Communication Sécurisée et Coopération dans les Réseaux sans Fil avec Interférences and of their Inverter

German Bassi

CentraleSupélec

N° d'ordre : 2015-18-TH

CentraleSupélec

ÉCOLE DOCTORALE STITS
« Sciences et Technologies de l'Information des Télécommunications et des Systèmes »

THÈSE DE DOCTORAT

DOMAINE : STIC
Spécialité : Télécommunications

Soutenue le
6 Juillet 2015

par:

Germán BASSI

Communication Sécurisée et Coopération dans les Réseaux sans Fil avec Interférence

Secure Communication and Cooperation in Interference-Limited Wireless Networks

Directeur de thèse :	Hikmet SARI	Professeur (CentraleSupélec)

Composition du jury :

Président du jury :	Michel KIEFFER	Professeur (Université Paris-Sud)
Rapporteurs :	Daniela TUNINETTI	Associate Professor (University of Illinois)
	Aydin SEZGIN	Professor (Ruhr-Universität Bochum)
Examinateurs :	Jean-Claude BELFIORE	Professeur (Télécom ParisTech)
	Deniz GÜNDÜZ	Lecturer (Imperial College London)
	Olivier RIOUL	Professeur (Télécom ParisTech)
Co-encadrants :	Pablo PIANTANIDA	Enseignant-Chercheur (CentraleSupélec)
	Sheng YANG	Enseignant-Chercheur (CentraleSupélec)

. . . we may have knowledge of the past but cannot control it;
we may control the future but have no knowledge of it.
– Claude E. Shannon[1]

And now that you don't have to be perfect, you can be good.
– John Steinbeck[2]

1 *Coding Theorems for a Discrete Source with a Fidelity Criterion: Collected Works of Claude E. Shannon*. IEEE Press, 1993, pp. 325–350.

2 Steinbeck, John. *East of Eden*. New York: Penguin, 2002.

ACKNOWLEDGMENTS

This thesis is the result of countless hours of work during more than three years of my life and, as such, its development is linked to my own growing up as a person. It is impossible to separate the work I have done for this thesis from other aspects of my life. For this reason, I will acknowledge in the following paragraphs all the people that not only have help me arrive at the end of my studies but also that have accompanied me throughout these years.

First of all, I would like to deeply thank my advisors Pablo and Sheng, who gave me the incredible opportunity of working on this 3-year thesis. They took a high risk in doing so because none of them had worked with me before. Gladly, they did more than just giving me this opportunity, they helped me along the road. For this, I will always be in debt with them.

Second, I would like to thank all the kind people I have met during my stay at CentraleSupélec (known before as Supélec). My dearest officemates Meryem, Chien-Chun, Chao, Andrés, Arash, and Victor and all the other students and postdocs, Bakarime, Stefano, João, Matha, Zheng, Salah Eddine, Asma, Abdulaziz, Gil, Daniel, Axel, Ejder, Emmanuel, Gisela and many others, with whom I had both fruitful and meaningless conversations during lunch or coffee breaks. I have also a deep gratitude towards the personnel of the telecommunications department, Catherine, José and Huu-Hung for all the help they kindly provided.

I would also like to thank a particular group of friends I have met at Supélec, Donovan, Nikola and Gilbert, and all the people that surrounded them, like Louise, Maria, Emma, Joan, Meena and Romulo. I have traveled around the world with them and I have taken many beers. And I am happy for all this.

Ma vie en France n'aurait jamais été complète sans un groupe d'amis français. J'ai eu la chance de trouver un excellent groupe au même temps que j'ai trouvé mon amour pour le tango argentin. Charlotte, Solenne, Flora, Teo, Sylvain, Capucine, Pierre, Guillaume, Aziz, Clara, Christine, François, Arnelle, Chloé, Françoise, Natalia, Sol et Mariana, entre autres. C'est grâce à eux que j'ai appris à parler en français.

Y por último, mi mayor deuda de gratitud es hacia mi familia que me acompañó a la distancia todos estos años. Zulema, Héctor, Natalia, Carolina, Valentín y la pequeña Daniela me sacaron innumerables horas de sueño a través de Skype pero me llenaron de alegría y compañía. Gracias a ellos, la vida en un país extranjero fue mucho más amena y nunca me faltó la fuerza para seguir.

CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF PUBLICATIONS

CONFERENCES PAPERS

- G. Bassi, P. Piantanida, and S. Yang, "Capacity to Within a Constant Gap for a Class of Interference Relay Channels," in *Proc. 51st Annual Allerton Conf. Commun., Control, Comput.*, Oct. 2013, pp. 1300–1306.
- ——, "Constant-Gap Results and Cooperative Strategies for a Class of Interference Relay Channels," in *Information Theory (ISIT), 2014 IEEE International Symposium on*, Jun. 2014, pp. 1421–1425.
- G. Bassi, P. Piantanida, and S. Shamai (Shitz), "On the Capacity of the Wiretap Channel with Generalized Feedback," in *Information Theory (ISIT), 2015 IEEE International Symposium on*, Jun. 2015.
- ——, "The Role of Noisy Feedback in Secure Communications," in *2015 European Conference on Networks and Communications (EuCNC) (invited paper)*, Jun. 2015.
- ——, "The Wiretap Channel with Generalized Feedback: Secure Communication and Key Generation," in *2015 IEEE Information Theory Workshop (ITW) (accepted)*, Oct. 2015.

JOURNAL ARTICLES

- G. Bassi, P. Piantanida, and S. Yang, "Capacity Bounds for a Class of Interference Relay Channels," *IEEE Transactions on Information Theory (accepted for publication)*, Mar. 2014. [Online]. Available: http://arxiv.org/abs/1403.3036
- G. Bassi, P. Piantanida, and S. Shamai (Shitz), "The Wiretap Channel with Generalized Feedback: Secure Communication and Key Generation," *IEEE Transactions on Information Theory (in preparation)*, 2015.

ACRONYMS

AWGN	additive white Gaussian noise
BC	broadcast channel
BS	base station
CF	compress-and-forward
DF	decode-and-forward
FME	Fourier-Motzkin elimination
HK	Han-Kobayashi
i.i.d.	independent and identically distributed
IC	interference channel
IRC	interference relay channel
IS-IC	injective semideterministic IC
IS-IRC	injective semideterministic IRC
JSCC	joint source-channel coding
MIMO	multiple-input multiple-output
NNC	noisy network coding
PD	probability distribution
PtP	point-to-point
RC	relay channel
RV	random variable
SK	Schalkwijk-Kailath
SNR	signal-to-noise ratio
WCGF	wiretap channel with generalized feedback
WTC	wiretap channel

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

The probability distribution (PD) of the random vector X^n, $p_{X^n}(x^n)$, is succinctly written as $p(x^n)$ without subscript when it can be understood from the argument x^n.

Given three random variables X, Y, and Z, if its joint PD can be decomposed as $p(xyz) = p(y)p(x|y)p(z|y)$, then they form a Markov chain, denoted by $X \multimap Y \multimap Z$.

Entropy is denoted by $H(\cdot)$ whereas differential entropy, $h(\cdot)$, and the mutual information, $I(\cdot;\cdot)$. The expression $\mathsf{C}[x] = \frac{1}{2}\log_2(1+x)$ stands for the capacity of a Gaussian channel with SNR of value x.

Definitions and properties of strongly typical sequences and delta-convention are provided in Appendix A.

Vectors

We use the notation $x_i^j = (x_i, x_{i+1}, \ldots, x_j)$ to denote the sequence of length $j - i + 1$ for $1 \leq i \leq j$. If $i = 1$, we drop the subscript for succinctness, i.e., $x^j = (x_1, x_2, \ldots, x_j)$. In the second part of the work, we deal primarily with double-indexed sequences where, unless noted otherwise, the indices $j \in [1 : b]$ and $i \in [1 : n]$ correspond to the block index and the time index inside a block, respectively. We shall give briefly some examples of this notation, where the block index is in brackets:

- $x_{i[j]}$ denotes the value of x in time slot i inside block j;
- $x_{[j]}^i = (x_{1[j]}, x_{2[j]}, \ldots, x_{i[j]})$ is a vector with the first i values of x of block j;
- $x_{i[1:j]} = (x_{i[1]}, x_{i[2]}, \ldots, x_{i[j]})$ is a vector with the values of x in time slot i for the first j blocks;
- $x_{[1:j]}^n = (x_{[1]}^n, x_{[2]}^n, \ldots, x_{[j]}^n)$ represents the vector of n-sequences of blocks 1 to j.

However, for ease of notation, we might drop the brackets if the meaning of the indices is clear from context, e.g., $x^n_{[1:j]} = (x^n_1, x^n_2, \ldots, x^n_j)$.

RÉSUMÉ DE LA THÈSE

1 MOTIVATION

Au cours des dernières décennies, le progrès technologique a rendu possible la disponibilité et l'omniprésence de dispositifs portables bon marché et puissants. Ces petits gadgets polyvalents sont devenus une partie importante de notre vie quotidienne, avec de nouvelles applications qui apparaissent périodiquement. D'appels téléphoniques vocaux jusqu'à la transmission de vidéo en haute qualité, la demande de données a considérablement augmenté. En conséquence, les réseaux cellulaires ont vu une augmentation importante du nombre d'utilisateurs mais aussi du trafic de données. Auparavant limités par le bruit, les réseaux cellulaires sont maintenant *limités par l'interférence* du fait d'un grand nombre d'utilisateurs. En exploitant cependant la nature de diffusion des canaux sans fils, les nœuds du réseau peuvent *coopérer* entre eux pour augmenter le débit global du réseau.

La nature ouverte du support sans fil néanmoins, le rend susceptible de nombreuses menaces de sécurité. Des utilisateurs malveillants pourraient perturber activement les transmissions en injectant un signal d'interférence, ou encore passivement acquérir les signaux transmis afin d'obtenir des informations privées. Dans ce deuxième scénario, les actions de l'espion ne sont pas détectées, et aucun des utilisateurs légitimes de la transmission n'est au courant de sa présence. Ces failles de *sécurité* plausibles représentent un défaut du support sans fil. Cependant, avec l'utilisation de la sécurité de la couche physique[1] et en fournissant à l'émetteur d'information supplémentaire présente dans le canal, par exemple, des informations d'état du canal ou un signal de *rétroaction*, la sécurité du système peut être améliorée.

Dans cette thèse, nous menons une étude dans le cadre de la théorie de l'information sur deux questions importantes de la communication sans fil : tout d'abord l'amélioration du débit de données dans les réseaux avec interférence grâce à la coopération entre utilisateurs, et ensuite le renforcement de la sécurité des transmissions à l'aide d'un signal de rétroaction. Nous essayons de donner un aperçu de ces deux problèmes en déterminant les limites de performance de ces systèmes. En particulier, nous nous concentrons sur le canal à relais

1 Par sécurité de la couche physique, nous entendons toute stratégie appliquée à la couche physique qui assure des transmissions *sécurisées* d'information en présence d'un espion, sans recourir au chiffrement au niveau des couches supérieures de la pile de protocoles de communication.

et interférence pour la première partie de la thèse et le canal avec espion et rétroaction généralisée pour la deuxième partie.

Le canal à relais et interférence[2] ou IRC est le modèle de canal le plus simple où l'interférence et le relayage apparaissent ensemble. Deux paires de nœuds émetteurs/récepteurs veulent communiquer indépendamment mais, ce faisant, ils interfèrent entre eux. Un cinquième nœud, le relais, participe dans la transmission afin d'atténuer l'interférence et donc d'améliorer la performance du réseau. Ce modèle soulève la question de la performance des réseaux cellulaires dans la proximité de la frontière de la cellule, mais permet aussi d'analyser une solution possible. Deux stations de base[3] ou BSs adjacentes ont une puissance de signal comparable dans la proximité de leur frontière de cellule, et les utilisateurs d'une cellule éprouvent une interférence significative provenant de la BS dans la cellule voisine. L'inclusion d'un relais fixe, un matériel d'infrastructure qui n'est pas connecté au réseau câblé, peut aider à la transmission entre les stations de base et les utilisateurs mobiles grâce à la réception et la retransmission de messages. En outre, ces relais d'infrastructure peuvent être moins cher à déployer et à entretenir, et peuvent consommer moins d'énergie que les BSs traditionnelles.

Les relais d'infrastructure offrent potentiellement un moyen économique et astucieux pour faire face à l'interférence, sans pour autant sacrifier de ressources. Aujourd'hui la méthode commune pour faire face à ce problème dans les réseaux sans fil est soit d'éviter l'interférence en orthogonalisant les transmissions des utilisateurs dans le temps, la fréquence ou l'espace, soit de la traiter comme un bruit. Cependant, ces techniques peuvent être nuisibles pour la performance du système global en raison d'une orthogonalisation imparfaite dans la pratique, ou dans les scénarios à fortes interférences. Éviter les interférences grâce à la coordination entre cellules est un sujet important d'études [2], car elle fournit des solutions à court terme. Néanmoins, afin d'exploiter pleinement le potentiel du support sans fil, un changement de paradigme est nécessaire pour les réseaux cellulaires de future génération. Dans l'IRC, il est supposé que tous les nœuds utilisent la même fréquence et il n'y a aucune orthogonalisation des signaux. En outre, le relais fonctionne en mode *full-duplex*[4], c'est-à-dire qu'il peut recevoir et transmettre simultanément sur la même ressource de fréquence, espace, ou temps. La mise en œuvre de dispositifs full-duplex bien qu'irréaliste aujourd'hui sera sans aucun doute possible dans un avenir proche.

Le canal avec espion et rétroaction généralisée[5] ou WCGF modèle le problème où un émetteur souhaite communiquer secrètement un message à un récepteur en présence d'un espion passif à l'aide d'un

2 Interference Relay Channel.
3 Base stations.
4 Canal bidirectionnel simultané.
5 Wiretap Channel with Generalized Feedback.

signal de rétroaction. Ce signal est corrélé aux sorties de canal du récepteur et de l'espion, et il est appelé « rétroaction généralisée » pour le différencier de types spécifiques de rétroaction, par exemple la « rétroaction parfaite » ou la « rétroaction d'état du canal ». Le signal de rétroaction peut être présent à l'encodeur par différents moyens. Les utilisateurs finaux peuvent envoyer à l'émetteur par un lien de rétroaction dédié, les observations de leurs canaux, une description de celles-ci, ou certains paramètres associés, par exemple, des coefficients d'évanouissement de leurs canaux. En outre, l'émetteur lui-même est capable d'effectuer des mesures sur le canal, et par conséquent de recueillir des données corrélées avec celles des utilisateurs finaux. La rétroaction généralisée comprend toutes ces différentes possibilités.

L'adoption de la sécurité de la couche physique pour protéger les communications contre les espions en exploitant le caractère aléatoire du milieu physique [3] a récemment fait l'objet d'une grande attention. Cette mise en œuvre pour sécuriser les réseaux sans fil est extrêmement attractive, non seulement parce que la nature ouverte du milieu rend les dispositifs de communication particulièrement sensible à l'écoute, mais aussi parce que l'aléatoirité est disponible en abondance dans de tels scénarios. De plus, la théorie actuelle de la sécurité de la couche physique indique que la sécurisation d'une partie des données peut être fournie à un coût minime dans le débit total. Une condition essentielle sous-jacente à ce résultat prometteur est qu'afin de garantir la sécurité, le récepteur légitime doit avoir un canal de meilleure qualité que celui de l'espion. Cette condition est néanmoins rarement remplie dans les scénarios sans fil où les nœuds sont mobiles. De plus, les utilisateurs légitimes peuvent être encore ignorants de la qualité du canal de l'espion. Toutes ces difficultés rendent la mise en œuvre de ce type de sécurité encore plus difficile. L'utilisation de la rétroaction dans le processus de codage peut cependant être un moyen de surmonter ces problèmes en créant artificiellement un canal de meilleure qualité pour la destination légitime que pour l'espion.

La manière dont la rétroaction devrait être utilisée est un problème intéressant qui doit être résolu. Dans le contexte de sécurisation, il y a deux méthodes différentes pour exploiter le potentiel du signal de rétroaction : une méthode analogique et une méthode numérique. La méthode numérique extrait des bits aléatoires à partir de l'information commune aux utilisateurs légitimes et les utilise pour chiffrer le message à envoyer. En revanche, la méthode analogique tente de cacher les séquences envoyées dans l'espace nul des observations de l'espion de manière à empêcher un décodage correct. La comparaison entre ces deux méthodes pour évaluer la meilleure d'entre elles s'il y en a une, est une question à laquelle nos aimerions répondre dans la deuxième partie de la thèse.

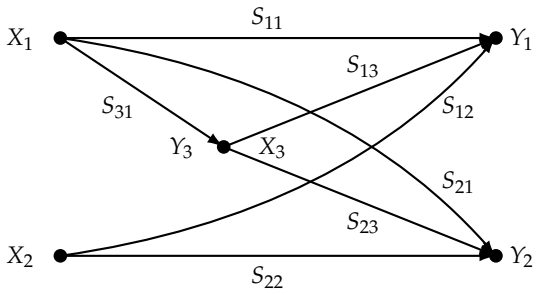


FIGURE 1. : L'IRC gaussien. Les valeurs S_{kl} représentent le SNR entre les nœuds l et k.

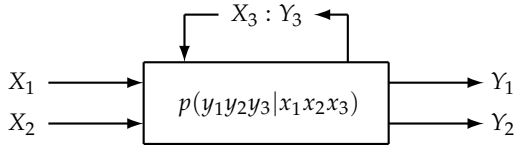


FIGURE 2. : Le modèle de canal à relais et interférence.

2 LE CANAL À RELAIS ET INTERFÉRENCE

Dans le cadre de ce travail, nous nous concentrons sur une version simplifiée de l'IRC [4] qui capte toujours l'interaction complexe entre l'interférence et le relayage. Il s'agit d'un canal à interférence avec deux émetteurs et un nœud de relais qui n'observe qu'un seul des émetteurs. Bien que ce ne soit pas le modèle général d'IRC, nous verrons qu'il présente encore le problème central de l'interférence et du relayage et nous cherchons en conséquence à fournir des indications utiles dans la compréhension de ce problème complexe. Pour la classe des IRCs gaussiens indiquée dans la fig. 1, nous visons notamment à déterminer les différents régimes de rapport signal sur bruit[6] ou SNR pour lesquels différentes techniques de codage et de décodage sont nécessaires pour atteindre la capacité du canal dans un écart constant (*constant gap*).

2.1 *Définition du Problème*

L'IRC se compose de deux codeurs de source, deux destinations et un nœud de relais. Codeur k souhaite envoyer un message $\tilde{m}_k \in \tilde{\mathcal{M}}_{n,k} \triangleq \{1, \ldots, M_{n,k}\}$ à la destination k, $k \in \{1, 2\}$, à l'aide du relais. L'IRC, représenté dans la fig. 2, est modélisé comme un canal sans mémoire et sans rétroaction défini par une distribution de probabilité conditionnelle :

$$p(y_1y_2y_3|x_1x_2x_3) : \mathcal{X}_1 \times \mathcal{X}_2 \times \mathcal{X}_3 \longmapsto \mathcal{Y}_1 \times \mathcal{Y}_2 \times \mathcal{Y}_3$$

6 Signal-to-noise ratio.

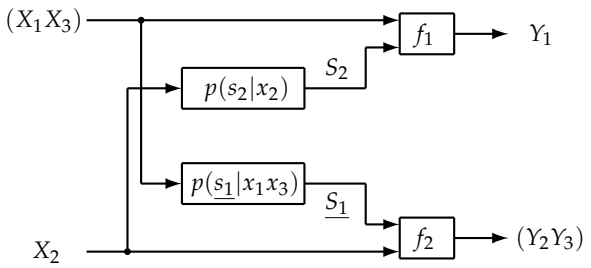


FIGURE 3. : Le modèle d'IRC semi-déterministe et injectif.

où $x_k \in \mathcal{X}_k$ et $y_k \in \mathcal{Y}_k$, $k \in \{1,2\}$, sont l'entrée de la source k et la sortie à la destination k, respectivement, alors que $x_3 \in \mathcal{X}_3$ et $y_3 \in \mathcal{Y}_3$ sont l'entrée et la sortie au relais, respectivement. Les fonctions de relayage sont définies comme $\{\phi_i : \mathcal{Y}_3^{i-1} \mapsto \mathcal{X}_3\}_{i=1}^n$.

Comme il a été indiqué précédemment, dans tout le travail nous traitons avec un type spécifique d'IRC dans lequel une seule des sources est relié au relais, à savoir,

$$p(y_1y_2y_3|x_1x_2x_3) = p(y_3|x_1x_3)p(y_1y_2|x_1x_2x_3y_3). \tag{1}$$

Sauf s'il est noté par ailleurs, ceci est une hypothèse de base de notre modèle.

Definition 0.1. *Une paire de débits (R_1, R_2) est atteignable pour un IRC si pour tout $\epsilon > 0$, il existe un bloc de longueur n, fonctions de codage $enc_k : \tilde{\mathcal{M}}_{n,k} \mapsto \mathcal{X}_k^n$, $M_{n,k} \geq 2^{n(R_k-\epsilon)}$, $k \in \{1,2\}$, et fonctions de décodage $dec_k : \mathcal{Y}_k^n \mapsto \tilde{\mathcal{M}}_{n,k}$, $k \in \{1,2\}$, de sorte que*

$$\frac{1}{M_{n,1}M_{n,2}} \sum_{\tilde{m}_1,\tilde{m}_2} \mathbb{P}\big\{ \big(dec_1(Y_1^n), dec_2(Y_2^n)\big) \neq (\tilde{m}_1, \tilde{m}_2) \mid X_1^n = enc_1(\tilde{m}_1), X_2^n = enc_2(\tilde{m}_2) \big\} \leq \epsilon.$$

La capacité *de l'IRC est la borne supérieure de toutes les paires de débits atteignables.*

Definition 0.2 (IRC Semi-Déterministe et Injectif (IS-IRC))**.** *Dans ce travail, nous allons nous concentrer sur la classe des IRCs dénommée semi-déterministe et injective, représentée sur la fig. 3, qui est une extension de celle introduite pour le canal à interférence [5]. Dans ce modèle, l'aléatoirité du canal est capturée par les signaux d'interférence S_1, S_2 et S_3. Pour plus de clarté, nous noterons la paire (S_1S_3) comme le vecteur $\underline{S_1}$.*

La distribution de probabilité conditionnelle des signaux d'interférence peut être décomposée comme

$$p(\underline{s_1}s_2|x_1x_2x_3) = p(\underline{s_1}|x_1x_3)p(s_2|x_2) \tag{2}$$

et les sorties du canal sont des fonctions déterministes de las variables aléatoires $(X_1, X_2, X_3, \underline{S_1}, S_2)$. Plus précisément, nous avons $Y_1 = f_1(X_1, X_3, S_2)$,

$Y_2 = f_2'(X_2, S_1)$, et $(Y_2 Y_3) = f_2(X_2, \underline{S_1})$, où f_1, f_2', et f_2 sont des fonctions qui, pour chaque (x_1, x_2, x_3),

$$\begin{aligned} f_1(x_1, x_3, \cdot): \ & \mathcal{S}_2 \to \mathcal{Y}_1, && s_2 \mapsto f_1(x_1, x_3, s_2), \\ f_2'(x_2, \cdot): \ & \mathcal{S}_1 \to \mathcal{Y}_2, && s_1 \mapsto f_2'(x_2, s_1), \\ f_2(x_2, \cdot): \ & \underline{\mathcal{S}_1} \to \mathcal{Y}_2 \times \mathcal{Y}_3, && \underline{s_1} \mapsto f_2(x_2, \underline{s_1}) \end{aligned}$$

sont inversibles.

Un cas particulier de l'IS-IRC est le modèle gaussien réel, comme il est montré dans la fig. 1, et défini par

$$Y_1 = h_{11} X_1 + h_{12} X_2 + h_{13} X_3 + Z_1, \tag{3a}$$
$$Y_2 = h_{21} X_1 + h_{22} X_2 + h_{23} X_3 + Z_2, \tag{3b}$$
$$Y_3 = h_{31} X_1 + Z_3, \tag{3c}$$

où chaque processus de bruit $Z_k \sim \mathcal{N}(0, N_k)$, $k \in \{1, 2, 3\}$, est indépendant des autres, et chaque entrée a une contrainte de puissance moyenne $\mathbb{E}[|X_k|^2] \leq P_k$, $k \in \{1, 2, 3\}$. Le lien entre le nœud l et k a un coefficient de canal fixe h_{kl}, et le SNR qui lui est associé est notée $S_{kl} \triangleq |h_{kl}|^2 P_l / N_k$. Dans ce modèle, les signaux d'interférence sont

$$\underline{S_1} = \begin{bmatrix} S_1 \\ S_3 \end{bmatrix} = \begin{bmatrix} h_{21} X_1 + h_{23} X_3 + Z_2 \\ h_{31} X_1 + Z_3 \end{bmatrix} \text{ and } \ S_2 = h_{12} X_2 + Z_1. \tag{4}$$

Par conséquent, les résultats de l'IS-IRC peuvent être appliquées carrément au cas gaussien.

2.2 *Borne Supérieure*

Dans cette section, nous développons une borne supérieure de la capacité de canal pour le modèle IS-IRC décrit dans la section 2.1. Le modèle de la fig. 3 est fourni pour aider le lecteur à comprendre la technique de génie assistée utilisée pour le calcul des bornes. Il est intéressant de souligner que ce modèle suppose que le relais n'a en aucun cas connaissance préalable des messages ni que X_3 ou Y_3 est une deuxième « antenne » de X_1 ou Y_2 comme il pourrait être mal interprété basé sur la figure précitée.

Soit $\mathcal{P}_1$ l'ensemble de toutes les distributions de probabilité jointes qui peuvent être décomposées comme

$$p(q) p(x_1 x_3 | q) p(x_2 | q) p(\underline{v_1} v_2 | x_1 x_2 x_3 q), \tag{5}$$

où $p(\underline{v_1} v_2 | x_1 x_2 x_3 q) = p_{\underline{S_1}|X_1 X_3}(\underline{v_1} | x_1 x_3) p_{S_2|X_2}(v_2 | x_2)$, c'est-à-dire $(\underline{V_1} V_2)$ est une copie conditionnellement indépendante de $(\underline{S_1} S_2)$ sachant $(X_1 X_2 X_3)$. Rappelons-nous que V_1 représente la première composante du $\underline{V_1}$.

Theorem 0.1 (borne supérieure). *Soit $P_1 \in \mathcal{P}_1$ une distribution de probabilité spécifique et soit $\mathcal{R}_o(P_1)$ la région des paires de débits non négatifs (R_1, R_2) qui satisfont*

$$
\begin{aligned}
R_1 &\le I(X_1; Y_1 Y_3 | X_2 X_3 Q), && \text{(6a)}\\
R_1 &\le I(X_1 X_3; Y_1 | X_2 Q), && \text{(6b)}\\
R_2 &\le I(X_2; Y_2 | X_1 X_3 Q), && \text{(6c)}\\
R_1 + R_2 &\le I(X_1 X_3; Y_1 | V_1 X_2 Q) + I(X_1 X_2 X_3; Y_2 | Q), && \text{(6d)}\\
R_1 + R_2 &\le I(X_1 X_2 X_3; Y_1 | V_1 Q) + I(X_1 X_2 X_3; Y_2 | V_2 Q), && \text{(6e)}\\
R_1 + R_2 &\le I(X_1 X_2 X_3; Y_1 | Q) + I(X_2; Y_2 | X_1 V_2 X_3 Q), && \text{(6f)}\\
R_1 + R_2 &\le I(X_1; Y_1 Y_3 | V_1 X_2 X_3 Q) + I(X_1 X_2 X_3; Y_2 | Q), && \text{(6g)}\\
R_1 + R_2 &\le I(X_1 X_2; Y_1 Y_3 | V_1 X_3 Q) + I(X_1 X_2 X_3; Y_2 | V_2 Q), && \text{(6h)}\\
R_1 + R_2 &\le I(X_1 X_2; Y_1 Y_3 | X_3 Q) + I(X_2; Y_2 | X_1 V_2 X_3 Q), && \text{(6i)}\\
R_1 + R_2 &\le I(X_1; Y_1 Y_3 | \underline{V_1} X_2 X_3 Q) + I(X_1 X_2; Y_2 Y_3 | X_3 Q), && \text{(6j)}\\
R_1 + R_2 &\le I(X_1 X_2; Y_1 Y_3 | \underline{V_1} X_3 Q) + I(X_1 X_2; Y_2 Y_3 | V_2 X_3 Q), && \text{(6k)}\\
2R_1 + R_2 &\le I(X_1 X_3; Y_1 | V_1 X_2 Q) + I(X_1 X_2 X_3; Y_1 | Q)\\
&\quad + I(X_1 X_2 X_3; Y_2 | V_2 Q), && \text{(6l)}\\
2R_1 + R_2 &\le I(X_1 X_3; Y_1 | V_1 X_2 Q) + I(X_1 X_2; Y_1 Y_3 | X_3 Q)\\
&\quad + I(X_1 X_2 X_3; Y_2 | V_2 Q), && \text{(6m)}\\
2R_1 + R_2 &\le I(X_1; Y_1 Y_3 | V_1 X_2 X_3 Q) + I(X_1 X_2 X_3; Y_1 | Q)\\
&\quad + I(X_1 X_2 X_3; Y_2 | V_2 Q), && \text{(6n)}\\
2R_1 + R_2 &\le I(X_1; Y_1 Y_3 | V_1 X_2 X_3 Q) + I(X_1 X_2; Y_1 Y_3 | X_3 Q)\\
&\quad + I(X_1 X_2 X_3; Y_2 | V_2 Q), && \text{(6o)}\\
2R_1 + R_2 &\le I(X_1; Y_1 Y_3 | \underline{V_1} X_2 X_3 Q) + I(X_1 X_2 X_3; Y_1 | Q)\\
&\quad + I(X_1 X_2; Y_2 Y_3 | V_2 X_3 Q), && \text{(6p)}\\
2R_1 + R_2 &\le I(X_1; Y_1 Y_3 | \underline{V_1} X_2 X_3 Q) + I(X_1 X_2; Y_1 Y_3 | X_3 Q)\\
&\quad + I(X_1 X_2; Y_2 Y_3 | V_2 X_3 Q), && \text{(6q)}\\
R_1 + 2R_2 &\le I(X_1 X_2 X_3; Y_1 | V_1 Q) + I(X_2; Y_2 | X_1 V_2 X_3 Q)\\
&\quad + I(X_1 X_2 X_3; Y_2 | Q), && \text{(6r)}\\
R_1 + 2R_2 &\le I(X_1 X_2; Y_1 Y_3 | V_1 X_3 Q) + I(X_2; Y_2 | X_1 V_2 X_3 Q)\\
&\quad + I(X_1 X_2 X_3; Y_2 | Q), && \text{(6s)}\\
R_1 + 2R_2 &\le I(X_1 X_2; Y_1 Y_3 | \underline{V_1} X_3 Q) + I(X_2; Y_2 | X_1 V_2 X_3 Q)\\
&\quad + I(X_1 X_2; Y_2 Y_3 | X_3 Q). && \text{(6t)}
\end{aligned}
$$

Il en résulte que une borne supérieure de la capacité de l'IS-IRC est définie par l'union de $\mathcal{R}_o(P_1)$ sur toutes les distributions de probabilité jointes $P_1 \in \mathcal{P}_1$ qui peuvent être décomposées comme (5).

