Achievable Secrecy Rate Regions of State Dependent Causal Cognitive Interference Channel

Aghigh Mollaaghajanzade, Bahareh Akhbari, Arash Kakaee
Faculty of Electrical Engineering, K.N.Toosi University of Technology, Tehran, Iran.
Emails: a.aghajanzade@email.kntu.ac.ir, akhbari@kntu.ac.ir, a.kakaee@email.kntu.ac.ir
Corresponding author: Bahareh Akhbari

***Abstract*- In this paper, the secrecy problem in the state dependent causal cognitive interference channel is studied. The channel state is non-causally known at the cognitive encoder. The message of the cognitive encoder must be kept secret from the primary receiver. We use a coding scheme which is a combination of compress-and-forward strategy with Marton coding, Gel'fand-Pinsker coding and Wyner's wiretap coding at the cognitive encoder. We use rate splitting for messages at both transmitters. Furthermore, the cognitive user compresses its channel observation using Wyner-Ziv coding and splits the index of its compressed signal. By using this scheme we derive an achievable secrecy rate region for this channel and extend the results to the Gaussian case and provide some numerical results.**

***Index Terms*-** Causal cognitive interference channel, State dependent channel, secrecy, Achievable secrecy rate region, rate-equivocation.

I. INTRODUCTION

Wyner introduced the wiretap channel [1], which is the basic information-theoretic model to achieve secure communication in the presence of an eavesdropper. This single-user model was extended to the broadcast channel with confidential messages by Csisz´ar and Körner [2], and its secrecy capacity region was computed. More recently, the secrecy problem in multi-user channels has attracted huge attention. We refer the interested readers to [3]-[7].

One of the most important models of multi-user channels is Interference Channel (IFC) [8] which is the simplest model for demonstrating interference in wireless networks. In IFC, the intended signal for one receiver causes interference at other receivers. Later, the IFC was extended to Cognitive Interference Channel (C-IFC). Cognitive interference channel was first introduced in [9], which consists of two transmitters and two receivers, where the cognitive user (secondary user) can attain the message of primary user in a non-causal or causal style. In [9], an achievable rate region for the non-causal C-IFC was derived using Gel'fand-Pinsker (GP) binning [10] and rate splitting [11]. There are many achievable rate regions and capacity results for the non-causal C-IFC [12]-[15].

Manuscript received 27-Nov.-2017 and revised 17-April-2018, *P- ISSN: 2322-4088*
Accepted on 22- June-2018 *E- ISSN: 2322-3936*

A more practical and appropriate model than the non-causal C-IFC is Causal C-IFC (CC-IFC), because the assumption that cognitive user has knowledge about the message of primary user is not reasonable in all practical models. In the causal C-IFC, the cognitive user can causally learn the primary user's data and exploit it to help the primary user, while in the non-causal C-IFC it is assumed that the cognitive user knows the entire message by the aid of a genie. Actually, in the causal C-IFC the cognitive user acts as a transmitter and receiver. The cognitive user can listen to the channel and learn the primary user's data, and based on the received information it transmits the appropriate signals. Hence, it can be considered as a relay node too. Therefore, two main different strategies according to strength of the cognitive link (the link between the primary user and the secondary one) can be used: Decode-and-Forward (DF) and Compress-and-Forward (CF) [16]. According to [16], none of these strategies is generally the best, but in some cases one can outperform the other one. In CF strategy [16.Theorem 6], the cognitive user can compress its channel observation using Wyner-Ziv coding rather than decoding the primary user's message that happened in DF strategy. In [17], an inner and outer bounds were derived for CC-IFC by using CF strategy and Marton coding [18] at the cognitive user, and the results were compared to DF-based achievable rate regions derived in [19]. We refer interested readers to [19]-[22] and references therein to see the works on CC-IFC.

Considering Channel State Information (CSI) is another practical problem in communication networks, which has been modeled theoretically by state dependent channels [10], [23]. Usually it is assumed that the channel state can be available causally [23] or non-causally [10] at the transmitter. The term *non-causal* CSI at the transmitter refers to the scenario for which the entire channel state of each block with length n is available at the beginning of that block. Therefore, the entire channel state S^n is available at the transmitter at each time instant i, while in the *causal* CSI case the transmitter at every time instant i knows only the past and the present CSI. For the IFC and C-IFC with non-causal CSI, some achievable rate regions and capacity regions have been established in [24]-[27].

In this paper, we study the secrecy problem in the state dependent CC-IFC which the CSI is assumed to be known non-causally at the cognitive transmitter (see Fig.1). The secrecy problem in this model has not been investigated before. Considering secrecy in this model is the main challenge of our work. This channel that we refer to it as the state dependent causal cognitive interference channel with a confidential message can be regarded as a new model in wiretap channels that can be a proper fundamental model for demonstrating interference, cognition, channel uncertainty and secrecy in wireless networks. In this channel, we assume that the cognitive node overhears the channel and has access to the non-causal CSI to help the primary user, while it wishes to keep its message confidential with respect to the primary receiver. It also should be noted that this assumption that the CSI is known only at one node (i.e, asymmetric case) is more difficult than the assumption that all nodes have access to the CSI.

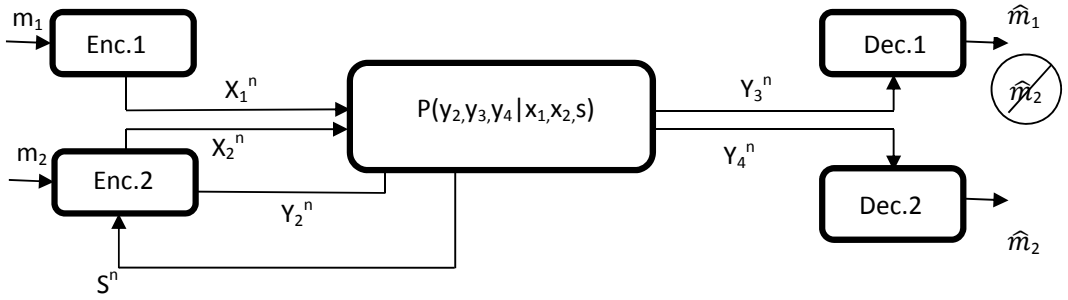

Fig. 1. The state dependent causal cognitive interference channel with a confidential message.

We aim to derive an achievable secrecy rate region for this channel. To derive a secrecy rate region for this model both reliability and *security constraints* should be satisfied. Hence, we use a coding scheme which combines Wyner's wiretap coding, CF strategy with Marton coding and GP coding at the cognitive encoder. Each user splits its message to common and private parts for interference cancellation at its non-intended receiver. The primary user uses superposition coding to create its codewords. The cognitive user compresses its channel observation using Wyner-Ziv coding and splits index of its compressed signal to common and private parts, but the private part is intended for the primary user's receiver to cooperate with the primary user. The cognitive user has common information for both receivers, and confidential message to cognitive user's receiver, which should be kept secret from the primary receiver. Hence, we use the Wyner's wiretap coding at the cognitive transmitter too. We use sliding-window decoding and simultaneous joint decoding [28] at the receivers. Based on this scheme, we obtain an achievable secrecy rate region for this channel and extend our achievable secrecy rate region to the Gaussian case, to provide some numerical examples to study the effects of state power, links' gain and secrecy. It should be noted again that considering causal cognition in C-IFC, and investigating state dependent channels with secrecy constraints are important problems in communication networks, which we intend to propose one model to study these problems simultaneously. Hence, this model includes previous models without secrecy, state and cognition.

The rest of this paper is organized as follows. Section II introduces the channel model and notations. In Section III, we present the main results. In Section IV, Gaussian case is investigated and some numerical results are provided. Finally, Section V concludes the paper.

