The Wiretap Channel With Generalized Feedback: Secure Communication and Key Generation

Germán Bassi, *Member, IEEE*, Pablo Piantanida, *Senior Member, IEEE*, and Shlomo Shamai (Shitz), *Fellow, IEEE*

***Abstract*— It is a well-known fact that feedback does not increase the capacity of point-to-point memoryless channels, however, its effect in secure communications is not fully understood yet. In this paper, an achievable scheme for the wiretap channel with generalized feedback is presented. This scheme, which uses the feedback signal to generate a shared secret key between the legitimate users, encrypts the message to be sent at the bit level. New capacity results for a class of channels are provided, as well as some new insights into the secret key agreement problem. Moreover, this scheme recovers previously reported rate regions from the literature, and thus it can be seen as a generalization that unifies several results in the field.**

***Index Terms*— Information-theoretic security, wiretap channel, feedback, secret key, secrecy capacity, secret key capacity.**

I. Introduction

In RECENT years, there has been great interest in the study of the wiretap channel (WTC) [2] as a model for secure communications against eavesdroppers by harnessing the randomness inherently present in the physical medium (see [3] and references therein). Application to secure wireless networks is extremely attractive, not only because the open nature of the medium makes communication devices particularly sensitive to eavesdropping, but also because randomness is abundantly available in such scenarios. As a matter of fact, the current theory of physical layer security indicates that the part of the data that is secured cannot be retrieved by the eavesdropper, regardless of its computational power.

Manuscript received May 9, 2017; revised September 13, 2018; accepted October 11, 2018. Date of publication November 26, 2018; date of current version March 15, 2019. This work was supported by the FP7 Network of Excellence in Wireless COMmunications NEWCOM#. G. Bassi was supported in part by the Knut and Alice Wallenberg Foundation and in part by the Swedish Foundation for Strategic Research. S. Shamai (Shitz) was supported by the European Union's Horizon 2020 Research and Innovation Programme under Grant 694630. This paper was presented in part at the 2015 IEEE Information Theory Workshop (ITW), October, 2015 [1].

G. Bassi was with the Laboratoire des Signaux et Systèmes (L2S, UMR CNRS 8506) CentraleSupélec–CNRS–Université Paris-Sud, F-91192 Gif-sur-Yvette, France. He is now with the School of Electrical Engineering and Computer Science, KTH Royal Institute of Technology, 100 44 Stockholm, Sweden (e-mail: germanb@kth.se).

P. Piantanida is with CentraleSupélec–French National Center for Scientific Research (CNRS)–Université Paris-Sud, F-91192 Gif-sur-Yvette, France, and also with the Montreal Institute for Learning Algorithms (MILA), Université de Montréal, Montréal, QC H3T 1N8, Canada (e-mail: pablo.piantanida@centralesupelec.fr).

S. Shamai (Shitz) is with the Department of Electrical Engineering, Technion–Israel Institute of Technology, Haifa 32000, Israel (e-mail: sshlomo@ee.technion.ac.il).

Communicated by A. Khisti, Associate Editor for Shannon Theory.

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TIT.2018.2883299

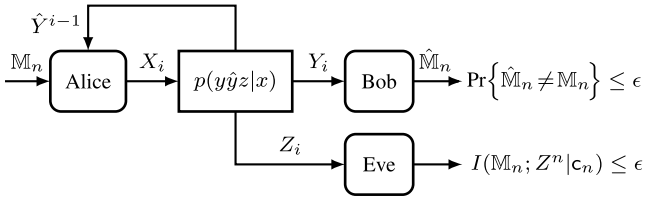

Fig. 1. Wiretap channel with generalized feedback.

A crucial observation behind this promising result is that unless the legitimate's and the eavesdropper's channels enjoy different statistical properties, which is often a nonrealistic assumption, secrecy cannot be guaranteed. Nevertheless, if both channels share the same statistical properties but some extra outdated side information is available at the transmitter, then the encoder can create the asymmetry required to ensure security (e.g., see [4], [5]). In fact, this observation reveals one of the major limitations of the wiretap model, whose performance strongly depends on the amount of outdated side information that may be available at the transmitter. Studying the impact on secrecy systems of different types of instantaneous information is therefore of both practical and theoretical interest.

In this work, we investigate the problem where a node, Alice, wishes to secretly communicate a message to another node, Bob, in presence of a passive eavesdropper, Eve, as depicted in Fig. 1. Alice can communicate with Bob using a general memoryless channel but Eve is listening this communication through another memoryless channel, whose statistical properties can be different or equal to Bob's. In addition, we assume that Alice observes general –may be noisy– outdated feedback which is correlated to the channel outputs of Bob and Eve, referred to as "generalized feedback". It is worth mentioning that this feedback model is rich enough since it handles several different types of outdated side information at the transmitter (e.g., delayed state-feedback or noisy feedback of the channel outputs) as well as both *secure* and *non-secure feedback* scenarios. Therefore, the generalized feedback model provides the adequate framework to investigate the impact of the feedback model.

A. Related Work

There has been substantial work on the wiretap channel with different feedback models, however, the capacity in the general case remains unresolved. Feedback, even partial, is known

to increase the capacity of several multi-terminal networks with respect to the non-feedback case (e.g., broadcast [6] and multiple access channels [7]). The transmitter uses the feedback signal to provide the decoder with noisy functions of the channel noise or parameters, and the messages. This communication is accomplished by two fundamentally different classes of coding schemes: those based on block Markov (digital) coding [6], [7], and those based on linear (analog) encoding [8], known as *Schalkwijk-Kailath* (S-K) scheme, which perform well over additive Gaussian models.

In the literature, there exist two complementary approaches on the use of the feedback signal to secure the communication. On the first one, Alice and Bob extract common randomness from their respective channel outputs which they use as a shared *secret key*. This key encrypts the message at the bit level which provides secrecy as long as Eve cannot obtain the key. On the second approach, Alice relies on a "feedback-dependent codebook" that correlates the codewords to be sent with the feedback signal. In this way, Alice seeks to hide as much as possible the transmitted codewords from Eve's observations (e.g., *beamforming* at the codeword level). Due to the inherently digital nature of encrypting the message bitwise, only the block Markov scheme is suited for the first approach, while both block Markov and S-K schemes are possible for the second methodology.

Results based on the secret key approach are numerous, as it seems natural to use the feedback link (secure or not) to agree upon a key. In [9], the authors analyze the WTC with perfect output feedback only at the encoder and propose a scheme based on this methodology. This scheme achieves the capacity of the *degraded*, i.e., $X \multimap Y \multimap Z$, and *reversely degraded*, i.e., $X \multimap Z \multimap Y$, WTC with perfect output feedback. The case of parallel channels, i.e., $Y \multimap X \multimap Z$, is studied in [10], where the secrecy capacity is characterized when one of the channels is *more capable* than the other. A similar model to [9], where the feedback link is in fact a secure rate-limited channel from Bob to Alice, is presented in [11]. In contrast to the previous schemes, the key is here created with *fresh* randomness that Bob transmits.

The use of state-feedback as a means to generate a key has also been analyzed, either when it is known only by the legitimate users [12] or by all the nodes in the network [13]. The authors of [12] propose a lower bound for the general discrete memoryless WTC with state information at both the encoder and decoder, which is tight in several scenarios, e.g., when Bob is *less noisy* than Eve, or when Eve is less noisy than Bob and the channel is independent of the state. In [13], the authors study a communication scenario where an encoder transmits private messages to several receivers through a broadcast erasure channel, and the receivers feed back (publicly) their channel states. Capacity is characterized based on linear complexity two-phase schemes: in the first phase appropriate secret keys are generated which are exploited during the second phase to encrypt each message.

Indeed, the generation of the secret key is a problem in and of itself [14], [15]. Two models exist that tackle this issue: the "source model", when the generation is based on the common randomness present in correlated sources, and the "channel model", when the common randomness is due to the correlation between inputs and outputs of a channel. The authors of [16] study the first model, where two nodes generate common randomness with the aid of a third "helper" node, all of them connected by noiseless rate-limited links. This common randomness may be kept secret from a fourth passive node that acts as an eavesdropper. The same authors also analyze the channel model in [17]. Capacity results are presented in both [16] and [17] when there is only one round of communication over the noiseless public link. General lower and upper bounds for both source and channel models when interaction is allowed are found in [18] and [19].

More recently, [20] investigates a similar problem as [16] but there is no helper node, the users communicate over a WTC, and a public discussion channel may or may not be available. On the other hand, [21] analyzes key agreement over a multiple access channel, i.e., the channel model. Here the receiver can actively send feedback, through a noiseless or noisy link, to increase the size of the shared key. The authors of [22] go one step further and study the simultaneous transmission of a secret message along with a key generation scheme using correlated sources. They obtain a simple expression that shows the trade-off between the achievable secrecy rate and the achievable secret key rate.

Results based on the "feedback-dependent codebook" approach, however, are not that numerous to the best of our knowledge. Early work in [23] and [24] study the multiple access channel (MAC) with generalized feedback and secrecy constraints. In [23] the eavesdropper is an external user to the MAC and the cooperating encoders use (partial) *decode-and-forward* strategies to enlarge their achievable rates. On the other hand, in [24], each encoder acts as an eavesdropper for the other user and the authors propose lower bounds based on *compress-and-forward* to increase the transmission rates to levels that are only decodable by the destination. Completely outdated state-feedback can also be used to enhance security. In [4] and [5], it is shown that outdated state-feedback of either the legitimate channel, the eavesdropper's channel or both, increases the secure degrees of freedom of the two-user Gaussian multiple-input multiple-output (MIMO) wiretap channel.

Active feedback in a half-duplex fashion is used in [25], where communication is split in two phases. In the first one, the destination sends a random codeword which cannot be decoded by the eavesdropper. On top of this "interference sequence", the codeword to be transmitted in the second phase is superimposed. This scheme achieves positive secrecy rates in the MIMO wiretap channel even when the eavesdropper has more antennas than the source. An analogous scheme is presented for the full-duplex two-way Gaussian wiretap channel in [26]. Here, the interference sequence sent in the first phase is canceled at the eavesdropper thanks to the full-duplex operation of the channel. Moreover, the authors show that neglecting the feedback signal can lead to unbounded loss in achievable rate under certain conditions.

In [27], the modulo-additive WTC with a full-duplex destination node is investigated. The authors propose a scheme where the legitimate receiver injects noise in the

backward (feedback) channel, effectively eliminating any correlation between the message sent and the eavesdropper's observation. This scheme achieves the full capacity of the point-to-point channel in absence of the wiretapper, i.e., full secrecy can be guaranteed at no rate cost. A similar conclusion is also drawn in [28], where the authors analyze an additive white Gaussian noisy (AWGN) channel with perfect output feedback from the legitimate receiver. They propose a S-K coding scheme which achieves the full capacity of the AWGN channel in absence of the wiretapper, as long as the eavesdropper has only access to a noisy feedback signal. This last result is generalized by the authors in [29], where an achievable strategy that combines block Markov and S-K schemes is introduced.

A closely related topic to the one addressed in this work is the WTC with *noncausal* side-information available to the parties. The model where the side-information is only available at the encoder is studied in [30], where a lower bound based on Gelfand and Pinsker's strategy for channels with state [31] is introduced. An extension to this model, with both the encoder and legitimate decoder having access to correlated side-information, is investigated in [32]. More recently, the authors of [33] analyze a slightly different scenario where the state affecting the legitimate decoder's channel is not equal to the one affecting the eavesdropper's channel. These channel states are correlated and the encoder only knows the state of the legitimate decoder's channel.

B. Contributions and Organization of the Paper

In this work, we derive the following results:

- We first introduce our main contribution (see Theorem 1), a lower bound based on the secret key approach, where the feedback link is used to generate a key that encrypts the message partially or completely.
- As an extension of Theorem 1, we derive a lower bound (see Theorem 2) on secret key agreement for the same channel model. The channel is used both as a source of correlated randomness and as a means of communication, i.e., there is no parallel public noiseless channel used by the terminals.
- In order to assess the optimality of these strategies, we derive upper bounds for a particular class of channels (see Theorems 3 and 4) and we show that the lower bound and its extension are optimal under some special conditions (see Propositions 1 to 6).
- In addition to these new capacity results, the first lower bound is shown to recover previously reported results for different channel and feedback models (see Theorems 5 and 6). Consequently, the lower bound provided in this work can be seen as a generalization and thus unification of several results in the field.

The rest of this paper is organized as follows. Section II introduces the general channel model and the one used for the capacity results, as well as some basic definitions. In Section III, we present our main results: the lower and upper bounds, whose proofs are deferred to the appendices. The new capacity results and the comparison with previously reported lower bounds are shown in Section IV, while the summary and concluding remarks are stated in Section V.

Notation and Conventions: In this work, we use the standard notation of [34]. Specifically, given two integers i and j, the expression $[i:j]$ denotes the set $\{i, i+1, \ldots, j\}$, whereas for real values a and b, $[a,b]$ denotes the closed interval between a and b. Lowercase letters such as x and y are mainly used to represent constants or realizations of random variables, capital letters such as X and Y stand for the random variables in itself, while calligraphic letters such as $\mathcal{X}$ and $\mathcal{Y}$ are reserved for sets, codebooks or special functions.

We use the notation $x_i^j = (x_i, x_{i+1}, \ldots, x_j)$ to denote the sequence of length $j-i+1$ for $1 \leq i \leq j$. If $i = 1$, we drop the subscript for succinctness, i.e., $x^j = (x_1, x_2, \ldots, x_j)$. For simplicity, n-sequences may be denoted either by x^n or $\mathbf{x}$. This comes in handy in the proofs where we deal with b blocks of n-sequences, i.e., $\mathbf{x}^b = (\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_b)$.

The probability distribution (PD) of the random vector X^n, $p_{X^n}(x^n)$, is succinctly written as $p(x^n)$ without subscript when it can be understood from the argument x^n. Given three random variables X, Y, and Z, if its joint PD can be decomposed as $p(xyz) = p(x)p(y|x)p(z|y)$, then they form a Markov chain, denoted by $X \multimap Y \multimap Z$. Entropy is denoted by $H(\cdot)$ and mutual information, $I(\cdot;\cdot)$. The expression $|x|^+$ stands for $\max\{x, 0\}$.

II. Problem Definition

In this work, we consider primarily the wiretap channel with generalized feedback (WTC-GF). Nonetheless, we also provide some insights on a specific class of channels that can be derived from the original system model. We now introduce these two models.

A. Wiretap Channel With Generalized Feedback

In the WTC-GF, Alice wants to securely transmit a message $\mathbb{M}_n$ (uniformly distributed over a message set $\mathcal{M}_n$) to Bob with the aid of a feedback signal while Eve observes the transmission. The WTC-GF, depicted in Fig. 1, is modeled as a discrete memoryless channel whose nth extension satisfies

$$p(y_i \hat{y}_i z_i | x^i y^{i-1} \hat{y}^{i-1} z^{i-1}) = p(y_i \hat{y}_i z_i | x_i), \tag{1}$$

for all $i \in [1:n]$. The right-hand side of (1) is independent of the time slot i and it is defined by the conditional probability distribution

$$p(y \hat{y} z | x) : \mathcal{X} \to \mathcal{Y} \times \hat{\mathcal{Y}} \times \mathcal{Z}, \tag{2}$$

where $x \in \mathcal{X}$ is Alice's channel input, $\hat{y} \in \hat{\mathcal{Y}}$ is the feedback signal, and $y \in \mathcal{Y}$ and $z \in \mathcal{Z}$ are Bob's and Eve's channel outputs, respectively.

Definition 1 (Code): A $(2^{nR}, n)$ code c_n for the WTC-GF consists of a message set $\mathcal{M}_n \triangleq [1 : 2^{nR}]$, a source of local randomness at the encoder $R_r \in \mathcal{R}_r$, a family of encoding functions $\text{enc}_i : (\mathcal{M}_n, \mathcal{R}_r, \hat{\mathcal{Y}}^{i-1}) \to \mathcal{X}_i$, and a decoding function $\text{dec} : \mathcal{Y}^n \to \mathcal{M}_n$.

The reliability performance of the $(2^{nR}, n)$ code c_n is measured in terms of its average probability of error

$$\mathsf{P}_e(\mathsf{c}_n) \triangleq \Pr\{\text{dec}(Y^n) \neq \mathbb{M}_n | \mathsf{c}_n\}, \tag{3}$$

while its secrecy performance is measured in terms of the information leakage

$$\mathsf{L}(\mathsf{c}_n) \triangleq I(\mathbb{M}_n; Z^n|\mathsf{c}_n). \tag{4}$$

Definition 2 (Achievable Rate): A *weak secrecy rate* R is achievable for the WTC-GF if for every $\epsilon > 0$ and sufficiently large n, there exists a $(2^{nR}, n)$ code c_n such that

$$\mathsf{P}_e(\mathsf{c}_n) \leq \epsilon \quad \text{and} \quad \frac{1}{n}\mathsf{L}(\mathsf{c}_n) \leq \epsilon. \tag{5}$$

On the other hand, a *strong secrecy rate* R is achievable for the WTC-GF if for every $\epsilon > 0$ and sufficiently large n, there exists a $(2^{nR}, n)$ code c_n such that

$$\mathsf{P}_e(\mathsf{c}_n) \leq \epsilon \quad \text{and} \quad \mathsf{L}(\mathsf{c}_n) \leq \epsilon. \tag{6}$$

Definition 3 (Capacity): The *weak secrecy capacity* C_{sf} of the WTC-GF is the supremum of all achievable weak secrecy rates. Similarly, the *strong secrecy capacity* $\overline{\mathrm{C}}_{sf}$ of the WTC-GF is the supremum of all achievable strong secrecy rates.

In this work, we also consider the situation where the source does not want to transmit a message but rather agree on a *secret key* (SK) with the legitimate decoder while keeping it private from the eavesdropper. The channel outputs, i.e., y, $\hat{y}$, and z, may be seen as correlated sources. This scenario is called "channel model" for key agreement, but in our case, the communication also takes place in the same channel rather than in a separate noiseless public broadcast channel.

Definition 4 (SK Code): A $(2^{nR_k}, n)$ secret key code c_n for the WTC-GF consists of a key set $\mathcal{K}_n \triangleq [1 : 2^{nR_k}]$, a source of local randomness at the encoder $R_r \in \mathcal{R}_r$, a family of encoding functions $\varphi_i : (\mathcal{R}_r, \hat{\mathcal{Y}}^{i-1}) \to \mathcal{X}_i$, a key generation function $\psi_a : (\mathcal{R}_r, \hat{\mathcal{Y}}^n) \to \mathcal{K}_n$, and a key generation function $\psi_b : \mathcal{Y}^n \to \mathcal{K}_n$.

Let $K = \psi_a(R_r, \hat{Y}^n)$, then, similar to (3)–(4), the performance of the $(2^{nR_k}, n)$ secret key code c_n is measured in terms of its average probability of error

$$\mathsf{P}_e(\mathsf{c}_n) \triangleq \Pr\{\psi_b(Y^n) \neq K|\mathsf{c}_n\}, \tag{7}$$

in terms of the information leakage

$$\mathsf{L}_k(\mathsf{c}_n) \triangleq I(K; Z^n|\mathsf{c}_n), \tag{8}$$

and in terms of the uniformity of the keys

$$\mathsf{U}_k(\mathsf{c}_n) \triangleq nR_k - H(K|\mathsf{c}_n). \tag{9}$$

Definition 5 (Achievable SK Rate): A *weak secret key rate* R_k is achievable for the WTC-GF if for every $\epsilon > 0$ and sufficiently large n, there exists a $(2^{nR_k}, n)$ SK code c_n such that

$$\mathsf{P}_e(\mathsf{c}_n) \leq \epsilon, \quad \frac{1}{n}\mathsf{L}_k(\mathsf{c}_n) \leq \epsilon, \text{ and } \frac{1}{n}\mathsf{U}_k(\mathsf{c}_n) \leq \epsilon. \tag{10}$$

On the other hand, a *strong secret key rate* R_k is achievable for the WTC-GF if for every $\epsilon > 0$ and sufficiently large n, there exists a $(2^{nR_k}, n)$ SK code c_n such that

$$\mathsf{P}_e(\mathsf{c}_n) \leq \epsilon, \quad \mathsf{L}_k(\mathsf{c}_n) \leq \epsilon, \text{ and } \mathsf{U}_k(\mathsf{c}_n) \leq \epsilon. \tag{11}$$

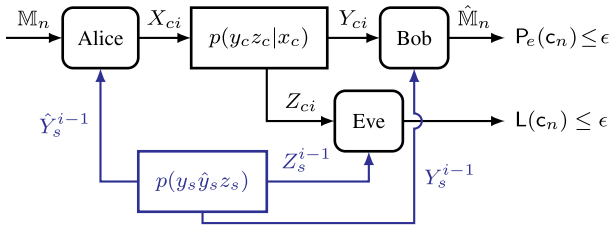

Fig. 2. Wiretap channel with independent correlated sources.

