The Secrecy Capacity of the Semi-deterministic Wiretap Channel with Three State Information

Mustafa El-Halabi
Department of Computer and Communications Engineering
American University of Science & Technology
Beirut, Lebanon
Email: mhalabi@aust.edu.lb

***Abstract*—Exploiting the channel state knowledge can play a fundamental role in improving security, hence a wiretap channel model with distinct channel state information is considered. In particular, it is assumed that the channel between the transmitter, the legitimate receiver and the eavesdropper is a function of three different states. One of the states is an unknown state, the second one is known to the legitimate receiver and the third state is non-causally known to the encoder. For this setting, a secrecy rate is shown to be achieved using a coding scheme based on structured binning in conjunction with a time-sharing argument. The secrecy capacity for this model is established for the specific case when the legitimate receiver's observation is a deterministic function of the the channel input and the states.**

***Index Terms*—Wiretap channel, state information, secrecy capacity, random binning, time-sharing.**

I. Introduction

In the race towards setting and defining the grounds for 5G wireless networks, information-theoretic security is steering lot of attention in recent years as a major player to safeguard data confidentiality. The 5G heterogeneous networks and the massive MIMO architecture call for a new security paradigm which is less dependent on secret key exchange; a problem with an order of complexity that increases with the ubiquity of the network [1].

Shannon in [2] introduced the channel state information to information theoretic models, wherein he considered the channel state to be a side information which is causally known to the transmitter. In [3], the side information was considered to be non-causally known to the transmitter and the capacity for the corresponding channel was obtained using a Gel'fand-Pinsker (GP) binning scheme.

In the context of information-theoretic security, there has been many attempts to investigate the role of state information on the secrecy performance of wiretap channels. A transmitter is attempting to send a confidential message to a designated receiver, through a channel governed by a certain state sequence, while a wiretapper is getting hold of the encoded message as a result of the openness nature of the communication channel. In [4], *Chen & Vinck* considered the problem of wiretap channel where the transition probability depends on a state sequence non-causally known to the encoder, and the wiretapper's signal is a degraded version of the legitimate receiver's signal. The achieved secrecy rate was based on a *double-binning* scheme; a synthesis of the *wiretap codes* used in [5], [6] for wiretap channels and the GP coding used in [3]. Interestingly, looking into the Gaussian model, it was shown that secrecy rate can actually be enhanced in the presence of known side information [4]. In [7],*Chia & El-Gamal* studied the problem of wiretap channel with causal side information, where an achievable secrecy rate was obtained using block Markov coding, Shannon strategy, and key generation from common state information.

In this paper, we propose a variant of the wiretap channel with state information problem. In our model, the signal received by the legitimate receiver depends on two state sequences S_1 and S_2, such that S_1 is non-causally known to the transmitter and S_2 is known to the receiver, while the signal received by the wiretapper depends on one unknown state sequence S_3. A model where the wiretap channel depends on two-sided state sequences was addressed in [8], where a rate-equivocation region was established using a time-sharing argument, whereas the assumption of the wiretapper's signal being affected by an unknown state sequence was treated in [9]. In this sense, our model can be viewed as a generalization of the previous two models and provides more insight on the impact of different kinds of side information on secure communication. In addition, we propose an upper bound on the secrecy capacity of the wiretap channel with three state information, and show that the secrecy rate achieved by our coding scheme matches the upper bound for the case when the legitimate receiver is a deterministic function of the channel input and the states.

The paper is organized as follows. Section II reviews the capacity of the channel with two-sided state information and the capacity for the corresponding deterministic channel. Section III introduces the problem and present the model. Section V presents the coding scheme and the achieved secrecy rate for the wiretap channel with three state information. Section IV derives an upper bound on the secrecy capacity. Section VI proves the secrecy capacity of the semi-deterministic model. Section VII summarizes the main results and the contribution of the paper.