II. CHANNEL MODEL AND NOTATIONS

In this paper, we use upper case letters (e.g.X) to denote Random Variables (RV) and lower case letters (e.g.x) to show their realizations. The probability mass function of a RV X with alphabet set $\mathcal{X}$, is denoted by $p_X(x)$ where subscript X is omitted. $A_\epsilon^n(X,Y)$ specifies the set of ϵ-strongly, jointly typical sequences of length n, abbreviated by A_ϵ^n [29]. The notation X^j is used instead of X_1^j. $\mathcal{N}(0,\sigma^2)$ denotes the normal distribution with zero mean and variance σ^2. Consider the state dependent CC-IFC in Fig. 1, which is denoted by ($\mathcal{X}_1 \times \mathcal{X}_2 \times$ S, $p(y_2,y_3,y_4|x_1,x_2,s)$, $\mathcal{Y}_2 \times \mathcal{Y}_3 \times \mathcal{Y}_4$), where $X_1 \in \mathcal{X}_1$ and $X_2 \in \mathcal{X}_2$ are inputs of Transmitter 1 and Transmitter 2 , respectively, $Y_2 \in \mathcal{Y}_2$ is the secondary user's output, $Y_3 \in \mathcal{Y}_3$ and $Y_4 \in \mathcal{Y}_4$ are channel outputs at the Receiver 1 and Receiver 2, respectively, and $p(y_2y_3y_4|x_1x_2s)$ is the channel transition probability distribution.

We also assume that channel states $S^n$are i.i.d and drawn from a given probability distribution $p(s)$. The Enc.j wishes to transmit the message m_j uniformly distributed on the set $M_j = \{1,\dots,2^{nR_j}\}$ where j=1,2. The conditional distribution of the channel output n-sequences Y_2^n, Y_3^n, Y_4^n given the inputs and the state, n-sequences X_1^n, X_2^n, S^n take the product form

$$P_{Y_2^nY_3^nY_4^n|X_1^nX_2^nS^n}(y_2^ny_3^ny_4^n|x_1^nx_2^ns^n) = \prod_{i=1}^n P_{Y_2Y_3Y_4|X_1X_2S}(y_2y_3y_4|x_1x_2s) \tag{1}$$

The encoders are defined by the mappings

$$\begin{aligned} \varphi_1 &: M_1 \to X_1 \\ \varphi_{2,i} &: m_2 \times y_2^{i-1} \times s^n \to x_{2,i} \quad : \ 1 \le i \le n \end{aligned} \tag{2}$$

The decoders are defined by the mappings

$$\begin{aligned} \psi_1 &: y_3^n \to M_1 \\ \psi_2 &: y_4^n \to M_2 \end{aligned} \tag{3}$$

We denote the error probability $P_e^{(n)} = \max(P_{e,1}^{(n)}, P_{e,2}^{(n)})$, where for $j \in \{1,2\}$

$$P_{e,j}^{(n)} = \frac{1}{2^{n(R_1+R_2)}} \sum_{m_1m_2} P(\psi_j(Y_{j+2}^n) \neq m_j|(m_1,m_2)sent) \tag{4}$$

Definition 1: The secrecy level of the cognitive encoder's message at the primary receiver is measured by normalized equivocation

$$R_{e2}^{(n)} = \frac{1}{n} H(M_2|Y_3) \tag{5}$$

Definition 2: A rate-equivocation triple (R_1, R_2, R_{e2}) is achievable if for any $\epsilon_n > 0$ there exists a $(2^{nR_1}, 2^{nR_2}, n)$ code such that $P_e^{(n)} < \epsilon$ as $\to \infty$ and

$$0 \le R_{e2} \le \lim_{n\to\infty} inf R_{e2}^{(n)} \tag{6}$$

The secrecy capacity region is the closure of the set of all achievable secrecy rate-triples.

III. MAIN RESULTS

As we explained before, in our scenario the cognitive encoder has causal access to the message of the primary sender. In addition, it is assumed that the state of the channel is known non-causally at the cognitive transmitter. The following result gives the achievable secrecy rate region for the finite alphabet causal cognitive interference channel with non-causal CSI at the cognitive encoder. Our coding scheme utilizes the ideas of rate splitting, Marton coding, GP coding, Wyner's wiretap coding at the cognitive encoder and Wyner-Ziv compression.

Theorem 1: The closure of the convex hull of the set of secrecy rate-triples (R_1, R_2, R_{e2}) satisfying

$$R_1 \le I\big(X_1; \hat{Y}_2 Y_3 | U_1 U_{20} U_{21}\big) + \min\{I\big(U_1; \hat{Y}_2 Y_3 | U_{20} U_{21}\big), I(U_1 U_{22}; Y_4 | U_{20}) - I(U_{22}; S | U_{20})\} \tag{7}$$

$$R_2 \le I(U_{22}; Y_4 | U_1 U_{20}) + I(U_{21}; Y_3 | U_{20}) + I\big(\hat{Y}_2; Y_3 | U_{20} U_{21}\big) - I\big(\hat{Y}_2; Y_2 | U_{20} U_{21}\big) + \min\{I(U_{20}; Y_3), I(U_{20}; Y_4 | U_1)\} - I(U_{22} U_{20}; S | U_{20}) - I(U_{21}; U_{22} S | U_{20}) \tag{8}$$

$$R_1 + R_2 \le I\big(X_1; \hat{Y}_2 Y_3 | U_1 U_{20} U_{21}\big) + I(U_1 U_{22}; Y_4 | U_{20}) + I(U_{21}; Y_3 | U_{20}) + I\big(\hat{Y}_2; Y_3 | U_{20} U_{21}\big) - I\big(\hat{Y}_2; Y_2 | U_{20} U_{21}\big) - \mathrm{I}(U_{21} U_{20}; S) - I(U_{22}; U_{21} S | U_{20}) + \min\{I(U_{20}; Y_3), I(U_{20}; Y_4)\} \tag{9}$$

$$subject\ to: \begin{cases} I\big(\hat{Y}_2; Y_2 S | U_{20} U_{21} Y_3\big) \le I(U_{20} U_{21}; Y_3) - I(U_{20} U_{21}; S) \\ I(U_{22}; U_{21} | U_{20} S) \le I(U_{21}; Y_3 | U_{20}) + I(U_{22}; Y_4 | U_{20} U_1) \end{cases} \tag{10}$$

$$\boldsymbol{R_{e2} \le I\big(U_{22}; Y_4 \hat{Y}_2 U_{20} U_{21}\big) - I(U_{22} S; X_1 Y_3 U_{20} U_{21})} \tag{11}$$

for input distribution factors as

$$P(u_1)P(x_1|u_1)P(u_{20}, s)P(u_{21}, u_{22}|u_{20}, s)P(x_2|u_{20}, u_{21}, u_{22}, s)P(y_2, y_3, y_4|x_1, x_2, s)P(\hat{y}_2|y_2, u_{20}, u_{21}, s) \tag{12}$$

is achievable for the finite alphabet causal cognitive interference channel with CSI non-causally available at the cognitive encoder and a confidential message.

Remark 1: If we omit receiver 2, i.e. $Y_4 = \emptyset$, and the cognitive user does not have any own message to transmit and to keep confidential, i.e. $R_2 = R_{e2} = 0$ the model reduces to the relay channel. By setting $U_1 = U_{21} = U_{22} = \emptyset, L_{20} = L_{22} = 0, U_{20} = X_2$ the rate region reduces to the CF rate for the state dependent relay channel [30].

Remark 2: If we assume that the cognitive user has causal CSI, the expression for the achievable secrecy rate region of this case can be obtained from the expression of that for non-causal CSI scenario by choosing auxiliary RVs U_{20}, U_{21}, U_{22} independent of the channel state S. However, the coding scheme for the causal CSI case is different with that for the non-causal CSI, but the expression of the region can be obtained by this way that has also been mentioned in [34].

