INFORMATION PROTECTION

Secrecy Results for Compound Wiretap Channels

I. Bjelaković, H. Boche, and J. Sommerfeld

Lehrstuhl für theoretische Informationstechnik, Technische Universität München, Germany
igor.bjelakovic@tum.de boche@tum.de jochen.sommerfeld@tum.de

Received June 20, 2011; in final form, October 24, 2012

Abstract—We derive a lower bound on the secrecy capacity of a compound wiretap channel with channel state information at the transmitter which matches the general upper bound on the secrecy capacity of general compound wiretap channels given by Liang et al. [1], thus establishing a full coding theorem in this case. We achieve this with a stronger secrecy criterion and the maximum error probability criterion, and with a decoder that is robust against the effect of randomization in the encoding. This relieves us from the need of decoding the randomization parameter, which is in general impossible within this model. Moreover, we prove a lower bound on the secrecy capacity of a compound wiretap channel without channel state information and derive a multiletter expression for the capacity in this communication scenario.

DOI: 10.1134/S0032946013010079

1. INTRODUCTION

Compound wiretap channels are among the simplest nontrivial models incorporating the requirement of security against a potential eavesdropper while at the same time legitimate users suffer from channel uncertainty. They may be considered therefore as a starting point for theoretical investigation tending towards applications, for example, in wireless systems, a fact explaining permanent research activity in this area in recent years (cf. [1,2] and references therein). In this paper we give capacity results for different scenarios of channel state information under a strong secrecy criterion and the maximum error probability criterion. In a more recent work [3], the authors make use of these results to derive capacity results for arbitrarily varying wiretap channels, a more realistic communication model, which, apart from eavesdropping, takes into account an active adversarial jamming situation.

In this paper we consider finite families of pairs of channels \( \mathcal{W} = \{ (W_t, V_t) : t = 1, \ldots, T \} \) with common input alphabet and possibly different output alphabets. Legitimate users control \( W_t \) and the eavesdropper observes the output of \( V_t \). We will be dealing with two communication scenarios. In the first, the transmitter is informed about the index \( t \) (channel state information (CSI) at the transmitter), while in the second the transmitter has no information about that index at all (no CSI). In both scenarios the eavesdropper knows and the legitimate receiver does not know the channel state. This setup is a generalization of Wyner’s [4] wiretap channel.

Along the way we will comment what our results look like when applied to widely used class of models of the form \( \mathcal{W} = \{ (W_t, V_s) : t = 1, \ldots, T, s = 1, \ldots, S \} \) with \( T \neq S \), which are special cases of the model we are dealing with in this paper.

Our contributions are summarized as follows: In [1] a general upper bound on the capacity of compound wiretap channel as the minimum secrecy capacity of the involved wiretap channels was

---

1 Supported in part by the Deutsche Forschungsgemeinschaft (DFG), project nos. BO 1734/16-1 and BO 1734/20-1, and Bundesministerium für Bildung und Forschung (BMBF), grant no. 01BQ1050.
given. We prove in Section 3.2 that the models whose secrecy capacity matches this upper bound contain all compound wiretap channels with CSI at the transmitter. At the same time, we achieve this bound with a substantially stronger security criterion employed already in [5–8]. Indeed, our security proof follows closely that developed in [8] for a single wiretap channel with classical input and quantum output. In order to achieve secrecy, we follow the common approach according to which randomized encoding is a permissible operation. Usually, the legitimate decoder can decode the sent codeword that represents both the message to be transmitted and the outcome of the random experiment as well. However, in the case of a compound wiretap channel with CSI at the transmitter, this strategy does not work, as is illustrated by an example in Section 4.1. We resolve this difficulty by developing a decoding strategy which is independent of the particular channel realization and is insensitive to randomization while decoding just at the optimal secrecy rate for all channels \{W_t : t = 1, \ldots, T\} simultaneously.

Moreover, a slight modification of our proofs allows us to determine the capacity of the compound wiretap channel without CSI by a (noncomputable) multiletter expression. This is the content of Section 3.3. We should mention, however, that the traditional proof strategy of sending the pair consisting of message and randomization parameter to the legitimate receiver works as well in the case where the transmitter has no CSI. The lower bound on the secrecy capacity that we prove under the strong secrecy criterion was used for parts of the secrecy results for arbitrarily varying wiretap channels in [3]. The lower bound on the secrecy capacity as well the as the multiletter expression were given earlier in [1], respectively in [2], for weaker secrecy criteria but without detailed proofs.

In Section 4.2 we give an example of a compound wiretap channel such that both the set of channels to the legitimate receiver and that to the eavesdropper are convex but whose secrecy capacities with CSI and without CSI at the transmitter are different. Indeed, the former is positive, while the latter is equal to 0.

Section 3.4 is devoted to the practically important model \(\mathcal{W} = \{(W_t, V_s) : t = 1, \ldots, T, s = 1, \ldots, S\}\) with the assumption that the transmitter has CSI for the \(T\)-part but has no CSI for the \(S\)-part of the channel. Here again we provide a multiletter expression for the capacity. Additionally, we give a computable description of the secrecy capacity in the case where the channels to the eavesdropper are degraded versions of those to the legitimate receiver.

Our results are easily extended to arbitrary sets (even uncountable) of wiretap channels via standard approximation techniques [9].

2. COMPOUND WIRETAP CHANNELS

2.1. Definitions

Let \(A, B, C\) be finite sets and \(\theta = \{1, \ldots, T\}\) an index set. We consider two families of channels \(W_t : A \rightarrow \mathcal{P}(B)^2\), \(V_t : A \rightarrow \mathcal{P}(C)\), \(t \in \theta\), which we collectively abbreviate by \(\mathcal{W}\) and call the compound wiretap channel generated by the given families of channels. Here the first family represents the communication link to the legitimate receiver, while the output of the latter is under control of the eavesdropper. In the rest of the paper, expressions like \(W_t^{\otimes n}\) or \(V_t^{\otimes n}\) stand for the \(n\)th memoryless extension of the stochastic matrices \(W_t, V_t\).

An \((n, J_n)\) code for the compound wiretap channel \(\mathcal{W}\) consists of a stochastic encoder \(E : J_n \rightarrow \mathcal{P}(A^n)\) (a stochastic matrix) with a message set \(J_n := \{1, \ldots, J_n\}\) and a collection of mutually disjoint decoding sets \(D_j \subset B^n : j \in J_n\). The maximum error probability of an \((n, J_n)\) code \(C_n\)

\(\mathcal{P}(B)\) denotes the set of probability distributions on \(B\).
is given by
\[ e(C_n) := \max_{t \in \mathcal{\Theta}} \max_{j \in \mathcal{J}_n} \sum_{x_n^T \in \mathcal{A}_n^n} E(x^n | j) W_t^{\otimes n}(D_j^c | x^n); \] (1)
i.e., neither the sender nor the receiver have CSI.

If channel state information is available at the transmitter, the notion of an \((n, J_n)\) code is modified in that the encoding may depend on the channel index, while the decoding sets remain universal, i.e., independent of the channel index \(t\). The probability of error in (1) changes to
\[ e_{\text{CSI}}(C_n) := \max_{t \in \mathcal{\Theta}} \max_{j \in \mathcal{J}_n} \sum_{x_n^T \in \mathcal{A}_n^n} E_t(x^n | j) W_t^{\otimes n}(D_j^c | x^n). \]

We assume throughout the paper that the eavesdropper always knows which channel is in use.

**Definition.** A nonnegative number \(R\) is an achievable secrecy rate for the compound wiretap channel \(\mathcal{W}\) with or without CSI, respectively, if there is a sequence \((C_n)_{n \in \mathbb{N}}\) of \((n, J_n)\) codes such that
\[ \lim_{n \to \infty} e(C_n) = 0, \quad \text{respectively,} \quad \lim_{n \to \infty} e_{\text{CSI}}(C_n) = 0, \]
and
\[ \lim_{n \to \infty} \min_{t \in \mathcal{\Theta}} \frac{1}{n} \log J_n \geq R, \] (2)
where \(J\) is a uniformly distributed random variable taking values in \(\mathcal{J}_n \) and \(Z^n_t\) are the resulting random variables at the output of eavesdropper’s channel \(V_t^{\otimes n}\).

The secrecy capacity in either scenario is given by the largest achievable secrecy rate and is denoted by \(C_{S}(\mathcal{W})\) and \(C_{S,\text{CSI}}(\mathcal{W})\).

### 2.2. Hints on Operational Meaning of Strong Secrecy

A weaker and widely used security criterion is obtained if we replace (2) by
\[ \lim_{n \to \infty} \max_{t \in \mathcal{\Theta}} \frac{1}{n} I(J; Z^n_t) = 0. \]
We prefer to follow [5, 7, 8] and require the validity of (2). A nice discussion on interrelation of several secrecy criteria is contained in [2]. We confine ourselves to giving some hints on the operational meaning of requirement (2). To this end, we restrict our attention to the case where the transmitter has no CSI in order to simplify our notation. The case of a compound wiretap channel with CSI at the transmitter can be treated accordingly. Set
\[ \varepsilon_n := \max_{t \in \mathcal{\Theta}} I(J; Z^n_t) \quad \text{with} \quad \lim_{n \to \infty} \varepsilon_n = 0. \]
Then Pinsker’s inequality implies that
\[ \|p_{jZ^n_t} - p_j \otimes p_{Z^n_t}\| \leq c\sqrt{\varepsilon_n}, \quad \forall t \in \mathcal{\Theta}, \] (3)
with a positive universal constant \(c\), where \(\| \cdot \|\) is the variational distance. Assume that the eavesdropper chooses for each \(t \in \mathcal{\Theta}\) decoding sets \(\{K_{j,t} \subset C^n : j \in \mathcal{J}_n\}\) with \(C^n = \bigcup_{j \in \mathcal{J}_n} K_{j,t}\). We will lower bound the average error probability (and consequently the maximum error probability) for every choice of the decoding rule the eavesdropper might make. Set
\[ e_{\text{av}}(t) := \frac{1}{J_n} \sum_{j \in \mathcal{J}_n} \sum_{x_n^T \in \mathcal{A}_n^n} E(x^n | j) V_t^{\otimes n}(K_{j,t}^c | x^n). \]
Then
\[ e_{av}(t) = \sum_{j \in J_n} p_{1N^n}(\{j\} \times K_{j,t}^c) = p_{1N^n}(\bigcup_{j \in J_n} \{j\} \times K_{j,t}^c) \]
\[ \geq p_j \otimes p_{Z^n_t}(\bigcup_{j \in J_n} \{j\} \times K_{j,t}^c) - c\varepsilon_n \]
\[ = \sum_{j \in J_n} p_j \otimes p_{Z^n_t}(\{j\} \times K_{j,t}^c) - c\varepsilon_n = \frac{1}{J_n} \sum_{j \in J_n} p_{Z^n_t}(K_{j,t}^c) - c\varepsilon_n \]
\[ = \frac{J_n - 1}{J_n} - c\varepsilon_n = 1 - 1 - \frac{1}{J_n} - c\varepsilon_n, \quad (4) \]

where in the first and third lines we have used the fact that the sets \(\{j\} \times K_{j,t}^c, j \in J_n\), are mutually disjoint, the second line follows from (3), and in the fourth line we merely observed that for any nonnegative numbers \(a_1, \ldots, a_J\) with \(\sum_{j=1}^{J} a_j = 1\) we have \(\sum_{j=1}^{J} (1 - a_j) = J - 1\). Consequently, the average (and hence maximum) error probability of every decoding strategy the eavesdropper might select tends to 1 as soon as \(J_n \to \infty\). It should be remarked, however, that although for the vast majority of messages the eavesdropper will be in error, there is still a possibility left that she/he can decode a small fraction of them correctly.

As will follow from the proofs below, we will have \(\varepsilon_n = 2^{-na}, a > 0\), and \(J_n = 2^{nR}, R > 0\), if the secrecy capacity is positive, so that the speed of convergence in (4) will be exponential.