II. Channel With Two-Sided State Information

In this section we review the building block for our model, which is the channel with two-sided state information introduced in [10], and derive the capacity for the corresponding

 ISBN: 978-1-61208-514-2

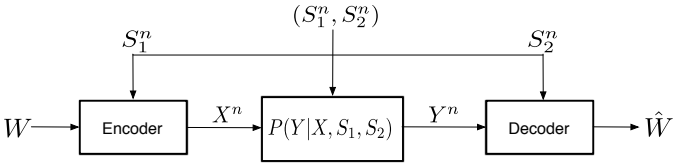

Figure 1. Channel with two-sided state information; S_1 non-causally known to the encoder, state S_2 known to the decoder.

deterministic channel. The conditional probability distribution depends on two correlated channel states S_1 and S_2 with joint probability distribution $p(s_1, s_2)$; the state S_1 is non-causally known to the receiver and the state S_2 is known to the receiver. See Figure. 1.

The capacity of this channel was obtained by *Cover et.al* in [10] and we restate the result in the following theorem.

Theorem 1. *The capacity C of the memoryless channel $p(y|x, s_1, s_2)$, with channel state S_1 non-causally known at the encoder as side information and channel state S_2 known to the decoder, is given by*

$$C = \max_{p(u,x|s_1)} \left[I(U;Y,S_2) - I(U;S_1) \right]. \tag{1}$$

where U is an auxiliary random variable verifying the following Markov chain: $U \to (X, S_1) \to (Y, S_2)$.

Proof: See proof in [10]. ■

We now characterize the capacity of the *deterministic* channel with two-sided states. In this case the channel output is a deterministic (bivariate) function of the channel input X and the channel states S_1 and S_2:

$$Y = f(X, S_1, S_2) \quad \textit{with probability 1} \tag{2}$$

Theorem 2. *The capacity of the deterministic channel with two-sided states is given by*

$$C = \max_{p(x|s_1)} H(Y|S_1, S_2) \tag{3}$$

Proof: Upper bound. An upper bound on the channel capacity for the model represented in Figure. 1, corresponds to the capacity of the channel where the states S_1 and S_2 are both fed to the encoder and the decoder. The capacity of this channel is given in [10, Corollary. 1] by $\max_{p(x|s_1,s_2)} I(X;Y|S_1,S_2)$. Hence, an upper bound on the capacity of the deterministic channel is

$$\begin{aligned} C &\leq \max_{p(x|s_1)} I(X;Y|S_1,S_2) \\ &= \max_{p(x|s_1)} [H(Y|S_1,S_2) - H(Y|X,S_1,S_2)] \\ &= \max_{p(x|s_1)} H(Y|S_1,S_2) \end{aligned} \tag{4}$$

where (4) is due to (2).

Lower bound. As the channel output is a deterministic function of (X, S_1, S_2), we can choose $U = (Y, S_2)$ and substitute back in (1). This gives the following lower bound on the capacity of the deterministic channel

$$\begin{aligned} C &\geq \max_{p(x|s_1)} [I(Y,S_2;Y,S_2) - I(Y,S_2;S_1)] \\ &= \max_{p(x|s_1)} H(Y,S_2|S_1) \\ &= \max_{p(x|s_1)} [H(S_2|S_1) + H(Y|S_1,S_2)] \\ &= \max_{p(x|s_1)} H(Y|S_1,S_2) \end{aligned} \tag{5}$$

where (5) is obtained by choosing S_1 and S_2 to be fully correlated. The matching between the upper bound and the lower bound proves the theorem. ■

III. Problem Formulation and System Model

Consider the discrete-time memoryless wiretap channel shown in Figure. 2. The transmitter wishes to send a message W from a message set $\mathcal{M}$ reliably to the legitimate receiver, while keeping it perfectly secured from an eavesdropper. The transition probability of the main channel and the wiretap channel depends on three state sequences S_1^n, S_2^n and S_3^n, with values in a finite set $(\mathcal{S}_1, \mathcal{S}_2, \mathcal{S}_3)$. The state sequence S_1^n is non-causally known at the encoder, while S_2^n is known to the legitimate receiver and S_3^n is unknown.