Démonstration. Voir l'annexe 3.A. □

Le modèle gaussien réel, présenté dans la section 2.1, est un cas particulier de l'IS-IRC. Par conséquent, selon (5), les entrées du canal X_1 et X_2 sont indépendantes, et X_1 est arbitrairement corrélées à la signal du relais X_3, c'est-à-dire $\mathbb{E}[X_1X_2] = 0$, $\mathbb{E}[X_1X_3] = \rho\sqrt{P_1P_3}$, et $\mathbb{E}[X_2X_3] = 0$. L'expression gaussienne de la borne supérieure est facilement trouvée en utilisant le modèle (3) et en générant les variables auxiliaires $\underline{V_1}$ et V_2 selon (4), mais avec des bruits indépendants.

2.3 *Bornes Inférieures*

Dans ce qui suit, nous fournissons deux bornes inférieures de la capacité correspondant à deux stratégies différentes de relayage, à savoir, *décoder-et-transmettre*[7] (DF) et *comprimer-et-transmettre*[8] (CF). Avec DF, le relais décode partiellement ou totalement le message de la seule source connectée, le recode et le transmet vers les deux destinations. Avec CF, le relais comprime le signal reçu, et envoie un indice de compression qui lui est associé. Une version précédente de ces stratégies a été présenté dans [4], mais ici nous montrons une expression plus compacte pour la stratégie CF et une nouvelle version nettement améliorée pour la stratégie DF. Quatre ingrédients principaux sont nécessaires : le fendage de débit [9], *binning*, et le codage de bloc-Markov. aux sources, et le décodage en arrière [10] aux destinations. Dans la suite, nous supposons les indices $(k, l) \in \{(1, 2), (2, 1)\}$.

Dans chaque stratégie, pour permettre la coopération du relais, la transmission est divisée en plusieurs blocs. Pendant bloc j, chaque source k divise son message $\tilde{m}_{kj}$ en deux messages : une partie commune m_{kj} et un partie privée w_{kj}. Comme dans la stratégie de Han et Kobayashi (HK), chaque récepteur décode la partie commune du message interférer, réduisant ainsi l'interférence.

Remark 0.1. *Les bornes inférieures énoncés ci-dessous sont applicables aux IRC générales sans mémoire et ainsi ils ne sont pas limités au modèle de l'IS-IRC.*

Décoder-et-Transmettre

Chaque source envoie b messages au cours de $b + 1$ blocs de temps, et le relais transmet dans le bloc j ce qu'il a décodé de la première source dans le bloc précédent. Dans ce schéma, le message *privé* de la première source est divisé en deux parties et le relais ne décode et retransmet qu'une d'elles en plus du message *commun*. À la fin de la transmission, le récepteur k décode en arrière le message privé w_{kj} ainsi que les deux messages communs m_{kj} et m_{lj}.

7 Decode-and-forward.
8 Compress-and-forward.
9 Rate-splitting.
10 Backward decoding.

Soit $\mathcal{P}_2$ l'ensemble de toutes les distributions de probabilité jointes qui peuvent être décomposées comme

$$p(q)p(x_1x_3|q)p(x_2|q)p(v_1|x_1x_3q)p(u_1|x_1q)p(v_2|x_2q)p(v_3|x_3q). \quad (7)$$

Theorem 0.2 (schéma DF partiel). *Soit $P_2 \in \mathcal{P}_2$ une distribution de probabilité spécifique et soit $\mathcal{R}_{p\text{-}DF}(P_2)$ la région des paires de débits non négatifs (R_1, R_2) qui satisfont*

$$\begin{aligned}
R_1 &\le I(U_1;Y_3|X_3Q) + I(X_1;Y_1|V_1U_1V_2X_3Q), && (8a)\\
R_1 &\le I(X_1X_3;Y_1|V_2Q), && (8b)\\
R_2 &\le I(X_2;Y_2|V_1V_3Q), && (8c)\\
R_2 &\le I(V_1X_2V_3;Y_2|Q) - I_b, && (8d)\\
R_1+R_2 &\le I(X_1X_3;Y_1|V_1V_2V_3Q) + I(V_1X_2V_3;Y_2|Q), && (8e)\\
R_1+R_2 &\le I(U_1;Y_3|V_1X_3Q) + I(X_1;Y_1|V_1U_1V_2X_3Q)\\
&\quad + I(V_1X_2V_3;Y_2|Q) - I_b, && (8f)\\
R_1+R_2 &\le I(X_1V_2X_3;Y_1|V_1V_3Q) + I(V_1X_2V_3;Y_2|V_2Q), && (8g)\\
R_1+R_2 &\le I(U_1;Y_3|V_1X_3Q) + I(X_1V_2;Y_1|V_1U_1X_3Q)\\
&\quad + I(V_1X_2V_3;Y_2|V_2Q) - I_b, && (8h)\\
R_1+R_2 &\le I(X_1V_2X_3;Y_1|Q) + I(V_1X_2V_3;Y_2|V_2Q) - I_b, && (8i)\\
R_1+R_2 &\le I(X_1V_2X_3;Y_1|Q) + I(X_2;Y_2|V_1V_2V_3Q), && (8j)\\
R_1+R_2 &\le I(U_1;Y_3|X_3Q) + I(X_1V_2;Y_1|V_1U_1X_3Q)\\
&\quad + I(X_2;Y_2|V_1V_2V_3Q), && (8k)\\
2R_1+R_2 &\le I(X_1X_3;Y_1|V_1V_2V_3Q) + I(X_1V_2X_3;Y_1|Q)\\
&\quad + I(V_1X_2V_3;Y_2|V_2Q), && (8l)\\
2R_1+R_2 &\le I(X_1X_3;Y_1|V_1V_2V_3Q) + I(X_1V_2;Y_1|V_1U_1X_3Q)\\
&\quad + I(U_1;Y_3|X_3Q) + I(V_1X_2V_3;Y_2|V_2Q), && (8m)\\
2R_1+R_2 &\le I(U_1;Y_3|V_1X_3Q) + I(X_1;Y_1|V_1U_1V_2X_3Q) - I_b\\
&\quad + I(X_1V_2X_3;Y_1|Q) + I(V_1X_2V_3;Y_2|V_2Q), && (8n)\\
R_1+2R_2 &\le I(X_1V_2X_3;Y_1|V_1V_3Q) + I(X_2;Y_2|V_1V_2V_3Q)\\
&\quad + I(V_1X_2V_3;Y_2|Q), && (8o)\\
R_1+2R_2 &\le I(U_1;Y_3|V_1X_3Q) + I(X_1V_2;Y_1|V_1U_1X_3Q) - I_b\\
&\quad + I(X_2;Y_2|V_1V_2V_3Q) + I(V_1X_2V_3;Y_2|Q) && (8p)
\end{aligned}$$

où $I_b \triangleq I(X_3;V_1|V_3Q)$. Il en résulte que une région atteignable dans l'IS-IRC est définie par l'union de $\mathcal{R}_{p\text{-}DF}(P_2)$ sur toutes les distributions de probabilité jointes $P_2 \in \mathcal{P}_2$ qui peuvent être décomposées comme (7).

Démonstration. Les séquences V_2^n et X_2^n véhiculent les messages communs et complets de la deuxième source, respectivement, avec X_2^n superposée sur V_2^n. Le code de la première source est cependant beaucoup plus complexe, afin de permettre au relais de coopérer, voir la

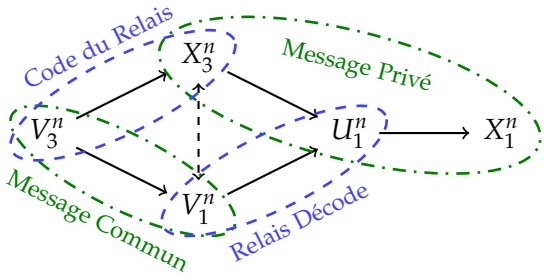


FIGURE 4. : Séquences du relais et de la première source. Les flèches pleines dénotent des séquences superposées et les flèches en pointillé indiquent binning.

fig. 4. Le schéma oblige le relais à décoder le message commun de la première source, c'est-à-dire la séquence V_1^n, entièrement, mais seulement une partie du message privé. Ainsi, contrairement à la seconde source, une couche intermédiaire U_1^n est compris entre V_1^n et X_1^n.

Les indices décodés par le relais sont transmises par des séquences superposées V_3^n et X_3^n, analogue à V_1^n et U_1^n. Une coopération cohérente est obtenue en superposant V_1^n et U_1^n sur V_3^n et X_3^n, respectivement. Une étape supplémentaire de binning entre les séquences V_1^n et X_3^n est nécessaire pour se conformer à (7), ainsi le terme négatif I_b dans (8).

Voir l'annexe 3.C pour plus de détails. □

Si le relais est en mesure de décoder complètement le message privé de la première source sans imposer une restriction au débit atteignable, la maximisation de la borne inférieure précédente entraînerait $U_1 = X_1$. Dans ce cas, soit $\mathcal{P}_3$ l'ensemble de toutes les distributions de probabilité jointes qui peuvent être décomposées comme

$$p(q)p(x_1x_3|q)p(x_2|q)p(v_1|x_1x_3q)p(v_2|x_2q)p(v_3|x_3q). \tag{9}$$

Corollary 0.1 (schéma DF total). *Soit $P_3 \in \mathcal{P}_3$ une distribution de probabilité spécifique et soit $\mathcal{R}_{f\text{-}DF}(P_3)$ la région des paires de débits non négatifs (R_1, R_2) qui satisfont*

$$R_1 \leq I(X_1; Y_3|X_3Q), \tag{10a}$$
$$R_1 \leq I(X_1X_3; Y_1|V_2Q), \tag{10b}$$
$$R_2 \leq I(X_2; Y_2|V_1V_3Q), \tag{10c}$$
$$R_2 \leq I(V_1X_2V_3; Y_2|Q) - I_b, \tag{10d}$$
$$R_1 + R_2 \leq I(X_1X_3; Y_1|V_1V_2V_3Q) + I(V_1X_2V_3; Y_2|Q), \tag{10e}$$
$$R_1 + R_2 \leq I(X_1; Y_3|V_1X_3Q) + I(V_1X_2V_3; Y_2|Q) - I_b, \tag{10f}$$
$$R_1 + R_2 \leq I(X_1V_2X_3; Y_1|V_1V_3Q) + I(V_1X_2V_3; Y_2|V_2Q), \tag{10g}$$
$$R_1 + R_2 \leq I(X_1V_2X_3; Y_1|Q) + I(V_1X_2V_3; Y_2|V_2Q) - I_b, \tag{10h}$$

$$R_1 + R_2 \leq I(X_1V_2X_3; Y_1|Q) + I(X_2; Y_2|V_1V_2V_3Q), \tag{10i}$$
$$2R_1 + R_2 \leq I(X_1X_3; Y_1|V_1V_2V_3Q) + I(X_1V_2X_3; Y_1|Q) + I(V_1X_2V_3; Y_2|V_2Q), \tag{10j}$$
$$2R_1 + R_2 \leq I(X_1; Y_3|V_1X_3Q) + I(X_1V_2X_3; Y_1|Q) + I(V_1X_2V_3; Y_2|V_2Q) - I_b, \tag{10k}$$
$$R_1 + 2R_2 \leq I(X_1V_2X_3; Y_1|V_1V_3Q) + I(X_2; Y_2|V_1V_2V_3Q) + I(V_1X_2V_3; Y_2|Q) \tag{10l}$$

où $I_b \triangleq I(X_3; V_1|V_3Q)$. *Il en résulte que une région atteignable dans l'IS-IRC est définie par l'union de* $\mathcal{R}_{f\text{-}DF}(P_3)$ *sur toutes les distributions de probabilité jointes* $P_3 \in \mathcal{P}_3$ *qui peuvent être décomposées comme* (9).

Démonstration. La région $\mathcal{R}_{\text{f-DF}}$ (10) n'est pas obtenue en mettant $U_1 = X_1$ en $\mathcal{R}_{\text{p-DF}}$ (8), puisque certaines limites supplémentaires redondantes restent. Pour éliminer facilement ces limites, il faut remplacer U_1 avec X_1 dans l'ensemble des débits partiels avant d'utiliser l'élimination de Fourier-Motzkin dans la preuve du théorème 0.2. Voir l'annexe 3.D pour plus de détails. □

Dans le schéma DF total, puisque le relais décode la séquence X_1^n complètement, il n'y a pas de limite à la quantité d'information qui peut être envoyé comme message commun. Toutefois, dans le schéma DF partiel, nous introduisons la variable U_1 entre X_1 et V_1, ce qui interdit $V_1 = X_1$. Par conséquent, la structure du code impose que le relais devrait décoder plus facilement le message commun V_1^n que la seconde destination. Si tel n'est pas le cas, nous devrions employer le schéma CF présenté dans la section suivante.

Comprimer-et-Transmettre

Dans ce schéma, le relais ne décode pas le message et il envoie uniquement une version compressée de son observation du canal. Les destinations décodent conjointement cette information avec leur message et la couche commune de l'interférence. La transmission se fait dans $b + b_s$ blocs de temps, de façon similaire à [6,7], et pendant les derniers b_s blocs, le relais répète son message pour assurer un décodage correct sur les deux destinations.

Soit $\mathcal{P}_4$ l'ensemble de toutes les distributions de probabilité jointes qui peuvent être décomposées comme

$$p(q)p(v_1x_1|q)p(v_2x_2|q)p(x_3|q)p(\hat{y}_3|x_3y_3q), \tag{11}$$

et considérez l'ensemble des expressions suivantes

$$I_{k1} \triangleq \min\{I(X_k; Y_k\hat{Y}_3|V_kV_lX_3Q), I(X_kX_3; Y_k|V_kV_lQ) - I_k\}, \tag{12a}$$
$$I_{k2} \triangleq \min\{I(X_k; Y_k\hat{Y}_3|V_lX_3Q), I(X_kX_3; Y_k|V_lQ) - I_k\}, \tag{12b}$$
$$I_{k3} \triangleq \min\{I(X_kV_l; Y_k\hat{Y}_3|V_kX_3Q), I(X_kV_lX_3; Y_k|V_kQ) - I_k\}, \tag{12c}$$
$$I_{k4} \triangleq \min\{I(X_kV_l; Y_k\hat{Y}_3|X_3Q), I(X_kV_lX_3; Y_k|Q) - I_k\} \tag{12d}$$

où $I_k \triangleq I(\hat{Y}_3; Y_3|X_kV_lX_3Y_kQ)$ et

$$I'_{k1} \triangleq I(X_k; Y_k|V_kV_lQ), \tag{13a}$$
$$I'_{k2} \triangleq I(X_k; Y_k|V_lQ), \tag{13b}$$
$$I'_{k3} \triangleq I(X_kV_l; Y_k|V_kQ), \tag{13c}$$
$$I'_{k4} \triangleq I(X_kV_l; Y_k|Q). \tag{13d}$$

Theorem 0.3 (schéma CF). *Soit $P_4 \in \mathcal{P}_4$ une distribution de probabilité spécifique et soit $\mathcal{R}_{CF_0}(P_4)$ la région des paires de débits non négatifs (R_1, R_2) qui satisfont*

$$R_k \leq I_{k2}, \tag{14a}$$
$$R_k + R_l \leq \min\{I_{k1} + I_{l4}, I_{k3} + I_{l3}\}, \tag{14b}$$
$$2R_k + R_l \leq I_{k1} + I_{k4} + I_{l3}, \tag{14c}$$

et soit $\mathcal{R}_{CF_k}(P_4)$

$$R_k \leq I_{k2}, \tag{15a}$$
$$R_l \leq I'_{l2}, \tag{15b}$$
$$R_k + R_l \leq \min\{I_{k1} + I'_{l4}, I_{k4} + I'_{l1}, I_{k3} + I'_{l3}\}, \tag{15c}$$
$$2R_k + R_l \leq I_{k1} + I_{k4} + I'_{l3}, \tag{15d}$$
$$R_k + 2R_l \leq I_{k3} + I'_{l1} + I'_{l4}. \tag{15e}$$

Il en résulte que une région atteignable dans l'IS-IRC est définie par l'union de $\mathcal{R}_{CF_0}(P_4) \cup \mathcal{R}_{CF_1}(P_4) \cup \mathcal{R}_{CF_2}(P_4)$ sur toutes les distributions de probabilité jointes $P_4 \in \mathcal{P}_4$ qui peuvent être décomposées comme dans (11).

Démonstration. Puisque le relais ne décode pas le message, les séquences V_k^n et X_k^n portent le message commun et complet du bloc actuel, respectivement. La variable X_3 est indépendante des signaux des sources et est utilisée pour reconstruire l'observation Y_3 du relais.

Chaque expression I_{ki} ressemble au débit atteignable du schéma CF pour le canal à relais, et lorsque le relais est ignoré, elle se réduit à l'expression I'_{ki}. La région $\mathcal{R}_{\text{CF}_0}$ (14) est obtenue lorsque les deux destinations décodent l'indice de compression alors que dans la région $\mathcal{R}_{\text{CF}_k}$ (15) seulement la destination k le décode.

	$S_{31} < S_{21}$	$S_{31} \geq S_{21}$
$S_{31} < S_{11}$	CF	DF partiel
$S_{31} \geq S_{11}$	DF total	

TABLE 2. : Régimes de SNR et meilleures stratégies par rapport à l'écart constant.

Régime de SNR		CF	DF
$S_{31} < S_{21}$	$S_{31} < S_{11}$	1.32	–
	$S_{31} \geq S_{11}$	1.32	1
$S_{31} \geq S_{21}$	$S_{31} \geq S_{11}$	–	1
	$S_{31} < S_{11}$	–	1.5

TABLE 3. : Écart de bits maximal de chaque stratégie pour chaque régime de SNR.

Étant donné que l'indice de compression est envoyé en utilisant le codage de bloc-Markov, chaque destination a besoin d'assurer son décodage correct dans chaque bloc, ce qui se traduit par des bornes supplémentaires non représentés ici. Toutefois, l'union $\mathcal{R}_{\mathrm{CF}_0} \cup \mathcal{R}_{\mathrm{CF}_1} \cup \mathcal{R}_{\mathrm{CF}_2}$ après la maximisation sur toutes les distributions de probabilité jointes fournit que ces limites sont redondantes. Voir l'annexe 3.E pour plus de détails. □

Remark 0.2. *Le relais ne génère qu'une indice de compression qui est décodable par les deux destinations, c'est-à-dire le débit de compression est déterminé par le canal le plus faible. Il est possible, cependant, d'améliorer la performance avec la technique de raffinement successif* [11] *non utilisée ici à cause de sa complexité. Comme nous le verrons dans la prochaine section, deux couches de raffinement successif ne sont pas nécessaires dans la mesure où l'écart constant est concerné.*

2.4 *Résultats d'Écart Constant & Discussion*

Dans cette section, nous évaluons l'écart entre les régions atteignables et la borne supérieure dans le cas gaussien (fig. 1). Ensuite, nous identifions les stratégies qui permettent d'atteindre le meilleur écart constant à la région de capacité pour toute valeur de SNR. Ceci est résumé dans la table 2, tandis que la valeur de l'écart pour chaque stratégie est présentée dans la table 3.

11 Successive refinement.

Le Schéma DF Atteint la Capacité avec un Écart de 1,5 Bits

Le table 3 montre deux valeurs différentes d'écart constant pour ce régime, 1.5 bits étant le plus grand. La différence vient du choix de la distribution de probabilité utilisée dans la borne inférieure comme nous le voyons dans la suite.

Lorsque le relais est proche de la source, c'est-à-dire quand le S_{31} est suffisamment élevé, le relais est capable de décoder le message complètement sans pénaliser le débit atteignable R_1. Par conséquent, comme il est mentionné dans la section 2.3, la distribution de probabilité vérifie $U_1 = X_1$ et la borne inférieure est celle du corollaire 0.1.

Proposition 0.1. *Si $S_{31} \geq S_{11}$, le schéma DF total du corollaire 0.1 atteint la capacité avec un écart de 1 bit.*

Démonstration. L'écart constant mentionné ci-dessus est assez prudent dans la majorité des cas, car il vient de choisir une distribution de probabilité fixe pour la borne inférieure (ce qui réduit le débit atteignable) et de utiliser la borne extérieure du corollaire 3.1. Voir l'annexe 3.F pour plus de détails. □

Si le canal source-relais n'est pas assez bon pour le relais de décoder le message complet, le relais doit le décoder partiellement, c'est-à-dire $U_1 \neq X_1$. Toutefois, en raison de la structure du code, le relais doit encore être en mesure de décoder le message commun.

Proposition 0.2. *Si $S_{31} \geq S_{21}$, le schéma DF partiel du théorème 0.2 atteint la capacité avec un écart de 1.5 bit.*

Démonstration. De la même manière que la preuve de la proposition 0.1, nous réduisons la borne inférieure en fixant la distribution de probabilité et agrandissons la borne extérieure en choisissant un sous-ensemble de ses conditions. Voir l'annexe 3.G pour plus de détails. □

Remark 0.3. *Si $S_{31} \geq S_{11}$ et $S_{31} \geq S_{21}$, le schéma DF, total ou partiel, atteint la capacité avec un écart constant. Néanmoins, ce régime apparaît dans le table 2 comme « DF total » car son écart est moindre.*

Le Schéma CF Atteint la Capacité avec un Écart de 1,32 Bits

Le schéma CF ne fixe aucune condition sur la structure du code des sources, néanmoins, un écart constant ne peut être trouvé que dans le régime $S_{31} \leq S_{21}$.

Proposition 0.3. *Si $S_{31} \leq S_{21}$, le schéma CF du théorème 0.3 atteint la capacité avec un écart de 1.32 bit.*

Démonstration. La preuve suit des étapes similaires que les preuves précédentes. Voir l'annexe 3.H pour plus de détails. □

Le Relayage Dispose d'un Avantage Limité

Il est compréhensible que pour un très faible SNR dans le lien source-relais, l'utilisation du relais a un avantage limité. Dans ce cas, il pourrait être préférable, en raison de la complexité, d'éteindre le relais et d'utiliser le schéma beaucoup plus simple de Han et Kobayashi pour le canal à interférence.

Proposition 0.4. *Si $S_{31} \leq S_{11}/(1+S_{12})$ et $S_{31} \leq S_{21}/(1+S_{22})$, le schéma HK (sans relais) atteint la capacité de l'IS-IRC avec un écart de 1 bit, c'est-à-dire le relais ne incrémente pas le débit atteignable plus de 1 bit.*

Démonstration. Voir l'annexe 3.I. □

Les deux conditions concernant le lien source-relais présentées ci-dessus peuvent être interprétées comme suit. Dans le premier cas, $S_{31} \leq S_{11}/(1+S_{12})$ implique que, en traitant l'interférence de la source 2 comme bruit, la destination 1 a une observation du signal de la source 1 encore meilleure que celle du relais. Par conséquent, l'observation du relais n'aide pas beaucoup la destination 1 à décoder son propre signal.

D'autre part, $S_{31} \leq S_{21}/(1+S_{22})$ implique que, en traitant son propre signal comme bruit, la destination 2 a une observation du signal de la source 1 encore meilleure que celle du relais. Par conséquent, l'observation du relais n'aide pas beaucoup la destination 2 à apprendre/décoder l'interférence de la source 1.

3 LE CANAL AVEC ESPION ET RÉTROACTION GÉNÉRALISÉE

Dans cette partie de la thèse, nous étudions le problème dans lequel un nœud nommé Alice souhaite communiquer secrètement un message à un autre nœud nommé Bob, en présence d'un espion passif nommé Eve. Alice peut communiquer avec Bob en utilisant un canal général sans mémoire, mais Eve écoute cette communication par un autre canal sans mémoire dont les propriétés statistiques peuvent être différentes ou égales au canal de Bob. En outre, nous supposons qu'Alice observe un signal de rétroaction générale qui est corrélé aux sorties de canal de Bob et d'Eve, nommé « rétroaction généralisée ». Il est à noter que ce modèle de rétroaction est assez riche car il permet d'analyser différents types d'informations supplémentaires vieillies à l'émetteur (par exemple les modèles avec rétroaction différée d'état du canal ou rétroaction bruyante des sorties du canal). Il fournit ainsi le cadre approprié pour étudier l'impact du modèle de rétroaction.

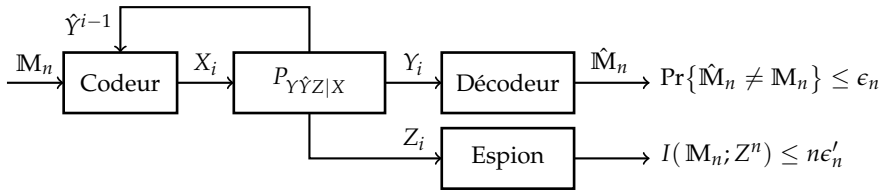


FIGURE 5. : Le canal avec espion et rétroaction généralisée.

3.1 *Définition du Problème*

Nous considérons le WCGF, où une source souhaite transmettre un message $\mathbb{M}_n \in \mathcal{M}_n$ en toute sécurité à une destination à l'aide d'un signal de rétroaction lorsqu'un espion est présent dans le canal. Le WCGF, représenté dans la fig. 5, est modélisé comme un canal sans mémoire défini par une distribution de probabilité conditionnelle

$$p(y\hat{y}z|x) : \mathcal{X} \longmapsto \mathcal{Y} \times \hat{\mathcal{Y}} \times \mathcal{Z}, \tag{16}$$

où $x \in \mathcal{X}$ est l'entrée de canal, $\hat{y} \in \hat{\mathcal{Y}}$ est le signal de rétroaction, et $y \in \mathcal{Y}$ et $z \in \mathcal{Z}$ sont les sorties de canal du récepteur légitime et de l'espion, respectivement.

Definition 0.3. *Un* débit secret *R est atteignable pour ce modèle si pour tout $(\epsilon_n, \epsilon'_n) > 0$ il existe un bloc de longueur n, $\|\mathcal{M}_n\| \geq 2^{n(R-\epsilon_n)}$, fonctions de codage stochastiques $enc_i : (\mathcal{M}_n, \hat{\mathcal{Y}}^{i-1}) \mapsto \mathcal{X}_i$, et une fonction de décodage $dec : \mathcal{Y}^n \mapsto \mathcal{M}_n$, de sorte que*

$$\frac{1}{\|\mathcal{M}_n\|} \sum_{m \in \mathcal{M}_n} \Pr\Big\{ dec(Y^n) \neq m \,|\, X^n = \{enc_i(m, \hat{Y}^{i-1})\}_{i=1}^n \Big\} \leq \epsilon_n,$$

$$\text{et } I(\mathbb{M}_n; Z^n) \leq n\epsilon'_n,$$

où ϵ_n et ϵ'_n sont des séquences tel que $(\epsilon_n, \epsilon'_n) \to 0$ quand $n \to \infty$.

La capacité secrète C_{sf} *du WCGF est la borne supérieure de tous les débits secrets atteignables.*

Nous allons également examiner la situation où la source ne veut pas transmettre un message, mais plutôt s'accorder avec le décodeur légitime sur une clé secrète tout en la cachant de l'espion. Les sorties de canal, c'est-à-dire y, $\hat{y}$, et z peuvent être considérées comme des sources corrélées. Ce scénario est appelé « modèle de canal » pour l'accord de clé, mais dans notre cas, la communication a également lieu dans le même canal, plutôt que dans un canal de diffusion public et sans bruit séparé.

Compte tenu de la nature strictement causale du lien de rétroaction, pour chaque intervalle de temps i, l'encodeur utilise ses observations passées pour générer un symbole $\varphi_i(\hat{Y}^{i-1})$ qui envoie par le canal. Après n intervalles de temps, l'encodeur et le décodeur légitime génèrent une clé secrète, c'est-à-dire $K_n = \psi_a(\hat{Y}^n)$ et $\hat{K}_n = \psi_b(Y^n)$, où $K_n, \hat{K}_n \in \mathcal{K}_n$.

Definition 0.4. *Une* clé secrète*, dont son débit est R_k, est atteignable pour ce modèle si pour tout $(\epsilon_n, \epsilon'_n) > 0$ il existe un bloc de longueur n, $\|\mathcal{K}_n\| \geq 2^{n(R_k - \epsilon_n)}$, fonctions $\psi_a(\cdot)$ et $\psi_b(\cdot)$ de sorte que les étapes précédentes peuvent être satisfaites et*

$$\begin{aligned} &\Pr\{K_n \neq \hat{K}_n\} \leq \epsilon_n, \\ &\text{et } I(K_n; Z^n) \leq n\epsilon'_n, \end{aligned}$$

où ϵ_n et ϵ'_n sont des séquences tel que $(\epsilon_n, \epsilon'_n) \to 0$ quand $n \to \infty$.

La capacité de clé secrète *du WCGF est la borne supérieure de tous les débits de clé secrète atteignables.*

3.2 *Résumé des Principaux Résultats*

Nous présentons ici les principaux résultats de la deuxième partie de la thèse. Les preuves de ces résultats sont présentées en annexe.

Borne Inférieure du Débit Secret Basée sur Codage Source-Canal Conjoint

Nous présentons d'abord un schéma de codage basé sur une stratégie de codage source-canal conjoint[12] (JSCC) où les séquences envoyées transmettent à la fois des informations numériques et analogiques.

Theorem 0.4 (schéma JSCC)**.** *Une borne inférieure de la capacité secrète du canal avec espion et rétroaction généralisée est donnée par tous les débits non négatifs qui satisfont*

$$\begin{aligned} R \leq \max_{p \in \mathcal{P}_1} \sup_{b \geq 1} \frac{1}{b} \Bigg[& I(U_1; Y^b) - I(U_1; Z^b) + \sum_{j=2}^{b} \min \Big\{ I(U_j; Y_j^b | U^{j-1} Y^{j-1}) \\ & - I(U_j; X^{j-1} \hat{Y}^{j-1} | U^{j-1} Y^{j-1}),\ I(U_j; Y^b | U^{j-1}) - I(U_j; Z^b | U^{j-1}) \Big\} \Bigg], \end{aligned} \tag{17}$$

où l'ensemble de toutes les distributions de probabilité jointes $\mathcal{P}_1$ est

$$\mathcal{P}_1 = \left\{ p(u^b x^b y^b \hat{y}^b z^b) = \prod_{j=1}^{b} p(u_j x_j | u^{j-1} x^{j-1} \hat{y}^{j-1}) p(y_j \hat{y}_j z_j | x_j) \right\}. \tag{18}$$

Démonstration. La transmission est divisée en b blocs et, dans chaque bloc, la séquence $u^n_{[j]}$ envoyée porte à la fois des informations numériques et analogiques, celle-ci par la corrélation avec les séquences des derniers blocs. La preuve complète est reléguée à l'annexe 5.A. □

12 Joint source-channel coding.

Corollary 0.2. *Une borne inférieure de la capacité secrète du canal avec espion et rétroaction généralisée est donnée par tous les débits non négatifs qui satisfont*

$$R \leq \max_{p \in \mathcal{P}_2} \left[I(UV;Y) - \max\{I(V;X\hat{Y}|U), I(UV;Z)\} \right], \tag{19}$$

où l'ensemble de toutes les distributions de probabilité jointes $\mathcal{P}_2$ est

$$\mathcal{P}_2 = \left\{ p(uvxy\hat{y}z) = p(ux)p(y\hat{y}z|x)p(v|ux\hat{y}) \right\}.$$

Démonstration. Voire l'annexe 5.B. □

Remark 0.4. *Si on fixe $V = \emptyset$, on récupère le débit secret atteignable du canal avec espion et sans rétroaction.*

Borne Inférieure du Débit Secret Basée sur Génération de Clé

Nous introduisons maintenant un schéma de codage qui emploie le lien de rétroaction pour générer simultanément avec la transmission une clé secrète partagée entre les utilisateurs légitimes. La clé est utilisée plus tard pour chiffrer le message à envoyer au niveau du bit.