Note that (3) means that the random variables \(Z^n_t\) at the output of the channel to the eavesdropper are almost independent of the random variable \(J\) embodying the messages to be transmitted to the legitimate receiver. Therefore, it is heuristically convincing that our criterion (2) offers secrecy to some extent for communication tasks going beyond the transmission of messages. To demonstrate this by an example, we introduce, based on [10], the notion of identification attack as follows. Assume that for each fixed \(t \in \theta\) and any \(j \in J_n\) there is a subset \(K_{j,t} \subset C^n\) on the eavesdropper’s output alphabet, where now the sets \(K_{j,t}\) need not necessarily be mutually disjoint. With \(E: J_n \to \mathcal{P}(A^n)\) being the stochastic encoder used to transmit messages to the legitimate receiver, we can write down the identification errors of first and second kind (cf. [10] for further explanation of this code concept) for the eavesdropper’s channel as
\[ \sum_{x^n \in A^n} E(x^n, j) V_t^{\otimes n}(K_{j,t}^c | x^n), \quad (5) \]
and
\[ \sum_{x^n \in A^n} E(x^n, i) V_t^{\otimes n}(K_{j,t} | x^n) \quad (6) \]
for \(j, i \in J_n, i \neq j\).

One possible interpretation of this attack, again based on [10], is that on the eavesdropper’s side of the channel there are persons \(F_1, \ldots, F_{J_n}\) observing the output of the channel. The sole interest of \(F_j\) is whether or not the message \(j\) has been sent to the legitimate receiver. Thus, \(F_j\) performs the hypothesis test represented by \(K_{j,t}\) based on his/her knowledge of \(t \in \theta\), and (5) and (6) are just the errors of the first and, respectively, second kind for that hypothesis test.

Let us define for \(j \in J_n\)
\[ g(j,t) := \sum_{x^n \in A^n} \left( E(x^n, j) V_t^{\otimes n}(K_{j,t}^c | x^n) + \frac{1}{J_n - 1} \sum_{i=1 \atop i \neq j}^{J_n} E(x^n, i) V_t^{\otimes n}(K_{j,t} | x^n) \right), \]
which is a number in \([0,2]\).
Note that if
\[ g(j, t) \geq 1 - \eta \]
for some \( \eta \in (0, 1) \), then either
\[ \sum_{x^n \in A^n} E(x^n | j)V_t^{\otimes n}(K^n_{j,t} | x^n) \geq \frac{1-\eta}{2}, \]
or there is at least one \( i \neq j \) with
\[ \sum_{x^n \in A^n} E(x^n | i)V_t^{\otimes n}(K^n_{j,t} | x^n) \geq \frac{1-\eta}{2}, \]
or both, so that no reliable identification of message \( j \) can be guaranteed. We show now that under the assumption of (2) we have
\[ \frac{1}{J_n} \sum_{j=1}^{J_n} g(j, t) \geq 1 - \eta_n, \quad \eta_n = o(n^0), \tag{7} \]
so that at most a fraction \( \frac{2}{3}(1 + \eta_n) \) of \( j \in J_n \) can satisfy the inequality
\[ g(j, t) < \frac{1}{2}. \]
This last assertion is readily seen from (7) by applying Markov’s inequality to the set
\[ F := \{ j \in J_n : 2 - g(j, t) > \frac{3}{2} \}. \]
In order to prove (7), note that for any \( t \in \theta \)
\[ \frac{1}{J_n} \sum_{j=1}^{J_n} g(j, t) = \sum_{j=1}^{J_n} \left( p_{JZ^n_t}(\{j\} \times K^n_{j,t}) + \frac{1}{J_n - 1} p_{JZ^n_t}(\{j\}^c \times K^n_{j,t}) \right) \]
\[ = p_{JZ^n_t} \left( \bigcup_{j \in J_n} \{j\} \times K^n_{j,t} \right) + \frac{1}{J_n - 1} \sum_{j=1}^{J_n} p_{JZ^n_t}(\{j\}^c \times K^n_{j,t}) \]
\[ \geq p_j \otimes p_{Z^n_t} \left( \bigcup_{j \in J_n} \{j\} \times K^n_{j,t} \right) + \frac{1}{J_n - 1} \sum_{j=1}^{J_n} p_j \otimes p_{Z^n_t}(\{j\}^c \times K^n_{j,t}) \]
\[ - c\sqrt{\varepsilon_n} - \frac{c}{J_n - 1} \sqrt{\varepsilon_n} \]
\[ = \frac{1}{J_n} \sum_{j=1}^{J_n} \left( p_{Z^n_t}(K^n_{j,t}) + p_{Z^n_t}(K^n_{j,t}) \right) - c\sqrt{\varepsilon_n} \frac{2J_n - 1}{J_n - 1} \]
\[ = 1 - c\sqrt{\varepsilon_n} \frac{2J_n - 1}{J_n - 1}, \]
where in the third line we have used (3) and in the fourth we inserted \( p_j(\{j\}^c) = \frac{J_n - 1}{J_n} \).

Besides the attempts of the eavesdropper to decode or identify messages, we can introduce attacks corresponding to each communication task introduced in [11]. It would be interesting, not only from the mathematical point of view, to see against which of them and to what extent secrecy can be guaranteed by condition (2).
3. CAPACITY RESULTS

3.1. Preliminaries

In what follows we use the notation as well as some properties of typical and conditionally typical sequences from [12]. For \( p \in \mathcal{P}(A) \), \( W: A \to \mathcal{P}(B) \), \( x^n \in A^n \), and \( \delta > 0 \), we denote by \( T^n_{p,\delta} \) the set of typical sequences and by \( T^n_{W,\delta}(x^n) \) the set of conditionally typical sequences given \( x^n \) in the sense of [12].

Basic properties of these sets that are needed in the sequel are summarized in the following three lemmas.

**Lemma 1.** Fixing \( \delta > 0 \), for every \( p \in \mathcal{P}(A) \) and \( W: A \to \mathcal{P}(B) \) we have

\[
p^\otimes n(T^n_{p,\delta}) \geq 1 - (n + 1)|A|2^{-n\delta^2},
\]

\[
W^\otimes n(T^n_{W,\delta}(x^n) | x^n) \geq 1 - (n + 1)|A||B|2^{-n\delta^2}
\]

for all \( x^n \in A^n \) with \( c = 1/(2 \ln 2) \). In particular, there is \( n_0 \in \mathbb{N} \) such that for each \( \delta > 0 \), \( p \in \mathcal{P}(A) \), \( W: A \to \mathcal{P}(B) \), and \( n > n_0 \), we have

\[
p^\otimes n(T^n_{p,\delta}) \geq 1 - 2^{-n\delta^2},
\]

\[
W^\otimes n(T^n_{W,\delta}(x^n) | x^n) \geq 1 - 2^{-n\delta^2}
\]

with \( c' = \frac{c}{2} \).

**Proof.** Standard Bernstein–Sanov trick using the properties of types from [12] and Pinsker’s inequality. Details can be found, e.g., in [13] and references therein. \( \triangleleft \)

Recall that for \( p \in \mathcal{P}(A) \) and \( W: A \to \mathcal{P}(B) \), \( pW \in \mathcal{P}(B) \) denotes the output distribution generated by \( p \) and \( W \) and that \( x^n \in T^n_{p,\delta} \) and \( y^n \in T^n_{W,\delta}(x^n) \) imply that \( y^n \in T^n_{pW,2|A|\delta} \).

**Lemma 2.** Let \( x^n \in T^n_{p,\delta} \). Then for \( V: A \to \mathcal{P}(C) \)

\[
|T^n_{pW,2|A|\delta}| \leq \alpha^{-1},
\]

\[
V^n(z^n | x^n) \leq \beta \text{ for all } z^n \in T^n_{V,\delta}(x^n)
\]

hold, where

\[
\alpha = 2^{-n(H(pV) + f_1(\delta))},
\]

\[
\beta = 2^{-n(H(V|p) - f_2(\delta))}
\]

(8)

with universal \( f_1(\delta), f_2(\delta) > 0 \) satisfying \( \lim_{\delta \to 0} f_1(\delta) = 0 = \lim_{\delta \to 0} f_2(\delta) \).

**Proof.** Cf. [12], \( \triangleleft \)

In addition, we need a further lemma, which will be used to determine the rates at which reliable transmission to the legitimate receiver is possible.

**Lemma 3.** Let \( p, \tilde{p} \in \mathcal{P}(A) \) and two stochastic matrices \( W, \tilde{W}: A \to \mathcal{P}(B) \) be given. Further, let \( q \in \mathcal{P}(B) \) be the output distribution generated by \( p \) and \( W \). Fix \( \delta \in (0, \frac{1}{4|A||B|}) \). Then for every \( n \in \mathbb{N} \)

\[
q^\otimes n(T^n_{W,\delta}(x^n)) \leq (n + 1)|A||B|2^{-n(H(\tilde{p}W) - f(\delta))}
\]

for all \( x^n \in T^n_{p,\delta} \) holds for a universal \( f(\delta) > 0 \) and \( \lim_{\delta \to 0} f(\delta) = 0 \).
Proof. The proof can be found in [13] but is given here for the sake of completeness. Let \( \tilde{x}^n \in T^n_{\hat{p},\hat{\delta}} \) and \( y^n \in T^n_{W,\delta} (\tilde{x}^n) \). Then with the empirical distribution \( p_{\hat{y}^n}(b) = \frac{N(b|y^n)}{n} \), \( b \in B \) it follows by Lemma 2.6 in [12] that

\[
q^n(y^n) = 2^{-n(D(p_{\hat{y}^n}||q) + H(p_{\hat{y}^n}))} \leq 2^{-nH(p_{\hat{y}^n})},
\]

where the inequality holds since \( D(p_{\hat{y}^n}||q) \geq 0 \). By Lemma 2.10 in [12], because \( \tilde{x}^n \in T^n_{\hat{p},\hat{\delta}} \) and \( y^n \in T^n_{W,\delta} (\tilde{x}^n) \), it follows that \( y^n \in T^n_{\tilde{q},2|X|\delta} \), where \( \tilde{q} \) is the output distribution generated by \( \tilde{p} \) and \( \tilde{W} \), and thus

\[
\sum_{b \in B} |p_{\hat{y}^n}(b) - \tilde{q}(b)| \leq 2|A||B|\delta.
\]

By the continuity of the entropy function, it follows by Lemma 2.7 in [12] that

\[
|H(p_{\hat{y}^n}) - H(\tilde{q})| \leq -2|A||B|\delta \log \frac{2|A||B|\delta}{|B|} =: \varphi(\delta)
\]

with \( \lim_{\delta \to 0} \varphi(\delta) = 0 \). By the last two inequalities we obtain that

\[
q^n(T^n_{W,\delta}(\tilde{x}^n)) \leq |T^n_{W,\delta}(\tilde{x}^n)| 2^{-n(H(\tilde{q}) - \varphi(\delta))}.
\]  

(9)

By the proof of Lemma 2.13 in [12] it follows that

\[
|T^n_{W,\delta}(\tilde{x}^n)| \leq (n + 1)^{|A||B|} 2^{n(H(\tilde{W}|\tilde{p}) + \psi(\delta))}
\]

with \( \psi(\delta) > 0 \) and \( \lim_{\delta \to 0} \psi(\delta) = 0 \). Then from (9) by defining \( f(\delta) := \varphi(\delta) + \psi(\delta) \) we end up with

\[
q^n(T^n_{W,\delta}(\tilde{x}^n)) \leq (n + 1)^{|A||B|} 2^{-n(I(\tilde{p},\tilde{W}) - f(\delta))}.
\]

The assertion still holds if we replace \( \tilde{W} \) by \( W \) and \( \tilde{p} \) by \( p \) throughout the proof. \( \triangle \)

The last lemma is a standard result from large deviation theory.

Lemma 4 (Chernoff–Hoeffding bounds). Let \( Z_1, \ldots, Z_L \) be i.i.d. random variables with values in \([0, 1]\) and expectation \( \mathbb{E} Z_i = \mu \), and let \( 0 < \varepsilon < \frac{1}{2} \). Then it follows that

\[
\Pr \left\{ \frac{1}{L} \sum_{i=1}^{L} Z_i \notin [(1 \pm \varepsilon)\mu] \right\} \leq 2 \exp \left( -L \frac{\varepsilon^2 \mu}{3} \right),
\]

where \([(1 \pm \varepsilon)\mu]\) denotes the interval \([(1 - \varepsilon)\mu, (1 + \varepsilon)\mu]\).

Proof. The proof is given in [14] (cf. Theorem 1.1) and in [15]. \( \triangle \)

3.2. CSI at the Transmitter

First we consider the case in which the transmitter has full knowledge of the channel state (CSI), while the legitimate receiver has no information about the channel state. The main result in this section is the following theorem.