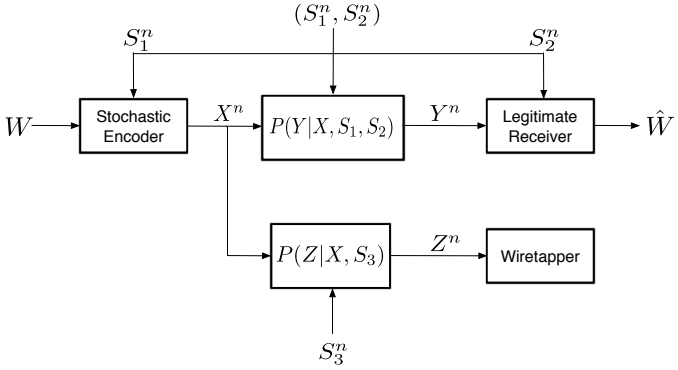

Figure 2. Wiretap channel with three channel state information; S_1 non-causally known to the encoder, state S_2 known to the legitimate receiver and state S_3 unknown to the wiretap channel

Using S_1^n, the encoder maps W to an $n-tuple$ channel input $X^n \in \mathcal{X}^n$ and sends it over the main channel and the wiretap channel. The main channel depends on the transition probability $p(y^n|x^n, s_1^n, s_2^n)$, with $Y^n \in \mathcal{Y}^n$ being the legitimate receiver observation. The wiretap channel depends on the transition probability $p(z^n|x^n, s_3^n)$, with $Z^n \in \mathcal{Z}^n$ being the wiretapper's observation. The channels are memoryless,i.e.,

$$\begin{aligned} p(y^n|x^n, s_1^n, s_2^n) &= \Pi_{i=1}^n p(y_i|x_i, s_{1i}, s_{2i}) \\ p(z^n|x^n, s_3^n) &= \Pi_{i=1}^n p(z_i|x_i, s_{3i}) \end{aligned}$$

We assume at different instances (S_1, S_2, S_3) to be independent identically distributed (i.i.d) random variables with joint probability distribution $p(s_1, s_2, s_3)$. The legitimate receiver aims at recovering $\hat{W}$; its estimate of the transmitted message, based on the received signal Y^n. The average decoding error

probability is defined as $P_e^{(n)} = \frac{1}{|\mathcal{M}|}\sum_{t=1}^{|\mathcal{M}|} Pr\{W \neq \hat{W}|W = t\}$. A secrecy rate R_s is achievable if there exists a sequence of length n code, such that the average error probability at the intended receiver and the leakage rate $\frac{1}{n}I(W;Z^n)$ between the message W and the the received signal Z^n, both approach zero as $n \to \infty$. The secrecy capacity is defined as the supremum of all achievable rates.

It is important to note that the considered formulation is a special instant of the general problem where all sorts of state information could affect the communication between the receiver and transmitter.

IV. Upper bound

We start by deriving an upper bound on the secrecy capacity for the model shown in Figure. 2. The upper bound will prove to be equal to the secrecy capacity for the semi-deterministic model in Section VI.

Proposition 1. *The secrecy capacity C_s of the discrete memoryless wiretap channel with three state information $p(y,z|x,s_1,s_2,s_3)$ with channel state S_1 non-causally known at the transmitter as side information, S_2 known to the legitimate receiver, and S_3 unknown to the wiretapper, can be bounded from above as*

$$C_s \leq \max_{p(x|s_1)} \min\left\{I(X;Y|S_1,S_2,S_3), I(X,S_1,S_3;Y,S_2|Z)\right\}. \tag{6}$$

Proof: We start by noting that $\max_{p(x|s_1)} I(X;Y|S_1,S_2,S_3)$ is an upper bound on the Shannon capacity of the legitimate receiver channel by creating a fictitious channel which gives the channel states S_1, S_2 and S_3 to the legitimate receiver as well as to the transmitter and uses the result from [10, Corollary. 1]. On the other hand, the term $\max_{p(x|s_1)} I(X,S_1,S_3;Y,S_2|Z)$ is an upper bound on the secrecy capacity of the wiretap channel, as it allows the channel state S_1, known to the transmitter, and the channel state S_3 to encode the transmitted message W, thus getting three encoded copies of the message instead of one (i.e.,*fully action-dependent state* [11]), and also by giving the signal received by the wiretapper Z to the legitimate receiver through a fictitious channel (i.e., Sato-like upper bound [12]). In order to move the maximization outside of the minimization, we need to recur to a single-letterization technique introduced in [13], which we apply as follows: By Fano's inequality, any achievable secrecy rate R_s must satisfy