Soit $\mathcal{P}_3$ l'ensemble de toutes les distributions de probabilité jointes

$$\mathcal{P}_3 = \{ p(quxvty\hat{y}z) = p(qu)p(x|u)p(y\hat{y}z|x)p(t|v)p(v|ux\hat{y}) \}, \tag{20}$$

et soit $\mathcal{P}_4$ le sous-ensemble de $\mathcal{P}_3$ tel que $Q = \emptyset$.

Pour toute distribution de probabilité spécifique $p \in \mathcal{P}_3$, soit R_{KG_1} l'ensemble de tous les débits non négatifs qui satisfont

$$\begin{aligned} R_{KG_1} &\leq I(U;Y) - I(U;Z|Q) - \max\{I(Q;Y),\, I(V;X\hat{Y}|UY)\} \\ &\quad + I(V;Y|UT) - I(V;Z|UT) - I(U;T|QZ), && \text{(21a)} \\ R_{KG_1} &\leq I(U;Y) - \max\{I(Q;Y),\, I(V;X\hat{Y}|UY)\}, && \text{(21b)} \end{aligned}$$

alors que, pour toute $p' \in \mathcal{P}_4$, soit R_{KG_2} l'ensemble de tous les débits non négatifs qui satisfont

$$\begin{aligned} R_{KG_2} &\leq I(V;Y|UT) - I(V;Z|UT) && \text{(22a)} \\ R_{KG_2} &\leq I(U;Y) - I(V;X\hat{Y}|UY). && \text{(22b)} \end{aligned}$$

Theorem 0.5 (schéma KG). *Une borne inférieure de la capacité secrète du canal avec espion et rétroaction généralisée est donnée par tous les débits non négatifs qui satisfont*

$$R \leq \max \left\{ \max_{p \in \mathcal{P}_3} R_{KG_1},\ \max_{p' \in \mathcal{P}_4} R_{KG_2} \right\}.$$

Démonstration. Dans ce schéma, la transmission est divisé en plusieurs blocs et le message transmis dans chaque bloc est chiffré complètement (R_{KG_2}) ou partiellement (R_{KG_1}). La séquence v^n sert à transmettre une description du signal de rétroaction $\hat{y}^n$ du bloc précédent, et par conséquent, elle permet que les utilisateurs légitimes *génèrent* une clé secrète lors de la transmission. Voir l'annexe 5.C pour plus de détails. □

Remark 0.5. *Si on fixe $Q = T = V = \emptyset$, on récupère le débit secret atteignable du canal avec espion et sans rétroaction.*

Borne Inférieure du Débit de Clé Secrète

Le schéma du théorème 0.5, en l'absence d'un message, peut être utilisé par les utilisateurs légitimes pour convenir d'une clé secrète. Cette clé pourrait ensuite être utilisée pour chiffrer la transmission dans une couche supérieure.

Corollary 0.3. *Une borne inférieure de la capacité de clé secrète du canal avec espion et rétroaction généralisée est donnée par tous les débits non négatifs qui satisfont*

$$R_k \leq \max_{p \in \mathcal{P}_4} \left[I(V;Y|UT) - I(V;Z|UT) \right], \tag{23}$$

sujet à

$$I(V; X\hat{Y}|UY) \leq I(U;Y). \tag{24}$$

Démonstration. Ce corollaire est un cas particulier de la stratégie R_{KG_2}, où il n'y a aucun message à transmettre, c'est-à-dire $R = 0$, et on est seulement intéressé à générer une clé secrète, c'est-à-dire $R_k \leq \bar{S}_2$.

La séquence U^n porte seulement les indices utilisés par la destination pour reconstruire les séquences T^n et V^n. L'inégalité (24) correspond au coût de transmission de ces indices. De plus, le but de la séquence T^n est d'extraire la majeure partie de l'aléatoirité commune entre Z^n and $(Y^n\hat{Y}^n)$, et elle est supposée d'être obtenue par l'espion. La clé secrète est donc l'incertitude qui subsiste dans V^n que l'espion ne peut pas supprimer avec sa propre observation Z^n.

Voir l'annexe 5.C.7 pour plus de détails, spécialement les limites (247). □

3.3 *Exemples d'Application à Quelques Canaux et Modèles de Rétroaction*

Dans cette section, nous montrons comment les schémas JSCC et KG contiennent plusieurs autres stratégies comme des cas particuliers avec le choix approprié de sa distribution de probabilité jointe.

Capacité de Clé Secrète du Canal avec Espion

Nous analysons d'abord la situation où deux terminaux reliés par un canal sans bruit à débit limité, et qui ont accès à des sources i.i.d. corrélées, veulent générer une clé partagée. Cette clé doit être cachée d'un espion qui est également relié au canal public sans bruit et a accès à une source corrélée.

Le modèle de canal (16) englobe cette situation. Prenons l'ensemble des variables suivantes :

$$\hat{Y} = \hat{Y}_s \tag{25}$$
$$Y = (Y_s X) \tag{26}$$
$$Z = (Z_s X), \tag{27}$$

où $H(X) = R$, c'est-à-dire le récepteur légitime et l'espion ont accès au canal sans bruit à débit limité. En outre, les sources corrélées à la disposition des nœuds $(\hat{Y}_S Y_s Z_s)$ sont indépendantes de l'entrée du canal X, c'est-à-dire $p(x y_s \hat{y}_s z_s) = p(x)p(y_s \hat{y}_s z_s)$.

Theorem 0.6 ([8, Thm. 2.6]). *Dans ce scénario, la* capacité de clé secrète *du canal avec espion et un canal public sans bruit de débit R est donnée par*

$$\mathrm{C}_{wsk} = \max_{p(y_s \hat{y}_s z_s) p(v|\hat{y}_s) p(t|v)} [I(V;Y_s|T) - I(V;Z_s|T)], \tag{28}$$

sujet à

$$I(V;\hat{Y}_s) - I(V;Y_s) < R, \tag{29}$$

et elle est atteignable par le schéma du corollaire 0.3.

Démonstration. Étant donné que les utilisateurs finaux ont accès à X, l'ensemble des auxiliaires à la suite est optimal

$$Q = \emptyset \tag{30}$$
$$U = X, \tag{31}$$

et (VT) indépendant de X, car elle ne modifie pas les sources corrélées. La distribution de probabilité jointe est $p(x)p(y_s \hat{y}_s z_s)p(v|\hat{y}_s)p(t|v)$, et donc (23) et (24) deviennent (28) et (29).

La borne supérieure peut être trouvée dans [8]. □

Canal avec Espion et Rétroaction Parfaite de Sortie

Dans [9], les auteurs analysent un canal avec espion et rétroaction parfaite de sortie à l'encodeur, c'est-à-dire $\hat{Y} = Y$, et complètement inaccessible par l'espion.

Theorem 0.7 ([9, Thm. 1]). *Dans ce modèle, le schéma KG du théorème 0.5 permet d'atteindre tous les débits qui satisfont*

$$R \leq \max_{p(ux)p(yz|x)} \min\left\{|I(U;Y) - I(U;Z)|^+ + H(Y|UZ),\, I(U;Y)\right\}. \tag{32}$$

Démonstration. Avec le choix suivant de variables aléatoires

$$V = Y \tag{33}$$

$$T = Q = \emptyset, \tag{34}$$

le débit R_{KG_1} (21) devient

$$R_{KG_1} \leq \min\{I(U;Y) - I(U;Z) + H(Y|UZ),\, I(U;Y)\}, \tag{35}$$

tandis que le débit R_{KG_2} (22) devient

$$R_{KG_2} \leq \min\{H(Y|UZ),\, I(U;Y)\}. \tag{36}$$

Par conséquent, l'union des deux régions peut être succinctement écrit comme (32). □

Remark 0.6. *Les résultats de capacité secrète pour le canal avec espion et rétroaction parfaite de sortie* dégradé *et* inversement dégradé *[9, Cor. 1 and 2] sont également valables ici.*

Remark 0.7. *Si on fixe $V = Y$ dans l'expression de débit secret du corollaire 0.2, qui étant donné la rétroaction parfaite de sortie semble être le meilleur choix de V, on obtient*

$$R \leq \max_{p(ux)p(yz|x)} \min\left\{I(U;Y) - I(U;Z) + H(Y|UZ),\, I(U;Y)\right\}, \tag{37}$$

qui est strictement inférieure à (32) si $I(U;Y) < I(U;Z)$.

Canal Gaussien avec Espion et Rétroaction Parfaite de Sortie

Dans [10], les auteurs analysent le canal gaussien avec espion et rétroaction parfaite de sortie au codeur, c'est-à-dire $\hat{Y} = Y$, et rétroaction bruyante à l'espion. Ce modèle peut être succinctement décrite comme

$$Y_j = X_j + N_j \tag{38}$$

$$Z_j = \begin{bmatrix} \bar{Z}_j \\ \bar{Y}_j \end{bmatrix} = \begin{bmatrix} X_j + M_j \\ Y_j + S_j \end{bmatrix}, \tag{39}$$

où Y_j, $\bar{Z}_j$, et $\bar{Y}_j$ sont les sorties de canal du récepteur légitime et celle de l'espion, et la rétroaction bruyante à l'instant de temps j, respectivement. Le signal du codeur X_j a une contrainte de puissance moyenne P, et N_j, M_j, et S_j sont des termes de bruit blanc gaussien additif arbitrairement corrélés de moyennes nulles et de variances σ_N^2, σ_M^2, et σ_S^2, respectivement.

Theorem 0.8 ([10, Thm. 5.1]). *La capacité secrète de ce modèle est donnée par*

$$\mathrm{C}_{sf} = \frac{1}{2}\log\left(1+\frac{P}{\sigma_N^2}\right), \tag{40}$$

à condition que l'espion a accès seulement à la rétroaction bruyante $\bar{Y}$, et elle est atteinte par le schéma JSCC.

Démonstration. On fixe la distribution de probabilité jointe suivante dans le schéma JSCC

$$U_j = \begin{cases} \alpha_1\theta & \text{si } j=1 \\ \varnothing & \text{si } j\in[2:b] \end{cases} \tag{41}$$

$$X_j = \begin{cases} U_1 & \text{si } j=1 \\ f_j(X_{j-1},Y_{j-1}) & \text{si } j\in[2:b] \end{cases} \tag{42}$$

où $\alpha_1=\alpha\triangleq\sqrt{1+P/\sigma_N^2}$ et $\theta\sim\mathcal{U}[-0.5,0.5]$ est une variable aléatoire continue. Les fonctions $f_j(\cdot)$ en (42) sont définies comme

$$X_j = \begin{cases} h_2\alpha_1\left(Y_1-X_1\right) & \text{si } j=2 \\ \dfrac{h_j}{h_{j-1}}\left[X_{j-1}+\alpha_{j-1}h_{j-1}\left(Y_{j-1}-X_{j-1}\right)\right] & \text{si } j\in[3:b], \end{cases} \tag{43}$$

où $\alpha_j\triangleq\sqrt{P/\sigma_N^2}\,\alpha^{j-1}$ et $h_j\triangleq-\alpha_j/\sum_{l=1}^{j-1}\alpha_l^2$ sont des paramètres similaires à ceux du schéma Schalkwijk-Kailath (SK), de telle sorte que $X_j=h_j\sum_{l=1}^{j-1}\alpha_l N_l$. Par conséquent, pour chaque $j\in[2:b]$, X_j est indépendant du message initial X_1 et il est une fonction déterministe de X_{j-1} et Y_{j-1}. Nous renvoyons le lecteur à [10] pour plus de détails.

Le débit atteignable (212) peut donc être écrit comme

$$bR < I(U_1;Y^b) - I(U_1;\bar{Z}^b\bar{Y}^b), \tag{44}$$

et nous analysons chaque terme dans la suite.

Le premier terme,

$$\begin{aligned}
I(U_1;Y^b) &= I(X_1;Y^b) && \text{(45a)}\\
&= I(X_1Y_1;Y_2^b) + h(Y_1|Y_2^b) - h(Y_1|X_1) && \text{(45b)}\\
&\geq \sum_{l=2}^{b} I(X_1Y_1;Y_l|Y_2^{l-1}) + h(X_1+N_1|Y_2^bN_1) - h(X_1+N_1|X_1) && \text{(45c)}\\
&= \sum_{l=2}^{b}\left[h(Y_l|Y_2^{l-1}) - h(Y_l|X_1Y^{l-1})\right] + h(X_1) - h(N_1) && \text{(45d)}\\
&= \sum_{l=2}^{b}\left[h(Y_l) - h(Y_l|X^lY^{l-1})\right] + \log|\alpha_1| - h(N_1) && \text{(45e)}\\
&= \sum_{l=2}^{b}\left[h(X_l+N_l) - h(N_l)\right] + \log|\alpha_1| - h(N_1) && \text{(45f)}\\
&= (b-1)\frac{1}{2}\log\left(1+\frac{P}{\sigma_N^2}\right) + \log|\alpha_1| - h(N_1). && \text{(45g)}
\end{aligned}$$

où l'inégalité (45c) est due au conditionnement supplémentaire dans l'entropie différentielle ; où dans (45d) on note que N_1 et X_2^b (en conséquence Y_2^b) sont indépendants de X_1 ; où dans (45e) on utilise certaines propriétés de ce schéma, à savoir, Y_l est indépendant de Y_2^{l-1} et X_l est une fonction déterministe de $(X_{l-1}Y_{l-1})$, et que $h(X_1) = \log|\alpha_1|$; et où dans (45g) on note que, pour $l \in [2 : b]$, $X_l \sim \mathcal{N}(0, P)$ et il est indépendant de N_l.

On trouve une borne supérieure pour le deuxième terme de la même façon que [10],

$$
\begin{aligned}
I(U_1; \bar{Z}^b \bar{Y}^b) &= I(\theta; \bar{Z}^b \bar{Y}^b) && \text{(46a)}\\
&\leq I(\theta; \bar{Z}^b \bar{Y}^b N^b) && \text{(46b)}\\
&= h(\theta) - h(\theta | \bar{Z}^b \bar{Y}^b N^b) && \text{(46c)}\\
&= h(\theta) - h(\theta | \alpha_1\theta + M_1, \alpha_1\theta + S_1, S_2^b, M_2^b, N^b) && \text{(46d)}\\
&= h(\theta) - h(\theta | \alpha_1\theta + M_1, \alpha_1\theta + S_1, N_1) && \text{(46e)}\\
&= I(\theta; \alpha_1\theta + M_1, \alpha_1\theta + S_1, N_1) && \text{(46f)}\\
&= I(\theta; \boldsymbol{A}\theta + \boldsymbol{B}) && \text{(46g)}\\
&\leq \frac{1}{2} \log\det\left(\boldsymbol{I} + \frac{1}{12} \boldsymbol{A}\boldsymbol{A}^T \mathbb{E}[\boldsymbol{B}\boldsymbol{B}^T]^{-1} \right), && \text{(46h)}
\end{aligned}
$$

où dans (46d) on utilise la séquence N^b pour construire X_2^b et le soustraire de $(\bar{Z}^b \bar{Y}^b)$; où (46e) suit car $(S_2^b M_2^b N_2^b)$ est indépendant de $(\theta S_1 M_1 N_1)$ en raison de la propriété sans mémoire du canal ; où dans (46g) on définit $\boldsymbol{A} \triangleq [0, \alpha_1, \alpha_1]^T$ et $\boldsymbol{B} \triangleq [N_1, M_1, S_1]^T$; et où (46h) découle du fait que l'information mutuelle est maximisée pour une distribution gaussienne avec la même variance que θ, qui est une variable uniforme.

L'expression (46h) a une valeur finie tant que

$$
\rho_{NM}^2 + \rho_{NS}^2 + \rho_{MS}^2 - 2\rho_{NM}\rho_{NS}\rho_{MS} - 1 \neq 0, \tag{47}
$$

où ρ_{NM}, ρ_{NS}, ρ_{MS} sont les coefficients de corrélation entre les bruits correspondants. Si cette condition est remplie, ce qui suit est un débit atteignable pour ce choix particulier de variables

$$
R \leq \left(\frac{b-1}{b} \right) \frac{1}{2} \log\left(1 + \frac{P}{\sigma_N^2} \right) + \frac{1}{b} \left[\log|\alpha_1| - h(N_1) - I(\theta; \boldsymbol{A}\theta + \boldsymbol{B}) \right], \tag{48}
$$

ce qui tend vers (40) quand $b \to \infty$. □

4 OBSERVATIONS GÉNÉRALES & CONCLUSIONS

Dans cette thèse, nous avons examiné deux aspects pertinents des futurs réseaux sans fil, à savoir la réduction d'interférence grâce à la coopération entre utilisateurs, et la transmission sécurisée grâce à la sécurité de la couche physique. À cette fin, nous avons mené une

étude de deux modèles de base, l'IRC et le WCGF, dans le cadre de la théorie de l'information.

Le Canal à Relais et Interférence

Dans la première partie de la thèse, nous avons étudié une classe d'IRCs où le relais n'observe qu'une des deux sources, et dans laquelle les sorties de canal sont des fonctions semi-déterministes et injectives des entrées de canal. Pour ce modèle particulier, nous avons proposé une borne supérieure de la capacité qui est une extension non triviale de celle de Telatar et Tse pour le canal à interférence. La contribution la plus pertinente ici est la modélisation des signaux d'interférence, étape clé en vue d'obtenir une borne supérieure à lettre simple[13]. De plus, nous avons introduit deux bornes inférieures qui combinent les stratégies de relayage DF (partiel) et CF avec le schéma de Han-Kobayashi pour le canal à interférence. Bien que cette approche ait déjà été étudiée, les stratégies présentées ici sont nouvelles notamment par l'introduction de DF *partiel* et l'utilisation de différentes stratégies de décodage dans CF. De ce fait la contribution principale ici est le développement de bornes inférieures qui ressemblent à la borne supérieure. Ces bornes nous ont permis de caractériser dans un écart constant, la région de capacité de la classe gaussienne d'IRCs étudiée. En outre, nous avons déterminé un régime de SNR dans le lien source-relais qui donne une augmentation limitée des débits atteignables indépendamment de tout autre paramètre de canal. Ce dernier résultat est d'une importance primordiale lorsque vient le temps de planifier l'infrastructure des réseaux cellulaires de prochaine génération.

Nous devons également rendre compte de certaines faiblesses de notre analyse dans cette première partie de la thèse. La proposition initiale était d'étendre le travail de Telatar et Tse à l'IRC afin de caractériser sa région de capacité dans un écart constant. Dans un cadre général où le relais observe les deux sources, cette tâche s'est avérée extrêmement ardue. La présence de l'entrée du relais corrèle les signaux d'interférence présents dans le modèle injectif et semi-déterministe, ce qui n'est pas le cas dans le canal à interférence. La borne extérieure résultante dans ce scénario général était difficile à appréhender, ce qui a limité la compréhension du problème. L'élimination du lien entre l'une des sources et le relais qui est une solution trouvée dans la littérature, nous a permis de simplifier considérablement la borne extérieure et de la comparer plus tard aux bornes inférieures. Néanmoins, même si le modèle est maintenant plus simple, la borne extérieure est toujours composée de 20 limites différentes alors que la borne extérieure de Telatar et Tse en a seulement 7. En effet, ce point

13 Single-letter.

montre qu'il est complexe de traiter simultanément avec le relayage et l'interférence, deux problèmes encore ouverts.

Le Canal avec Espion et Rétroaction Généralisée

La deuxième partie de la thèse s'est concentrée sur la compréhension de l'avantage et la manière d'employer la rétroaction dans la sécurité de la couche physique à travers l'analyse du WCGF. À cette fin, nous avons dérivé deux bornes inférieures en utilisant les deux méthodes différentes trouvées dans la littérature. La première de ces méthodes qui ne pas la plus populaire, utilise le signal de rétroaction pour créer des séquences qui « s'alignent » dans le canal d'une manière qui est préjudiciable au décodage de l'espion. Notre première borne inférieure a été basée sur cette méthode et l'utilisation de codage source-canal conjoint. D'autre part, la deuxième méthode utilise le signal de rétroaction en tant que source d'aléatoirité commune entre les utilisateurs légitimes, avec laquelle ils se mettent d'accord sur une clé secrète. Sur la base de cette méthode, nous avons développé une seconde borne inférieure et, comme un résultat supplémentaire, nous avons obtenu une borne inférieure sur l'accord de clé secrète pour le même modèle de canal. Les deux bornes inférieures récupèrent avec succès des résultats précédents trouvés dans la littérature pour des modèles spécifiques de canal et de rétroaction. Cependant, aucune d'elles ne semble être plus générale que l'autre parce que chaque stratégie a échoué à récupérer tous les résultats pris en considération. Basés sur ces résultats, nous pensons que les deux méthodes sont complémentaires et une borne inférieure unifiée serait plus générale. Néanmoins, nous ne pouvons pas prouver cette conjecture sans réellement dériver le schéma unifié.

À nouveau, les choix faits dans notre travail de la deuxième partie de la thèse ont fait apparaître quelques faiblesses dont les deux suivantes. Tout d'abord, la complexité de l'expression multi-lettre[14] du schéma JSCC rend difficile toute analyse. En effet, la distribution de probabilité jointe optimale n'a pu être trouvée que dans deux exemples en raison de similitudes entre les stratégies. Nous avons eu recours ainsi à une version simplifiée du schéma JSCC, c'est-à-dire le corollaire 0.2, ce qui nous a aidé à gagner une certaine perspective sur le problème, mais sans aboutir un résultat de capacité. La proposition du schéma KG a été une conséquence de ce problème. Concernant la deuxième faiblesse, les bornes inférieures proposées ont été calculées pour remplir la condition de *faible sécurité*, c'est-à-dire $I(\mathbb{M}_n; Z^n) \leq n\epsilon_n$, plutôt que la condition de *forte sécurité*, c'est-à-dire $I(\mathbb{M}_n; Z^n) \leq \epsilon_n$. Par conséquent, l'un des résultats précédents dans la littérature, élaboré avec la condition de forte sécurité, n'est pas

14 Multi-letter.

réellement compris comme un cas particulier de nos stratégies. Une autre démonstration, par exemple sur la base de la résolvabilité du canal[15] [11], doit être effectuée afin d'inclure correctement le résultat ci-dessus.

15 Channel resolvability.

1

INTRODUCTION

In this chapter, we first state the motivation behind our work and we then briefly introduce the two channel models studied. For each of these models, we summarize the most relevant known results in the literature and we finally present our contribution.

1.1 MOTIVATION

Over the past decades, technological advances have made possible the availability of cheap and powerful mobile devices everywhere. These small multipurpose gadgets have become an important part of our everyday life, with new applications appearing periodically. From voice-only phone calls to high quality video streaming, the demand for data has increased substantially over time. Indeed, cellular networks have seen an unstoppable increase in both number of users and data traffic. The existence of a large amount of users in cellular networks has driven communication channels from being noise-limited to *interference-limited*. However, by leveraging the broadcast nature of the wireless medium, nodes in the network can *cooperate* between themselves to boost the overall network throughput.

The open nature of the wireless medium, on the other hand, makes it susceptible to numerous security threats. Malicious users might actively disrupt transmissions by injecting an interference signal, or they might passively acquire the transmitted signals in order to obtain private information. In this second scenario, due to the undetected actions of the eavesdropper, none of the legitimate users in the transmission may be even aware of its presence. These plausible *security* vulnerabilities represent a drawback of the wireless medium. However, with the use of physical layer security[1] and by providing additional information present in the channel to the transmitter, e.g., channel state information or a *feedback* signal, the security of the system can be enhanced.

In this thesis, we conduct an information-theoretic study on these two aspects of wireless communications: how to improve the data

1 By physical layer security, we mean any strategy applied at the physical layer which ensures *safe* transmission of information in the presence of an eavesdropper, without resorting to enciphering at higher layers of the communication protocol stack.

throughput in interference-limited networks by means of cooperation between users and how to strengthen the security of transmissions with the help of feedback. We try to provide insight into these two problems by determining the performance limits of these systems. In particular, we focus on the interference relay channel (IRC) for the first part of the thesis and on the wiretap channel with generalized feedback (WCGF) for the second part.

Even though these two problems might seem completely different, they have some similarities, specifically, in the encoding process. Due to the causal behavior of the channel, both the relay in the IRC and the transmitter in the WCGF have only access to past channel observations. In other words, in time slot $i \in [1 : n]$, the relaying function in the IRC is defined as $\phi_i : \mathcal{Y}_3^{i-1} \mapsto \mathcal{X}_3$, where $\mathcal{X}_3$ and $\mathcal{Y}_3$ correspond to the input and output at the relay, while the encoder function in the WCGF is defined as $\text{enc}_i : (\mathcal{M}_n, \hat{\mathcal{Y}}^{i-1}) \mapsto \mathcal{X}$, where $\mathcal{X}$ corresponds to the input of the channel, $\hat{\mathcal{Y}}$, the feedback signal, and $\mathcal{M}_n$, the message the encoder wants to transmit. For this reason, we can find similar coding ideas in problems with relaying and feedback.

The interference relay channel is the simplest channel model where interference and relaying appear together. Two pairs of transmitter-receiver nodes want to communicate independently but, in doing so, they interfere between each other. A fifth node, the relay, participates in the transmission in order to mitigate the interference and hence improve the performance of the network. This model encapsulates the issue and a possible solution for cellular network performance close to the cell border. Two adjacent base stations (BSs) have comparable signal strength near their cell border, and users in one cell experience a significant interference coming from the BS in the neighboring cell. The inclusion of a fixed relay, an infrastructure equipment that is not connected to the wired backhaul, may aid in the signal transmission between the BSs and the mobile users by receiving and retransmitting messages. Moreover, these infrastructure relays may be cheaper to deploy and maintain, and may consume less power than traditional BSs.

Infrastructure relays potentially offer a cheap and canny way to deal with interference without sacrificing resources. The common approach to cope with interference in present day's wireless networks is either to avoid it, by orthogonalizing users' transmissions in time, frequency, or space, or to treat it as noise. However, these techniques may be detrimental for the performance of the global system due to imperfect orthogonalization in practice or strong interference scenarios. To avoid interference through inter-cell coordination is a main topic of study [2] because it provides solutions in the short term. Nonetheless, in order to harness the full potential of the wireless medium, a change of paradigm is needed for future generation's cellular networks. In the IRC, it is assumed that all the nodes employ the same frequency

and there is no orthogonalization of signals. Moreover, the relay operates in *full-duplex* mode, i.e., it can receive and transmit simultaneously over the same time-frequency-space resource. This assumption may not be realistic nowadays, but a practical implementation of full-duplex devices will be in the near future.

The wiretap channel with generalized feedback models the problem where a transmitter wishes to secretly communicate a message to a receiver in presence of a passive eavesdropper with the help of a feedback signal. This signal is correlated to the channel outputs of the receiver and the eavesdropper, and it is called "generalized feedback" to differentiate it from specific types of feedback, e.g., "perfect output feedback" or "state feedback". Feedback may be present at the encoder by different means. End users may send back to the transmitter through a dedicated feedback link their channels' observations, a description of them, or some parameter related to them, e.g., fading coefficient. Additionally, the transmitter itself may be able to perform measurements over the channel, thus it may gather information correlated to that of the end users. Generalized feedback sums up all these different possibilities.

The adoption of physical layer security to protect communications against eavesdroppers by harnessing the randomness present in the physical medium [3] has gather great attention lately. Application to secure wireless networks is extremely attractive, not only because the open nature of the medium makes communication devices particularly sensitive to eavesdropping, but also because randomness is abundantly available in such scenarios. Furthermore, the current theory of physical layer security indicates that securing part of the data can be provided at minimal –or even no– cost in the total throughput. *Security is for free.* A crucial observation behind this promising result is that, in order to guarantee secrecy, the legitimate receiver must experience a better channel than the eavesdropper, which is often a nonrealistic assumption in wireless scenarios. Moreover, the legitimate users may be even unaware of the channel conditions present at the eavesdropper. All these difficulties make the implementation of this type of security almost impractical. The use of feedback in the encoding process, however, may be a means to overcome these issues by artificially creating a better effective channel to the legitimate destination with respect to the eavesdropper.

How the feedback should be used is an interesting problem that needs to be addressed. In the context of security, there are two different approaches to harness the potential of the feedback signal: an analog and a digital approach. The digital one extracts randoms bits from the common information the legitimate users have and uses these bits to encrypt the message to be sent. On the other hand, the analog approach tries to hide the codewords sent in the null space of the eavesdropper's observations so as to prevent a correct decoding.

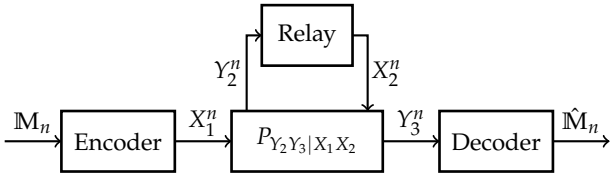


Figure 6.: Relay channel.

How these two approaches relate and which one is better, if there is one, are some of the questions we would like to answer.

1.2 INTERFERENCE RELAY CHANNEL

The IRC combines two channel models: the relay channel (RC) and the interference channel (IC), which we introduce in the sequel.

1.2.1 *Relay Channel*

The RC was first introduced by van der Meulen [12], but it was the seminal work of Cover and El Gamal [13] which presented the main cooperative strategies of (partial) decode-and-forward (DF) and compress-and-forward (CF), as well as the cutset bound.

The RC consists of one source, one destination, and one relay node. The source wishes to transmit a message $\mathbb{M}_n \in \mathcal{M}_n \triangleq \{1, \ldots, M_n\}$ to the destination with the help of the relay. The RC, depicted in Fig. 6, is modeled as a memoryless channel defined by a conditional probability distribution (PD):

$$p(y_2 y_3 | x_1 x_2) : \mathcal{X}_1 \times \mathcal{X}_2 \longmapsto \mathcal{Y}_2 \times \mathcal{Y}_3$$

where $x_1 \in \mathcal{X}_1$ and $y_3 \in \mathcal{Y}_3$ are the input at the source and output at the destination, respectively, whereas $x_2 \in \mathcal{X}_2$ and $y_2 \in \mathcal{Y}_2$ are the input and output at the relay, respectively. The relaying functions are defined as a sequence of mappings $\{\phi_i : \mathcal{Y}_2^{i-1} \mapsto \mathcal{X}_2\}_{i=1}^n$.