Theorem 1. The secrecy capacity of the compound wiretap channel \( \mathcal{W} \) with CSI at the transmitter is given by

\[
C_{S,\text{CSI}}(\mathcal{W}) = \min_{t} \max_{U_t \rightarrow X_t \rightarrow (Y Z)_t} (I(U_t, Y_t) - I(U_t, Z_t)).
\]
Here $X_t$ is a random variable with probability distribution in $\mathcal{P}(A)$, and $U_t$ is an auxiliary random variable with range $A$ such that $U_t, X_t, (YZ)_t$ form a Markov chain $U_t \rightarrow X_t \rightarrow (YZ)_t$ in this order. Then the maximum refers to all random variables satisfying the Markov chain condition such that $X_t$ is connected with $Y_t$ (respectively, $Z_t$) by the channels $W_t$ (respectively, $V_t$) for every $t \in \theta$.

Note first that the inequality
\[
C_{S,\text{CSI}}(\mathcal{W}) \leq \min_{t \in \theta} \max_{U_t \rightarrow X_t \rightarrow (YZ)_t} (I(U_t, Y_t) - I(U_t, Z_t))
\]
is trivially true, since we cannot exceed the secrecy capacity of the worst wiretap channel in the family $\mathcal{W}$. This has been already pointed out in [1]. The rest of this section is devoted to the proof of the achievability.

Proof. It suffices to prove that $\min_{t \in \Theta} (I(X_t, Y_t) - I(X_t, Z_t))$ for $(XYZ)_t$ as above is an achievable secrecy rate. Then we will have shown that $R = \min_{t \in \Theta} (I(U_t, Y_t) - I(U_t, Z_t))$, with $U_t \rightarrow X_t \rightarrow (YZ)_t$ forming a Markov chain, is an achievable secrecy rate (cf. [12, p. 411]). We choose $p_1, \ldots, p_T \in \mathcal{P}(A)$ and define new probability distributions on $A^n$ by
\[
p'_t(x^n) := \begin{cases} p_t^{\otimes n}(x^n) & \text{if } x^n \in T^n_{p_t, \delta}, \\ 0 & \text{otherwise.} \end{cases}
\]
Define then for $z^n \in C^n$ and $x^n \in A^n$
\[
\tilde{Q}_{t,x^n}(z^n) = V_t^n(z^n \mid x^n) \cdot 1_{T^n_{p_t, \delta}(x^n)}(z^n)
\]
on $C^n$. Additionally, we set for $z^n \in C^n$
\[
\Theta'_t(z^n) = \sum_{x^n \in T^n_{p_t, \delta}} p'_t(x^n) \tilde{Q}_{t,x^n}(z^n).
\]

Now let $S := \{z^n \in C^n : \Theta'_t(z^n) \geq \varepsilon \alpha_t \}$ where $\varepsilon = 2^{-n\epsilon_\delta^2}$ (cf. Lemma 1) and $\alpha_t$ is from (8) in Lemma 2 computed with respect to $p_t$ and $V_t$. By Lemma 3.2, the support of $\Theta'_t$ has cardinality at most $\alpha^{-1}_t$, since for each $x^n \in T^n_{p_t, \delta}$ it holds that $T^n_{V_t, \delta}(x^n) \subseteq T^n_{p_t, \delta}$, which implies that
\[
\sum_{z^n \in S} \Theta_t(z^n) \geq 1 - 2\varepsilon
\]
if
\[
\Theta_t(z^n) = \Theta'_t(z^n) \cdot 1_S(z^n),
\]
\[
\tilde{Q}_{t,x^n}(z^n) = \tilde{Q}_{t,x^n}(z^n) \cdot 1_S(z^n).
\]

Now for each $t \in \theta$ define $J_n \cdot L_{n,t}$ i.i.d. random variables $X^{(t)}_{j,l}$ with $j \in [J_n] := \{1, \ldots, J_n\}$ and $l \in [L_{n,t}] := \{1, \ldots, L_{n,t}\}$, each of them distributed according to $p'_t$ with
\[
J_n = \left\lfloor 2^{n \min_{t \in \Theta} (I(p, W_t) - I(p, V_t)) - \tau} \right\rfloor, \quad \quad (13)
\]
\[
L_{n,t} = \left\lfloor 2^{n \left(I(p, V_t) + \frac{\delta}{4}\right) + \frac{1}{4}} \right\rfloor \quad (14)
\]
for $\tau > 0$. We also assume that the random matrices $\{X^{(t)}_{j,l}, j \in [J_n], l \in [L_{n,t}]\}$ and $\{X^{(t')}_{j,l}, j \in [J_n], l \in [L_{n,t}]\}$ are independent for $t \neq t'$. Now it is obvious from (11) and the definition of the set $S$ that for
any \( z^n \in S \) we have \( \Theta_t(z^n) = \mathbf{E} Q_{t,X_{jl}^{(t)}}(z^n) \geq \varepsilon \alpha_t \) if \( \mathbf{E} \) is the expectation value with respect to the distribution \( p_t' \). For the random variables \( \beta_t^{-1} Q_{t,X_{jl}^{(t)}}(z^n) \), define the event

\[
\tau_j(t) = \bigcap_{z^n \in C^n} \left\{ \frac{1}{L_{n,t}} \sum_{l=1}^{L_{n,t}} Q_{t,X_{jl}^{(t)}}(z^n) \in [(1 \pm \varepsilon) \Theta_t(z^n)] \right\},
\]

and keeping in mind that \( \Theta_t(z^n) \geq \varepsilon \alpha_t \) for all \( z^n \in S \) it follows that for all \( j \in [J_n] \) and for all \( t \in \theta \)

\[
\Pr\{ (\tau_j(t))^c \} \leq 2|C|^n \exp\left(-L_{n,t} \frac{2^{-n[I(p_n,V_t)]+g(\delta)\varepsilon^n}}{3}\right)
\]

by Lemma 4, Lemma 2, and our choice \( \varepsilon = 2^{-nc_3\delta^2} \) with \( g(\delta) := f_1(\delta) + f_2(\delta) + 3c_3^3\varepsilon^2 \). Making \( \delta > 0 \) sufficiently small, we have for all sufficiently large \( n \in \mathbb{N} \)

\[
L_{n,t}2^{n[I(p_n,V_t)]+g(\delta)\varepsilon^n} \geq 2^{n\varepsilon}\).
\]

Thus, for this choice of \( \delta \), the right-hand side of (16) is double exponential in \( n \) uniformly in \( t \) and can be made smaller than \( \varepsilon J_n^{-1} \) for all \( j \in [J_n] \) and all sufficiently large \( n \in \mathbb{N} \). Hence,

\[
\Pr\{ (\tau_j(t))^c \} \leq \varepsilon J_n^{-1}, \quad \forall t \in \theta.
\]

Now let us turn to the coding part of the problem. Let \( p_t' \in \mathcal{P}(A^n) \) be given as in (10). We abbreviate \( X := \{X^{(t)}\}_{t \in \theta} \) for the family of random matrices \( X^{(t)} = \{X_{jl}^{(t)}\}_{j \in [J_n], t \in [L_{n,t}]} \) whose components are i.i.d. according to \( p_t' \). Now we will show how reliable transmission of the message \( j \in [J_n] \) can be achieved when randomizing over the index \( l \in L_{n,t} \) without any attempt to decode the randomization parameter at the legitimate receiver (see Section 4.1). To this end, let us define for each \( j \in [J_n] \) a random set

\[
D'_j(X) := \bigcup_{s \in \theta} \bigcup_{k \in [L_{n,s}]} T^n_{W_s,\delta}(X_{j,k}^{(s)}),
\]

and the subordinate random decoder \( \{D_j(X)\}_{j \in [J_n]} \subseteq B^n \) is given by

\[
D_j(X) := D'_j(X) \cap \left( \bigcup_{j' \in [J_n]} D'_{j'}(X) \right)^c.
\]

Consequently, we can define the random average probabilities of error for a specific channel \( t \in \theta \) by

\[
\lambda_n^{(t)}(X) := \frac{1}{J_n} \sum_{j \in [J_n]} \frac{1}{L_{n,t}} \sum_{l \in [L_{n,t}]} \mathbf{W}_{t} \mathbb{E}((D_j(X))^c | X_{jl}^{(t)}).
\]

Now (18) implies for each \( t \in \theta \) and \( l \in [L_{n,t}] \)

\[
\mathbf{W}_{t} \mathbb{E}((D_j(X))^c | X_{jl}^{(t)}) \leq \mathbf{W}_{t} \mathbb{E} \left( \bigcap_{s \in \theta} \bigcap_{k \in [L_{n,s}]} \left( T^n_{W_s,\delta}(X_{j,k}^{(s)}) \right)^c | X_{jl}^{(t)} \right) + \sum_{j' \in [J_n]} \sum_{s \in \theta} \sum_{k \in [L_{n,s}]} \mathbf{W}_{t} \mathbb{E} \left( T^n_{W_s,\delta}(X_{j,k}^{(s)}) | X_{jl}^{(t)} \right) \leq \mathbf{W}_{t} \mathbb{E} \left( \bigcap_{s \in \theta} \bigcap_{k \in [L_{n,s}]} \left( T^n_{W_s,\delta}(X_{j,k}^{(s)}) \right)^c | X_{jl}^{(t)} \right) + \sum_{j' \in [J_n]} \sum_{s \in \theta} \sum_{k \in [L_{n,s}]} \mathbf{W}_{t} \mathbb{E} \left( T^n_{W_s,\delta}(X_{j,k}^{(s)}) | X_{jl}^{(t)} \right),
\]

PROBLEMS OF INFORMATION TRANSMISSION  Vol. 49  No. 1  2013
where the second inequality follows by the monotonicity of the probability. By Lemma 1 and the
independence of all involved random variables, we obtain

\[
E_X(W_t^{\otimes n}((D_j(X))^c | X_{jl}^{(t)})) \leq (n + 1)^{|A||B|} \cdot 2^{-nc\delta^2} + \sum_{j' \in [L_n]} \sum_{s \in \theta} \sum_{k \in [L_n,s]} E_{X_{j'k}}^{(s)} E_{X_{jl}}^{(t)} W_t^{\otimes n}(T_{W,s}^{n}(X_{j'k}^{(s)} | X_{jl}^{(t)})).
\]

(21)

Now we shall find for \(j' \neq j\) an upper bound on

\[
E_{X_{jl}}^{(t)} W_t^{\otimes n}(T_{W,s}^{n}(X_{j'k}^{(s)}) | X_{jl}^{(t)}) = \sum_{x^n \in A^n} p_t^n(x^n)W_t^{\otimes n}(T_{W,s}^{n}(X_{j'k}^{(s)}) | x^n) \leq \sum_{x^n \in A^n} \frac{p_t^n(x^n)}{p_t^{\otimes n}(T_{W,s}^{n})}W_t^{\otimes n}(T_{W,s}^{n}(X_{j'k}^{(s)}) | x^n) = \frac{q_t^n(T_{W,s}^{n}(X_{j'k}^{(s)}))}{p_t^{\otimes n}(T_{W,s}^{n})}.
\]

(22)

By Lemmas 1 and 3 for any \(t, s \in \theta\) we have

\[
\begin{align*}
p_t^{\otimes n}(T_{W,s}^{n}) & \geq 1 - (n + 1)^{|A|} \cdot 2^{-nc\delta^2}, \\
q_t^n(T_{W,s}^{n}(X_{j'k}^{(s)})) & \leq (n + 1)^{|A||B|} \cdot 2^{-n(I(p_s,W_s) - f(\delta))}
\end{align*}
\]