Outline of Proof: We use a block Markov coding scheme with B blocks of transmission, each of n symbols, which uses CF strategy, Marton coding, GP coding and Wyner's wiretap coding at the cognitive user. The message of the primary user (Enc.1) is split into two parts: $m_1 = (m_{10}, m_{11})$ and $R_1 = R_{10} + R_{11}$. The common part (m_{10}) is conveyed through U_1 and can be decoded at both receivers to cancel the interference at Dec.2, the private part (m_{11}) is conveyed through X_1 which is superimposed on U_1 and can be decoded only at Dec.1. Cognitive user (Enc.2) splits its message into two parts: $m_2 = (m_{20}, m_{22})$ and $R_2 = R_{20} + R_{22}$, again for interference cancellation at Dec.1. At the end of the previous block, to cooperate with Enc.1, the cognitive user compresses its channel observation to $\hat{Y}_2$ by using Wyner-Ziv coding. The index of $\hat{Y}_2$ is split into common and private parts: z_p, z_c, respectively. The purpose of this splitting is to cancel interference at Dec.2. The private part can be decoded only at Dec.1. Therefore, Enc.2 sends common messages (m_{20}, z_c) to both receivers, a private message (z_p) to Dec.1 and a confidential message (m_{22}) to Dec.2, which should be kept secret from primary receiver. Based on Marton coding, GP coding and Wyner's wiretap coding, Enc.2 creates $U_{20}, U_{21}$and U_{22} to convey $(m_{20}, z_c), z_p$and m_{22}, respectively, which are independent of the codewords of Enc.1.

Dec.1 uses a dual-step process for decoding at the end of each block. In the first step, It jointly decodes $U_{20}, U_{21}$and $\hat{Y}_2$ by sliding-window technique. In the second step, Dec.1 finds $m_1 = (m_{10}, m_{11})$ by jointly decoding U_1 and X_1 using $U_{20}, U_{21}$and $\hat{Y}_2$. Dec.2 jointly decodes $U_{20}, U_{22}$and U_1 in a single step.

Generation of Codebook: Repeat the following procedure two times and independently generate codebooks 1 and 2, respectively, for encoding at the blocks with odd and even indices. Probabilities of these events can be computed in the analysis of the probability of error for sliding-window decoding technique.

1. Generate $2^{nR_{10}}$ independent and identically distributed (i.i.d) u_1^n sequences, each drawn according to $\prod_{i=1}^{n} p(u_{1,i})$. Index them as $u_1^n(m_{10})$, where $m_{10} \in [1, 2^{nR_{10}}]$.
2. For each $u_1^n(m_{10})$, generate $2^{nR_{11}}$ i.i.d x_1^n sequences, each drawn according to $\prod_{i=1}^{n} p(x_{1,i}|u_{1,i})$. Index them as $x_1^n(m_{11}, m_{10})$, where $m_{11} \in [1, 2^{nR_{11}}]$.
3. Generate $2^{nR_{10}}$ independent and identically distributed (i.i.d) u_1^n sequences, each drawn according to $\prod_{i=1}^{n} p(u_{1,i})$. Index them as $u_1^n(m_{10})$, where $m_{10} \in [1, 2^{nR_{10}}]$.

4. Generate $2^{nR_{10}}$ independent and identically distributed (i.i.d) u_1^n sequences, each drawn according to $\prod_{i=1}^{n} p(u_{1,i})$. Index them as $u_1^n(m_{10})$, where $m_{10} \in [1, 2^{nR_{10}}]$.
5. For each $u_1^n(m_{10})$, generate $2^{nR_{11}}$ i.i.d x_1^n sequences, each drawn according to $\prod_{i=1}^{n} p(x_{1,i}|u_{1,i})$. Index them as $x_1^n(m_{11}, m_{10})$, where $m_{11} \in [1, 2^{nR_{11}}]$.
6. Generate $2^{n(R_{20}+\hat{R}_c+T_0)}$ i.i.d u_{20}^n sequences, each drawn according to $\prod_{i=1}^{n} p(u_{20,i})$. Index them as $u_{20}^n(m_{20}, z_c, l_0)$, where $m_{20} \in [1, 2^{nR_{20}}]$, $z_c \in [1, 2^{n\hat{R}_c}]$ and $l_0 \in [1, 2^{nT_0}]$.
7. For each $u_{20}^n(m_{20}, z_c, l_0)$, generate $2^{n(\hat{R}_p+T_1)}$ i.i.d u_{21}^n sequences, each drawn according to $\prod_{i=1}^{n} p(u_{21,i}|u_{20,i})$. Index them as $u_{21}^n([z_p, l_1]|m_{20}, z_c, l_0)$, where $z_p \in [1, 2^{n\hat{R}_p}]$, and $l_1 \in [1, 2^{nT_1}]$.
8. For each $u_{20}^n(m_{20}, z_c, l_0)$, generate $2^{n(R_{22}+T_2)}$ i.i.d u_{22}^n sequences, each drawn according to $\prod_{i=1}^{n} p(u_{22,i}|u_{20,i})$. Index them as $u_{22}^n([m_{22}, l_2]|m_{20}, z_c, l_0)$, where $m_{22} \in [1, 2^{nR_{22}}]$, and $l_2 \in [1, 2^{nT_2}]$.
9. For each $(u_{20}^n(m_{20}, z_c, l_0), u_{21}^n([z_p, l_1]|m_{20}, z_c, l_0))$ generate $2^{n(\hat{R}_p+\hat{R}_c)}$ i.i.d $\hat{y}_2^n$sequences, each with probability$\prod_{i=1}^{n} p(\hat{y}_{2,i}^n|u_{20,i}, u_{21,i})$. Index them as $\hat{y}_2^n(z_p', z_c', m_{20}, z_c, l_0, z_p, l_1)$, where $z_p' \in [1, 2^{n\hat{R}_p}]$ and $z_c' \in [1, 2^{n\hat{R}_c}]$. The indices z_c' and z_p' show z_c and z_p in the next block, respectively.

Encoding (at the beginning of block b): We suppose that the channel state in each block is non-causally known to the cognitive transmitter.

Primary User: In order to transmit message $m_{1b} = (m_{10b}, m_{11b})$, Enc.1 sends $x_1^n(m_{11}, m_{10})$.

Cognitive User: The channel state in each block is non-causally known to the cognitive transmitter. Enc.2 at the beginning of block b, knows z_{pb}, z_{cb} from decoding at the end of the block $b-1$ by the cognitive user. Knowing z_{cb}, m_{20b} and channel state (S^n), it searches for $l_0 \in [1, 2^{nT_0}]$ such that $(u_{20}^n(m_{20}, z_c, l_0), s^n) \in A_\epsilon^n$. If there is more than one l_0, Enc.2 picks the smallest. If there is none, it declares an error. Based on the GP coding, for sufficiently large n there exists such an index l_0 , if

$$T_0 \geq I(U_{20}; S) \tag{13}$$

The encoder next finds $l_{1,b} \in [1, 2^{nT_1}]$, $l_{2,b} \in [1, 2^{nT_2}]$, such that

$$(u_{20}^n(m_{20}, z_c, l_0), s^n, u_{21}^n([z_p, l_1]|m_{20}, z_c, l_0), u_{22}^n([m_{22}, l_2]|m_{20}, z_c, l_0)) \in A_\epsilon^n$$

If there is more than one such index quadruple, Enc.2 picks the smallest. If there are no such code words, it declares an error. Using mutual covering lemma [28], it can be shown that there exist such indices $l_{1,b}$, $l_{2,b}$ with enough high probability, if n is large enough and

$$T_1 \geq I(U_{21}; S|U_{20}) \tag{14}$$

$$T_2 \geq I(U_{22}; S|U_{20}) \tag{15}$$

$$T_1 + T_2 \geq I(U_{21}; S|U_{20}) + I(U_{22}; S|U_{20}) + I(U_{22}; U_{21}|U_{20}S) \quad (16)$$

Then, cognitive user sends x_2^n generated according to $\prod_{i=1}^{n} P(x_{2,i}|u_{22,i}, u_{21,i}, u_{20,i}, S_i)$.

We assume that in the first block, the index of the compressed signal is: $(z_{p,b}, z_{c,b}) = (z_{p,1}, z_{c,1}) = (1,1)$ and in the last block, a previously known message for the primary user $m_{1b} = (m_{10b}, m_{11b}) = (m_{10B}, m_{11B}) = (1,1)$ is transmitted. Note that, as $B \to \infty$, rate $R_1 \times \frac{B-1}{B} \to R_1$.