Outer Bound

Theorem 1.1 (cutset bound)**.** *An outer bound on the capacity of the RC is defined by all the nonnegative rates R satisfying*

$$C \leq \max_{p(x_1 x_2)} \min \left\{ I(X_1 X_2; Y_3),\, I(X_1; Y_2 Y_3 | X_2) \right\}. \tag{49}$$

The terms in the minimum can be seen as cooperative transmission or reception, i.e., for a message to be reliably decoded at the destination, its rate cannot be higher than if both sources or both destinations fully cooperate. This bound is not tight in general.

Decode-and-Forward Inner Bound

In DF, the relay decodes the message and coherently cooperates with the transmitter to send it to the receiver. The receiver then decodes simultaneously the messages sent by the sender and the relay. This scheme employs the techniques of block Markov coding and backward decoding, as we see next.

Theorem 1.2 (DF inner bound). *An inner bound on the capacity of the RC is defined by all the nonnegative rates R satisfying*

$$R \leq \max_{p(x_1 x_2)} \min \{ I(X_1 X_2; Y_3),\ I(X_1; Y_2 | X_2) \}. \tag{50}$$

Proof. The transmission time is split in $b+1$ time blocks, each consisting of n time slots, and the message are sent in each block using block Markov coding. In total, a sequence of b independent and identically distributed (i.i.d.) messages $\mathbb{M}_{n,j} \in [1 : 2^{nR}]$, $j \in [1 : b]$, is sent over the channel in $n(b+1)$ transmissions, thus the rate of information approaches R as both n and b tend to infinity.

CODEBOOK GENERATION Fix the joint PD $p(x_1 x_2)$ that attains the maximum in the inner bound (50). Then, for each block proceed as follows:

1. Generate 2^{nR} i.i.d. sequences $x_2^n(m_{j-1})$, where $m_{j-1} \in [1 : 2^{nR}]$, according to the PD
$$p(x_2^n) = \prod_{i=1}^n p(x_{2i}).$$
2. For each sequence $x_2^n(m_{j-1})$, generate 2^{nR} conditionally independent sequences $x_1^n(m_{j-1}, m_j)$, where $m_j \in [1 : 2^{nR}]$, according to the conditional PD
$$p(x_1^n | x_2^n(m_{j-1})) = \prod_{i=1}^n p(x_{1i} | x_{2i}(m_{j-1})).$$

ENCODING In block j, the encoding proceed as follows:

1. The relay knows the message m_{j-1} from the decoding step in the previous block, thus, it transmits $x_2^n(m_{j-1})$.
2. To send the message m_j, the encoder transmits the sequence $x_1^n(m_{j-1}, m_j)$, where $m_0 = m_{b+1} = 1$.

See Table 4 for details.

DECODING

1. In block j, the relay looks for the unique index $m_j \equiv \hat{m}$ such that
$$(x_1^n(m_{j-1}, \hat{m}), x_2^n(m_{j-1}), y_{2j}^n) \in T_\delta^n(X_1 X_2 Y_2).$$

$j=1$	$j=2$	$\dots$	$j=b$	$j=b+1$
$x_1^n(1,m_1)$	$x_1^n(m_1,m_2)$	$\dots$	$x_1^n(m_{b-1},m_b)$	$x_1^n(m_b,1)$
$x_2^n(1)$	$x_2^n(m_1)$	$\dots$	$x_2^n(m_{b-1})$	$x_2^n(m_b)$

Table 4.: Codewords in the DF scheme.

The probability of error in the decoding of $\hat{m}$ can be made arbitrarily small if,

$$R < I(X_1;Y_2|X_2) - \delta.$$

2. On the other hand, the destination waits until the transmission has ended and decodes the messages starting from the last one. In other words, assuming its past message estimates are correct, the destination looks for the index $m_{j-1} \equiv \hat{m}$ backwardly such that

$$(x_1^n(\hat{m}, m_j), x_2^n(\hat{m}), y_{3j}^n) \in T_\delta^n(X_1X_2Y_3).$$

The probability of error in the decoding of $\hat{m}$ can be made arbitrarily small if,

$$R < I(X_1X_2;Y_3) - \delta.$$

Letting $n \to \infty$ and taking an arbitrarily small δ, we obtain (50). □

Remark 1.1. *This scheme achieves capacity for the* degraded RC*, i.e.,* $X_1 - \circ\!\!- (X_2Y_2) -\!\!\circ\!\!- Y_3$.

Partial Decode-and-Forward Inner Bound

In DF, the relay decodes the message completely, which is optimal for the degraded RC because the relay receives a strictly better version of X_1 than the destination. If that is not the case, the decoding at the relay can restrict the achievable rate. Therefore, in *partial* DF, the relay decodes only part of the message. This yields a tighter lower bound on the capacity than both DF and direct transmission.

Theorem 1.3 (partial DF inner bound)**.** *An inner bound on the capacity of the RC is defined by all the nonnegative rates R satisfying*

$$R \le \max_{p(ux_1x_2)} \min\left\{I(X_1X_2;Y_3),\, I(U;Y_2|X_2) + I(X_1;Y_3|X_2U)\right\}. \tag{51}$$

Sketch of proof. As in the DF scheme, the transmission is split into b time blocks, and it employs block Markov coding and backward decoding. The message in each block $j \in [1:b]$ is now divided in two, i.e., $\mathbb{M}_{n,j} = (\mathbb{M}'_{n,j}, \mathbb{M}''_{n,j})$ where $\mathbb{M}'_{n,j} \in [1:2^{nR'}]$ and $\mathbb{M}''_{n,j} \in [1:2^{nR''}]$. Thus, $R = R' + R''$.

The source and the relay cooperate in the transmission of only the message $\mathbb{M}'_{n,j}$, whereas $\mathbb{M}''_{n,j}$ is decoded solely by the destination. In order to achieve this, the codebook in each block has $2^{nR'}$ i.i.d. sequences $x_2^n(m'_{j-1})$, where each one has $2^{nR'}$ conditionally independent sequences $u^n(m'_{j-1}, m'_j)$ superimposed, and where each one of these has $2^{nR''}$ conditionally independent sequences $x_1^n(m'_{j-1}, m'_j, m''_j)$ superimposed.

In each block $j \in [1 : b]$, the relay decodes m'_j knowing m'_{j-1} and transmits that message in the next block. On the other hand, the destination waits until the end of the transmission and then it backwardly decodes the indices m'_{j-1} and m''_j. The probability of error in the decoding of can be made arbitrarily small as long as (51) holds. □

Compress-and-Forward Inner Bound

In CF, the relay does not attempt to recover the message but instead, it compresses its channel observation and sends this description. Since this description is correlated with the received sequence, Wyner-Ziv coding is used to reduce the rate needed to communicate it to the receiver. The receiver reconstructs this information and uses it together with its own observation to recover the message.

Theorem 1.4 (CF inner bound)**.** *An inner bound on the capacity of the RC is defined by all the nonnegative rates R satisfying*

$$R \leq \max_{p \in \mathcal{P}_{cf}} \min \left\{ I(X_1X_2; Y_3) - I(Y_2; \hat{Y}_2|X_1X_2Y_3),\ I(X_1; \hat{Y}_2Y_3|X_2) \right\}, \tag{52}$$

where the joint PD $\mathcal{P}_{cf}$ is of the form $p(x_1)p(x_2)p(\hat{y}_2|x_2y_2)$.

Proof. The transmission time is now split in $b + b_s$ time blocks, each consisting of n time slots. The source transmits b i.i.d. messages $\mathbb{M}_{n,j} \in [1 : 2^{nR}]$, $j \in [1 : b]$, and during the additional b_s blocks, the relay repeats the same compression index to ensure a correct decoding at the destination.

CODEBOOK GENERATION Fix the PD $p \in \mathcal{P}_{cf}$ that attains the maximum in the inner bound. Then, for each block proceed as follows:

1. Generate 2^{nR} i.i.d. sequences $x_1^n(m_j)$, where $m_j \in [1 : 2^{nR}]$, according to the PD
$$p(x_1^n) = \prod_{i=1}^n p(x_{1i}).$$
2. Generate $2^{n\hat{R}}$ i.i.d. sequences $x_2^n(s_{j-1})$, where $s_{j-1} \in [1 : 2^{n\hat{R}}]$, according to the PD
$$p(x_2^n) = \prod_{i=1}^n p(x_{2i}).$$

$j=1$	$j=2$	$\dots$	$j=b$	$j=b+1$	$\dots$	$j=b+b_s$
$x_1^n(m_1)$	$x_1^n(m_2)$	$\dots$	$x_1^n(m_b)$	$x_1^n(1)$	$\dots$	$x_1^n(1)$
$x_2^n(1)$	$x_2^n(s_1)$	$\dots$	$x_2^n(s_{b-1})$	$x_2^n(s_b)$	$\dots$	$x_2^n(s_b)$
$\hat{y}_2^n(1,s_1)$	$\hat{y}_2^n(s_1,s_2)$	$\dots$	$\hat{y}_2^n(s_{b-1},s_b)$	$\emptyset$	$\dots$	$\emptyset$

Table 5.: Codewords in the CF scheme.

3. For each sequence $x_2^n(s_{j-1})$, generate $2^{n\hat{R}}$ conditionally independent sequences $\hat{y}_2^n(s_{j-1},s_j)$, where $s_j \in [1:2^{n\hat{R}}]$, according to the conditional PD

$$p(\hat{y}_2^n|x_2^n(s_{j-1})) = \prod_{i=1}^n p(\hat{y}_{2i}|x_{2i}(s_{j-1})).$$

ENCODING In block j, the encoding proceed as follows:

1. To send the message m_j, the encoder transmits the sequence $x_1^n(m_j)$, where $m_j = 1$ for $j \in [b+1:b+b_s]$.

2. At the end of block $j \in [1:b]$, the relay looks for at least one index $s_j \equiv \hat{s}$, with $j_0 = 1$ such that

$$\left(x_2^n(s_{j-1}), \hat{y}_2^n(s_{j-1},\hat{s}), y_{2j}^n\right) \in T_{\delta'}^n(X_2\hat{Y}_2Y_2).$$

The probability of finding such index goes to one as $n \to \infty$ if

$$\hat{R} > I(Y_2;\hat{Y}_2|X_2) + \delta'. \tag{53}$$

It then transmits $x_2^n(s_j)$ in the next time block. Moreover, for blocks $j \in [b+1:b+b_s]$, the last compression index s_b is repeated.

See Table 5 for details.

DECODING

1. The destination decodes the compression index in two steps. First, it looks for the unique index $s_b \equiv \hat{s}$ such that, $\forall j \in [b+1:b+b_s]$,

$$\left(x_1^n(1), x_2^n(\hat{s}), y_{3j}^n\right) \in T_\delta^n(X_1X_2Y_3).$$

For a finite but sufficiently large b_s, the probability of incorrectly decoding s_b can be made arbitrarily small.

2. After finding s_b, the destination looks for the unique set of indices $(m_j, s_{j-1}) \equiv (\hat{m},\hat{s})$ such that

$$\left(x_1^n(\hat{m}), x_2^n(\hat{s}), \hat{y}_2^n(\hat{s},s_j), y_{3j}^n\right) \in T_\delta^n(X_1X_2\hat{Y}_2Y_3).$$

The probability of error in the decoding of $\hat{m}$ can be made arbitrarily small if,

$$R < I(X_1; \hat{Y}_2 Y_3 | X_2) - \delta, \tag{54a}$$
$$\hat{R} < I(X_2; Y_3 | X_1) + I(X_1 Y_3; \hat{Y}_2 | X_2) - \delta, \tag{54b}$$
$$R + \hat{R} < I(X_1 X_2; Y_3) + I(X_1 Y_3; \hat{Y}_2 | X_2) - \delta. \tag{54c}$$

Combining the bounds (53) and (54), and taking into account that $\hat{Y}_2 \multimap (X_2 Y_2) \multimap (X_1 Y_3)$ form a Markov chain, we obtain,

$$\begin{aligned} R &< I(X_1; \hat{Y}_2 Y_3 | X_2) - \delta, \\ 0 &< I(X_2; Y_3 | X_1) - I(Y_2; \hat{Y}_2 | X_1 X_2 Y_3) - \delta - \delta', \\ R &< I(X_1 X_2; Y_3) - I(Y_2; \hat{Y}_2 | X_1 X_2 Y_3) - \delta - \delta'. \end{aligned}$$

It can be proven that, whenever the second inequality does not hold, the rate achieved by the CF scheme with $X_2 = \hat{Y}_2 = \emptyset$ is larger. The last inequality is hence redundant in the maximization process and it can be eliminated. Letting $n \to \infty$ and taking an arbitrarily small δ and δ', we obtain (52). □

1.2.2 *Interference Channel*

The IC was first studied by Ahlswede [14], who introduced basic inner and outer bounds. To date, there is one achievable rate region believed to be the largest, the one due to Han and Kobayashi [15], however, there are several outer bounds, each one with different advantages with respect to the others. We only present two in the sequel, the outer bound for *strong interference* due to Sato [16, 17] and the one for the injective semideterministic IC (IS-IC) due to Telatar and Tse [5].

The IC consists of two source encoders and two destinations. Encoder k wishes to send a message $\mathbb{M}_{n,k} \in \tilde{\mathcal{M}}_{n,k} \triangleq \{1, \ldots, M_{n,k}\}$ to destination k, $k \in \{1, 2\}$. The IC, depicted in Fig. 7, is modeled as a memoryless channel defined by a conditional PD:

$$p(y_1 y_2 | x_1 x_2) : \mathcal{X}_1 \times \mathcal{X}_2 \longmapsto \mathcal{Y}_1 \times \mathcal{Y}_2$$

where $x_k \in \mathcal{X}_k$ and $y_k \in \mathcal{Y}_k$, $k \in \{1, 2\}$, are the input at source k and output at destination k, respectively.

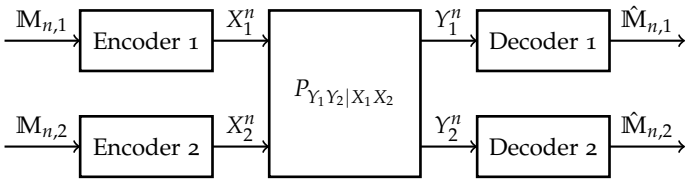


Figure 7.: Interference channel.

Han-Kobayashi Inner Bound

The Han-Kobayashi (HK) inner bound is based on the idea of rate-splitting introduced by Carleial [18] and is tight for all interference channels with known capacity regions.

Theorem 1.5 (Han-Kobayashi inner bound). *An inner bound on the capacity of the IC is defined by all the nonnegative rate pairs (R_1, R_2) satisfying*

$$\begin{aligned}
R_1 &\leq I(X_1; Y_1|U_2Q),\\
R_2 &\leq I(X_2; Y_2|U_1Q),\\
R_1+R_2 &\leq I(X_1; Y_1|U_1U_2Q) + I(U_1X_2; Y_2|Q),\\
R_1+R_2 &\leq I(X_1U_2; Y_1|Q) + I(X_2; Y_2|U_1U_2Q),\\
R_1+R_2 &\leq I(X_1U_2; Y_1|U_1Q) + I(U_1X_2; Y_2|U_2Q),\\
2R_1+R_2 &\leq I(X_1U_2; Y_1|Q) + I(X_1; Y_1|U_1U_2Q) + I(U_1X_2; Y_2|U_2Q),\\
R_1+2R_2 &\leq I(X_1U_2; Y_1|U_1Q) + I(U_1X_2; Y_2|Q) + I(X_2; Y_2|U_1U_2Q).
\end{aligned}$$

for some joint PD of the form $p(q)p(u_1x_1|q)p(u_2x_2|q)$.

Proof. Each source $k \in \{1,2\}$ splits its message $\tilde{m}_k$ into a common message m_k and a private one w_k, each with partial rate R_{k0} and R_{kk}, respectively, such that $R_k = R_{k0} + R_{kk}$. In addition to decoding the intended message, each destination decodes the interfering common message, thus reducing the interference.

CODE GENERATION Fix a PD $p(q)p(u_1x_1|q)p(u_2x_2|q)$.

1. Generate the time-sharing sequence q^n where each element is i.i.d. according to the PD
$$p(q^n) = \prod_{i=1}^n p(q_i).$$
2. For each source $k \in \{1,2\}$ and the sequence q^n, generate $2^{nR_{k0}}$ conditionally independent sequences $u_k^n(m_k)$, $m_k \in \left[1 : 2^{nR_{k0}}\right]$, and distributed according to the conditional PD
$$p(u_k^n|q^n) = \prod_{i=1}^n p(u_{ki}|q_i).$$
3. For each source $k \in \{1,2\}$ and for each $u_k^n(m_k)$, generate $2^{nR_{kk}}$ conditionally independent sequences $x_k^n(m_k, w_k)$, where $w_k \in \left[1 : 2^{nR_{kk}}\right]$, and distributed according to the conditional PD
$$p(x_k^n|u_k^n(m_k), q^n) = \prod_{i=1}^n p(x_{ki}|u_{ki}(m_k), q_i).$$

ENCODING To send the message $\tilde{m}_k = (m_k, w_k)$, source $k \in \{1,2\}$ transmits $x_k^n(m_k, w_k)$.

DECODING

1. Destination 1 looks for the unique set of indices $(m_1, w_1) \equiv (\hat{m}, \hat{w})$ for some index $m_2 \equiv \hat{s}$ such that

$$\left(u_1^n(\hat{m}), x_1^n(\hat{m}, \hat{w}), u_2^n(\hat{s}), y_1^n, q^n\right) \in T_\delta^n(U_1 X_1 U_2 Y_1 Q).$$

   The probability of error in the decoding of $(\hat{m}, \hat{w})$ can be made arbitrarily small if,

$$R_{11} < I(X_1; Y_1|U_1 U_2 Q) - \delta, \tag{55a}$$
$$R_{10} + R_{11} < I(X_1; Y_1|U_2 Q) - \delta, \tag{55b}$$
$$R_{20} + R_{11} < I(X_1 U_2; Y_1|U_1 Q) - \delta, \tag{55c}$$
$$R_{10} + R_{11} + R_{20} < I(X_1 U_2; Y_1|Q) - \delta. \tag{55d}$$

2. Destination 2 performs similarly, and all the above inequalities hold by swapping the indices 1 and 2.

After running Fourier-Motzkin elimination (FME) to the system composed by (55) and its symmetric one for the second user, and letting $n \to \infty$, we obtain the region in Theorem 1.5 plus two bounds:

$$R_1 \leq I(X_1; Y_1|U_1 U_2 Q) + I(U_1 X_2; Y_2|U_2 Q),$$
$$R_2 \leq I(X_1 U_2; Y_1|U_1 Q) + I(X_2; Y_2|U_1 U_2 Q).$$

It can be shown that these two inequalities are redundant because whenever one of them is active for a given PD, there is another PD that attains a higher rate. □

Strong and Weak Interference

Definition 1.1. *An IC is said to have* strong interference *if*

$$I(X_1; Y_1|X_2) \leq I(X_1; Y_2|X_2),$$
$$I(X_2; Y_2|X_1) \leq I(X_2; Y_1|X_1).$$

for all joint PDs of the form $p(x_1)p(x_2)$.

Theorem 1.6. *The capacity region of the IC with strong interference is defined by all the nonnegative rate pairs* (R_1, R_2) *satisfying*

$$R_1 \leq I(X_1; Y_1|X_2 Q),$$
$$R_2 \leq I(X_2; Y_2|X_1 Q),$$
$$R_1 + R_2 \leq \min\{I(X_1 X_2; Y_1|Q),\ I(X_1 X_2; Y_2|Q)\}.$$

Proof. In this scenario, the optimal strategy is to decode the interfering messages, i.e., $U_k = X_k$ for $k \in \{1, 2\}$ in the HK scheme. The converse can be proved using the multi-letter expression of the strong interference condition, i.e., $I(X_k^n; Y_k^n|X_l^n) \leq I(X_k^n; Y_l^n|X_l^n)$ for $(k, l) = \{(1, 2), (2, 1)\}$ [17]. □

The capacity region of the Gaussian IC is also known under the *weak interference* condition. This region is achieved by the other extreme special case of the HK scheme, $U_k = \emptyset$ for $k \in \{1, 2\}$, i.e., the receivers should treat the interference as noise.

Injective Semideterministic IC

In the general case, the capacity region is unknown, however, it has been shown by Etkin-Tse-Wang [19] that a suboptimal evaluation of the HK inner bound achieves the capacity region of the Gaussian IC within 1 bit per complex dimension. Telatar and Tse extended the upper bounding technique from [19] to a more general class of channels [5], later on referred to as IS-IC.

Definition 1.2 (injective semideterministic IC)**.** *In the injective semideterministic IC (IS-IC), the randomness of the channel is captured by the interference signals S_1 and S_2. The conditional PD of the interference signals may be decomposed as follows, $p(s_1 s_2|x_1 x_2) = p(s_1|x_1)p(s_2|x_2)$, and the outputs of the channel are deterministic functions of (X_1, X_2, S_1, S_2). Specifically, we have that $Y_1 = f_1(X_1, S_2)$ and $Y_2 = f_2(X_2, S_1)$, where f_1 and f_2 are functions that, for every (x_1, x_2),*

$$f_1(x_1, \cdot) : \mathcal{S}_2 \to \mathcal{Y}_1,\ s_2 \mapsto f_1(x_1, s_2),$$
$$f_2(x_2, \cdot) : \mathcal{S}_1 \to \mathcal{Y}_2,\ s_1 \mapsto f_2(x_2, s_1)$$

are invertible.

Theorem 1.7. *The capacity region of the IS-IC is upper bounded by all nonnegative rate pairs (R_1, R_2) satisfying:*

$$\begin{aligned}
R_1 &\le I(X_1; Y_1|X_2 Q),\\
R_2 &\le I(X_2; Y_2|X_1 Q),\\
R_1{+}R_2 &\le I(X_1; Y_1|U_1 X_2 Q) + I(X_1 X_2; Y_2|Q),\\
R_1{+}R_2 &\le I(X_1 X_2; Y_1|Q) + I(X_2; Y_2|X_1 U_2 Q),\\
R_1{+}R_2 &\le I(X_1 X_2; Y_1|U_1 Q) + I(X_1 X_2; Y_2|U_2 Q),\\
2R_1{+}R_2 &\le I(X_1 X_2; Y_1|Q) + I(X_1; Y_1|U_1 X_2 Q) + I(X_1 X_2; Y_2|U_2 Q),\\
R_1{+}2R_2 &\le I(X_1 X_2; Y_1|U_1 Q) + I(X_1 X_2; Y_2|Q) + I(X_2; Y_2|X_1 U_2 Q).
\end{aligned}$$

for some PD of the form $p(q)p(x_1|q)p(x_2|q)p_{S_1|X_1}(u_1|x_1)p_{S_2|X_2}(u_2|x_2)$.

Sketch of proof. The outer bound is established by using a genie-aided strategy that employs auxiliary random variables (RVs) U_k which are conditionally independent copies of S_k given X_k. We only derive the first sum-rate in the sequel, but all the other bounds can be obtained in the same way. First consider,

$$\begin{aligned}
n(R_1 - \epsilon_n) &\le I(X_1^n; Y_1^n) \qquad (56a)\\
&\le I(X_1^n; Y_1^n U_1^n X_2^n)
\end{aligned}$$

$$= I(X_1^n; U_1^n|X_2^n) + I(X_1^n; Y_1^n|U_1^n X_2^n) \tag{56b}$$
$$= H(U_1^n) - H(U_1^n|X_1^n) + I(X_1^n; Y_1^n|U_1^n X_2^n) \tag{56c}$$
$$= H(S_1^n) - H(Y_2^n|X_1^n X_2^n) + I(X_1^n; Y_1^n|U_1^n X_2^n), \tag{56d}$$

where in (56a) we use Fano's inequality; in (56b) we note that X_2 is independent of X_1; in (56c) we further note that U_1 only depends on X_1 and is thus independent of X_2; and in (56d) we take into account the IS-IC model, in particular, $H(U_1^n) = H(S_1^n)$ and $H(U_1^n|X_1^n) = H(S_1^n|X_1^n) = H(Y_2^n|X_1^n X_2^n)$. Now consider,

$$\begin{aligned} n(R_2 - \epsilon_n) &\leq I(X_2^n; Y_2^n) \\ &= H(Y_2^n) - H(Y_2^n|X_2^n) \\ &= H(Y_2^n) - H(S_1^n|X_2^n), \qquad (57a) \\ &= H(Y_2^n) - H(S_1^n), \qquad (57b) \end{aligned}$$

where in (57a) we use again the IS-IC model; and in (57b) we note that S_1 is independent of X_2. Adding up (56d) and (57b), we obtain a bound that can be single-letterized,

$$\begin{aligned} n(R_1 + R_2 - \epsilon_n') &\leq I(X_1^n; Y_1^n|U_1^n X_2^n) + I(X_1^n X_2^n; Y_2^n) \\ &\leq \sum_{i=1}^{n} \left[I(X_{1i}; Y_{1i}|U_{1i} X_{2i}) + I(X_{1i} X_{2i}; Y_{2i}) \right] \\ &= n \left[I(X_1; Y_1|U_1 X_2 Q) + I(X_1 X_2; Y_2|Q) \right], \end{aligned}$$

where in the last step we add the time-sharing RV Q uniformly distributed in $[1 : n]$. □

1.2.3 *Interference Relay Channel*

The interest on the IRC, depicted in Fig. 8, is quite recent [20], however, several inner and outer bounds can be found in the literature. As previously mentioned, neither the capacity of the RC nor the one of the IC is known in the general case. The IRC, being a combination of these two models, has only a handful of capacity results for specific channel conditions, e.g., *strong interference* or *degradedness*.

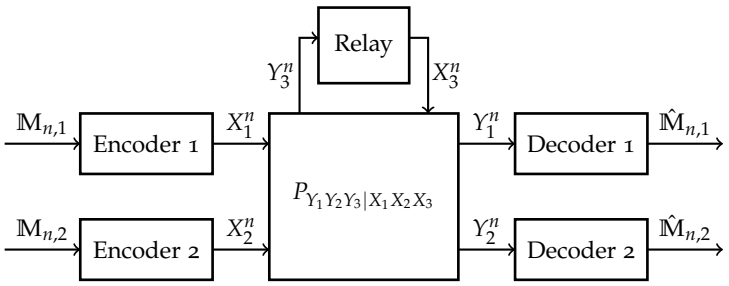


Figure 8.: Interference relay channel.

Contribution

Our goal in this part of the thesis is to characterize within a fixed number of bits the capacity region of the Gaussian IRC, independent of any channel conditions. To do so, we derive a novel outer bound and two inner bounds based on the ideas shown so far. Specifically, we propose a nontrivial extension of the *injective semideterministic* class of channels for the IRC and we derive an outer bound for it. Additionally, we propose two inner bounds, which combine the (partial) DF and CF relaying strategies with the HK scheme for the IC to deal with interference.

Although the use of DF and CF schemes in the context of the IRC is not new, our aim is to provide a set of simple but powerful enough strategies in order to characterize the capacity region of Gaussian IRCs within a constant gap, as previously stated. In this regard, our main contributions with respect to the literature are the introduction of *partial* DF, where the relay forwards only part of the source's message, and the use of different decoding strategies in the CF scheme which helps us obtain a compact expression of the inner bound. Moreover, our proposed inner bounds generalize existing ones from the literature and achieve capacity in the situations where capacity is known for the IRC.

Due to the complexity of the model, we study a particular class of IRC where the relay observes the signal from only one of the transmitters. Nonetheless, interesting insights about the usefulness of the relay and the different relaying strategies arise from the analysis of the Gaussian IRC. In particular, the main outcome of this work is the characterization of the capacity region of the aforementioned Gaussian IRC within a constant gap. We show that, for any channel realization, at least one of the proposed schemes achieves the capacity region within a constant gap.

1.3 WIRETAP CHANNEL WITH GENERALIZED FEEDBACK

We first present some background information about wiretap channel (WTC) without feedback and then, we proceed with the WCGF.

1.3.1 *Wiretap Channel*

Information theoretic secrecy was introduced by Shannon [21]. In his work, he investigates a communication system between a source, a legitimate destination and an eavesdropper, where the source and the legitimate destination share a *secret key* through a dedicated private link. Shannon's pessimistic result is that to achieve perfect secrecy

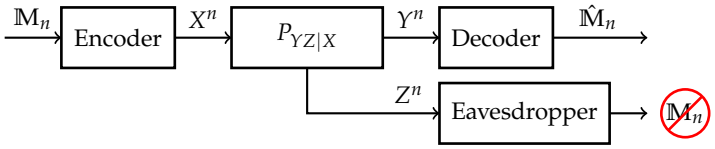


Figure 9.: Wiretap channel.

the size of the key must be at least as large as the size of the message. In other words, we could directly use the dedicated private link to convey the message. Subsequent work by Wyner [22], where he introduced the notion of WTC showed that secrecy is still possible without a secret key in a broadcast channel (BC) if the eavesdropper's channel is degraded with respect to the legitimate destination's.

The WTC consists of one source, one legitimate destination, and one eavesdropper. The source wishes to transmit a message $\mathbb{M}_n \in \mathcal{M}_n$ securely to a destination while an eavesdropper is present in the channel. The WTC, depicted in Fig. 9, is modeled as a memoryless channel defined by a conditional PD

$$p(yz|x) : \mathcal{X} \longmapsto \mathcal{Y} \times \mathcal{Z},$$

where $x \in \mathcal{X}$ is the source's channel input, and $y \in \mathcal{Y}$ and $z \in \mathcal{Z}$ are the legitimate receiver's and eavesdropper's channel outputs, respectively.

The main objective of this model is not only to analyze transmission schemes that assure *reliable* communication between the legitimate nodes but also that the schemes do not *leak* information to the eavesdropper. In other words, the conditional probability of the message given the eavesdropper's observation has to be approximately uniform over the message set, i.e., $\lim_{n\to\infty} \frac{1}{n} H(\mathbb{M}_n|Z^n) = R$, or equivalently $\lim_{n\to\infty} \frac{1}{n} I(\mathbb{M}_n; Z^n) = 0$.

Csiszár and Körner established the rate-leakage region of a general BC with common and confidential messages in [23], from where we can derive the secrecy capacity of the WTC.

Theorem 1.8. *The secrecy capacity of the WTC is*

$$C_s = \max_{p(ux)} \{I(U;Y) - I(U;Z)\}. \tag{58}$$

Proof. The transmission strategy is based on the idea of stochastic encoding, where the source buries the useful signal under a noise sequence. The rate of this noise sequence should be high enough to saturate the capacity of the eavesdropper's link, but low enough to enable the legitimate receiver to recover the message.

