The Secrecy Capacity of the Wiretap Channel With Additive Noise and Rate-Limited Help

Sergey Loyka, *Senior Member, IEEE*, and Neri Merhav, *Life Fellow, IEEE*

***Abstract*— The wiretap channel with additive (possibly non-Gaussian) noise and rate-limited help, available at the legitimate receiver (Rx) or/and transmitter (Tx), is studied under various channel configurations (degraded, reversely degraded and non-degraded) and power/amplitude constraints. For all channel configurations, the rate-limited Rx help results in a (weak or strong) secrecy capacity boost equal to the help rate. This holds irrespective of whether the help is secure or not, or whether the helper is aware of the message being transmitted or not; the secrecy of help or helper's knowledge of the message does not provide any extra capacity boost. The secrecy capacity is positive for the reversely-degraded channel (where the no-help secrecy capacity is zero) and no wiretap coding is needed to achieve it under weak secrecy. The same capacity boost also holds if non-secure help is available to the transmitter (encoder), in addition to or instead of the same Rx help, so that, in the case of the joint Tx/Rx help, one help link can be omitted without affecting the capacity. If Rx/Tx help links are independent of each other, the capacity boost is the sum of help rates and no link can be omitted without loss in the capacity. Non-singular correlation of the receiver and eavesdropper noises does not affect the secrecy capacity and non-causal help does not bring in any capacity increase over the causal one. The choice of the secrecy criterion (weak/strong) affects the complexity of implementation but not the secrecy capacity. Stronger noise at the legitimate receiver can sometimes result in higher secrecy capacity.**

***Index Terms*— Wiretap channel, secrecy capacity, rate-limited help.**

I. Introduction

PHYSICAL-LAYER security has emerged as a valuable alternative to cryptography-based techniques [1], [2], [3], especially over wireless channels and networks, and it also plays an important role in modern industrial standards [4], [5], [6]. While the original work on information-theoretic secrecy dates back to Shannon himself [7], Wyner's wiretap channel (WTC) model [8] established itself as a very useful tool for many different settings and configurations. It includes one legitimate transmitter-receiver pair and one wiretapper (or eavesdropper) to be kept ignorant of the transmitted message; see [9] for a simplified analysis of this model. Its key performance metric is the secrecy capacity, i.e. the largest achievable rate subject to (weak or strong) secrecy in addition to a reliability constraint, possibly under a power constraint. The original degraded WTC model has been extended and developed in many respects, of which we mention here only a few. Csiszar and Korner [10] extended it to broadcast channels with confidential messages, including non-degraded WTC as a special case and established its secrecy capacity, which became a starting point for many further extensions and developments, see e.g. [1], [2], [3], and [4] and references therein. The discrete memoryless model was extended to single-antenna (SISO) Gaussian settings in [11] and further to multi-antenna (MIMO) settings in [12], [13], and [14]; the respective secrecy capacities and optimal signalling strategies were also established [11], [12], [13], [14], [15] and were further extended to interference-constrained channels [16], [17]. The SISO Gaussian WTC with interference known to the transmitter was studied in [18] and its achievable secrecy rates were obtained. Encoding individual (deterministic) source sequences for the degraded memoryless WTC was studied in [19]; a necessary condition for secure and reliable transmission of such sequences was obtained and an achievability scheme was also given. More refined performance metrics (beyond secrecy capacity), including secrecy exponents, finite blocklength and second-order coding rates, have also been studied, see [20] and [21] and references therein. More general information-unstable wiretap channels have been considered in [22] using information-spectrum techniques.

WTCs under various cost (power/amplitude) constraints have also been studied [22], [23], [24], [25], [26]. While adding a cost constraint to the standard WTC setup amounts, in most cases, to using the same capacity formula (e.g. the maximized difference of mutual information terms) but with the input optimization being limited to meet the constraint, there are some exceptions where this is not the case and the capacity formula itself needs to be modified (two auxiliary random variables are needed instead of one) [25].

While the above models assume the availability of complete knowledge of the channel, such knowledge may be incomplete or inaccurate in many practical settings and a compound channel model emerges. Finite-state compound WTCs have been studied in [27] and [28] and their secrecy capacities were established under certain degradedness assumptions.

Manuscript received 15 September 2022; revised 7 June 2023; accepted 19 September 2023. Date of publication 4 October 2023; date of current version 26 December 2023. An earlier version of this paper was presented in part at the IEEE International Symposium on Information Theory [DOI: 10.1109/ISIT50566.2022.9834880] and in part at the IEEE Information Theory Workshop [DOI: 10.1109/ITW55543.2023.10161609]. *(Corresponding author: Sergey Loyka.)*

Sergey Loyka is with the School of Electrical Engineering and Computer Science, University of Ottawa, Ottawa, ON K1N 6N5, Canada (e-mail: sergey.loyka@uottawa.ca).

Neri Merhav is with the Andrew and Erna Viterbi Faculty of Electrical and Computer Engineering, Technion—Israel Institute of Technology, Haifa 32000, Israel (e-mail: merhav@ee.technion.ac.il).

Communicated by M. Bloch, Associate Editor for Security and Privacy.

Color versions of one or more figures in this article are available at https://doi.org/10.1109/TIT.2023.3322116.

Digital Object Identifier 10.1109/TIT.2023.3322116

The secrecy capacity of a class of compound Gaussian wiretap MIMO channels with normed uncertainty (not necessarily degraded or finite state) and an optimal signalling strategy were established in [29].

The original WTC model can also be extended in other respects, including the addition of side information and feedback, which are often available in modern systems and networks. While feedback does not increase the ordinary (no secrecy) capacity of memoryless channels, it is often able to boost the secrecy capacity, even in the memoryless settings, see e.g. [30] and references therein. The memoryless Gaussian WTC with noiseless (and hence rate-unlimited) feedback was considered in [31], whereby the transmitter (Tx) has access to the signal of the legitimate receiver (Rx) in a causal manner while the eavesdropper (Ev) has access to a noisy version of the feedback. Its secrecy capacity C_{snf} was shown to be equal to the ordinary (no Ev, no feedback) AWGN channel capacity C_0,

$$C_{snf} = C_0 \tag{1}$$

i.e. secrecy comes for free with the noiseless feedback and the secrecy capacity with feedback exceeds the no-feedback one, even though the channel is memoryless and, possibly, not degraded. The capacity-achieving strategy is the Schalkwijk-Kailath scheme [32] (which is also optimal for the no-Ev/no-secrecy case) and no wiretap coding is needed. This result was further extended to a colored (ARMA) Gaussian noise channel with noiseless (rate-unlimited) feedback in [30] and a generalized Schalkwijk-Kailath scheme was shown to be optimal. Note, however, that, in this setting, the Tx has access to the noiseless feedback while the Ev observes only its noisy version, i.e. the Ev is at a significant disadvantage and the feedback is at least partially secure (hidden by the noise in the Ev feedback link). The situation changes dramatically if the Ev has access to the same noiseless (and, hence, non-secure) feedback as well or if the Rx-to-Tx feedback link is also noisy or rate-limited (the Schalkwijk-Kailath scheme does not work in this case). The degraded memoryless Gaussian WTC with a secure *rate-limited* feedback of rate $R_f < \infty$ was considered in [33] and its secrecy capacity C_{sf} was established:

$$C_{sf} = \min\{C_0, C_{s0} + R_f\} \tag{2}$$

where C_{s0} is the secrecy capacity without feedback.[1] An optimal Tx strategy is fundamentally different from [30] and [31] in this setting: it is a combination of the standard wiretap coding as in [8] with a secure key generated by the Rx and sent to the Tx via the secure rate-limited feedback link (it is this second part that is responsible for the $+R_f$ boost in the secrecy capacity as it protects a part of the message which was dummy in [8]). Note, however, that this strategy requires a secure feedback link, so that the feedback is (completely) unknown to the Ev, and it does not apply otherwise.

In modern communication systems/networks, various forms of side information, beyond feedback, are often available to the encoder or/and decoder (e.g. in a cloud radio access network with a centralized processing unit or in a cooperative communication system). This can be used to facilitate reliable communications and often results in a boost to the capacity [34]. One particular configuration was recently studied in [35], [36], [37], and [38], where a rate-limited (and error-free) help is available to the decoder or/and encoder. In particular, a helper observes the noise sequence (which can be a signal intended for other users in a multi-user environment) and communicates his observation to the receiver (decoder) or transmitter (encoder) via an error-free but rate-limited data pipe. This model is, in our opinion, important from a practical perspective since it considers a rate-limited help, unlike some noiseless feedback models that essentially require rate-unlimited and error-free feedback links, which are hardly possible in practice. This rate-limited help was shown in [35], [36], [37], and [38] to provide a channel capacity boost equal to the help rate R_h so that the resulting channel capacity is C_0+R_h; flash signalling (i.e. using high-resolution help infrequently) was shown to be an optimal help strategy, in combination with two-phase time sharing. These results were further extended to other capacity definitions in [39]. Error exponents of Gaussian and modulo-additive channels with rate-limited Tx help were established in [40], where it was also shown that the channel with Tx help is equivalent, in this respect, to the regular (no-help) channel and an additional parallel error-free bit-pipe of rate R_h.

In the present paper, we extend the help setting in [35], [36], [37], and [38] to the memoryless wiretap channel with additive (not necessarily Gaussian) noise under power/amplitude constrains. In the case of Rx help, we show that the same capacity boost as in [36] also holds for the wiretap channel in terms of its weak or strong secrecy capacity C_s: a receiver help of rate R_h results in the capacity boost of R_h,

$$C_s = C_{s0} + R_h, \tag{3}$$

where C_{s0} is the no-help secrecy capacity. This holds for all possible configurations of the SISO Gaussian WTC, i.e. degraded, reversely degraded and non-degraded.[2] Under non-Gaussian noise, this holds for degraded and reversely-degraded configurations and $C_s \geq C_{s0} + R_h$ for non-degraded one, i.e. $C_{s0} + R_h$ is an achievable rate. Some surprising properties are observed. In particular, the secrecy capacity is the same irrespective of whether the help is secure (i.e. unknown to the eavesdropper) or not, so that the secrecy of help does not bring in any increase in the secrecy capacity; this also applies to the case of partially-secure help. For the reversely-degraded channel (where the secrecy capacity is zero without help), we show that the secrecy capacity with Rx help is positive and equal to the help rate, and, under weak secrecy, no wiretap coding is needed to achieve it - burst signaling (along with regular channel coding) is optimal; however, wiretap codes are needed under strong secrecy. Unlike the no-help case, stronger noise at the legitimate receiver can sometimes result in higher secrecy capacity. Surprisingly, the secrecy capacity with Rx

[1] It follows that $C_{sf} = C_{snf} = C_0$ if the feedback rate is sufficiently large, $R_f \geq C_0 - C_{s0}$, i.e. the increase in C_{sf} with R_f saturates at $C_{sf} = C_0$ and further increase in R_f does not bring in any capacity increase so that the rate-unlimited feedback, as in [31], is not necessary to achieve $C_{sf} = C_0$.

[2] While the standard (no help) SISO non-degraded Gaussian WTC is equivalent to either degraded or reversely-degraded one, this is not the case anymore when Rx/Tx help is also available to the Ev.

TABLE I
SUMMARY OF THE RESULTS

Help	WTC	Capacity/rate
Rx	degraded	Theorem 1, Propositions 1, 2
Rx	rev.-degraded	Theorem 2, Proposition 3
Rx	non-degraded	Theorem 3
Tx/Rx	degraded	Theorem 4
Tx/Rx	rev.-degraded	Theorem 5
Tx/Rx	non-degraded	Proposition 4
indep. Tx & Rx	degraded	Theorem 6
indep. Tx & Rx	rev.-degraded	Theorem 7

help, secure or non-secure, is not increased even if the helper is aware of the message being transmitted.

An optimal Tx strategy to achieve C_s in (3) is fundamentally different from those in [30], [31], and [33]: it is a two-phase time sharing whereby no help is used in Phase 1 but just regular (no help) wiretap coding; much shorter Phase 2 makes use of high-resolution help and, under weak secrecy, regular (no Ev) channel coding but no wiretap coding. For the reversely-degraded WTC, Phase 1 is not needed and, therefore, no wiretap coding is needed at all under weak secrecy; burst signaling alone (with regular channel coding) is sufficient. However, wiretap coding is needed in Phase 2 under strong secrecy for all channel configurations but the secrecy capacity itself remains the same as under weak secrecy. Therefore, the choice of the secrecy criterion (weak/strong) affects the complexity of implementation but not the secrecy capacity.

Comparing (3) to (2) with $R_h = R_f$, note that $C_s > C_{sf}$ if the help/feedback rate is sufficiently high, $R_h = R_f > C_0 - C_{s0}$, i.e. the helper setting provides larger secrecy capacity compared to the rate-limited but secure feedback setting, even though the help is not required to be secure. The same applies to (1), where the feedback is rate-unlimited and at least partially-secure. Note also that, unlike C_{sf} in (2), the increase in C_s in (3) with R_h does not saturate.

We further show that, in the case of the degraded or reversely-degraded Gaussian WTC, the same secrecy capacity boost, and hence (3), holds when non-secure help is available to the transmitter, in addition to or instead of the same Rx help, and an optimal signalling is still two-phase time sharing. Thus, if the Tx and Rx help links are identical (carry the same information), then any one can be omitted without affecting the capacity. This is not the case anymore if the help links are independent: in this case, the secrecy capacity boost is the sum of help rates, an optimal signalling is a three-phase time sharing and no help link can be omitted without capacity loss. The main results are summarized in Table I.

While causality is immaterial for Rx help (since the receiver starts decoding after the whole block of symbols is received), it becomes important for the Tx help since the transmitter performs sequential symbol-by-symbol transmission. Therefore, we distinguish between causal and non-causal Tx help. In the latter case, the help is based on the whole noise sequence and is available to the Tx in advance. In the former case, the Tx help at time i is based on the noise sequence up to time i only. Interestingly, the causality of Tx help, unlike that of feedback, has no impact on the secrecy capacity (this property is similar to that of the no-secrecy channel capacity with Tx help in [37]).