Decoding (at the end of block b):

Cognitive User: At the end of block b, Enc.2 knows $u_{20}^n(m_{20,b}, z_{c,b}, l_{0,b})$, $u_{21}^n([z_{p,b}, l_{1,b}]|m_{20,b}, z_{c,b}, l_{0,b})$ which have been sent at the beginning of block b. By using Wyner-Ziv method for compressing $y_2(b)$, Enc.2 finds a unique index pair $(z_{p,b+1}, z_{c,b+1})$ such that

$$(y_2^n(b), \hat{y}_2^n(z_{p,b+1}, z_{c,b+1}, z_{p,b}, z_{c,b}, l_{0,b}, l_{1,b}, m_{20,b}), u_{20}^n(m_{20,b}, z_{c,b}, l_{0,b}), u_{21}^n([z_{p,b}, l_{1,b}]|m_{20,b}, z_{c,b}, l_{0,b}), s^n) \in A_\epsilon^n$$

If more than one such index pair are found, Enc.2 picks the smallest. If no one can be found, it declares error. Based on covering lemma, for large enough n there exists such an index pair $(z_{p,b+1}, z_{c,b+1})$ with high probability, if

$$\hat{R}_c + \hat{R}_p \geq I(\hat{Y}_2; Y_2|U_{21}U_{20}) \quad (17)$$

Reciever1: At the end of block b, $b = 2,3, \dots, B$, Dec.1 uses both $y_3^n(b-1)$ and $y_3^n(b)$ in order to perform two-step decoding procedure with sliding-window technique in the first step and joint decoding in the second one.

First step: Dec.1 searches for a unique tuple $(\hat{z}_{p,b}, \hat{z}_{c,b}, \hat{m}_{20,b}, \hat{l}_{0,b}, \hat{l}_{1,b})$ such that

$$(y_3^n(b), u_{21}^n([\hat{z}_{p,b}, \hat{l}_{1,b}]|\hat{z}_{c,b}, \hat{l}_{0,b}, \hat{m}_{20,b}), u_{20}^n(\hat{m}_{20,b}, \hat{z}_{c,b}, \hat{l}_{0,b})) \in A_\epsilon^n$$

and

$$(y_3^n(b-1), \hat{y}_2^n(\hat{z}_{p,b}, \hat{z}_{c,b}, z_{p,b-1}, z_{c,b-1}, m_{20,b-1}, l_{0,b-1}, l_{1,b-1}), u_{21}^n([z_{p,b-1}, l_{1,b-1}]|z_{c,b-1}, l_{0,b-1}, m_{20,b-1}), u_{20}^n(m_{20,b-1}, z_{c,b-1}, l_{0,b-1})) \in A_\epsilon^n$$

where $z_{p,b-1}, z_{c,b-1}, m_{20,b-1}$ were decoded in the decoding at the end of block $b-1$. Because of independence of codebooks in two adjacent blocks and packing lemma [28], for large enough n, $(\hat{z}_{p,b}, \hat{z}_{c,b}, \hat{m}_{20,b}) = (z_{p,b}, z_{c,b}, m_{20,b})$ with small probability of error, if

$$T_0 + T_1 + R_{20} + \hat{R}_c + \hat{R}_p \leq I(U_{20}U_{21}; Y_3) + I(\hat{Y}_2; Y_3|U_{21}U_{20}) = I(U_{21}U_{20}\hat{Y}_2; Y_3) \quad (18)$$

$$T_1 + \hat{R}_p \leq I(U_{21}; Y_3|U_{20}) + I(\hat{Y}_2; Y_3|U_{21}U_{20}) = I(U_{21}\hat{Y}_2; Y_3|U_{20}) \quad (19)$$

$$\boldsymbol{T_1 \leq I(U_{21}; Y_3|U_{20})} \quad (20)$$

$$\boldsymbol{T_0 + T_1 + R_{20} \leq I(U_{20}U_{21}; Y_3)} \quad (21)$$

Second step: Recovering $\hat{y}_2^n\left(z_{p,b}, z_{c,b}, z_{p,b-1}, z_{c,b-1}, m_{20,b-1}, l_{0,b-1}, l_{1,b-1}\right)$ in the previous step, i.e., the compressed version of $y_2^n(b-1)$, Dec.1 tries to decode $m_{1,b-1}$ by using $y_3^n(b-1)$. It implies that the pair $(\hat{m}_{10,b-1}, \hat{m}_{11,b-1})$ was sent in the block $b-1$ if there are unique indices $(\hat{m}_{10,b-1}, \hat{m}_{11,b-1})$ such that

$$\left(y_3^n(b-1), \hat{y}_2^n\left(z_{p,b}, z_{c,b}, z_{p,b-1}, z_{c,b-1}, m_{20,b-1}, l_{0,b-1}, l_{1,b-1}\right), u_1^n\left(\hat{m}_{10,b-1}\right), x_1^n\left(\hat{m}_{11,b}, \hat{m}_{10,b}\right), u_{21}^n\left(\left[z_{p,b-1}, l_{1,b-1}\right]\middle| z_{c,b-1}, l_{0,b-1}, m_{20,b-1}\right), u_{20}^n\left(m_{20,b-1}, z_{c,b-1}, l_{0,b-1}\right)\right) \in A_\epsilon^n$$

This step can be done with small probability of error, i.e., $(\hat{m}_{10,b-1}, \hat{m}_{11,b-1}) = (m_{10,b-1}, m_{11,b-1})$, if n is large enough and

$$\boldsymbol{R_{10} + R_{11} \le I(U_1 X_1; \hat{Y}_2 Y_3 | U_{20} U_{21})} \quad (22)$$

$$\boldsymbol{R_{11} \le I(X_1; \hat{Y}_2 Y_3 | U_1 U_{20} U_{21})} \quad (23)$$

Reciever2: At the end of block b, $b = 1,2,3, \dots, B$, Dec.2 finds a unique pair $(\hat{m}_{20,b-1}, \hat{m}_{22,b-1})$ and some tuple $(\hat{m}_{10,b}, \hat{z}_{c,b}, \hat{l}_{2,b}, \hat{l}_{0,b})$ such that

$$\left(y_4^n(b), u_{22}^n\left(\left[\hat{m}_{22,b}, \hat{l}_{2,b}\right]\middle| z_{c,b}, l_{0,b}, m_{20,b}\right), u_{20}^n\left(\hat{m}_{20,b}, \hat{z}_{c,b}, \hat{l}_{0,b}\right), u_1^n\left(\hat{m}_{10,b-1}\right)\right) \in A_\epsilon^n$$

The probability of error at Dec.2 can be small, i.e., $(\hat{m}_{20,b-1}, \hat{m}_{22,b-1}) = (m_{20,b-1}, m_{22,b-1})$, if n is large enough and

$$T_0 + T_2 + R_{20} + \hat{R}_c + R_{22} \le I(U_{20} U_{22}; Y_4 | U_1) \quad (24)$$

$$T_0 + T_2 + R_{20} + \hat{R}_c + R_{22} + R_{10} \le I(U_1 U_{20} U_{22}; Y_4) \quad (25)$$

$$\boldsymbol{T_2 + R_{22} \le I(U_{22}; Y_4 | U_1 U_{20})} \quad (26)$$

$$\boldsymbol{T_2 + R_{22} + R_{10} \le I(U_1 U_{22}; Y_4 | U_{20})} \quad (27)$$

We apply Fourier-Motzkin procedure [24] to (13)-(27) with the constraints $R_{jj} = R_j - R_{j0}, 0 \le R_{j0} \le R_j$ for $j = 1,2$, to eliminate $T_0, T_1, T_2, R_{10}, R_{20}, \hat{R}_p, \hat{R}_c$. ■

For the proof of achievability of the equivocation-rate region, see Appendix A.