CODEBOOK GENERATION Let us define the quantity

$$\tilde{R} = I(U;Z) - \epsilon,$$

and fix the PD that attains the maximum in (58). Then, generate $2^{n(R+\tilde{R})}$ i.i.d. sequences $u^n(m,l)$, where $m \in [1:2^{nR}]$ and $l \in [1:2^{n\tilde{R}}]$, according to the PD

$$p(u^n) = \prod_{i=1}^{n} p(u_i).$$

ENCODING To send the message m, the encoder chooses an index l uniformly at random and selects the codeword $u^n(m,l)$. It then transmits the associated jointly typical sequence $x^n(m,l)$ that is randomly generated according to the conditional PD

$$p(x^n|u^n(m,l)) = \prod_{i=1}^{n} p(x_i|u_i(m,l)).$$

DECODING The decoder finds the unique set of indices $(m,l) \equiv (\hat{m},\hat{l})$ such that

$$(u^n(\hat{m},\hat{l}), y^n) \in T_\delta^n(UY).$$

The probability of error in the decoding of $(\hat{m},\hat{l})$ can be made arbitrarily small if,

$$R + \tilde{R} < I(U;Y) - \delta.$$

Given the definition of $\tilde{R}$, and letting $n \to \infty$ while taking an arbitrarily small δ and ϵ, we obtain (58).

INFORMATION LEAKAGE Let us denote with $\mathbb{M}_n$ and L the RVs associated with the message and the noise index. Then, consider,

$$\begin{aligned}
I(\mathbb{M}_n; Z^n) &= I(\mathbb{M}_n L; Z^n) - I(L; Z^n|\mathbb{M}_n) \\
&\leq I(U^n; Z^n) - I(L; Z^n|\mathbb{M}_n) && \text{(59a)} \\
&= I(U^n; Z^n) - H(L|\mathbb{M}_n) + H(L|Z^n\mathbb{M}_n) \\
&= I(U^n; Z^n) - n[I(U;Z) - \epsilon] + H(L|Z^n\mathbb{M}_n) && \text{(59b)} \\
&\leq I(U^n; Z^n) - n[I(U;Z) - \epsilon] + n\epsilon_n && \text{(59c)} \\
&= nI(U;Z) - n[I(U;Z) - \epsilon] + n\epsilon_n && \text{(59d)} \\
&= n(\epsilon + \epsilon_n), && \text{(59e)}
\end{aligned}$$

where (59a) stems from the Markov chain $(\mathbb{M}_n L) \multimap U^n \multimap Z^n$ and the data processing inequality; where (59b) is due to L being independent of $\mathbb{M}_n$ and its cardinality being $n\tilde{R}$; where (59c) follows from the fact that the uncertainty the eavesdropper has on L once it knows $\mathbb{M}_n$ is bounded by Fano's inequality (given the size of $\tilde{R}$); and where (59d) follows from the i.i.d. codebook construction and that the channel is memoryless. Letting $n \to \infty$ and taking an arbitrarily small ϵ and ϵ_n, (59e) assures that $\lim_{n\to\infty} \frac{1}{n} I(\mathbb{M}_n; Z^n) = 0$. This ends the proof of achievability.

For the converse, consider a code with arbitrarily small probability of error in the decoding and arbitrarily small information leakage as $n \to \infty$. Then, by Fano's inequality,

$$
\begin{aligned}
& n(R-\epsilon_n) \\
& \quad \leq I(\mathbb{M}_n; Y^n) \\
& \quad \leq I(\mathbb{M}_n; Y^n) - I(\mathbb{M}_n; Z^n) + n\eta && \text{(60a)} \\
& \quad \leq \sum_{i=1}^{n} \left[I(\mathbb{M}_n; Y_i | Y^{i-1}) - I(\mathbb{M}_n; Z_i | Z_{i+1}^n) \right] + n\eta \\
& \quad \leq \sum_{i=1}^{n} \left[I(\mathbb{M}_n Z_{i+1}^n; Y_i | Y^{i-1}) - I(\mathbb{M}_n Y^{i-1}; Z_i | Z_{i+1}^n) \right] + n\eta && \text{(60b)} \\
& \quad \leq \sum_{i=1}^{n} \left[I(\mathbb{M}_n; Y_i | Y^{i-1} Z_{i+1}^n) - I(\mathbb{M}_n; Z_i | Y^{i-1} Z_{i+1}^n) \right] + n\eta && \text{(60c)} \\
& \quad \leq \sum_{i=1}^{n} \left[I(U_i; Y_i | V_i) - I(U_i; Z_i | V_i) \right] + n\eta && \text{(60d)} \\
& \quad \leq n \left[I(U; Y | V) - I(U; Z | V) + \eta \right] && \text{(60e)} \\
& \quad \leq \max_v n \left[I(U; Y | V = v) - I(U; Z | V = v) + \eta \right] \\
& \quad \leq n \left[C_s + \eta \right], && \text{(60f)}
\end{aligned}
$$

where (60a) stems from the condition on the information leakage, i.e., $I(\mathbb{M}_n; Z^n) \leq n\eta$; where (60b) and (60c) follow by the Csiszár sum identity; where (60d) is due to the identification of auxiliary RVs $V_i = (Y^{i-1} Z_{i+1}^n)$ and $U_i = (\mathbb{M}_n V_i)$; where (60e) follows by introducing a time-sharing RV Q uniformly distributed in $[1 : n]$, and defining $U = (U_Q, Q)$, $V = (V_Q, Q)$, $Y = Y_Q$, and $Z = Z_Q$; and (60f) is due to $U \multimap X \multimap (Y, Z)$ being a Markov chain given $V = v$. □

To achieve positive secrecy rates, (58) imposes that the legitimate user must have a *better* channel than the eavesdropper. This assumption might be reasonable in wired networks, where the eavesdropper has to physically tap a wire without being detected and would likely lead to signal degradation. However, the broadcast nature of the wireless medium allows eavesdroppers to easily intercept communications. To worsen the situation, these nodes could be potentially closer to the transmitter than the legitimate users and better equipped, e.g., larger number of receive antennas, improved RF circuitry, and more powerful computing power. Therefore, the assumption that the legitimate user experiences a better channel becomes more *unrealistic* in wireless networks.

The use of feedback, as we see next, improves the security of wireless transmissions, since it can be employed to artificially create asymmetries in the decoding capabilities of the legitimate user and the eavesdropper.

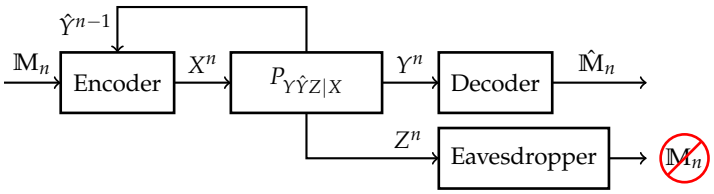


Figure 10.: Wiretap channel with generalized feedback.

1.3.2 *Wiretap Channel with Generalized Feedback*

The study of the WCGF, depicted in Fig. 10, has become relevant recently due to the increased concern on wireless security. To the best of our knowledge, one of the first works on this topic analyzes the WTC with perfect output feedback [9], a special case of the WCGF. The proposed transmission strategy employs the shared signal between the legitimate users (which is not available at the eavesdropper) to generate a secret key and then uses it to encrypt the message. The encrypted message behaves like the noise index in Wyner's scheme which helps increase the achievable rate.

Over the years, there has been substantial work on the WTC with different feedback models, however, the capacity in the general case remains unknown. In the literature, there exist two complimentary approaches based on the use of the feedback signal. On the first one, already presented, the legitimate users extract common randomness from their respective channel output which they use as a shared *secret key*. This key encrypts the message at the bit level which provides secrecy as long as the eavesdropper cannot obtain the key. On the second approach, the encoder relies on a "feedback-dependent codebook" that correlates the codewords to be sent with the feedback signal. In this way, the source seeks to hide as much as possible the transmitted codewords from the eavesdropper's observations (e.g. *beamforming* at the codeword level).

The generation of the secret key from the first approach is a problem in and of itself. Many present day secure systems rely on the use of temporary security credentials that change from time to time. The moment these credentials are exchanged is when the system is most vulnerable and, if they are compromised, the integrity of the whole system cannot be guaranteed. For this reason, the analysis of a secure way to generate shared secret keys between the legitimate users is of significant importance in cryptography.

Contribution

In the second part of this thesis, our goal is to provide a general transmission strategy that encompasses the existing results for different feedback models found in the literature. In doing so, we hope to

shed some light into the similarities of the two distinct approaches in the use of feedback mentioned previously. To this end, we propose two different inner bounds on the capacity of the memoryless WCGF, using the two aforementioned approaches.

We first derive an inner bound that is based on the use of joint source-channel coding, which introduces time dependencies between the feedback outputs and the channel inputs through different time blocks. We then introduce a second inner bound based on the secret key approach, where the feedback link is used to generate a key that encrypts the message partially or completely. Moreover, as a side result, we derive an inner bound on secret key agreement for the same channel model.

All these new bounds extend several existing bounds that were obtained for special classes of networks and feedback models. Our results can be seen as a generalization and thus unification of several results in the field.

1.4 THESIS OUTLINE

The dissertation is organized as follows.

In Chapter 1, we present the motivation behind this work and we introduce the models to be analyzed. Then, we review some basic background material for these models and we briefly enounce our contributions.

The main body of the dissertation is divided in two parts. In the first part, composed by Chapters 2 and 3, we investigate the interference relay channel (IRC). In Chapter 2, we introduce this problem and we review the most important and related works in the literature. We additionally present our contributions for this part of the thesis and we define the system model. In Chapter 3, we show the outer and inner bounds proposed for the IRC, and we present the constant-gap results we have obtained for the Gaussian IRC. These results allow us to provide some insight into this complex model. All the proofs are deferred to the appendices at the end of the chapter.

The second part of the dissertation, composed by Chapters 4 and 5, deals with the wiretap channel with generalized feedback (WCGF). In Chapter 4, we introduce the WCGF and we survey related works in the literature. We also present the contributions we have made for this part of the thesis and we define the system model. In Chapter 5, we develop two inner bounds for the WCGF based on two different approaches in the use of feedback, and we show how these schemes recover previous results from the literature. We finally provide some insight into the difference between these two approaches. Again, the proofs for the schemes are deferred to the appendices at the end of the chapter.

This dissertation ends with Chapter 6 where we present general conclusions and future perspectives of the work.

Part I

INTERFERENCE RELAY CHANNEL

2

INTRODUCTION AND SETUP

2.1 INTRODUCTION

Cellular networks have reached practical limits in many dense urban areas while data traffic and the number of users seem to be continuously increasing. Interference has become one of the most crucial problems in these networks where users must compete for the available resources, e.g., an improvement in terms of data rate for one of them may be detrimental to the performance of another user. Although the existence of a large amount of users in cellular networks has driven communication channels from being noise-limited to interference-limited, this characteristic can also be exploited to boost the overall network throughput by means of user cooperation.

In order to provision a new communication infrastructure, network operators are rethinking conventional cellular system topologies to consider a new paradigm called heterogeneous networks. This topology consists of planned macro base stations (BSs) deployments that typically transmit at high power overlaid with several low power nodes such as: relay and pico BSs, distributed antennas, and femto BSs. These lower power nodes are deployed to further increase the coverage of the network, especially when terminals are far away from the macro BS. Fixed relays are infrastructure equipment that connect wirelessly to the BS and these relays aid in the signal transmission between the macro BS and the mobile users by receiving and retransmitting messages. Indeed, these relays may offer a flexible option where backhauls are not available. In order to assess the benefits of this strategy, an information-theoretic analysis of cooperation through relaying in interference-limited environments should be carried out. Nonetheless, each one of these two fundamental problems –relaying and interference– appears to be rather involved and unfortunately only partial results are available in the literature.

2.1.1 *Related Work*

Perhaps the simplest model of a communication network with interference is the interference channel (IC), whose capacity region –even without a relay– is still an open problem. The largest known achiev-

able rate region is due to Han and Kobayashi [15] and it is based on the idea of interference decoding via "rate-splitting" at the sources, also referred to as "Han-Kobayashi (HK) scheme". This scheme has been shown by Etkin-Tse-Wang [19] to achieve the capacity region of the Gaussian IC within 1 bit per complex dimension. The important feature behind the notion of "constant gap" is that it guarantees a maximum gap between the inner and the outer bound over all channel coefficients and hence all possible fading statistics. This result hinges on a new upper-bounding technique that has been later on extended to a more general class of ICs [5], also referred to as injective semideterministic IC (IS-IC) [1].

Another challenging problem is the relay channel (RC), where a relay node tries to improve the communication between a source-destination pair. Since the seminal work of Cover and El Gamal [13], which has introduced the main cooperative strategies of decode-and-forward (DF) and compress-and-forward (CF), there has been a great deal of research on this topic. Although the capacity of the RC is still unknown in general, the benefits of cooperation by relaying are rather clear by now, at least in the context of single source and/or single destination relay networks [24]. An approximation approach to general networks via deterministic channels was introduced by Avestimehr-Diggavi-Tse [25]. This approach yields a novel improvement over CF scheme –referred to as "quantize-map-and-forward" (QMF)– that achieves capacity to within a constant gap for unicast additive white Gaussian noise (AWGN) networks with an arbitrary number of relays. As a matter of fact, both DF and CF schemes can perform within the same constant gap to the capacity of the Gaussian RC, regardless of the channel parameters [25,26] and thus of the fading statistics. More recently, Lim *et al.* [27] generalized the QMF approach to arbitrary memoryless multicast networks via the noisy network coding (NNC) scheme. Relay nodes based on a NNC scheme send the same –long– message over many blocks of equal length and the descriptions at the relays do not require binning while their indices are non-uniquely decoded at the destination.

In wireless networks with multiple source nodes that communicate simultaneously to several destinations, "interference" becomes the central issue, and the different roles that relays can play to enhance the reliability in such scenarios are not well understood yet. In this part of the thesis, we consider the simplest scenario where interference and relaying appear together, that is the interference relay channel (IRC). The problem itself is not new [20] and the research on this topic has been growing during the past years. In [28], among other works, the authors proposed inner bounds on the capacity region of the NNC based on the standard CF scheme while DF-based schemes are also studied in [29]. It is worth mentioning here that these coding schemes do not use "joint decoding" at the destination

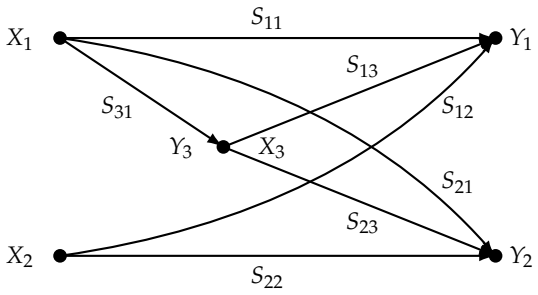


Figure 11.: The Gaussian IRC where the values S_{kl} represent the SNR between nodes l and k.

to recover all transmit messages and the compression indices. The idea of NNC was later on extended to the IRC in [30] by adding rate-splitting. Besides these works, capacity of the *physically degraded* IRC in the *strong interference* regime was determined in [31] by assuming that the relay node can only observe one of the two source encoders. Several variations of this problem have also been investigated, e.g., the "cognitive" IRC where the relay has noncausal knowledge of the sources' messages was treated in [32, 33]. Additionally, the IRC with an "out-of-band relay", i.e., the relay operates over an orthogonal band with respect to the underlying IC, was also studied in [34–38]. Capacity results were obtained in [38] for an IRC with oblivious relaying in which the relay is unaware of the codebook used by the source encoders.

The IC with cooperation at either the transmitter or receiver end, or both has also been investigated. In the extreme regimes where the relay can be thought of being collocated with the transmitters or the receivers, the IRC becomes a virtual multi-antenna IC with transmitter or receiver cooperation. The benefits of such a system have been studied in [39]. Additionally, constant-gap results regardless of channel conditions were provided in [40–43], whereas capacity results in strong interference regime were determined in [44] for the case of transmitter cooperation. Recently, in the case of unilateral source cooperation, improved outer bounds were reported in [45].

2.1.2 *Contribution*

In this work, we focus on a simplified version of the two-user IRC [4] which still captures the rather complex interplay between interference and relaying. This is the two-user IC with a relay node which can only observe one of the source encoders. Although this is not the most general two-user IRC, we shall see that it still captures the central issue of interference and relaying and hence, we seek to provide some useful insights into the understanding of this complex problem. In particular, for the class of Gaussian IRCs shown in Fig. 11, we aim at

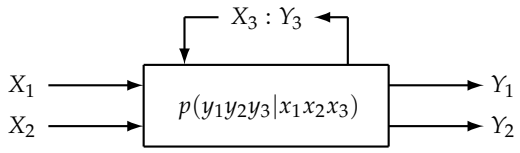


Figure 12.: Interference relay channel model.

determining the underlying SNR regimes together with the adequate coding schemes and decoding techniques that are needed to achieve capacity within a *constant gap*.

Our results involve a novel outer bound for the considered class of IRCs –the injective semideterministic IRC– and two inner bounds based on rate-splitting and different relaying strategies (building on DF and CF schemes) with the adequate interference decoding technique. Although the use of DF and CF schemes in the context of the IRC is not new [20, 28–31], our aim is to provide a set of simple but powerful enough strategies in order to characterize the capacity region of Gaussian IRCs within a constant gap, as previously stated. In this regard, our main contributions with respect to the literature are the introduction of *partial* DF, where the relay forwards only part of the source's message, and the use of different decoding strategies in the CF scheme which helps us obtain a compact expression of the inner bound.

The main outcome of this work is the characterization within a constant gap of the capacity of the aforementioned Gaussian IRC. We show that, for any channel realization, at least one of the proposed schemes achieves the capacity region within a constant gap. More precisely, it is shown that when the source-to-relay channel is stronger than the source-to-destination channel full DF scheme is recommended (this regime includes the capacity result in [31, Thm. 3]). As the strength of the source-to-relay channel reduces, it is preferable to partially decode the message and thus partial DF scheme is required. Finally, when the source-to-relay channel is weaker than the interfering channel from the source to the other destination, CF scheme together with different ways of decoding is needed instead.

2.2 PROBLEM DEFINITION

The IRC consists of two source encoders, two destinations and one relay node. Encoder k wishes to send a message $\tilde{m}_k \in \tilde{\mathcal{M}}_{n,k} \triangleq \{1, \ldots, M_{n,k}\}$ to destination k, $k \in \{1, 2\}$, with the help of the relay. The IRC, depicted in Fig. 12, is modeled as a memoryless channel without feedback defined by a conditional probability distribution (PD):

$$p(y_1y_2y_3|x_1x_2x_3) : \mathcal{X}_1 \times \mathcal{X}_2 \times \mathcal{X}_3 \longmapsto \mathcal{Y}_1 \times \mathcal{Y}_2 \times \mathcal{Y}_3$$

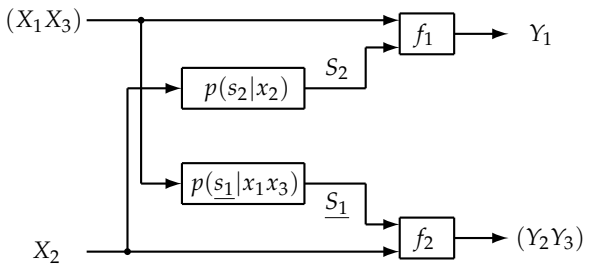


Figure 13.: Injective semideterministic IRC model.

where $x_k \in \mathcal{X}_k$ and $y_k \in \mathcal{Y}_k$, $k \in \{1,2\}$, are the input at source k and output at destination k, respectively, whereas $x_3 \in \mathcal{X}_3$ and $y_3 \in \mathcal{Y}_3$ are the input and output at the relay, respectively. The relaying functions are defined as a sequence of mappings $\{\phi_i : \mathcal{Y}_3^{i-1} \mapsto \mathcal{X}_3\}_{i=1}^n$.

As it was previously stated, throughout the work we deal with a specific type of IRC in which only one of the sources is connected to the relay, i.e.,

$$p(y_1y_2y_3|x_1x_2x_3) = p(y_3|x_1x_3)p(y_1y_2|x_1x_2x_3y_3). \tag{61}$$

Unless it is noted otherwise, this is a basic assumption of our model.

We also recall that a pair of rates (R_1, R_2) is said to be achievable for an IRC if for every $\epsilon > 0$ there exists a block length n, encoders functions $\text{enc}_k : \tilde{\mathcal{M}}_{n,k} \mapsto \mathcal{X}_k^n$, $M_{n,k} \geq 2^{n(R_k-\epsilon)}$, $k \in \{1,2\}$, and decoder functions $\text{dec}_k : \mathcal{Y}_k^n \mapsto \tilde{\mathcal{M}}_{n,k}$, $k \in \{1,2\}$, such that

$$\frac{1}{M_{n,1}M_{n,2}} \sum_{\tilde{m}_1,\tilde{m}_2} \mathbb{P}\big\{\big(\text{dec}_1(Y_1^n), \text{dec}_2(Y_2^n)\big) \neq (\tilde{m}_1, \tilde{m}_2) \,| \\ X_1^n = \text{enc}_1(\tilde{m}_1), X_2^n = \text{enc}_2(\tilde{m}_2)\big\} \leq \epsilon.$$

Definition 2.1 (injective semideterministic IRC)**.** *In this work, we shall focus on the class of IRCs referred to as the injective semideterministic IRC (IS-IRC), as shown in Fig. 13, which is an extension of that introduced in [5] for the IC. In this model, the randomness of the channel is captured by the interference signals S_1, S_2 and S_3. For sake of clarity, we will denote the pair (S_1S_3) as the vector $\underline{S_1}$.*

The conditional PD of the interference signals may be decomposed as,

$$p(\underline{s_1}s_2|x_1x_2x_3) = p(\underline{s_1}|x_1x_3)p(s_2|x_2) \tag{62}$$

and the outputs of the channel are deterministic functions of the random variables (RVs) $(X_1, X_2, X_3, \underline{S_1}, S_2)$. Specifically, we have $Y_1 = f_1(X_1, X_3, S_2)$, $Y_2 = f_2'(X_2, S_1)$, and $(Y_2Y_3) = f_2(X_2, \underline{S_1})$, where f_1, f_2', and f_2 are functions that, for every (x_1, x_2, x_3),

$$\begin{aligned} f_1(x_1, x_3, \cdot) &: \mathcal{S}_2 \to \mathcal{Y}_1, & s_2 &\mapsto f_1(x_1, x_3, s_2), \\ f_2'(x_2, \cdot) &: \mathcal{S}_1 \to \mathcal{Y}_2, & s_1 &\mapsto f_2'(x_2, s_1), \\ f_2(x_2, \cdot) &: \underline{\mathcal{S}_1} \to \mathcal{Y}_2 \times \mathcal{Y}_3, & \underline{s_1} &\mapsto f_2(x_2, \underline{s_1}) \end{aligned}$$

are invertible.

Remark 2.1. *Since the relay only observes the first source, its input X_3 cannot depend on X_2. Therefore, X_3 is regarded as desired signal at Y_1 and as interference at Y_2, which motivates us to model this class of IRCs as depicted in Fig. 13. It comes as no surprise that the pair (X_1X_3) should be taken as a whole. However, as it is shown later in the derivation of the outer bound, it is also convenient to put the pair (Y_2Y_3) together.*

A special case of the IS-IRC is the real Gaussian model, as it is shown in Fig. 11, and defined by

$$Y_1 = h_{11}X_1 + h_{12}X_2 + h_{13}X_3 + Z_1, \tag{63a}$$
$$Y_2 = h_{21}X_1 + h_{22}X_2 + h_{23}X_3 + Z_2, \tag{63b}$$
$$Y_3 = h_{31}X_1 + Z_3, \tag{63c}$$

where each noise process $Z_k \sim \mathcal{N}(0, N_k)$, $k \in \{1,2,3\}$, is independent of each other, and each input has an average power constraint $\mathbb{E}[|X_k|^2] \leq P_k$, $k \in \{1,2,3\}$. The link between node l and k has a fixed channel coefficient h_{kl}, and the SNR associated to it is denoted $S_{kl} \triangleq |h_{kl}|^2 P_l / N_k$. In this model, the interference signals are

$$\underline{S_1} = \begin{bmatrix} S_1 \\ S_3 \end{bmatrix} = \begin{bmatrix} h_{21}X_1 + h_{23}X_3 + Z_2 \\ h_{31}X_1 + Z_3 \end{bmatrix} \text{ and } S_2 = h_{12}X_2 + Z_1. \tag{64}$$

Therefore, results for the IS-IRC can be applied straightforwardly to the Gaussian case.

3

CONSTANT GAP RESULTS FOR A CLASS OF IRCs

We introduce the proposed outer bound and the two inner bounds in Sections 3.1 and 3.2, respectively. The constant gap results are shown in Section 3.3, while all proofs are relegated to the appendices.

3.1 OUTER BOUND

In this section, we develop an outer bound for the IS-IRC model described in Section 2.2. The model in Fig. 13 is provided to help the reader understand the genie-aided technique used in the derivation of the bounds. It would be worth to emphasize that this model by no means assumes that the relay has previous knowledge of any message nor that X_3 or Y_3 are collocated with X_1 or Y_2 as it could be wrongly interpreted based on the aforementioned figure.

Let $\mathcal{P}_1$ be the set of all joint PDs that can be factored as:

$$p(q)p(x_1x_3|q)p(x_2|q)p(\underline{v_1}v_2|x_1x_2x_3q), \tag{65}$$

where $p(\underline{v_1}v_2|x_1x_2x_3q) = p_{\underline{S_1}|X_1X_3}(\underline{v_1}|x_1x_3)p_{S_2|X_2}(v_2|x_2)$, i.e., $(\underline{V_1}V_2)$ is a conditionally independent copy of $(\underline{S_1}S_2)$ given $(X_1X_2X_3)$. Let us recall that V_1 represents the first component of $\underline{V_1}$.

Theorem 3.1 (outer bound). *Given a specific $P_1 \in \mathcal{P}_1$, let $\mathcal{R}_o(P_1)$ be the region of nonnegative rate pairs (R_1, R_2) satisfying*

$$R_1 \leq I(X_1; Y_1Y_3|X_2X_3Q), \tag{66a}$$
$$R_1 \leq I(X_1X_3; Y_1|X_2Q), \tag{66b}$$
$$R_2 \leq I(X_2; Y_2|X_1X_3Q), \tag{66c}$$
$$R_1 + R_2 \leq I(X_1X_3; Y_1|V_1X_2Q) + I(X_1X_2X_3; Y_2|Q), \tag{66d}$$
$$R_1 + R_2 \leq I(X_1X_2X_3; Y_1|V_1Q) + I(X_1X_2X_3; Y_2|V_2Q), \tag{66e}$$
$$R_1 + R_2 \leq I(X_1X_2X_3; Y_1|Q) + I(X_2; Y_2|X_1V_2X_3Q), \tag{66f}$$
$$R_1 + R_2 \leq I(X_1; Y_1Y_3|V_1X_2X_3Q) + I(X_1X_2X_3; Y_2|Q), \tag{66g}$$
$$R_1 + R_2 \leq I(X_1X_2; Y_1Y_3|V_1X_3Q) + I(X_1X_2X_3; Y_2|V_2Q), \tag{66h}$$
$$R_1 + R_2 \leq I(X_1X_2; Y_1Y_3|X_3Q) + I(X_2; Y_2|X_1V_2X_3Q), \tag{66i}$$
$$R_1 + R_2 \leq I(X_1; Y_1Y_3|\underline{V_1}X_2X_3Q) + I(X_1X_2; Y_2Y_3|X_3Q), \tag{66j}$$

$$R_1 + R_2 \leq I(X_1X_2; Y_1Y_3|\underline{V_1}X_3Q) + I(X_1X_2; Y_2Y_3|V_2X_3Q), \quad (66k)$$
$$2R_1 + R_2 \leq I(X_1X_3; Y_1|V_1X_2Q) + I(X_1X_2X_3; Y_1|Q) + I(X_1X_2X_3; Y_2|V_2Q), \quad (66l)$$
$$2R_1 + R_2 \leq I(X_1X_3; Y_1|V_1X_2Q) + I(X_1X_2; Y_1Y_3|X_3Q) + I(X_1X_2X_3; Y_2|V_2Q), \quad (66m)$$
$$2R_1 + R_2 \leq I(X_1; Y_1Y_3|V_1X_2X_3Q) + I(X_1X_2X_3; Y_1|Q) + I(X_1X_2X_3; Y_2|V_2Q), \quad (66n)$$
$$2R_1 + R_2 \leq I(X_1; Y_1Y_3|V_1X_2X_3Q) + I(X_1X_2; Y_1Y_3|X_3Q) + I(X_1X_2X_3; Y_2|V_2Q), \quad (66o)$$
$$2R_1 + R_2 \leq I(X_1; Y_1Y_3|\underline{V_1}X_2X_3Q) + I(X_1X_2X_3; Y_1|Q) + I(X_1X_2; Y_2Y_3|V_2X_3Q), \quad (66p)$$
$$2R_1 + R_2 \leq I(X_1; Y_1Y_3|\underline{V_1}X_2X_3Q) + I(X_1X_2; Y_1Y_3|X_3Q) + I(X_1X_2; Y_2Y_3|V_2X_3Q), \quad (66q)$$
$$R_1 + 2R_2 \leq I(X_1X_2X_3; Y_1|V_1Q) + I(X_2; Y_2|X_1V_2X_3Q) + I(X_1X_2X_3; Y_2|Q), \quad (66r)$$
$$R_1 + 2R_2 \leq I(X_1X_2; Y_1Y_3|V_1X_3Q) + I(X_2; Y_2|X_1V_2X_3Q) + I(X_1X_2X_3; Y_2|Q), \quad (66s)$$
$$R_1 + 2R_2 \leq I(X_1X_2; Y_1Y_3|\underline{V_1}X_3Q) + I(X_2; Y_2|X_1V_2X_3Q) + I(X_1X_2; Y_2Y_3|X_3Q). \quad (66t)$$

Then, an outer bound for the IS-IRC is defined by the union of $\mathcal{R}_o(P_1)$ over all joint PDs $P_1 \in \mathcal{P}_1$, as decomposed in (65).

Proof. See Appendix 3.A. □

The real Gaussian model, presented in Section 2.2, is a special case of the IS-IRC. Therefore, according to (65), the sources' inputs X_1 and X_2 are independent, and X_1 is arbitrarily correlated to the relay's input X_3, i.e., $\mathbb{E}[X_1X_2] = 0$, $\mathbb{E}[X_1X_3] = \rho\sqrt{P_1P_3}$, and $\mathbb{E}[X_2X_3] = 0$. The Gaussian expression of the outer bound is readily found using the model (63) and generating the auxiliaries $\underline{V_1}$ and V_2 according to (64), but with independent noises.

The foregoing Gaussian outer bound $\mathcal{R}_o = \bigcup_{\rho\in[-1,1]} \mathcal{R}_o(\rho)$ depends on the correlation coefficient ρ between X_1 and X_3 and, due to the large number of bounds, only a numerical maximization results viable. In order to obtain analytical expressions which can be used later to characterize the gap between inner and outer bounds, we establish an outer bound on $\mathcal{R}_o$. This outer bound is obtained by maximizing each individual rate constrain in $\mathcal{R}_o(\rho)$ independently.

Let us define any of the bounds in $\mathcal{R}_o(\rho)$ as $b(\rho)$ and $\rho_{\max}$ as the value that maximizes that particular bound. Then, it can be shown that $b(\rho_{\max}) = b(0)$ or $b(\rho_{\max}) \leq b(0) + \Delta$, where Δ is either 0.5 or 1 bit. Therefore, we can simplify the expressions in the outer bound and

avoid the maximization procedure if we use uncorrelated inputs and enlarge certain bounds, as we see in the following corollary. A similar observation has also been made in [25, Appendix A] and [27, (19)].