Unlike the studies of Gaussian WTCs with noiseless (and hence rate-unlimited) feedback in [30] and [31], our help links are rate-limited, as in [36], [37], and [38], and we also allow here the Ev to have access to the same help as the legitimate Rx or/and Tx (in the case of non-secure help). In our rate-limited setting, causality of help has no impact on the secrecy capacity and, in the case of Rx help, the secrecy capacity is the same for perfectly secure and completely non-secure help (i.e. when exactly the same help is also available to the Ev). Unlike the study in [33], our help link is not required to be secure or causal and the channel is not required to be degraded.

In a related line of work, secure communication with a helper acting as a cooperating jammer was studied in [41] and [42] (this setting is partialy equivalent to an interference channel). However, no secrecy capacity was established but only the generalized degrees of freedom (GDoF), which characterize the high-SNR scaling of the secrecy capacity and are essentially the multiplexing gain in terms of secrecy rates. Unlike [41], [42], the present paper considers no jamming at all; rather, the help comes in a form of rate-limited error-free information about the noise sequence affecting the legitimate Rx, which is available to the Rx and/or Tx.

The rest of the paper is organized as follows. Various configurations (degraded, reversely-degraded and non-degraded) of the WTC with additive (possibly non-Gaussian) noise and Rx help are considered in Sections II to IV and their secrecy capacities are established in Theorems 1 - 3 and Propositions 1-3. The case of Tx help, instead of or in addition to the Rx help, is studied in Sections V - VIII and the respective secrecy capacities are established/characterized in Theorems 4 - 7 and Proposition 4, including the same and independent Tx/Rx help links, and the case of correlated Rx and Ev noises.

Notations: we follow the standard notations as much as possible, where random variables and their realizations are denoted by capital and lower case letters, respectively, and their alphabets follow from the respective channel models; X^n denotes the sequence $(X_1, \ldots, X_n)$; $H(\cdot)$, $h(\cdot)$ and $h(\cdot|\cdot)$ are the entropy, differential and conditional differential entropies, respectively, and $I(\cdot;\cdot)$ is the mutual information; $\mathbb{E}\{\cdot\}$ and $\Pr\{\cdot\}$ are statistical expectation and probability with respect to relevant random variables; $X - Y - Z$ denotes a Markov chain of random variables X, Y, and Z.

II. Degraded Wiretap Channel With Rx Help

We begin with the real-valued degraded (discrete-time) wiretap channel with additive noise:

$$Y_i = X_i + W_i,\ Z_i = Y_i + V_i,\ i = 1, \ldots, n \qquad (4)$$

where X_i is the real-valued transmitted symbol at time i, W_i, V_i are Rx and Ev noises, which are zero-mean, possibly non-Gaussian, independent of each other, with variances σ_W^2 and σ_V^2, respectively, see Fig. 1. The channel is stationary and memoryless, so that W^n and V^n are i.i.d. sequences.

We further assume that the differential entropies of W_i and V_i are finite and that $0 < \sigma_W^2,\ \sigma_V^2 < \infty$ (unless stated otherwise). In the case of Gaussian noise V, the finiteness of its differential entropy, $|h(V)| < \infty$, is equivalent to $0 < \sigma_V < \infty$. In the case of non-Gaussian noise W, we assume that it satisfies the following conditions:

$$\mathbb{E}\{|W|^{2+\delta}\} < \infty \text{ for some } \delta > 0$$
$$\alpha_W = \int_{-\infty}^{\infty} p_W(w)^{1/3} dw < \infty \tag{5}$$

where $p_W(w)$ is the probability density function of W. This will guarantee the existence of a high-resolution quantizer with sufficiently small quantization error, see Theorem 3 in [37]. In the case of Gaussian noise, these conditions are satisfied.

The helper model is as in [36], [37], and [38] but extended to the WTC setting, whereby discrete help $T = T(W^n)$ of rate $n^{-1}H(T) \leq R_h < \infty$ is available to the Rx and Ev (no further constraints on the helper function $T(W^n)$ are assumed, beyond its rate, unless stated otherwise), which we term "non-secure Rx help", so that the Rx and the Ev can estimate transmitted message M using T and their respective received signals Y^n and Z^n. This falls into the framework of cooperative communications or communications with side information [34] and models practical links, which are always rate-limited (albeit the rate can be high, as in e.g. optical fiber links). If no help is available to the Ev, we call it "secure Rx help". For Rx help, the difference between causal and non-causal help is immaterial, since the Rx waits until the whole block of length n is received before decoding it.

We use the standard definition of the secrecy capacity as the supremum of all achievable secrecy rates, subject to the reliability, secrecy and power constraints, see e.g. [1], [2], [3], [4], [8], [9], and [10]. In particular, the (secret) message M is selected randomly and uniformly from $\{1, \ldots, 2^{nR_s}\}$, where R_s is a secrecy rate and n is the blocklength. The Tx encoder maps it into X^n and the Rx decoder maps Y^n and the available help T into a message estimate $\hat{M}$. The constraints are as follows:

Reliability Constraint: the error probability $P_e \triangleq \Pr\{M \neq \hat{M}\} \leq \varepsilon$ for any $\varepsilon > 0$ and sufficiently large n.

Weak Secrecy Constraint: information leakage rate (to the Ev) R_l satisfies

$$R_l \triangleq n^{-1} I(M; Z^n T) \leq \delta \tag{6}$$

for any $\delta > 0$ and sufficiently large n; T is omitted in the case of secure help. Strong secrecy criterion will also be considered, see (44).

Power constraint: under the average power constraint,

$$\frac{1}{n}\sum_{i=1}^{n} \mathbb{E}\{X_i^2\} \leq P \tag{7}$$

We further assume that $0 < P < \infty$ (if $P = 0$, the capacity is, of course, zero). Our results will also hold under the peak power constraint, $\mathbb{E}\{X_i^2\} \leq P$ for each i, as well as the amplitude constraint $|X_i| \leq \sqrt{P}$. More general power constraints can also be considered,[3] as in [35].

[3]The ideas to consider non-Gaussian noise and various power/amplitude constraints were suggested by anonymous reviewers.

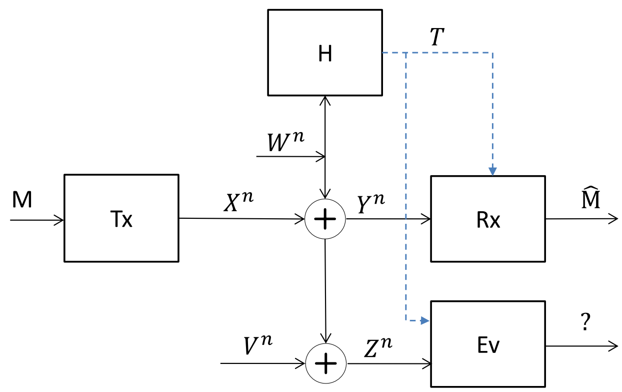

Fig. 1. Degraded wiretap channel with additive noises and a rate-limited help T at the Rx and Ev (if the help is not secure). W^n and V^n are i.i.d. noise sequences independent of each other and of M, X^n; $X^n = X^n(M)$, $T = T(W^n)$, $H(T) \leq nR_h$.

The secrecy capacity of this channel with Rx help is established below.

Theorem 1: Consider the degraded memoryless WTC with additive, possibly non-Gaussian noises and with secure or non-secure Rx help of rate R_h, under any of the above power/amplitude constraints. Let $0 < \sigma_V^2, P < \infty$ and, in the case of non-Gaussian noises, $h(V) > -\infty$ and (5) to hold. Its (weak) secrecy capacity C_s is

$$C_s = C_{s0} + R_h \tag{8}$$

where C_{s0} is the secrecy capacity without help.

Proof: Converse: For the converse, we consider the case of secure Rx help T (not available to the Ev); the case of non-secure help will follow since the availability of help to the Ev cannot increase secrecy rate. The converse is based on the following chain of inequalities, incorporating the secrecy and reliability constraints as well as functional relationships between various random variables in the channel model:

$$\begin{aligned}
nR_s &= H(M) \\
&= H(M|Z^n) + I(M;Z^n) && (9)\\
&\leq H(M|Z^n) + n\epsilon && (10)\\
&= H(M|Z^n) - H(M|Y^nT) + H(M|Y^nT) + n\epsilon && (11)\\
&\leq H(M|Z^n) - H(M|Y^nT) + 2n\epsilon && (12)\\
&\leq H(M|Z^n) - H(M|Y^nZ^nT) + 2n\epsilon && (13)\\
&= I(M;Y^nT|Z^n) + 2n\epsilon && (14)\\
&\leq I(X^n;Y^nT|Z^n) + 2n\epsilon && (15)\\
&= I(X^n;Y^n|Z^n) + I(X^n;T|Y^nZ^n) + 2n\epsilon && (16)\\
&\leq I(X^n;Y^n|Z^n) + H(T) + 2n\epsilon && (17)\\
&\leq nI_0(X;Y|Z) + nR_h + 2n\epsilon && (18)\\
&= n(I_0(X;Y) - I_0(X;Z) + R_h + 2\epsilon) && (19)\\
&\leq n(C_{s0} + R_h + 2\epsilon) && (20)
\end{aligned}$$

where (10) follows from the secrecy constraint $I(M;Z^n) \leq n\epsilon$; (12) follows from Fano inequality (due to the reliability constraint) $H(M|Y^nT) \leq n\epsilon$; (15) follows from Markov chain $M - X^n - Y^nT - Z^n$; (17) follows from

$I(X^n;T|Y^nZ^n) \leq H(T)$; (18) follows from

$$I(X^n;Y^n|Z^n) \leq \sum_{i=1}^{n} I(X_i;Y_i|Z_i) \leq nI_0(X;Y|Z) \quad (21)$$

where the first inequality holds since the channel is memoryless and the second one is due to the concavity of the mutual information in the input distribution [8], [9]; I_0 is the mutual information induced by input X with the distribution $p_0(x) = n^{-1}\sum_i p_{x_i}(x)$, where $p_{x_i}(x)$ is the distribution of X_i; (19) follows from Markov chain $X - Y - Z$ and (20) follows from [29, Theorem 3] (applied to a single-state channel). Thus,

$$R_s \leq C_{s0} + R_h + 2\epsilon \quad (22)$$

Since this holds for any $\epsilon > 0$, it follows that $R_s \leq C_{s0} + R_h$. This establishes the converse with secure Rx help. Since the presence of help at Ev cannot increase secrecy rate, the same upper bound applies with non-secure Rx help. Note that no assumption of Gaussian noise is made in the above proof.

Achievability. To prove achievability, we combine the regular (no help) wiretap coding with the no-Ev flash signaling in [36]. We consider first the case of non-secure Rx help (when the same help is available at the Rx and Ev), from which achievability with secure Rx help follows. To this end, recall that the ordinary (no Ev) flash signaling with Rx help consists of two phases of time-sharing [35], [36]:

- Phase 1: no help is used at all for a fraction $(1-\tau)$ of the time, which achieves, with regular channel coding, a rate arbitrary close to the ordinary channel capacity C for a sufficiently large blocklength.
- Phase 2: Rx help is used at rate R_h/τ for a (very small) fraction τ of the time. In this phase, in addition to regular channel coding, a high-resolution scalar quantization (with $\lfloor 2^{R_h/\tau} \rfloor$ levels) of each noise sample is provided to the Rx, so that the help is $T = \hat{W}^n$, where $\hat{W}_i = Q(W_i)$ and $Q(\cdot)$ is a scalar quantizer. The Rx subtracts $\hat{W}_i$ from its received signal Y_i and, after receiving the whole block, decodes it using nearest-neighbour decoding; for sufficiently large blocklength, this achieves a rate arbitrarily close to

$$h(X) - \frac{1}{2}\log(2\pi e \sigma_W^2) + \frac{R_h}{\tau} = \frac{R_h}{\tau}(1 + o(1)) \quad (23)$$

  where $o(1) \rightarrow 0$ as $\tau \rightarrow 0$, see [36, eq. (20)], and $h(X) > -\infty$ for some i.i.d. input X satisfying the power/amplitude constraints. We silently assume here that τ is sufficiently small so that the rate in (23) is positive, which is consistent with $\tau \rightarrow 0$ in the next step. An alternative Phase 2 strategy, which maximizes error exponents using a simple lattice code with a uniform scalar quantizer (no need for i.i.d.-generated codebooks), can be found in [40].

Overall, as $\tau \rightarrow 0$, the rate achieved after two-phase time-sharing is arbitrarily close to

$$(1-\tau)C + \tau R_h/\tau(1 + o(1)) \rightarrow C + R_h \quad (24)$$

which is the channel capacity with Rx help. This also implies that providing high-resolution help infrequently ("flash signalling") is optimal.

To accommodate the Ev and the secrecy constraint, we modify this strategy as follows:

- Phase 1: use the regular WTC coding with no help [1], [2], [3], [4], [8], [9], [11] for the fraction $(1-\tau)$ of the time; this achieves a secrecy rate R_s arbitrarily close to the regular WTC secrecy capacity C_{s0}: $R_s = C_{s0} - \epsilon$ for any $\epsilon > 0$ and sufficiently large blocklength.
- Phase 2: for the small fraction τ of the time, use no WTC coding but ordinary channel coding under the flash signaling as above.