IV. THE GAUSSIAN EXAMPLE

In this section, we consider the Gaussian CC-IFC with non-causal CSI at the cognitive transmitter and confidential message, to denote our results more clearly. The channel model is shown in Fig.2, and can be described at time $i = 1,2, \dots, n$ as follows:

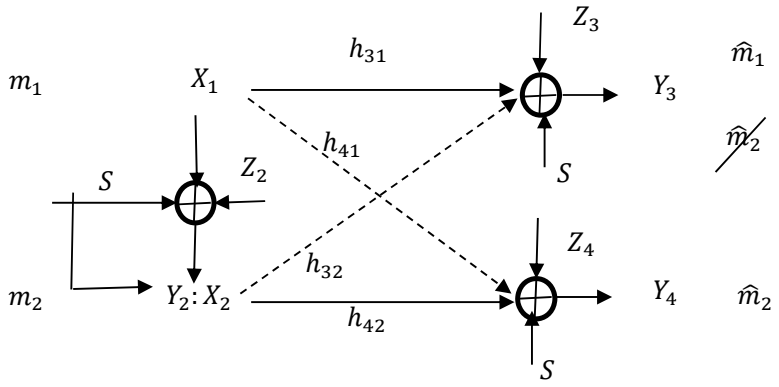

Fig. 2. Gaussian state dependent CC-IFC with non-causal CSI known at the cognitive encoder and a confidential message.

$$Y_{2,i} = h_{21}X_{1,i} + Z_{2,i} + S_i$$
$$Y_{3,i} = h_{31}X_{1,i} + h_{32}X_{2,i} + Z_{3,i} + S_i$$
$$Y_{4,i} = h_{41}X_{1,i} + h_{42}X_{2,i} + Z_{4,i} + S_i \quad (28)$$

where $h_{21}, h_{31}, h_{41}, h_{32}$ and h_{42} are known as link gains. $X_{1,i}$ and $X_{2,i}$ are input signals with average power constraints

$$\frac{1}{n}\sum_{i=1}^{n}(x_{ji})^2 \leq P_j \quad (29)$$

for $j \in \{1,2\}$.$Z_{2,i}$, $Z_{3,i}$, $Z_{4,i}$ and S_i are i.i.d and independent zero mean Gaussian noise components with powers N_2, N_3, N_4 and K respectively.

The secrecy rate region $\mathcal{R}$ in Theorem 1 can be extended to the discrete-time Gaussian memoryless case with continuous alphabets [29]. Hence, we evaluate the (7)-(12) with an appropriate choice of input distribution to obtain the Gaussian counterpart of $\mathcal{R}$, namely $\mathcal{R}^*$. We constrain all the inputs to be Gaussian. For certain $\{0 \leq \beta_r \leq 1, r \in \{1,2,3,4\}\}$,$\{0 \leq \alpha_q \leq 1, q \in \{1,2,3,4,5\}\}$, where $\beta_2 + \beta_3 + \beta_4 = 1$ consider the following mapping for the generated codebook in Theorem 1 with respect to the p.m.f (1), which contains rate splitting, superposition coding, Marton coding, GP coding and Wyner-Ziv compression:

$U_1 \sim \mathcal{N}(0, \beta_1 P_1)$
$X_1 = X_1' + U_1$ where $X_1' \sim \mathcal{N}(0, (1-\beta_1)P_1)$
$U_{20} = U_{20}' + \alpha_1 S$ where $U_{20}' \sim \mathcal{N}(0, \beta_2 P_2)$
$U_{21} = U_{21}' + U_{20} + \alpha_2 S$ where $U_{21}' \sim \mathcal{N}(0, \beta_3 P_2)$

$U_{22} = U'_{22} + U_{20} + \alpha_4 U_{21} + \alpha_3 S$ where $U'_{22} \sim \mathcal{N}(0, \beta_4 P_2)$

$X_2 = U'_{22} + U'_{21} + U'_{20}$

$\hat{Y}_2 = \alpha_5 Y_2 + Z'$ where $Z' \sim \mathcal{N}(0, N')$

Parameter β_1 determines the amount of P_1 which is dedicated for collaborative strategy by sending the common message. Parameters β_2, β_3 and β_4 specify the amounts of P_2 which are used to transmit a common message to both receivers, a private message to Dec.1 and a confidential message to Dec.2, respectively. Parameter α_4 enables Enc.2 to bin its codewords (U_{21}, U_{22}) against each other. $\hat{Y}_2$ is defined to perform Wyner-Ziv compression, where α_5 is constant, and quantization noise Z' is a zero-mean Gaussian random variable with variance N' which is independent of other RVs. Parameters $\alpha_1, \alpha_2, \alpha_3$ specify using Dirty Paper Coding (DPC), which is the GP coding proposed for Gaussian case [31]. Using the above mapping with the channel model in (28), we can obtain the mutual information terms of $\mathcal{R}^*$ which are omitted here for brevity.

Fig. 3 shows the region $\mathcal{R}^*$ of Theorem 1 without secrecy for different values of *K* (the power of S), for weak and strong interference. Fig. 4 compares the region $\mathcal{R}^*$ of Theorem 1 without the secrecy constraint with the DF based region of [32]. We set the parameters $P_1 = P_2 = 6$, $h_{31} = h_{42} = 1$,$N_2 = N_3 = N_4 = 1$ in both figures.

In the strong interference case $h_{32} = h_{41} = \sqrt{1.5}$ and in weak interference, $h_{32} = h_{41} = \sqrt{0.55}$. In each figure, we study two scenarios for the cognitive link, where $h_{21} = 1$ corresponds to a moderate cognitive link and $h_{21} = 4$ indicates a strong cognitive link. It is shown that increasing the value of K results in decreasing the amount of R_1. The achievable rate region without state is almost similar to [17]. In Fig.3 we also study the effect of GP coding on the rate region, in which without DPC refers to the case without using dirty paper coding. It can be seen that using DPC causes significant improve in the rate region. We can see that when cognitive link is good enough ($h_{21} = 4$) and is better than the direct link (link between the primary user and intended receiver), DF strategy outperforms CF, because in this case cognitive user can decode the message of the primary user (because of the strong cognitive link). But, when the cognitive link is worse than the direct link (or equal in average), CF is suggested because of performing better in some cases or almost equally to DF meanwhile being simpler than DF.

Fig.5 shows the region R^* of Theorem 1 with secrecy constraint for weak and strong interference and also for different values of K, in which $R_{e2} \leq R_2$. For brevity, we just show the results for moderate cognitive link, i.e. $h_{21} = 1$. Similar to the case without secrecy constraint, it can be seen that increasing the value of K results in decreasing the rate region.

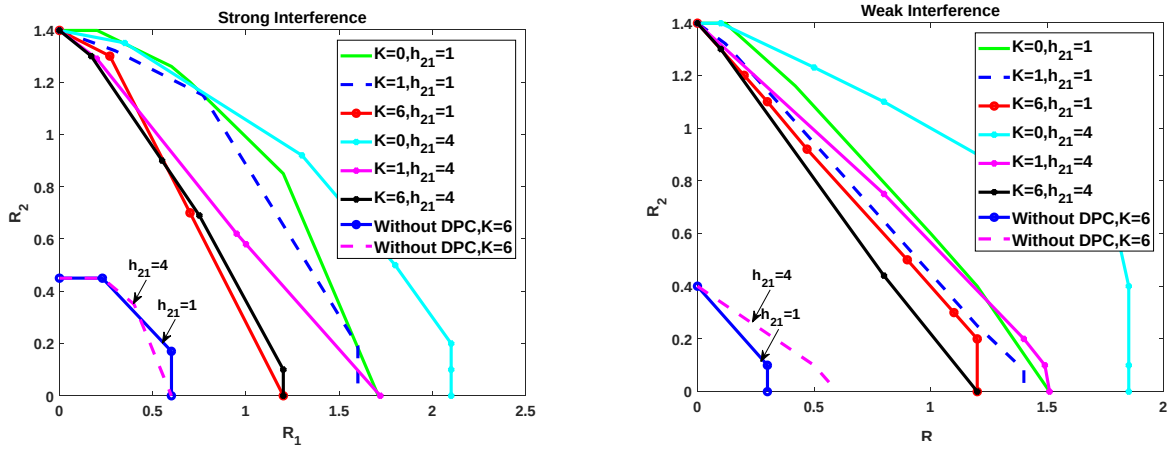

Fig. 3. $\boldsymbol{R}^*$ of Theorem 1 (without secrecy) for different values of $\boldsymbol{K}$ and $\mathbf{h_{21}}$,where $\boldsymbol{P_1 = P_2 = 6}$. Left: Strong interference ($\boldsymbol{h_{32} = h_{41} = \sqrt{1.5}}$). Right: Weak interference ($\boldsymbol{h_{32} = h_{41} = \sqrt{.55}}$).