Corollary 3.1 (outer bound for the Gaussian case)**.** *An outer bound for the Gaussian IRC is given by the set of nonnegative rate pairs* (R_1, R_2) *satisfying*

$$R_1 \leq \mathsf{C}[S_{11} + S_{31}]\,, \tag{67a}$$

$$R_1 \leq \mathsf{C}[S_{11} + S_{13}] + \frac{1}{2}, \tag{67b}$$

$$R_2 \leq \mathsf{C}[S_{22}]\,, \tag{67c}$$

$$R_1 + R_2 \leq \mathsf{C}\left[\frac{S_{11}+S_{13}+\delta}{1+S_{21}+S_{23}}\right] + \mathsf{C}[S_{21}+S_{22}+S_{23}] + \frac{1}{2}, \tag{67d}$$

$$R_1 + R_2 \leq \mathsf{C}\left[S_{12} + \frac{S_{11}+S_{13}+\delta}{1+S_{21}+S_{23}}\right] + \mathsf{C}\left[S_{21} + S_{23} + \frac{S_{22}}{1+S_{12}}\right] + \frac{1}{2}, \tag{67e}$$

$$R_1 + R_2 \leq \mathsf{C}[S_{11} + S_{12} + S_{13}] + \mathsf{C}\left[\frac{S_{22}}{1+S_{12}}\right] + \frac{1}{2}, \tag{67f}$$

$$R_1 + R_2 \leq \mathsf{C}\left[\frac{S_{11} + S_{31}}{1+S_{21}}\right] + \mathsf{C}[S_{21} + S_{22} + S_{23}] + \frac{1}{2}, \tag{67g}$$

$$R_1 + R_2 \leq \mathsf{C}\left[S_{12} + \frac{S_{11}+S_{31}(1+S_{12})}{1+S_{21}}\right] + \mathsf{C}\left[S_{21} + S_{23} + \frac{S_{22}}{1+S_{12}}\right] + \frac{1}{2}, \tag{67h}$$

$$R_1 + R_2 \leq \mathsf{C}[S_{11} + S_{12} + S_{31}(1+S_{12})] + \mathsf{C}\left[\frac{S_{22}}{1+S_{12}}\right], \tag{67i}$$

$$R_1 + R_2 \leq \mathsf{C}\left[\frac{S_{11} + S_{31}}{1+S_{21}+S_{31}}\right] + \mathsf{C}[S_{21} + S_{22} + S_{31}(1+S_{22})]\,, \tag{67j}$$

$$R_1 + R_2 \leq \mathsf{C}\left[S_{12} + \frac{S_{11}+S_{31}(1+S_{12})}{1+S_{21}+S_{31}}\right] + \mathsf{C}\left[S_{21} + S_{31} + \frac{S_{22}(1+S_{31})}{1+S_{12}}\right], \tag{67k}$$

$$\begin{aligned} 2R_1 + R_2 \leq\ & \mathsf{C}\left[\frac{S_{11} + S_{13} + \delta}{1+S_{21}+S_{23}}\right] + \mathsf{C}\left[S_{21} + S_{23} + \frac{S_{22}}{1+S_{12}}\right] \\ & + \mathsf{C}[S_{11} + S_{12} + S_{13}] + 1, \end{aligned} \tag{67l}$$

$$\begin{aligned} 2R_1 + R_2 \leq\ & \mathsf{C}\left[\frac{S_{11} + S_{13} + \delta}{1+S_{21}+S_{23}}\right] + \mathsf{C}\left[S_{21} + S_{23} + \frac{S_{22}}{1+S_{12}}\right] \\ & + \mathsf{C}[S_{11} + S_{12} + S_{31}(1+S_{12})] + \frac{1}{2}, \end{aligned} \tag{67m}$$

$$\begin{aligned} 2R_1 + R_2 \leq\ & \mathsf{C}\left[\frac{S_{11}+S_{31}}{1+S_{21}}\right] + \mathsf{C}[S_{11}+S_{12}+S_{13}] + \mathsf{C}\left[S_{21}+S_{23}+\frac{S_{22}}{1+S_{12}}\right] \\ & + 1, \end{aligned} \tag{67n}$$

$$2R_1+R_2 \leq \mathsf{C}\left[\frac{S_{11}+S_{31}}{1+S_{21}}\right]+\mathsf{C}[S_{11}+S_{12}+S_{31}(1+S_{12})] + \mathsf{C}\left[S_{21}+S_{23}+\frac{S_{22}}{1+S_{12}}\right]+\frac{1}{2}, \tag{67o}$$

$$2R_1+R_2 \leq \mathsf{C}\left[\frac{S_{11}+S_{31}}{1+S_{21}+S_{31}}\right]+\mathsf{C}[S_{11}+S_{12}+S_{13}] + \mathsf{C}\left[S_{21}+S_{31}+\frac{S_{22}(1+S_{31})}{1+S_{12}}\right]+\frac{1}{2}, \tag{67p}$$

$$2R_1+R_2 \leq \mathsf{C}\left[\frac{S_{11}+S_{31}}{1+S_{21}+S_{31}}\right]+\mathsf{C}[S_{11}+S_{12}+S_{31}(1+S_{12})] + \mathsf{C}\left[S_{21}+S_{31}+\frac{S_{22}(1+S_{31})}{1+S_{12}}\right], \tag{67q}$$

$$R_1+2R_2 \leq \mathsf{C}\left[S_{12}+\frac{S_{11}+S_{13}+\delta}{1+S_{21}+S_{23}}\right]+\mathsf{C}\left[\frac{S_{22}}{1+S_{12}}\right] + \mathsf{C}[S_{21}+S_{22}+S_{23}]+\frac{1}{2}, \tag{67r}$$

$$R_1+2R_2 \leq \mathsf{C}\left[S_{12}+\frac{S_{11}+S_{31}(1+S_{12})}{1+S_{21}}\right]+\mathsf{C}\left[\frac{S_{22}}{1+S_{12}}\right] + \mathsf{C}[S_{21}+S_{22}+S_{23}]+\frac{1}{2}, \tag{67s}$$

$$R_1+2R_2 \leq \mathsf{C}\left[S_{12}+\frac{S_{11}+S_{31}(1+S_{12})}{1+S_{21}+S_{31}}\right]+\mathsf{C}\left[\frac{S_{22}}{1+S_{12}}\right] + \mathsf{C}[S_{21}+S_{22}+S_{31}(1+S_{22})], \tag{67t}$$

where $\delta \triangleq \left(\sqrt{S_{11}S_{23}} \pm \sqrt{S_{13}S_{21}}\right)^2$.

Proof. See Appendix 3.B. □

Remark 3.1. *If we define the following matrices,*

$$\boldsymbol{H} = \begin{bmatrix} h_{11} & h_{13} \\ h_{21} & h_{23} \end{bmatrix} \text{ and } \boldsymbol{Q} = \frac{1}{\sqrt{N_1 N_2}} \begin{bmatrix} P_1 & 0 \\ 0 & P_3 \end{bmatrix},$$

we readily see that $\delta = \det(\boldsymbol{H}\boldsymbol{Q}\boldsymbol{H}^T)$. *Thus, the sign in the expression* δ *depends on the sign of the channel coefficients. If there is an even number of negative coefficients in* $\boldsymbol{H}$, *then* $\delta = \left(\sqrt{S_{11}S_{23}} - \sqrt{S_{13}S_{21}}\right)^2$, *otherwise* $\delta = \left(\sqrt{S_{11}S_{23}} + \sqrt{S_{13}S_{21}}\right)^2$.

Remark 3.2. *In the strong interference regime, where each receiver can decode the interfering message completely without restricting its rate, tighter outer bounds can be derived, similarly to the IC under strong interference [1, Remark 6.9]. The sum-rates in the capacity regions under strong interference [28, Thm. 5] and [31, Thm. 2], the former with the assumption of a potent relay, i.e.,* $P_3 \to \infty$, *are tighter than the ones presented here, namely* (67i), (67j), (66d), (66f), *and* (66g).

Remark 3.3. *Outer bound sum-rates using genie-aided techniques are given in [28, Thm. 4] and [31, Thm. 4], the former extending the "useful" and "smart" genie from [46] while the latter using Kramer's approach [47].*

As it is shown in [46], the "smart" genie provides an outer bound that is tighter than Etkin et al.*'s [19] under weak interference, thus, the sum-rate [28, Thm. 4] is tighter than the analogous in our region, namely,* (67k)*. Additionally, the optimization of parameters in the sum-rate [31, Thm. 4] can potentially give tight bounds. For example, if* $d_1 = h_{21}$, $d_2 = d_3 = 0$, $d_4 = \sqrt{N_2}$, *and* $d_5 = h_{23}$ *the genie signal* Y_{1g} *becomes* $V_1 = h_{21}X_1 + h_{23}X_3 + Z_2'$ *and it is easy to verify that the sum-rate [31, Thm. 4] is tighter than* (66e)*.*

3.2 INNER BOUNDS

In the following, we provide two inner bounds corresponding to two different relaying strategies, namely, DF and CF. With DF, the relay decodes the message from the only connected source (partially or completely), re-encodes it, and transmits it to both destinations. With CF, the relay compresses the received signal, and sends a compression index associated to it. A previous version of these schemes was presented in [4], but here we show a more compact expression for the CF scheme and a completely new and improved version for the DF scheme. Four main ingredients are required: rate-splitting, binning, and block Markov coding at the sources, and backward decoding at the destinations. In the sequel, we assume the indices $(k, l) \in \{(1, 2), (2, 1)\}$.

In every strategy, to allow cooperation from the relay, the transmission is split in several blocks. During block j, each source k divides its message $\tilde{m}_{kj}$ into two short messages: a common part m_{kj} and a private part w_{kj}. As in the HK scheme, each receiver decodes the common part of the interfering message, hence reducing the interference.

The use of DF and CF schemes for IRCs is well-known [20, 28–31], however, our goal is to derive *simple* but powerful enough strategies in order to characterize the capacity region of the IRC within a *constant gap*. The biggest obstacle to obtaining an inner bound with a manageable number of inequalities is the use of a relaying strategy jointly with rate-splitting to deal with interference. This issue may be overcome by assuming some special condition in the model, e.g., symmetric channels [20, 29] or strong interference [31], or by employing successive decoding of codewords instead of joint-decoding [28, 29]. However, we do not want to rely on these assumptions here.

Additionally, the proposed schemes have some key differences with respect to the literature. In the DF scheme, the amount of information decoded by the relay is optimized separately from the rate-splitting

used to deal with interference, which can potentially improve the achievable rates. Moreover, the CF scheme presented in Section 3.2.2 does not force both receivers to decode the compression index, unlike [28, 30], which could reduce the performance of the scheme if there is a large asymmetry among the channels.

Remark 3.4. *The inner bounds stated below apply to general memoryless IRCs and thus they are not limited to the IS-IRC.*

3.2.1 *Decode-and-Forward*

Each source sends b messages during $b+1$ time blocks, and the relay forwards in block j what it has decoded from the first source in the previous block. In this scheme, the *private* message of the first source is split into two parts and the relay only decodes and retransmits one of them (plus the *common* message). At the end of transmission, receiver k decodes backwardly the private message w_{kj} as well as both common messages m_{kj} and m_{lj}.

Let $\mathcal{P}_2$ be the set of PDs that factor as

$$p(q)p(x_1x_3|q)p(x_2|q)p(v_1|x_1x_3q)p(u_1|x_1q)p(v_2|x_2q)p(v_3|x_3q). \quad (68)$$

Theorem 3.2 (partial DF scheme). *Given a $P_2 \in \mathcal{P}_2$, let $\mathcal{R}_{p\text{-}DF}(P_2)$ be the region of nonnegative rate pairs (R_1, R_2) satisfying*

$$\begin{aligned}
R_1 &\le I(U_1;Y_3|X_3Q) + I(X_1;Y_1|V_1U_1V_2X_3Q), && (69a)\\
R_1 &\le I(X_1X_3;Y_1|V_2Q), && (69b)\\
R_2 &\le I(X_2;Y_2|V_1V_3Q), && (69c)\\
R_2 &\le I(V_1X_2V_3;Y_2|Q) - I_b, && (69d)\\
R_1+R_2 &\le I(X_1X_3;Y_1|V_1V_2V_3Q) + I(V_1X_2V_3;Y_2|Q), && (69e)\\
R_1+R_2 &\le I(U_1;Y_3|V_1X_3Q) + I(X_1;Y_1|V_1U_1V_2X_3Q)\\
&\quad + I(V_1X_2V_3;Y_2|Q) - I_b, && (69f)\\
R_1+R_2 &\le I(X_1V_2X_3;Y_1|V_1V_3Q) + I(V_1X_2V_3;Y_2|V_2Q), && (69g)\\
R_1+R_2 &\le I(U_1;Y_3|V_1X_3Q) + I(X_1V_2;Y_1|V_1U_1X_3Q)\\
&\quad + I(V_1X_2V_3;Y_2|V_2Q) - I_b, && (69h)\\
R_1+R_2 &\le I(X_1V_2X_3;Y_1|Q) + I(V_1X_2V_3;Y_2|V_2Q) - I_b, && (69i)\\
R_1+R_2 &\le I(X_1V_2X_3;Y_1|Q) + I(X_2;Y_2|V_1V_2V_3Q), && (69j)\\
R_1+R_2 &\le I(U_1;Y_3|X_3Q) + I(X_1V_2;Y_1|V_1U_1X_3Q)\\
&\quad + I(X_2;Y_2|V_1V_2V_3Q), && (69k)\\
2R_1+R_2 &\le I(X_1X_3;Y_1|V_1V_2V_3Q) + I(X_1V_2X_3;Y_1|Q)\\
&\quad + I(V_1X_2V_3;Y_2|V_2Q), && (69l)
\end{aligned}$$

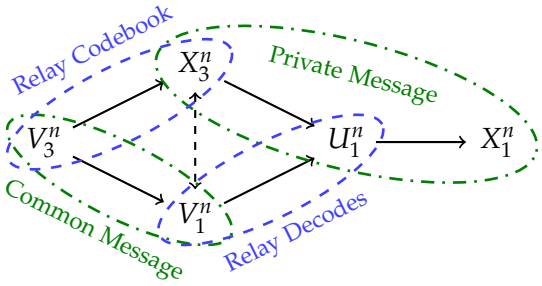


Figure 14.: Codewords of the relay and the first source. Solid arrows denote superimposed codewords while dashed arrows denote binning.

$$
\begin{aligned}
2R_1 + R_2 \leq\ & I(X_1X_3; Y_1|V_1V_2V_3Q) + I(X_1V_2; Y_1|V_1U_1X_3Q) \\
& + I(U_1; Y_3|X_3Q) + I(V_1X_2V_3; Y_2|V_2Q), && \text{(69m)} \\
2R_1 + R_2 \leq\ & I(U_1; Y_3|V_1X_3Q) + I(X_1; Y_1|V_1U_1V_2X_3Q) - I_b \\
& + I(X_1V_2X_3; Y_1|Q) + I(V_1X_2V_3; Y_2|V_2Q), && \text{(69n)} \\
R_1 + 2R_2 \leq\ & I(X_1V_2X_3; Y_1|V_1V_3Q) + I(X_2; Y_2|V_1V_2V_3Q) \\
& + I(V_1X_2V_3; Y_2|Q), && \text{(69o)} \\
R_1 + 2R_2 \leq\ & I(U_1; Y_3|V_1X_3Q) + I(X_1V_2; Y_1|V_1U_1X_3Q) - I_b \\
& + I(X_2; Y_2|V_1V_2V_3Q) + I(V_1X_2V_3; Y_2|Q) && \text{(69p)}
\end{aligned}
$$

where $I_b \triangleq I(X_3; V_1|V_3Q)$. *Then, an achievable region for the IRC is defined by the union of all rate pairs in* $\mathcal{R}_{\text{p-DF}}(P_2)$ *over all joint PDs* $P_2 \in \mathcal{P}_2$, *as defined in* (68).

Proof. The codewords V_2^n and X_2^n convey the common and full messages of the second source, respectively, with X_2^n superimposed over V_2^n. This representation follows the steps proposed in [48], due to its simplicity compared to [15], though both representations are equivalent [49].

The codebook of the first source, however, is much more involved in order to allow the relay to cooperate, see Fig. 14. The scheme forces the relay to decode the common message of the first source, i.e., the codeword V_1^n, entirely but only a part of the private message. Thus, unlike the second source, an intermediate layer U_1^n is included between V_1^n and X_1^n.

The indices decoded by the relay are forwarded through superimposed codewords V_3^n and X_3^n, analogous to V_1^n and U_1^n. Coherent cooperation is achieved by superimposing V_1^n and U_1^n over V_3^n and X_3^n, respectively. An additional binning step between the codewords V_1^n and X_3^n is required to comply with (68), thus the negative term I_b in (69).

The region $\mathcal{R}_{\text{p-DF}}$ (69) is strictly smaller than the actual partial DF region since we have reduced all the bounds with $I(V_1U_1; Y_3|X_3)$ into

$I(U_1; Y_3|X_3)$ on purpose, namely, (69a), (69k), and (69m), in order to have a more compact expression of the whole region. See Appendix 3.C for details. □

If the relay is able to decode the private message of the first source completely without imposing a restriction on the achievable rate, the maximization of the previous inner bound would result in $U_1 = X_1$. In this case, let $\mathcal{P}_3$ be the set of PDs which factor as

$$p(q)p(x_1x_3|q)p(x_2|q)p(v_1|x_1x_3q)p(v_2|x_2q)p(v_3|x_3q). \tag{70}$$

Corollary 3.2 (full DF scheme). *Given a $P_3 \in \mathcal{P}_3$, let $\mathcal{R}_{f\text{-}DF}(P_3)$ be the region of nonnegative rate pairs (R_1, R_2) satisfying*

$$\begin{aligned}
R_1 &\le I(X_1; Y_3|X_3Q), && \text{(71a)}\\
R_1 &\le I(X_1X_3; Y_1|V_2Q), && \text{(71b)}\\
R_2 &\le I(X_2; Y_2|V_1V_3Q), && \text{(71c)}\\
R_2 &\le I(V_1X_2V_3; Y_2|Q) - I_b, && \text{(71d)}\\
R_1 + R_2 &\le I(X_1X_3; Y_1|V_1V_2V_3Q) + I(V_1X_2V_3; Y_2|Q), && \text{(71e)}\\
R_1 + R_2 &\le I(X_1; Y_3|V_1X_3Q) + I(V_1X_2V_3; Y_2|Q) - I_b, && \text{(71f)}\\
R_1 + R_2 &\le I(X_1V_2X_3; Y_1|V_1V_3Q) + I(V_1X_2V_3; Y_2|V_2Q), && \text{(71g)}\\
R_1 + R_2 &\le I(X_1V_2X_3; Y_1|Q) + I(V_1X_2V_3; Y_2|V_2Q) - I_b, && \text{(71h)}\\
R_1 + R_2 &\le I(X_1V_2X_3; Y_1|Q) + I(X_2; Y_2|V_1V_2V_3Q), && \text{(71i)}\\
2R_1 + R_2 &\le I(X_1X_3; Y_1|V_1V_2V_3Q) + I(X_1V_2X_3; Y_1|Q)\\
&\quad + I(V_1X_2V_3; Y_2|V_2Q), && \text{(71j)}\\
2R_1 + R_2 &\le I(X_1; Y_3|V_1X_3Q) + I(X_1V_2X_3; Y_1|Q)\\
&\quad + I(V_1X_2V_3; Y_2|V_2Q) - I_b, && \text{(71k)}\\
R_1 + 2R_2 &\le I(X_1V_2X_3; Y_1|V_1V_3Q) + I(X_2; Y_2|V_1V_2V_3Q)\\
&\quad + I(V_1X_2V_3; Y_2|Q) && \text{(71l)}
\end{aligned}$$

where $I_b \triangleq I(X_3; V_1|V_3Q)$. Then, an achievable region for the IRC is defined by the union of all rate pairs in $\mathcal{R}_{f\text{-}DF}(P_3)$ over all joint PDs $P_3 \in \mathcal{P}_3$, as defined in (70).

Proof. The region $\mathcal{R}_{\text{f-DF}}$ (71) is not obtained by setting $U_1 = X_1$ in $\mathcal{R}_{\text{p-DF}}$ (69), since some additional redundant bounds remain. To easily eliminate these bounds, one should replace U_1 with X_1 in the set of partial rates before applying Fourier-Motzkin elimination (FME) in the proof of Theorem 3.2. See Appendix 3.D for details. □

The keen reader can see the resemblance between the region $\mathcal{R}_{\text{f-DF}}$ (71) and the HK region (Theorem 1.5), with the addition of bounds regarding the decoding at the relay or the presence of binning.

Remark 3.5. *The capacity of the* physically degraded *IRC in the* strong interference *regime [31, Thm. 3] is achieved by the full DF scheme.*

The choice of variables $V_k = X_k$ for $k \in [1:3]$ eliminates the private messages and renders the binning process unnecessary. Then, by using the strong interference condition $I(X_1X_3;Y_1|X_2) \leq I(X_1X_3;Y_2|X_2)$, the full DF inner bound becomes

$$R_1 \leq I(X_1;Y_3|X_3Q), \tag{72a}$$
$$R_1 \leq I(X_1X_3;Y_1|X_2Q), \tag{72b}$$
$$R_2 \leq I(X_2;Y_2|X_1X_3Q), \tag{72c}$$
$$R_1 + R_2 \leq I(X_1X_2X_3;Y_1|Q), \tag{72d}$$
$$R_1 + R_2 \leq I(X_1X_2X_3;Y_2|Q). \tag{72e}$$

The region (72) coincides with the outer bound [31, Thm. 2] by choosing $U_1 = X_3$ and $U_2 = X_2$, and considering that

1. *the relay is only able to observe the first source, i.e., $p(y_3|x_1x_2x_3) = p(y_3|x_1x_3)$, and*
2. *the IRC is physically degraded, i.e., the Markov chain $(X_1X_2) \multimap (X_3Y_3) \multimap (Y_1Y_2)$ holds.*

In the full DF scheme, since the relay decodes the codeword X_1^n completely, there is no limit in the amount of information that can be sent as common message. However, in the partial DF scheme, we are introducing the variable U_1 between X_1 and V_1, effectively prohibiting $V_1 = X_1$. Therefore, the structure of the codebook imposes that the relay should be in a better condition to decode the common message V_1^n than the second destination. If that is not the case, we should employ the CF scheme presented in the following section.

3.2.2 *Compress-and-Forward*

In this scheme, the relay does not decode any message and it only sends a compressed version of its channel output. The destinations jointly decode this information with their message and the common layer of the interference. Transmission takes place in $b + b_s$ time blocks, similarly to [6, 7], and during the last b_s blocks, the relay repeats its message to assure a correct decoding at both destinations.

Let $\mathcal{P}_4$ be the set of PDs that factor as

$$p(q)p(v_1x_1|q)p(v_2x_2|q)p(x_3|q)p(\hat{y}_3|x_3y_3q), \tag{73}$$

and let us define the following set of expressions

$$I_{k1} \triangleq \min\{I(X_k;Y_k\hat{Y}_3|V_kV_lX_3Q), I(X_kX_3;Y_k|V_kV_lQ) - I_k\}, \tag{74a}$$
$$I_{k2} \triangleq \min\{I(X_k;Y_k\hat{Y}_3|V_lX_3Q), I(X_kX_3;Y_k|V_lQ) - I_k\}, \tag{74b}$$
$$I_{k3} \triangleq \min\{I(X_kV_l;Y_k\hat{Y}_3|V_kX_3Q), I(X_kV_lX_3;Y_k|V_kQ) - I_k\}, \tag{74c}$$
$$I_{k4} \triangleq \min\{I(X_kV_l;Y_k\hat{Y}_3|X_3Q), I(X_kV_lX_3;Y_k|Q) - I_k\} \tag{74d}$$

where $I_k \triangleq I(\hat{Y}_3; Y_3|X_k V_l X_3 Y_k Q)$ and

$$I'_{k1} \triangleq I(X_k; Y_k|V_k V_l Q), \tag{75a}$$
$$I'_{k2} \triangleq I(X_k; Y_k|V_l Q), \tag{75b}$$
$$I'_{k3} \triangleq I(X_k V_l; Y_k|V_k Q), \tag{75c}$$
$$I'_{k4} \triangleq I(X_k V_l; Y_k|Q). \tag{75d}$$

Theorem 3.3 (CF scheme). *Given a specific $P_4 \in \mathcal{P}_4$, let $\mathcal{R}_{CF_0}(P_4)$ be the region of nonnegative rate pairs (R_1, R_2) that satisfy*

$$R_k \leq I_{k2}, \tag{76a}$$
$$R_k + R_l \leq \min\{I_{k1} + I_{l4}, I_{k3} + I_{l3}\}, \tag{76b}$$
$$2R_k + R_l \leq I_{k1} + I_{k4} + I_{l3}, \tag{76c}$$

and $\mathcal{R}_{CF_k}(P_4)$ defined by

$$R_k \leq I_{k2}, \tag{77a}$$
$$R_l \leq I'_{l2}, \tag{77b}$$
$$R_k + R_l \leq \min\{I_{k1} + I'_{l4}, I_{k4} + I'_{l1}, I_{k3} + I'_{l3}\}, \tag{77c}$$
$$2R_k + R_l \leq I_{k1} + I_{k4} + I'_{l3}, \tag{77d}$$
$$R_k + 2R_l \leq I_{k3} + I'_{l1} + I'_{l4}. \tag{77e}$$

An achievable region for the IRC is defined by the union of $\mathcal{R}_{CF_0}(P_4) \cup \mathcal{R}_{CF_1}(P_4) \cup \mathcal{R}_{CF_2}(P_4)$ over all joint PDs $P_4 \in \mathcal{P}_4$, as defined in (73).

Proof. Since the relay does not decode any message, the codewords V_k^n and X_k^n carry the common and full message of the present block, respectively. The variable X_3 is independent of the sources' signals and is used to reconstruct the relay's observation Y_3.

Each expression I_{ki} resembles the CF inner bound for the relay channel, and when the relay is ignored it reduces to the expression I'_{ki}. The region $\mathcal{R}_{\text{CF}_0}$ (76) is obtained when both destinations decode the compression index whereas in region $\mathcal{R}_{\text{CF}_k}$ (77) only destination k decodes it.

Since the compression index is sent via block Markov coding, each destination needs to assure its correct decoding in each block, which results in additional bounds not shown here. However, the union $\mathcal{R}_{\text{CF}_0} \cup \mathcal{R}_{\text{CF}_1} \cup \mathcal{R}_{\text{CF}_2}$ after the maximization over all joint PDs provides that these bounds are redundant. See Appendix 3.E for details. □

Remark 3.6. *The relay only generates one compression index that is decodable by both destinations, i.e., the compression rate is determined by the worst channel. It is possible, however, to improve the performance with successive refinement that is not used here because of its complexity. As we shall see in the next section, two layers of successive refinement are not needed as far as the constant gap is concerned.*

	$S_{31} < S_{21}$	$S_{31} \geq S_{21}$
$S_{31} < S_{11}$	CF	partial DF
$S_{31} \geq S_{11}$	full DF	

Table 6.: SNR regimes and corresponding best constant-gap strategies.

SNR regime		CF	DF
$S_{31} < S_{21}$	$S_{31} < S_{11}$	1.32	–
	$S_{31} \geq S_{11}$	1.32	1
$S_{31} \geq S_{21}$	$S_{31} \geq S_{11}$	–	1
	$S_{31} < S_{11}$	–	1.5

Table 7.: Maximum gap in bits of each scheme for each SNR regime.

Remark 3.7. *If both users ignore the compression index, this strategy reduces to the HK scheme, a special case of $\mathcal{R}_{CF_0}$. Additionally, $\mathcal{R}_{CF_0}$ is equal to the extension of NNC [30, Thm. 1] for one relay, i.e., $N = 1$.*

Remark 3.8. *The region $\mathcal{R}_{CF_0}$ contains both the CF and GCF schemes presented in [28, Thm. 1 and 2]. It is easy to see that the bounds on the partial rates of the first scheme [28, (5)–(8)] are below (74) if we relax the constraint [28, (9)] to $I(X_3; Y_k) \geq I(Y_3; \hat{Y}_3 | X_3 Y_k)$ with $k \in \{1, 2\}$. Additionally, relaxing R_0 in [28, Thm. 2], shows that GCF_1 is equal to $\mathcal{R}_{CF_0}$ with $V_1 = V_2 = \emptyset$ and GCF_2 is equal to $\mathcal{R}_{CF_0}$ with $V_1 = X_1$ and $V_2 = X_2$. Therefore, the capacity results [28, Thm. 4 and 5] are achieved by the proposed CF scheme.*

3.3 CONSTANT GAP RESULTS & DISCUSSION

In this section, we evaluate the gap between the achievable regions and the outer bound in the Gaussian case (Fig. 11). Then, we identify the strategies that achieve the best constant gap to the capacity region for any SNR value. This is summarized in Table 6, while the value of the gap for each strategy is shown in Table 7.

3.3.1 *DF Scheme Achieves Capacity Within 1.5 Bits*

Table 7 shows two different constant-gap values for this scheme, 1.5 bits being the largest. The difference comes from the choice of input PD used in the inner bound as we see next.

When the relay is close to the source, i.e., when S_{31} is high enough, the relay is able to decode the entire message without penalizing the rate R_1. Therefore, as mentioned in Section 3.2.1, the input PD verifies $U_1 = X_1$ and the inner bound is found in Corollary 3.2.

Proposition 3.1. *If $S_{31} \geq S_{11}$, the full DF scheme presented in Corollary 3.2 achieves capacity to within 1 bit.*

Proof. The mentioned constant gap is quite conservative in the majority of cases since it arises from choosing a fixed input PD for the inner bound (which reduces the achievable rate) and using the loose outer bound from Corollary 3.1. See Appendix 3.F for details. □

Remark 3.9. *The capacity result in [31, Thm. 3] is contained in this regime. This capacity result, which is valid for general memoryless channels, relies on three conditions, namely,*

1. *the relay can only observe one source signal;*
2. *the IRC is* physically degraded, *i.e.,* $(X_1X_2) \multimap (X_3Y_3) \multimap (Y_1Y_2)$*; and,*
3. *the IRC is under the* strong interference *regime, i.e.,* $I(X_kX_3; Y_k|X_l) \leq I(X_kX_3; Y_l|X_l)$.

The IRC model (61) used in this work only verifies the first condition. However, if we further assume that the conditions of physically degradedness and strong interference hold, the full DF scheme presented in Corollary 3.2 also achieves capacity (see Remark 3.5). As we see next, the lack of these two assumptions imposes the 1-bit gap.

First, our Gaussian model (63) does not admit any kind of degradedness, however, if $S_{31} \geq S_{11}$, we can bound the corresponding term by 0.5 bits, as in (130),

$$I(X_1; Y_1|X_2X_3Y_3Q) = \mathsf{C}\left[\frac{S_{11}}{1+S_{31}}\right] \leq \frac{1}{2}.$$

Second, the strong interference condition renders the rate-splitting useless, since both encoders send only common messages, and allows the development of a tighter outer bound, similar to the IC with strong interference [1, Remark 6.9]. Without common messages, not only the binning term I_b disappears but also the simplifications made in Appendix 3.F, namely the choice of auxiliary RVs (127) and the uncorrelation between X_1 and X_3, can be dropped. For example, as seen in Appendix 3.F, the choice of auxiliaries (127) inflicts half a bit of gap in (131) and (132), while another half a bit of gap is due to the uncorrelation between X_1 and X_3 in (131) and due to the binning term I_b in (132).