(23)

with a universal \(f(\delta) > 0\) satisfying \(\lim_{\delta \to 0} f(\delta) = 0\), since \(X_{j'k}^{(s)} \in T_{W,s}^{n}\) with probability 1. Thus, inserting this into (22), we obtain

\[
E_{X_{jl}}^{(t)} W_t^{\otimes n}(T_{W,s}^{n}(X_{j'k}^{(s)}) | X_{jl}^{(t)}) \leq \frac{(n + 1)^{|A||B|}}{1 - (n + 1)^{|A|} \cdot 2^{-nc\delta^2}} \cdot 2^{-n(I(p_s,W_s) - f(\delta))}
\]

for all \(s, t, \theta, j' \neq j\), and all \(t \in [L_n,t], k \in [L_n,s]\). Now, by defining \(\nu_n(\delta) := (n + 1)^{|A||B|} \cdot 2^{-nc\delta^2}\) and \(\mu_n(\delta) := 1 - (n + 1)^{|A|} \cdot 2^{-nc\delta^2}\), for each \(t \in \theta, l \in [L_n,t]\), and \(j \in [J_n]\), relations (21) and (22) thus lead to

\[
E_X(W_t^{\otimes n}((D_j(X))^c | X_{jl}^{(t)})) \leq \nu_n(\delta) + \frac{(n + 1)^{|A||B|}}{\mu_n(\delta)} J_n \sum_{s \in \theta} L_{n,s} 2^{-n(I(p_s,W_s) - f(\delta))} - \frac{\tau}{4}
\]

\[
\leq \nu_n(\delta) + \frac{(n + 1)^{|A||B|}}{\mu_n(\delta)} J_n 2^{-n(I(p_s,W_s) - I(p_s,V_s) - f(\delta) - \frac{\tau}{4})}
\]

\[
\leq \nu_n(\delta) + \frac{(n + 1)^{|A||B|}}{\mu_n(\delta)} T \cdot J_n 2^{-n(I(p_s,W_s) - I(p_s,V_s) - f(\delta) - \frac{\tau}{4})}
\]

\[
\leq \nu_n(\delta) + \frac{(n + 1)^{|A||B|}}{\mu_n(\delta)} T \cdot 2^{-n(\tau - f(\delta) - \frac{\tau}{4})}
\]

\[
\leq \nu_n(\delta) + \frac{(n + 1)^{|A||B|}}{\mu_n(\delta)} T \cdot 2^{-n\frac{\tau}{2}}
\]

(24)

where we have used (14), (13), and we have chosen \(\delta > 0\) small enough to ensure that \(\tau - f(\delta) - \frac{\tau}{4} \geq \frac{\tau}{2}\). Defining \(a = a(\delta, \tau) := \frac{1}{2} \min\left\{cd^2, \frac{\tau}{4}\right\}\), we can find \(n(\delta, \tau, |A|, |B|) \in \mathbb{N}\) such that for all \(n \geq n(\delta, \tau, |A|, |B|)\)

\[
E_X(W_t^{\otimes n}((D_j(X))^c | X_{jl}^{(t)})) \leq T \cdot 2^{-na}
\]

PROBLEMS OF INFORMATION TRANSMISSION Vol. 49 No. 1 2013
holds for all \( t \in \theta, l \in [L_{n,t}], \) and \( j \in [J_n] \). Consequently, for any \( t \in \theta \) we obtain

\[
\mathbf{E}_\mathcal{X}(\lambda_n^{(t)}(\mathcal{X})) \leq T \cdot 2^{-na}.
\]

Additionally, we define for any \( t \in \theta \) an event

\[
u_0(t) = \{ \lambda_n^{(t)}(\mathcal{X}) \leq \sqrt{T}2^{-n\frac{a}{2}} \}.
\]

Then, using the Markov inequality applied to \( \lambda_n^{(t)}(\mathcal{X}) \) along with (25), we obtain that

\[
\Pr\{\nu_0(t)\} \leq \sqrt{T}2^{-n\frac{a}{2}}.
\]

Set

\[
l := \bigcap_{t \in \theta} \bigcap_{k=0}^{J_n} \nu_k(t).
\]

Then with (17), (26), and applying the union bound we obtain

\[
\Pr\{l^c\} \leq \sum_{t \in \theta} \sum_{k=0}^{J_n} \Pr\{\nu_k(t)\} \leq T \cdot \varepsilon + T^{\frac{3}{4}} \cdot 2^{-n\frac{a}{2}} \leq T^2 \cdot 2^{-nc''}
\]

for a suitable positive constant \( c'' > 0 \) and all sufficiently large \( n \in \mathbb{N} \).

Hence, we have shown that for each \( t \in \theta \) there exist realizations \( \{(x_{jl}^{(t)})_{j \in [J_n], l \in [L_{n,t}]} : t \in \theta\} \in \nu \) of \( \mathcal{X} \). Now, denoting by \( \| \cdot \| \) the variational distance

\[
\|p - q\| := \sum_{x \in A} |p(x) - q(x)|
\]

for \( p, q \in A \), we show that the secrecy level is fulfilled uniformly in \( t \in \theta \) for any particular \( \{(x_{jl}^{(t)})_{j \in [J_n], l \in [L_{n,t}]} : t \in \theta\} \in \nu \). We have

\[
\left\| \frac{1}{L_{n,t}} \sum_{l=1}^{L_{n,t}} V_t^n(x_{jl}^{(t)}) - \Theta_t(\cdot) \right\| \leq \frac{1}{L_{n,t}} \sum_{l=1}^{L_{n,t}} \left\| V_t^n(x_{jl}^{(t)}) - \tilde{Q}_{t,x_{jl}^{(t)}}(\cdot) \right\|
\]

\[
+ \left\| \frac{1}{L_{n,t}} \sum_{l=1}^{L_{n,t}} (\tilde{Q}_{t,x_{jl}^{(t)}}(\cdot) - Q_{t,x_{jl}^{(t)}}(\cdot)) \right\| + \left\| \frac{1}{L_{n,t}} \sum_{l=1}^{L_{n,t}} Q_{t,x_{jl}^{(t)}}(\cdot) - \Theta_t(\cdot) \right\| \leq 5 \varepsilon.
\]

In the first term, the functions \( V_t^n(x_{jl}^{(t)}) \) and \( \tilde{Q}_{t,x_{jl}^{(t)}}(\cdot) \) differ if \( z^n \notin T^n_{p_{V_t},2|A|\theta} \), so it makes a contribution of \( \varepsilon \) to the bound. In the second term, \( \tilde{Q}_t \) and \( Q_t \) are different for \( z^n \notin S \) and because \( \nu_j(t) \) and \( \sum_{z^n \in S} \Theta_t(z^n) \geq 1 - 2 \varepsilon \) imply that

\[
\frac{1}{L_{n,t}} \sum_{l=1}^{L_{n,t}} \sum_{z^n \in S} Q_{t,x_{jl}^{(t)}}(z^n) \geq 1 - 3 \varepsilon,
\]

the second term is bounded by \( 3 \varepsilon \). The third term is bounded by \( \varepsilon \), which follows directly from (15).

For any \( \{(x_{jl}^{(t)})_{j \in [J_n], l \in [L_{n,t}]} : t \in \theta\} \in \nu \) with the corresponding decoding sets \( \{D_j : j \in [J_n]\} \), it follows by the construction that

\[
\frac{1}{J_n} \sum_{j \in [J_n]} \frac{1}{L_{n,t}} \sum_{l \in [L_{n,t}]} W_t^\otimes (D_j^c | x_{jl}^{(t)}) \leq \sqrt{T} \cdot 2^{-na'}
\]

(29)
for all \( t \in \theta \) with \( a' > 0 \), which means that we have found an \((n, J_n)\) code with average error probability tending to zero for \( n \in \mathbb{N} \) sufficiently large for any channel realization. Now by a standard expurgation scheme we show that this still holds for the maximum error probability. We define the set

\[
G_t := \left\{ j \in J_n : \frac{1}{L_{n,t}} \sum_{t \in [L_{n,t}]} W_t^{\otimes n}(D_{j}^{c} \mid x_{ji}^{(t)}) \leq \sqrt{\eta} \right\}
\]

with \( \eta := \sqrt{T} \cdot 2^{-n a'} \) and denote its complement by \( B_t := G_t^c \) and the union of all complements by \( B = \bigcup_{t \in \theta} B_t \). Then (29) and (30) imply that

\[
\eta \geq \frac{1}{J_n} \sum_{j \in [J_n]} \frac{1}{L_{n,t}} \sum_{t \in [L_{n,t}]} W_t^{\otimes n}(D_{j}^{c} \mid x_{ji}^{(t)}) \geq \frac{|B_t|}{J_n} \sqrt{\eta}
\]

for all \( t \in \theta \) and by the union bound it follows that

\[
|B| \leq \sum_{t \in \theta} |B_t| \leq T \cdot \sqrt{n} \cdot J_n.
\]

After removing all \( j \in B \) (which are at most a fraction of \( T \cdot 2^{-n a'} \) of \( J_n \)) and relabeling we obtain a new \((n, J_n)\) code \((E_j, D_j)_{j \in [J_n]}\) without changing the rate. The maximum error probability of the new code fulfills for sufficiently large \( n \in \mathbb{N} \)

\[
\max_{t \in \theta} \max_{j \in [J_n]} \frac{1}{L_{n,t}} \sum_{t \in [L_{n,t}]} W_t^{\otimes n}(D_{j}^{c} \mid x_{ji}^{(t)}) \leq T^* \cdot 2^{-n a'}.
\]

On the other hand, if we set

\[
\tilde{V}_t^n(z^n \mid (j, l)) := V_t^n(z^n \mid x_{ji}^{(t)})
\]

and further define

\[
\tilde{V}_{t,j}^n(z^n) = \frac{1}{L_{n,t}} \sum_{t \in [L_{n,t}]} \tilde{V}_t^n(z^n \mid (j, l)),
\]

\[
\tilde{V}_t^n(z^n) = \frac{1}{J_n} \sum_{j = 1}^{J_n} \tilde{V}_{t,j}^n(z^n),
\]

we obtain that

\[
\|\tilde{V}_{t,j}^n - \tilde{V}_t^n\| \leq \|\tilde{V}_{t,j}^n - \Theta_t\| + \|\Theta_t - \tilde{V}_t^n\| \leq 10\varepsilon,
\]

for all \( j \in [J_n] \) and \( t \in \theta \) with \( \varepsilon = 2^{-n a' \delta^2} \), where we have used the convexity of the variational distance and (28), which still applies by our expurgation procedure. For a uniformly distributed random variable \( J \) taking values in the set \( \{1, \ldots, J_n\} \), we obtain with Lemma 2.7 of [12] (uniform continuity of the entropy function)

\[
I(J; Z_t^n) = \sum_{j = 1}^{J_n} \frac{1}{J_n} (H(\tilde{V}_t^n) - H(\tilde{V}_{t,j}^n)) = H(Z_t^n) - H(Z_{j}^n \mid J) \leq -10\varepsilon \log(10\varepsilon) + 10n\varepsilon \log |C|
\]

uniformly in \( t \in \theta \) (for \( 10\varepsilon \leq e^{-1} \)). Hence, the strong secrecy level of the definition in Section 2.1 holds uniformly in \( t \in \theta \). Using standard arguments (cf. [12, p. 411]), we then have shown the achievability of the secrecy rate

\[
R_S = \min_{t \in \theta} \max_{U_t \rightarrow X_t \rightarrow (Y,Z)_t} (I(U_t, Y_t) - I(U_t, Z_t)). \quad \triangle
\]
Remark 1. Note that in the case that $\mathcal{W} := \{W_t, V_s : t = 1, \ldots, T, s = 1, \ldots, S\}$ with $S \neq T$ and the pair $(s, t)$ known to the transmitter prior to transmission nothing new happens. A slight modification of the arguments presented above shows that

$$C_{S,\text{CSI}}(\mathcal{W}) = \min_{(t, s)} \max_{U \rightarrow X \rightarrow (Y_t, Z_s)} (I(U, Y_t) - I(U, Z_s)).$$

3.3. No CSI

In the previous section we have assumed that the channel state is known to the transmitter. Now we consider the case where neither the transmitter nor the receiver has knowledge of the channel state. We will prove the following.