$$\begin{aligned}
n(R_s-\epsilon_n) &\leq I(W;Y^n)\\
&\leq I(W;Y^n,S_1^n,S_2^n,S_3^n)\\
&\leq I(X^n;Y^n|S_1^n,S_2^n,S_3^n)\\
&= H(Y^n|S_1^n,S_2^n,S_3^n) - H(Y^n|X^n,S_1^n,S_2^n,S_3^n)\\
&= H(Y^n|S_1^n,S_2^n,S_3^n) - \sum_{i=1}^n H(Y_i|X_i,S_{1i},S_{2i},S_{3i})\\
&\leq \sum_{i=1}^n H(Y_i|S_{1i},S_{2i},,S_{3i}) - \sum_{i=1}^n H(Y_i|X_i,S_{1i},S_{2i},S_{3i})\\
&= n[H(Y_Q|S_{1Q},S_{2Q},S_{3Q},Q)\\
&\quad -H(Y_Q|X_Q,S_{1Q},S_{2Q},S_{3Q},Q)]\\
&\leq n[H(Y_Q|S_{1Q},S_{2Q},S_{3Q}) - H(Y_Q|X_Q,S_{1Q},S_{2Q},S_{3Q})]\\
&= n\cdot I(X_Q;Y_Q|S_{1Q},S_{2Q},S_{3Q})
\end{aligned}$$

where $\epsilon_n \to 0$ in the limit as $n \to \infty$, and Q is a standard time-sharing variable. Similarly, for any achievable secrecy rate R_s we have

$$\begin{aligned}
n(R_s-\epsilon_n) &\leq I(W;Y^n) - I(W;Z^n)\\
&\leq I(W;Y^n,Z^n) - I(W;Z^n)\\
&= I(W;Y^n|Z^n)\\
&\leq I(X^n,S_1^n,S_3^n;Y^n,S_2^n|Z^n)\\
&= H(Y^n,S_2^n|Z^n) - H(Y^n,S_2^n|X^n,S_1^n,S_3^n,Z^n)\\
&= H(Y^n,S_2^n|Z^n) - \sum_{i=1}^n H(Y_i,S_{2i}|X_i,S_{1i},S_{3i},Z_i)\\
&\leq \sum_{i=1}^n H(Y_i,S_{2i}|Z_i) - \sum_{i=1}^n H(Y_i,,S_{2i}|X_i,S_{1i},S_{3i},Z_i)\\
&= n[H(Y_Q,S_{2Q}|Z_Q,Q) - H(Y_Q,S_{2Q}|X_Q,S_{1Q},S_{3Q},Z_Q,Q)]\\
&\leq n[H(Y_Q,S_{2Q}|Z_Q) - H(Y_Q,S_{2Q}|X_Q,S_{1Q},S_{3Q},Z_Q)]\\
&= n\cdot I(X_Q,S_{1Q},S_{3Q};Y_Q,S_{2Q}|Z_Q).
\end{aligned}$$

Note that the channel states are memoryless, so S_{1Q}, S_{2Q} and S_{3Q} have the same distribution as $S_{j,i}$ for any $i = 1,\ldots,n$ and $j = 1,2,3$. The channel is also memoryless, so the conditional distribution of (Y_Q,Z_Q) given $(X_Q,S_{1Q},S_{2Q},S_{3Q})$ is given by the channel transition probability $p(y|x,s_1,s_2)$ and $p(z|x,s_3)$. Letting $X_Q = X$, $S_{1Q} = S_1$, $S_{2Q} = S_2$, $S_{3Q} = S_3$, $Y_Q = Y_1$, $Z_Q = Z$, and $n \to \infty$ completes the proof. ■

V. Achievable Secrecy Rate

The following theorem presents an achievable rate R_s for our model.

Theorem 3. *An achievable rate for the* wiretap channel with three states information *is*

$$R_s = \max_{p(u,x|s_1)} I(U;Y,S_2) - \max\{I(U;S_1,S_3), I(U;Z)\} \tag{7}$$

where U is an auxiliary random variable such that $U \to (X,S_1,S_2,S_3) \to (Y,Z)$.

Proof: We fix $p_U(u), p_{X|U,S_1}(x|u,s_1)$ and $\epsilon_1,\epsilon_2,\epsilon_3 > 0$. Let $R_s \doteq I(U;Y,S_2) - \max\{I(U;S_1,S_3), I(U;Z)\} - \epsilon_1 - \epsilon_3$ and $R \doteq \max\{I(U;S_1,S_3), I(U;Z)\} - I(U;Z) + \epsilon_3 + \epsilon_2$.