Therefore, the 1-bit gap the full DF scheme presents in contrast to the capacity-achieving scheme of [31] comes from the last two conditions, which are not assumed by our model.

If the source-to-relay link is not good enough for the relay to decode the entire message, the relay should decode it partially, i.e., $U_1 \neq X_1$. However, due to the structure of the codebook, the relay should still be able to decode the common message.

Proposition 3.2. *If $S_{31} \geq S_{21}$, the partial DF scheme presented in Theorem 3.2 achieves capacity to within 1.5 bits.*

Proof. Similarly to the proof of Proposition 3.1, we reduce the inner bound by fixing the input PD and enlarge the outer bound by choosing a subset of bounds from it. See Appendix 3.G for details. □

Remark 3.10. *The gap between the original expression in the inner bound, $I(V_1U_1; Y_3|X_3Q)$, and the one used to compact the region, $I(U_1; Y_3|X_3Q)$, is 0.5 bit at most with the choice of auxiliaries (127) and (133) used in Appendix 3.G. This is the cause of the larger gap for the partial DF scheme.*

Remark 3.11. *If $S_{31} \geq S_{11}$ and $S_{31} \geq S_{21}$ the DF scheme, full or partial, achieves a constant gap to capacity. Nonetheless, this regime appears in Table 6 as "full DF" since its gap is smaller.*

3.3.2 *CF Scheme Achieves Capacity Within 1.32 Bits*

The CF scheme does not impose any condition on the sources' codebook structure, nonetheless, a constant gap could only be found in the regime $S_{31} \leq S_{21}$.

Proposition 3.3. *If $S_{31} \leq S_{21}$ the CF scheme presented in Theorem 3.3 achieves capacity to within 1.32 bits.*

Proof. The proof follows similar steps as the previous ones. See Appendix 3.H for details. □

3.3.3 *Limited Relaying Benefit*

It sounds reasonable that for a really low SNR in the source-to-relay link, the use of relaying has limited benefit. In this case, it might be preferable, due to complexity, to shut the relay down and fall back to the much simpler HK scheme for the IC.

Proposition 3.4. *If $S_{31} \leq S_{11}/(1+S_{12})$ and $S_{31} \leq S_{21}/(1+S_{22})$, the HK scheme (without relay) achieves the capacity of the IS-IRC within 1 bit, i.e., relaying does not improve the achievable rate in more than 1 bit.*

Proof. See Appendix 3.I. □

The two conditions over the source-to-relay link presented above can be interpreted as follows. In the first case, $S_{31} \leq S_{11}/(1+S_{12})$ implies that, by treating the interference from source 2 as noise, destination 1 can still have a better observation on source 1's signal than the relay does. Therefore, the relay's observation cannot help much for destination 1 to decode its own signal.

On the other hand, $S_{31} \leq S_{21}/(1+S_{22})$ implies that, by treating its own signal as noise, destination 2 can still have a better observation on source 1's signal than the relay does. Therefore, the relay's observation cannot help much for destination 2 to learn/decode the interference from source 1.

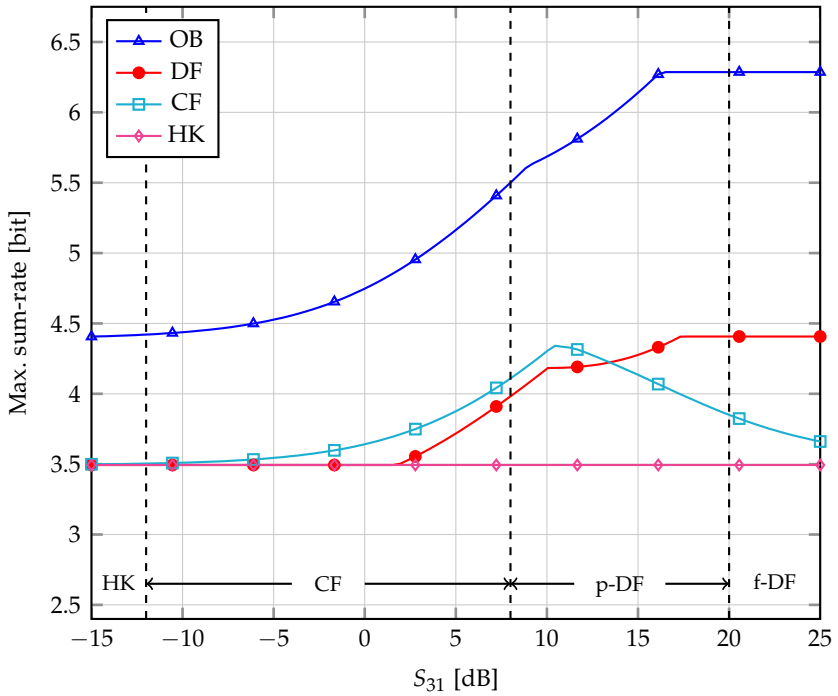
3·3·4 *Numerical Example*

To illustrate the regimes described before, we plot the maximum attainable sum-rate for the outer bound and each inner bound in Fig. 15a. Additionally, we delimit each regime with vertical dashed lines and we add the HK scheme as a means of comparison. The SNR of each link in the channel remains fixed while we vary the SNR of the source-to-relay link S_{31}.

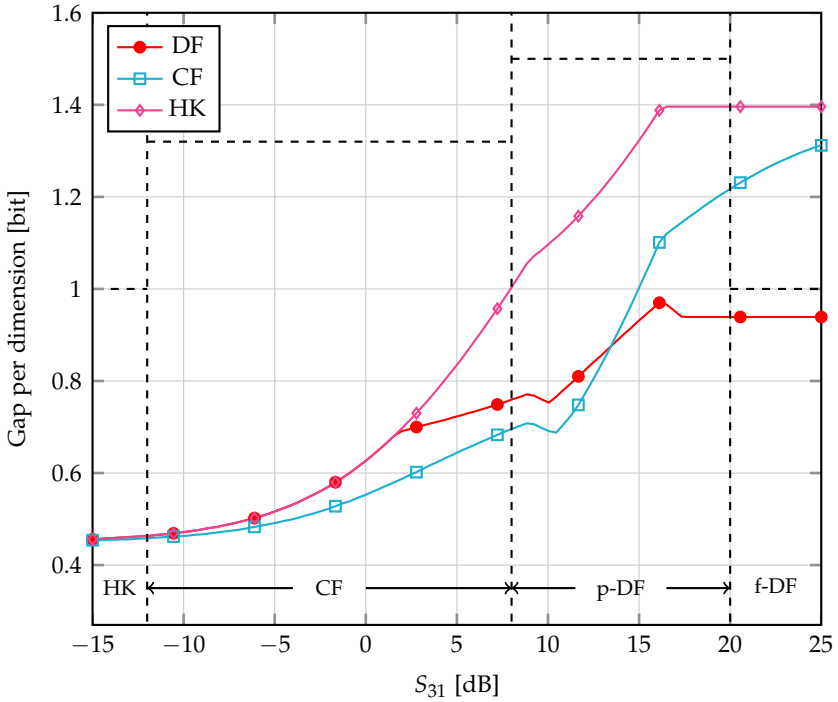
All the inner bounds present in the figure are the simplified versions used in the computation of the gap, i.e., there is no maximization of the PDs employed in them. The curve labeled DF is the maximum achievable rate attained by either the simplified inner bound of Proposition 3.1 or 3.2, or the HK inner bound (in the case the relay is turned-off); the reader should refer to the appropriate appendix for details. The HK inner bound is not optimized either since we use the auxiliaries proposed in [5], but this is needed to make a fair comparison with our schemes. Moreover, Corollary 3.1 is the outer bound used in here.

We see that when the source-to-relay link is strong DF outperforms CF, namely in the regime labeled "f-DF", i.e., when $S_{31} \geq S_{11}$. As the quality of this link degrades, CF achieves higher rates and eventually surpasses DF, mainly in the "CF" regime, i.e., when $S_{31} < S_{21}$. Below certain threshold in the quality of the source-to-relay link, the DF scheme even collapses to the HK scheme. The cause of this might lie in the numerous simplifications made. However, due to the many auxiliary RVs present in the scheme, we did not carry out an extensive optimization of the scheme to prove this conjecture. Finally, when the source-to-relay link is really weak, CF performs as good as the HK scheme. This regime, denoted "HK" in the figure, is the one from Preposition 3.4.

Another way of analyzing these curves is by looking at the gap per dimension, as in Fig. 15b. Here, the maximum theoretical gap in each regime is represented by horizontal dashed lines, and we see that they hold.



(a) Maximum attainable sum-rate



(b) Gap per dimension

Figure 15.: Performance analysis for the Gaussian IRC (Fig. 11) with the following fixed SNRs: $S_{11} = S_{22} = 20$dB, $S_{12} = S_{21} = 8$dB, $S_{13} = S_{23} = 20$dB.

3·4 SUMMARY AND CONCLUDING REMARKS

We derived a novel outer bound and two inner bounds for a class of IRCs where the relay can only observe one of the sources. These bounds allowed us to identify the main SNR regimes of interest, and for them, we found the adequate relaying strategies that achieve capacity of the Gaussian IRC within a constant gap regardless of the channel parameters.

While the proposed inner and outer bounds suggest the existence of different SNR regimes for the Gaussian IRC, in which different coding strategies are needed to achieve a constant gap to capacity, whether there exists a single coding scheme that achieves the constant gap in all SNR regimes is still an open question. In other words, there may be ways to improve the outer bound, the inner bounds, or both, which remains an interesting future work.

Additionally, the general IRC where the relay observes both sources is not an straightforward extension of our work. The central difficulty lies in the way of modeling the interference signals used in the injective semideterministic model and hence the derivation of an adequate outer bound. Since in the general IRC X_3 can be arbitrarily correlated to both X_1 and X_2, the interference signal S_k is no longer independent of the input X_l, with $(k,l) \in \{(1,2),(2,1)\}$. This, in turn, forbids us from single-letterizing the outer bound the way we did. A new technique to derive outer bounds for this problem is therefore needed, which also remains as future work.

APPENDIX

3.A PROOF OF THEOREM 3.1 (OUTER BOUND)

The proof follows by using a similar approach to that developed in [5] and it was partially presented in [4, 50]. As explained before, the inputs X_1 and X_3 are arbitrarily correlated and they are independent of X_2. Since we are not considering noise correlation in the outputs, the interference signals $\underline{S_1}$ and S_2 are therefore independent.

First, let us recall that the inputs X_1^n and X_2^n are functions of the messages $\tilde{m}_1$ and $\tilde{m}_2$, each one independent of the other, and the relay's input is a deterministic function of its past observations, i.e., $X_{3i} = \phi_i(Y_3^{i-1})$, $i \in [1:n]$. Then, we add two new RVs $\underline{V_1}^n$ and V_2^n, which are obtained by passing X_1^n, X_2^n and X_3^n through the memoryless channel $p_{\underline{S_1}|X_1X_3}p_{S_2|X_2}$.

A multi-letter outer bound on each rate can be derived using Fano's inequality, i.e.,

$$n(R_k - \epsilon_n) \leq I(X_k^n; Y_k^n),$$

where ϵ_n denotes a sequence such that $\epsilon_n \to 0$ as $n \to \infty$. Therefore, we present different derivations of $I(X_k^n; Y_k^n)$ in the sequel. We first see that

$$\begin{aligned} I(X_1^n; Y_1^n) &\leq I(X_1^n X_3^n; Y_1^n) \\ &= H(Y_1^n) - H(Y_1^n|X_1^n X_3^n) \\ &= H(Y_1^n) - H(S_2^n|X_1^n X_3^n) && \text{(78a)} \\ &= H(Y_1^n) - \boxed{H(S_2^n)}, && \text{(78b)} \end{aligned}$$

where (78a) follows from the IS-IRC model; and in (78b) we take into account that the interference signal S_2^n is independent of the inputs $(X_1^n X_3^n)$. We can provide the interference X_2^n,

$$I(X_1^n; Y_1^n) \leq I(X_1^n X_3^n; Y_1^n|X_2^n), \tag{79}$$

where (79) follows from the fact that X_2^n is independent of $(X_1^n X_3^n)$. Also, we can augment the bound with the auxiliary RV V_1^n,

$$\begin{aligned} I(X_1^n; Y_1^n) &\leq I(X_1^n X_3^n; Y_1^n V_1^n) \\ &= I(X_1^n X_3^n; V_1^n) + I(X_1^n X_3^n; Y_1^n|V_1^n) \\ &= H(V_1^n) - H(V_1^n|X_1^n X_3^n) + H(Y_1^n|V_1^n) - H(Y_1^n|X_1^n X_3^n) && \text{(80a)} \\ &= \boxed{H(S_1^n)} - H(Y_2^n|X_1^n X_2^n X_3^n) + H(Y_1^n|V_1^n) - \boxed{H(S_2^n)}, && \text{(80b)} \end{aligned}$$

where in the fourth term of (80a) we use the Markov chain $V_1^n \multimap (X_1^n X_3^n) \multimap (\cdots)$; and (80b) is due to the channel property and the

fact that interchanging V_1 and S_1 does not change the entropies in question, i.e., $H(V_1^n) = H(S_1^n)$ and $H(V_1^n|X_1^nX_3^n) = H(S_1^n|X_1^nX_3^n) = H(S_1^n|X_1^nX_2^nX_3^n) = H(Y_2^n|X_1^nX_2^nX_3^n)$. We repeat the same procedure with the auxiliary RV $\underline{V_1^n}$,

$$\begin{aligned} I(X_1^n;Y_1^n) &\le I(X_1^nX_3^n;Y_1^n\underline{V_1^n}) \\ &= I(X_1^nX_3^n;\underline{V_1^n}) + I(X_1^nX_3^n;Y_1^n|\underline{V_1^n}) \\ &= H(\underline{V_1^n}) - H(\underline{V_1^n}|X_1^nX_3^n) + H(Y_1^n|\underline{V_1^n}) - H(Y_1^n|X_1^nX_3^n) \qquad (81a) \\ &= \boxed{H(\underline{S_1^n})} - H(Y_2^nY_3^n|X_1^nX_2^nX_3^n) + H(Y_1^n|\underline{V_1^n}) - \boxed{H(S_2^n)}, \qquad (81b) \end{aligned}$$

where in (81a) we use the Markov chain $\underline{V_1^n} \multimap (X_1^nX_3^n) \multimap (\cdots)$; and in (81b) we again interchange $\underline{V_1}$ and $\underline{S_1}$, i.e., $H(\underline{V_1^n}) = H(\underline{S_1^n})$ and $H(\underline{V_1^n}|X_1^nX_3^n) = H(\underline{S_1^n}|X_1^nX_3^n) = H(\underline{S_1^n}|X_1^nX_2^nX_3^n) = H(Y_2^nY_3^n|X_1^nX_2^nX_3^n)$. We can now increase the bound with both X_2^n and V_1^n,

$$\begin{aligned} I(X_1^n;Y_1^n) &\le I(X_1^nX_3^n;Y_1^nV_1^n|X_2^n) \\ &= I(X_1^nX_3^n;V_1^n|X_2^n) + I(X_1^nX_3^n;Y_1^n|V_1^nX_2^n) \\ &= H(V_1^n|X_2^n) - H(V_1^n|X_1^nX_3^n) + I(X_1^nX_3^n;Y_1^n|V_1^nX_2^n) \qquad (82a) \\ &= \boxed{H(S_1^n)} - H(Y_2^n|X_1^nX_2^nX_3^n) + I(X_1^nX_3^n;Y_1^n|V_1^nX_2^n), \qquad (82b) \end{aligned}$$

where the key steps in (82a) and (82b) are the same as in (80a) and (80b). Similarly, we can derive

$$I(X_1^n;Y_1^n) \le \boxed{H(\underline{S_1^n})} - H(Y_2^nY_3^n|X_1^nX_2^nX_3^n) + I(X_1^nX_3^n;Y_1^n|\underline{V_1^n}X_2^n). \quad (83)$$

In an analogous way as (78), (79), (80), and (82), we derive similar bounds for the rate R_2,

$$\begin{aligned} I(X_2^n;Y_2^n) &\le H(Y_2^n) - \boxed{H(S_1^n)}, \qquad (84) \\ I(X_2^n;Y_2^n) &\le I(X_2^n;Y_2^n|X_1^nX_3^n), \qquad (85) \\ I(X_2^n;Y_2^n) &\le \boxed{H(S_2^n)} - H(Y_1^n|X_1^nX_2^nX_3^n) + H(Y_2^n|V_2^n) - \boxed{H(S_1^n)}, \qquad (86) \\ I(X_2^n;Y_2^n) &\le \boxed{H(S_2^n)} - H(Y_1^n|X_1^nX_2^nX_3^n) + I(X_2^n;Y_2^n|X_1^nV_2^nX_3^n). \qquad (87) \end{aligned}$$

Additionally, if we add the sequence Y_3^n next to Y_2^n in the first steps of the derivation of (84) and (86), we obtain

$$\begin{aligned} I(X_2^n;Y_2^n) &\le H(Y_2^nY_3^n) - \boxed{H(\underline{S_1^n})}, \qquad (88) \\ I(X_2^n;Y_2^n) &\le \boxed{H(S_2^n)} - H(Y_1^n|X_1^nX_2^nX_3^n) + H(Y_2^nY_3^n|V_2^n) - \boxed{H(\underline{S_1^n})}. \qquad (89) \end{aligned}$$

The use of Fano's inequality and all the possible linear combinations of the expressions (78)–(89) where the boxed terms get canceled gives rise to multi-letter bounds that can be single-letterized, as summarized in Table 8. For instance, (79) and (85) allow us to find bounds

R_1	(66a)	(79)*
	(66b)	(79)
R_2	(66c)	(85)
$R_1 + R_2$	(66d)	(82) +(84)
	(66e)	(80) +(86)
	(66f)	(78) +(87)
	(66g)	(82)*+(84)
	(66h)	(80)*+(86)
	(66i)	(78)*+(87)
	(66j)	(83)*+(88)
	(66k)	(81)*+(89)
$2R_1 + R_2$	(66l)	(82) +(78) +(86)
	(66m)	(82) +(78)*+(86)
	(66n)	(82)*+(78) +(86)
	(66o)	(82)*+(78)*+(86)
	(66p)	(83)*+(78) +(89)
	(66q)	(83)*+(78)*+(89)
$R_1 + 2R_2$	(66r)	(80) +(87) +(84)
	(66s)	(80)*+(87) +(84)
	(66t)	(81)*+(87) +(88)

Table 8.: Combination of multi-letter outer bounds. Terms with * need the addition of Y_3^n.

on the single rates, whereas the addition of (82) and (84) gives us the sum-rate (66d),

$$\begin{aligned} n(R_1 + R_2 - \epsilon_n') &\le I(X_1^n; Y_1^n) + I(X_2^n; Y_2^n) \\ &\le I(X_1^n X_3^n; Y_1^n | V_1^n X_2^n) + I(X_1^n X_2^n X_3^n; Y_2^n) && \text{(90a)} \\ &\le \sum_{i=1}^{n} I(X_{1i} X_{3i}; Y_{1i} | V_{1i} X_{2i}) + I(X_{1i} X_{2i} X_{3i}; Y_{2i}) && \text{(90b)} \\ &= n[\, I(X_1 X_3; Y_1 | V_1 X_2 Q) + I(X_1 X_2 X_3; Y_2 | Q)], && \text{(90c)} \end{aligned}$$

where (90a) follows from the addition of (82b) and (84); (90b) is due to the chain rule of the mutual information, the fact that removing conditioning increases the entropy, and the Markov chain $(Y_{1i} Y_{2i}) - \!\circ\!- (X_{1i} X_{2i} X_{3i}) - \!\circ\!- (\cdots)$; and (90c) follows from the addition of the time-sharing variable Q uniformly distributed in $[1 : n]$.

In this way, we obtain all the bounds in (66) except for the ones with the pair $(Y_1 Y_3)$. For them, we need to add the sequence Y_3^n next to Y_1^n, like in the cutset bound, before applying the chain rule in the

mutual information. These terms are denoted with * in Table 8. For example, continuing from (90a) we obtain the bound (66g),

$$\begin{aligned} n(R_1 + R_2 - \epsilon_n') &\\ &\leq I(X_1^n X_3^n; Y_1^n Y_3^n | V_1^n X_2^n) + I(X_1^n X_2^n X_3^n; Y_2^n) \\ &\leq \sum_{i=1}^{n} I(X_{1i}; Y_{1i} Y_{3i} | V_{1i} X_{2i} X_{3i}) + I(X_{1i} X_{2i} X_{3i}; Y_{2i}) \qquad (91a) \\ &= n[\, I(X_1; Y_1 Y_3 | V_1 X_2 X_3 Q) + I(X_1 X_2 X_3; Y_2 | Q)] \qquad (91b) \end{aligned}$$

where (91a) follows from the fact that X_{3i} is a function of Y_3^{i-1}.

3.B PROOF OF COROLLARY 3.1

The expression of the bounds (66a)–(66c) in the Gaussian case is

$$R_1 \leq \mathsf{C}\left[(1-\rho^2)(S_{11}+S_{31})\right], \qquad (92)$$

$$R_1 \leq \mathsf{C}\left[S_{11}+S_{13}+2\rho\sqrt{S_{11}S_{13}}\right], \qquad (93)$$

$$R_2 \leq \mathsf{C}[S_{22}], \qquad (94)$$

where we assume the channel coefficients h_{11} and h_{13} have the same sign, otherwise, the analysis is the same by inverting the sign in ρ. For any $|\rho| \leq 1$, we can upper bound the previous terms as follows

$$R_1 \leq \mathsf{C}[S_{11}+S_{31}], \qquad (95)$$

$$R_1 \leq \mathsf{C}[S_{11}+S_{13}] + \frac{1}{2}, \qquad (96)$$

$$R_2 \leq \mathsf{C}[S_{22}], \qquad (97)$$

which, in turn, gives us (67a)–(67c).

All the other bounds behave similarly. If both X_1 and X_3 appear in the conditioning part of a mutual information, it does not depend on ρ, like (94). If only X_3 appears in the conditioning, it depends on $(1-\rho^2)$, like (92). Otherwise, it depends on $2\rho\sqrt{(\,\cdot\,)}$, like (93). In the first two situations, the expressions are maximized with its value at $\rho = 0$, whereas, the last one has its maximum at $\rho = 1$.

The bounds containing V_1 in the conditioning part, but not X_3, e.g. (66d), present a more complicated behavior and it is not clear which value of ρ maximizes the bound. We analyze the sum-rate (66d) in the sequel.

Let us first define

$$\boldsymbol{H} = \begin{bmatrix} h_{11} & h_{13} \\ h_{21} & h_{23} \end{bmatrix},$$

$$\boldsymbol{Q} = \begin{bmatrix} 1 & \rho \\ \rho & 1 \end{bmatrix} = \underbrace{\begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{bmatrix}}_{\boldsymbol{U}} \underbrace{\begin{bmatrix} 1+\rho & 0 \\ 0 & 1-\rho \end{bmatrix}}_{\boldsymbol{\Lambda}} \underbrace{\begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{bmatrix}}_{\boldsymbol{U}^T},$$

where we have normalized the sources' power and noise power. We are interested in

$$D_0 \triangleq \det(\boldsymbol{I}+\boldsymbol{H}\boldsymbol{H}^T) = \det(\boldsymbol{I}+\boldsymbol{H}\boldsymbol{U}\boldsymbol{U}^T\boldsymbol{H}^T) = \det(\boldsymbol{I}+\boldsymbol{G}\boldsymbol{G}^T),$$
$$D \triangleq \det(\boldsymbol{I}+\boldsymbol{H}\boldsymbol{Q}\boldsymbol{H}^T) = \det(\boldsymbol{I}+\boldsymbol{H}\boldsymbol{U}\boldsymbol{\Lambda}\boldsymbol{U}^T\boldsymbol{H}^T) = \det(\boldsymbol{I}+\boldsymbol{G}\boldsymbol{\Lambda}\boldsymbol{G}^T)$$

where we define $\boldsymbol{G} \triangleq \boldsymbol{H}\boldsymbol{U} = [g_{ij}]_{i,j=1,2}$. For convenience, we also define the normalized matrix $\boldsymbol{V}$ such that

$$\boldsymbol{G} = \begin{bmatrix} \sqrt{G_1} & 0 \\ 0 & \sqrt{G_2} \end{bmatrix} \boldsymbol{V}, \quad G_i \triangleq g_{i1}^2 + g_{i2}^2,\ i = 1,2$$

where $v_{ij} \triangleq g_{ij}/\sqrt{G_i}$. Note that $v_{i1}^2 + v_{i2}^2 = 1$, $i = 1,2$. We let $V_{ij} \triangleq v_{ij}^2$ hereafter.

Then, we can rewrite

$$D_0 = 1 + G_1 + G_2 + G_1G_2 \underbrace{\det(\boldsymbol{V}\boldsymbol{V}^T)}_{\gamma}$$
$$D = 1 + G_1(1 + \underbrace{(V_{11}-V_{12})}_{\alpha_1}\rho) + G_2(1 + \underbrace{(V_{21}-V_{22})}_{\alpha_2}\rho) + G_1G_2\gamma(1-\rho^2)$$

where $\gamma \in [0,1]$ and $\alpha_1, \alpha_2 \in [-1,1]$. In fact, γ can be presented as a function of α_1 and α_2

$$\gamma = (v_{11}v_{22} - v_{21}v_{12})^2 \tag{98a}$$
$$\geq \left(\sqrt{V_{11}V_{22}} - \sqrt{V_{21}V_{12}}\right)^2 \tag{98b}$$
$$= \frac{1-\alpha_1\alpha_2}{2} - \frac{1}{2}\sqrt{(1-\alpha_1^2)(1-\alpha_2^2)} \triangleq \gamma_*. \tag{98c}$$

Given the sum-rate (66d),

$$R_1 + R_2 \leq I(X_1X_3; Y_1|V_1X_2) + I(X_1X_2X_3; Y_2)$$
$$= I(X_1X_3; Y_1V_1|X_2) - I(X_1X_3; V_1|X_2) + I(X_1X_2X_3; Y_2),$$

the ultimate goal is to quantify the maximum gap between the value of this bound with and without correlation in the inputs (X_1X_3). In other words, we shall obtain an upper bound on

$$\frac{D}{D_0}\frac{1+G_2}{1+G_2(1+\alpha_2\rho)}\frac{1+G_2(1+\alpha_2\rho)+S_{22}}{1+G_2+S_{22}}. \tag{99}$$

If $S_{22} \to 0$, the expression (99) tends to D/D_0, and since the eigenvalues of $\boldsymbol{\Lambda}$ are less or equal than 2, it can be easily upper-bounded,

$$\frac{D}{D_0} = \frac{\det(\boldsymbol{I}+\boldsymbol{G}\boldsymbol{\Lambda}\boldsymbol{G}^T)}{\det(\boldsymbol{I}+\boldsymbol{G}\boldsymbol{G}^T)} \leq \frac{\det(\boldsymbol{I}+2\boldsymbol{G}\boldsymbol{G}^T)}{\det(\boldsymbol{I}+\boldsymbol{G}\boldsymbol{G}^T)} \leq 2.$$

On the other hand, if $S_{22} \to \infty$, (99) becomes

$$\frac{D}{D_0}\frac{1+G_2}{1+G_2(1+\alpha_2\rho)} = \frac{1+G_1\dfrac{1+\alpha_1\rho+G_2\gamma(1-\rho^2)}{1+G_2(1+\alpha_2\rho)}}{1+G_1\dfrac{1+G_2\gamma}{1+G_2}} = \frac{1+G_1A}{1+G_1B}.$$

We observe that this function is upper-bounded by 1 when $A \leq B$, while it is otherwise upper-bounded by A/B. Therefore, it suffices to find an upper bound on A/B that can be rewritten as

$$\frac{A}{B} = \frac{(1+\alpha_1\rho)+G_2\gamma(1-\rho^2)+G_2(1+\alpha_1\rho)+G_2^2\gamma(1-\rho^2)}{(1+G_2\gamma)(1+G_2(1+\alpha_2\rho))}$$
$$= (1+\alpha_1\rho)\frac{1+G_2}{1+G_2(1+\alpha_2\rho)}\frac{1+G_2\frac{\gamma(1-\rho^2)}{1+\alpha_1\rho}}{1+G_2\gamma}. \tag{100}$$

Without loss of generality, we assume that $\rho \geq 0$. The case when $\rho < 0$ follows straightforwardly by simply changing both signs of α_1 and α_2. In the following, we shall show that

$$\frac{A}{B} \leq 2.$$

First, from (100), we derive a trivial upper bound

$$\frac{A}{B} \leq (1+\alpha_1\rho)\max\left\{1, \frac{1}{1+\alpha_2\rho}\right\}\max\left\{1, \frac{1-\rho^2}{1+\alpha_1\rho}\right\} \tag{101a}$$
$$= \max\left\{1-\rho^2, 1+\alpha_1\rho, \frac{1-\rho^2}{1+\alpha_2\rho}, \frac{1+\alpha_1\rho}{1+\alpha_2\rho}\right\}, \tag{101b}$$

where both maximizations in (101a) come from the monotonicity of $\frac{1+G_2x}{1+G_2y}$ w.r.t. G_2 and that it is bounded by the extreme values for $G_2 = 0$ and $G_2 \to \infty$. Note that only the last term in (101b) is not always upper-bounded by 2. In the following, we focus on the case $\frac{1-\rho^2}{1+\alpha_1\rho} < 1$, i.e., $\alpha_1 > -\rho$, since the opposite would imply that the last term in (101b) is upper-bounded by the third term. In this case ($\alpha_1 > -\rho$), the third term in (100), and thus A/B, is decreasing with γ. Therefore, the worst case in which A/B is maximized is when γ achieves γ_*. It suffices to show that

$$\sup_{G_2\geq 0}\frac{1+\alpha_1\rho+G_2\left(1+\alpha_1\rho+\gamma_*(1-\rho^2)\right)+G_2^2\gamma_*(1-\rho^2)}{(1+G_2\gamma_*)(1+G_2(1+\alpha_2\rho))} \leq 2,$$

$\forall\,(\alpha_1,\alpha_2,\rho) \in \mathcal{A}$ where we define the set $\mathcal{A}$

$$\mathcal{A} \triangleq \{\alpha_1,\alpha_2 \in (-1,1),\ \rho \in (0,1)\ :\ \alpha_1 > \alpha_2,\ \alpha_1 > -\rho\}.$$

We observe that for each point at the boundary of the set $\mathcal{A}$, the objective function is upper-bounded by 2. Note that, in the denominator, $\gamma_* > 0$ since $\alpha_1 \neq \alpha_2$, and $1+\alpha_2\rho > 0$ since $\rho < 1$. Therefore, the objective function is the ratio between two quadratic functions in the form $(a_0+a_1G_2+a_2G_2^2)/((1+b_1G_2)(1+b_2G_2))$ with $a_0,a_1,a_2 \geq 0$ and $b_1,b_2 > 0$, that are continuous functions of (α_1,α_2,ρ). Let us first assume that $b_1 \neq b_2$. It is readily shown that

$$f(G_2) = \frac{a_0+a_1G_2+a_2G_2^2}{(1+b_1G_2)(1+b_2G_2)} \tag{102}$$
$$= c_0 + \frac{c_1}{1+b_1G_2} + \frac{c_2}{1+b_2G_2}, \quad \forall\, G_2 \tag{103}$$

where (c_0, c_1, c_2) is a continuous function of $\{a_i\}$ and $\{b_i\}$. Then, we differentiate the function $f(G_2)$

$$f'(G_2) = -\frac{b_1 c_1}{(1+b_1 G_2)^2} - \frac{b_2 c_2}{(1+b_2 G_2)^2}.$$

It is clear that there is at most one solution in $[0, \infty]$ such that $f'(G_2) = 0$. If such a solution does not exist, then $f'(G_2)$ is either strictly positive or strictly negative in $[0, \infty]$. In this case, both extreme values $f(0)$ and $f(\infty)$ are upper-bounded by 2 from (100). If such a solution does exist, it is in the following form

$$G_2^* = \frac{\beta - 1}{b_1 - b_2 \beta}, \quad \beta \triangleq \sqrt{-\frac{b_1 c_1}{b_2 c_2}}, \quad \frac{c_1}{c_2} < 0. \tag{104}$$

Note that the function f defined in (102), alternatively denoted as f_{b_1,b_2}, converges pointwise to $f_{b,b}$ when $b_1, b_2 \to b$, $\forall\, b > 0$, and that f'_{b_1,b_2} converges uniformly to $f'_{b,b}$. Therefore, the solution (104) holds even when $b_1 = b_2$ by taking the limit. Finally, let us define a set $\mathcal{B}$ of $(\alpha_1, \alpha_2, \rho)$ such that $c_1/c_2 < 0$ and $G_2^* \geq 0$. It remains to show that

$$\sup_{(\alpha_1,\alpha_2,\rho) \in \mathcal{A} \cap \mathcal{B}} f(G_2^*) \leq 2. \tag{105}$$

Since $\mathcal{A} \cap \mathcal{B}$ is a bounded set and the objective function is continuous in $(\alpha_1, \alpha_2, \rho)$ in $\mathcal{A} \cap \mathcal{B}$, we can perform numerical optimization and obtain the value 2, which confirms the claim in (105).