Definition 6 (SK Capacity): The *weak secret key capacity* C_{kf} of the WTC-GF is the supremum of all achievable weak SK rates. Similarly, the *strong secret key capacity* $\overline{\mathrm{C}}_{kf}$ of the WTC-GF is the supremum of all achievable strong SK rates.

B. Wiretap Channel With Parallel Sources

The channel model (2) is general enough to encompass different special scenarios; one of them, that we use later in the derivation of our capacity results, is depicted in Fig. 2. This model is a WTC without channel feedback where each node has causal access to correlated sources; in particular, Alice, Bob, and Eve observe $\hat{Y}_s$, Y_s, and Z_s, respectively. The sources are i.i.d. and independent of the main channel's variables (X_c, Y_c, Z_c). The new model may thus be defined based on the original one by the specific set of variables

$$\hat{Y} \triangleq \hat{Y}_s, \quad Y \triangleq (Y_s, Y_c), \quad \text{and} \quad Z \triangleq (Z_s, Z_c), \tag{12a}$$

with the following probability distribution

$$p(y_s y_c \hat{y}_s z_s z_c|x_c) = p(y_c z_c|x_c)\, p(y_s \hat{y}_s z_s). \tag{12b}$$

The performance metrics (3)–(4) and (7)–(9) as well as Definitions 1–6 for the problems of weak secrecy capacity (C_s), strong secrecy capacity ($\overline{\mathrm{C}}_s$), weak secret key capacity (C_k), and strong secret key capacity ($\overline{\mathrm{C}}_k$), may be readily extended to this new model using the set of variables (12).

III. Summary of Main Results

We present the main results of this work in the sequel. The proofs of these results are deferred to the appendices.

A. Wiretap Channel With Generalized Feedback

1) Secrecy Rate Lower Bound: We first introduce our main contribution, a coding scheme that allows Alice and Bob to agree on a secret key simultaneously with the transmission of a message. The secret key is generated by virtue of the feedback link and is used to encrypt at the bit level the next message to be sent. For ease of reference, the achievable scheme is denoted as "KG lower bound".

Theorem 1 (KG Lower Bound): A lower bound on the *strong secrecy capacity* of the WTC-GF is given by

$$\overline{\mathrm{C}}_{sf} \geq \max\left\{ \max_{p \in \mathcal{P}_{I_1}} R_{KG_1}(p), \max_{p' \in \mathcal{P}_{I_2}} R_{KG_2}(p') \right\},$$

where $R_{KG_1}(p)$ is the set of all nonnegative rates satisfying

$$\begin{aligned} R_{KG_1} \le\ & I(U;Y) - I(U;Z|Q) - I(U;T|QZ) \\ & - \max\{I(Q;Y),\ I(V;X\hat{Y}|UY)\} \\ & + I(V;Y|UT) - I(V;Z|UT), \qquad (13a) \\ R_{KG_1} \le\ & I(U;Y) - \max\{I(Q;Y),\ I(V;X\hat{Y}|UY)\}, \qquad (13b) \end{aligned}$$

whereas $R_{KG_2}(p')$ is the set of all nonnegative rates satisfying

$$\begin{aligned} R_{KG_2} &\le I(V;Y|UT) - I(V;Z|UT), \qquad (14a) \\ R_{KG_2} &\le I(U;Y) - I(V;X\hat{Y}|UY). \qquad (14b) \end{aligned}$$

The maximization is performed over $\mathcal{P}_{I_1}$, the set of all probability distributions given by

$$\begin{aligned} \mathcal{P}_{I_1} = \big\{ & p(quxvty\hat{y}z) \\ & = p(qu)p(x|u)p(y\hat{y}z|x)p(t|v)p(v|ux\hat{y}) \big\}, \qquad (15) \end{aligned}$$

and $\mathcal{P}_{I_2}$, the subset in $\mathcal{P}_{I_1}$ with $Q = \emptyset$. In the maximization, it suffices to consider $|\mathcal{Q}| \le |\mathcal{X}| + 4$, $|\mathcal{U}| \le |\mathcal{Q}|(|\mathcal{X}| + 3)$, $|\mathcal{T}| \le |\mathcal{X}| \cdot |\hat{\mathcal{Y}}| + 2$, and $|\mathcal{V}| \le |\mathcal{T}|(|\mathcal{X}| \cdot |\hat{\mathcal{Y}}| + 1)$.

Proof: In this scheme, the transmission is split into several blocks and the transmitted message in each block is encrypted fully (R_{KG_2}) or partially (R_{KG_1}). The codewords $\mathbf{T}$ and $\mathbf{V}$ are used to convey a description of the feedback signal $\hat{\mathbf{Y}}$ from the previous block, and thus they allow the legitimate users to *generate* the secret key during the transmission. In R_{KG_1}, the description is sent partially by $\mathbf{Q}$ and $\mathbf{U}$, hence the presence of the maximum in (13). Refer to Appendix A for further details. ∎

Insights behind (13) may be found by rewriting it as

$$\begin{aligned} R_{KG_1} \le\ & I(U;Y|Q) - I(U;Z|Q) - I(U;T|QZ) \\ & + I(V;Y|UT) - I(V;Z|UT), \qquad (16a) \\ R_{KG_1} \le\ & I(U;Y|Q), \qquad (16b) \end{aligned}$$

subject to

$$I(V;X\hat{Y}|UY) \le I(Q;Y). \qquad (16c)$$

The achievable secrecy rate (16a) has two main components: a part due to Wyner's wiretap coding scheme, given by the first two terms, and a part due to the encrypted message, given by the last two terms in (16a). The remaining term, i.e., $I(U;T|QZ)$, represents a rate penalty due to the correlation between the channel codeword $\mathbf{U}$ and the description $\mathbf{T}$ that Eve decodes. Moreover, the achievable secrecy rate cannot be larger than the "effective link capacity" (16b), i.e., the link capacity $I(U;Y)$ once the cost of the key agreement scheme (16c) is subtracted.

A similar analysis may be performed with (14), where only an encrypted message is sent.

Remark 1: If we set $Q = T = V = \emptyset$, we recover the achievable secrecy rate of the WTC without feedback.

2) SK Rate Lower Bound: In the absence of a message, the scheme in Theorem 1 may be employed by Alice and Bob to agree upon a secret key. This key could later be used to encrypt the transmission or part of it on a higher layer.

Theorem 2: A lower bound on the *strong secret key capacity* of the WTC-GF is given by

$$\begin{aligned} \overline{\mathrm{C}}_{kf} \ge \max_{p\in\mathcal{P}_{I_1}} \Big[& I(V;Y|UT) - I(V;Z|UT) + \big| I(U;Y) \\ & - \max\{I(Q;Y),\ I(V;X\hat{Y}|UY)\} \\ & - I(U;Z|Q) - I(U;T|QZ) \big|^+ \Big], \qquad (17) \\ \text{subject to } & I(V;X\hat{Y}|UY) \le I(U;Y). \qquad (18) \end{aligned}$$

The maximization in (17) is performed over $\mathcal{P}_{I_1}$, defined in (15), and it suffices to consider random variables with the same bounded cardinalities as in Theorem 1.

Proof: This result is a special case of the strategy in Theorem 1, where there is no message to be transmitted, i.e., $R = 0$, and we are only interested in generating a secret key. Refer to Appendix B for details. ∎

Remark 2: The results of Theorems 1 and 2 are obtained using the *weak* secrecy conditions (5) and (10), respectively. However, employing the method introduced in [35], we can show that the *strong* secrecy conditions (6) and (11) also hold true; therefore the theorems are expressed in terms of these stronger notions of secrecy.

B. Wiretap Channel With Parallel Sources

1) Secrecy Rate Upper Bound for a Class of Channels: For the specific channel model depicted in Fig. 2, we derive the following upper bound on the secrecy capacity.

Theorem 3: An upper bound on the *strong secrecy capacity* of the wiretap channel with parallel sources is given by

$$\overline{\mathrm{C}}_s \le \max_{p\in\mathcal{P}_o} R, \qquad (19)$$

where R is a nonnegative rate satisfying

$$\begin{aligned} R &\le I(U;Y_c) - I(U;Z_c) + I(V;Y_s|T) - I(V;Z_s|T), \qquad (20a) \\ R &\le I(X_c;Y_c) - I(V;\hat{Y}_s|Y_s), \qquad (20b) \end{aligned}$$

and the set of all input probability distributions is given by

$$\begin{aligned} \mathcal{P}_o = \big\{ & p(ux_cvty_cz_cy_s\hat{y}_sz_s) \\ & = p(ux_c)p(y_cz_c|x_c)p(y_s\hat{y}_sz_s)p(t|v)p(v|\hat{y}_s) \big\}, \qquad (21) \end{aligned}$$

with $|\mathcal{U}| \le |\mathcal{X}_c|$, $|\mathcal{T}| \le |\hat{\mathcal{Y}}_s| + 1$, and $|\mathcal{V}| \le (|\hat{\mathcal{Y}}_s| + 1)^2$.

Proof: Refer to Appendix C. ∎

Remark 3: In the absence of the correlated sources, the bound (20) collapses to the upper bound of the wiretap channel.

2) SK Rate Upper Bound for a Class of Channels: Let us now consider that, in the scenario depicted in Fig. 2, Alice and Bob want to agree upon a secret key by means of the correlated sources and the communication through the wiretap channel.

Theorem 4: An upper bound on the *strong secret key capacity* of this channel model is given by

$$\begin{aligned} \overline{\mathrm{C}}_k \le \max_{p\in\mathcal{P}_o} \big[& I(U;Y_c) - I(U;Z_c) + I(V;Y_s|T) \\ & - I(V;Z_s|T) \big], \qquad (22) \\ \text{subject to } & I(V;\hat{Y}_s|Y_s) \le I(X_c;Y_c), \qquad (23) \end{aligned}$$

where the set of all input probability distributions $\mathcal{P}_o$ is defined in (21) and the auxiliary random variables have the same bounded cardinalities as in Theorem 3.

Proof: Refer to Appendix D. ∎

Remark 4: The upper bound (22) is the sum of the secrecy capacity of the wiretap channel $p(y_c z_c|x_c)$, the first two terms on the right-hand side of (22), and the secret key capacity of the WTC with a public noiseless channel and correlated sources [16, Th. 2.6], the other two terms in (22).

Remark 5: Although the upper bounds in Theorems 3 and 4 are derived under the assumption that Alice observes its source sequence causally, both upper bounds are valid even if Alice has *noncausal* access to it.

IV. Capacity Results for Some Channel and Feedback Models

In this section, we first introduce new capacity results for the wiretap channel with parallel sources obtained by the KG lower bound (Sections IV-A and IV-B). Next, we show that previously reported results for other types of channel and feedback models are recovered by this scheme as well (Sections IV-C and IV-D). Finally, we present an example where the KG lower bound is not optimal (Section IV-E).

A. Secret Key Capacity for the WTC With Parallel Sources

We first analyze the secret key agreement problem for the model depicted in Fig. 2, where the nodes have access to correlated sources independent of the main channel. The upper bound for this model is found in Theorem 4, whereas the lower bound is derived from Theorem 2 by taking the set of variables (12) and restricting the input probability distributions, cf. (21), to the form:

$$p(qu)p(x_c|u)p(y_c z_c|x_c)p(y_s \hat{y}_s z_s)p(t|v)p(v|\hat{y}_s). \quad (24)$$

Then, the lower bound on the secret key rate (17) is given by

$$\overline{\mathrm{C}}_k \geq I(V;Y_s|T) - I(V;Z_s|T) + \big|I(U;Y_c) - I(U;Z_c|Q) - \max\{I(Q;Y_c),\ I(V;\hat{Y}_s|Y_s)\}\big|^+, \quad (25)$$

maximized over (24) and subject to

$$I(V;\hat{Y}_s|Y_s) \leq I(U;Y_c). \quad (26)$$

This bound is tight in some special cases.

1) Eve Has a Less Noisy Channel: If Eve has a less noisy channel than Bob, no secrecy can be guaranteed in the main channel and the secret key is generated using only the correlated sources.

Proposition 1: In this scenario, the strong secret key capacity is given by

$$\overline{\mathrm{C}}_k = \max_{p(x_c)p(t|v)p(v|\hat{y}_s)} \big[I(V;Y_s|T) - I(V;Z_s|T)\big], \quad (27)$$

$$\text{subject to } I(V;\hat{Y}_s|Y_s) \leq I(X_c;Y_c). \quad (28)$$

Proof: For a given PD in (21) and given the less noisy condition on Eve's channel, i.e., $I(U;Y_c) \leq I(U;Z_c)$ for any RV U such that $U \multimap X_c \multimap (Y_c Z_c)$, the upper bound from Theorem 4 reduces to (27)–(28) which is equal to the lower bound (25)–(26) with $Q = \emptyset$ and $U = X_c$. ∎

Remark 6: The secret key capacity of the WTC with a public noiseless channel of rate R [16, Th. 2.6] is a special case of Proposition 1, where $X_c = Y_c = Z_c$ and $H(X_c) = R$. This result was also noted in [36, Th. 1].

2) Eve Has a Less Noisy Side Information: If Eve has a less noisy side information than Bob, the legitimate users cannot extract any secret bits from the correlated sources; the key is the message carried by the codeword $\mathbf{U}$, which is secured from Eve by Wyner's wiretap coding scheme.

Proposition 2: In this scenario, the strong secret key capacity is given by

$$\overline{\mathrm{C}}_k = \max_{p(u x_c)} \big[I(U;Y_c) - I(U;Z_c)\big]. \quad (29)$$

Proof: Given the less noisy condition on Eve's side information, i.e., $I(V;Y_s) \leq I(V;Z_s)$ for any RV V such that $V \multimap \hat{Y}_s \multimap (Y_s Z_s)$, the upper bound reduces to (29) and the condition (23) disappears. Additionally, the lower bound (25)–(26) achieves (29) with $Q = T = V = \emptyset$. ∎

Remark 7: Since the side information cannot be used to generate a secret key, the secret key capacity (29) is equal to the secrecy capacity of the WTC.

3) Alice and Bob Have the Same Side Information: If the legitimate users have access to the same side information, there is no need to transmit the bin indices of the description.

Proposition 3: In this scenario, the strong secret key capacity is given by

$$\overline{\mathrm{C}}_k = \max_{p(u x_c)} \Big[H(Y_s|Z_s) + \big|I(U;Y_c) - I(U;Z_c)\big|^+\Big]. \quad (30)$$

Proof: If $\hat{Y}_s = Y_s$, the transmission cost of the description associated to the source disappears, i.e., $I(V;\hat{Y}_s|Y_s) = 0$, which renders the conditions (23) and (26) redundant, and an achievable rate according to both the upper and lower bounds satisfies

$$R_k \leq I(V;Y_s|Z_s) + \big|I(U;Y_c) - I(U;Z_c)\big|^+ \quad (31a)$$

$$\leq H(Y_s|Z_s) + \big|I(U;Y_c) - I(U;Z_c)\big|^+, \quad (31b)$$

where

- (31a) stems from the Markov chain $T \multimap V \multimap Y_s \multimap Z_s$ (due to $\hat{Y}_s = Y_s$), and $Q = \emptyset$ in the lower bound; and,
- in (31b) we maximize the first term with $V = Y_s$. ∎

B. Secrecy Capacity for the WTC With Parallel Sources

We now study the secrecy capacity for the model depicted in Fig. 2. The upper bound for this model is found in Theorem 3, whereas the lower bound can be derived from Theorem 1 by taking the set of variables (12) and restricting the input probability distributions to the form (24). Then, the achievable secrecy rate R_{KG_1} (13) is given by

$$R_{KG_1} \leq I(V;Y_s|T) - I(V;Z_s|T) + I(U;Y_c) - I(U;Z_c|Q) - \max\{I(Q;Y_c),\ I(V;\hat{Y}_s|Y_s)\}, \quad (32a)$$

$$R_{KG_1} \leq I(U;Y_c) - \max\{I(Q;Y_c),\ I(V;\hat{Y}_s|Y_s)\}, \quad (32b)$$

and R_{KG_2} (14) by

$$R_{KG_2} \leq I(V;Y_s|T) - I(V;Z_s|T), \quad (33a)$$

$$R_{KG_2} \leq I(U;Y_c) - I(V;\hat{Y}_s|Y_s). \quad (33b)$$

This bound is tight in some special cases.

1) Eve Has a Less Noisy Channel: As in Section IV-A1, in the situation where Eve has a less noisy channel than Bob, the achievable secrecy rate is only due to the secret key generated using the correlated sources.

Proposition 4: In this scenario, the strong secrecy capacity is given by

$$\overline{\mathrm{C}}_s = \max_{p(x_c)p(t|v)p(v|\hat{y}_s)} \min\Big\{ I(V;Y_s|T) - I(V;Z_s|T), \; I(X_c;Y_c) - I(V;\hat{Y}_s|Y_s)\Big\}. \quad (34)$$

Proof: For a probability distribution in (21) and given the less noisy condition on Eve's channel, the upper bound from Theorem 3 reduces to (34) which is equal to the lower bound (33) with $U = X_c$. ∎

2) Eve Has a Less Noisy Side Information: If Eve has a less noisy side information than Bob, the legitimate users cannot extract any secret bits from the correlated sources, and this problem reduces to the wiretap channel.

Proposition 5: In this scenario, the strong secrecy capacity is given by

$$\overline{\mathrm{C}}_s = \max_{p(ux_c)} \big[I(U;Y_c) - I(U;Z_c)\big]. \quad (35)$$

Proof: Given the less noisy condition on Eve's side information, the bound (20a) becomes (35) while the bound (20b) becomes redundant. The bound (35) is achieved by the lower bound (32) with $Q = T = V = \emptyset$. ∎

3) Alice and Bob Have the Same Side Information and Bob Has a Less Noisy Channel: Unlike Section IV-A3, in order to achieve capacity the legitimate users not only have to share the same side information but also Bob needs a less noisy channel than Eve.

Proposition 6: In this scenario, the strong secrecy capacity is given by

$$\overline{\mathrm{C}}_s = \max_{p(x_c)} \min\big\{ I(X_c;Y_c), \; I(X_c;Y_c) - I(X_c;Z_c) + H(Y_s|Z_s)\big\}. \quad (36)$$

Proof: If $\hat{Y}_s = Y_s$, the transmission cost of the description associated to the source disappears, i.e., $I(V;\hat{Y}_s|Y_s) = 0$, and following similar arguments as those in (31), an achievable rate according to the upper bound (20) satisfies

$$R \le \min\{I(X_c;Y_c),\; I(U;Y_c) - I(U;Z_c) + H(Y_s|Z_s)\}.$$

We may further upper-bound part of this expression as follows:

$$\begin{aligned} &I(U;Y_c) - I(U;Z_c) \\ &\quad = I(X_c;Y_c) - I(X_c;Y_c|U) - I(X_c;Z_c) + I(X_c;Z_c|U) \\ &\quad \le I(X_c;Y_c) - I(X_c;Z_c), \end{aligned}$$

where the inequality is due to Bob's channel being less noisy than Eve's. Hence, the upper bound becomes (36) under the aforementioned conditions, which is achieved by the lower bound (32) with $Q = T = \emptyset$, $V = Y_s$, and $U = X_c$. ∎

C. Wiretap Channel With Perfect Output Feedback

In [9], the authors analyze a wiretap channel with perfect output feedback at the encoder, i.e., $\hat{Y} = Y$, and perfectly secured from the eavesdropper.