**Theorem 2.** For the secrecy capacity $C_S(\mathcal{W})$ of the compound wiretap channel $\mathcal{W}$ without CSI it holds that

$$C_S(\mathcal{W}) \geq \max_{p \in \mathcal{P}(A)} \left( \min_{t \in \theta} I(p, W_t) - \max_{t \in \theta} I(p, V_t) \right).$$

**Proof.** Caused by the lack of channel knowledge, we use a stochastic encoder independent of the channel realization. For any $p \in \mathcal{P}(A)$, let $p' \in \mathcal{P}(A^n)$ be the distribution by

$$p'(x^n) := \begin{cases} \frac{p^\otimes n(x^n)}{p^\otimes n(T_p, \delta)} & \text{if } x^n \in T_{p, \delta}^n, \\ 0 & \text{otherwise.} \end{cases}$$

Then, analogously to the case with CSI, we define $\tilde{Q}_{t,x^n}(z^n)$, $Q_{t,x^n}(z^n)$, $\Theta'_t(z^n)$, and $\Theta_t(z^n)$ for $z_n \in C^n$, but now with respect to the distribution $p'$. Consequently, $\Theta'_t(\cdot)$ has support only on $T_{p, \delta}^n$, and $Q_{t,x^n}(\cdot)$ and $\Theta_t(\cdot)$ only on the set $S$. Furthermore, $\Theta_t(z^n) \geq \varepsilon \alpha_t$ for all $z^n \in S$. Now define $J_n \cdot L_n$ i.i.d. random variables $X_{jl}$ according to the distribution $p'$ independent of $t \in \theta$ with $j \in [J_n]$ and $l \in [L_n]$ with

$$J_n = \left[ 2^n \left[ \min_t I(p, W_t) - \max_t I(p, V_t) - \tau \right] \right],$$

$$L_n = \left[ 2^n \left[ \max_t I(p, V_t) + \frac{1}{2} \right] \right],$$

for $\tau > 0$. Now, because $\Theta_t(z^n) = \mathbb{E} Q_{t,X_{jl}}(z^n) \geq \varepsilon \alpha_t$ for all $z^n \in S$, we define the event $\iota_j(t)$ as in (15) for the random variables $\beta_t^{-1} Q_{t,X_{jl}}$

$$\iota_j(t) = \bigcap_{z^n \in C^n} \left\{ \frac{1}{L_n} \sum_{l=1}^{L_n} Q_{t,X_{jl}}(z^n) \in \left[ (1 \pm \varepsilon) \Theta_t(z^n) \right] \right\},$$

but considering the difference that the random variables $X_{jl}$ are independent of the channel state. Then analogously to (16) we obtain that

$$\Pr\{ \iota_j(t)^c \} \leq 2|C|^n \exp\left( -L_n \frac{2^{-n}(I(p,V_t) + g(\delta))}{3} \right)$$

by Lemma 4 and Lemma 2. Note that, because the sender does not know which channel is used, we need the maximum in the definition of $L_n$. Thus, the right-hand side is double exponential in $n$ and can be made smaller than $\varepsilon J_n^{-1}$ for all $j$ and for all $t \in \theta$ and sufficiently large $n$.

Now let $J_n$ and $L_n$ be defined as stated above, and let $X^n = \{X_{jl}\}_{j \in [J_n], t \in [L_n]}$ be the set of i.i.d. random variables, each of them distributed according to $p'$ independent of $t \in \theta$. As in the case of
CSI, we can show that reliable transmission of the message \( j \in [J_n] \) can be achieved. To this end, define now the random decoder \( \{ D_j(X^n) \}_{j \in [J_n]} \subseteq B^n \) as in (18) but with
\[
D_j^n(X^n) := \bigcup_{s \in \theta} \bigcup_{k \in [L_n]} \mathcal{T}^{n}_{W_s,\delta}(X_{jk}),
\]
and the random average probabilities of error for a specific channel \( \lambda_n^{(t)}(X^n) \) as in (19). Note that now both \( X^n \) and \( L_n \) do not depend on \( t \in \theta \), and this holds throughout the entire proof. Then we can give the bound in (20) now by
\[
W^\otimes_t ((D_j(X^n))^c | X_{jl}) \leq W^\otimes_t ((\mathcal{T}^{n}_{W_s,\delta}(X_{jl}))^c | X_{jl}) + \sum_{j' \neq j} \sum_{s \in \theta} \sum_{k \in [L_n]} W^\otimes_t ((\mathcal{T}^{n}_{W_s,\delta}(X_{j'k}) | X_{jl}).
\]
We can bound the first term in the inequality by \( \nu_n(\delta) := (n+1)^{|A||B|} \cdot 2^{-nc_0^2} \) (see (21)). If we average over all codebooks, we get
\[
\mathbb{E}_{X^n}(W^\otimes_t ((D_j(X^n))^c | X_{jl})) \leq \nu_n(\delta) + \sum_{j' \neq j} \sum_{s \in \theta} \sum_{k \in [L_n]} \mathbb{E}_{X_{j'k}} \mathbb{E}_{X_{jl}} W^\otimes_t ((\mathcal{T}^{n}_{W_s,\delta}(X_{j'k}) | X_{jl}).
\]
By the same reasoning as in (22) and (23), we can give an upper bound on
\[
\mathbb{E}_{X_{jl}} W^\otimes_t (\mathcal{T}^{n}_{W_s,\delta}(X_{j'k}) | X_{jl}) \leq \frac{q^\otimes_t (\mathcal{T}^{n}_{W_s,\delta}(X_{j'k}))}{p^\otimes_t (\mathcal{T}^{n}_{p,\delta})} \leq \frac{(n+1)^{|A||B|}}{1 - (n+1)^{|A|} \cdot 2^{-nc_0^2}} \cdot 2^{-n(I(p,W_s) - f(\delta))}
\]
for all \( t \in \theta \), all \( j' \neq j \), and all \( k,l \in [L_n] \) with a universal \( f(\delta) > 0 \) satisfying \( \lim_{\delta \rightarrow 0} f(\delta) = 0 \). Here \( q^\otimes_t \) denotes the output distribution generated by the conditional distribution \( W^\otimes_t \) and the input distribution \( p^\otimes_t \). Additionally, we define \( \mu_n(\delta) := 1 - (n+1)^{|A|} \cdot 2^{-nc_0^2} \). Then (24) changes to
\[
\mathbb{E}_{X^n}(W^\otimes_t ((D_j(X^n))^c | X_{jl})) \leq \nu_n(\delta) + \frac{(n+1)^{|A||B|}}{\mu_n(\delta)} T \cdot J_n L_n \cdot 2^{-n(I(p,W_s) - f(\delta))}
\]
by the definition of \( J_n \) and \( L_n \) in (35) and (36) and by choosing \( \delta > 0 \) small enough so that \( \tau - \frac{T}{4} - f(\delta) \geq \frac{T}{2} \). Now, by defining \( a := \frac{1}{2} \min\{c_0^2 \cdot \frac{T}{2}\} \) and by the definition of the error probability, the last inequality results in the upper bound
\[
\mathbb{E}_{X^n}(\lambda_n^{(t)}(X^n)) \leq T \cdot 2^{-n a}
\]
for any \( t \in \theta \) and \( n \in \mathbb{N} \) large enough.

Now we define the event \( \epsilon_t(t) \) for any \( t \in \theta \) and the event \( \epsilon \) as in (25) and (27) but with the difference that the input is independent of the channel realization. Thus, by the same reasoning we end in
\[
\Pr \{ \epsilon \} \leq T^2 \cdot 2^{-nc''}
\]
for a constant \( c'' > 0 \) and all sufficiently large \( n \in \mathbb{N} \), which implies that there exist realizations \( \{ x_{jl} \} \) of \( \{ X_{jl} \} \) such that \( x_{jl} \in \epsilon \) for all \( j \in [J_n] \) and \( l \in [L_n] \). Then analogously to (28) we get for any channel \( t \in \theta \)
\[
\left\| \frac{1}{L_n} \sum_{l=1}^{L_n} V^n_t(\cdot | x_{jl}) - \Theta_t(\cdot) \right\| \leq 5 \varepsilon,
\]
which differs from the former by $L_n$ in place of $L_{n,t}$ only. Hence, following the same arguments subsequent to (29), we have shown that there is a sequence of $(n, \hat{J}_n)$ codes for which

$$\max_{t \in \theta} \max_{j \in \hat{J}_n} \frac{1}{n} \sum_{t \in [L_n]} W_i^{\infty}(D_j^c | x_{jt}) \leq T^{-\varepsilon} \cdot 2^{-n \frac{\varepsilon}{2}}$$

holds for sufficiently large $n \in \mathbb{N}$, and the strong secrecy level is fulfilled for every channel $t \in \theta$ by

$$\|\hat{V}_{t,j}^n - \hat{V}_t^n\| \leq 6\varepsilon$$

($\hat{V}_{t,j}^n, \hat{V}_t^n$ defined as in (32) and (33)) and thus by

$$I(J; Z_t^n) \leq -10\varepsilon \log(10\varepsilon) + 10n\varepsilon \log |\mathcal{C}|,$$

which tends to zero for $n \to \infty$ uniformly in $t \in \theta$. △

Now we turn to the converse of Theorem 2. Actually, we give only a multiletter formula for the upper bound of the secrecy rates. First we need the following lemma.

**Lemma 5.** Let $\mathcal{W} = \{(W_t, V_t) : t \in \theta\}$ be an arbitrary compound wiretap channel without CSI. Then

$$\lim_{n \to \infty} \frac{1}{n} \max_{U \to X^n \to Y_t^n Z_t^n} \left( \inf_{t \in \theta} I(U; Y_t^n) - \sup_{t \in \theta} I(U; Z_t^n) \right)$$

exists, and we have

$$\lim_{n \to \infty} \frac{1}{n} \max_{U \to X^n \to Y_t^n Z_t^n} \left( \inf_{t \in \theta} I(U; Y_t^n) - \sup_{t \in \theta} I(U; Z_t^n) \right) = \sup_{n \in \mathbb{N}} \frac{1}{n} \max_{U \to X^n \to Y_t^n Z_t^n} \left( \inf_{t \in \theta} I(U; Y_t^n) - \sup_{t \in \theta} I(U; Z_t^n) \right).$$

**Proof.** The proof is based on Fekete’s lemma [16]. Consequently, if we apply the lemma to the sequence $(a_n)_{n \in \mathbb{N}}$ defined by

$$a_n := \max_{U \to X^n \to Y_t^n Z_t^n} \left( \inf_{t \in \theta} I(U; Y_t^n) - \sup_{t \in \theta} I(U; Z_t^n) \right),$$

it suffices to show that the inequality

$$a_{n+m} \geq a_n + a_m$$

holds for all $n, m \in \mathbb{N}$. This will be done by considering two independent Markov chains $U_1 \rightarrow X^n \rightarrow (Y_t^n, Z_t^n)$ and $U_2 \rightarrow X^n \rightarrow (\hat{Y}_t^n, \hat{Z}_t^n)$ and setting $U := (U_1, U_2)$, $X^{n+m} := (X^n, \hat{X}_m)$, and $(Y_t^{n+m}, Z_t^{n+m}) := ((Y_t^n, \hat{Y}_t^m), (Z_t^n, \hat{Z}_t^m))$. Then, by the definition of $a_n$,

$$a_{n+m} \geq \inf_{t \in \theta} I(U; Y_t^{n+m}) - \sup_{t \in \theta} I(U; Z_t^{n+m})$$

$$\geq \inf_{t \in \theta} I(U_1; Y_t^n) + \inf_{t \in \theta} I(U_2; \hat{Y}_t^m) - \sup_{t \in \theta} I(U_1; Z_t^n) - \sup_{t \in \theta} I(U_2; \hat{Z}_t^m).$$

By the independence of the two Markov chains mentioned above and because, apart from that, these Markov chains were arbitrary, we can conclude that

$$a_{n+m} \geq a_n + a_m$$

holds for all $n, m \in \mathbb{N}$. △
Proposition 1. The secrecy capacity of the compound wiretap channel in the case of no CSI $C_S(\mathcal{M})$ is upper bounded by

$$C_S(\mathcal{M}) \leq \lim_{n \to \infty} \frac{1}{n} \max_{U \to X^n \to Y^n_t Z^n_t} \left( \inf_{t \in \theta} I(U; Y^n_t) - \sup_{t \in \theta} I(U; Z^n_t) \right).$$

Proof. Let $(C_n)_{n \in \mathbb{N}}$ be any sequence of $(n, J_n)$ codes such that, with

$$\sup_{t \in \theta} \frac{1}{J_n} \sum_{j=1}^{J_n} \sum_{x^n \in \mathcal{A}^n} E(x^n | j) W^n_1 \circ (D^n_2 | x^n) =: \varepsilon_{1,n}$$

and

$$\sup_{t \in \theta} I(J; Z^n_t) =: \varepsilon_{2,n},$$

it holds that $\lim \varepsilon_{1,n} = 0$ and $\lim \varepsilon_{2,n} = 0$, where $J$ denotes the random variable which is uniformly distributed on the message set $\{1, \ldots, J_n\}$. Let us denote by $\hat{J}$ the random variable with values in $\{1, \ldots, J_n\}$ determined by the Markov chain $J \to X^n \to Y^n_t \to \hat{J}$ where the first transition is governed by $E$, the second by $W^n_1 \circ$, and the last by the decoding rule. Then we have for any $t \in \theta$

$$\log J_n = H(J) = I(J; \hat{J}) + H(J | \hat{J}) \leq I(J; Y^n_t) + H(J | \hat{J}),$$