Codebook: Generate $2^{I(U;Y,S_2)-\epsilon_1}$ identically independent sequences u^n, each according to $p(\mathbf{u}) = \Pi_{i=1}^n p(u_i)$. We distribute the u^n sequences randomly into 2^{nR_s} bins, indexed by $m \in \{1,...,M = 2^{nR_s}\}$. Now each bins has

$2^{n[\max\{I(U;S_1,S_3),I(U;Z)\}+\epsilon_3]}$. Further we randomly distribute the sequences in each bin into 2^{nR} subbing, indexed by $j \in \{1, ..., J = 2^{nR}\}$. Thus each subbing has $2^{n[I(U;Z)-\epsilon_2]}$.

Encoding: To send message m, the transmitter looks into the m-th bin and select a $u^n(m)$ such that $u^n(m)$ and the interfering sequence s_1^n are jointly typical; $(u^n(m), s_1^n) \in T_\epsilon^n(p_{US_1})$. If there are more than one pair, then we randomly select one. We generate the channel input x^n according to the mapping $p_{x^n|u^n,s_1^n}(X|U, S_1)$.

Decoding: The decoder chooses m so that $(u^n(m), s_2^n, y^n) \in T_\epsilon^n(p_{US_2Y})$ if such m exists and is unique; otherwise, an error is declared.

Performance Analysis: We start by analyzing the error probability. There are three types of errors relating to encoding and decoding:

1) $\mathcal{E}_1$: error event corresponding to encoding; given the message bin m and the state sequence s_1^n, there is no jointly typical $(u^n(m), s_1^n)$ in bin m.
2) $\mathcal{E}_2$: error event corresponding to decoding; given the received sequence y^n and the state sequence s_2^n, there is no $u^n(m)$ such that $(u^n(m), y^n, s_2^n)$ is jointly typical.
3) $\mathcal{E}_3$: error event corresponding to decoding; given the received sequence y^n and the state sequence s_2^n, there is $u^n(m')$ such that $(u^n(m'), y^n, s_2^n)$ is jointly typical, where $m' \neq m$.

Without loss of generality, we assume that message $m = 1$ was sent. Since the probability that $(u^n(m), s_1^n)$ is jointly typical is larger than $(1-\epsilon)2^{-nI(U;S_1)}$, and that there are $2^{n[\max\{I(U;S_1,S_3),I(U;Z)\}+\epsilon_3]}$ sequences per bin, we have the following

$$\begin{aligned}
&Pr(E_1)\\
&\leq [1-(1-\epsilon)2^{-N[I(U;S_1)+3\epsilon]}]^{n[\max\{I(U;S_1,S_3),I(U;Z)\}+\epsilon_3]}\\
&\leq exp\{-(1-\epsilon)2^{-N[I(U;S_1)+3\epsilon]}\}^{n[\max\{I(U;S_1,S_3),I(U;Z)\}+\epsilon_3]}\\
&= exp\{-(1-\epsilon)2^{n[\max\{I(U;S_1,S_3),I(U;Z)\}-I(U;S_1)+\epsilon_3-3\epsilon]}\}\\
&\leq \delta_\epsilon^{(1)}(n)
\end{aligned}$$

Having the Markov chain: $U \to (X, S_1, S_2, S_3) \to (Y, Z)$, we then have $U \to (X, S_1) \to (Y, S_2)$. Hence, if $(u^n(m), x^n, s_1^n)$ is jointly typical, then $(u^n(m), x^n, s_1^n, s_2^n, y^n)$ is jointly typical. As a result,

$$Pr(E_2) \leq \delta_\epsilon^{(2)}(n)$$

Denoting by $E_3^{'}$ the event that we can find a $u^n(m')$ $(m' \neq m)$ which is jointly typical with y^n, then

$$\begin{aligned}
Pr(E_3) &\leq Pr\{E_3^{'}\}\\
&\leq \sum_{u^n \neq u^n(m)} 2^{-n[I(U;Y)]-3\epsilon}\\
&= \left(2^{n[I(U;Y,S_2)-\epsilon_1]}-1\right)2^{-n[I(U;Y)-3\epsilon]}\\
&\leq 2^{n[I(U;Y,S_2)-I(U:Y)-\epsilon_1+3\epsilon]}\\
&\leq \delta_\epsilon^{(3)}(n)
\end{aligned}$$