While it is clear that secrecy is guaranteed during Phase 1 (via wiretap coding), it is also clear that secrecy is not guaranteed during Phase 2 (since no wiretap coding is used) so it is not clear whether secrecy is guaranteed overall (after time sharing). To demonstrate that this is indeed the case, we show that, during Phase 2, the information leakage rate R_{l2} to the Ev is uniformly bounded,

$$R_{l2} \leq R_0 < \infty \quad (25)$$

for any τ and some R_0, where R_0 is independent of τ (but where R_{l2} may depend on τ), so that the overall leakage rate R_l (after the time sharing) is

$$R_l = (1-\tau)R_{l1} + \tau R_{l2} \leq (1-\tau)\delta + \tau R_0 \rightarrow \delta \quad (26)$$

as $\tau \rightarrow 0$, for any $\delta > 0$ (or, equivalently, $R_l \leq 2\delta$ for sufficiently small τ, $\tau \leq \delta/R_0$), where $R_{l1} \leq \delta$ is the information leakage rate during Phase 1.

To see that indeed $R_{l2} \leq R_0 < \infty$ uniformly in τ, note the following:

$$\begin{aligned} R_{l2} &= n^{-1}I(M_2;Z^n\hat{W}^n|\mathcal{C}) && (27)\\ &\leq n^{-1}I(M_2;Z^n\hat{W}^nW^n|\mathcal{C}) && (28)\\ &= n^{-1}I(M_2;Z^n|W^n\mathcal{C}) && (29)\\ &\leq n^{-1}I(X^n;Z^n|W^n\mathcal{C}) && (30)\\ &= n^{-1}I(X^n;X^n+W^n+V^n|W^n\mathcal{C}) && (31)\\ &= n^{-1}I(X^n;X^n+V^n|\mathcal{C}) && (32)\\ &\leq n^{-1}(h(X^n+V^n)-h(V^n)) && (33)\\ &= h(X+V)-h(V) && (34)\\ &\leq \frac{1}{2}\log\left(2\pi e(P+\sigma_V^2)\right)-h(V) = R_0 < \infty && (35) \end{aligned}$$

where M_2 is a message sent in Phase 2, X^n is a codeword (which depends on M_2, see Fig. 1), and the conditioning is on an i.i.d. randomly-generated codebook $\mathcal{C}$ (the codebook generation, encoding and decoding are as in [36]); (29) follows from independence of M_2 and $W^n, \hat{W}^n$ and from $\hat{W}_i = Q(W_i)$; (30) follows from the Markov chain $M_2 - X^n - Z^nW^n$; (32) follows from independence of W^n and X^n, V^n; (34) follows since X^n and V^n are i.i.d. sequences; the first inequality in (35) follows from the fact that Gaussian distribution maximizes differential entropy under the constrained variance and the last inequality is due to $h(V) > -\infty$ and $P, \sigma_V^2 < \infty$.

Hence, arbitrary low information leakage rate is guaranteed after time sharing with $\tau \rightarrow 0$, which satisfies the secrecy constraint. At the same time, the overall secrecy rate (after time sharing) is

$$(1-\tau)(C_{s0}-\epsilon)+\tau R_h/\tau(1+o(1)) \rightarrow C_{s0}+R_h-\epsilon \quad (36)$$

for any $\epsilon > 0$, as $\tau \rightarrow 0$, so that the secrecy capacity is $C_{s0}+R_h$, as required.

In the above secrecy analysis, we assume that the help is not secure, i.e. it is available to the Ev. Clearly, the secrecy constraint is also satisfied if the help is secure, i.e. not available to the Ev (since the lack of Ev help cannot increase leakage rate), and an achievable secrecy rate remains the same. Since the converse also holds for the secure Rx help, the secrecy capacity also remains the same, regardless whether help is secure or not, i.e. the secrecy of help does not increase the secrecy capacity.

Also note that both the converse and achievability hold under the same power constraint as the no-help secrecy capacity C_{s0} (this is ensured by enforcing the power constraint in each phase and, therefore, after the time sharing as well). In particular, they hold under the average/peak power or/and amplitude constraint(s), or any combination of the above (with C_{s0} being the no-help secrecy capacity under the same constraints). □

It is worthwhile to note that flash signaling with Rx help provides here the same boost in the secrecy capacity as in the regular (no Ev) channel capacity in [36], i.e. the $+R_h$ boost comes with secrecy for free in the degraded WTC. This holds even if noises are not Gaussian and also under various power constraints.

Note from (8) that

$$C_s \approx R_h \text{ if } C_{s0} \ll R_h \quad (37)$$

and, from the achievability proof, this is achievable with Phase 2 alone (no Phase 1), i.e. burst signaling over very short time. Under weak secrecy, no wiretap code is needed in this case (just a regular channel code), i.e. it is a remarkably simple strategy whereby secrecy is ensured by sending a secret message over a very short interval of time without any further protection against eavesdropping. This strategy may be attractive for low-complexity devices (e.g. IoT). The next Section will demonstrate that it is optimal for the reversely-degraded WTC.

Since C_s in Theorem 1 is the same for secure and non-secure help, i.e. the secrecy of help does not bring in any capacity advantage, it also applies to the case of partially-secure help, i.e. when the Ev has access to a part of T.

Surprisingly, even if the helper H is aware of the message M being transmitted, i.e. $T=T(W^n,M)$ as in Fig. 2, the secrecy capacity is not affected and Theorem 1 still holds.

Proposition 1: Consider the degraded WTC with Rx help as in Theorem 1 and let the helper H be aware of the message being transmitted, i.e. $T=T(W^n,M)$ as in Fig. 2. Then, Theorem 1 still holds.

Proof: It is sufficient to show that the same converse still holds (for achievability, the helper can always ignore the message). To this end, note that (10) - (14) still hold since the

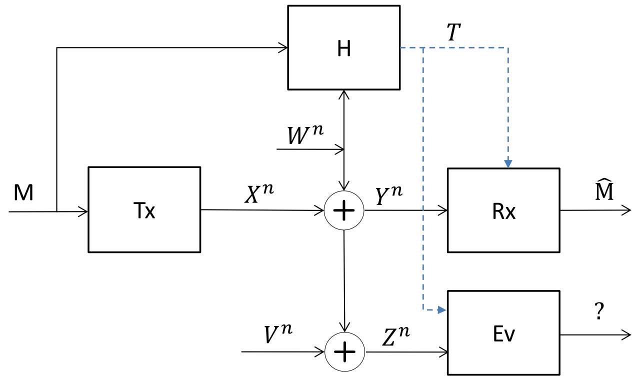

Fig. 2. The degraded WTC of Fig. 1 when the helper H is aware of the message M being sent, $T=T(W^n,M)$.

independence of T and M plays no role there so that

$$\begin{aligned} nR_s &\leq I(M;Y^nT|Z^n)+2n\epsilon \\ &\leq I(X^nM;Y^nT|Z^n)+2n\epsilon && (38)\\ &= I(X^nM;Y^n|Z^n)+I(X^nM;T|Y^nZ^n)+2n\epsilon && (39)\\ &\leq I(X^nM;Y^n|Z^n)+H(T)+2n\epsilon && (40)\\ &= I(X^n;Y^n|Z^n)+H(T)+2n\epsilon && (41)\\ &\leq n(C_{s0}+R_h+2\epsilon) && (42)\end{aligned}$$

where (41) is due to $I(M;Y^n|X^nZ^n)=0$, i.e., the independence of M and Y^n given X^n and Z^n; (42) follows from (18)-(20). □

For the degraded Gaussian WTC with non-secure Rx help, the secrecy capacity is zero if $\sigma_V^2=0$, since the Ev has access to the same information as the Rx in this case, so no secrecy is possible. This implies that $C_s(\sigma_V^2)$ is a discontinuous function at $\sigma_V^2=0$ for non-secure help with any $R_h>0$:

$$\lim_{\sigma_V^2\rightarrow 0^+} C_s(\sigma_V^2)=R_h>0, \quad (43)$$

while $C_s(0)=0$ (the help becomes useless in this case). This is in stark contrast to the no-help case where $C_{s0}(\sigma_V^2)$ is a continuous function for every σ_V^2, including $\sigma_V^2=0$, so that the help becomes especially important when σ_V^2 approaches 0, i.e., when the Tx-Ev link SNR approaches that of the Tx-Rx link.

A. From Weak to Strong Secrecy

While Theorem 1 and Proposition 1 were established under the weak secrecy criterion in (6) (which may be considered as too weak for certain applications), the same results also hold under the strong secrecy criterion,[4] whereby information leakage (not rate) to the Ev satisfies

$$I(M;Z^nT)\leq\delta \quad (44)$$

for any $\delta>0$ and sufficiently large n, where T is omitted in the case of secure help.

[4]The idea to extend the weak secrecy results to strong secrecy was suggested by the Associate Editor (M. Bloch).

Proposition 2: The (weak) secrecy capacity in Theorem 1 and Proposition 1 also hold under the strong secrecy criterion in (44).

Proof: First, note that the converse established in Theorem 1 and Proposition 1 also holds under strong secrecy (where C_{s0} is the no-help strong secrecy capacity). To establish achievability, note that Phase 1 needs no modification, since it involves no help and the standard strong secrecy capacity result applies. However, Phase 2 does need a modification since the simple (no wiretap code) strategy cannot guarantee strong secrecy, even after $\tau \to 0$. To this end, we use the same signaling as in Phase 2 of Theorem 1 but combined with a wiretap code. To determine an achievable strong secrecy rate for this phase, consider an equivalent channel, whereby the legitimate Tx-Rx link is $X - (Y, \hat{W})$ and, under non-secure help, the Ev link is $X - (Z, \hat{W})$. The strong secrecy capacity C_{se} of this equivalent channel is lower bounded, from [29, Theorem 3] applied to a single-state channel, as follows:

$$C_{se} \geq \sup_X [I(X;Y\hat{W}) - I(X;Z\hat{W})] \geq I(X;Y\hat{W}) - I(X;Z\hat{W}) \quad (45)$$

so that an achievable strong secrecy rate R_{s2} is

$$R_{s2} = I(X;Y\hat{W}) - I(X;Z\hat{W}) - \epsilon \quad (46)$$

for arbitrary-small $\epsilon > 0$, where negative value is interpreted as zero rate and first term is just the rate of the legitimate link, which is lower-bounded as in (23),

$$I(X;Y\hat{W}) \geq \frac{R_h}{\tau}(1 + o(1)) \quad (47)$$

Second term can be upper bounded as follows:

$$I(X;Z\hat{W}) \leq I(X;ZW) = I(X;Z|W) = I(X;X+V) = h(X+V) - h(V) \leq R_0 < \infty \quad (48)$$

where R_0 is as in (35). Combining (46)-(48), we obtain an achievable strong secrecy rate of Phase 2:

$$R_{s2} \geq \frac{R_h}{\tau}(1 + o(1)) - R_0 - \epsilon = \frac{R_h}{\tau}(1 + o(1)) \quad (49)$$

and using it in the time-sharing strategy in (36), the desired result follows. □

Thus, while imposing the strong secrecy criterion instead of the weak one does not alter the secrecy capacity, it does increase the complexity of Phase 2 (due to the use of wiretap codes).

III. Reversely-Degraded WTC With Rx Help

Let us now consider the reversely-degraded case of the wiretap channel as in Fig. 3:

$$Z_i = X_i + V_i, \ Y_i = Z_i + \Delta W_i \quad (50)$$

where ΔW_i is an extra Rx noise, independent of the Ev noise V_i, so that the sequences V^n and ΔW^n are i.i.d and independent of each other. Note that the total Rx noise is $W_i = V_i + \Delta W_i$ and its variance is

$$\sigma_W^2 = \sigma_V^2 + \sigma_{\Delta W}^2 \geq \sigma_V^2 > 0 \quad (51)$$

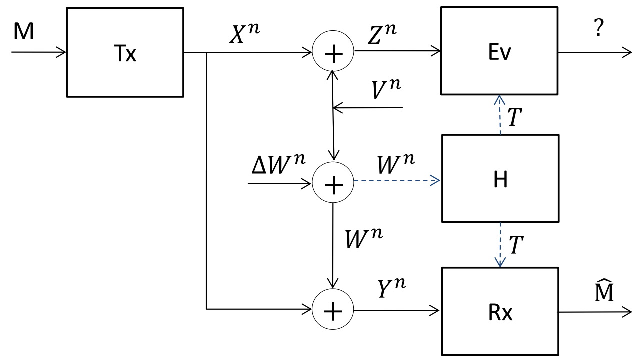

Fig. 3. Reversely-degraded wiretap channel with additive noises (not necessarily Gaussian) and a rate-limited Rx help T. ΔW^n and V^n are i.i.d. noise sequences independent of each other and of M, X^n; $X^n = X^n(M)$, $T = T(W^n)$, $H(T) \leq nR_h$.

We exclude the trivial case $\sigma_V^2 = 0$, for which the secrecy capacity is zero, and further assume that both noises have finite differential entropies, $|h(V_i)|, |h(\Delta W_i)| < \infty$, and that $\sigma_W^2 < \infty$. In the case of non-Gaussian noise W, we also assume that the conditions in (5) are satisfied. It is well-known that, without help, the secrecy capacity of this channel is zero, $C_{s0} = 0$. However, the availability of Rx help, whether or not securely, changes the situation dramatically.

Theorem 2: Consider the reversely-degraded WTC with additive (not necessarily Gaussian) noise, as introduced above, with secure or non-secure Rx help of rate R_h. Its weak or strong secrecy capacity is

$$C_s = R_h \quad (52)$$

If $\sigma_{\Delta W}^2 = 0$, then $C_s = R_h$ if the help is secure and $C_s = 0$ otherwise.