(38)

where the inequality follows from the data processing inequality. Then, using Fano’s inequality, we find that

$$H(J | \hat{J}) \leq 1 + \varepsilon_{1,n} \log J_n$$

with (37). Thus, we can rewrite inequality (38) as

$$(1 - \varepsilon_{1,n}) \log J_n \leq I(J; Y^n_t) + 1$$

for all $t \in \theta$. On the other hand, we have for every $t \in \theta$

$$I(J; Y^n_t) = I(J; Y^n_t) - \sup_{t \in \theta} I(J; Z^n_t) + \varepsilon_{2,n},$$

where we have used the validity of the secrecy criterion stated above. Then the last two inequalities imply that for any $t \in \theta$

$$(1 - \varepsilon_{1,n}) \log J_n \leq I(J; Y^n_t) - \sup_{t \in \theta} I(J; Z^n_t) + \varepsilon_{2,n}. \quad (39)$$

Since the left-hand side of (39) does not depend on $t$, we arrive at

$$(1 - \varepsilon_{1,n}) \log J_n \leq \max_{U \to X^n \to Y^n_t Z^n_t} \left( \inf_{t \in \theta} I(U; Y^n_t) - \sup_{t \in \theta} I(U; Z^n_t) \right) + \varepsilon_{2,n},$$

which concludes the proof after dividing by $n \in \mathbb{N}$, taking limsup, and taking into account the assertion of Lemma 5. △

Remark 2. Following the same arguments subsequent to (34) concerning the use of the channels defined by $P_{Y_t | T} = W_t \cdot P_{X | T}$ and $P_{Z_t | T} = V_t \cdot P_{X | T}$ instead of $W_t$ and $V_t$ and applying the assertion of Theorem 2 to the $n$-fold product of channels $W_t$ and $V_t$, we can give the coding theorem for the multiletter case. The capacity of the compound wiretap channel in the case of no CSI is

$$C_S(\mathcal{M}) = \lim_{n \to \infty} \frac{1}{n} \max_{U \to X^n \to Y^n_t Z^n_t} \left( \inf_{t \in \theta} I(U; Y^n_t) - \sup_{t \in \theta} I(U; Z^n_t) \right).$$
Now let us consider the case \( \mathfrak{W} := \{W_t, V_s : t = 1, \ldots, T, s = 1, \ldots, S\} \) with \( S \neq T \) and the pair \((s, t)\) unknown to both the transmitter and the legitimate receiver. Additionally, we assume that each \( V_s \) is a degraded version of every \( W_t \), which is characterized by

\[
V_s(z | x) = \sum_{y \in B} W_t(y | x) D_{(t,s)}(z | y), \tag{40}
\]

for all \( x \in A \) and \( z \in C \) if \( D \) is defined as the stochastic matrix \( D : B \to \mathcal{P}(C) \). Then we have the following statement.

**Lemma 6.** Let \( p \in \mathcal{P}(A) \), \( W : A \to \mathcal{P}(B) \), \( V : A \to \mathcal{P}(C) \), and assume that \( V \) is a degraded version of \( W \). Then \( I(X; Y | Z) \) is a concave with respect to the input distribution \( p_X = p \).

**Proof.** Let \( X, Y, Z \) be random variables with values in \( A, B, C \), respectively, distributed according to

\[
\Pr(X = x, Y = y, Z = z) := p_{XYZ}(x, y, z) = p(x)W(y | x)D(z | y) \tag{41}
\]

for all \( x \in A, y \in B \), and \( z \in Z \). Because

\[
I(X; Y | Z) = H(Y | Z) - H(Y | X, Z),
\]

the proof is based on the two assertions:

1. \( H(Y | Z) \) depends concavely on \( p_X \);
2. \( H(Y | X, Z) \) is an affine function of \( p_X \).

First, \( H(Y | Z) \) is a concave function with respect to \( p_{YZ} \) by the log-sum inequality (cf. [12, Lemma 3.1]). Then, because \( p_{XYZ} \) depends affinely on \( p_X \) by (41), so does \( p_{YZ} \), and the first assertion follows. For the second consider that (40) and (41) imply that

\[
p_{YZ}(y | x, z) = \frac{W(y | x)D(z | y)}{V(z | x)}
\]

for every input distribution \( p_X \), any \( y \in B \), and all \( x \in A, z \in C \) with \( p_{XZ}(x, z) > 0 \). Then we have

\[
H(Y | X, Z) = \sum_{x \in A, z \in C} p_{XZ}(x, z) H \left( \frac{W(\cdot | x)D(\cdot | z)}{V(z | x)} \right),
\]

showing that \( H(Y | X, Z) \) is an affine function of \( p_{XZ} \), which in turn depends affinely on \( p_X \). \( \triangle \)

Now because the random variables \( X, Y_t, \) and \( Z_s \) (\( Y_t \) and \( Z_s \) are the channel outputs of \( W_t \) and \( V_s \), respectively) form a Markov chain for all \( t \in \Theta \) and \( s \in \mathcal{S} \), we obtain that

\[
I(X; Y_t | Z_s) = I(X, Y_t) - I(X, Z_s). \tag{42}
\]

By virtue of Theorem 2 of [17] we can show that for the secrecy rate it holds that

\[
R_S \leq \frac{1}{n} \sum_{i=1}^{n} I(X_i; Y_{i,t} | Z_{i,s}) + \varepsilon' \leq \max_{p \in \mathcal{P}(A)} \min_{(t, s)} (I(p, W_t) - I(p, V_s)).
\]

Now we can state the following result.
Proposition 2. If $V_s$ is a degraded version of $W_t$ for all $s \in S$ and $t \in \theta$, the capacity of the compound wiretap channel is given by

$$C_S(\mathcal{M}) = \max_{p \in \mathcal{P}(A)} \min_{(t,s)} (I(p,W_t) - I(p,V_s))$$

$$= \max_{p \in \mathcal{P}(A)} (\min_t I(p,W_t) - \max_s I(p,V_s)).$$

Remark 3. This result was obtained in [1] with a weaker notion of secrecy.

3.4. Channel State to the Legitimate Receiver is Known at the Transmitter (CSI_t)

We now consider the case in which the transmitter has knowledge of the channel state to the legitimate receiver $t \in \theta$ but the channel state to the eavesdropper $s \in S$ is unknown. We will denote this kind of channel state information by CSI_t. Consequently, we get for each $t \in \theta$ possible channel realizations $\mathcal{M}_t := \{(W_t,V_s) : s = 1, \ldots, S\}$. Then we can describe the compound channel as $\mathcal{M} = \bigcup_{t \in \theta} \mathcal{M}_t$.

Theorem 3. For the secrecy capacity $C_{S,CSI_t}(\mathcal{M})$ of the compound wiretap channel with CSI_t it holds that

$$C_{S,CSI_t}(\mathcal{M}) \geq \min_{t \in \theta} \max_{p \in \mathcal{P}(A)} (I(p,W_t) - \max_s I(p,V_s)).$$

Proof. Adapted to the channel realization $W_t$, define

$$p_t'(x^n) := \begin{cases} p_t^{n}(x^n) & \text{if } x^n \in T_{p_t,\delta}^n, \\ 0 & \text{otherwise} \end{cases}$$

for arbitrary input distributions $p_1, \ldots, p_T \in \mathcal{P}(A)$. Now define for $z^n \in C^n$ and $s \in S$

$$\tilde{Q}_{s,x^n}(z^n) = V_s^n(z^n | x^n) \cdot 1_{T_{V_s,\delta}^n(x^n)}(z^n)$$

on $C^n$. Additionally, we set for $z^n \in C^n$

$$\Theta_s'(z^n) = \sum_{x^n \in T_{p_t,\delta}^n} p_t'(x^n)\tilde{Q}_{s,x^n}(z^n).$$

Now let $S := \{z^n \in C^n : \Theta_s'(z^n) \geq \varepsilon \alpha_t,s\}$ where $\varepsilon = 2^{-nc'/\delta^2}$ and $\alpha_t,s$ is from (8) similarly to the former cases but computed with respect to $p_t$ and $V_s$. Then the support of $\Theta_s'$ has cardinality at most $\alpha_t^{-1,s}$, which implies that $\sum_{z^n \in S} \Theta_s(z^n) \geq 1 - 2\varepsilon$. Analogously to (12), define $\Theta_s(z^n)$ and $Q_{s,x^n}(z^n)$ with support on $S$ and further

$$J_n = \left\lfloor 2^n \left[ \min_t (I(p_t,W_t) - \max_s I(p_t,V_s)) - \tau \right] \right\rfloor,$$

$$L_{n,t} = \left\lfloor 2^n \left[ \max_s I(p_t,V_s) + \frac{\tau}{2} \right] \right\rfloor.$$  

As in the case of CSI, define random matrices $\{X_j^{(t)}\}_{j \in [J_n], t \in [L_{n,t}]}$ where the random variables $X_j^{(t)}$ are i.i.d. according to $p_t'$. We assume additionally that $\{X_j^{(t)}\}_{j,t}$ and $\{X_{j'}^{(t')}\}_{j',t}$ are independent for
We will show how reliable transmission of the message \( t \neq t' \). For any \( z^n \in S \) it follows that \( \Theta_s(z^n) = E Q_{s,t} (z^n) \geq \varepsilon \alpha_{t,s} \) if \( E \) is the expectation value with respect to the distribution \( p'_l \). For the random variables \( \beta_{t,s}^{-1} Q_{s,t} (z^n) \), define the event
\[
l_j(s, t) = \bigcap_{z^n \in C^n} \left\{ \frac{1}{L_{n,t}} \sum_{l=1}^{L_{n,t}} Q_{s,t} (z^n) \in [(1 \pm \varepsilon) \Theta_s(z^n)] \right\}.
\]
Then it follows that for all \( j \in [J_n] \) and for all \( s \in S \) it holds for each \( t \in \theta \)
\[
Pr\{ (t_j(s, t))^{c} \} \leq 2|C'| n \exp \left( \frac{-L_{n,t} 2^{-n(I(p_t,V_s) + g(\delta))}}{3} \right)
\]
by Lemmas 4 and 2. Thus, the right-hand side is double exponential in \( n \) uniformly in \( s \in S \) and \( t \in \theta \) (guaranteed by the maximum in \( s \in S \) in the definition of \( L_{n,t} \)) and can be made smaller than \( \varepsilon J_n^{-1} \) for all \( j \in [J_n] \) and all sufficiently large \( n \). Now the coding part of the problem is similar to the case with CSI. Let \( p'_l \in P(A^n) \) be given as in (43). We abbreviate \( X := \{ X(t) \}_{t \in \theta} \) for the family of random matrices \( X(t) = \{ X_{jl}^{(t)} \}_{j \in [J_n], t \in [L_{n,t}]} \) whose components are i.i.d. according to \( p'_l \).