Theorem 5 [9, Th. 1]: In this model, the KG lower bound introduced in Theorem 1 achieves all rates satisfying

$$R \le \max_{p(ux)} \min\big\{ I(U;Y), \; |I(U;Y) - I(U;Z)|^+ + H(Y|UZ)\big\}. \quad (37)$$

Proof: With the following choice of RVs

$$V = Y \quad \text{and} \quad T = Q = \emptyset,$$

the achievable secrecy rate R_{KG_1} (13) becomes

$$R_{KG_1} \le \min\{I(U;Y) - I(U;Z) + H(Y|UZ),\; I(U;Y)\},$$

while the achievable secrecy rate R_{KG_2} (14) reads

$$R_{KG_2} \le \min\{H(Y|UZ),\; I(U;Y)\}.$$

Therefore, the maximization over both strategies can be succinctly written as (37). ∎

Remark 8: The secrecy capacity results for the *degraded* and *reversely degraded* WTC with perfect output feedback [9, Corollaries 1 and 2] also apply here.

D. Wiretap Channel With Causal State Information

In [12], the authors analyze a wiretap channel affected by a random state S, i.e., $p(yz|xs)p(s)$, where the state is available causally only at the encoder and the legitimate decoder, i.e., $\hat{Y} = S$ and $Y = (Y, S)$.

Theorem 6 [12, Th. 1]: In this model, a slightly modified version of the KG scheme presented in Theorem 1 achieves all the rates satisfying

$$\begin{aligned} R \le \max \Bigg\{ &\max_{p(u)u'(u,s)p(x|u's)} \min\{I(U;YS) - I(U;ZS) \\ &+ H(S|Z),\; I(U;YS)\}, \\ &\max_{p(u)p(x|us)} \min\{H(S|ZU),\; I(U;Y|S)\} \Bigg\}. \end{aligned} \quad (38)$$

Proof: First, we make the choice of RVs

$$V = S \quad \text{and} \quad T = Q = \emptyset.$$

Second, since the KG scheme is derived to handle *strictly* causal feedback, and the present model assumes the state is known causally at the encoder, i.e., s^i is present at time slot i, we need to perform a slight modification of the scheme.

We can modify step 4) from the encoding procedure (Appendix A-B) in the following way. For R_{KG_1}, after the encoder has chosen the codeword to transmit in block j, i.e., $\mathbf{u}(\underline{r}_j)$, it computes $u'_i = u'(u_i(\underline{r}_j), s_i)$ and transmits a randomly generated symbol x_i according to $p(x_i|u'_i s_i)$ for each time slot $i \in [1:n]$. The rate (13) becomes

$$\begin{aligned} R_{KG_1} &\le I(U;YS) - I(U;Z) + H(S|ZU) \\ &= I(U;YS) - I(U;ZS) + H(S|Z), \\ R_{KG_1} &\le I(U;YS). \end{aligned}$$

For R_{KG_2}, we proceed similarly but without the inclusion of the function $u'(\cdot)$ between the codeword $\mathbf{u}(\underline{r}_j)$ and the generation of x_i. The rate (14) becomes

$$R_{KG_2} \leq I(S; YS|U) - I(S; Z|U) = H(S|ZU),$$
$$R_{KG_2} \leq I(U; YS) = I(U; Y|S).$$

Therefore, the final expression for the rate is (38). ∎

Remark 9: The secrecy capacity result for *less noisy* WTC with state information available causally or noncausally at the encoder and decoder [9, Th. 3] also applies here.

E. Erasure Wiretap Channel With State-Feedback

In [13], the authors analyze the erasure WTC with public state-feedback from the legitimate receiver; therefore, both the encoder and the eavesdropper know if there was an erasure or not at the legitimate end. In other words, let $S \triangleq \mathbb{1}\{Y = e\}$ indicate the erasure event at the legitimate user, then

$$\hat{Y} \triangleq S \quad \text{and} \quad Z \triangleq (Z', S), \tag{39}$$

where Z' is the eavesdropper's channel output. Moreover, the channels experience independent erasures, i.e., $p(yz'|x) = p(y|x)p(z'|x)$.

Proposition 7: In this scenario, it can be shown that the KG lower bound from Theorem 1 achieves any rate

$$R \leq (1-\delta)\delta_E \max\left\{\frac{1-\delta}{1-\delta\delta_E}, \frac{1}{1+\delta_E}\right\}, \tag{40}$$

where δ denotes the erasure probability of the legitimate receiver and δ_E, the one of the eavesdropper.

Proof: See Appendix G. ∎

Even though (40) is the maximum secrecy rate achieved by the KG scheme, it is strictly suboptimal. The secrecy capacity of this channel model is given by [13, Corollary 1]

$$\overline{\mathsf{C}}_{sf} = (1-\delta)\delta_E \frac{1-\delta\delta_E}{1-\delta\delta_E^2}, \tag{41}$$

and numerical analysis shows that (40) is strictly below (41) for all δ and $\delta_E \in (0, 1)$.

V. Summary and Concluding Remarks

In this work, we presented an achievable scheme for the wiretap channel with generalized feedback, the KG lower bound, which allows the legitimate users to agree on a secret key simultaneously with the transmission of a message. As an extension to this scheme, we introduced a strategy for the problem of secret key agreement, which is essentially the KG lower bound when no message is transmitted.

Due to the complexity of the general problem, we resorted to simpler channel models to characterize the merit of these schemes. For a special class of channels, which we named wiretap channel with parallel sources, we derived two novel upper bounds and we showed the optimality of the KG lower bound and its secret key counterpart under some special conditions. As a side note, it should be mentioned that the capacity result in Proposition 4 was recently re-discovered in [37, Corollary 1] by employing a different coding scheme than our work in [38].

In addition to these new capacity results, the KG lower bound also recovered previously reported results for different channel and feedback models. Consequently, this lower bound could be seen as a generalization, and hence unification of several results in the field. Nonetheless, the unification is not complete since the KG lower bound failed to recover all known results, as shown in Section IV-E.

Appendix A
Proof of Theorem 1 (KG Lower Bound)

The encoder splits the transmission in b blocks of n channel uses, during which it transmits $b-1$ messages of rate R. During each transmission block and in addition to the messages, the encoder also sends the bin indices corresponding to two layers of description of the feedback sequence it observed in the previous block. This allows the legitimate users to agree on a secret key which is used to encrypt part of the transmission.

The messages are sent using one of the following two strategies. In the first one, the rate $R = R_{KG_1}$ is achievable by the joint use of Wyner's wiretap coding scheme, which provides a secure rate of R_0 bits, and a bitwise-encrypted message, which grants the remaining $R_1 = R - R_0$ secure bits. The second strategy only relies on the aforementioned secret key to send an encrypted message of rate $R = R_{KG_2}$.

In the sequel, we present the proof for R_{KG_1} in detail while only a sketch of the proof of R_{KG_2} is provided after that. We note that the rates are shown to be achievable according to the weak secrecy condition (5). Nonetheless, we demonstrate at the end of this Appendix that the strong secrecy condition (6) also holds true.

A. Codebook Generation

Let us define the quantities

$$S_1 = I(T; UX\hat{Y}|Q) + \epsilon_1, \tag{42a}$$
$$\tilde{S}_1 = I(T; UX\hat{Y}|Q) - I(T; UY|Q) + \epsilon_1 + \tilde{\epsilon}_1, \tag{42b}$$
$$S_2 = I(V; X\hat{Y}|UT) + \epsilon_2, \tag{42c}$$
$$\tilde{S}_2 = I(V; X\hat{Y}|UT) - I(V; Y|UT) + \epsilon_2 + \tilde{\epsilon}_2, \tag{42d}$$
$$\bar{S}_2 = I(V; Y|UT) - I(V; Z|UT), \tag{42e}$$
$$R_1 + R_f = I(U; TZ|Q) - \epsilon', \tag{42f}$$

and fix the joint distribution (15) that achieves the maximum in R_{KG_1}. Then, for each block, create independent codebooks as follows:

1) Randomly pick $2^{n\tilde{S}'}$ sequences $\mathbf{q}(l')$, $l' \in [1 : 2^{n\tilde{S}'}]$, from $\mathcal{T}_\delta^n(Q)$.
2) For each $\mathbf{q}(l')$, randomly pick $2^{n(\tilde{S}''+R_0+R_1+R_f)}$ sequences $\mathbf{u}(\underline{r}) \equiv \mathbf{u}(l', l'', m_0, m_1, l_f)$, where $l'' \in [1 : 2^{n\tilde{S}''}]$, $m_0 \in [1 : 2^{nR_0}]$, $m_1 \in [1 : 2^{nR_1}]$, and $l_f \in [1 : 2^{nR_f}]$, from $\mathcal{T}_\delta^n(U|\mathbf{q}(l'))$.
3) For each $\mathbf{q}(l')$, randomly pick 2^{nS_1} sequences $\mathbf{t}(l', s_1)$, where $s_1 \in [1 : 2^{nS_1}]$, from $\mathcal{T}_\delta^n(T|\mathbf{q}(l'))$. Distribute the sequences uniformly at random in $2^{n\tilde{S}_1}$ equal-sized bins $B_1(l_1)$, which is possible since $\tilde{S}_1 \leq S_1$.
4) For each possible triplet $(\mathbf{q}(l'), \mathbf{u}(\underline{r}), \mathbf{t}(l', s_1))$, randomly pick 2^{nS_2} sequences $\mathbf{v}(\underline{r}, s_1, s_2)$, where

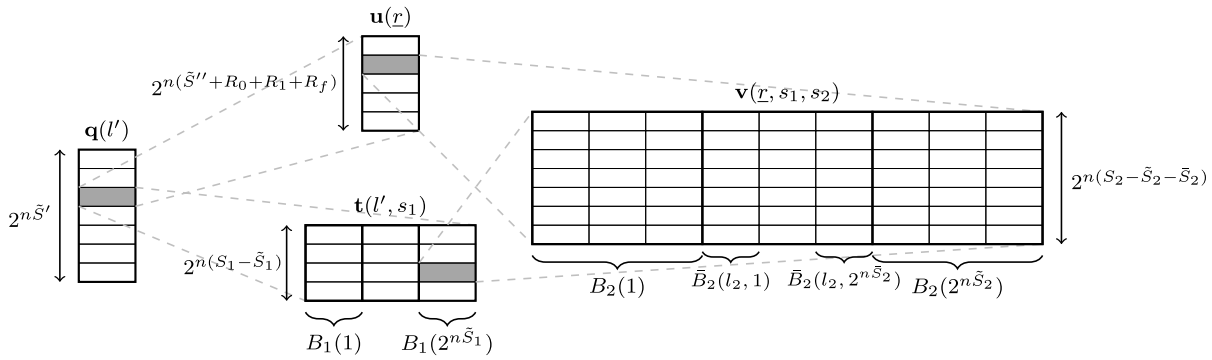

Fig. 3. Schematic representation of the codebook. The index s_1 in the bins and sub-bins of $\mathbf{v}(\cdot)$ is not shown to improve readability.

$s_2 \in [1 : 2^{nS_2}]$, from $\mathcal{T}_\delta^n(V|\mathbf{q}(l'), \mathbf{u}(\underline{r}), \mathbf{t}(l', s_1))$. Distribute the sequences uniformly at random in $2^{n\tilde{S}_2}$ equal-sized bins $B_2(s_1, l_2)$ and the sequences in each bin in $2^{n\bar{S}_2}$ equal-sized sub-bins $\bar{B}_2(s_1, l_2, k)$. This binning process is feasible if

$$\tilde{S}_2 \le S_2, \tag{43a}$$

$$\bar{S}_2 \le S_2 - \tilde{S}_2, \tag{43b}$$

which holds according to (42) as long as $I(V; Z|UT) \le I(V; Y|UT)$. Moreover, partition the set $[1 : 2^{n\bar{S}_2}]$ in 2^{nR_1} equal-sized subsets, which defines the mapping $k' = M_k(k)$, where $k' \in [1 : 2^{nR_1}]$. This partition is possible if

$$R_1 \le \bar{S}_2. \tag{44}$$

See Fig. 3 for details.

B. Encoding

In the first block, the encoder chooses a codeword $\mathbf{u}(\underline{r}_1)$ uniformly at random. It then transmits the sequence $\mathbf{x}_1$ that is randomly generated according to the conditional PD $p(\mathbf{x}|\mathbf{u}(\underline{r}_1)) = \prod_{i=1}^n p(x_i|u_i(\underline{r}_1))$.

In block $j \in [2 : b]$, proceed as follows:

1) Given the channel input and the feedback signal from the previous block, the encoder looks for an index $s_{1(j-1)} \equiv \hat{s}_1$ such that

$$\Big(\mathbf{t}(l'_{j-1}, \hat{s}_1), \mathbf{q}(l'_{j-1}), \mathbf{u}(\underline{r}_{j-1}), \mathbf{x}_{j-1}, \hat{\mathbf{y}}_{j-1}\Big) \in \mathcal{T}_{\delta'}^n(TQUX\hat{Y}),$$

where $\delta' < \epsilon_1$. If more than one index is found, choose one uniformly at random, whereas if there is no such index, choose one uniformly at random in $[1 : 2^{nS_1}]$. The probability of not finding such an index is arbitrarily small as $n \to \infty$.

2) Then, the encoder looks for an index $s_{2(j-1)} \equiv \hat{s}_2$ such that

$$\big(\mathbf{v}(\underline{r}_{j-1}, s_{1(j-1)}, \hat{s}_2), \mathbf{t}(l'_{j-1}, s_{1(j-1)}), \mathbf{q}(l'_{j-1}), \mathbf{u}(\underline{r}_{j-1}), \mathbf{x}_{j-1}, \hat{\mathbf{y}}_{j-1}\big) \in \mathcal{T}_{\delta'}^n(VTQUX\hat{Y}),$$

where $\delta' < \epsilon_2$. If more than one index is found, choose one uniformly at random, whereas if there is no such index, choose one uniformly at random in $[1 : 2^{nS_2}]$. The probability of not finding such an index is arbitrarily small as $n \to \infty$.

3) Let $\mathbf{v}(\underline{r}_{j-1}, s_{1(j-1)}, s_{2(j-1)}) \in \bar{B}_2(s_{1(j-1)}, l_{2(j-1)}, k_{j-1})$ and $\mathbf{t}(l'_{j-1}, s_{1(j-1)}) \in B_1(l_{1(j-1)})$, and define the following mapping. Let $(l'_j, l''_j) = M_l(l_{1(j-1)}, l_{2(j-1)})$, such that $M_l(\cdot)$ is invertible. This function can be defined if

$$\tilde{S}' + \tilde{S}'' = \tilde{S}_1 + \tilde{S}_2. \tag{45}$$

4) In order to transmit the message $m_j = (m_{0j}, m_{1j})$, the encoder chooses uniformly at random a value for the index $l_{fj} \in [1 : 2^{nR_f}]$ and selects the codeword $\mathbf{u}(l'_j, l''_j, m_{0j}, m'_{1j}, l_{fj}) = \mathbf{u}(\underline{r}_j)$, where $m'_{1j} = m_{1j} \oplus k'_{j-1}$ and $k'_{j-1} = M_k(k_{j-1})$. It then transmits the sequence $\mathbf{x}_j$ that is randomly generated according to the conditional PD $p(\mathbf{x}|\mathbf{u}(\underline{r}_j)) = \prod_{i=1}^n p(x_i|u_i(\underline{r}_j))$.

C. Decoding

At the end of each transmission block $j \in [1 : b]$, the legitimate decoder looks for the unique set of indices $\underline{r}_j = (l'_j, l''_j, m_{0j}, m'_{1j}, l_{fj}) \equiv (\hat{l}', \hat{l}'', \hat{m}_0, \hat{m}'_1, \hat{l}_f)$ such that

$$\big(\mathbf{q}(\hat{l}'), \mathbf{u}(\hat{l}', \hat{l}'', \hat{m}_0, \hat{m}'_1, \hat{l}_f), \mathbf{y}_j\big) \in \mathcal{T}_\delta^n(QUY).$$

The probability of error in decoding can be made arbitrarily small provided that

$$\tilde{S}'' + R_0 + R_1 + R_f < I(U; Y|Q) - \delta, \tag{46a}$$

$$\tilde{S}' + \tilde{S}'' + R_0 + R_1 + R_f < I(U; Y) - \delta. \tag{46b}$$

Additionally, in block $j \in [2 : b]$, proceed as follows:

1) The legitimate decoder computes $(l_{1(j-1)}, l_{2(j-1)}) = M_l^{-1}(l'_j, l''_j)$.
2) It then looks for the unique index $s_{1(j-1)} \equiv \hat{s}_1$ such that $\mathbf{t}(l'_{j-1}, \hat{s}_1) \in B_1(l_{1(j-1)})$ and

$$\Big(\mathbf{t}(l'_{j-1}, \hat{s}_1), \mathbf{q}(l'_{j-1}), \mathbf{u}(\underline{r}_{j-1}), \mathbf{y}_{j-1}\Big) \in \mathcal{T}_\delta^n(TQUY),$$

where $\delta < \tilde{\epsilon}_1$. The probability of error in decoding is arbitrarily small as $n \to \infty$.

3) The legitimate decoder additionally looks for the unique index $s_{2(j-1)} \equiv \hat{s}_2$ such that $\mathbf{v}(\underline{r}_{j-1}, s_{1(j-1)}, \hat{s}_2) \in B_2(s_{1(j-1)}, l_{2(j-1)})$ and

$$\big(\mathbf{v}(\underline{r}_{j-1}, s_{1(j-1)}, \hat{s}_2), \mathbf{t}(l'_{j-1}, s_{1(j-1)}), \mathbf{q}(l'_{j-1}), \mathbf{u}(\underline{r}_{j-1}), \mathbf{y}_{j-1}\big) \in \mathcal{T}_\delta^n(VTQUY),$$

where $\delta < \tilde{\epsilon}_2$. The probability of error in decoding is arbitrarily small as $n \to \infty$.

4) The legitimate decoder is therefore able to recover the secret key $k'_{j-1} = M_k(k_{j-1})$ from the sub-bin k_{j-1}, i.e., $\mathbf{v}(\underline{r}_{j-1}, s_{1(j-1)}, s_{2(j-1)}) \in \bar{B}_2(s_{1(j-1)}, l_{2(j-1)}, k_{j-1})$, and with this key, it decrypts the message of the present block, i.e., $m_j = (m_{0j}, m'_{1j} \oplus k'_{j-1})$.

D. Key Leakage

Let us denote with L_{1j} the random variable associated with the bin index of codeword $\mathbf{T}_j$ in block j, and L_{2j} and K_j the random variables associated with the bin and sub-bin index of codeword $\mathbf{V}_j$ in block j, respectively.

Remark 10: Owing to the encoding procedure, the variables L_{1j}, L_{2j}, and $K'_j = M_k(K_j)$ are the only cause of the correlation between blocks, the latter through $\mathbb{M}'_{1(j+1)} = \mathbb{M}_{1(j+1)} \oplus K'_j$. This fact is used in many of the subsequent Markov chains.