Proof: Converse: to prove the converse, we consider the case of secure Rx help (i.e. no Ev help) and weak secrecy. The case of non-secure help or strong secrecy will follow, since the availability of help to the Ev cannot increase the secrecy rate and since the strong secrecy capacity cannot exceed the weak one. The proof follows the steps similar to those in Theorem 1. In particular, we observe that (10)-(17) still hold for the reversely-degraded channel (since channel degradedness plays no role there), so that

$$nR_s \leq I(X^n;Y^n|Z^n) + H(T) + 2n\epsilon \quad (53)$$
$$\leq n(R_h + 2\epsilon), \quad (54)$$

where the last inequality is due to $I(X^n;Y^n|Z^n) = 0$, which in turn follows from Markov chain $X^n - Z^n - Y^n$. Thus, $R_s \leq R_h + \epsilon$ for any $\epsilon > 0$ and therefore $R_s \leq R_h$, as required.

Achievability: to prove achievability under weak secrecy, we consider the case of non-secure Rx help (when the same help is also available to the Ev); the case of secure help will follow since the absence of help to the Ev cannot increase leakage rate and hence cannot decrease secrecy rate.

To this end, we use the same two-phase flash signaling as in Theorem 1 except that nothing is transmitted in Phase 1 and the whole message is transmitted in Phase 2 (without wiretap coding). To show that this provides an arbitrary-low leakage rate after time-sharing (which is equivalent to burst signaling of duration τ in this case), we show that the Phase 2 leakage rate R_{l2} is uniformly bounded in τ (as before). To this end, observe that

$$\begin{aligned}
R_{l2} &= n^{-1} I(M_2; Z^n \hat{W}^n | \mathcal{C}) && (55)\\
&\leq n^{-1} I(M_2; Z^n \hat{W}^n W^n | \mathcal{C}) && (56)\\
&= n^{-1} I(M_2; Z^n | W^n \mathcal{C}) && (57)\\
&\leq n^{-1} I(X^n; Z^n | W^n \mathcal{C}) && (58)\\
&= n^{-1} I(X^n; X^n + V^n | V^n + \Delta W^n, \mathcal{C}) && (59)\\
&= n^{-1} (h(X^n + V^n | V^n + \Delta W^n, \mathcal{C}) && (60)\\
&\quad - h(V^n | X^n, V^n + \Delta W^n, \mathcal{C})) &&\\
&\leq n^{-1} (h(X^n + V^n) - h(V^n | V^n + \Delta W^n) && (61)\\
&= h(X + V) - h(V) - h(\Delta W) + h(V + \Delta W) && (62)\\
&\leq \frac{1}{2} \log(2\pi e (P + \sigma_V^2)) + \frac{1}{2} \log(2\pi e \sigma_W^2) && (63)\\
&\quad - h(V) - h(\Delta W) &&\\
&= R_0 < \infty && (64)
\end{aligned}$$

where we assumed that $\sigma_{\Delta W}^2 > 0$; (55)-(58) hold due to the same reasons as in the proof of Theorem 1; (61) holds since (i) conditioning cannot increase the entropy and (ii) $V^n, \Delta W^n$ are independent of $X^n, \mathcal{C}$; (62) holds since

$$\begin{aligned}
&h(V^n | V^n + \Delta W^n)\\
&\quad = h(V^n, V^n + \Delta W^n) - h(V^n + \Delta W^n) && (65)\\
&\quad = h(V^n) + h(\Delta W^n) - h(V^n + \Delta W^n) && (66)\\
&\quad = n(h(V) + h(\Delta W) - h(V + \Delta W)) && (67)
\end{aligned}$$

where (66) is due to the independence of ΔW^n and V^n; (63) holds since Gaussian distribution maximizes differential entropy under bounded variance; the inequality in (64) holds since all terms in (63) are bounded. Thus, the total leakage rate (after time-sharing) is

$$\begin{aligned}
R_l &= (1 - \tau) 0 + \tau R_{l2} && (68)\\
&\leq \tau R_0 \to 0 && (69)
\end{aligned}$$

when $\tau \to 0$, as required (notice that the condition $\sigma_{\Delta W}^2 > 0$ is essential here, as $\sigma_{\Delta W}^2 = 0$ results in zero secrecy capacity for non-secure help). The overall secrecy rate (after time-sharing) is

$$R_s = (1 - \tau) 0 + \tau R_h / \tau (1 + o(1)) \to R_h \qquad (70)$$

when $\tau \to 0$.

Let us now consider the case of $\sigma_{\Delta W}^2 = 0$, which implies $Y^n = Z^n$. If the help is not secure, the same information is available to the Ev and Rx and hence no positive secrecy rate is achievable, $C_s = 0$. However, if the help is secure, then the Rx has an extra information not available to the Ev. It is not difficult to see that the above converse still holds if $\sigma_{\Delta W}^2 = 0$. To prove achievability, we use the same signaling as above and show that the leakage rate R_{l2} of Phase 2 is uniformly bounded:

$$\begin{aligned}
R_{l2} &= n^{-1} I(M_2; Z^n | \mathcal{C}) && (71)\\
&\leq n^{-1} I(X^n; Z^n | \mathcal{C}) && (72)\\
&\leq n^{-1} (h(Z^n) - h(V^n)) && (73)\\
&= h(X + V) - h(V) && (74)\\
&\leq \frac{1}{2} \log(2\pi e (P + \sigma_V^2)) - h(V) = R_0 < \infty && (75)
\end{aligned}$$

Thus, secrecy is guaranteed after time-sharing with $\tau \to 0$ and the achieved secrecy rate is as in (70).

One can further show, using the same arguments as in Proposition 2 but without Phase 1 (since $C_{s0} = 0$ in this case), that the rate in (70) is also achievable under strong secrecy if wiretap codes are used in Phase 2. In particular, (46) - (47) do hold under the present configuration and (48) is replaced by

$$\begin{aligned}
I(X; Z\hat{W}) &\leq I(X; ZW) = I(X; Z | W)\\
&= I(X; X + V | V + \Delta W)\\
&\leq h(X + V) - h(V | V + \Delta W)\\
&\leq R_0 < \infty && (76)
\end{aligned}$$

where R_0 is as in (64) so that (49) does hold under strong secrecy and, hence, the desired result follows. □

It may feel counter-intuitive that $C_s = R_h > 0$ for the reversely-degraded WTC, even if the help is not secure, i.e. also available to the Ev, since, in this case, the Ev is getting more information than the Rx. However, one should also note that, even though the Ev has the right (public) "key" $T = \hat{W}^n$, it does not have the right "lock" W^n to which this key applies and hence it cannot "unlock" it (i.e., cancel its own noise), unlike the legitimate Rx.

A related surprising observation follows from Theorem 2: in the case of non-secure help, $C_s = 0$ if $\sigma_W^2 = \sigma_V^2$ (i.e. $\sigma_{\Delta W}^2 = 0$) but $C_s = R_h > 0$ if $\sigma_W^2 > \sigma_V^2$, so that more noise at the legitimate Rx is actually better for secrecy in this case. This is due to the fact that the extra Rx noise $\Delta W_i \neq 0$ makes it impossible for the Ev to cancel its own noise using non-secure help $\hat{W}^n$ in the same way the Rx does (since $V_i \neq W_i$ in this case). However, if $\Delta W_i = 0$, then the Ev can do noise cancellation in the same way the Rx does, which results in $C_s = 0$ and renders the help useless. This also implies that $C_s(\sigma_W^2)$ is a discontinuous function at $\sigma_W^2 = \sigma_V^2$.

To summarize, the weak or strong secrecy capacity C_s of the degraded or reversely degraded wiretap channel with Rx help of rate R_h (secure or not) is given by

$$C_s = C_{s0} + R_h \qquad (77)$$

if either $\sigma_W^2 \neq \sigma_V^2$ or else the help is secure, where, of course, $C_{s0} = 0$ for the reversely-degraded case. Thus, not only the secrecy capacity is boosted by R_h for the degraded case, but also the secrecy capacity is positive for the reversely-degraded case, where it is zero without help, and, under weak secrecy, this capacity is achievable by burst signalling without any wiretap coding at all. Therefore, the choice of the secrecy criterion (weak/strong) does not affect the capacity but only the complexity of implementation: while weak secrecy does not require wiretap coding, strong secrecy does require a strong enough wiretap code for Phase 2 (the only active phase for the reversely-degraded WTC).

Similarly to the degraded WTC, Theorem 2 still holds even if the helper H is aware of the message M being transmitted, $T = T(W^n, M)$, so that there is no boost in the secrecy capacity due to the message being available to the helper.

Proposition 3: Consider the reversely-degraded WTC with Rx help as in Theorem 2 and let the helper H be aware of the message being transmitted, i.e. $T = T(W^n, M)$. Then, Theorem 2 still holds.

Proof: The converse follows since (53), (54) still hold for $T = T(W^n, M)$. The achievability holds since the helper can always ignore the message. □

IV. Non-Degraded WTC With Rx Help

Let us now consider the case where the channel is neither degraded nor reversely-degraded, as in Fig. 4:

$$Z_i = X_i + V_i,\ Y_i = X_i + W_i \tag{78}$$

where the noise sequences V^n and W^n are i.i.d but possibly non-Gaussian and correlated with each other; the covariance matrix of (W_i, V_i) is

$$\begin{aligned} \boldsymbol{R}_{WV} &= \mathbb{E}(W_i, V_i)(W_i, V_i)' \\ &= \begin{bmatrix} \sigma_W^2 & r\sigma_W\sigma_V \\ r\sigma_W\sigma_V & \sigma_V^2 \end{bmatrix} \end{aligned} \tag{79}$$

where r is the normalized correlation coefficient, $|r| \le 1$, and $(\cdot)'$ means transposition. This correlation may be due to e.g. an external user's signal acting as the noise affecting the Rx and Ev. We further assume that its covariance matrix is not singular, i.e. the determinant $|\boldsymbol{R}_{WV}| \neq 0$, which is equivalent to $|r| < 1$. If $r = 0$ and noises are Gaussian, then V^n and W^n are independent of each other.

For Gaussian noise, it is well-known that, without help, this non-degraded WTC can be equivalently reduced to either degraded or reversely-degraded one, since the Rx and Ev performance depends on the marginal distributions of W^n and V^n, respectively, not on their joint distribution [1]. While this is still true for secure Rx help (no Ev help), it is no longer true for non-secure help since Ev performance now depends on both V^n and W^n. Thus, the secrecy capacity of this channel can potentially be affected by correlation and does not follow from that of the degraded or reversely-degraded one. Yet, we show below that it is still $C_{s0} + R_h$, irrespective of r (as long as $|r| < 1$). For non-Gaussian noise, this becomes a lower bound (since we are not able to establish the converse in this case).

Theorem 3: Consider the non-degraded WTC as in Fig. 4 with i.i.d. (not necessarily Gaussian) noise sequences correlated with each other as in (79) and with secure or non-secure Rx help of rate R_h; let $0 < \sigma_W^2, \sigma_V^2, P < \infty$ and $h(W, V) > -\infty$. Its weak or strong secrecy capacity C_s is lower-bounded as

$$C_s \ge C_{s0} + R_h \tag{80}$$

and this holds with equality if noises are Gaussian and $|r| < 1$.

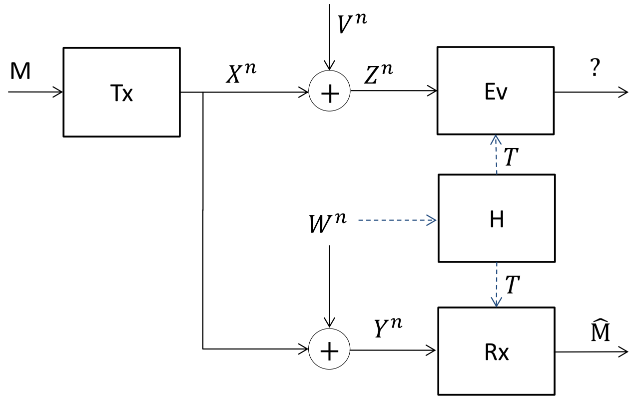

Fig. 4. Non-degraded wiretap channel with additive noises and a rate-limited Rx help T; noise sequences W^n and V^n are i.i.d. (but possibly correlated with each other and non-Gaussian) and independent of M, X^n; $\sigma_W^2, \sigma_V^2 > 0$; $h(W, V) > -\infty$; $X^n = X^n(M)$, $T = T(W^n)$, $H(T) \le nR_h$.

Proof: *Converse:* to establish the converse, we assume that the noises are Gaussian and consider first the case of secure Rx help (no Ev help). Note that, in this case, Ev's performance depends on V^n only, not on W^n; likewise, Rx's performance depends on W^n only, not on V^n. Hence, this channel can now be equivalently reduced to degraded or reversely-degraded case, for which the converse have been established in Theorem 1 or 2, respectively, so that $R_s \le C_{s0} + R_h$ under both strong and weak secrecy. This argument does not apply for non-secure Rx help. However, since the availability of help to Ev cannot increase the secrecy rate, the same upper bound still holds. This establishes the converse for non-secure Rx help as well.

Achievability: To prove achievability under weak secrecy, we do not assume that noises are Gaussian and use the same two-phase signaling as in Theorem 1; if $C_{s0} = 0$, no Phase 1 is needed. Since Phase 1 makes no use of help, its maximum achievable secrecy rate is C_{s0}. On the other hand, Phase 2 rate in (23) is not affected by noise correlation since it depends on W^n only (not on V^n) so that, after time sharing, the weak secrecy rate is as in (36). To show that weak secrecy is guaranteed after the two-phase time sharing, we show that the leakage rate R_{l2} of Phase 2 is uniformly bounded for any τ:

$$\begin{aligned} R_{l2} &= n^{-1} I(M_2; Z^n \hat{W}^n | \mathcal{C}) && (81)\\ &\le n^{-1} I(M_2; Z^n W^n | \mathcal{C}) && (82)\\ &\le n^{-1} I(X^n; Z^n W^n) && (83)\\ &\le I_0(X; ZW) && (84)\\ &= h(X+V, W) - h(V, W) && (85)\\ &\le h(X+V) + h(W) - h(V, W) && (86)\\ &\le \frac{1}{2}\log\left(2\pi e(P+\sigma_V^2)\right) + \frac{1}{2}\log\left(2\pi e\sigma_W^2\right) - h(V, W) && (87)\\ &= R_0 < \infty && (88) \end{aligned}$$

where (83) follows from Markov chain $(\mathcal{C}, M_2) - X^n - (Z^n, W^n)$; (84) holds since the channel is memoryless; (87) holds since Gaussian distribution maximizes differential entropy and (88) holds since all terms in (87) are finite. In the case of Gaussian noise, $h(V, W) > -\infty$ is equivalent to $|r| < 1$, since

$$h(W,V) = \frac{1}{2}\log\left((2\pi e)^2|\boldsymbol{R}_{WV}|\right) = \frac{1}{2}\log\left((2\pi e)^2\sigma_W^2\sigma_V^2(1-r^2)\right) \quad (89)$$

Thus, the overall leakage rate after two-phase time sharing is arbitrarily low, as in (26), and the weak secrecy rate in (36) is indeed achievable, as required.