We will show how reliable transmission of the message \( j \in [J_n] \) can be achieved. To this end, define now the random decoder \( D_j(X)_{j \in [J_n]} \subseteq B^n \) as in (18) and with
\[
D_j(X) := \bigcup_{r \in \theta} \bigcup_{k \in [L_{n,r}]} T_{W_r, \delta}(X_{j,k}^{(r)}),
\]
and the random average probabilities of error for a specific channel \( \lambda_n^{(t)}(X(t)) \) as in (19) by
\[
\lambda_n^{(t)}(X(t)) := \frac{1}{J_n} \sum_{j \in [J_n]} \frac{1}{L_{n,t}} \sum_{l \in [L_{n,t}]} W_t^{\otimes n}( (D_j(X) \cap X_{jl}^{(t)}) \).
\]
As in (20), we get for each \( t \in \theta \) and \( l \in [L_{n,t}] \)
\[
W_t^{\otimes n}( (D_j(X) \cap X_{jl}^{(t)}) \leq W_t^{\otimes n}( (T_{W_r, \delta}(X_{jl}^{(t)})) \cap X_{jl}^{(t)}) + \sum_{j' \in [J_n]} \sum_{r \in \theta} \sum_{k \in [L_{n,r}]} W_t^{\otimes n}( T_{W_r, \delta}(X_{j',k}^{(r)}) | X_{jl}^{(t)}).
\]
Then by Lemma 1 we can bound the first term on the right-hand side, so that together with the independence of all involved random variables we end up with
\[
E_{X} \left( \sum_{j' \neq j} \sum_{r \in \theta} \sum_{k \in [L_{n,r}]} W_t^{\otimes n}( T_{W_r, \delta}(X_{j',k}^{(r)}) | X_{jl}^{(t)}) \right) \leq (n + 1)|A||B| \cdot 2^{-n \delta^2} + \sum_{j' \neq j} \sum_{r \in \theta} \sum_{k \in [L_{n,r}]} E_{X_{jl}^{(t)}} E_{X_{j',k}^{(r)}} W_t^{\otimes n}( T_{W_r, \delta}(X_{j',k}^{(r)}) | X_{jl}^{(t)}).
\]
(46)

Now we shall find for \( j' \neq j \) by the same reasoning as in (22) and (23) an upper bound on
\[
E_{X_{jl}^{(t)}} W_t^{\otimes n}( T_{W_r, \delta}(X_{j,k}^{(r)}) | X_{jl}^{(t)}) \leq \frac{q_t^{n}(T_{W_r, \delta}(X_{j,k}^{(r)}))}{p_t^{n}(T_{p_t, \delta})} \leq \frac{(n + 1)|A||B|}{1 - (n + 1)|A| \cdot 2^{-n \delta^2}} \cdot 2^{-n(I(p_t,V_r) - f(\delta))}
\]
for all \( r, t \in \theta \), all \( j' \neq j \), and all \( l \in [L_{n,t}], k \in [L_{n,r}] \). Now, by defining \( \nu_n(\delta) := (n + 1)|A||B| \cdot 2^{-n \delta^2} \) and \( \mu_n(\delta) := 1 - (n + 1)|A| \cdot 2^{-n \delta^2} \), for each \( t \in \theta \), \( l \in [L_{n,t}] \), and \( j \in [J_n] \), relation (46) and the
last inequality thus lead to

\[ E_X(W_t^{\otimes n}((D_J(X)))^c | X^{(t)}) \leq \nu_n(\delta) + \frac{(n+1)|A||B|}{\mu_n(\delta)} J_n \sum_{r \in \Theta} L_{n,r} 2^{-n(I(p_r,W_r)-f(\delta))} \]

\[ \leq \nu_n(\delta) + \frac{(n+1)|A||B|}{\mu_n(\delta)} T J_n \cdot \frac{2^{-n}\min_{r \in \Theta}(I(p_r,W_r)-\max_{s}I(p_r,V_s))}{\mu_n(\delta)} \]

\[ \leq \nu_n(\delta) + \frac{(n+1)|A||B|}{\mu_n(\delta)} T \cdot 2^{-n\tau}, \]

where we have used the definitions of \( J_n \) and \( L_{n,r} \) in (44) and (45) and have chosen \( \delta > 0 \) small enough to ensure that \( \tau - f(\delta) - \frac{\tau}{4} \geq \frac{\tau}{2} \). Defining \( a = a(\delta, \tau):= \frac{1}{2} \min\{c\delta^2, \frac{\tau}{2}\} \), we can find \( n(\delta, \tau, |A|, |B|) \in \mathbb{N} \) such that for all \( n \geq n(\delta, \tau, |A|, |B|) \) we end in

\[ E_X(\lambda_{n}^{(t)}(X)) \leq T \cdot 2^{-na} \]

for any \( t \in \Theta \). To give a bound on the average probability of error, we define the event \( \iota_0(t) \) for any \( t \in \Theta \) as in (25), and the event

\[ \iota := \bigcap_{t \in \Theta} \bigcap_{s \in \mathcal{S}} \bigcap_{k=0}^{J_n} \iota_k(t, s) \]

differs from (27) only by the intersection over the unknown channel states \( s \in \mathcal{S} \). Thus, we can conclude that

\[ \Pr\{\iota^c\} \leq S \cdot T \cdot \varepsilon + S \cdot T^{\frac{4}{7}} \cdot 2^{-n\frac{\tau}{2}} \leq S \cdot T^2 \cdot 2^{-nc''} \]

holds for a suitable positive constant \( c'' > 0 \) and all sufficiently large \( n \in \mathbb{N} \), and we have shown that for each \( t \in \Theta \) there exist realizations \( \{(x_{jl}^{(t)})_{j \in \mathcal{J}_n, l \in \mathcal{L}_{n,t}} : t \in \Theta\} \in \iota \) of \( \mathcal{X} \). By the same reasoning as in (28), we get for any channel realization \( t \in \Theta \) to the legitimate receiver

\[ \left\| \frac{1}{L_{n,t}} \sum_{l=1}^{L_{n,t}} V_s^n(\cdot | x_{jl}^{(t)}) - \Theta_s(\cdot) \right\| \leq 5\varepsilon \]

for each of the unknown channels \( s \in \mathcal{S} \) to the eavesdropper. Now, because for any \( t \in \Theta \) we have a different codeword set \( \{x_{jl}^{(t)}\} \), we slightly change the definition in (31) to

\[ \tilde{V}_{(s,t)}^n(z^n | j, l) := V_s^n(z^n | x_{jl}^{(t)}) \]

and accordingly to \( \tilde{V}_{(s,t),j}^n \) and \( \tilde{V}_{(s,t)}^n \) in (32) and (33) in that way that these distributions are defined separately for each codeword set \( t \in \Theta \). Thus, we get that

\[ \left\| \tilde{V}_{(s,t),j}^n - \tilde{V}_{(s,t)}^n \right\| \leq 10\varepsilon \]

is fulfilled for all \( s \in \mathcal{S} \) for each individual channel \( t \in \Theta \) to the legitimate receiver.

Hence, using the same expurgation scheme as in the previous sections, we have shown that there is a sequence of \( (n, J_n) \) codes for which

\[ \max_{t \in \Theta} \max_{j \in \mathcal{J}_n} \frac{1}{L_{n,t}} \sum_{l \in \mathcal{L}_{n,t}} W_t^{\otimes n}(D_j^c | x_{jl}^{(t)}) \leq T^{\frac{2}{7}} \cdot 2^{-n\frac{\tau}{2}} \]

holds for sufficiently large \( n \in \mathbb{N} \), and the strong secrecy level is fulfilled for every channel \( t \in \Theta \) by

\[ I(J; Z_s^n) \leq -10\varepsilon \log(10\varepsilon) + 10n\varepsilon \log |C|, \]
which tends to zero for $n \to \infty$ for all channels $s \in S$ to the eavesdropper. Thus, we have shown that

$$R_S = \min_{t \in \theta} \max_{p \in \mathcal{P}(A)} \left( I(p, W_t) - \max_{s: (s,t) \in S \times \theta} I(p, V_s) \right)$$

is an achievable secrecy rate for the compound wiretap channel $\bigcup_{t \in \theta} \mathcal{M}_t$ in the case where the channel state to the legitimate receiver is known at the transmitter. $\triangle$

Remark 4. By considering the converse of Theorem 3, we get for each $t \in \theta$ possible channel realizations $\mathcal{M}_t := \{ (W_t, V_s) : s = 1, \ldots, S \}$. Then we can describe the compound channel as $\mathcal{M} = \bigcup_{t \in \theta} \mathcal{M}_t$. In accordance to the case of no CSI, for each $t \in \theta$ we obtain that

$$C_S(\mathcal{M}_t) = \lim_{n \to \infty} \frac{1}{n} \max_{U \to X^n \to Y^n Z^n} \left( I(U; Y^n_t) - \sup_{s \in S} I(U; Z^n_s) \right).$$

**Proposition 3.** The secrecy capacity $C_{S, \text{CSI}}(\mathcal{M})$ of the compound wiretap channel in the case where only the channel state to the legitimate receiver is known at the transmitter is given by

$$C_{S, \text{CSI}}(\mathcal{M}) = \inf_{t \in \theta} C_S(\mathcal{M}_t).$$

Now, let us additionally assume that each $V_s$ is a degraded version of every $W_t$ for $s \in S$ and $t \in \theta$. Then, as is shown in Lemma 6, $I(X; Y_t | Z_s)$ is a concave function with respect to the input distribution $p_X = p$. In particular, this still holds for $\min_{s \in S} I(X; Y_t | Z_s)$. Now, because the random variables $X, Y_t, Z_s$ form a Markov chain for all $t \in \theta$ and $s \in S$ and

$$\min_{s \in S} I(X; Y_t | Z_s) = I(X, Y_t) - \max_{s \in S} I(X, Z_s),$$

for any $t \in \theta$ we get the upper bound on the secrecy rate as the secrecy capacity of a single channel $W_t$ with $S$ channels to the eavesdropper. Then we can conclude as follows.

**Proposition 4.** The secrecy capacity of the channel where only channel states to the legitimate receiver are known and channels to the eavesdropper are degraded versions of those to the legitimate receiver is given by

$$C_{S, \text{CSI}}(\mathcal{M}) = \min_{t \in \theta} \max_{p \in \mathcal{P}(A)} \left( I(p, W_t) - \max_{s \in S} I(p, V_s) \right).$$

### 3.5. Compound Wiretap Channel with $C_S = C_{S, \text{CSI}}$

Let $\mathcal{M} := \{ (W_t, V_s) : t = 1, \ldots, T, s = 1, \ldots, S \}$ with $S \neq T$ and the pair $(t,s)$ unknown to both the transmitter and the legitimate receiver. In addition, let us assume that

$$\exists \hat{t} \in \theta \forall t \in \theta \exists U_t : W_{t} = U_t W_{\hat{t}},$$

which means that $W_{t}$ is a degraded version of all channels $W_t$ with $t \neq \hat{t}$. We further assume that

$$\exists \hat{s} \in S \forall s \in S \exists \hat{U}_s : V_{s} = \hat{U}_s V_{\hat{s}},$$

which means that all $V_s$ with $s \neq \hat{s}$ are degraded versions of $V_{\hat{s}}$. Then we can show that the capacity of this channel equals the capacity of the same channel with CSI at the transmitter, i.e.,

$$C_S(\mathcal{M}) = C_{S, \text{CSI}}(\mathcal{M}).$$

First, by Theorem 2 it holds that

$$C_S(\mathcal{M}) \geq \max_{M \to X \to (Y_t Z_s)} \min_{(t,s)} \left( I(M, Y_t) - I(M, Z_s) \right),$$

\[ (49) \]
where $M$ is an auxiliary random variable such that $M, X, (Y_t, Z_s)$ form a Markov chain $M \rightarrow X \rightarrow (Y_t Z_s)$ in this order. Now let

$$p^*_M = \arg \max_{M \rightarrow X \rightarrow (Y_t Z_s)} (I(M, Y_t) - I(M, Z_s))$$

be the joint distribution of $M$ and $X$ that achieves capacity for the single wiretap channel $(W_t, V_s)$. Because the capacity of the compound wiretap channel $\mathcal{W}$ is less than or equal to the capacity of each single channel, we obtain

$$C_{S, CSI}(\mathcal{W}) \leq I(p^*_M, W_t \cdot P^*_X | M) - I(p^*_M, V_s \cdot P^*_X | M)$$

$$\leq I(p^*_M, U_t(W_t \cdot P^*_X | M)) - I(p^*_M, \hat{U}_s(V_s \cdot P^*_X | M))$$

$$\leq I(p^*_M, W_t \cdot P^*_X | M) - I(p^*_M, V_s \cdot P^*_X | M)$$

(50)

for all $(s, t) \in S \times \theta$ because of (47) and (48). Then by the last inequality it follows that

$$I(p^*_M, W_t \cdot P^*_X | M) - I(p^*_M, V_s \cdot P^*_X | M) = \min_{(s, t)} (I(p^*_M, W_t \cdot P^*_X | M) - I(p^*_M, V_s \cdot P^*_X | M))$$

$$\leq \max_{M \rightarrow X \rightarrow (Y_t Z_s)} \min_{(t, s)} (I(M, Y_t) - I(M, Z_s)).$$

Now taking into account (49) and (50), we end in

$$C_{S, CSI}(\mathcal{W}) \leq C_S(\mathcal{W}),$$

and therewith for this channel the lower bound of the capacity without CSI matches the capacity of the compound wiretap channel with CSI.