By the union bound on these three probabilities of error, the average probability of error $P_e^n \to 0$ as $n \to \infty$ This concludes the proof of reliability. Now we turn into verifying the secrecy performance of our code, through the calculation of the leakage rate between the transmitted message W and the received signal Z^n.

$$\begin{aligned}
&I(W; Z^n)\\
&= H(W) - H(W|Z^n)\\
&= H(W) - H(W, Z^n) + H(Z^n)\\
&= H(W) - H(W, J, Z^n) + H(J|W, Z^n) + H(Z^n)\\
&= H(W) - H(W, J, Z^n, U^n) + H(U^n|W, J, Z^n)\\
&\quad + H(J|W, Z^n) + H(Z^n)\\
&= H(W) - H(W, J|Z^n, U^n) - H(U^n, Z^n)\\
&\quad + H(U^n|W, J, Z^n) + H(J|W, Z^n) + H(Z^n)\\
&\overset{a}{\leq} \log|\mathcal{M}| - H(U^n|Z^n) + H(U^n|W, J, Z^n)\\
&\quad + H(J|W, Z^n)\\
&\overset{b}{\leq} \log|\mathcal{M}| - H(U^n|Z^n) + H(U^n|W, J, Z^n)\\
&\quad + \log|\mathcal{J}| + H(U^n|Y^n, S_2^n)\\
&= nR_s - H(U^n|Z^n) + H(U^n|W, J, Z^n)\\
&\quad + n[\max\{I(U; S_1, S_3); I(U; Z)\} - I(U; Z)]\\
&\quad + n(\epsilon_2 + \epsilon_3) + H(U^n|Y^n, S_2^n)\\
&\overset{c}{=} nR_s - n[I(U; Y, S_2) - I(U; Z)]\\
&\quad + H(U^n|W, J, Z^n) + n\max\{I(U; S_1, S_3); I(U; Z)\}\\
&\quad - nI(U; Z) + n(\epsilon_3 + \epsilon_2)\\
&= n(\epsilon_3 + \epsilon_2) + H(U^n|W, J, Z^n)\\
&\overset{d}{\leq} n(\epsilon_3 + \epsilon_2) + h(\bar{p}) + n\bar{p}[I(U; Z) - \epsilon_2] \qquad (8)
\end{aligned}$$

where,

(a) follows from $H(W) \leq \log|\mathcal{M}|$ and $H(W, J|Z^n, U^n) = 0$.
(b) follows from $H(J|W, Z^n) \leq H(J) \leq \log|\mathcal{J}|$ and $H(U^n|Y^n, S_2^n)) \geq 0$.
(c) follows from $I(U^n|Y^n, S_2^n) = nI(U|Y, S_2)$ and $I(U^n; Z^n) = nI(U; Z)$.
(d) follows from applying Fano's inequality to the wiretap channel whose input is U^n in the codebook consisting of the subbin j in bin m.

Applying the common random channel coding argument to (8), $\bar{p} \to 0$ as $n \to \infty$, hence

$$\lim_{n\to\infty} \frac{1}{n} I(W; Z^n) \to 0 \qquad (9)$$

This concludes the achievability proof for our coding scheme. ■

VI. Semi-deterministic wiretap channel with three state information

In this section we characterize the secrecy capacity of the *semi-deterministic* wiretap channel with three states, for the case where legitimate receiver output is a deterministic

(bivariate) function of the channel input X and the channel states S_1 and S_2:

$$Y = f(X, S_1, S_2) \quad \textit{with probability 1} \tag{10}$$

For the *semi-deterministic* model, the lower bound (7) and the upper bound (6) coincide, leading to a *precise* characterization of the secrecy capacity. The result is summarized in the following theorem.