To show that the same secrecy rate is achievable under the strong secrecy criterion, one can follow the same steps as in the proof of Proposition 2 by considering an equivalent channel with wiretap coding for Phase 2, where the Ev link rate is upper bounded as in (84)-(88) so that the rates in (49) and, after time sharing, in (36) are achievable under strong secrecy. □

Note that, if $\sigma_W^2 \geq \sigma_V^2$ and both noises are Gaussian, then $C_{s0} = 0$ and $C_s = R_h$, i.e. if the Tx-Rx channel is weaker than the Tx-Ev channel, the secrecy capacity with Rx help is still positive (if $R_h > 0$) and independent of r (as long as $|r| < 1$), even if the help is not secure. This also holds if $\sigma_W^2 = \sigma_V^2$, unlike the case of the reversely-degraded channel, where $C_s = 0$ if $\sigma_W^2 = \sigma_V^2$ and the help is not secure. This is due to $W^n \neq V^n$ in the non-degraded channel (with non-singular correlation) which makes the public "key" $T = \hat{W}^n$ useful to the Rx only, but not to the Ev.

Similarly to the degraded and reversely-degraded WTCs, the same secrecy capacity results even if the helper is aware of the message being transmitted, $T = T(W^n, M)$, under weak or strong secrecy criterion.

V. The Degraded WTC With Tx Help

Let us now consider the setting of Fig. 5 and extend Theorem 1 to the scenario where rate-limited help is available to the Tx, in addition to or instead of the Rx help. Unlike the Rx help case where the causality of help is immaterial (since the Rx starts decoding after the whole block of length n is received), it becomes important for the Tx help setting. Thus, we distinguish between causal Tx help, whereby at time i the Tx help is based on the Rx noise sequence up to time i, and non-causal Tx help, whereby the Tx help at time $i = 1$ (the very beginning of the transmission) is based on the whole noise sequence W^n. Interestingly, the causality of Tx help has no impact on the secrecy capacity (this mimics the respective property of the no-Ev/no-secrecy channel capacity with Tx help in [37]).

Theorem 4: Consider the degraded WTC as in in Fig. 5 with additive, possibly non-Gaussian noises, and causal or non-causal Tx help of rate R_h, secure or non-secure, in addition to or instead of the same Rx help. Let $0 < \sigma_V^2, P < \infty$ and, in the case of non-Gaussian noises, $h(V) > -\infty$ and (5) to hold. Its weak or strong secrecy capacity C_s satisfies

$$C_s \geq C_{s0} + R_h \quad (90)$$

where C_{s0} is the secrecy capacity without help. This holds with equality if the help is not secure and noises are Gaussian.

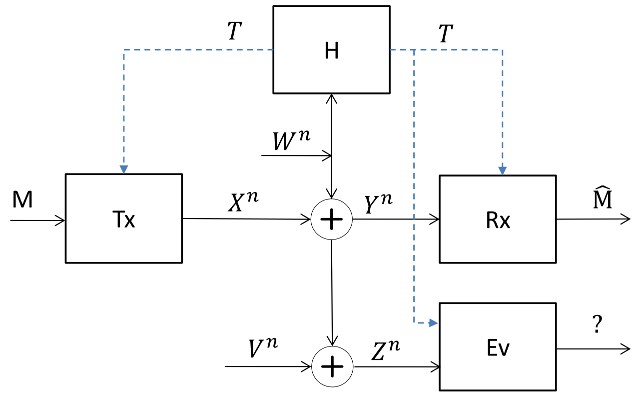

Fig. 5. Degraded wiretap channel with additive (not necessarily Gaussian) noise and a rate-limited help T at the Tx, Rx and Ev (T is not available to the Ev if the help is secure). W^n and V^n are i.i.d. noise sequences, $\sigma_V^2 > 0$; V^n is independent of W^n, X^n, M; $X^n = X^n(M,T)$, $T = T(W^n)$, $H(T) \leq nR_h$.

Proof: We consider the case of non-secure help, from which the case of secure help follows (since the availability of help to the Ev cannot increase the secrecy rate). The achievability is based on the two-phase flash signaling as in Theorem 1, with noise pre-cancellation at the Tx (a.k.a. dirty-paper coding, as in [37]) in Phase 2. The converse is based on the functional relationship between the involved random variables as well as the secrecy constraint, in addition to the reliability and power constraints.

Converse: we assume that noises are Gaussian and prove the converse under weak secrecy and when the same non-causal non-secure help T is available to all ends, i.e. the Tx, Rx and Ev as in Fig. 5. Clearly, the same converse will hold if no Rx help is available, if the help is causal, or under strong secrecy. Using the appropriate Markov chain and functional relationships between the random variables, in addition to the secrecy and reliability constraints, note the following:

$$\begin{aligned}
nR_s &= H(M) && (91)\\
&\leq H(M|Z^nT) + n\epsilon && (92)\\
&= I(M;Y^n|Z^nT) + H(M|Y^nZ^nT) + n\epsilon && (93)\\
&\leq I(M;Y^n|Z^nT) + 2n\epsilon && (94)\\
&\leq I(X^n;Y^n|Z^nT) + 2n\epsilon && (95)\\
&= I(X^n;Y^n|T) - I(X^n;Z^n|T) + 2n\epsilon && (96)\\
&= h(Y^n|T) - h(Y^n|X^nT) && (97)\\
&\quad - [h(Z^n|T) - h(Z^n|X^nT)] + 2n\epsilon \\
&= h(W^n+V^n|T) - h(W^n|T) + h(Y^n|T) && (98)\\
&\quad - h(Z^n|T) + 2n\epsilon \\
&\leq \frac{n}{2}\log(2\pi e(\sigma_V^2+\sigma_W^2)) + I(W^n;T) - h(W^n) && (99)\\
&\quad + h(Y^n|T) - h(Z^n|T) + 2n\epsilon \\
&= \frac{n}{2}\log\frac{\sigma_V^2+\sigma_W^2}{\sigma_W^2} + H(T) + h(Y^n|T) && (100)\\
&\quad - h(Z^n|T) + 2n\epsilon \\
&\leq nR_h + \frac{n}{2}\log\frac{\sigma_V^2+\sigma_W^2}{\sigma_W^2}\frac{\sigma_W^2+P}{\sigma_W^2+\sigma_V^2+P} + 2n\epsilon && (101)
\end{aligned}$$

$$= nR_h + \frac{n}{2}\log\left(1+\frac{P}{\sigma_W^2}\right) - \frac{n}{2}\log\left(1+\frac{P}{\sigma_V^2+\sigma_W^2}\right) + 2n\epsilon \quad (102)$$

$$= n(R_h + C_{s0} + 2\epsilon) \quad (103)$$

where (92) follows from the secrecy constraint $I(M;Z^nT) \le n\epsilon$; (94) follows from Fano inequality (due to the reliability constraint) $H(M|Y^nZ^nT) = H(M|Y^nT) \le n\epsilon$; (95) and (96) follow from Markov chain $M - X^n - Y^n - Z^n$ conditional on T; (98) is due to the independence of X^n and (W^n, V^n) conditional on T; (99) follows since conditioning cannot increase entropy; (100) is due to $I(W;T) = H(T)$; (101) follows from Lemma 1 below. Since (103) holds for any $\epsilon > 0$, it follows that $C_s \le C_{s0} + R_h$, as desired. Clearly, the same inequality holds if T is not available to the Rx.

Lemma 1: The following inequality holds in the considered setting:

$$\Delta h = h(Y^n|T) - h(Z^n|T) \le \frac{n}{2}\log\frac{\sigma_W^2+P}{\sigma_W^2+\sigma_V^2+P} \quad (104)$$

Proof: It has been proved in [37, eq. (46)] that

$$h(Y^n|T) \le \frac{n}{2}\log(2\pi e(\sigma_W^2+P)) \quad (105)$$

(the proof is not trivial since X^n and W^n are *not* independent, due to help $T = T(W^n)$). To bound $h(Z^n|T)$ likewise, note that

$$h(Z^n|T) = \sum_t p_T(t) h(Y^n + V^n|T=t) \quad (106)$$

where $p_T(t)$ is the distribution of T. Using the entropy power inequality

$$2^{\frac{2}{n}h(Y^n+V^n|T=t)} \ge 2^{\frac{2}{n}h(Y^n|T=t)} + 2^{\frac{2}{n}h(V^n|T=t)} \quad (107)$$

it follows that

$$h(Y^n+V^n|T=t) \ge \frac{n}{2}\log(2^{\frac{2}{n}h(Y^n|T=t)} + 2\pi e\sigma_V^2) \quad (108)$$

and hence

$$h(Z^n|T) \ge \frac{n}{2}\log\left(2^{\frac{2}{n}\sum_t p_T(t)h(Y^n|T=t)} + 2\pi e\sigma_V^2\right) \quad (109)$$

$$= \frac{n}{2}\log\left(2^{\frac{2}{n}h(Y^n|T)} + 2\pi e\sigma_V^2\right)$$

where the inequality is due to the convexity of the log-sum-exp function [44, p. 72]. Finally,

$$\Delta h \le h(Y^n|T) - \frac{n}{2}\log\left(2^{\frac{2}{n}h(Y^n|T)} + 2\pi e\sigma_V^2\right) \quad (110)$$

$$\le \frac{n}{2}\log(2\pi e(\sigma_W^2+P)) - \frac{n}{2}\log\left(2^{\log(2\pi e(\sigma_W^2+P))} + 2\pi e\sigma_V^2\right) \quad (111)$$

$$= \frac{n}{2}\log\frac{\sigma_W^2+P}{\sigma_W^2+\sigma_V^2+P} \quad (112)$$

as required, where the inequality is due to (105) and $f(x) = x - \log(2^x + c)$ being an increasing function of x for any $c > 0$. □

Achievability: To establish the achievability under weak secrecy, we do not assume that noises are Gaussian and consider the case of causal help being available to the Tx and Ev but not to the Rx. This will also establish achievability when the same help is also available to the Rx or/and when Tx help is non-causal (since adding Rx help or removing causality constraint cannot decrease achievable rates). Similarly to Theorem 1, we use a two-phase signalling, where Phase 1 of duration $(1-\tau)$ makes use of no-help regular wiretap coding and thus achieves the secrecy rate $C_{s0} - \epsilon$ for any $\epsilon > 0$. Phase 2 of duration τ is the same as in [37], which makes use of regular (no-wiretap) coding and pre-substraction of the scalar-quantized noise (available via the rate-limited help link) at the Tx, as shown in Fig. 6:

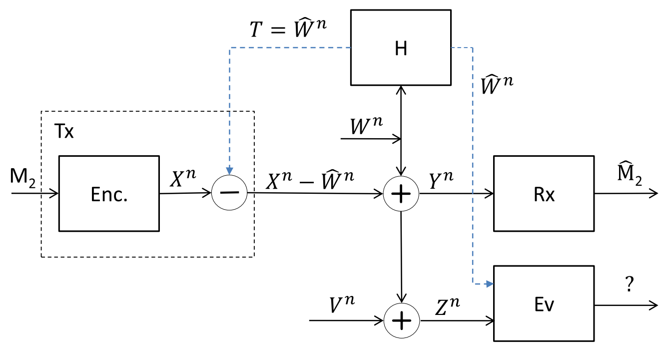

Fig. 6. Phase 2 signalling for the degraded WTC: the causal help T is a scalar-quantized noise $\hat{W}^n$, $\hat{W}_i = Q(W_i)$, pre-subtracted at the Tx; $X^n = X^n(M_2)$ is a codeword from i.i.d.-generated codebook, as in [37].

$$Y_i = X_i - \hat{W}_i + W_i$$
$$Z_i = Y_i + V_i \quad (113)$$

where $X^n = X^n(M_2)$ using i.i.d.-generated codebook $\mathcal{C}$, $T = \hat{W}^n$ is a scalar-quantized noise, $\hat{W}_i = Q(W_i)$, where the quantizer uses $L = \lfloor 2^{R_h/\tau} \rfloor$ levels for each sample, which require the average rate $\tau\log(L) \le R_h$ to be transmitted over the help link.[5] For further use, note that $V^n \perp (W^n, \hat{W}^n, X^n, M_2)$ and $(W^n, \hat{W}^n) \perp (V^n, X^n, M_2)$, where $\perp$ means statistical independence, so that the following Markov chains hold:

$$(M_2, \mathcal{C}) - X^n - Y^n - Z^n;$$
$$(M_2, \mathcal{C}) - X^n - (Z^n, W^n, \hat{W}^n) \quad (114)$$

Following [37, eq. (24)], this Phase 2 signalling achieves the rate arbitrary close to

$$\frac{R_h}{\tau} + \frac{1}{2}\log\left(2^{-2R_h/\tau} + \frac{12P}{\alpha_W^3}(1-2^{-R_h/\tau})^2[1+o(1)]\right)$$
$$= \frac{R_h}{\tau}[1+o(1)] \quad (115)$$

where $o(1) \to 0$ as as $\tau \to 0$. Thus, the overall two-phase signalling rate (after time sharing) is

$$(1-\tau)(C_{s0}-\epsilon) + \tau R_h/\tau(1+o(1)) \to C_{s0} + R_h - \epsilon \quad (116)$$

for any $\epsilon > 0$, as $\tau \to 0$.