4. EXAMPLES

In this section we provide some examples which display some striking features of compound wiretap channels as opposed to the usual compound channels. Our first example shows clearly that for compound wiretap channels with CSI at the transmitter the strategy of sending both the message and the randomization parameter does not work. The second example demonstrates that even in the case where the sets of channels to the legitimate receiver and the eavesdropper are both convex, we can have

$$C_{S, CSI}(\mathcal{W}) > 0 \quad \text{and} \quad C_S(\mathcal{W}) = 0,$$

as opposed to the case of the usual compound channel, where the minimax theorem applies.

In the following we use some simple facts, which we state here without proof.

**Fact 1.** The binary entropy function

$$h(x) := -x \log x - (1 - x) \log(1 - x), \quad x \in [0, 1],$$

is strictly increasing on $[0, \frac{1}{2}]$.

**Fact 2.** Let $\eta \in [0, 1]$ and set

$$D_\eta := \begin{pmatrix} 1 - \eta & \eta \\ \eta & 1 - \eta \end{pmatrix}.$$

Then for every $\tau, \tau' \in [0, 1]$ it follows that

$$D_\tau D_{\tau'} = D_{\tau + \tau' - 2\tau \tau'}.$$
Moreover, if \( \tau, \tau' \in (0, \frac{1}{2}) \), then

\[ \tau + \tau' - 2\tau\tau' \in (0, \frac{1}{2}) \quad \text{and} \quad \tau + \tau' - 2\tau\tau' > \tau, \tau'. \]

**Fact 3.** For \( \tau, t \in [0, 1] \),

\[ (1 - t)D_0 + tD_\tau = D_{t\tau}. \]

### 4.1. Example 1

Consider a compound wiretap channel \( \mathfrak{W} = \{(W_t, V_t) : t = 0, 1\} \) in the case of CSI at the transmitter. First we define the channels to the legitimate receiver and to the eavesdropper for \( t = 0 \) by

\[ W_0 = D_\eta, \quad \eta \in [0, \frac{1}{2}), \quad \eta \approx 0, \quad V_0 := D_\tau W_0, \quad \tau \in [0, \frac{1}{2}), \quad \tau \approx 0, \]

and for \( t = 1, \hat{\tau} \in (0, 1/2] \)

\[ W_1 := D_{\hat{\tau}} V_0 = D_{\hat{\tau}} D_\tau W_0, \quad V_1 := \begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix}. \]

Hence \( V_0 \) and \( W_1 \) are degraded versions of \( W_0 \), and

\[ I(p, V_1) = 0, \quad \forall p \in \mathcal{P}(A), \]

by the definition of \( V_1 \). Now for every \( p \in \mathcal{P}(A) \) we can choose \( \tau \) small enough such that

\[ I(p, W_0) - I(p, V_0) < I(p, W_1). \]

Now with \( p_0 = (\frac{1}{2}, \frac{1}{2}), \nu > 0 \), and because we have CSI at the transmitter, we have by the defining equations (13) and (14)

\[ J_n = 2^{n[I(p_0, W_0) - I(p_0, V_0)] - \nu], \]
\[ L_{n,0} = 2^{n[I(p_0, V_0) + \frac{\nu}{4}]}, \]

so that we obtain

\[ J_n L_{n,0} = 2^{n[I(p_0, W_0) - \frac{3\nu}{4}]} \]

But for \( \hat{\tau} \) close to \( 1/2 \) it holds then that

\[ I(p_0, W_0) - \frac{3\nu}{4} > I(p_0, W_1) = \max_{p \in \mathcal{P}(A)} I(p, W_1) = C_{\text{CSI}}\{W_0, W_1\}, \]

where \( C_{\text{CSI}}\{W_0, W_1\} \) is the capacity of a compound channel with CSI at the transmitter. Hence we have shown that we can achieve reliable transmission of the message \( j \in [J_n] \), but identifying both the message and the randomizing indices is not possible for all pairs \( j \in [J_n] \) and \( l \in [L_{n,t}] \).

This is in contrast to the case where we have only one channel to both the legitimate receiver and the eavesdropper (cf. [5,8]).
4.2. Example 2

Now, for η, τ ∈ (0, 1/2) we set

\[ W_0 = D_\eta, \quad V_0 := D_\tau W_0 = D_{\eta+\tau-2\eta\tau}, \]
\[ W_1 := D_\tau V_0 = D_{2\tau-2\tau^2} W_0, \quad V_1 := D_\tau V_1. \]

Note that \( V_0 \) is a degraded version of \( W_0 \), \( W_1 \) of \( V_0 \), and \( V_1 \) of \( W_1 \). Next we define for \( t \in [0, 1] \)

\[ W_t := (1-t)W_0 + tW_1 = [(1-t)D_0 + tD_{2\tau-\tau^2}]W_0, \quad (51) \]
\[ V_t := (1-t)V_0 + tV_1 = D_\tau [(1-t)D_0 + tD_{2\tau-2\tau^2}]W_0 = D_\tau W_t. \quad (52) \]

By the definition, the set of channels to the legitimate receiver \( \{W_t\} \) and the set of channels to the eavesdropper \( \{V_t\} \) are both convex. Nevertheless, we will show now that for the compound wiretap channel \( \mathfrak{W} := \{(W_t, V_t) : t \in [0, 1]\} \) we have

\[ C_{S,CSI}(\mathfrak{W}) > 0, \quad C_S(\mathfrak{W}) = 0. \]

To this end, note that by (51), Fact 3, and Fact 2 we have

\[ W_t = D_s(2\tau-\tau^2) D_\eta = D_{f(t,\eta,\tau)} \]

with

\[ f(t, \eta, \tau) := \eta + t(2\tau - 2\tau^2) - 2\eta t(2\tau - 2\tau^2) \in (0, \frac{1}{2}). \quad (53) \]

Similarly, from (52) and Fact 2 we obtain

\[ V_t = D_\tau D_{f(t,\eta,\tau)} = D_{\tau+f(t,\eta,\tau)-2\tau f(t,\eta,\tau)}. \]

Additionally, from (53) and Fact 2 we get

\[ \tau + f(t, \eta, \tau) - 2\tau f(t, \eta, \tau) \in (0, \frac{1}{2}) \]

and

\[ \tau + f(t, \eta, \tau) - 2\tau f(t, \eta, \tau) > f(t, \eta, \tau). \quad (54) \]
Taking $p = (1/2, 1/2)$, we obtain for every $t \in [0, 1]$
\[
I(p, W_t) - I(p, V_t) = h(\tau + f(t, \eta, \tau) - 2\tau f(t, \eta, \tau)) - h(f(t, \eta, \tau)) > 0,
\]
where the last inequality follows from Fact 1 and (54). Thus, we have shown that
\[
C_{S,CSI}(W) > 0
\]
holds by Theorem 1.

In order to show that $C_S(W) = 0$, we have to employ our multiletter converse in the case of no CSI, Proposition 1. First, a simple algebra shows that for any $t \in [0, 1]$
\[
V_t = ((1-t)D_0 + tD_{2r-2r^2})V_0
\]
by (52), and thus each $V_t$ is a degraded version of $V_0$. Now let us consider the Markov chain $U \rightarrow X^n \rightarrow (Y^n_t, Z^n_t)$ where the transition from the random variable $U$ to $Y^n_t$ is governed by $P_{Y^n_t|U} = V^n_t \cdot P_{X^n|U}$ for all $t \in [0, 1]$. Then we obtain that each $P_{Y^n_t|U}$ is a degraded version of $P_{Y^n_0|U} = V^n_0 \cdot P_{X^n|U}$, and the data processing inequality implies that for each $n \in \mathbb{N}$
\[
\max_{t \in [0,1]} I(U, Y^n_t) = I(U, Y^n_0)
\]
(55)
for all distributions $P_{UX^n}$ that satisfy the Markov chain condition $U \rightarrow X^n \rightarrow (Y^n_t, Z^n_t)$.

On the other hand, since $W_1 = D_\tau V_0$, we obtain for the matrix $P_{Z^n_t|U} = W^n_1 \cdot P_{X^n|U}$ by the data processing inequality and (55) for all $n \in \mathbb{N}
\[
I(U, Z^n_t) - \max_{t \in [0,1]} I(U, Y^n_t) = I(U, Z^n_1) - I(U, Y^n_0) \leq 0,
\]
for all $P_{UX^n}$. Then Proposition 1 implies that
\[
C_S(W) = 0,
\]
as desired.

REFERENCES
1. Liang, Y., Kramer, G., Poor, H.V., and Shamai (Shitz), S., Compound Wiretap Channels, EURASIP J. Wireless Commun. Networking, 2009, Art. ID 142374, 12 pp.
2. Bloch, M. and Laneman, J.N., On the Secrecy Capacity of Arbitrary Wiretap Channels, in Proc. 46th Ann. Allerton Conf. on Communication, Control, and Computing, Monticello, IL, USA, 2008, pp. 818–825.
3. Bjelaković, I., Boche, H., and Sommerfeld, J., Capacity Results for Arbitrarily Varying Wiretap Channels, accepted for publication in LNCS Volume in Memory of R. Ahlswede. 2012.
4. Wyner, A.D., The Wire-Tap Channel, Bell System Tech. J., 1975, vol. 54, no. 8, pp. 1355–1387.
5. Csiszár, I., Almost Independence and Secrecy Capacity, Probl. Peredachi Inf., 1996, vol. 32, no. 1, pp. 48–57 \[Probl. Inf. Trans. (Engl. Transl.), 1996, vol. 32, no. 1, pp. 40–47\].
6. Maurer, U.M. and Wolf, S., Information-Theoretic Key Agreement: From Weak to Strong Secrecy for Free, Advances in Cryptology – EUROCRYPT 2000 (Proc. Int. Conf. on the Theory and Application of Cryptographic Techniques, Bruges, Belgium, 2000), Preneel B., Ed., Lect. Notes Comp. Sci., vol. 1807, Berlin: Springer, 2000, pp. 351–368.
7. Cai, N., Winter, A., and Yeung, R.W., Quantum Privacy and Quantum Wiretap Channels, *Probl. Peredachi Inf.*, 2004, vol. 40, no. 4, pp. 26–47 [Probl. Inf. Trans. (Engl. Transl.), 2004, vol. 40, no. 4, pp. 318–336].

8. Devetak, I., The Private Classical Capacity and Quantum Capacity of a Quantum Channel, *IEEE Trans. Inform. Theory*, 2005, vol. 51, no. 1, pp. 44–55.

9. Blackwell D., Breiman L., Thomasian A.J. The Capacity of a Class of Channels, *Ann. Math. Statist.*, 1959, vol. 30, no. 4, pp. 1229–1241.

10. Ahlswede, R. and Dueck, G., Identification via Channels, *IEEE Trans. Inform. Theory*, 1989, vol. 35, no. 1, pp. 15–29.

11. Ahlswede, R., General Theory of Information Transfer: Updated, *Discrete Appl. Math.*, 2008, vol. 156, no. 9, pp. 1348–1388.

12. Csiszár, I. and Körner, J., *Information Theory: Coding Theorems for Discrete Memoryless Systems*, Cambridge: Cambridge Univ. Press, 2011, 2nd ed. First edition translated under the title *Teoriya informatsii: teoremy kodirovaniya dlya diskretnykh sistem bez pamyati*, Moscow: Mir, 1985.

13. Wyrembelski, R.F., Bjelaković, I., Oechtering, T.J., and Boche, H., Optimal Coding Strategies for Bidirectional Broadcast Channels under Channel Uncertainty, *IEEE Trans. Commun.*, 2010, vol. 58, no. 10, pp. 2984–2994.

14. Dubhashi, D.P. and Panconesi, A., *Concentration of Measure for the Analysis of Randomized Algorithms*, Cambridge: Cambridge Univ. Press, 2009.

15. Ahlswede, R. and Winter, A., Strong Converse for Identification via Quantum Channels, *IEEE Trans. Inform. Theory*, 2002, vol. 48, no. 3, pp. 569–579.

16. Fekete, M., Über die Verteilung der Wurzeln bei gewissen algebraischen Gleichungen mit ganzzahligen Koeffizienten, *Math. Z.*, 1923, vol. 17, no. 1, pp. 228–249.

17. Ahlswede, R. and Csiszár, I., Common Randomness in Information Theory and Cryptography—Part I: Secret Sharing, *IEEE Trans. Inform. Theory*, 1993, vol. 39, no. 4, pp. 1121–1132.