Consider the following,

$$\begin{aligned}
H(K^{b-1}|\mathcal{C}\mathbf{Z}^b) &= \sum_{j=1}^{b-1} H(K_j|\mathcal{C}\mathbf{Z}^b K^{j-1}) \\
&\geq \sum_{j=1}^{b-1} H(K_j|\mathcal{C}\mathbf{U}_j\mathbf{Z}_j^b) && \text{(47a)} \\
&\geq \sum_{j=1}^{b-1} H(K_j|\mathcal{C}\mathbf{U}_j\mathbf{Z}_j L_{1j} L_{2j}\mathbb{M}'_{1(j+1)}) && \text{(47b)} \\
&\geq \sum_{j=1}^{b-1} H(K_j|\mathcal{C}\mathbf{U}_j\mathbf{Z}_j\mathbf{T}_j L_{2j}\mathbb{M}'_{1(j+1)}) \\
&= \sum_{j=1}^{b-1} H(K_j\mathbf{X}_j\hat{\mathbf{Y}}_j|\mathcal{C}\mathbf{U}_j\mathbf{Z}_j\mathbf{T}_j L_{2j}\mathbb{M}'_{1(j+1)}) \\
&\quad - H(\mathbf{X}_j\hat{\mathbf{Y}}_j|\mathcal{C}\mathbf{U}_j\mathbf{Z}_j\mathbf{T}_j L_{2j} K_j), && \text{(47c)}
\end{aligned}$$

where

- (47a) is due to $(\mathbf{Z}^{j-1}K^{j-1}) \multimap (\mathcal{C}\mathbf{U}_j) \multimap (\mathbf{Z}_j^b K_j)$ being a Markov chain since $\mathbf{U}_j$ contains $(L_{1(j-1)}L_{2(j-1)}K'_{j-1})$, see Remark 10; and,
- (47b) is due to $\mathbf{Z}_{j+1}^b \multimap (\mathcal{C}L_{1j}L_{2j}\mathbb{M}'_{1(j+1)}) \multimap (K_j\mathbf{U}_j\mathbf{Z}_j)$.

The first term in (47c) can be bounded from below as follows,

$$\begin{aligned}
&H(\mathbf{X}_j\hat{\mathbf{Y}}_j|\mathcal{C}\mathbf{U}_j\mathbf{T}_j\mathbf{Z}_j L_{2j}\mathbb{M}'_{1(j+1)}) \\
&\quad = H(\mathbf{X}_j\hat{\mathbf{Y}}_j|\mathcal{C}\mathbf{U}_j\mathbf{T}_j\mathbf{Z}_j) - I(\mathbf{X}_j\hat{\mathbf{Y}}_j; L_{2j}|\mathcal{C}\mathbf{U}_j\mathbf{T}_j\mathbf{Z}_j) \\
&\qquad - I(\mathbf{X}_j\hat{\mathbf{Y}}_j; \mathbb{M}'_{1(j+1)}|\mathcal{C}\mathbf{U}_j\mathbf{T}_j\mathbf{Z}_j L_{2j}) \\
&\quad \geq H(\mathbf{X}\hat{\mathbf{Y}}|\mathcal{C}\mathbf{U}\mathbf{T}\mathbf{Z}) - H(L_{2j}) - I(K'_j; \mathbb{M}'_{1(j+1)}) && \text{(48a)} \\
&\quad \geq H(\mathbf{X}\hat{\mathbf{Y}}|\mathcal{C}\mathbf{U}\mathbf{T}\mathbf{Z}) - n\tilde{S}_2 && \text{(48b)} \\
&\quad \geq H(\mathbf{X}\hat{\mathbf{Y}}\mathbf{T}\mathbf{Z}|\mathcal{C}\mathbf{U}) - H(\mathbf{T}\mathbf{Z}|\mathcal{C}\mathbf{U}) - n\tilde{S}_2 \\
&\quad \geq H(\mathbf{X}\hat{\mathbf{Y}}\mathbf{Z}|\mathcal{C}\mathbf{U}) - H(\mathbf{Z}|\mathcal{C}\mathbf{U}) - H(\mathbf{T}|\mathcal{C}\mathbf{U}\mathbf{Z}) - n\tilde{S}_2 \\
&\quad \geq n\big[H(X\hat{Y}|UZ) - \epsilon'\big] - H(\mathbf{T}|\mathcal{C}\mathbf{U}\mathbf{Z}) - n\tilde{S}_2 && \text{(48c)} \\
&\quad \geq n\big[H(X\hat{Y}|UTZ) - \epsilon_1 - \eta - \epsilon' - \tilde{S}_2\big], && \text{(48d)}
\end{aligned}$$

where

- (48a) is due to $\mathbb{M}'_{1(j+1)} \multimap K'_j \multimap (\mathcal{C}\mathbf{U}_j\mathbf{T}_j\mathbf{X}_j\hat{\mathbf{Y}}_j\mathbf{Z}_j L_{2j})$ being a Markov chain, and the block index j in the first term being removed for notational simplicity;
- (48b) is due to $H(L_{2j}) \leq n\tilde{S}_2$, and $H(\mathbb{M}_{1(j+1)} \oplus K'_j) = H(\mathbb{M}_{1(j+1)})$ since $\mathbb{M}_{1(j+1)}$ is uniformly distributed on $[1 : 2^{nR_1}]$ and independent of K'_j;
- (48c) is due to $\mathcal{C} \multimap \mathbf{U} \multimap (\mathbf{X}\hat{\mathbf{Y}}\mathbf{Z})$ being a Markov chain, and $H(\mathbf{X}\hat{\mathbf{Y}}\mathbf{Z}|\mathbf{U}) \geq n\big[H(X\hat{Y}Z|U) - \epsilon'\big]$ for some $\epsilon' > 0$ since all the sequences are jointly typical[1]; and,
- (48d) stems from the following lemma.[2]

Lemma 1: Let $\eta > 0$ and ϵ_1 defined in (42). Then, given the codebook generation and encoding procedure of the scheme,

$$H(\mathbf{T}|\mathcal{C}\mathbf{Q}\mathbf{U}\mathbf{Z}) \leq n\big[I(T; X\hat{Y}|UZ) + \epsilon_1 + \eta\big], \tag{49}$$

for sufficiently large n.

Proof: The proof is found in Appendix E. ∎

On the other hand, the second term in (47c) can be bounded from above as

$$\begin{aligned}
&H(\mathbf{X}\hat{\mathbf{Y}}|\mathcal{C}\mathbf{U}\mathbf{Z}\mathbf{T}L_2K) \\
&\quad = H(\mathbf{X}\hat{\mathbf{Y}}|\mathcal{C}\mathbf{U}\mathbf{Z}\mathbf{T}\mathbf{V}) + I(\mathbf{X}\hat{\mathbf{Y}}; \mathbf{V}|\mathcal{C}\mathbf{U}\mathbf{Z}\mathbf{T}L_2K) \\
&\quad \leq nH(X\hat{Y}|UTVZ) + H(\mathbf{V}|\mathcal{C}\mathbf{U}\mathbf{Z}\mathbf{T}L_2K) \\
&\quad \leq n\big[H(X\hat{Y}|UTVZ) + \epsilon_n\big], && \text{(50)}
\end{aligned}$$

where the last inequality stems from the following lemma.

Lemma 2: Given the codebook generation and encoding procedure of the scheme,

$$H(\mathbf{V}|\mathcal{C}\mathbf{U}\mathbf{Z}\mathbf{T}L_2K) \leq n\epsilon_n, \tag{51}$$

where ϵ_n denotes a sequence such that $\epsilon_n \to 0$ as $n \to \infty$.

Proof: The proof is found in Appendix F. ∎

Therefore, joining (47), (48a), and (50), we obtain

$$\begin{aligned}
H(K^{b-1}|\mathcal{C}\mathbf{Z}^b) &\geq \sum_{j=1}^{b-1} n\big[I(V; X\hat{Y}|UTZ) - \tilde{S}_2 - \epsilon_1 - \eta - \epsilon_n\big] \\
&= \sum_{j=1}^{b-1} n\big[\bar{S}_2 - (\epsilon_1 + \epsilon_2 + \tilde{\epsilon}_2 + \eta + \epsilon_n)\big] \\
&= n(b-1)(\bar{S}_2 - \epsilon), && \text{(52)}
\end{aligned}$$

for some $\epsilon > 0$. Finally,

$$\begin{aligned}
\mathbb{E}[\mathsf{L}_k(\mathcal{C})] &= I(K^{b-1}; \mathbf{Z}^b|\mathcal{C}) \\
&= H(K^{b-1}|\mathcal{C}) - H(K^{b-1}|\mathcal{C}\mathbf{Z}^b) \\
&\leq n(b-1)\bar{S}_2 - n(b-1)(\bar{S}_2 - \epsilon) \\
&= n(b-1)\epsilon,
\end{aligned}$$

and the key is asymptotically secure.

[1] Given the encoding procedure, $\mathbf{X}$ is generated in an i.i.d. fashion given $\mathbf{U}$, and thus $p(\mathbf{x}\hat{\mathbf{y}}\mathbf{z}|\mathbf{u}) = \prod_i p(x_i\hat{y}_i z_i|u_i)$. Although it is not true in general that $p(\hat{\mathbf{y}}\mathbf{z}|\mathbf{x}) = \prod_i p(\hat{y}_i z_i|x_i)$ due to the use of feedback in the encoding procedure, cf. (1), the scheme only correlates *adjacent* transmission blocks. Therefore, *inside* a transmission block, we have a DMC without feedback.

[2] Although $\mathbf{Q}$ is not explicitly denoted in the conditioning of the entropy in (48c), it is assumed to be there hidden behind $\mathbf{U}$.

E. Key Uniformity

The uniformity of the keys is defined in (9). Using (52), we obtain

$$\begin{aligned}\mathbb{E}[\mathsf{U}_k(\mathcal{C})] &= n(b-1)\bar{S}_2 - H(K^{b-1}|\mathcal{C}) \\ &\le n(b-1)\bar{S}_2 - H(K^{b-1}|\mathcal{C}\mathbf{Z}^b) \\ &\le n(b-1)\epsilon,\end{aligned}$$

and thus the key is asymptotically uniform.

F. Information Leakage

We now proceed to bound the information leakage of the $b-1$ messages $\mathbb{M}^b = (\mathbb{M}_0^b, \mathbb{M}_1^b)$. Consider first,

$$\begin{aligned}&I(\mathbb{M}_0^b; \mathbf{Z}^b|\mathcal{C}) \\ &\quad= \sum_{j=2}^{b} I(\mathbb{M}_{0j}; \mathbf{Z}^b|\mathcal{C}\mathbb{M}_0^{j-1}) \\ &\quad\le \sum_{j=2}^{b} I(\mathbb{M}_{0j}; \mathbf{Z}^b\mathbf{T}_j\mathbb{M}_0^{j-1}L_{1(j-1)}L_{2(j-1)}K'_{j-1}|\mathcal{C}) \\ &\quad= \sum_{j=2}^{b}\Big[I(\mathbb{M}_{0j}; \mathbf{Z}_j\mathbf{T}_j|\mathcal{C}L_{1(j-1)}L_{2(j-1)}K'_{j-1}) \\ &\qquad+ I(\mathbb{M}_{0j}; \mathbf{Z}_{j+1}^b|\mathcal{C}\mathbf{Z}_j\mathbf{T}_jL_{1(j-1)}L_{2(j-1)}K'_{j-1})\Big], \qquad (53)\end{aligned}$$

where the last equality is due to $(L_{1(j-1)}L_{2(j-1)}K'_{j-1})$ being independent of $\mathbb{M}_{0j}$ and the Markov chain $(\mathbf{Z}^{j-1}\mathbb{M}_0^{j-1}) \multimap (\mathcal{C}L_{1(j-1)}L_{2(j-1)}K'_{j-1}) \multimap (\mathbb{M}_{0j}\mathbf{Z}_j^b)$, see Remark 10.

The first term on the right-hand side of (53) corresponds to the information leakage in block j of the message $\mathbb{M}_{0j}$ given the indices $(L'_jL''_j)$, which is upper-bounded by $n\eta_1$ thanks to (42f). The conditioning over K'_{j-1} does not affect this term because $\mathbf{Z}_j$ is only correlated to $\mathbb{M}'_{1j} = \mathbb{M}_{1j} \oplus K'_{j-1}$ which is independent of K'_{j-1}, given that $\mathbb{M}_{1j}$ is uniformly distributed on $[1 : 2^{nR_1}]$ and independent of K'_{j-1}.

On the other hand, the second term on the right-hand side of (53) can be bounded as follows

$$\begin{aligned}&I(\mathbb{M}_{0j}; \mathbf{Z}_{j+1}^b|\mathcal{C}\mathbf{Z}_j\mathbf{T}_jL_{1(j-1)}L_{2(j-1)}K'_{j-1}) \\ &\quad\le I(\mathbb{M}_{0j}L_{1(j-1)}L_{2(j-1)}K'_{j-1}\mathbf{Z}_j; \mathbf{Z}_{j+1}^b|\mathcal{C}\mathbf{T}_j) \\ &\quad\le I(\mathbf{U}_j\mathbf{Z}_j; \mathbf{Z}_{j+1}^b|\mathcal{C}\mathbf{T}_j) \qquad (54a) \\ &\quad\le I(\mathbf{U}_j\mathbf{Z}_j; L_{1j}L_{2j}\mathbb{M}'_{1(j+1)}|\mathcal{C}\mathbf{T}_j) \qquad (54b) \\ &\quad= I(\mathbf{U}_j\mathbf{Z}_j; L_{2j}|\mathcal{C}\mathbf{T}_j) + I(\mathbf{U}_j\mathbf{Z}_j; \mathbb{M}'_{1(j+1)}|\mathcal{C}\mathbf{T}_jL_{2j}) \\ &\quad\le I(\mathbf{U}_j\mathbf{Z}_j; L_{2j}|\mathcal{C}\mathbf{T}_j) + I(K'_j; \mathbb{M}'_{1(j+1)}) \qquad (54c) \\ &\quad= I(\mathbf{U}_j\mathbf{Z}_j; L_{2j}|\mathcal{C}\mathbf{T}_j), \qquad (54d)\end{aligned}$$

where

- (54a) is due to $(\mathbb{M}_{0j}L_{1(j-1)}L_{2(j-1)}K'_{j-1}) \multimap (\mathcal{C}\mathbf{U}_j) \multimap (\mathbf{T}_j\mathbf{Z}_j^b)$ being a Markov chain since $\mathbf{U}_j$ hides the indices;
- (54b) is due to $(\mathbf{U}_j\mathbf{T}_j\mathbf{Z}_j) \multimap (\mathcal{C}L_{1j}L_{2j}\mathbb{M}'_{1(j+1)}) \multimap \mathbf{Z}_{j+1}^b$, see Remark 10;
- (54c) is due to the Markov chain $\mathbb{M}'_{1(j+1)} \multimap K'_j \multimap (\mathcal{C}\mathbf{U}_j\mathbf{T}_j\mathbf{Z}_jL_{2j})$; and,
- (54d) is again due to $H(\mathbb{M}_{1(j+1)} \oplus K'_j) = H(\mathbb{M}_{1(j+1)})$.

We proceed to bound (54d), where we remove the block index j for notational simplicity,

$$\begin{aligned}&I(\mathbf{UZ}; L_2|\mathcal{C}\mathbf{T}) \\ &\quad= H(L_2|\mathcal{C}\mathbf{T}) - H(L_2|\mathcal{C}\mathbf{UTZ}) \\ &\quad= H(L_2|\mathcal{C}\mathbf{T}) - H(L_2K\mathbf{V}|\mathcal{C}\mathbf{UTZ}) \\ &\qquad+ H(K|\mathcal{C}\mathbf{UTZ}L_2) + H(\mathbf{V}|\mathcal{C}\mathbf{UTZ}L_2K) \\ &\quad\le n\tilde{S}_2 - H(\mathbf{V}|\mathcal{C}\mathbf{UTZ}) + n\bar{S}_2 + n\epsilon_n, \qquad (55)\end{aligned}$$

where the inequality follows from bounding the indices L_2 and K by their cardinality, and the last entropy by Lemma 2. The remaining entropy may be bounded using the following lemma.

Lemma 3: Let $\eta > 0$ and ϵ_2 defined in (42). Then, given the codebook generation and encoding procedure of the scheme,

$$H(\mathbf{V}|\mathcal{C}\mathbf{UTZ}) \ge n\big[I(V; X\hat{Y}|UTZ) + \epsilon_2 - \eta\big]. \qquad (56)$$

for sufficiently large n.

Proof: The proof is found in Appendix E. ∎

Using the definitions of $\tilde{S}_2$ and $\tilde{S}_2$ from (42), and Lemma 3, we bound (55) as follows

$$I(\mathbf{UZ}; L_2|\mathcal{C}\mathbf{T}) \le n(\tilde{\epsilon}_2 + \epsilon_n + \eta) \triangleq n\eta_2,$$

for some $\eta_2 > 0$, which let us bound (54), and in turn, (53),

$$I(\mathbb{M}_0^b; \mathbf{Z}^b|\mathcal{C}) \le \sum_{j=2}^{b}(n\eta_1 + n\eta_2) \triangleq n(b-1)\eta_3.$$

Now consider,

$$\begin{aligned}&I(\mathbb{M}_1^b; \mathbf{Z}^b|\mathcal{C}\mathbb{M}_0^b) \\ &\quad= \sum_{j=2}^{b} I(\mathbb{M}_{1j}; \mathbf{Z}^b|\mathcal{C}\mathbb{M}_0^b\mathbb{M}_1^{j-1}) \\ &\quad\le \sum_{j=2}^{b} I(\mathbb{M}_{1j}; \mathbf{U}_{j-1}\mathbf{T}_{j-1}^j\mathbf{Z}^b|\mathcal{C}\mathbb{M}_0^b\mathbb{M}_1^{j-1}) \\ &\quad= \sum_{j=2}^{b}\Big[I(\mathbb{M}_{1j}; \mathbf{U}_{j-1}\mathbf{T}_{j-1}\mathbf{Z}^{j-1}|\mathcal{C}\mathbb{M}_0^b\mathbb{M}_1^{j-1}) \\ &\qquad+ I(\mathbb{M}_{1j}; \mathbf{T}_j\mathbf{Z}_j|\mathcal{C}\mathbb{M}_0^b\mathbb{M}_1^{j-1}\mathbf{U}_{j-1}\mathbf{T}_{j-1}\mathbf{Z}^{j-1}) \\ &\qquad+ I(\mathbb{M}_{1j}; \mathbf{Z}_{j+1}^b|\mathcal{C}\mathbb{M}_0^b\mathbb{M}_1^{j-1}\mathbf{U}_{j-1}\mathbf{T}_{j-1}^j\mathbf{Z}^j)\Big]. \qquad (57)\end{aligned}$$

The first term in (57) is zero due to the independence between $(\mathcal{C}\mathbf{U}_{j-1}\mathbf{T}_{j-1}\mathbf{Z}^{j-1}\mathbb{M}_0^b\mathbb{M}_1^{j-1})$ and $\mathbb{M}_{1j}$, while the second term can be bounded as follows

$$\begin{aligned}&I(\mathbb{M}_{1j}; \mathbf{T}_j\mathbf{Z}_j|\mathcal{C}\mathbb{M}_0^b\mathbb{M}_1^{j-1}\mathbf{U}_{j-1}\mathbf{T}_{j-1}\mathbf{Z}^{j-1}) \\ &\quad\le I(\mathbb{M}_{1j}; \mathbb{M}'_{1j}|\mathcal{C}\mathbb{M}_0^b\mathbb{M}_1^{j-1}\mathbf{U}_{j-1}\mathbf{T}_{j-1}\mathbf{Z}^{j-1}) \qquad (58a) \\ &\quad\le I(\mathbb{M}_0^b\mathbb{M}_1^j\mathbf{Z}^{j-2}; \mathbb{M}'_{1j}|\mathcal{C}\mathbf{U}_{j-1}\mathbf{T}_{j-1}\mathbf{Z}_{j-1}) \\ &\quad= I(\mathbb{M}_0^b\mathbb{M}_1^j\mathbf{Z}^{j-2}; K'_{j-1}|\mathcal{C}\mathbf{U}_{j-1}\mathbf{T}_{j-1}\mathbf{Z}_{j-1}) \\ &\qquad+ H(\mathbb{M}'_{1j}|\mathcal{C}\mathbf{U}_{j-1}\mathbf{T}_{j-1}\mathbf{Z}_{j-1}) \\ &\qquad- H(K'_{j-1}|\mathcal{C}\mathbf{U}_{j-1}\mathbf{T}_{j-1}\mathbf{Z}_{j-1}) \\ &\quad\le nR_1 - H(K_{j-1}|\mathcal{C}\mathbf{U}_{j-1}\mathbf{T}_{j-1}\mathbf{Z}_{j-1}) \\ &\qquad+ H(K_{j-1}|\mathcal{C}\mathbf{U}_{j-1}\mathbf{T}_{j-1}\mathbf{Z}_{j-1}K'_{j-1}) \qquad (58b) \\ &\quad\le n\bar{S}_2 - H(K|\mathcal{C}\mathbf{UTZ}), \qquad (58c) \\ &\quad= n\bar{S}_2 - H(KL_2\mathbf{V}|\mathcal{C}\mathbf{UTZ}) + H(L_2|\mathcal{C}\mathbf{UTZ}K) \\ &\qquad+ H(\mathbf{V}|\mathcal{C}\mathbf{UTZ}L_2K)\end{aligned}$$

$$\leq n\big[\bar{S}_2 - I(V; X\hat{Y}|UTZ) - \epsilon_2 + \eta + \tilde{S}_2 + \epsilon_n\big] \quad (58d)$$
$$= n(\bar{\epsilon}_2 + \eta + \epsilon_n), \quad (58e)$$

where

- (58a) is due to $\mathbb{M}_{1j} \multimap \mathbb{M}'_{1j} \multimap (\mathbf{T}_j\mathbf{Z}_j)$ being a Markov chain since $\mathbb{M}'_{1j} = \mathbb{M}_{1j} \oplus K'_{j-1}$;
- (58b) is due to $(\mathbb{M}_0^b\mathbb{M}_1^j\mathbf{Z}^{j-2}) \multimap (\mathcal{C}\mathbf{U}_{j-1}\mathbf{T}_{j-1}\mathbf{Z}_{j-1}) \multimap K'_{j-1}$ being a Markov chain and $H(\mathbb{M}'_{1j}) = nR_1$;
- (58c) is due to $H(K_{j-1}|\mathcal{C}K'_{j-1}) \leq n(\tilde{S}_2 - R_1)$ and the block index j being removed for brevity; and,
- (58d) follows similar steps as (55).