Theorem 4. *The secrecy capacity of the* semi-deterministic wiretap channel with three states *is given by:*

$$C_s = \max_{p(x|s_1)} \min\{H(Y|S_1, S_2, S_3), H(Y, S_2|Z)\} \tag{11}$$

Proof: As the legitimate receiver output is a deterministic function of the channel input X and the channel states S_1 and S_2, and we have the following Markov chain $U \rightarrow (X, S_1, S_2, S_3) \rightarrow (Y, Z)$, we can let the auxiliary random variable $U = (Y, S_2)$.By substituting back in (7), we get the following

$$\begin{aligned} & I(U; Y, S_2) - I(U; S_1, S_3) \\ & \quad = H(Y, S_2) - H(Y, S_2|Y, S_2) - H(Y, S_2) \quad (12) \\ & + H(Y, S_2|S_1, S_3) \\ & \quad = H(Y, S_2|S_1, S_3) \\ & \quad = H(S_2|S_1, S_3) + H(Y|S_1, S_2, S_3) \\ & \quad = H(Y|S_1, S_2, S_3) \quad (13) \end{aligned}$$

where (13) is obtained by choosing the channel states to be fully correlated.Similarly,

$$I(U; Y, S_2) - I(U; Z) = H(Y, S_2|Z)$$

Thus

$$C_s \geq \max_{p(x|s_1)} \min\{H(Y|S_1, S_2, S_3), H(Y, S_2|Z)\}$$

The converse part of the theorem follows from the upper bound (6) and the fact that Y is a deterministic function of (X, S_1, S_2), so we have

$$\begin{aligned} I(X; Y|S_1, , S_2, S_3) &= H(Y|S_1, S_2, S_3) - \\ & \quad H(Y|X, S_1, S_2, S_3) \\ &= H(Y|S_1, S_2, S_3) \end{aligned}$$

and

$$\begin{aligned} I(X, S_1, S_3; Y, S_2|Z) &= H(Y, S_2|Z) - H(Y, S_2|X, S_1, S_2, Z) \\ &= H(Y, S_2|Z). \end{aligned}$$

This completes the proof of the theorem. ■

VII. Conclusion

For a number of channels, the conditional probability distribution is affected by certain channel state information. The state information could be available to the transmitter, or to the receiver or not available to either one of them. Also, the state information could be causally-known or non-causally known. This motivated the inspection of a special instant of the general problem, where the conditional probability distribution at the channel's output depends on three state information; one of unknown nature, another always available at the receiver as side information, and a third state non-causally known at the encoder. The paper suggests the use of a structured-binning scheme along with a time sharing argument to achieve a certain secrecy rate, which meets the upper bound and the achieves the secrecy capacity under the assumption that the channel is semi-deterministic. It is conjectured that this scheme can be used under any other assumptions on the nature and the number of state information affecting the conditional probability distribution of the channel. The author aims at tacking the same scenario under the assumption of constrained stochastic encoding, wherein the encoder is generating pseudo-randomness which is limited rather than being unlimited.

References

[1] N. Yang, L. Wang, G. Geraci, and M. El kashlan, "Safeguarding 5G wireless communication networks using physical layer security," *IEEE Communication Magazine*, vol. IT-53, no. 4, pp. 20–27, April 2015.

[2] C. E. Shannon, "Channels with side information at the transmitter," *J. Res. Devel.*, vol. 2, pp. 289-293, 1958.

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

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

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

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

[7] Y. K. Chia and A. El Gamal, "3-receiver broadcast channel with common and confidential messages," *Proc. IEEE Int. Symp. Inf. Theory*, Seoul, Korea, July 2009, pp. 1849–1853.

[8] W. Liu and B. Chen, "Wiretap channel with two-sided state information," in *Proc. 41st Asilomar Conference on Signals, Systems and Computers*, Pacific Grove, CA, pp. 893–897, Nov. 2007.

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

[10] T. .M. Cover and M. Chiang, "Duality between channel capacity and rate distortion with two-sided state information," *IEEE Trans. Inf. Theory*, vol. IT-48, no. 6, pp. 1629–1638, June 2002.

[11] T. Weissman, "Capacity of channels with action-dependent states," *IEEE Trans. Inf. Theory*, vol. 56, no. 11, pp. 5396–5411, Nov. 2010.

[12] H. Sato,"An outer bound to the capacity region of broadcast channels," *IEEE Trans. Inf. Theory*, vol. 24, pp. 374–77, May 1978.

[13] F. M. J. Willems, "An information theoretic approach to information embedding," in *Proc. 21st Symp. Inf. Theory Benelux*, Wassenaar, The Netherlands, May 2000, pp. 255–260.

 ISBN: 978-1-61208-514-2