V; Y, L|U) - I(V; X, S|U) \geq H(L). \tag{7}$$

On the other hand, it can be shown that the opposite inequality in (7) is also true, thus implying an equality. The reader may verify that an equality in (7), implies the Markov relation $V - U - (S, X)$ and that L is a deterministic function of (U, V). Combining $V - U - (S, X)$ with the independence of U and S in [9, Theorem 1], we have that (U, V) and S are independent too. Interestingly, this means that the inability of the scheme from [9, Theorem 1] to support GP coding in the inner layer implies, for the considered example, that GP coding is not supported at all.

We next focus on the remaining rate bound (6a). Using the above derived properties, it can be shown that

$$I(U,V;Y,L) - I(U,V;S,L) \leq I(U,V;G) \leq \max_{q_T q_{X|S,T}} I(T;G).$$

Note that the RHS above is the capacity of the MSAF channel with *causal* CSI, which equals $1 - h\left(\frac{\sigma}{2}\right)$ [16]. Thus, $R_{\mathsf{PER}}(\lambda, \epsilon, \sigma) \leq 1 - h\left(\frac{\sigma}{2}\right)$. Recalling that $R_{\mathsf{A}}(\lambda, \epsilon, \sigma) = H(L)$ and noticing that $H(L) > 1 - h\left(\frac{\sigma}{2}\right)$ concludes the proof. ■

Remark 4 *This example actually demonstrates that [6, Theorem 1] (which is a special case of Theorem 1, when $R_K = 0$) achieves strictly higher SM rates than [9, Theorem 1].*

VI. A Missing Condition in a Recently Reported SK Achievability Result

In [10], a lower bound on the SK capacity of the GP-WTC was reported. In our notation, [10, Theorem 1] states the following lower bound on the GP-WTC's SK capacity C_{SK} [1]

$$C_{\mathsf{SK}} \geq R_{\mathsf{Zib}} \triangleq \max \Big[I(V;Y|U) - I(V;Z|U) \Big], \tag{8}$$

where the maximization is over all $q_{U|V}$ and $q_{V,X|S}$ satisfying $I(V;Y) \geq I(V;S)$. The underlying joint distribution is $W_S q_{U|V} q_{V,X|S} W_{Y,Z|S,X}$, where $U - V - (S, X) - (Y, Z)$ forms a Markov chain.

R_{Zib} suggests that no secrecy rate-loss is inflicted when the inner layer is not decodable on its own by the legitimate receiver, i.e., when $I(U;S) > I(U;Y)$. Consequently, R_{Zib} seemingly attains higher SK rates than Theorem 1. However, following the steps of the proof of [10, Theorem 1], it appears

[1] [10, Theorem 1] considers a setting with state observations at the receiver and the eavesdropper, and a public communication link. As Remark 1 explains, this is simply a special case of the GP-WTC. It can be verified that [10, Theorem 1] (in its original form) is recoverable from its restatement here.

that another condition was assumed without being explicitly stated. Namely, the missing condition is $I(U;Y) \geq I(U;S)$, which would assure decodability of the inner code layer by the legitimate receiver without relying on the outer layer. Taking this additional constraint into consideration, our inner bound recovers the amended Theorem 1 from [10] by setting $R_M = 0$, $V = (U, V)$, and maximizing only over distributions that satisfy $I(U;Y) - I(U;S) > 0$.

To verify that (8) is not achievable without the additional constraint, consider the following setup.

- Let A, B and Q be three i.i.d. $\mathsf{Ber}(\frac{1}{2})$ random variables.
- Let $T = t(A, B, Q)$, where

$$t(a,b,q) = \begin{cases} a, & q = 0 \\ b, & q = 1 \end{cases} . \tag{9}$$

- Let Ψ be a *private* (i.e., unobserved by the eavesdropper) bib-pipe of rate 1.

Setting $S = (A, B)$, $X = \Psi$, $Y = (T, Q, \Psi)$ and $Z = A \oplus B$, gives rise to the following operational problem. Consider n rounds such that at each round $i \in [1 : n]$, the encoder observes two memoryless fair coin tosses, A_i and B_i (i.i.d. copies of A and B). The decoder observes only one of them, namely T_i, chosen at random, using a third memoryless fair coin Q_i. The decoder also observes Q_i, which informs it if $T_i = A_i$ or $T_i = B_i$; the encoder does not know which coin the decoder observed. The eavesdropper observes only the modulo 2 addition of the two coins. After n coin tossing rounds (recall that CSI is non-causal in our setup), the encoder transmits n bits to the decoder using the private bit-pipe. This transmission is inaccessible to the eavesdropper. The legitimate parties wish to agree upon a key that is kept secret from the eavesdropper.

A valid choice of random variables for (8) is

1) $\Psi \sim \mathsf{Ber}(\frac{1}{2})$ independent of (A, B, Q),
2) $U = Z = A \oplus B$,
3) $V = (A, B, \Psi)$,

which achieves $R_{\mathsf{Zib}} = 2$. Hence, by showing that the SK capacity of the proposed setup is strictly less than 2, we contradict the achievability of R_{Zib}. We do so by showing that the *vanishing average error probability* and the *weak secrecy* of the SK, used in the definition of achievability in [10], cannot coexist in this setup while a SK rate of 2 is attained.