The third term in (57) may be bounded from above as follows

$$\begin{aligned} &I(\mathbb{M}_{1j}; \mathbf{Z}_{j+1}^b|\mathcal{C}\mathbb{M}_0^b\mathbb{M}_1^{j-1}\mathbf{U}_{j-1}\mathbf{T}_{j-1}^j\mathbf{Z}^j) \\ &\quad\leq I(\mathbb{M}_{1j}; L_{1j}L_{2j}\mathbb{M}'_{1(j+1)}|\mathcal{C}\mathbb{M}_0^b\mathbb{M}_1^{j-1}\mathbf{U}_{j-1}\mathbf{T}_{j-1}^j\mathbf{Z}^j) \\ &\quad\leq I(\mathbb{M}_0^b\mathbb{M}_1^j\mathbf{U}_{j-1}\mathbf{T}_{j-1}\mathbf{Z}^j; L_{1j}L_{2j}\mathbb{M}'_{1(j+1)}|\mathcal{C}\mathbf{T}_j) \\ &\quad\leq I(\mathbf{U}_j\mathbf{Z}_j; L_{1j}L_{2j}\mathbb{M}'_{1(j+1)}|\mathcal{C}\mathbf{T}_j) \\ &\quad\leq n\eta_2, \end{aligned}$$

where the last inequality is bounded exactly as (54b). Thus, (57) is upper-bounded as

$$I(\mathbb{M}_1^b; \mathbf{Z}^b|\mathcal{C}\mathbb{M}_0^b) \leq \sum_{j=2}^{b} 2n\eta_2 = 2n(b-1)\eta_2.$$

Finally, the total information leakage is

$$\begin{aligned} \mathbb{E}[\mathsf{L}(\mathcal{C})] &= I(\mathbb{M}_0^b\mathbb{M}_1^b; \mathbf{Z}^b|\mathcal{C}) \\ &= I(\mathbb{M}_0^b; \mathbf{Z}^b|\mathcal{C}) + I(\mathbb{M}_1^b; \mathbf{Z}^b|\mathcal{C}\mathbb{M}_0^b) \\ &\leq n(b-1)(2\eta_2 + \eta_3), \end{aligned}$$

which assures that the eavesdropper has negligible knowledge of the messages asymptotically.

G. Sufficient Conditions (R_{KG_1})

Putting all the pieces together, we have proved that the proposed scheme allows the encoder to transmit a message uniformly distributed in $[1 : 2^{nR}]$, $R = R_{KG_1} = R_0 + R_1$, while keeping it secret from the eavesdropper if

$$\begin{aligned} I(V; Z|UT) &\leq I(V; Y|UT), \\ \tilde{S}' + \tilde{S}'' = \tilde{S}_1 + \tilde{S}_2 &= I(V; X\hat{Y}|UY) + \epsilon_{12}, \\ R_1 \leq \bar{S}_2 &= I(V; Y|UT) - I(V; Z|UT), \\ \tilde{S}'' + R_0 + R_1 + R_f &< I(U; Y|Q) - \delta, \\ \tilde{S}' + \tilde{S}'' + R_0 + R_1 + R_f &< I(U; Y) - \delta, \\ R_1 + R_f &= I(U; Z|Q) + I(U; T|QZ) - \epsilon', \end{aligned}$$

where $\epsilon_{12} = \epsilon_1 + \epsilon_2 + \tilde{\epsilon}_1 + \tilde{\epsilon}_2$. After applying Fourier-Motzkin elimination, we obtain the bounds in (13) subject to

$$I(V; Z|UT) \leq I(V; Y|UT), \quad (59a)$$
$$I(U; TZ|Q) \leq I(U; Y|Q), \quad (59b)$$
$$I(V; X\hat{Y}|UY) + I(U; TZ|Q) \leq I(U; Y). \quad (59c)$$

Nonetheless, these conditions are redundant after the maximization process. If for a certain PD, condition (59a) is not satisfied, then, R_{KG_1} with $T = V = \emptyset$ attains a higher value. Similarly, if either (59b) or (59c) does not hold for a certain PD, then, R_{KG_2} with $Q = \emptyset$ attains a higher value.

We have shown thus far that, *averaged* over all possible codebooks, the probability of error, the key leakage and (non-)uniformity, and the information leakage rate become negligible as $(n, b) \to \infty$ if conditions (13) hold true. Nonetheless, by applying the selection lemma [39, Lemma 2.2], we may conclude that there exists a *specific* sequence of codebooks such that the probability of error, the key leakage and (non-)uniformity, and the information leakage rate tend to zero as $(n, b) \to \infty$.

The bounds on the cardinality of the alphabets $\mathcal{Q}$, $\mathcal{U}$, $\mathcal{T}$, and $\mathcal{V}$ follow from Fenchel–Eggleston–Carathéodory's theorem and the standard cardinality bounding technique [34, Appendix C]; therefore their proof is omitted.

H. Achievable Rate R_{KG_2}

The second strategy tackles the situation where the eavesdropper experiences a better channel than the legitimate receiver and can therefore decode everything sent by the encoder. In R_{KG_1}, when either the condition (59b) or (59c) is not satisfied, the rate of the unencrypted message (R_0) is negative. Therefore, in this second strategy the message is encrypted completely. The proof is similar to the one of R_{KG_1} and we only point out the differences in what follows.

1) Codebook Generation: Since the eavesdropper is able to decode everything, there is no need for the codeword $\mathbf{q}(\cdot)$ as a lower layer for $\mathbf{u}(\cdot)$, which in turn makes the bit recombination $(l'_j, l''_j) = M_l(l_{1(j-1)}, l_{2(j-1)})$ unnecessary. Additionally, since the encoder cannot send the message without encrypting it, $R_0 = 0$ and $R_f = 0$, and the condition (42f) disappears. We therefore take the joint distribution (15) with $Q = \emptyset$ and build the codebooks for each block as in Appendix A-A without $\mathbf{q}(\cdot)$ and with $\mathbf{t}(\cdot)$ superimposed over $\mathbf{u}(\cdot)$. The quantities (42) are modified as follows:

$$\begin{aligned} S_1 &= I(T; X\hat{Y}|U) + \epsilon_1, \\ \tilde{S}_1 &= I(T; X\hat{Y}|U) - I(T; Y|U) + \epsilon_1 + \tilde{\epsilon}_1. \end{aligned}$$

2) Encoding and Decoding: These steps are analogous to the previous proof with two main differences. First, there is no bit recombination in the transmission of the bin indices. Second, the encoder only sends an encrypted message $m'_j = m_j \oplus k'_{j-1}$ using the key obtained from the feedback of the previous block. Briefly, if $\mathbf{t}(\underline{r}_{j-1}, s_{1(j-1)}) \in B_1(l_{1(j-1)})$ and $\mathbf{v}(\underline{r}_{j-1}, s_{1(j-1)}, s_{2(j-1)}) \in \bar{B}_2(s_{1(j-1)}, l_{2(j-1)}, k_{j-1})$, the encoder sends $\mathbf{u}(l_{1(j-1)}, l_{2(j-1)}, m'_j) = \mathbf{u}(\underline{r}_j)$ during block j.

3) Key and Information Leakage: The proof for the key secrecy and uniformity is the same while the one for the information leakage is simplified. Since there is no unencrypted message, i.e., $R_0 = 0$ the bounding of $I(\mathbb{M}_0^b; \mathbf{Z}^b|\mathcal{C})$ becomes trivial and the condition (42f) is no longer necessary.

4) Final Expression: The sufficient conditions in this second strategy for the encoder to transmit a message uniformly distributed in $[1 : 2^{nR}]$, $R = R_{KG_2}$, while keeping it secret

from the eavesdropper are given by

$$I(V;Z|UT) \le I(V;Y|UT), \tag{60a}$$
$$\tilde{S}_1 + \tilde{S}_2 = I(V;X\hat{Y}|UY) + \epsilon_1 + \epsilon_2 + \tilde{\epsilon}_1 + \tilde{\epsilon}_2, \tag{60b}$$
$$R \le \bar{S}_2 = I(V;Y|UT) - I(V;Z|UT), \tag{60c}$$
$$\tilde{S}_1 + \tilde{S}_2 + R < I(U;Y) - \delta, \tag{60d}$$

which yields (14) after applying Fourier Motzkin elimination.

I. Final Remarks

The preceding proof guarantees that there exists a specific $(2^{nR}, n)$ code $\mathtt{c}_n$ whose rate is achievable under the *weak secrecy* condition (5). Nevertheless, using the method proposed in [35], we can show that the achievable secrecy rate also complies with the *strong secrecy* condition (6). In the sequel, we show how this is achieved following [39, Proposition 4.10].

Let $\epsilon > 0$ and consider a code $\mathtt{c}_n$ with rate

$$R = \max\left\{\max_{p\in\mathcal{P}_{I_1}} R_{KG_1}(p),\ \max_{p'\in\mathcal{P}_{I_2}} R_{KG_2}(p')\right\} - \epsilon, \tag{61}$$

where the definitions for the rates are found in (13) and (14), such that condition (5) holds. The encoder then uses this code m times[3] to transmit m independent messages. In each transmission $i \in [1:m]$, the encoder transmits $\mathbb{M}_i$, the decoder obtains $\hat{\mathbb{M}}_i$, and the eavesdropper observes $\mathbf{Z}_i$. This situation is akin to the "source model" in the problem of secret key generation where the encoder, the decoder, and the eavesdropper observe m realizations of the random variables

$$X' \triangleq \mathbb{M}, \quad Y' \triangleq \hat{\mathbb{M}}, \quad \text{and} \quad Z' \triangleq \mathbf{Z}, \tag{62}$$

respectively. According to [39, Th. 4.7] and for some $\epsilon' > 0$, the legitimate users can agree on a strong secret key $\bar{K}$ of length

$$k = m\big[I(X';Y') - I(X';Z') - \epsilon'\big] \ge mn(R - \epsilon''),$$

where the inequality follows, for some $\epsilon'' > 0$, from the definitions in (62), the condition (5), and the fact that the rate of $\mathbb{M}$ is determined by (61).

The strong secret key $\bar{K}$ is obtained by means of a one-way direct reconciliation protocol and privacy amplification with extractors. These two steps involve the transmission of additional information through the channel; in particular, the one-way reconciliation protocol needs $m[H(X'|Y') + \delta]$ bits of communication and the privacy amplification, $m\delta'$ bits, for some $\delta, \delta' > 0$. Nonetheless, these additional m' channel uses are negligible compared to the total transmission time for large m and n, i.e., $m' \le mn\delta''$, for some small $\delta'' > 0$; thus, the rate of the strong secret key $\bar{K}$ is bounded from below as

$$\frac{k}{mn + m'} \ge R - \bar{\epsilon},$$

for some $\bar{\epsilon} > 0$. We refer the reader to [39, Sec. 4.5] for the details.

Lastly, it remains to be seen if the secret key $\bar{K}$ can be interpreted as a message. Given that all the transmissions are one-way, it is possible for the encoder to choose the key $\bar{K}$ ahead of time and "invert" the reconciliation and privacy amplification processes; the encoder then obtains the m messages to transmit using the weak code $\mathtt{c}_n$. Therefore, the final strong secret-key $\bar{K}$ can be treated as a message $\mathbb{M}$ that satisfies the strong secrecy condition (6). This concludes the proof of Theorem 1. ■

APPENDIX B
PROOF OF THEOREM 2 (SK RATE LOWER BOUND)

In this scheme, the encoder is not interested in transmitting a message but rather agreeing on a secret key with the legitimate receiver. As in the proof of Theorem 1, the encoder splits the transmission in b blocks of n channel uses and employs one of two available strategies to generate the shared secret key.

In the first strategy, the secret key has two components: one is sent over the channel and is kept secret from the eavesdropper by using Wyner's wiretap coding scheme, while the second component is generated thanks to the correlation between the outputs Y and $\hat{Y}$. On the other hand, the second strategy generates a secret key only relying on the correlation between the channel outputs.

In the following, we present a brief sketch of the proof for both strategies given the similarities with respect to the proof of Theorem 1 in Appendix A. Consequently, the secret key rate is achievable according to the weak secrecy condition (10) but we show at the end of this Appendix that the strong secrecy condition (11) also holds true.

A. First Strategy

This part follows the same steps as the proof of the achievable secrecy rate R_{KG_1}, found in Appendix A, but without the transmission of an encrypted message. Thus, at the end of the b transmission blocks, the encoder and the legitimate receiver will agree with high probability on a key of rate $\frac{b-1}{b}R_k$. Due to the similarity with the proof of R_{KG_1}, we only point out the differences in the sequel.

1) Codebook Generation: The codebook is generated in the same way as for the achievable rate R_{KG_1}, with the exception of the codeword $\mathbf{u}(\cdot)$. Specifically, the message m_0 carried by that scheme becomes a part of the secret key here, i.e., $R_0 = R_{k0}$, and the key generated through the feedback link is not used to encrypt a message but rather becomes the second part of the secret key, i.e., $R_1 = 0$, $R_{k1} = \bar{S}_2$, and $R_f = I(U;TZ|Q) - \epsilon'$ replaces (42f).

Step 2 in Appendix A-A thus becomes:

2) For each $\mathbf{q}(l')$, randomly pick $2^{n(\tilde{S}'' + R_{k0} + R_f)}$ sequences $\mathbf{u}(\underline{r}) \equiv \mathbf{u}(l', l'', k_0, l_f)$, where $l'' \in [1 : 2^{n\tilde{S}''}]$, $k_0 \in [1 : 2^{nR_{k0}}]$, and $l_f \in [1 : 2^{nR_f}]$, from $\mathcal{T}_\delta^n(U|\mathbf{q}(l'))$.

2) Encoding and Decoding: These steps are similar to the ones for the achievable rate R_{KG_1} but no message is transmitted. In each block $j \in [2 : b]$, the encoder chooses

[3]The proof of the scheme is based on splitting the transmission in b blocks of n channel uses; thus, the whole weakly secret transmission takes place in nb channel uses. To simplify the presentation of this part, we consider that a weakly secret transmission, i.e., each of the m times the code $\mathtt{c}_n$ is employed, takes place in n channel uses.

uniformly at random a key index $k_{0j} \in [1 : 2^{nR_{k0}}]$ and a noise index $l_{fj} \in [1 : 2^{nR_f}]$. It then sends these indices, along with the bin indices (l'_j, l''_j) of the description of the previous block's feedback sequence, through the codeword $\mathbf{u}(l'_j, l''_j, k_{0j}, l_{fj}) = \mathbf{u}(\underline{r}_j)$.

3) Key and Information Leakage: The proof for the key leakage of the achievable rate R_{KG_1} assures that the part of the key that is created using the description, i.e., k_1, is kept secret from the eavesdropper, while the proof of the information leakage guarantees that the part that is sent through the codeword $\mathbf{u}(\underline{r})$, i.e., k_0, is also secure. Both proofs get simplified since k_1 is not used to encrypt a message, and, therefore, it is not transmitted. Remark 10 should now state that only the variables L_{1j} and L_{2j} are responsible for the correlation between blocks.

4) Key Uniformity: The encoding procedure states that the first part of the key, i.e., k_0, is chosen uniformly at random, while the proof of the key uniformity of the achievable rate R_{KG_1} assures that the other part, i.e., k_1, is asymptotically uniform.

5) Final Expression: The sufficient conditions in this first strategy, which allows the legitimate users to agree upon a key uniformly distributed in $[1 : 2^{nR_k}]$, $R_k = R_{k0} + R_{k1}$, while keeping it secret from the eavesdropper, are

$$\begin{aligned} I(V;Z|UT) &\le I(V;Y|UT), \\ \tilde{S}' + \tilde{S}'' = \tilde{S}_1 + \tilde{S}_2 &= I(V;X\hat{Y}|UY) + \epsilon_1 + \epsilon_2 + \tilde{\epsilon}_1 + \tilde{\epsilon}_2, \\ R_{k1} \le \bar{S}_2 &= I(V;Y|UT) - I(V;Z|UT), \\ \tilde{S}'' + R_{k0} + R_f &< I(U;Y|Q) - \delta, \\ \tilde{S}' + \tilde{S}'' + R_{k0} + R_f &< I(U;Y) - \delta, \\ R_f &= I(U;Z|Q) + I(U;T|QZ) - \epsilon'. \end{aligned}$$

After applying Fourier Motzkin elimination to this set of inequalities, we obtain

$$\begin{aligned} R_k \le\ & I(U;Y) - I(U;Z|Q) + I(V;Y|UT) - I(V;Z|UT) \\ & - I(U;T|QZ) - \max\{I(Q;Y), I(V;X\hat{Y}|UY)\}, \end{aligned} \tag{63}$$

subject to the conditions (59). However, these conditions are redundant after the maximization process as in R_{KG_1}.

B. Second Strategy

This part is derived from the achievable rate R_{KG_2}, where we are only interested in generating a secret key, i.e., $R_k \le \bar{S}_2$. As before, the encoder does not transmit an encrypted message, i.e., $R = 0$, and the codeword $\mathbf{u}(\cdot)$ is modified accordingly. Refer to Appendix A-H for details.