It remains to show that this rate is indeed weakly secure, i.e. the information leakage rate to the Ev is arbitrary small.

[5] An alternative Phase 2 strategy using a simple lattice code with a uniform scalar quantizer is proposed in [40].

This is clearly the case in Phase 1 since regular wiretap coding is used in this phase so that its leakage rate is $R_{l1} = n^{-1}I(M_1; Z^n) \leq \delta$ for any $\delta > 0$ and sufficiently-large n. To see that secrecy is guaranteed after two-phase time sharing (even though no wiretap coding is used in Phase 2), we show that Phase 2 leakage rate is uniformly bounded for any τ:

$$\begin{aligned} R_{l2} &= n^{-1}I(M_2; Z^n\hat{W}^n|\mathcal{C}) && (117)\\ &\leq n^{-1}I(X^n; Z^n\hat{W}^n|\mathcal{C}) && (118)\\ &\leq n^{-1}I(X^n; Z^n\hat{W}^n) && (119)\\ &\leq n^{-1}I(X^n; Z^nW^n) && (120)\\ &\leq I_0(X; ZW) && (121)\\ &= I_0(X; X+V) && (122)\\ &\leq \frac{1}{2}\log\left(P+\sigma_V^2\right) - h(V) = R_0 < \infty && (123) \end{aligned}$$

where (118) is due to Markov chain $M_2 - X^n - Z^n\hat{W}^n$; (119) is due to Markov chain $\mathcal{C} - X^n - Z^n\hat{W}^n$; (120) is due to $\hat{W}^n = Q(W^n)$; (121) holds since the channel is memoryless; I_0 is the mutual information induced by input X with the distribution $p_0(x) = n^{-1}\sum_i p_{x_i}(x)$; the last inequality in (123) holds since all terms are finite.

Thus, the overall leakage rate after two-phase time sharing is

$$R_l = (1-\tau)R_{l1} + \tau R_{l2} \leq (1-\tau)\delta + \tau R_0 \to \delta \quad (124)$$

as $\tau \to 0$, for any $\delta > 0$, as required.

To establish achievability under strong secrecy, we follow the strategy of Proposition 2. The Phase 1 rate $C_{s0} - \epsilon$ holds under strong secrecy as well (since no help is used). For Phase 2, noise pre-cancellation at the Tx is combined with wiretap coding. After the pre-cancellation, the equivalent channel is as in (113), where $\hat{W}_i$ is also available to the Ev, so that an achievable strong secrecy rate is

$$R_{s2} = I(X;Y) - I(X; Z\hat{W}) - \epsilon \quad (125)$$

where first term is the rate of the legitimate link and it is lower-bounded by (115),

$$I(X;Y) \geq \frac{R_h}{\tau}[1 + o(1)] \quad (126)$$

while second term is the Ev link rate that is upper bounded as in (121)-(123):

$$\begin{aligned} I(X; Z\hat{W}) &\leq I(X; ZW)\\ &\leq \frac{1}{2}\log\left(P+\sigma_V^2\right) - h(V) = R_0 < \infty \quad (127) \end{aligned}$$

so that

$$R_{s2} \geq \frac{R_h}{\tau}(1+o(1)) - R_0 - \epsilon = \frac{R_h}{\tau}(1+o(1)) \quad (128)$$

and, after time sharing, (116) holds under strong secrecy as well.

□

Note that, for Gaussian noises, the availability of the Rx help, in addition to the Tx help, does not increase the secrecy capacity (provided the help T is the same in both cases) so that one help link can be omitted without affecting the capacity.

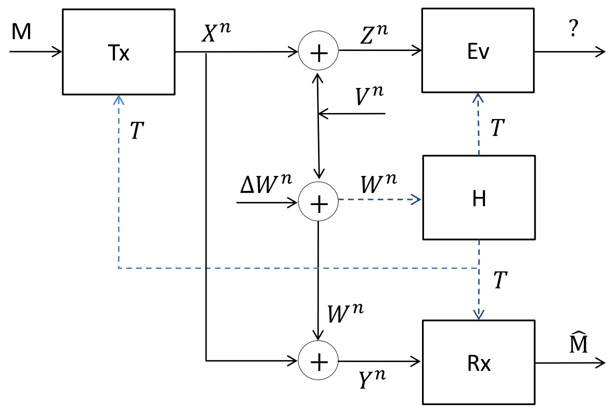

Fig. 7. Reversely-degraded wiretap channel with a rate-limited help T at the Tx, Rx and Ev. ΔW^n and V^n are i.i.d. noise sequences, $\sigma_V^2, \sigma_{\Delta W}^2 > 0$; V^n, ΔW^n and M are independent of each other; $X^n = X^n(M,T)$, $T = T(W^n)$, $H(T) \leq nR_h$.

Similarly to the Rx help case, if $\sigma_V^2 = 0$ and the Tx (or joint Tx/Rx) help is not secure, then the secrecy capacity is zero, since the Ev has access to exactly the same information as the Rx so that no secrecy is possible, i.e. $C_s(\sigma_V^2)$ is a discontinuous function at $\sigma_V^2 = 0$:

$$\lim_{\sigma_V^2 \to 0^+} C_s(\sigma_V^2) = R_h > 0 \quad (129)$$

while $C_s(0) = 0$.

VI. The Reversely-Degraded WTC With Tx Help

Let us consider the reversely-degraded (possibly non-Gaussian) WTC, as in Fig. 7, with Tx help, in addition to or instead of the Rx help (T is not available to the Ev if help is secure). While its secrecy capacity is zero without help, this is not the case when help is present, even if it is not secure, as the following Theorem shows.

Theorem 5: Consider the reversely-degraded WTC with additive (not necessarily Gaussian) noises and causal or non-causal Tx help of rate R_h, secure or not, in addition to or instead of the same Rx help, as in Fig. 7. Let $0 < \sigma_V^2, \sigma_{\Delta W}^2, P < \infty$. In the case of non-Gaussian noise, let $h(V), h(\Delta W) > -\infty$ and (5) be satisfied. Then, the weak or strong secrecy capacity C_s satisfies

$$C_s \geq R_h \quad (130)$$

and this holds with equality if the help is not secure.

Proof: It is sufficient to consider the case of non-secure help since the case of secure one follows from it.

Converse: we prove the converse under weak secrecy and when the same (non-secure non-causal) help T is available to all ends, i.e. the Tx, Rx and Ev as in Fig. 7. Clearly, the same converse will hold if no Rx help is available or if the help is causal. First, note that (91)-(95) still hold, since channel

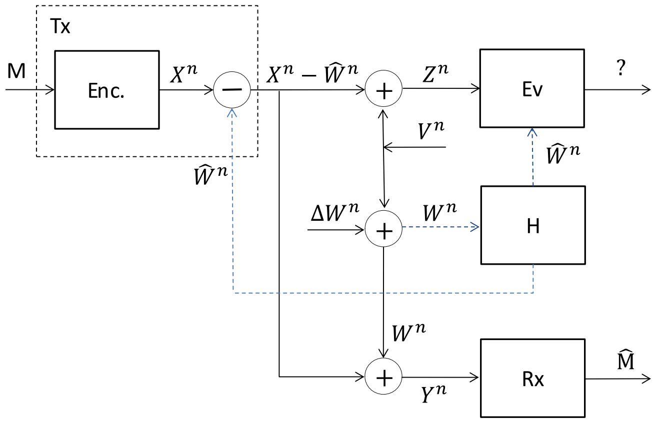

Fig. 8. Phase 2 signalling for the reversely-degraded WTC: the causal help $T = \hat{W}^n$ is a scalar-quantized noise, $\hat{W}_i = Q(W_i)$, pre-subtracted at the Tx; $X^n = X^n(M_2)$ is a codeword from i.i.d.-generated codebook.

degradedness plays no role there. Therefore,

$$nR_s = H(M)$$
$$\leq I(X^n; Y^n|Z^n T) + 2n\epsilon \quad (131)$$
$$= I(X^n; X^n + V^n + \Delta W^n | X^n + V^n, T) + 2n\epsilon \quad (132)$$
$$= I(X^n; \Delta W^n | X^n + V^n, T) + 2n\epsilon \quad (133)$$
$$= h(\Delta W^n | X^n + V^n, T) \quad (134)$$
$$- h(\Delta W^n | X^n, V^n, T) + 2n\epsilon$$
$$\leq h(\Delta W^n|T) - h(\Delta W^n | V^n, T) + 2n\epsilon \quad (135)$$
$$\leq h(\Delta W^n|T) - h(\Delta W^n) + H(T) + 2n\epsilon \quad (136)$$
$$\leq H(T) + 2n\epsilon \quad (137)$$

where (135) follows from Markov chain $X^n - T - (V^n, \Delta W^n)$ (i.e., conditional independence of X^n and $(V^n, \Delta W^n)$ given T) and since conditioning cannot increase the entropy; (136) is due to

$$h(\Delta W^n | V^n, T) \geq h(\Delta W^n) - H(T) \quad (138)$$

which in turn follows from

$$I(\Delta W^n; T|V^n) = h(\Delta W^n|V^n) - h(\Delta W^n|V^n, T) \quad (139)$$
$$= h(\Delta W^n) - h(\Delta W^n|V^n, T) \quad (140)$$
$$\leq H(T) \quad (141)$$

where (140) is due to the independence of ΔW^n and V^n. Since (137) holds for any $\epsilon > 0$, it follows that $R_s \leq n^{-1}H(T) = R_h$, as required.

Achievability: We start with weak secrecy and consider the case where causal help $T = \hat{W}^n$ is a scalar-quantized noise, $\hat{W}_i = Q(W_i)$, available to the Tx and Ev but not to the Rx. Two-phase transmission is used again, where nothing is transmitted in Phase 1 and regular (no wiretap coding) flash signalling is used in Phase 2, where the latter achieves the rate as in (115) so that, after time sharing, the achieved rate is arbitrary close to

$$R_s = \tau \frac{R_h}{\tau}(1 + o(1)) \to R_h \quad (142)$$

as $\tau \to 0$. To see that this rate is indeed weakly-secure after the time-sharing (i.e., the information leakage rate is arbitrary-low), we show that the Phase 2 leakage rate is uniformly bounded:

$$R_{l2} = n^{-1}I(M_2; Z^n \hat{W}^n | \mathcal{C}) \quad (143)$$
$$\leq n^{-1}I(X^n; Z^n \hat{W}^n | \mathcal{C}) \quad (144)$$
$$\leq n^{-1}I(X^n; Z^n \hat{W}^n) \quad (145)$$
$$= n^{-1}I(X^n; \hat{W}^n) + n^{-1}I(X^n; Z^n|\hat{W}^n) \quad (146)$$
$$= n^{-1}I(X^n; X^n - \hat{W}^n + V^n|\hat{W}^n) \quad (147)$$
$$= n^{-1}h(X^n + V^n|\hat{W}^n) - n^{-1}h(V^n|\hat{W}^n, X^n) \quad (148)$$
$$\leq n^{-1}h(X^n + V^n) - n^{-1}h(V^n|\hat{W}^n) \quad (149)$$
$$\leq \frac{1}{2}\log\left(2\pi e(P + \sigma_V^2)\right) - h(V) + \frac{1}{2}\log(2\pi e \sigma_W^2)$$
$$- h(\Delta W) = R_0 < \infty \quad (150)$$

where (144) is due to Markov chain $M_2 - X^n - Z^n\hat{W}^n$; (145) is due to Markov chain $\mathcal{C} - X^n - Z^n\hat{W}^n$; (147) and (149) are due to the independence of X^n and $(V^n, \hat{W}^n)$; (150) follows from

$$h(X^n + V^n) \leq \frac{n}{2}\log(2\pi e(P + \sigma_V^2)), \quad (151)$$
$$h(V^n|\hat{W}^n) \geq h(V^n|W^n) \quad (152)$$
$$= h(V^n) - h(W^n) + h(\Delta W^n) \quad (153)$$
$$\geq nh(V) - \frac{n}{2}\log(2\pi e \sigma_W^2) + nh(\Delta W) \quad (154)$$

Thus, after time-sharing, which is equivalent here to Phase 2 only signaling, the leakage rate is

$$R_l = \tau R_{l2} \leq \tau R_0 \to 0 \quad (155)$$

when $\tau \to 0$, as required.