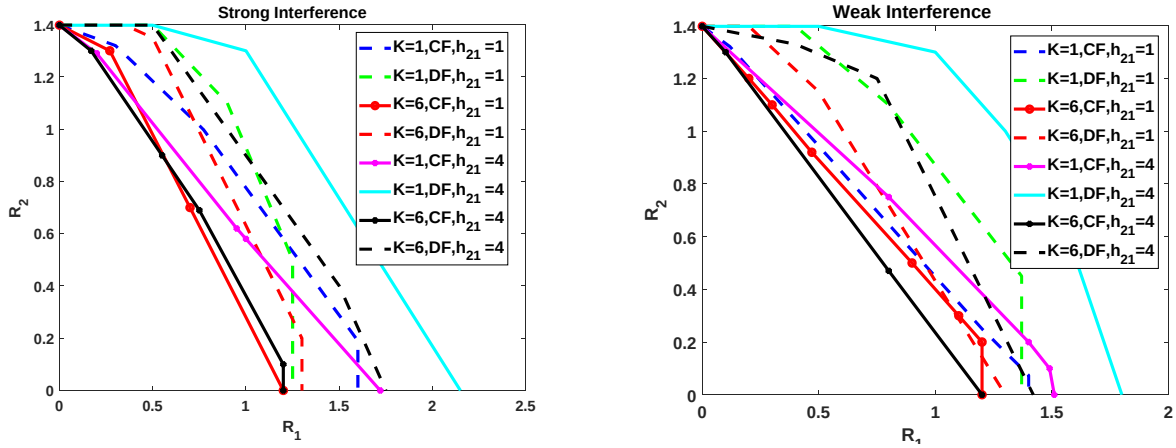

Fig. 4. Comparison between $\boldsymbol{R}^*$ of Theorem 1 (without secrecy constraint) and DF based region [32] ,where $\boldsymbol{P_1 = P_2 = 6}$. Left: Strong interference ($\boldsymbol{h_{32} = h_{41} = \sqrt{1.5}}$). Right: Weak interference ($\boldsymbol{h_{32} = h_{41} = \sqrt{.55}}$).

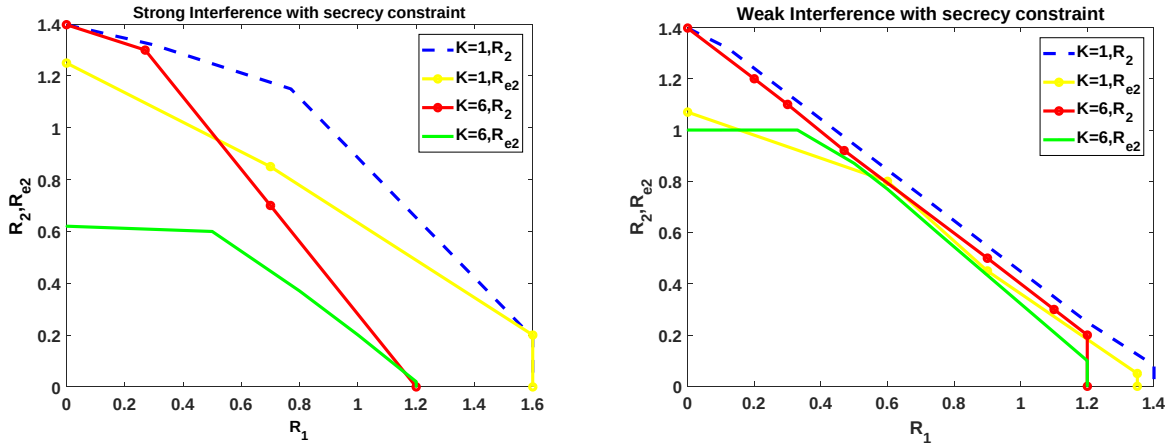

Fig. 5. $\boldsymbol{R}^*$ of Theorem 1for different values of K, where $\boldsymbol{P_1 = P_2 = 6, h_{21} = 1}$. Left: Strong interference ($\boldsymbol{h_{32} = h_{41} = \sqrt{1.5}}$). Right: Weak interference ($\boldsymbol{h_{32} = h_{41} = \sqrt{.55}}$).

V. CONCLUSION

In this paper the secrecy problem of the state dependent causal cognitive interference channel was considered in which the CSI is available non-causally at the cognitive transmitter. The cognitive transmitter wishes to keep its message confidential at the primary receiver, in order to have a reliable communication with its destination. We used a coding scheme which combined CF strategy with Wyner's wiretap coding, Marton coding and GP coding at the cognitive encoder. In this strategy, besides cooperation, the cognitive user mitigated part of the interference by binning its codewords against each other. Sliding window and simultaneous joint decoding techniques were used at the receivers. The achievable secrecy rate region was derived that shows the rate region for which both reliability and security constraints are satisfied. This achievable secrecy rate region was extended to the Gaussian case and some numerical examples were provided. In conclusion, considering causal cognition in C-IFC, and investigating state dependent channels with secrecy constraints are important problems in communication networks, which we tried to propose one model to study these problems simultaneously.

APPENDIX: THE PROOF OF ACHIEVABILITY OF THE EQUIVOCATION-RATE REGION

In this section, we drive the achievability of the equivocation-rate region (11). To achieve this purpose, we follow a proof based on [5], [26] and change it according to our model. By focusing on one block, we compute the equivocation as follows.

$$
\begin{aligned}
&H(\boldsymbol{m_{22}, m_{20}}|Y_3^n) \geq H\big(\boldsymbol{m_{22}, m_{20}}\big|Y_3^n, \boldsymbol{m_1, m_{20}, z_c, z_p}\big) = \\
&H\big(\boldsymbol{m_{22}}, Y_3^n\big|\boldsymbol{m_1, m_{20}, z_c, z_p}\big) - H\big(Y_3^n\big|\boldsymbol{m_1, m_{20}, z_c, z_p}\big) = \\
&H\big(\boldsymbol{m_{22}}, Y_3^n, U_{22}^n\big|\boldsymbol{m_1, m_{20}, z_c, z_p}\big) - H\big(U_{22}^n\big|\boldsymbol{m_1, m_{20}, z_c, z_p, m_{22}}, Y_3^n\big) - H\big(Y_3^n\big|\boldsymbol{m_1, m_{20}, z_c, z_p}\big) = \\
&H\big(\boldsymbol{m_{22}}, U_{22}^n\big|\boldsymbol{m_1, m_{20}, z_c, z_p}\big) + H\big(Y_3^n\big|\boldsymbol{m_1, m_{20}, z_c, m_{22}, z_p}, U_{22}^n\big) - H\big(\boldsymbol{U_{22}}^n\big|\boldsymbol{m_1, m_{20}, z_c, z_p, m_{22}}, Y_3^n\big) - \\
&H\big(Y_3^n\big|\boldsymbol{m_1, m_{20}, z_c, z_p}\big) \geq^{(a)} H\big(U_{22}^n\big|\boldsymbol{m_1, m_{20}, z_c, z_p}\big) + H\big(Y_3^n|U_{22}^n, U_{20}^n, U_{21}^n, X_1^n\big) - \\
&H\big(U_{22}^n\big|\boldsymbol{m_1, m_{20}, z_c, z_p, m_{22}}, Y_3^n\big) - H\big(Y_3^n\big|\boldsymbol{m_1, m_{20}, z_c, z_p}\big) \qquad (30)
\end{aligned}
$$

where (a) is because of the fact that Y_3^n is independent of $(m_1, m_{20}, z_c, m_{22}, z_p)$ given $(X_1, U_{20}, U_{22}, U_{21})$. Now, we bound each term of (30). For the first term in (30), we have