The sufficient conditions in this second strategy are derived from (60):

$$\begin{aligned} I(V;Z|UT) &\le I(V;Y|UT), \\ \tilde{S}_1 + \tilde{S}_2 &= I(V;X\hat{Y}|UY) + \epsilon_1 + \epsilon_2 + \tilde{\epsilon}_1 + \tilde{\epsilon}_2, \\ R_k \le \bar{S}_2 &= I(V;Y|UT) - I(V;Z|UT), \\ \tilde{S}_1 + \tilde{S}_2 &< I(U;Y) - \delta. \end{aligned}$$

After applying Fourier Motzkin elimination to this system, we obtain

$$R_k \le I(V;Y|UT) - I(V;Z|UT) \tag{64}$$

subject to the condition

$$I(V;X\hat{Y}|UY) \le I(U;Y). \tag{65}$$

C. Final Remarks

The final achievable secret key rate R_k, which is the union of (63) and (64) conditioned on (65) and maximized over all possible joint PDs, can be succinctly written as (17) and (18). As in the proof of Theorem 1, the preceding rate was shown to be achievable under the *weak secrecy* condition (10). Nonetheless, following the same procedure as in Appendix A-I, we can show that said rate is also achievable under the *strong secrecy* condition (11).

In short, the encoder employs the previously described SK code $\mathtt{c}_n$ m times and the legitimate users agree on m weakly secure keys. These keys may be considered as m observations of correlated sources and, similarly to [39, Proposition 4.10], they may be further distilled to obtain a strong secret key by means of information reconciliation and privacy amplification with extractors. The proof is a simplified version of the one presented in Appendix A-I, and thus we omit it here. The main difference is the absence of a transmitted message, which eliminates the need to "invert" the reconciliation and privacy amplification processes. This concludes the proof of Theorem 2. ∎

Appendix C
Proof of Theorem 3 (Secrecy Rate Upper Bound)

Let R be an achievable strong secrecy rate according to Definition 2 with the appropriate modifications for the model with parallel sources. Then, for $\epsilon > 0$ and sufficiently large n, there exist functions $\mathrm{enc}_i(\cdot)$ and $\mathrm{dec}(\cdot)$ such that

$$X_{ci} = \mathrm{enc}_i(\mathbb{M}_n, R_r, \hat{Y}_s^{i-1}), \tag{66a}$$

$$\hat{\mathbb{M}}_n = \mathrm{dec}(Y_s^n, Y_c^n), \tag{66b}$$

which verify

$$\Pr\{\hat{\mathbb{M}}_n \ne \mathbb{M}_n\} \le \epsilon, \tag{67}$$

$$I(\mathbb{M}_n; Z_s^n Z_c^n) \le \epsilon, \tag{68}$$

where we have dropped the conditioning on the codebook $\mathtt{c}_n$ from (68) and all subsequent calculations for clarity.

First consider,

$$\begin{aligned} nR &= H(\mathbb{M}_n) \\ &= H(\mathbb{M}_n|Z_s^n Y_c^n) + I(\mathbb{M}_n; Z_s^n Y_c^n) \\ &\le H(\mathbb{M}_n|Z_s^n Y_c^n) + I(\mathbb{M}_n; Z_s^n Y_c^n) - I(\mathbb{M}_n; Z_s^n Z_c^n) + \epsilon \qquad (69a) \\ &= H(\mathbb{M}_n|Z_s^n Y_c^n) + I(\mathbb{M}_n; Y_c^n|Z_s^n) - I(\mathbb{M}_n; Z_c^n|Z_s^n) + \epsilon \\ &\le H(\mathbb{M}_n|Z_s^n Y_c^n) - H(\mathbb{M}_n|Y_s^n Y_c^n) \\ &\quad + I(\mathbb{M}_n; Y_c^n|Z_s^n) - I(\mathbb{M}_n; Z_c^n|Z_s^n) + n\epsilon_n \qquad (69b) \end{aligned}$$

$$= \underbrace{I(\mathbb{M}_n; Y_s^n|Y_c^n) - I(\mathbb{M}_n; Z_s^n|Y_c^n)}_{R_s} + \underbrace{I(\mathbb{M}_n; Y_c^n|Z_s^n) - I(\mathbb{M}_n; Z_c^n|Z_s^n)}_{R_c} + n\epsilon_n, \tag{69c}$$

where

- (69a) is due to the security condition (68); and,
- (69b) follows from (66), (67), and Fano's inequality, $H(\mathbb{M}_n|Y_s^n Y_c^n) \le n\epsilon_n'$.

We now study separately the "source" term R_s and the "channel" term R_c.

$$\begin{aligned} R_s &= \sum_{i=1}^n I(\mathbb{M}_n; Y_{si}|Y_c^n Y_s^{i-1}) - I(\mathbb{M}_n; Z_{si}|Y_c^n Z_{s(i+1)}^n) \\ &= \sum_{i=1}^n I(\mathbb{M}_n; Y_{si}|Y_c^n Y_s^{i-1} Z_{s(i+1)}^n) \\ &\quad - I(\mathbb{M}_n; Z_{si}|Y_c^n Y_s^{i-1} Z_{s(i+1)}^n) && (70a) \\ &= \sum_{i=1}^n I(V_i; Y_{si}|T_i) - I(V_i; Z_{si}|T_i) && (70b) \\ &= n\big[I(V_J; Y_{sJ}|T_J J) - I(V_J; Z_{sJ}|T_J J)\big] && (70c) \\ &= n\big[I(V; Y_s|T) - I(V; Z_s|T)\big], && (70d) \end{aligned}$$

where

- (70a) is due to Csiszár sum identity;
- (70b) stems from the definition of the auxiliary RVs $T_i = (Y_c^n Y_s^{i-1} Z_{s(i+1)}^n)$ and $V_i = (\mathbb{M}_n T_i)$;
- in (70c) we add the auxiliary RV J uniformly distributed on $[1:n]$ and independent of all the other variables; and,
- (70d) follows from the definition of random variables $T = (T_J J)$, $V = (V_J J)$, $Y_s = Y_{sJ}$, and $Z_s = Z_{sJ}$.

This establishes the "source" term in (69c) with auxiliary RVs (TV) that satisfy the following Markov chain

$$T_i \multimap V_i \multimap \hat{Y}_{si} \multimap (Y_{si} Z_{si}). \tag{71}$$

The first part of (71) is trivial given the definition $V_i = (\mathbb{M}_n T_i)$, whereas the second part follows from the i.i.d. nature of the sources and that they are correlated to the main channel only through the encoder's input (66a),

$$(\mathbb{M}_n Y_c^n Y_s^{i-1} Z_{s(i+1)}^n) \multimap \hat{Y}_{si} \multimap (Y_{si} Z_{si}).$$

The "channel" term R_c can be single-letterized similarly,

$$\begin{aligned} R_c &= \sum_{i=1}^n I(\mathbb{M}_n; Y_{ci}|Z_s^n Y_c^{i-1}) - I(\mathbb{M}_n; Z_{ci}|Z_s^n Z_{c(i+1)}^n) \\ &= \sum_{i=1}^n I(\mathbb{M}_n; Y_{ci}|Z_s^n Y_c^{i-1} Z_{c(i+1)}^n) \\ &\quad - I(\mathbb{M}_n; Z_{ci}|Z_s^n Y_c^{i-1} Z_{c(i+1)}^n) && (72a) \\ &= \sum_{i=1}^n I(U_i; Y_{ci}|Q_i) - I(U_i; Z_{ci}|Q_i) && (72b) \\ &= n\big[I(U_L; Y_{cL}|Q_L L) - I(U_L; Z_{cL}|Q_L L)\big] && (72c) \\ &= n\big[I(U; Y_c|Q) - I(U; Z_c|Q)\big], && (72d) \end{aligned}$$

where

- (72a) is due to Csiszár sum identity;
- (72b) stems from the definition of the auxiliary RVs $Q_i = (Z_s^n Y_c^{i-1} Z_{c(i+1)}^n)$ and $U_i = (\mathbb{M}_n Q_i)$;
- in (72c) we add the auxiliary RV L uniformly distributed on $[1:n]$ and independent of all the other variables; and,
- (72d) follows from the definition of random variables $Q = (Q_L L)$, $U = (U_L L)$, $Y_c = Y_{cL}$, and $Z_c = Z_{cL}$.

The auxiliary RVs in this term, i.e., (QU), satisfy the following Markov chain

$$Q_i \multimap U_i \multimap X_{ci} \multimap (Y_{ci} Z_{ci}),$$

where the nontrivial part is due to the memorylessness property of the channel and (66a). Since neither Q nor U appear on other parts of the upper bound, we may expand R_c as

$$\begin{aligned} R_c &= n \sum_{q\in\mathcal{Q}} p_Q(q)\big[I(U; Y_c|Q=q) - I(U; Z_c|Q=q)\big] \\ &\le n \max_{q\in\mathcal{Q}} \big[I(U; Y_c|Q=q) - I(U; Z_c|Q=q)\big] \\ &= n\big[I(U^\star; Y_c) - I(U^\star; Z_c)\big], \end{aligned} \tag{73}$$

where in the last step we set the auxiliary RV $U^\star \sim p_{U|Q}(\cdot|q)$ with the specific q that maximizes the preceding expression.

Putting (69), (70), and (73) together, letting $n \to \infty$, and taking arbitrarily small ϵ_n, we obtain the bound (20a).

In order to obtain (20b), consider the following,

$$\begin{aligned} &n(R-\epsilon_n) \\ &\quad \le I(\mathbb{M}_n; Y_s^n Y_c^n) && (74a) \\ &\quad = I(\mathbb{M}_n; \hat{Y}_s^n Y_s^n Y_c^n) - I(\mathbb{M}_n; \hat{Y}_s^n|Y_s^n Y_c^n) \\ &\quad = I(\mathbb{M}_n; Y_c^n|\hat{Y}_s^n) - I(\mathbb{M}_n; \hat{Y}_s^n|Y_s^n Y_c^n) && (74b) \\ &\quad = I(\mathbb{M}_n \hat{Y}_s^n; Y_c^n) - I(\hat{Y}_s^n; Y_c^n) - I(\mathbb{M}_n; \hat{Y}_s^n|Y_s^n Y_c^n) \\ &\quad \le I(\mathbb{M}_n \hat{Y}_s^n; Y_c^n) - I(\hat{Y}_s^n; Y_c^n|Y_s^n) - I(\mathbb{M}_n; \hat{Y}_s^n|Y_s^n Y_c^n) && (74c) \\ &\quad = I(\mathbb{M}_n \hat{Y}_s^n; Y_c^n) - I(\mathbb{M}_n Y_c^n; \hat{Y}_s^n|Y_s^n) \\ &\quad \le I(X_c^n; Y_c^n) - I(\mathbb{M}_n Y_c^n; \hat{Y}_s^n|Y_s^n) && (74d) \\ &\quad \le nI(X_c; Y_c) - I(\mathbb{M}_n Y_c^n; \hat{Y}_s^n|Y_s^n), && (74e) \end{aligned}$$

where

- (74a) stems from Fano's inequality;
- (74b) and (74c) follow from $\hat{Y}_s^n$ being independent of $\mathbb{M}_n$ and the Markov chain $Y_s^n \multimap \hat{Y}_s^n \multimap (\mathbb{M}_n Y_c^n)$;
- (74d) stems from the encoding procedure (66a); and,
- (74e) is due to the channel being memoryless.

The second term in (74e) can be lower-bounded as follows,

$$\begin{aligned} &I(\mathbb{M}_n Y_c^n; \hat{Y}_s^n|Y_s^n) \\ &\quad = I(\mathbb{M}_n Y_c^n; \hat{Y}_s^n Z_s^n|Y_s^n) && (75a) \\ &\quad = \sum_{i=1}^n I(\mathbb{M}_n Y_c^n; \hat{Y}_{si} Z_{si}|Y_s^n \hat{Y}_{s(i+1)}^n Z_{s(i+1)}^n) \\ &\quad \ge \sum_{i=1}^n I(\mathbb{M}_n Y_c^n Y_s^{i-1} Z_{s(i+1)}^n; \hat{Y}_{si} Z_{si}|Y_{si}) && (75b) \\ &\quad = \sum_{i=1}^n I(V_i; \hat{Y}_{si} Z_{si}|Y_{si}) && (75c) \\ &\quad \ge \sum_{i=1}^n I(V_i; \hat{Y}_{si}|Y_{si}) \\ &\quad = nI(V_J; \hat{Y}_{sJ}|Y_{sJ} J) && (75d) \\ &\quad = nI(V_J J; \hat{Y}_{sJ}|Y_{sJ}) && (75e) \\ &\quad = nI(V; \hat{Y}_s|Y_s), && (75f) \end{aligned}$$

where

- (75a) is due to $Z_s^n \multimap (Y_s^n \hat{Y}_s^n) \multimap (\mathbb{M}_n Y_c^n)$;
- (75b) follows from the sources being i.i.d., i.e., $(\hat{Y}_{si} Z_{si}) \multimap Y_{si} \multimap (Y_s^{i-1} Y_{s(i+1)}^n \hat{Y}_{s(i+1)}^n Z_{s(i+1)}^n)$;

- in (75c) we introduce the auxiliary RV V_i, see (70b);
- in (75d) we introduce the auxiliary RV J, see (70c);
- (75e) is due to the independence of J and $(\hat{Y}_{sJ}Y_{sJ})$; and,
- (75f) stems from the definition of random variables $V = (V_J J)$, $Y_s = Y_{sJ}$, and $\hat{Y}_s = \hat{Y}_{sJ}$.

Putting (74) and (75) together, letting $n \to \infty$, and taking an arbitrarily small ϵ_n, we obtain the bound (20b).

Although the definition of the auxiliary RVs (UTV) used in the proof makes them arbitrarily correlated, the bound (20) only depends on the *marginal* PDs $p(ux_c)$ and $p(tv|\hat{y}_s)$. Consequently, we can restrict the set of possible joint PDs to (21), i.e., independent source and channel variables, and still achieve the maximum.

The bound on the cardinality of the alphabets $\mathcal{U}$, $\mathcal{T}$, and $\mathcal{V}$ follow from Fenchel–Eggleston–Carathéodory's theorem and the standard cardinality bounding technique [34, Appendix C]; therefore their proof is omitted. This concludes the proof of Theorem 3. ∎

Appendix D
Proof of Theorem 4 (SK Rate Upper Bound)

Let R_k be an achievable strong secret key rate according to Definition 5. Then, for $\epsilon > 0$ and sufficiently large n, there exist functions $\varphi_i(\cdot)$, $\psi_a(\cdot)$, and $\psi_b(\cdot)$ such that

$$X_{ci} = \varphi_i(R_r, \hat{Y}_s^{i-1}), \tag{76a}$$
$$K_n = \psi_a(R_r, \hat{Y}_s^n), \tag{76b}$$
$$\hat{K}_n = \psi_b(Y_s^n, Y_c^n), \tag{76c}$$

which verify

$$\Pr\{\hat{K}_n \neq K_n\} \leq \epsilon, \tag{77}$$
$$I(K_n; Z_s^n Z_c^n) \leq \epsilon, \tag{78}$$
$$nR_k - H(K_n) \leq \epsilon, \tag{79}$$

where we have dropped the conditioning on the codebook $\mathtt{c}_n$ from (78), (79), and all subsequent calculations for clarity.

This proof follows similar steps as the proof presented in Appendix C, thus we only point out the differences. First consider,

$$\begin{aligned} nR_k &\leq H(K_n) + \epsilon \\ &\leq I(K_n; Y_s^n|Y_c^n) - I(K_n; Z_s^n|Y_c^n) + I(K_n; Y_c^n|Z_s^n) \\ &\quad - I(K_n; Z_c^n|Z_s^n) + n\epsilon_n \qquad (80a) \\ &\leq n\big[I(V; Y_s|T) - I(V; Z_s|T) + I(U; Y_c) \\ &\quad - I(U; Z_c) + \epsilon_n\big], \qquad (80b) \end{aligned}$$

where

- (80a) is obtained using similar steps as those in (69); and,
- (80b) arises from the same procedure as in (70), (72), and (73) but with K_n instead of $\mathbb{M}_n$.

Letting $n \to \infty$, and taking arbitrarily small ϵ_n, we obtain the bound (22).

In order to obtain (23), we use the following Markov chain that is a consequence of (76a),

$$(Y_s^n Z_s^n) \multimap \hat{Y}_s^n \multimap X_c^n \multimap (Y_c^n Z_c^n). \tag{81}$$

Due to the data processing inequality, we have

$$I(\hat{Y}_s^n; Y_c^n) \leq I(X_c^n; Y_c^n) \leq nI(X_c; Y_c), \tag{82}$$

where the last inequality is due to the memorylessness property of the channel. Next consider,

$$\begin{aligned} I(\hat{Y}_s^n; Y_c^n) &= I(\hat{Y}_s^n Y_s^n; Y_c^n) \qquad (83a) \\ &\geq I(\hat{Y}_s^n; Y_c^n|Y_s^n) \\ &= I(\hat{Y}_s^n; K_n Y_c^n|Y_s^n) - I(\hat{Y}_s^n; K_n|Y_s^n Y_c^n) \\ &\geq I(\hat{Y}_s^n; K_n Y_c^n|Y_s^n) - n\epsilon_n \qquad (83b) \\ &\geq n\big[I(\hat{Y}_s; V|Y_s) - \epsilon_n\big], \qquad (83c) \end{aligned}$$

where

- (83a) follows from the Markov chain (81);
- (83b) stems from $H(K_n|Y_s^n Y_c^n) \leq n\epsilon_n$ due to (76), (77), and Fano's inequality, and $H(K_n|Y_s^n Y_c^n \hat{Y}_s^n) \geq 0$ since K_n is a discrete RV; and,
- (83c) is obtained using similar steps as those in (75) with the proper definition for the auxiliary RV V.

Putting (82) and (83) together, letting $n \to \infty$, and taking an arbitrarily small ϵ_n, we obtain the bound (23).

As in the proof of Theorem 3, we can restrict the cardinality of the auxiliary RVs and the set of possible joint PDs to (21), i.e., independent source and channel variables, and still achieve the maximum. This concludes the proof of Theorem 4. ∎

Appendix E
Proof of Lemmas 1 and 3

The proof of Lemmas 1 and 3 are similar, and thus we only present the first one in detail. The specific differences in the proof of Lemma 3 are shown later in Appendix E-B.

A. Proof of Lemma 1

The proof of this lemma follows largely from the proofs of [34, Lemma 22.2] and [39, Lemma 4.1]. Unlike those proofs, however, we analyze here the behavior of the codeword $\mathbf{T}_j$ rather than the bin index associated to a source sequence. In the sequel, we remove the block index j to improve clarity in the presentation.

Let us first introduce the random variable Υ, such that

$$\Upsilon \triangleq \mathbb{1}\Big\{(\mathbf{Q}, \mathbf{U}, \mathbf{X}, \hat{\mathbf{Y}}, \mathbf{Z}) \in \mathcal{T}_\delta^n(QUX\hat{Y}Z)\Big\}.$$

Given the random codebook $\mathcal{C}$, the randomness in the codeword $\mathbf{T}$ comes from its index S. Then, using the binary variable Υ, it follows that,

$$\begin{aligned} H(\mathbf{T}|\mathcal{C}\mathbf{Q}\mathbf{U}\mathbf{Z}) &= H(S|\mathcal{C}\mathbf{Q}\mathbf{U}\mathbf{Z}) \\ &\leq 1 + H(S|\mathcal{C}\mathbf{Q}\mathbf{U}\mathbf{Z}\Upsilon) \\ &\leq 1 + H(S|\mathcal{C}\mathbf{Q}\mathbf{U}\mathbf{Z}, \Upsilon = 1) + nS_1\epsilon', \qquad (84) \end{aligned}$$

where the last inequality is due to $\Pr\{\Upsilon = 0\} \leq \epsilon'$.