For strong secrecy, wiretap coding has to be added to noise pre-cancellation and the equivalent channel is

$$Y_i = X_i - \hat{W}_i + W_i$$
$$Z_i = X_i - \hat{W}_i + V_i \quad (156)$$

Following the strategy of Proposition 2, its achievable strong secrecy rate is

$$R_{s2} = I(X;Y) - I(X;Z\hat{W}) - \epsilon \quad (157)$$

where

$$I(X;Y) \geq \frac{R_h}{\tau}[1 + o(1)] \quad (158)$$

and, using (145)-(150), second term can be upper bounded as follows

$$I(X;Z\hat{W}) \leq R_0 < \infty \quad (159)$$

where R_0 is as in (150), so that

$$R_{s2} \geq \frac{R_h}{\tau}[1 + o(1)] \quad (160)$$

and therefore the rate in (142) is achievable under strong secrecy as well. □

We remark that, as in the reversely-degraded WTC with Rx help, no wiretap coding is needed here to achieve its weak

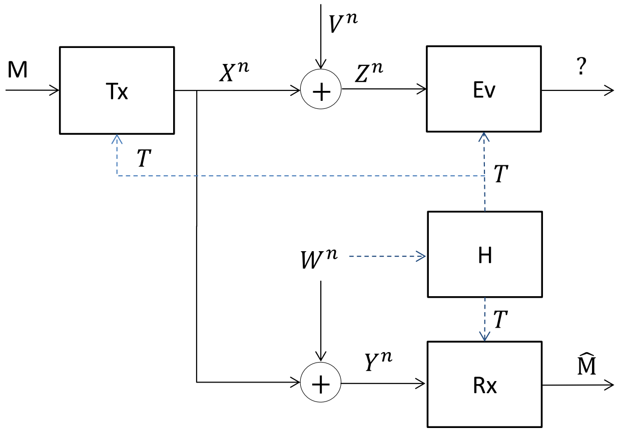

Fig. 9. Non-degraded wiretap channel with a rate-limited help T at the Tx, Rx and Ev. W^n and V^n are i.i.d. noise sequences (possibly non-Gaussian and correlated with each other) independent of M; $0 < \sigma_W^2, \sigma_V^2, P < \infty$; $h(W,V) > -\infty$; $X^n = X^n(M,T)$, $T = T(W^n)$, $H(T) \le nR_h$; conditional on T, X^n is independent of W^n, V^n.

secrecy capacity if the help is not secure. Burst signalling alone (with regular coding) is sufficient and arbitrarily low leakage rate can be achieved by reducing signaling interval τ. The presence of help T at the Rx, in addition to the Tx, does not increase the capacity. Even though the help is not secure, it still boosts significantly the secrecy capacity, which is zero without help. This is so since the help T serves here as a public key: even though this key is available to the Ev, it cannot make use of it since it does not have the right "lock".

Similarly to the reversely-degraded WTC with Rx help, $C_s = 0$ if $\sigma_{\Delta W}^2 = 0$ and help is not secure (since the Ev receives the same information as the Rx so that no secrecy is possible) and therefore $C_s(\sigma_{\Delta W}^2)$ is discontinuous at $\sigma_{\Delta W}^2 = 0$:

$$C_s(\sigma_{\Delta W}^2) = R_h > 0 \ \forall \ \sigma_{\Delta W}^2 > 0 \tag{161}$$

while $C_s(0) = 0$, for any $R_h > 0$, i.e. more noise at the Rx ($\sigma_{\Delta W}^2 > 0$) is better for the secrecy capacity of this channel.

VII. The Non-Degraded WTC With Tx Help

Let us now consider the non-degraded wiretap channel where W^n and V^n are i.i.d. noise sequences, possibly non-Gaussian and correlated with each other as in (79), see Fig. 9 (if help is secure, T is not available to the Ev). Similarly to the case of Rx help, this channel cannot be equivalently reduced to degraded or reversely-degraded case when help is present (even if it is secure). Its secrecy capacity is characterized below.

Proposition 4: Consider the non-degraded WTC channel with additive possibly non-Gaussian noises and secure or non-secure Tx help of rate R_h, causal or non-causal, in addition to or instead of the same Rx help, as in Fig. 9, where the noise sequences W^n and V^n are i.i.d. but possibly correlated with each other as in (79) and $0 < \sigma_W^2, \sigma_V^2, P < \infty$. For non-Gaussian noise, let $h(W,V) > -\infty$. Its weak or strong secrecy capacity is lower bounded as follows:

$$C_s \ge C_{s0} + R_h \tag{162}$$

Proof: To show the achievability of $C_{s0}+R_h$ under weak secrecy, we use the same two-phase signalling as in Theorem 4, where Phase 1 makes use of the standard wiretap codes and no help and thus achieves the secrecy rate arbitrary close to C_{s0} (no Phase 1 is needed if $C_{s0} = 0$). Likewise, Phase 2 makes use of standard (not wiretap) codes and pre-subtracts quantized noise at the Tx, as in Fig. 6, and achieves the rate as in (115) (regardless of the correlation), so that, after the time sharing, the rate is as in (116). To show that this rate is indeed secure, we show that Phase 2 leakage rate is uniformly bounded for any τ. To this end, note that (118)-(121) still hold since channel degradedness or noise correlation play no role there so that

$$\begin{aligned}
R_{l2} &\le I_0(X;ZW) && (163)\\
&= I_0(X;X+V,W) && (164)\\
&\le h(X+V) + h(W) - h(V,W) && (165)\\
&\le \frac{1}{2}\log\left(2\pi e(P+\sigma_V^2)\right) + \frac{1}{2}\log\left(2\pi e\sigma_W^2\right) - h(V,W) && (166)\\
&= R_0 < \infty && (167)
\end{aligned}$$

where (166) holds since Gaussian distribution maximizes differential entropy and (167) holds since all terms in (166) are finite. Therefore, the overall leakage rate after the two-phase time sharing is arbitrary small as in (124), as required, and the achieved rate in (116) is indeed secure.

Under strong secrecy, Phase 1 remains the same but Phase 2 makes use of wiretap codes, in addition to noise pre-cancellation, as for the previously-considered WTC configurations. Using the equivalent channel as in Theorems 4 and 5, one can show that Phase 2 strong secrecy rate

$$\begin{aligned}
R_{s2} &= I(X;Y) - I(X;Z\hat{W}) - \epsilon\\
&\ge \frac{R_h}{\tau}[1+o(1)] - R_0 - \epsilon\\
&= \frac{R_h}{\tau}[1+o(1)] && (168)
\end{aligned}$$

is achievable, where R_0 is as in (167), so that, after time sharing, the rate in (116) is achievable under strong secrecy as well.

□

Thus, the Tx help of rate R_h, secure or non-secure, causal or non-causal, brings in the secrecy capacity boost of at least R_h in this configuration, regardless of the correlation (as long as $h(W,V) > -\infty$ or, for Gaussian noises, $|r| < 1$). It is an open question whether $C_s = C_{s0} + R_h$.

VIII. Independent Tx/Rx Help Links

In the preceding sections, we have considered the scenarios where the same help was available at the Tx and Rx and have shown that the presence of Tx help in addition to the same Rx help (or vice versa) has no impact on the secrecy capacity and therefore one link can be removed without affecting the capacity.

One may wonder whether this still holds if help links are not identical. Therefore, we consider the scenario whereby independent help links are available to the Tx and Rx of rate

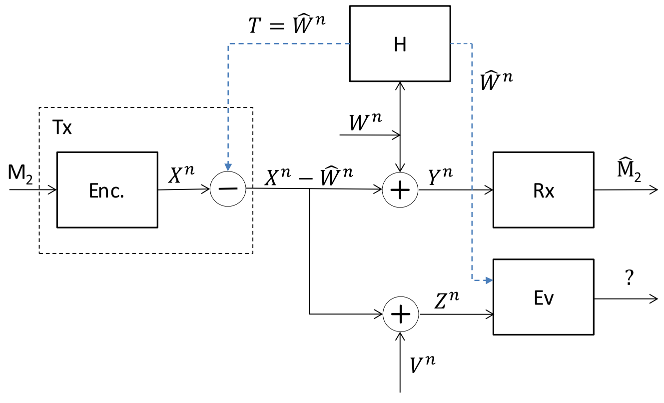

Fig. 10. Phase 2 signalling for the non-degraded WTC: $\hat{W}^n = Q(W^n)$ is scalar-quantized noise, pre-subtracted at the Tx; $X^n = X^n(M_2)$ is a codeword from i.i.d.-generated codebook.

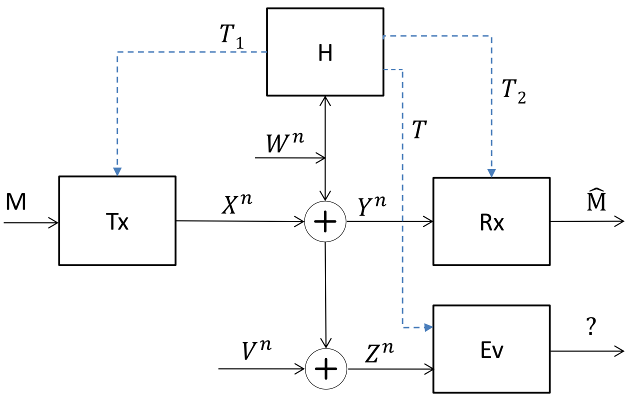

Fig. 11. Degraded wiretap channel with independent help links to the Tx and Rx of rate R_{h1} and R_{h2}, respectively; the total help $T = (T_1, T_2)$ is available to the Ev (if help is not secure). W^n and V^n are i.i.d. noise sequences; $P, \sigma_V^2 > 0$; V^n is independent of W^n, X^n, M; $X^n = X^n(M, T_1)$, $T = T(W^n)$, $H(T_k) \le nR_{hk}$.

R_{h1} and R_{h2}, respectively. The total help T is composite: $T = (T_1, T_2)$, where T_1 is available to the Tx and T_2 - to the Rx while the whole help T is available to the Ev (in the case of non-secure help); T_1, T_2 are independent of each other (e.g. based on different parts of the i.i.d. noise sequence W^n) and $H(T_k) \le nR_{hk}, \ \ k = 1, 2$, so that

$$H(T) = H(T_1) + H(T_2) \le R_{h1} + R_{h2} = R_h \tag{169}$$

We consider first the degraded WTC as in Fig. 11.

Theorem 6: Consider the degraded WTC with causal or non-causal Tx help of rate R_{h1} and Rx help of rate R_{h2} independent of each other (secure or not) as in Fig. 11, and let $0 < \sigma_V^2, P < \infty$ and, in the case of non-Gaussian noises, $h(V) > -\infty$ and (5) to hold. Its weak or strong secrecy capacity C_s satisfies

$$C_s \ge C_{s0} + R_{h1} + R_{h2} \tag{170}$$

where C_{s0} is the secrecy capacity without help. This holds with equality if help is not secure and noises are Gaussian.

Proof: To prove achievability, we use three-phase signalling combining Rx and Tx help in independent phases:

1) Phase 1 of duration $(1 - \tau_1 - \tau_2)$: the standard wiretap coding is used without any help, as in Theorems 1, 4.

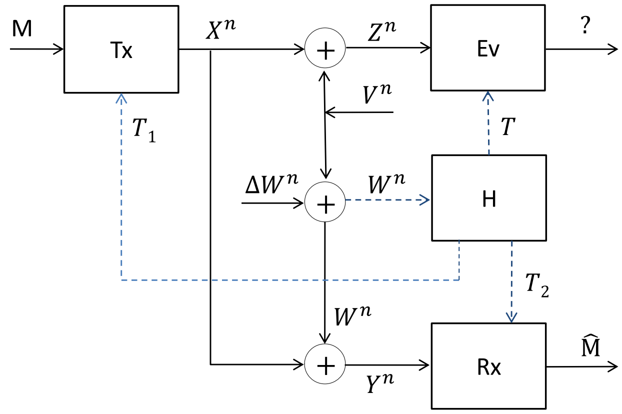

Fig. 12. Reversely-degraded wiretap channel with independent help links to the Tx and Rx of rate R_{h1} and R_{h2}, respectively; the total help $T = (T_1, T_2)$ is available to the Ev (if help is not secure). ΔW^n and V^n are i.i.d. noise sequences independent of each other; $\sigma_{\Delta W}^2, \sigma_V^2, P > 0$; $X^n = X^n(M, T_1)$, $T = T(W^n)$, $H(T_k) \le nR_{hk}$.

2) Phase 2 of duration τ_1: the same as for the Tx help in Theorem 4 (flash signalling with noise pre-cancellation using Tx help); no Rx help is used in this phase.
3) Phase 3 of duration τ_2: the same as for the Rx help in Theorem 1 (flash signalling with Rx help); no Tx help is used in this phase.

Clearly, a secrecy rate arbitrary close to C_{s0} is achievable in Phase 1, as before. Likewise, based on Theorems 1 and 4, secrecy rates arbitrary close to $R_{h1}/\tau_1(1 + o(1))$ and $R_{h2}/\tau_2(1 + o(1))$ are achievable in Phases 2 and 3, and, after three-phase time sharing, a secrecy rate arbitrary close to

$$\begin{aligned} (1 - \tau_1 - \tau_2)C_{s0} + (R_{h1} + R_{h2})(1 + o(1)) \\ \to C_{s0} + R_{h1} + R_{h2} \end{aligned} \tag{171}$$

is achievable as $\tau_1, \tau_2 \to 0$.

Converse: a key observation here is that the converse of Theorem 4 still holds with $T = (T_1, T_2)$. Indeed, (91) - (103) do hold, where (94) holds since

$$H(M|Y^n Z^n T) \le H(M|Y^n T_2) \le n\epsilon \tag{172}$$

(101) holds since Lemma 1 still holds, due to

$$h(Y^n|T) \le h(Y^n|T_1) \le \frac{n}{2}\log(2\pi e(\sigma_W^2 + P)) \tag{173}$$

where the last inequality is due to (105), and since (106) - (112) do hold with $T = (T_1, T_2)$. □

Note that if Tx/Rx help links are independent of each other, the secrecy capacity boost is their combined rate $R_{h1} + R_{h2}$, unlike the case of identical Tx/Rx help where the boost is just an individual help rate, as in Theorem 4, and one of the two help links can be removed without any effect on the capacity.

Next, we consider the reversely-degraded channel with independent help links as in Fig. 12, where T_1 and T_2 are independent of each other.

Theorem 7: Consider the reversely-degraded WTC with independent causal or non-causal help links as in Fig. 12, where $0 < \sigma_W^2, P < \infty$ and, in the case of non-Gaussian noises, $h(V) > -\infty$ and (5) holds. Its weak or strong secrecy capacity C_s satisfies

$$C_s \geq R_{h1} + R_{h2} \tag{174}$$

This holds with equality if the help is not secure and noises are Gaussian.

Proof: The achievability makes use of the three-phase signaling as in Theorem 6 where nothing is transmitted in Phase 1. The converse is established by observing that (131)-(141) still hold with $T = (T_1, T_2)$. □

For the non-degraded channel with independent Tx/Rx help links, it can be shown, in a similar way, that Proposition 4 still holds with $R_h = R_{h1} + R_{h2}$.