$$
\begin{aligned}
&H\big(\boldsymbol{U_{22}}^n\big|\boldsymbol{m_1, m_{20}, z_c, z_p}\big) \geq^{(b)} H(\boldsymbol{U_{22}}^n|\boldsymbol{X_1}^n, \boldsymbol{U_{20}}^n, \boldsymbol{U_{21}}^n) \geq \\
&H(\boldsymbol{U_{22}}^n|\boldsymbol{X_1}^n, \boldsymbol{U_{20}}^n, \boldsymbol{U_{21}}^n) - H\big(\boldsymbol{U_{22}}^n\big|\boldsymbol{Y_4}^n, \boldsymbol{U_{20}}^n, \boldsymbol{U_{21}}^n, \widehat{\boldsymbol{Y}}_2^{\,n}\big) = \\
&I\big(\boldsymbol{U_{22}}^n; \boldsymbol{Y_4}^n\widehat{\boldsymbol{Y}}_2^{\,n}\big|\boldsymbol{U_{20}}^n, \boldsymbol{U_{21}}^n\big) - I(\boldsymbol{U_{22}}^n; \boldsymbol{X_1}^n|\boldsymbol{U_{20}}^n, \boldsymbol{U_{21}}^n) \geq^{(c)} \boldsymbol{n}[I\big(\boldsymbol{U_{22}}; \boldsymbol{Y_4}\widehat{\boldsymbol{Y}}_2\big|\boldsymbol{U_{20}, U_{21}}\big) - \\
&I(\boldsymbol{U_{22}}; \boldsymbol{X_1}|\boldsymbol{U_{20}, U_{21}}) \qquad (31)
\end{aligned}
$$

where (b) is because of using the data processing inequality [29], which expresses that $\mathrm{U}_{22}^{\mathrm{n}}$, is independent of $(\mathrm{z_c}, \mathrm{m}_{20}, \mathrm{m}_1, \mathrm{z_p})$ given $(\mathrm{U}_{20}^{\mathrm{n}}, \mathrm{X}_1^{\mathrm{n}}, \mathrm{U}_{21}^{\mathrm{n}})$ and (c) is derived by using [33, Lemma 3]. For

the second term of (30) we follow the related equations in [5] and obtain

$$\boldsymbol{\frac{1}{n}H(Y_3^n|U_{22}^n,X_1^n,U_{20}^n,U_{21}^n)\geq H(Y_3|U_{22},X_1,U_{20},U_{21},S)-\epsilon_1} \tag{32}$$

where $\epsilon_1 \to 0$ for $n \to \infty$. For the third term of (30), we use Fano's inequality [28] and obtain

$$\frac{1}{n}H(U_{22}^n|m_{20},z_c,z_p,m_1,m_{22},Y_3^n)<\epsilon_2 \tag{33}$$

where $\epsilon_2 \to 0$ for $n \to \infty$. For computing the fourth term in (30), similar to [26], first we define

$$\hat{Y}_3^n=\begin{cases}Y_3^n & if\ (U_1^n,X_1^n,Y_3^n,U_{20}^n,U_{21}^n)\in A_\epsilon^n\\ Z^n & otherwise\end{cases} \tag{34}$$

where Z^n is an arbitrary sequence that is contained in Y_3^n. Now, we have

$$\begin{aligned}&\tfrac{1}{n}H\big(Y_3^n\big|m_{20},z_c,z_p,m_1\big)\ =\tfrac{1}{n}\textstyle\sum_{m_1,m_{20},z_c}[\Pr\{M_1=m_1,M_{20}=m_{20},Z_c=z_c,Z_p=\\&z_p\}H\big(Y_3^n\big|M_1=m_1,M_{20}=m_{20},Z_c=z_c,Z_p=z_p\big)]\leq\tfrac{1}{n}\textstyle\sum_{m_1,m_{20},z_c}[\Pr\{M_1=m_1,M_{20}=m_{20},Z_c=\\&z_c,Z_p=z_p\}H\big(\hat{Y}_3^n,Y_3^n\big|M_1=m_1,M_{20}=m_{20},Z_c=z_c,Z_p=z_p\big)]=\tfrac{1}{n}\textstyle\sum_{m_1,m_{20},z_c}[\Pr\{M_1=m_1,M_{20}=\\&m_{20},Z_c=z_c,Z_p=\\&z_p\}[H\big(\hat{Y}_3^n\big|M_1=m_1,M_{20}=m_{20},Z_c=z_c,Z_p=z_p\big)+\\&H\big(Y_3^n\big|M_1=m_1,M_{20}=m_{20},Z_c=z_c,Z_p=z_p,\hat{Y}_3^n\big)]]\end{aligned} \tag{35}$$

For the first term in (35) we can write

$$\begin{aligned}&\boldsymbol{\tfrac{1}{n}\textstyle\sum_{m_1,m_{20},z_c,z_p}\Pr\{M_1=m_1,M_{20}=m_{20},Z_c=z_c,Z_p=}\\&\boldsymbol{z_p\}H\big(\hat{Y}_3^n\big|M_1=m_1,M_{20}=m_{20},Z_c=z_c,Z_p=z_p\big)\leq^{(d)}\tfrac{1}{n}\textstyle\sum_{m_1,m_{20},z_c,z_p}\Pr\{M_1=m_1,M_{20}=}\\&\boldsymbol{m_{20},z_c=z_c,Z_p=z_p\}\log\left|A_\epsilon^{(n)}\big(P_{Y_3|U_{20},X_1,U_{21}}\big)\right|\leq\textstyle\sum_{m_1,m_{20},z_c,z_p}\Pr\{M_1=m_1,M_{20}=m_{20},z_c=}\\&\boldsymbol{z_c,Z_p=z_p\}[H(Y_3|U_{20},U_{21},X_1)+\epsilon_3]\leq H((Y_3|U_{20},U_{21},X_1)+\epsilon_3}\end{aligned} \tag{36}$$

where (d) is because of AEP [28], and $\epsilon_3 \to 0$ for $n \to \infty$. In order to bound the second term of (35), by using Fano's inequality, we can write

$$\begin{aligned}&\tfrac{1}{n}\textstyle\sum_{m_1,m_{20},z_c,z_p}\Pr\{M_1=m_1,M_{20}=m_{20},Z_c=z_c,Z_p=\\&z_p\}H\big(Y_3^n\big|M_1=m_1,M_{20}=m_{20},Z_c=z_c,Z_p=z_p,\hat{Y}_3^n\big)\leq\tfrac{1}{n}\textstyle\sum_{m_1,m_{20},z_c,z_p}\Pr\{M_1=m_1,M_{20}=m_{20},Z_c=\\&z_c,Z_p=z_p\}(1+\Pr\{Y_3^n\neq\hat{Y}_3^n|M_1=m_1,M_{20}=m_{20},Z_c=z_c,Z_p=z_p\}\log|y_3|)=\\&\tfrac{1}{n}+\log|y_3|\textstyle\sum_{m_1,m_{20},z_c,z_p}\Pr\{M_1=m_1,M_{20}=m_{20},Z_c=z_c,Z_p=z_p\}.\Pr\{Y_3^n\neq\hat{Y}_3^n|M_1=m_1,M_{20}=m_{20},Z_c=\\&z_c,Z_p=z_p\}\leq\epsilon_4\end{aligned} \tag{37}$$

where $\epsilon_4 \to 0$ for $n \to \infty$. Hence, from (36) and (37), we can bound the forth term of (30) as

$$\frac{1}{n}H(Y_3^n|m_1, m_{20}, z_c, z_p) \le H(Y_3|X_1, U_{20}, U_{21}) + \epsilon_5 \tag{38}$$

where $\epsilon_5 \to 0$ for $n \to \infty$. Substituting (31), (32), (33) and (38) into (30), we obtain

$$\frac{1}{n}H(m_{20}, m_{22}|Y_3^n) \ge I(U_{22}; Y_4\hat{Y}_2U_{20}U_{21}) - I(U_{22}; X_1U_{20}U_{21}) + H(Y_3|X_1, U_{20}, U_{21}, U_{22}, S) - H(Y_3|X_1, U_{20}, U_{21}) - \epsilon_6 \ge I(U_{22}; Y_4\hat{Y}_2U_{20}U_{21}) - I(U_{22}S; X_1U_{20}U_{21}) - I(Y_3; U_{22}S|X_1U_{20}U_{21}) - \epsilon_6 = I(U_{22}; Y_4\hat{Y}_2U_{20}U_{21}) - I(U_{22}S; Y_3X_1U_{20}U_{21}) - \epsilon_6 \tag{39}$$

where $\epsilon_6 \to 0$ for $n \to \infty$. According to the definition of R_{e2} in (5)-(6) we conclude

$$R_{e2} \le I(U_{22}; Y_4\hat{Y}_2U_{20}U_{21}) - I(U_{22}S; X_1Y_3U_{20}U_{21}) \tag{40}$$

Therefore (11) is proved. ■

REFERENCES

[1] A. D. Wyner, "The wire-tap channel," Bell System Technical Journal, vol. 57, no. 8, pp. 1355-1367, Oct. 1975.