Now, for a specific codebook $\mathcal{C} = \mathtt{c}_n$ (which determines the codewords $\mathbf{Q} = \mathbf{q}$ and $\mathbf{U} = \mathbf{u}$) and a sequence $\mathbf{Z} = \mathbf{z}$, let us define the random variable S_c with distribution

$$p_{S_c} \triangleq p_{S|\mathcal{C}=\mathtt{c}_n, \mathbf{Q}=\mathbf{q}, \mathbf{U}=\mathbf{u}, \mathbf{Z}=\mathbf{z}, \Upsilon=1}.$$

Therefore,

$$H(S_c) = H(S|\mathcal{C} = \mathtt{c}_n, \mathbf{Q} = \mathbf{q}, \mathbf{U} = \mathbf{u}, \mathbf{Z} = \mathbf{z}, \Upsilon = 1). \quad (85)$$

Before proceeding, we note that although $S \in [1 : 2^{nS_1}]$, the index S_c has only a non-zero probability in a smaller subset of indices given the condition on $\mathbf{U} = \mathbf{u}$, $\mathbf{Z} = \mathbf{z}$, and $\Upsilon = 1$. In other words, $S_c \in \mathcal{S}$ where $\mathcal{S} = [1 : 2^{nS_1'}]$ and the average value of S_1' is provided in the following lemma.

Lemma 4: Let $\eta_1 > 0$ and $\varepsilon_1 > 0$, and let χ_1 be a function of the codebook $\mathtt{c}_n$ and the sequence $\mathbf{z}$ defined as

$$\chi_1(\mathtt{c}_n, \mathbf{z}) = \mathbb{1}\Big\{\big|S_1' - I(T; X\hat{Y}|UZ) - \epsilon_1\big| \geq \eta_1\Big\}, \quad (86)$$

where ϵ_1 is defined in (42). Then, for sufficiently large n, $\Pr\{\chi_1(\mathcal{C}, \mathbf{Z}) = 1 \mid \Upsilon = 1\} \leq \varepsilon_1$.

Proof: According to the codebook generation procedure from Appendix A-A, the expected number of sequences $\mathbf{t} \in \mathtt{c}_n$ such that $\mathbf{t} \in \mathcal{T}_\delta^n(T|\mathbf{quz})$ is $\mathbb{E}_{\mathcal{C}\mathbf{Z}}[|\mathcal{S}|] = 2^{n(S_1-\alpha)}$ where

$$\alpha = -\frac{1}{n}\log\frac{|\mathcal{T}_\delta^n(T|\mathbf{quz})|}{|\mathcal{T}_\delta^n(T|\mathbf{q})|}.$$

for some $(\mathbf{q}, \mathbf{u}, \mathbf{z}) \in \mathcal{T}_\delta^n(QUZ)$. If we calculate the variance of $|\mathcal{S}|$, we may then use Chebyshev's inequality to bound the values of $|\mathcal{S}|$

$$\Pr\Big\{\big||\mathcal{S}| - \mathbb{E}_{\mathcal{C}\mathbf{Z}}[|\mathcal{S}|]\big| \geq \epsilon\,\mathbb{E}_{\mathcal{C}\mathbf{Z}}[|\mathcal{S}|]\Big\} \leq \epsilon^{-2}2^{-n(S_1-\alpha)}. \quad (87)$$

The value of α may be bounded using standard bounds for the cardinality of typical sets. Finally, taking the logarithm in the argument of the probability of (87) and with an appropriate definition of η_1 and ε_1, we recover the lemma's statement. ∎

Continuing from (85), and due to $\mathbf{Q}$ and $\mathbf{U}$ being deterministic given the codebook $\mathcal{C}$,

$$\begin{aligned} &H(S|\mathcal{C}\mathbf{QUZ}, \Upsilon = 1) \\ &\quad = \mathbb{E}_{\mathcal{C}\mathbf{Z}}\big[H(S_c)\big] \\ &\quad \leq \mathbb{E}_{\mathcal{C}\mathbf{Z}}\big[H(S_c) \mid \chi_1(\mathcal{C}, \mathbf{Z}) = 0\big] + nS_1\varepsilon_1, \end{aligned} \quad (88)$$

where the last step follows from Lemma 4. Due to the symmetry of the random codebook generation and encoding procedure, the probability p_{S_c} is independent of the specific value of the index and it only depends on whether the index belongs or not to $\mathcal{S}$. This is addressed in the following lemma.

Lemma 5: Let $\epsilon > 0$ and $\varepsilon_2 > 0$, and let χ_2 be a function of the codebook $\mathtt{c}_n$ and the sequence $\mathbf{z}$ defined as

$$\chi_2(\mathtt{c}_n, \mathbf{z}) = \mathbb{1}\Big\{\big|p_{S_c}(1) - |\mathcal{S}|^{-1}\big| \geq \epsilon\,|\mathcal{S}|^{-1}\Big\}. \quad (89)$$

Then, $\Pr\{\chi_2(\mathcal{C}, \mathbf{Z}) = 1 \mid \chi_1(\mathcal{C}, \mathbf{Z}) = 0, \Upsilon = 1\} \leq \varepsilon_2$ for sufficiently large n.

Proof: See Appendix E-C. ∎

Therefore,

$$\begin{aligned} &\mathbb{E}_{\mathcal{C}\mathbf{Z}}\big[H(S_c) \mid \chi_1(\mathcal{C}, \mathbf{Z}) = 0\big] \\ &\quad \leq \mathbb{E}_{\mathcal{C}\mathbf{Z}}\big[H(S_c) \mid \chi_{\mathcal{C}\mathbf{Z}}\big] + \varepsilon_2 \log|\mathcal{S}| && (90a) \\ &\quad = \sum_{s\in\mathcal{S}} \mathbb{E}_{\mathcal{C}\mathbf{Z}}[-p_{S_c}(s)\log p_{S_c}(s) \mid \chi_{\mathcal{C}\mathbf{Z}}] + \varepsilon_2\log|\mathcal{S}| \\ &\quad = |\mathcal{S}|\,\mathbb{E}_{\mathcal{C}\mathbf{Z}}[-p_{S_c}(1)\log p_{S_c}(1) \mid \chi_{\mathcal{C}\mathbf{Z}}] + \varepsilon_2\log|\mathcal{S}| \\ &\quad \leq (1+\epsilon)\big[\log|\mathcal{S}| - \log(1-\epsilon)\big] + \varepsilon_2\log|\mathcal{S}| && (90b) \\ &\quad \leq (1+\epsilon+\varepsilon_2)\,n\big[I(T; X\hat{Y}|UZ) + \epsilon_1 + \eta_1\big] \\ &\qquad - (1+\epsilon)\log(1-\epsilon) && (90c) \\ &\quad \leq n\big[I(T; X\hat{Y}|UZ) + \epsilon_1 + \eta'\big], && (90d) \end{aligned}$$

where

- (90a) is due to Lemma 5, and $\chi_{\mathcal{C}\mathbf{Z}}$ is shorthand notation for $\{\chi_1(\mathcal{C}, \mathbf{Z}) = 0, \chi_2(\mathcal{C}, \mathbf{Z}) = 0\}$;
- (90b) follows from bounding $p_{S_c}(1)$ using Lemma 5;
- (90c) follows from bounding $|\mathcal{S}|$ using Lemma 4; and,
- (90d) holds for some $\eta' > 0$.

Finally, combining (84), (88), and (90), we obtain

$$H(\mathbf{T}|\mathcal{C}\mathbf{QUZ}) \leq n\,[I(T; X\hat{Y}|UZ) + \epsilon_1 + \eta''],$$

where $\eta'' = \eta' + n^{-1} + (\epsilon' + \varepsilon_1)S_1$, which concludes the proof of Lemma 1. ∎

B. Proof of Lemma 3

Let us first introduce a new definition[4] for the auxiliary random variable Υ,

$$\Upsilon \triangleq \mathbb{1}\Big\{(\mathbf{U}, \mathbf{T}, \mathbf{X}, \hat{\mathbf{Y}}, \mathbf{Z}) \in \mathcal{T}_\delta^n(UTX\hat{Y}Z)\Big\}.$$

Second, we note again that given the random codebook $\mathcal{C}$, the randomness in the codeword $\mathbf{V}$ comes from its index S. Third, for a specific codebook $\mathcal{C} = \mathtt{c}_n$ (which determines the codewords $\mathbf{U} = \mathbf{u}$ and $\mathbf{T} = \mathbf{t}$) and a sequence $\mathbf{Z} = \mathbf{z}$, let us define the random variable S_c with distribution

$$p_{S_c} \triangleq p_{S|\mathcal{C}=\mathtt{c}_n, \mathbf{U}=\mathbf{u}, \mathbf{T}=\mathbf{t}, \mathbf{Z}=\mathbf{z}, \Upsilon=1}. \quad (91)$$

Fourth, we note that although $S \in [1 : 2^{nS_2}]$, the index S_c has only a non-zero probability in a smaller subset of indices given the condition on $\mathbf{Z} = \mathbf{z}$ and $\Upsilon = 1$. In other words, $S_c \in \mathcal{S}$ where $\mathcal{S} = [1 : 2^{nS_2'}]$ and the average value of S_2' is provided in the following lemma.

Lemma 6: Let $\eta_1 > 0$ and $\varepsilon_1 > 0$, and let χ_1 be a function of the codebook $\mathtt{c}_n$ and the sequence $\mathbf{z}$ defined as

$$\chi_1(\mathtt{c}_n, \mathbf{z}) = \mathbb{1}\Big\{\big|S_2' - I(V; X\hat{Y}|UTZ) - \epsilon_2\big| \geq \eta_1\Big\}, \quad (92)$$

where ϵ_1 is defined in (42). Then, for sufficiently large n, $\Pr\{\chi_1(\mathcal{C}, \mathbf{Z}) = 1 \mid \Upsilon = 1\} \leq \varepsilon_1$.

Proof: It follows similar steps as those in Lemma 4, and thus it is omitted. ∎

Fifth, due to the symmetry of the random codebook generation and encoding procedure, the probability p_{S_c} is independent of the specific value of the index and it only depends on whether the index belongs or not to $\mathcal{S}$. The statement of Lemma 5 holds although the proof involves characterizing the behavior of the index of $\mathbf{V}$

[4]The sequence $\mathbf{Q}$ is omitted in the sequel given the Markov chain $\mathbf{Q} \multimap (\mathcal{C}\mathbf{UT}) \multimap (\mathbf{VX}\hat{\mathbf{Y}}\mathbf{Z})$ that arises due to the codebook generation procedure.

instead of that of $\mathbf{T}$. The proof is omitted due to its similarity.

Finally, since we are interested in a lower bound of the index of the codeword $\mathbf{V}$, (84), (88), and (90) may be simplified as

$$\begin{aligned}
&H(\mathbf{V}|\mathcal{C}\mathbf{UTZ})\\
&\quad= H(S|\mathcal{C}\mathbf{UTZ})\\
&\quad\geq H(S|\mathcal{C}\mathbf{UTZ},\Upsilon=1)(1-\epsilon') && \text{(93a)}\\
&\quad= \mathbb{E}_{\mathcal{C}\mathbf{Z}}\big[H(S_c)\big](1-\epsilon') && \text{(93b)}\\
&\quad\geq \mathbb{E}_{\mathcal{C}\mathbf{Z}}\big[H(S_c)\mid \chi_1(\mathcal{C},\mathbf{Z})=0\big](1-\epsilon')(1-\varepsilon_1) && \text{(93c)}\\
&\quad\geq \mathbb{E}_{\mathcal{C}\mathbf{Z}}\big[H(S_c)\mid \chi_{\mathcal{C}\mathbf{Z}}\big](1-\varepsilon) && \text{(93d)}\\
&\quad= |\mathcal{S}|\,\mathbb{E}_{\mathcal{C}\mathbf{Z}}[-p_{S_c}(1)\log p_{S_c}(1)\mid \chi_{\mathcal{C}\mathbf{Z}}](1-\varepsilon)\\
&\quad\geq (1-\epsilon)\big[\log|\mathcal{S}|-\log(1+\epsilon)\big](1-\varepsilon) && \text{(93e)}\\
&\quad\geq (1-\epsilon)\,n\big[I(V;X\hat{Y}|UTZ)+\epsilon_2-\eta_1\big](1-\varepsilon)\\
&\qquad-(1-\epsilon)\log(1+\epsilon)(1-\varepsilon) && \text{(93f)}\\
&\quad\geq n\big[I(V;X\hat{Y}|UTZ)+\epsilon_2-\eta'\big], && \text{(93g)}
\end{aligned}$$

where

- (93a) follows from $\Pr\{\Upsilon=1\}\geq 1-\epsilon'$;
- (93b) stems from (91) since $\mathbf{u}$ and $\mathbf{t}$ are fixed given the codebook $\mathtt{c}_n$;
- (93c) is due to $\Pr\{\chi_1(\mathcal{C},\mathbf{Z})=0\mid\Upsilon=1\}\geq 1-\varepsilon_1$ according to Lemma 6;
- (93d) follows from Lemma 5, $\chi_{\mathcal{C}\mathbf{Z}}$ as defined in (90a), and $(1-\varepsilon)=(1-\epsilon')(1-\varepsilon_1)(1-\varepsilon_2)$;
- (93e) stems from bounding $p_{S_c}(1)$ using Lemma 5;
- (93f) stems from bounding $|\mathcal{S}|$ using Lemma 6; and,
- (93g) holds for some $\eta'>0$.

This concludes the proof of Lemma 3. ∎

C. Proof of Lemma 5

According to the encoding procedure detailed in Appendix A-B, the index S is chosen uniformly among all the jointly typical codewords or, if there is no jointly typical codeword, uniformly on the whole codebook. However, due to the conditioning on $\mathbf{U}$, $\mathbf{Z}$, and $\Upsilon=1$, we restrict the indices to the set $\mathcal{S}$. We may thus characterize $p_{S_c}(1)$ as

$$p_{S_c}(1)=\sum_{(\mathbf{x},\hat{\mathbf{y}})\in\mathcal{T}_\delta^n(X\hat{Y})}\frac{p(\mathbf{x},\hat{\mathbf{y}})}{\Pr\Big\{\mathcal{T}_\delta^n(X\hat{Y})\Big\}}\,\Upsilon_{\mathbf{x},\hat{\mathbf{y}}}, \tag{94}$$

where

$$\Upsilon_{\mathbf{x},\hat{\mathbf{y}}}=\frac{\nu_1}{1+\sum_{i=2}^{|\mathcal{S}|}\nu_i}+|\mathcal{S}|^{-1}\prod_{i=1}^{|\mathcal{S}|}(1-\nu_i) \tag{95}$$

and ν_i is the event that the codeword $\mathbf{t}(i)$ is jointly typical with the pair $(\mathbf{x},\hat{\mathbf{y}})$, i.e.,

$$\begin{aligned}\nu_i\triangleq\mathbb{1}\big\{&\mathbf{t}(i)\in\mathcal{T}_\delta^n(T|\mathbf{u},\mathbf{x},\hat{\mathbf{y}})\mid\mathbf{t}(i)\in\mathcal{T}_\delta^n(T|\mathbf{q},\mathbf{u},\mathbf{z}),\\ &(\mathbf{q},\mathbf{u},\mathbf{z})\in\mathcal{T}_\delta^n(QUZ|\mathbf{x},\hat{\mathbf{y}})\big\}.\end{aligned}$$

The first term in (95) distributes the probability of each pair $(\mathbf{x},\hat{\mathbf{y}})\in\mathcal{T}_\delta^n(X\hat{Y})$ uniformly among all the jointly typical codewords, while the second term in (95) distributes this probability uniformly among all codewords in $\mathcal{S}$, given that no one was jointly typical with $(\mathbf{x},\hat{\mathbf{y}})$. It is not hard to see that the expected value of ν_i is

$$\mathbb{E}_{\mathcal{C}\mathbf{Z}}[\nu_i]=\frac{|\mathcal{T}_\delta^n(T|\mathbf{u},\mathbf{x},\hat{\mathbf{y}})|}{|\mathcal{T}_\delta^n(T|\mathbf{q},\mathbf{u},\mathbf{z})|}\triangleq\gamma,$$

for some $(\mathbf{q},\mathbf{u},\mathbf{x},\hat{\mathbf{y}},\mathbf{z})\in\mathcal{T}_\delta^n(QUX\hat{Y}Z)$.

The expected value of (94) depends on the behavior of $\Upsilon_{\mathbf{x},\hat{\mathbf{y}}}$. Each ν_i is a Bernoulli RV with $\mathbb{E}_{\mathcal{C}\mathbf{Z}}[\nu_i]=\gamma$ and it is independent of the other ν_i's. Let us define

$$\nu=\sum_{i=2}^{|\mathcal{S}|}\nu_i,$$

then ν is a Binomial RV, and thus, for $j\in[0:|\mathcal{S}|-1]$,

$$p_\nu(j)=\binom{|\mathcal{S}|-1}{j}\gamma^j(1-\gamma)^{|\mathcal{S}|-1-j}.$$

After some manipulations, it is possible to show that

$$\mathbb{E}_{\mathcal{C}\mathbf{Z}}\left[\frac{1}{1+\nu}\right]=\frac{1-(1-\gamma)^{|\mathcal{S}|}}{\gamma\,|\mathcal{S}|}.$$

Hence,

$$\mathbb{E}_{\mathcal{C}\mathbf{Z}}[\Upsilon_{\mathbf{x},\hat{\mathbf{y}}}]=\mathbb{E}_{\mathcal{C}\mathbf{Z}}\left[\frac{\nu_1}{1+\nu}+\frac{1}{|\mathcal{S}|}\prod_{i=1}^{|\mathcal{S}|}(1-\nu_i)\right]=\frac{1}{|\mathcal{S}|},$$

and consequently, the expected value of (94) is

$$\mathbb{E}_{\mathcal{C}\mathbf{Z}}[p_{S_c}(1)]=\mathbb{E}_{\mathcal{C}\mathbf{Z}}[\Upsilon_{\mathbf{x},\hat{\mathbf{y}}}]=|\mathcal{S}|^{-1}.$$

Noting that $\Upsilon_{\mathbf{x},\hat{\mathbf{y}}}$ and $\Upsilon_{\mathbf{x}',\hat{\mathbf{y}}'}$ are independent variables given different pairs of sequences $(\mathbf{x},\hat{\mathbf{y}})$ and $(\mathbf{x}',\hat{\mathbf{y}}')$, and that $(\Upsilon_{\mathbf{x},\hat{\mathbf{y}}})^2\leq\Upsilon_{\mathbf{x},\hat{\mathbf{y}}}$, we obtain

$$\mathbb{E}_{\mathcal{C}\mathbf{Z}}[(p_{S_c}(1))^2]\leq 2^{-n[H(X\hat{Y})-\xi]}|\mathcal{S}|^{-1}+|\mathcal{S}|^{-2},$$

for some $\xi>0$. Therefore,

$$\mathrm{Var}[p_{S_c}(1)]\leq 2^{-n[H(X\hat{Y})-\xi]}|\mathcal{S}|^{-1},$$

and in view of Chebyshev's inequality,

$$\begin{aligned}&\Pr\Big\{\big|p_{S_c}(1)-|\mathcal{S}|^{-1}\big|\geq\epsilon\,|\mathcal{S}|^{-1}\Big\}\\ &\quad\leq\epsilon^{-2}2^{-n[H(X\hat{Y})-\xi]}|\mathcal{S}|\\ &\quad\leq\epsilon^{-2}2^{-n[H(X\hat{Y})-I(T;X\hat{Y}|UZ)-\epsilon_1-\eta_1-\xi]}\\ &\quad=\epsilon^{-2}2^{-n[I(UZ;X\hat{Y})+H(X\hat{Y}|UTZ)-\epsilon_1-\eta_1-\xi]},\end{aligned}$$

where the last inequality follows from Lemma 4. This concludes the proof of Lemma 5. ∎

Appendix F
Proof of Lemma 2

Let us modify the problem definition and then extend the scheme of Theorem 1 by introducing a virtual receiver. For each transmission block j, this new receiver observes the same channel output $\mathbf{Z}_j$ as the eavesdropper, but it has also perfect access to the codewords $\mathbf{Q}_j$, $\mathbf{U}_j$, and $\mathbf{T}_j$ as well as the indices L_{2j} and K_j. In this new setup, we require the virtual receiver to decode the codeword $\mathbf{V}_j$ in each block j.