A formulation of the subsequently outlined ideas is found in [13, Appendix B]. Assume a SK rate of 2 bits per channel use is attainable. Thus, there exists a sequence of codes $\{c_n\}_n$, inducing a sequence of SKs $\{K_n\}_n$. The sequence of keys approaches the rate of 2 bits, as n grows, while the decoding error and the information leakage rate vanish. All subsequent multi-letter entropy terms are taken with respect to the distribution induced by the corresponding c_n.

As stated in [13, Lemma 8], the rate assumption along with the vanishing decoding error requirement imply

$$\frac{1}{n} H(A^n, B^n | K_n) \xrightarrow[n\to\infty]{} 0. \tag{10}$$

This is proven in Appendix E of [13]; the proof utilizes the statistical relations between the random variables in play, as well as standard information identities. The meaning of (10) is that, asymptotically, the coin realizations can be reconstructed from the SK.

Then, we notice that the common randomness (CR) rate of this setup [17], which upper-bounds the SK rate $\frac{1}{n} H(K_n)$, is 2. Combining this observation with (10), it follows that

$$\frac{1}{n} H(K_n | A^n, B^n) \xrightarrow[n\to\infty]{} 0.$$

Thus, K_n and (A^n, B^n) are asymptotically recoverable from one another, which means that the only way the encoder and decoder can achieve a CR rate of 2, is by using the coin realizations as their CR. Finally, since, in each round, the eavesdropper observes $Z_i \triangleq A_i + B_i$, we have $\frac{1}{n} I(K_n; Z^n) \approx \frac{1}{n} I(A^n, B^n; Z_n) = 1$. This contradicts security.

REFERENCES

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

[2] U. M. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Inf. Theory*, vol. 39, no. 3, pp. 733–742, May 1993.

[3] R. Ahlswede and I. Csiszár, "Common randomness in information theory and cryptography. part i: secret sharing," *IEEE Trans. Inf. Theory*, vol. 39, no. 4, pp. 1121–1132, Jul. 1993.

[4] S. I. Gelfand and M. S. Pinsker, "Coding for channel with random parameters," *Problemy Pered. Inform. (Problems of Inf. Trans.)*, vol. 9, no. 1, pp. 19–31, 1980.

[5] Y. Chen and A. J. H. Vinck, "Wiretap channel with side information," *IEEE Trans. Inf. Theory*, vol. 54, no. 1, pp. 395–402, Jan. 2008.

[6] 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, available on ArXiv at https://arxiv.org/abs/1608.00743.

[7] A. Khisti, S. N. Diggavi, and G. W. Wornell, "Secret-key agreement with channel state information at the transmitter," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 672–681, Mar. 2011.

[8] G. Bassi, P. Piantanida, and S. Shamai (Shitz), "Secret key generation over noisy channels with common randomness," *ArXiv preprint*, Sep. 2016, available at https://arxiv.org/abs/1609.08330.

[9] V. Prabhakaran, K. Eswaran, and K. Ramchandran, "Secrecy via sources and channels," *IEEE Trans. Inf. Theory*, vol. 85, no. 11, pp. 6747–6765, Nov. 2012.

[10] A. Zibaeenejad, "Key generation over wiretap models with non-causal side information," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 7, pp. 1456–1471, July 2015.

[11] E. Song, P. Cuff, and V. Poor, "The likelihood encoder for lossy compression," *IEEE Trans. Inf. Theory*, vol. 62, no. 4, pp. 1836–1849, Apr. 2016.

[12] A. Bunin, Z. Goldfeld, H. H. Permuter, S. Shamai (Shitz), P. Cuff, and P. Piantanida, "Semantically-secured message-key trade-off over wiretap channels with random parameters," in *Proceedings of the 2nd Workshop on Communication Security: Cryptography and Physical Layer Security*. Springer International Publishing, 2018, pp. 33–48.

[13] ——, "Key and message semantic-security over state-dependent channels," *Accepted to IEEE Trans. Inf. Forensics Security*, Aug 2017, available at https://arxiv.org/abs/1708.04283.

[14] C. E. Shannon, "Channels with side information at the transmitter," *IBM J. Res. Devel.*, vol. 2, no. 4, pp. 289–293, Oct. 1958.

[15] A. V. Kuznetsov and B. S. Tsybakov, "Coding in a memory with defective cells," *Problemy Pered. Inform. (Problems of Inf. Trans.)*, vol. 10, no. 2, pp. 52–60, 1974.

[16] S. A. Jafar, "Channel capacity with causal and noncaudal side information - a unified view," *IEEE Trans. Inform. Theory*, vol. 52, no. 12, pp. 5468–5474, Dec. 2006.

[17] R. Ahlswede and I. Csiszár, "Common randomness in information theory and cryptography. ii. cr capacity," *IEEE Trans. Inf. Theory*, vol. 44, no. 1, pp. 225–240, Jan 1998.