[2] I. Csisz´ar and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inform. Theory*, vol. 24, no. 3, pp. 339-348, May 1978.

[3] Y. Liang, H. V. Poor, and S. Shamai, Information Theoretic Security, 1st ed. Hanover, MA, USA: Now Publishers Inc., 2009.

[4] M. Bloch and J. Barros, Physical-Layer Security: From Information Theory to Security Engineering, Cambridge University Press, 2011.

[5] Y. Liang, A. Somekh-Baruch, H. V. Poor, S. Shamai, and S. Verd´u, "Capacity of cognitive interference channels with and without secrecy," *IEEE Trans. Inform. Theory*, vol. 55, no. 2, pp. 604–618, Feb. 2009.

[6] H. Zivari-Fard, B. Akhbari, M. Ahmadian-Attari, and M. R. Aref, "Multiple access channel with common message and secrecy constraint," *IET Comm*., vol. 10, no. 1, pp.98-110, Sep. 2016.

[7] H. Zivari-Fard, B. Akhbari, M. Ahmadian-Attari, and M. R. Aref, "Imperfect and perfect secrecy in compound multiple access channel with confidential message," *IEEE Trans. on Inform. Forensics and Security*, vol. 11, no.6, pp.1239-1251, Mar. 2016.

[8] T. S. Han and K. Kobayashi, "A new achievable rate region for the interference channel," *IEEE Trans. on Inform. Theory*, vol. 27, pp. 49-60, Jan. 1981.

[9] N. Devroye, P. Mitran, V. Tarokh, "Achievable rates in cognitive radio channels," *IEEE Trans. on Inform. Theory*, vol. 52, pp. 1813-1827, May 2006.

[10] S. Gel'fand and M. Pinsker, "Coding for channels with random parameters," *Prob. Contr. Inform. Theory*, vol. 9, no. 1, pp. 19-31, Jan. 1980.

[11] A. Jovicic, P. Viswanath, "Cognitive radio: An information-theoretic perspective," *IEEE Trans. on Inform. Theory*, vol.55, pp. 3945-3958,Sep. 2009.

[12] H. G. Bafghi and B. Seyfe, "On the secrecy of the cognitive interference channel with channel state," *Journal of Communication Engineering*, vol. 2, no. 1, pp. 54-62, Winter 2013.

[13] S. Rini, D. Tuninetti, and N. Devroye. "Inner and outer bounds for the Gaussian cognitive interference channel and new capacity results," *IEEE Trans. on Inform. Theory*, vol. 58, no. 2, pp. 820-848, Feb. 2012.

[14] J. Jiang and Y. Xin, "On the achievable rate regions for interference channels with degraded message sets," *IEEE Trans. on Inform. Theory*, vol. 54, pp. 4707-4712, Oct. 2008.

[15] S. Rini, and C. Huppert. "On the capacity of cognitive interference channel with a common cognitive message," *Trans. on Emerging Telecomm. Technologies*, vol. 26, no. 3, pp. 432-447, Mar. 2015.

[16] T. M. Cover and A. El Gamal, "Capacity theorems for relay channels," *IEEE Trans. on Inform. Theory*, vol. 25, pp. 572-584, Sep. 1979.

[17] M. Mirmohseni, B. Akhbari, and M. Aref, "Compress-and-forward strategy for causal cognitive interference channel," in *IEEE Int. Symp. on Inform. Theory and Inform. Security (ICITIS)*, Beijing, China, Dec. 2010, pp. 1088-1095.

[18] K. Marton, "A coding theorem for the discrete memoryless broadcast channel," *IEEE Trans. on Inform. Theory*, vol. 25, no. 3, pp. 306-311, May 1979.

[19] M. Mirmohseni, B. Akhbari, and M. R. Aref. "On the capacity of interference channel with causal and noncausal generalized feedback at the cognitive transmitter," *IEEE Trans. on Inform. Theory*, vol. 58, no.5, pp. 2813-2837, May 2012.

[20] S.H. Seyedmehdi, J. Jiang, Y. Xin, and X. Wang, "An improved achievable rate region for causal cognitive radio," in *IEEE Int. Symp. On Inform. Theory (ISIT)*, Seoul, South Korea, June 2009, pp. 611-615.

[21] D. Maamari, D. Tuninetti, and N. Devroye. "Multi-user Cognitive Interference Channels: A Survey and New Capacity Results," *IEEE Trans. on Cognitive Comm. and Networking*, vol. 1, no. 1, pp.29-44, Mar. 2015.

[22] M. Cardone , D. Tuninetti, and R. Knopp, "The two-user causal cognitive interference channel: Novel outer bounds and constant gap result for the symmetric Gaussian noise channel in weak interference," *IEEE Trans. on Inform. Theory*, vol. 62, no. 9, pp.4993-5017, Sep. 2016.

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

[24] R. Duan and Y. Liang. "Bounds and capacity theorems for cognitive interference channels with state," *IEEE Trans. on Inform. Theory*, vol. 61, no. 1, pp. 280-304, Jan. 2015.

[25] A. Somekh-Baruch, S. Shamai, and S. Verd´u, "Cognitive interference channels with state information," in *IEEE Int. Symp. on Inform. Theory (ISIT)*, Toronto, Canada , July 2008, pp. 1353-1357.

[26] H.G. Bafghi, B. Seyfe, M. Mirmohseni, and M.R. Aref, "On the secrecy of the cognitive interference channel with partial channel states," *Trans. on Emerging Telecomm. Technologies*, vol. 27, no. 11, pp.1472-1485, Nov. 2016.

[27] L. Zhang, J. Jiang, and C. Shuguang, "Gaussian interference channel with state information," *IEEE Trans. on Wireless Commun.*, vol. 12, no. 8, pp. 4058-4071, Aug. 2013.

[28] A. El Gamal and Y.-H. Kim, Network information theory: Cambridge university press, 2011.

[29] T. M. Cover and J. A. Thomas, Elements of Information Theory, 2nd ed. Wiley Series in Telecomm, 2006.

[30] B. Akhbari, M. Mirmohseni, and M. Aref, "Compress-and-forward strategy for the relay channel with causal and non-causal channel state information," *IET comm.*, vol. 4, no.10, pp. 1174-1186, June 2009.

[31] M. H. M. Costa, "Writing on dirty paper," *IEEE Trans. on Inform. Theory*, vol. 29, pp. 439-441, May 1983.

[32] S. Rahbarfam, B. Akhbari, "Achievable rate regions for state dependent causal cognitive interference channel," submitted to *IEEE Trans. on Cognitive Comm. and Networking*, 2016.

[33] R. Liu, I. Maric, P. Spasojevic, and R. D. Yates, "Discrete memoryless interference and broadcast channels with confidential messages: Secrecy rate regions," *IEEE Trans. on Inform. Theory*, vol. 54, no.6, pp. 2493-2507, June 2008.

[34] S. A. Jafar. "Capacity with causal and non-causal side information: A unified view," *IEEE Trans. on Inform. Theory*, vol. 52, no.12, pp. 5468-5474, Dec. 2006.