With a slight abuse of notation, we know that according to the codebook generation procedure from Appendix A-A

and conditioned on the codewords $\mathbf{U}_j$ and $\mathbf{T}_j$, there are 2^{nS_2} codewords $\mathbf{V}(L_{2j}, K_j, S_{dj})$. The dummy index S_{dj} represents the position of codeword $\mathbf{V}$ inside the sub-bin K_j and, given the decoding step 3 in Appendix A-C, it is correctly decoded by the legitimate decoder. Therefore, if we redefine the probability of error for this *enhanced* WTC-GF as

$$\mathsf{P}'_e(\mathsf{c}_n) \triangleq \Pr\Big\{(\hat{\mathbb{M}}^b, \hat{S}_d^b) \neq (\mathbb{M}^b, S_d^b) \text{ or } \hat{S}_d^b \neq S_d^b \,|\, \mathsf{c}_n\Big\},$$

we see that a valid code for the enhanced WTC-GF described here is also a valid code for the original WTC-GF.

The extension of Theorem 1 is then straightforward; we only need to define the decoding procedure at the virtual receiver. At each block $(j+1) \in [2:b]$, and given $\mathbf{q}_j$, $\mathbf{u}_j$, $\mathbf{t}_j$, $\mathbf{z}_j$, l_{2j}, and k_j, the virtual receiver looks for the unique index $s_{dj} \equiv \hat{s}$ such that

$$\big(\mathbf{v}(l_{2j}, k_j, \hat{s}), \mathbf{q}_j, \mathbf{u}_j, \mathbf{t}_j, \mathbf{z}_j\big) \in \mathcal{T}_\delta^n(VQUTZ).$$

Given that $S_2 - \tilde{S}_2 - \bar{S}_2 = I(V;Z|UT) - \tilde{\epsilon}_2$, the probability of error in decoding is arbitrarily small as $n \to \infty$ if $\delta < \tilde{\epsilon}_2$. Then, using Fano's inequality, we have

$$H(S_{dj}|\mathcal{C}\mathbf{Q}_j\mathbf{U}_j\mathbf{T}_j\mathbf{Z}_j L_{2j} K_j) \leq n\epsilon_n,$$

where ϵ_n denotes a sequence such that $\epsilon_n \to 0$ as $n \to \infty$. The lemma's statement follows from the deterministic relationship between S_{dj} and $\mathbf{V}$ given the codebook, and where we omitted $\mathbf{Q}_j$ due to the Markov chain $\mathbf{Q}_j \multimap (\mathcal{C}\mathbf{U}_j\mathbf{T}_j\mathbf{Z}_j) \multimap \mathbf{V}$. This concludes the proof of Lemma 2. ∎

Appendix G
Proof of Proposition 7

We proceed to bound from above expressions (13) and (14), for which we will make use of the variables defined in (39). We then show that these upper bounds are achievable with a specific set of random variables. In particular, an upper bound of (13a) is given by

$$R_{KG_1} \leq I(U;Y|Q) - I(U;Z'S|Q) + I(V;Y|UT) - I(V;Z'S|UT), \quad (96)$$

since $I(U;T|QZ'S) \geq 0$ and $I(V;XS|UY)$ might be larger than $I(Q;Y)$. Consider now the first two terms on the right-hand side of (96), where we note that we may add the auxiliary variables $S \triangleq \mathbb{1}\{Y=e\}$ and $S_E \triangleq \mathbb{1}\{Z'=e\}$ alongside Y and Z' without increasing the mutual informations,

$$\begin{aligned}
&I(U;Y|Q) - I(U;Z'S|Q)\\
&\quad= I(U;YS|Q) - I(U;Z'SS_E|Q)\\
&\quad= I(U;Y|QS) - I(U;Z|QSS_E) && (97a)\\
&\quad= I(U;X|Q,S=0)(1-\delta)\\
&\qquad - I(U;X|QS,S_E=0)(1-\delta_E)\\
&\quad= I(U;X|Q)(\delta_E - \delta) && (97b)\\
&\quad\leq I(U;X)(\delta_E - \delta), && (97c)
\end{aligned}$$

where

- (97a) and (97b) are due to (Q,U,X) being independent of (S,S_E); and,
- (97c) follows from the Markov chain $Q \multimap U \multimap X$ assuming that $\delta_E - \delta \geq 0$. If $\delta_E - \delta < 0$, (97) is negative, which means that it is not possible to transmit an unencrypted message, and the rate R_{KG_2} is larger. The reader may later compare the final expressions (100) and (103) to corroborate this claim.

Let us concentrate now on the last two terms on the right-hand side of (96),

$$\begin{aligned}
&I(V;Y|UT) - I(V;Z'S|UT)\\
&\quad= I(V;YS|UT) - I(V;Z'SS_E|UT)\\
&\quad= I(V;Y|UTS) - I(V;Z'S_E|UTS)\\
&\quad= I(V;Y|UTS) - I(V;Z'|UTSS_E) && (98a)\\
&\quad= I(V;X|UT,S=0)(1-\delta)\\
&\qquad - I(V;X|UTS,S_E=0)(1-\delta_E)\\
&\quad= I(V;X|UT,S=0)(1-\delta)\delta_E\\
&\qquad - I(V;X|UT,S=1)(1-\delta_E)\delta && (98b)\\
&\quad\leq I(V;X|UT,S=0)(1-\delta)\delta_E && (98c)\\
&\quad\leq H(X|UT,S=0)(1-\delta)\delta_E\\
&\quad\leq H(X|U)(1-\delta)\delta_E, && (98d)
\end{aligned}$$

where

- (98a) and (98b) are due to (U,X,T,V,S) being independent of S_E; and,
- (98c) stems from the non-negativity of the mutual information.

On the other hand, an upper bound of (13b) is given by

$$R_{KG_1} \leq I(U;Y|Q) = I(U;X|Q)(1-\delta) \leq I(U;X)(1-\delta), \quad (99)$$

which follows similar steps as (97). Therefore, joining (96)–(99), the rate R_{KG_1} may be bounded from above by

$$R_{KG_1} \leq \max_{p(ux)} \min\big\{I(U;X)(\delta_E - \delta) + H(X|U)(1-\delta)\delta_E, I(U;X)(1-\delta)\big\}, \quad (100)$$

which is indeed achievable by selecting the following set of variables:

$$T = Q = \emptyset \quad \text{and} \quad V = \begin{cases} X & \text{if } S=0\\ \emptyset & \text{if } S=1. \end{cases} \quad (101)$$

Given that $0 \leq H(X|U) \leq H(X) \leq 1$, we may rewrite the bound (100) using $H(X|U) = \beta$, $\beta \in [0,1]$,

$$R_{KG_1} \leq \max_{\beta\in[0,1]} \min\big\{(1-\beta)(\delta_E - \delta) + \beta(1-\delta)\delta_E, (1-\beta)(1-\delta)\big\}.$$

Upon inspection, we see that the first term increases linearly with β while the second one decreases. Therefore, there is a unique maximizer:

$$R_{KG_1} \leq (1-\delta)\delta_E \frac{1-\delta}{1-\delta\delta_E} \quad \text{for } \beta = \frac{1-\delta_E}{1-\delta\delta_E}. \quad (102)$$

We can proceed similarly for the rate R_{KG_2}, by selecting the variables as indicated in (101), and obtain

$$R_{KG_2} \leq \max_{p(ux)} \min\left\{H(X|U)(1-\delta)\delta_E,\ I(U;X)(1-\delta)\right\}, \tag{103}$$

or equivalently:

$$R_{KG_2} \leq \max_{\beta\in[0,1]} \min\left\{\beta(1-\delta)\delta_E,\ (1-\beta)(1-\delta)\right\},$$

whose maximization gives

$$R_{KG_2} \leq (1-\delta)\delta_E \frac{1}{1+\delta_E} \quad \text{for } \beta = \frac{1}{1+\delta_E}. \tag{104}$$

Finally, joining (102) and (104) we obtain the statement of Proposition 7. ∎

ACKNOWLEDGMENT

The authors are grateful to Prof. Sheng Yang for valuable discussions at the early stage of this work. The authors would also like to thank the Associate Editor and the anonymous reviewers for their constructive and helpful comments on the earlier version of the paper, which helped to improve the manuscript.

REFERENCES

[1] G. Bassi, P. Piantanida, and S. Shamai (Shitz), "The wiretap channel with generalized feedback: Secure communication and key generation," in *Proc. IEEE Inf. Theory Workshop—Fall (ITW)*, Oct. 2015, pp. 282–286.

[2] Y. Liang, H. V. Poor, and S. Shamai (Shitz), "Information theoretic security," in *Foundations and Trends in Communications and Information Theory*, vol. 5, nos. 4–5. Hanover, MA, USA: Now, 2009, pp. 355–580.

[3] R. Bassily *et al.*, "Cooperative security at the physical layer: A summary of recent advances," *IEEE Signal Process. Mag.*, vol. 30, no. 5, pp. 16–28, Sep. 2013.

[4] S. Yang, M. Kobayashi, P. Piantanida, and S. Shamai (Shitz), "Secrecy degrees of freedom of MIMO broadcast channels with delayed CSIT," *IEEE Trans. Inf. Theory*, vol. 59, no. 9, pp. 5244–5256, Sep. 2013.

[5] R. Tandon, P. Piantanida, and S. Shamai (Shitz), "On multi-user MISO wiretap channels with delayed CSIT," in *Proc. IEEE Int. Symp. Inf. Theory*, Jun./Jul. 2014, pp. 211–215.

[6] G. Dueck, "Partial feedback for two-way and broadcast channels," *Inf. Control*, vol. 46, no. 1, pp. 1–15, Jul. 1980.

[7] T. Cover and C. Leung, "An achievable rate region for the multiple-access channel with feedback," *IEEE Trans. Inf. Theory*, vol. IT-27, no. 3, pp. 292–298, May 1981.

[8] J. Schalkwijk and T. Kailath, "A coding scheme for additive noise channels with feedback–I: No bandwidth constraint," *IEEE Trans. Inf. Theory*, vol. IT-12, no. 2, pp. 172–182, Apr. 1966.

[9] R. Ahlswede and N. Cai, "Transmission, identification and common randomness capacities for wire-tape channels with secure feedback from the decoder," in *General Theory of Information Transfer and Combinatorics*, vol. 4123. Berlin, Germany: Springer, 2006, pp. 258–275.

[10] B. Dai, A. J. H. Vinck, Y. Luo, and Z. Zhuang, "Capacity region of non-degraded wiretap channel with noiseless feedback," in *Proc. IEEE Int. Symp. Inf. Theory*, Jul. 2012, pp. 244–248.

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

[12] Y.-K. Chia and A. El Gamal, "Wiretap channel with causal state information," *IEEE Trans. Inf. Theory*, vol. 58, no. 5, pp. 2838–2849, May 2012.

[13] L. Czap, V. M. Prabhakaran, C. Fragouli, and S. N. Diggavi, "Secret communication over broadcast erasure channels with state-feedback," *IEEE Trans. Inf. Theory*, vol. 61, no. 9, pp. 4788–4808, Sep. 2015.

[14] R. Ahlswede and I. Csiszàr, "Common randomness in information theory and cryptography. I. Secret sharing," *IEEE Trans. Inf. Theory*, vol. 39, no. 4, pp. 1121–1132, Jul. 1993.

[15] 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.

[16] I. Csiszàr and P. Narayan, "Common randomness and secret key generation with a helper," *IEEE Trans. Inf. Theory*, vol. 46, no. 2, pp. 344–366, Mar. 2000.

[17] I. Csiszàr and P. Narayan, "Secrecy capacities for multiterminal channel models," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2437–2452, Jun. 2008.

[18] A. A. Gohari and V. Anantharam, "Information-theoretic key agreement of multiple terminals—Part I," *IEEE Trans. Inf. Theory*, vol. 56, no. 8, pp. 3973–3996, Aug. 2010.

[19] A. A. Gohari and V. Anantharam, "Information-theoretic key agreement of multiple terminals—Part II: Channel model," *IEEE Trans. Inf. Theory*, vol. 56, no. 8, pp. 3997–4010, Aug. 2010.

[20] A. Khisti, S. N. Diggavi, and G. W. Wornell, "Secret-key generation using correlated sources and channels," *IEEE Trans. Inf. Theory*, vol. 58, no. 2, pp. 652–670, Feb. 2012.

[21] S. Salimi, M. Skoglund, J. D. Golic, M. Salmasizadeh, and M. R. Aref, "Key agreement over a generalized multiple access channel using noiseless and noisy feedback," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1765–1778, Sep. 2013.

[22] V. M. Prabhakaran, K. Eswaran, and K. Ramchandran, "Secrecy via sources and channels," *IEEE Trans. Inf. Theory*, vol. 58, no. 11, pp. 6747–6765, Nov. 2012.

[23] X. Tang, R. Liu, P. Spasojević, and H. V. Poor, "Multiple access channels with generalized feedback and confidential messages," in *Proc. IEEE Inf. Theory Workshop*, Sep. 2007, pp. 608–613.

[24] E. Ekrem and S. Ulukus, "Effects of cooperation on the secrecy of multiple access channels with generalized feedback," in *Proc. 42nd Annu. Conf. Inf. Sci. Syst. (CISS)*, Mar. 2008, pp. 791–796.

[25] T. T. Kim and H. V. Poor, "Secure communications with insecure feedback: Breaking the high-SNR ceiling," *IEEE Trans. Inf. Theory*, vol. 56, no. 8, pp. 3700–3711, Aug. 2010.

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

[27] L. Lai, H. El Gamal, and H. V. Poor, "The wiretap channel with feedback: Encryption over the channel," *IEEE Trans. Inf. Theory*, vol. 54, no. 11, pp. 5059–5067, Nov. 2008.

[28] D. Gündüz, D. R. Brown, and H. V. Poor, "Secret communication with feedback," in *Proc. Int. Symp. Inf. Theory Appl.*, Dec. 2008, pp. 1–6.

[29] G. Bassi, P. Piantanida, and S. Shamai (Shitz), "On the capacity of the wiretap channel with generalized feedback," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jun. 2015, pp. 1154–1158.

[30] 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.

[31] S. I. Gel'fand and M. S. Pinsker, "Coding for channel with random parameters," *Problems Control Inf. Theory*, vol. 9, no. 1, pp. 19–31, 1980.

[32] W. Liu and B. Chen, "Wiretap channel with two-sided channel state information," in *Proc. Conf. Rec. 41st Asilomar Conf. Signals, Syst. Comput. (ACSSC)*, Nov. 2007, pp. 893–897.

[33] H. G. Bafghi, B. Seyfe, M. Mirmohseni, and M. R. Aref, "On the achievable rate region of a new Gaussian wiretap channel with side information," in *Proc. IEEE Inf. Theory Workshop (ITW)*, Sep. 2012, pp. 657–661.

[34] A. El Gamal and Y.-H. Kim, *Network Information Theory*. Cambridge, U.K.: Cambridge Univ. Press, 2011.

[35] U. Maurer and S. Wolf, "Information-theoretic key agreement: From weak to strong secrecy for free," in *Advances in Cryptology—EUROCRYPT*, B. Preneel, Ed. Berlin, Germany: Springer, 2000, pp. 351–368.

[36] V. Prabhakaran and K. Ramchandran, "A separation result for secure communication," in *Proc. 45th Annu. Allerton Conf. Commun., Control, Comput.*, Sep. 2007, pp. 34–41.

[37] Z. Goldfeld, P. Cuff, and H. H. Permuter. (Aug. 2016). "Wiretap channels with random states non-causally available at the encoder." [Online]. Available: https://arxiv.org/abs/1608.00743

[38] G. Bassi, P. Piantanida, and S. Shamai (Shitz). (Jul. 2015). "The wiretap channel with generalized feedback: Secure communication and key generation." [Online]. Available: https://arxiv.org/abs/1507.07091

[39] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*. Cambridge, U.K.: Cambridge Univ. Press, 2011.

Germán Bassi (S'10–M'16) received the B.Sc. and M.Sc. degrees in Electrical Engineering from the University of Buenos Aires (Argentina) in 2010, and the Ph.D. degree in Telecommunications from CentraleSupélec (France) in 2015. He is now with the Department of Information Science and Engineering at KTH Royal Institute of Technology (Sweden). His current research focuses on multi-user information theory, physical-layer security, and inference and statistics, with applications to privacy and machine learning.

Pablo Piantanida (S'04–M'08–SM'16) received both B.Sc. in Electrical Engineering and the M.Sc. (with honors) from the University of Buenos Aires (Argentina) in 2003, and the Ph.D. from Université Paris-Sud (Orsay, France) in 2007. Since October 2007 he has joined the Laboratoire des Signaux et Systèmes (L2S), at CentraleSupélec together with CNRS (UMR 8506) and Université Paris-Sud, as an Associate Professor of Network Information Theory. He is currently associated with the Montreal Institute for Learning Algorithms (MILA) at Université de Montréal. He is an IEEE Senior Member and General Co-Chair of the 2019 IEEE International Symposium on Information Theory (ISIT). His research interests lie broadly in information theory and its interactions with other fields, including multi-terminal information theory, Shannon theory, machine learning and representation learning, statistical inference, cooperative communications, communication mechanisms for security and privacy.

Shlomo Shamai (Shitz) (S'80–M'82–SM'88–LF'18) received the B.Sc., M.Sc., and Ph.D. degrees in electrical engineering from the Technion—Israel Institute of Technology, in 1975, 1981, and 1986, respectively.

During 1975–1985 he was with the Communications Research Labs, in the capacity of a Senior Research Engineer. Since 1986 he is with the Department of Electrical Engineering, Technion—Israel Institute of Technology, where he is now a Technion Distinguished Professor, and holds the William Fondiller Chair of Telecommunications. His research interests encompasses a wide spectrum of topics in information theory and statistical communications.

Dr. Shamai (Shitz) is an IEEE Fellow, an URSI Fellow, a member of the Israeli Academy of Sciences and Humanities and a foreign member of the US National Academy of Engineering. He is the recipient of the 2011 Claude E. Shannon Award, the 2014 Rothschild Prize in Mathematics/Computer Sciences and Engineering and the 2017 IEEE Richard W. Hamming Medal.

He has been awarded the 1999 van der Pol Gold Medal of the Union Radio Scientifique Internationale (URSI), and is a co-recipient of the 2000 IEEE Donald G. Fink Prize Paper Award, the 2003, and the 2004 joint IT/COM societies paper award, the 2007 IEEE Information Theory Society Paper Award, the 2009 and 2015 European Commission FP7, Network of Excellence in Wireless COMmunications (NEWCOM++, NEWCOM#) Best Paper Awards, the 2010 Thomson Reuters Award for International Excellence in Scientific Research, the 2014 EURASIP Best Paper Award (for the EURASIP Journal on Wireless Communications and Networking), the 2015 IEEE Communications Society Best Tutorial Paper Award and the 2018 IEEE Signal Processing Best Paper Award. He is also the recipient of 1985 Alon Grant for distinguished young scientists and the 2000 Technion Henry Taub Prize for Excellence in Research. He has served as Associate Editor for the Shannon Theory of the IEEE TRANSACTIONS ON INFORMATION THEORY, and has also served twice on the Board of Governors of the Information Theory Society. He has also served on the Executive Editorial Board of the IEEE TRANSACTIONS ON INFORMATION THEORY and on the IEEE Information Theory Society Nominations and Appointments Committee.