Thus, in all considered configurations, the independent Tx/Rx help links provide additive boost $R_{h1} + R_{h2}$ in secrecy rates, unlike the same help links whereby one link can be omitted without affecting the capacity. This mimics the respective property of the no-Ev channel with independent help links in [38].

Finally, one may envision the case of composite help $T = (T_1, T_2)$ where T_1, T_2 are not independent of each other but are not identical either (which may be due to e.g. certain limitations in the system architecture). In this case, if the help is not secure and noises are Gaussian, it is not difficult to see that Theorems 6 and 7 still hold with

$$C_{s0} + \max\{R_{h1}, R_{h2}\} \leq C_s \leq C_{s0} + R_h \tag{175}$$

where $C_{s0} = 0$ for the latter, and $H(T) \leq nR_h$, so that the boost in the secrecy capacity is at least $\max\{R_{h1}, R_{h2}\}$ (and this lower bound is achievable with one help link only). It remains to be seen whether the upper bound is achieved with equality, i.e. whether the boost is actually $R_h > \max\{R_{h1}, R_{h2}\}$.

IX. Conclusion

The SISO wiretap channel with additive (not necessarily Gaussian) noise and with rate-limited help at the receiver (decoder) or/and the transmitter (encoder) was studied and its weak/strong secrecy capacity has been established under various channel configurations (degraded, reversely degraded and non-degraded) with secure or non-secure help. In all considered WTC and helper configurations, $C_{s0} + R_h$ is either the (weak or strong) secrecy capacity or an achievable rate. In most cases, it is the former, i.e. the rate-limited help results in the secrecy capacity boost (compared to the standard "no help" case) equal to the help rate, so that positive secrecy rate is achievable even for reversely-degraded channel, where the secrecy capacity is zero without help. In fact, the weak secrecy rate R_h is achievable for *any* WTC configuration *without any wiretap codes at all* and this strategy is optimal for the reversely-degraded WTC. This may be attractive for many applications which do not require excessive security.

Surprisingly, secure Rx help does not result in higher capacity compared to non-secure one and stronger noise at the legitimate receiver can sometimes be beneficial for secrecy capacity. When Tx and Rx help links are identical (carry the same help), any one can be removed without affecting the capacity. However, when the help links are independent, the boost in secrecy capacity equals to the sum of help rates and no one link can be omitted without loss in the capacity. Non-singular Rx and Ev noise correlation has no impact on the secrecy capacity. In the case of Rx help, secure or non-secure, the secrecy capacity is not increased even if the helper is aware of the message being transmitted. The choice of the secrecy criterion (weak/strong) affects the complexity of implementation but not the secrecy capacity. In the case of non-secure Tx help, non-causal help does not bring in any increase in the secrecy capacity over the causal one. Comparing the above results to those for the no-Ev channel with help in [36], [37], and [38], we conclude that the boost in capacity equal to the help rate comes with secrecy "for free". It remains to be seen whether the secrecy of Tx help or helper's knowledge of the message brings in any increase in the secrecy capacity.

Acknowledgment

The ideas to consider non-Gaussian noise and more general power constraints (beyond the average power constraint) were proposed by anonymous reviewers of this article. The idea to extended the weak secrecy constraint to a strong one was proposed by the Associate Editor (M. Bloch). Their technical contributions to this article are gratefully acknowledged.

References

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

[2] R. F. Schaefer, H. Boche, A. Khisti, and H. V. Poor, *Information Theoretic Security and Privacy of Information Systems*. Cambridge, U.K.: Cambridge Univ. Press, 2017.

[3] P. A. Regalia, A. Khisti, Y. Liang, and S. Tomasin, "Secure communications via physical-layer and information-theoretic techniques," *Proc. IEEE*, vol. 103, no. 10, pp. 1698–1701, Oct. 2015.

[4] Y. Wu, A. Khisti, C. Xiao, G. Caire, K.-K. Wong, and X. Gao, "A survey of physical layer security techniques for 5G wireless networks and challenges ahead," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 4, pp. 679–695, Apr. 2018.

[5] L. Mucchi et al., "Physical-layer security in 6G networks," *IEEE Open J. Commun. Soc.*, vol. 2, pp. 1901–1914, 2021.

[6] A. Chorti et al., "Context-aware security for 6G wireless: The role of physical layer security," *IEEE Commun. Standards Mag.*, vol. 6, no. 1, pp. 102–108, Mar. 2022.

[7] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, no. 4, pp. 656–715, Oct. 1949.

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

[9] J. L. Massey, "A simplified treatment of Wyner's wiretap channel," in *Proc. 21st Allerton Conf. Commun., Control Comput.*, Monticello, IL, USA, 1983, pp. 268–276.

[10] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. IT-24, no. 3, pp. 339–348, May 1978.

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

[12] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas—Part I: The MISOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 7, pp. 3088–3104, Jul. 2010.

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

[14] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," *IEEE Trans. Inf. Theory*, vol. 57, no. 8, pp. 4961–4972, Aug. 2011.

[15] S. Loyka and C. D. Charalambous, "Optimal signaling for secure communications over Gaussian MIMO wiretap channels," *IEEE Trans. Inf. Theory*, vol. 62, no. 12, pp. 7207–7215, Dec. 2016.
[16] L. Dong, S. Loyka, and Y. Li, "The secrecy capacity of Gaussian MIMO wiretap channels under interference constraints," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 4, pp. 704–722, Apr. 2018.
[17] L. Dong, S. Loyka, and Y. Li, "Algorithms for globally-optimal secure signaling over Gaussian MIMO wiretap channels under interference constraints," *IEEE Trans. Signal Process.*, vol. 68, pp. 4513–4528, 2020.
[18] C. Mitrpant, A. J. H. Vinck, and Y. Luo, "An achievable region for the Gaussian wiretap channel with side information," *IEEE Trans. Inf. Theory*, vol. 52, no. 5, pp. 2181–2190, May 2006.
[19] N. Merhav, "Encoding individual source sequences for the wiretap channel," *Entropy*, vol. 23, no. 12, p. 1694, Dec. 2021.
[20] M. Bastani Parizi, E. Telatar, and N. Merhav, "Exact random coding secrecy exponents for the wiretap channel," *IEEE Trans. Inf. Theory*, vol. 63, no. 1, pp. 509–531, Jan. 2017.
[21] W. Yang, R. F. Schaefer, and H. V. Poor, "Wiretap channels: Nonasymptotic fundamental limits," *IEEE Trans. Inf. Theory*, vol. 65, no. 7, pp. 4069–4093, Jul. 2019.
[22] M. R. Bloch and J. N. Laneman, "Strong secrecy from channel resolvability," *IEEE Trans. Inf. Theory*, vol. 59, no. 12, pp. 8077–8098, Dec. 2013.
[23] T. S. Han, H. Endo, and M. Sasaki, "Reliability and secrecy functions of the wiretap channel under cost constraint," *IEEE Trans. Inf. Theory*, vol. 60, no. 11, pp. 6819–6843, Nov. 2014.
[24] O. Ozel, E. Ekrem, and S. Ulukus, "Gaussian wiretap channel with amplitude and variance constraints," *IEEE Trans. Inf. Theory*, vol. 61, no. 10, pp. 5553–5563, Oct. 2015.
[25] S. Sreekumar, A. Bunin, Z. Goldfeld, H. H. Permuter, and S. Shamai (Shitz), "The secrecy capacity of cost-constrained wiretap channels," *IEEE Trans. Inf. Theory*, vol. 67, no. 3, pp. 1433–1445, Mar. 2021.
[26] A. Favano, L. Barletta, and A. Dytso, "Amplitude constrained vector Gaussian wiretap channel: Properties of the secrecy-capacity-achieving input distribution," *Entropy*, vol. 25, no. 5, p. 741, Apr. 2023.
[27] Y. Liang, G. Kramer, H. V. Poor, and S. Shamai (Shitz), "Compound wiretap channels," *EURASIP J. Wireless Commun. Netw.*, vol. 2009, no. 1, Oct. 2009, Art. no. 142374.
[28] I. Bjelaković, H. Boche, and J. Sommerfeld, "Secrecy results for compound wiretap channels," *Problems Inf. Transmiss.*, vol. 49, no. 1, pp. 73–98, Jan. 2013.
[29] R. F. Schaefer and S. Loyka, "The secrecy capacity of compound Gaussian MIMO wiretap channels," *IEEE Trans. Inf. Theory*, vol. 61, no. 10, pp. 5535–5552, Oct. 2015.
[30] C. Li, Y. Liang, H. V. Poor, and S. Shamai (Shitz), "Secrecy capacity of colored Gaussian noise channels with feedback," *IEEE Trans. Inf. Theory*, vol. 65, no. 9, pp. 5771–5782, Sep. 2019.
[31] D. Gunduz, D. R. Brown, and H. V. Poor, "Secret communication with feedback," in *Proc. Int. Symp. Info. Theory Appl.*, Auckland, New Zealand, Dec. 2008, pp. 1–6.
[32] 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.
[33] 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.
[34] G. Keshet, Y. Steinberg, and N. Merhav, "Channel coding in the presence of side information," *Found. Trends Commun. Inf. Theory*, vol. 4, no. 6, pp. 445–586, 2008.
[35] S. I. Bross and A. Lapidoth, "The additive noise channel with a helper," in *Proc. IEEE Info. Theory Workshop (ITW)*, Aug. 2019, pp. 1–5.
[36] S. I. Bross, A. Lapidoth, and G. Marti, "Decoder-assisted communications over additive noise channels," *IEEE Trans. Commun.*, vol. 68, no. 7, pp. 4150–4161, Jul. 2020.
[37] A. Lapidoth and G. Marti, "Encoder-assisted communications over additive noise channels," *IEEE Trans. Inf. Theory*, vol. 66, no. 11, pp. 6607–6616, Nov. 2020.
[38] G. Marti, "Channels with a helper," M.S. thesis, Signal Info. Process. Lab., ETH Zürich, Zürich, Switzerland, Sep. 2019.
[39] A. Lapidoth, G. Marti, and Y. Yan, "Other helper capacities," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jul. 2021, pp. 1272–1277.
[40] N. Merhav, "On error exponents of encoder-assisted communication systems," *IEEE Trans. Inf. Theory*, vol. 67, no. 11, pp. 7019–7029, Nov. 2021.
[41] R. Fritschek and G. Wunder, "Towards a constant-gap sum-capacity result for the Gaussian wiretap channel with a helper," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jul. 2016, pp. 2978–2982.
[42] J. Chen and C. Geng, "Optimal secure GDoF of symmetric Gaussian wiretap channel with a helper," *IEEE Trans. Inf. Theory*, vol. 67, no. 4, pp. 2334–2352, Apr. 2021.
[43] T. M. Cover and J. A. Thomas, *Elements of Information Theory*. Hoboken, NJ, USA: Wiley, 2006.
[44] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge, U.K.: Cambridge Univ. Press, 2004.

Sergey Loyka (Senior Member, IEEE) was born in Minsk, Belarus. He received the M.S. degree (Hons.) from the Minsk Radioengineering Institute, Minsk, in 1992, and the Ph.D. degree in radio engineering from the Belarusian State University of Informatics and Radioelectronics (BSUIR), Minsk, in 1995. Since 2001, he has been a Faculty Member with the School of Electrical Engineering and Computer Science, University of Ottawa, Canada. Prior to that, he was a Research Fellow with the Laboratory of Communications and Integrated Microelectronics (LACIME), École de Technologie Supérieure, Montreal, Canada; a Senior Scientist with the Laboratory of Electromagnetic Compatibility, BSUIR; and an invited Scientist with the Laboratory of Electromagnetism and Acoustic (LEMA), Swiss Federal Institute of Technology Lausanne, Lausanne, Switzerland. His research interests include information theory, wireless communications and networks and, in particular MIMO systems and security aspects of such systems, in which he has published extensively. He received a number of awards from URSI, IEEE, the Swiss, Belarus and former USSR governments, and the Soros Foundation.

Neri Merhav (Life Fellow, IEEE) was born in Haifa, Israel, in March 1957. He received the B.Sc., M.Sc., and D.Sc. degrees in electrical engineering from the Technion—Israel Institute of Technology, in 1982, 1985, and 1988, respectively. From 1988 to 1990, he was with AT&T Bell Laboratories, Murray Hill, NJ, USA. Since 1990, he has been with the Department of Electrical Engineering, Technion—Israel Institute of Technology, where he is currently an Irving Shepard Professor. From 1994 to 2000, he was a Consultant with Hewlett-Packard Laboratories-Israel (HPL-I). His research interests include information theory, statistical communications, and statistical signal processing. He is especially interested in the areas of lossless/lossy source coding and prediction/filtering, relationships between information theory and statistics, detection, estimation, Shannon theory, including topics in joint source-channel coding, source/channel simulation, and coding with side information with applications to information hiding and watermarking systems. Another recent research interest concerns the relationships between information theory and statistical physics. He was a co-recipient of the Paper Award from the IEEE Information Theory Society in 1993, the American Technion Society Award for Academic Excellence in 1994, and the 2002 Technion Henry Taub Prize for Excellence in Research. More recently, he was a co-recipient of the Best Paper Award from the 2015 IEEE Workshop on Information Forensics and Security (WIFS 2015). He served as the Co-Chairperson for the Program Committee of the 2001 IEEE International Symposium on Information Theory. From 1996 to 1999, he served as an Associate Editor for source coding of IEEE TRANSACTIONS ON INFORMATION THEORY. From 2017 to 2020, he served as an Associate Editor for Shannon theory of IEEE TRANSACTIONS ON INFORMATION THEORY. He is on the editorial board of *Foundations and Trends in Communications and Information Theory*.