Similar steps can be performed in every other bound containing V_1 in the conditioning, which concludes the proof.

3.C PROOF OF THEOREM 3.2 (PARTIAL DF)

Each source transmits b messages during $b+1$ time blocks, each of them of length n. The messages are sent using block Markov coding and the destinations employ backward decoding to retrieve them.

The second source splits its message $\tilde{m}_2$ into a common message m_2 and a private one w_2, with partial rates R_{20} and R_{22}, respectively, such that $R_2 = R_{20} + R_{22}$. On the other hand, the first source splits its message $\tilde{m}_1$ into three parts: (m_1, w_1', w_1''). The relay decodes and retransmits the common message and a part of the private one, i.e., (m_1, w_1'), whereas the other part is only decoded by the final destination. The rate of the first user is therefore the sum of these three partial rates: $R_1 = R_{10} + R_{11}' + R_{11}''$.

3.C.1 *Code Generation*

1. Generate the time-sharing sequence q^n where each element is i.i.d. according to the PD

$$p(q^n) = \prod_{i=1}^{n} p_Q(q_i).$$

2. For each sequence q^n, generate $2^{nT_{10}}$ conditionally independent sequences $v_3^n(t_0)$, where $t_0 \in \left[1 : 2^{nT_{10}}\right]$, and distributed according to the conditional PD

$$p(v_3^n|q^n) = \prod_{i=1}^{n} p_{V_3|Q}(v_{3i}|q_i).$$

3. For each $v_3^n(t_0)$, generate $2^{nR'_{11}}$ conditionally independent sequences $x_3^n(t_0, r_0)$, where $r_0 \in \left[1 : 2^{nR'_{11}}\right]$, and distributed according to the conditional PD

$$p(x_3^n|v_3^n(t_0), q^n) = \prod_{i=1}^{n} p_{X_3|V_3Q}(x_{3i}|v_{3i}(t_0), q_i).$$

4. For each $v_3^n(t_0)$, generate $2^{nT_{10}}$ conditionally independent sequences $v_1^n(t_0, t_1)$, where $t_1 \in \left[1 : 2^{nT_{10}}\right]$, and distributed according to the conditional PD

$$p(v_1^n|v_3^n(t_0), q^n) = \prod_{i=1}^{n} p_{V_1|V_3Q}(v_{1i}|v_{3i}(t_0), q_i).$$

5. Partition the set $\left[1 : 2^{nT_{10}}\right]$ into $2^{nR_{10}}$ cells and label them $\mathcal{T}(m_1)$, where $m_1 \in \left[1 : 2^{nR_{10}}\right]$.

6. For every pair $(x_3^n(t_0, r_0), v_1^n(t_0, t_1))$, generate $2^{nR'_{11}}$ conditionally independent sequences $u_1^n(t_0, t_1, r_0, r_1)$, where $r_1 \in \left[1 : 2^{nR'_{11}}\right]$, and distributed according to the conditional PD

$$p(u_1^n|v_1^n(t_0, t_1), x_3^n(t_0, r_0), v_3^n(t_0), q^n) = \prod_{i=1}^{n} p(u_{1i}|v_{1i}(t_0, t_1), x_{3i}(t_0, r_0), v_{3i}(t_0), q_i).$$

7. For each $u_1^n(t_0, t_1, r_0, r_1)$, generate $2^{nR''_{11}}$ conditionally independent sequences $x_1^n(t_0, t_1, r_0, r_1, r_2)$, where $r_2 \in \left[1 : 2^{nR''_{11}}\right]$, and distributed according to the conditional PD

$$p(x_1^n|u_1^n(\cdot), v_1^n(t_0, t_1), x_3^n(t_0, r_0), v_3^n(t_0), q^n) = \prod_{i=1}^{n} p(x_{1i}|u_{1i}(\cdot), v_{1i}(t_0, t_1), x_{3i}(t_0, r_0), v_{3i}(t_0), q_i).$$

$j=1$	$j=2$	$\dots$	$j=b+1$
$v_3^n(1)$	$v_3^n(t_{11})$	$\dots$	$v_3^n(t_{1b})$
$x_3^n(1,1)$	$x_3^n(t_{11},w'_{11})$	$\dots$	$x_3^n(t_{1b},w'_{1b})$
$v_1^n(1,t_{11})$	$v_1^n(t_{11},t_{12})$	$\dots$	$v_1^n(t_{1b},1)$
$x_1^n(1,t_{11},1,w'_{11},w''_{11})$	$x_1^n(t_{11},t_{12},w'_{11},w'_{12},w''_{12})$	$\dots$	$x_1^n(t_{1b},1,w'_{1b},1,1)$
$v_2^n(1)$	$v_2^n(m_{21})$	$\dots$	$v_2^n(m_{2b})$
$x_2^n(1,1)$	$x_2^n(m_{21},w_{21})$	$\dots$	$x_2^n(m_{2b},w_{2b})$

Table 9.: Codewords in the proposed partial DF scheme.

8. For each sequence q^n, generate $2^{nR_{20}}$ conditionally independent sequences $v_2^n(s_0)$, where $s_0 \in \left[1 : 2^{nR_{20}}\right]$, and distributed according to the conditional PD

$$p(v_2^n|q^n) = \prod_{i=1}^{n} p_{V_2|Q}(v_{2i}|q_i).$$

9. For each $v_2^n(s_0)$, generate $2^{nR_{22}}$ conditionally independent sequences $x_2^n(s_0,s_1)$, where $s_1 \in \left[1 : 2^{nR_{22}}\right]$, and distributed according to the conditional PD

$$p(x_2^n|v_2^n(s_0),q^n) = \prod_{i=1}^{n} p_{X_2|V_2Q}(x_{2i}|v_{2i}(s_0),q_i).$$

3.C.2 *Encoding Part*

Encoding in block j proceeds as follows,

1. The relay knows the indices $(t_{1(j-1)}, w'_{1(j-1)})$ from decoding step 1 in the previous block, thus it transmits $x_3^n(t_{1(j-1)}, w'_{1(j-1)})$. For block $j=1$, it transmits the dummy message $x_3^n(1,1)$.

2. Encoder 1 wants to transmit $\tilde{m}_{1j} = (m_{1j}, w'_{1j}, w''_{1j})$, thus, it looks for an index $t_{1j} \in \mathcal{T}(m_{1j})$ such that

$$\left(v_1^n(t_{1(j-1)}, t_{1j}), x_3^n(t_{1(j-1)}, w'_{1(j-1)}), v_3^n(t_{1(j-1)}), q^n\right) \in T_{\delta'}^n(V_1X_3V_3Q).$$

   The success of this step requires that

$$T_{10} - R_{10} > I_b + \delta', \tag{106}$$

   where $I_b \triangleq I(X_3; V_1|V_3Q)$ and $\delta' > 0$ is an arbitrarily small constant. It then sends the codeword $x_1^n(t_{1(j-1)}, t_{1j}, w'_{1(j-1)}, w'_{1j}, w''_{1j})$. The source sends the dummy messages $\tilde{m}_{10} = (1,1,1)$ and $\tilde{m}_{1(b+1)} = (1,1,1)$ known to all users at the beginning and at the end of the transmission.

3. Encoder 2 sends its message $\tilde{m}_{2(j-1)} = (m_{2(j-1)}, w_{2(j-1)})$ through the codeword $x_2^n(m_{2(j-1)}, w_{2(j-1)})$. During block $j = 1$, it sends the dummy message $x_2^n(1,1)$.

See Table 9 for references.

3.C.3 *Decoding Part*

1. Let $\delta > \delta'$. At the end of block $j \in [1:b]$ and assuming its past message estimates are correct, the relay looks for the unique pair of indices $(t_{1j}, w'_{1j}) \equiv (\hat{t}, \hat{w}')$ such that

$$\begin{aligned}\big(v_3^n(t_{1(j-1)}), x_3^n(t_{1(j-1)}, w'_{1(j-1)}), v_1^n(t_{1(j-1)}, \hat{t}), y_{3j}^n, q^n,\\ u_1^n(t_{1(j-1)}, \hat{t}, w'_{1(j-1)}, \hat{w}')\big) \in T_\delta^n(V_3X_3V_1U_1Y_3Q).\end{aligned}$$

   The probability of error becomes arbitrarily small if

$$R'_{11} < I(U_1; Y_3|V_1X_3Q) - \delta, \tag{107a}$$
$$T_{10} + R'_{11} < I(V_1U_1; Y_3|X_3Q) + I_b - \delta. \tag{107b}$$

2. Starting at the end of block $b+1$ and assuming its past message estimates are correct, destination 1 looks for the indices $(t_{1(j-1)}, w'_{1(j-1)}, w''_{1j}, m_{2(j-1)}) \equiv (\hat{t}, \hat{w}', \hat{w}'', \hat{m})$ backwardly such that

$$\begin{aligned}\big(v_3^n(\hat{t}), v_1^n(\hat{t}, t_{1j}), x_3^n(\hat{t}, \hat{w}'), u_1^n(\hat{t}, t_{1j}, \hat{w}', w'_{1j}), x_1^n(\hat{t}, t_{1j}, \hat{w}', w'_{1j}, \hat{w}''),\\ v_2^n(\hat{m}), y_{1j}^n, q^n\big) \in T_\delta^n(V_3V_1X_3U_1X_1V_2Y_1Q).\end{aligned}$$

   The probability of error becomes arbitrarily small if

$$R''_{11} < I(X_1; Y_1|V_1U_1V_2X_3Q) - \delta, \tag{108a}$$
$$R'_{11} + R''_{11} < I(X_1X_3; Y_1|V_1V_2V_3Q) + I_b - \delta, \tag{108b}$$
$$T_{10} + R'_{11} + R''_{11} < I(X_1X_3; Y_1|V_2Q) + I_b - \delta, \tag{108c}$$
$$R''_{11} + R_{20} < I(X_1V_2; Y_1|V_1U_1X_3Q) - \delta, \tag{108d}$$
$$R'_{11} + R''_{11} + R_{20} < I(X_1V_2X_3; Y_1|V_1V_3Q) + I_b - \delta, \tag{108e}$$
$$T_{10} + R'_{11} + R''_{11} + R_{20} < I(X_1V_2X_3; Y_1|Q) + I_b - \delta. \tag{108f}$$

3. Destination 2 performs similarly, thus, it looks for the indices $(t_{1(j-1)}, m_{2(j-1)}, w_{2(j-1)}) \equiv (\hat{t}, \hat{m}, \hat{w})$ backwardly such that

$$\big(v_3^n(\hat{t}), v_1^n(\hat{t}, t_{1j}), v_2^n(\hat{m}), x_2^n(\hat{m}, \hat{w}), y_{2j}^n, q^n\big) \in T_\delta^n(V_3V_1V_2X_2Y_2Q).$$

   The probability of error becomes arbitrarily small if

$$R_{22} < I(X_2; Y_2|V_1V_2V_3Q) - \delta, \tag{109a}$$
$$R_{20} + R_{22} < I(X_2; Y_2|V_1V_3Q) - \delta, \tag{109b}$$
$$T_{10} + R_{22} < I(V_1X_2V_3; Y_2|V_2Q) - \delta, \tag{109c}$$
$$T_{10} + R_{20} + R_{22} < I(V_1X_2V_3; Y_2|Q) - \delta, \tag{109d}$$
$$T_{10} < I(V_1V_3; Y_2|X_2Q) - \delta. \tag{109e}$$

Remark 3.12. *If at this point we replace U_1 with X_1, the region boils down to the one attained by the full DF scheme (Corollary 3.2). See Appendix 3.D.*

Remark 3.13. *The bound (109e) represents the perfect decoding of the common layer of interference. This bound is needed, however, because of the block Markov coding technique and the assumption that the index t_{1j} present in $v_1^n(\cdot)$ is correct. Nonetheless, this term only appears in some of the additional bounds shown below and it does not affect the final region $\mathcal{R}_{p\text{-}DF}$.*

After running FME to the set (106)–(109) and letting $n \to \infty$, we obtain the region $\mathcal{R}_{\text{p-DF}}(P_2)$ (69) with the term $I(V_1U_1;Y_3|X_3Q)$ instead of $I(U_1;Y_3|X_3Q)$ in (69a), (69k), and (69m), plus four additional bounds

$$R_1 < I(X_1X_3;Y_1|V_1V_2V_3Q) + I(V_1V_3;Y_2|X_2Q), \tag{110a}$$

$$R_1 < I(U_1;Y_3|V_1X_3Q) + I(X_1;Y_1|V_1U_1V_2X_3Q) + I(V_1V_3;Y_2|X_2Q) - I_b, \tag{110b}$$

$$R_2 < I(X_1V_2;Y_1|V_1U_1X_3Q) + I(X_2;Y_2|V_1V_2V_3Q), \tag{110c}$$

$$R_2 < I(X_1V_2;Y_1|V_1U_1X_3Q) + I(V_1X_2V_3;Y_2|V_2Q) - I_b. \tag{110d}$$

These bounds on the single rates arise from the decoding of the common message of the interference at the interfered receiver. It is reasonable to assume that the maximizing PD will render these bounds *inactive*, i.e., if the single rates are penalized due to the large amount of common information, another PD with *less* common information will increase the achievable rate.

In order to eliminate the bounds (110) –a necessary condition to later compare to the outer bound– we proceed in a similar way as [49, Lemma 2]. First, let us define, for a given PD $p \in \mathcal{P}_2$, the region $\mathcal{R}^o_{\text{p-DF}}(p)$ as the *original* region after FME, i.e., the region $\mathcal{R}_{\text{p-DF}}(p)$ (69) with the term $I(V_1U_1;Y_3|X_3Q)$ instead of $I(U_1;Y_3|X_3Q)$ plus the four bounds (110).

Second, we define $\mathcal{R}^{c_1}_{\text{p-DF}}(p)$ as the region $\mathcal{R}^o_{\text{p-DF}}(p)$ without bounds (110c) and (110d), thus, it is easy to see that $\mathcal{R}^o_{\text{p-DF}}(p) \subseteq \mathcal{R}^{c_1}_{\text{p-DF}}(p)$. On the other hand, when either (110c) or (110d) is active in $\mathcal{R}^o_{\text{p-DF}}(p)$, then $\mathcal{R}^o_{\text{p-DF}}(p^{**})$ with $p^{**} = \sum_{v_2} p$ attains higher rates than $\mathcal{R}^{c_1}_{\text{p-DF}}(p)$. The PD p^{**} is the marginal of p w.r.t. V_2, therefore, effectively eliminating the common message from the second source. In summary, $\mathcal{R}^{c_1}_{\text{p-DF}}(p) \subseteq \mathcal{R}^o_{\text{p-DF}}(p) \cup \mathcal{R}^o_{\text{p-DF}}(p^{**})$. After maximizing over all joint PDs, we obtain $\mathcal{R}^{c_1}_{\text{p-DF}} = \mathcal{R}^o_{\text{p-DF}}$, thus (110c) and (110d) are redundant.

Third, we reduce the achievable region $\mathcal{R}^{c_1}_{\text{p-DF}}(p)$ by replacing the terms $I(V_1U_1;Y_3|X_3Q)$ with $I(U_1;Y_3|X_3Q)$, let us call this reduced region $\mathcal{R}^{c_2}_{\text{p-DF}}(p)$. We define the region $\mathcal{R}_{\text{p-DF}}(p)$ based on $\mathcal{R}^{c_2}_{\text{p-DF}}(p)$ and eliminate the bounds (110a) and (110b) from it. After this, it is easy to prove that both $\mathcal{R}^{c_2}_{\text{p-DF}}(p) \subseteq \mathcal{R}_{\text{p-DF}}(p)$ and $\mathcal{R}_{\text{p-DF}}(p) \subseteq$

$\mathcal{R}^{c_2}_{\text{p-DF}}(p) \cup \mathcal{R}^{c_2}_{\text{p-DF}}(p^*)$, with $p^* = \sum_{v_1 v_3} p$, hold. Therefore, after the maximization, we obtain $\mathcal{R}_{\text{p-DF}} = \mathcal{R}^{c_2}_{\text{p-DF}}$.

Remark 3.14. *The region $\mathcal{R}_{p\text{-}DF}$ (69) is not the optimal one for partial DF because of the aforementioned reduction, i.e. $\mathcal{R}_{p\text{-}DF} = \mathcal{R}^{c_2}_{p\text{-}DF} \subseteq \mathcal{R}^{c_1}_{p\text{-}DF} = \mathcal{R}^{o}_{p\text{-}DF}$. However, as we see later, this loss does not prevent us from obtaining a constant-gap result.*

3.D PROOF OF COROLLARY 3.2 (FULL DF)

Since $U_1 = X_1$, the first source does not split its private message in two, i.e., $R''_{11} = 0$ and $R_1 = R_{10} + R'_{11}$. The codebook generation, encoding and decoding is carried out as in the partial DF scheme.

After running FME to the set (106)–(109) and letting $n \to \infty$, we obtain the region $\mathcal{R}_{\text{f-DF}}(P_3)$ (71), plus three additional bounds

$$R_1 < I(X_1X_3; Y_1|V_1V_2V_3Q) + I(V_1V_3; Y_2|X_2Q), \tag{111a}$$
$$R_1 < I(X_1; Y_3|V_1X_3Q) + I(V_1V_3; Y_2|X_2Q) - I_b, \tag{111b}$$
$$R_2 < I(X_1V_2X_3; Y_1|V_1V_3Q) + I(X_2; Y_2|V_1V_2V_3Q) + I_b. \tag{111c}$$

As in the partial DF scheme, these bounds are redundant when maximized over all possible PDs. Let us define $\mathcal{R}^{o}_{\text{f-DF}}(P_3)$ as the *original* region after FME. Then, it is clear that for a given PD $p \in \mathcal{P}_3$, $\mathcal{R}^{o}_{\text{f-DF}}(p) \subseteq \mathcal{R}_{\text{f-DF}}(p)$, because of the presence of (111).

When either (111a) or (111b) is active in $\mathcal{R}^{o}_{\text{f-DF}}(p)$, then $\mathcal{R}^{o}_{\text{f-DF}}(p^*)$ with $p^* = \sum_{v_1 v_3} p$ attains higher rates than $\mathcal{R}_{\text{f-DF}}(p)$. Similarly, when (111c) is active, $\mathcal{R}^{o}_{\text{f-DF}}(p^{**})$ with $p^{**} = \sum_{v_2} p$ outperforms $\mathcal{R}_{\text{f-DF}}(p)$. Succinctly, $\mathcal{R}_{\text{f-DF}}(p) \subseteq \mathcal{R}^{o}_{\text{f-DF}}(p) \cup \mathcal{R}^{o}_{\text{f-DF}}(p^*) \cup \mathcal{R}^{o}_{\text{f-DF}}(p^{**})$.

Therefore, after maximizing over all possible PDs, $\mathcal{R}_{\text{f-DF}} = \mathcal{R}^{o}_{\text{f-DF}}$, which renders (111) redundant.

3.E PROOF OF THEOREM 3.3 (CF SCHEME)

As before, each source $k \in \{1, 2\}$ splits its message $\tilde{m}_k$ into a common message m_k and a private one w_k, each with partial rate R_{k0} and R_{kk}, respectively, such that $R_k = R_{k0} + R_{kk}$. But now, each source transmits b messages during $b + b_s$ time blocks, each of them of length n. During these additional b_s time blocks, the relay repeats the same compression index to ensure a correct decoding at each destination [6, 7].

3.E.1 *Code Generation*

1. Generate the time-sharing sequence q^n where each element is i.i.d. according to the PD

$$p(q^n) = \prod_{i=1}^{n} p_Q(q_i).$$

2. For each source $k \in \{1,2\}$ and the sequence q^n, generate $2^{nR_{k0}}$ conditionally independent sequences $v_k^n(m_k)$, $m_k \in \left[1 : 2^{nR_{k0}}\right]$, and distributed according to the conditional PD

$$p(v_k^n|q^n) = \prod_{i=1}^{n} p_{V_k|Q}(v_{ki}|q_i).$$

3. For each source $k \in \{1,2\}$ and for each $v_k^n(m_k)$, generate $2^{nR_{kk}}$ conditionally independent sequences $x_k^n(m_k, w_k)$, where $w_k \in \left[1 : 2^{nR_{kk}}\right]$, and distributed according to the conditional PD

$$p(x_k^n|v_k^n(m_k), q^n) = \prod_{i=1}^{n} p_{X_k|V_kQ}(x_{ki}|v_{ki}(m_k), q_i).$$

4. For the sequence q^n, generate $2^{n\hat{R}}$ conditionally independent sequences $x_3^n(s_1)$, where $s_1 \in \left[1 : 2^{n\hat{R}}\right]$ for $\hat{R} = I(\hat{Y}_3; Y_3|X_3Q) + \delta'$, and distributed according to the conditional PD

$$p(x_3^n|q^n) = \prod_{i=1}^{n} p_{X_3|Q}(x_{3i}|q_i).$$

5. For the sequence q^n and each $x_3^n(s_1)$, generate $2^{n\hat{R}}$ conditionally independent sequences $\hat{y}_3^n(s_1, s_2)$, where $s_2 \in \left[1 : 2^{n\hat{R}}\right]$, and distributed according to the conditional PD

$$p(\hat{y}_3^n|x_3^n(s_1), q^n) = \prod_{i=1}^{n} p_{\hat{Y}_3|X_3Q}(\hat{y}_{3i}|x_{3i}(s_1), q_i).$$

3.E.2 *Encoding Part*

Encoding in block j proceeds as follows,

1. Each source $k \in \{1,2\}$ uses its present message $\tilde{m}_{kj}$ to choose the codeword it transmits, $x_k^n(m_{kj}, w_{kj})$ for blocks $j \in [1 : b]$. During blocks $j \in [b+1 : b+b_s]$, the sources send the dummy message $\tilde{m}_{kj} = 1$ known to all users.

2. At the end of block $j \in [1 : b]$, the relay looks for at least one index $s_j \equiv \hat{s}$, with $s_0 = 1$, such that $\left(x_3^n(s_{j-1}), \hat{y}_3^n(s_{j-1}, \hat{s}), y_{3j}^n, q^n\right) \in$

$j=1$	$j=2$	$\dots$	$j=b$	$j=b+1$	$\dots$	$j=b+b_s$
$v_1^n(m_{11})$	$v_1^n(m_{12})$	$\dots$	$v_1^n(m_{1b})$	$v_1^n(1)$	$\dots$	$v_1^n(1)$
$x_1^n(m_{11},w_{11})$	$x_1^n(m_{12},w_{12})$	$\dots$	$x_1^n(m_{1b},w_{1b})$	$x_1^n(1,1)$	$\dots$	$x_1^n(1,1)$
$v_2^n(m_{21})$	$v_2^n(m_{22})$	$\dots$	$v_2^n(m_{2b})$	$v_2^n(1)$	$\dots$	$v_2^n(1)$
$x_2^n(m_{21},w_{21})$	$x_2^n(m_{22},w_{22})$	$\dots$	$x_2^n(m_{2b},w_{2b})$	$x_2^n(1,1)$	$\dots$	$x_2^n(1,1)$
$\hat{y}_3^n(1,s_1)$	$\hat{y}_3^n(s_1,s_2)$	$\dots$	$\hat{y}_3^n(s_{b-1},s_b)$	$\emptyset$	$\dots$	$\emptyset$
$x_3^n(1)$	$x_3^n(s_1)$	$\dots$	$x_3^n(s_{b-1})$	$x_3^n(s_b)$	$\dots$	$x_3^n(s_b)$

Table 10.: Codewords in the proposed CF scheme.

$T_{\delta'}^n(X_3\hat{Y}_3Y_3Q)$. The probability of finding such s_j goes to one as n approaches infinity. It then transmits $x_3^n(s_j)$ in the next time block. Moreover, for blocks $j \in [b+1 : b+b_s]$, the last compression index s_b is repeated.

See Table 10 for references.

3.E.3 *Decoding Part*

1. Destination 1 decodes the compression index in two steps. First, it looks for the unique index $s_b \equiv \hat{s}$ such that, $\forall\ j \in [b+1 : b+b_s]$,

$$\left(v_1^n(1), x_1^n(1,1), v_2^n(1), x_3^n(\hat{s}), y_{1j}^n, q^n\right) \in T_\delta^n(V_1X_1V_2X_3Y_1Q).$$

   For a finite but sufficiently large b_s, the probability of incorrectly decoding s_b can be made arbitrarily small.

2. After finding s_b, destination 1 looks for the unique set of indices $(m_{1j}, w_{1j}, m_{2j}, s_{j-1}) \equiv (\hat{m}, \hat{w}, \hat{m}', \hat{s})$ for $j \in [1 : b]$ such that

$$\left(v_1^n(\hat{m}), x_1^n(\hat{m},\hat{w}), v_2^n(\hat{m}'), x_3^n(\hat{s}), \hat{y}_3^n(\hat{s},s_j), y_{1j}^n, q^n\right) \in T_\delta^n(V_1X_1V_2X_3\hat{Y}_3Y_1Q).$$

   The probability of error can be made arbitrarily small provided that,

$$R_{11} < I_{11} - \delta, \tag{112a}$$
$$R_{10} + R_{11} < I_{12} - \delta, \tag{112b}$$
$$R_{20} + R_{11} < I_{13} - \delta, \tag{112c}$$
$$R_{10} + R_{11} + R_{20} < I_{14} - \delta, \tag{112d}$$
$$R_{20} < I(V_2X_3; Y_1|X_1Q) - I_1 - \delta, \tag{112e}$$
$$I_1 < I(X_3; Y_1|X_1V_2Q) - \delta \tag{112f}$$

   where $I_1 \triangleq I(\hat{Y}_3; Y_3|X_1V_2X_3Y_1Q) + \delta'$ and

$$I_{11} \triangleq \min\{I(X_1; Y_1\hat{Y}_3|V_1V_2X_3Q),\ I(X_1X_3; Y_1|V_1V_2Q) - I_1\}$$
$$I_{12} \triangleq \min\{I(X_1; Y_1\hat{Y}_3|V_2X_3Q),\ I(X_1X_3; Y_1|V_2Q) - I_1\}$$

$$I_{13} \triangleq \min\{I(X_1V_2; Y_1\hat{Y}_3|V_1X_3Q),\ I(X_1V_2X_3; Y_1|V_1Q) - I_1\}$$
$$I_{14} \triangleq \min\{I(X_1V_2; Y_1\hat{Y}_3|X_3Q),\ I(X_1V_2X_3; Y_1|Q) - I_1\}.$$

3. If destination 1 ignores the compression index, it looks for the indices $(m_{1j}, w_{1j}, m_{2j}) \equiv (\hat{m}, \hat{w}, \hat{m}')$ for $j \in [1 : b]$ such that

$$\left(v_1^n(\hat{m}), x_1^n(\hat{m}, \hat{w}), v_2^n(\hat{m}'), y_{1j}^n, q^n\right) \in T_\delta^n(V_1X_1V_2Y_1Q).$$

The probability of error can be made arbitrarily small provided that,

$$R_{11} < I(X_1; Y_1|V_1V_2Q) - \delta, \tag{113a}$$
$$R_{10} + R_{11} < I(X_1; Y_1|V_2Q) - \delta, \tag{113b}$$
$$R_{20} + R_{11} < I(X_1V_2; Y_1|V_1Q) - \delta, \tag{113c}$$
$$R_{10} + R_{11} + R_{20} < I(X_1V_2; Y_1|Q) - \delta. \tag{113d}$$

4. Destination 2 performs similarly, and all the above inequalities hold by swapping the indices 1 and 2.

It is noteworthy that the bound in the rate of the interfering common message (112e), i.e., $R_{l0} \leq I(V_lX_3; Y_k|X_kQ) - I_k$, is a by-product of the CF scheme. Although the error in decoding the index of the interfering common message is normally not taken into account in the IC, this bound is needed in order to assure that the compression index s_j is the right one at time j. Nonetheless, both the bound (112e) and (112f) are redundant as we see next.

When (112e) does not hold, (112c) and (112d) become:

$$\begin{aligned} R_{11} &< I(X_1V_2X_3; Y_1|V_1Q) - I(V_2X_3; Y_1|X_1Q) \\ &= I(X_1; Y_1|V_1Q), \end{aligned} \tag{114a}$$
$$\begin{aligned} R_{10} + R_{11} &< I(X_1V_2X_3; Y_1|Q) - I(V_2X_3; Y_1|X_1Q) \\ &= I(X_1; Y_1|Q). \end{aligned} \tag{114b}$$

This is included in the region (113) for the special case $V_2 = \emptyset$.

Moreover, if (112f) does not hold, the first five bounds of (112) become:

$$\begin{aligned} R_{11} &< I(X_1X_3; Y_1|V_1V_2Q) - I_1 \\ &< I(X_1X_3; Y_1|V_1V_2Q) - I(X_3; Y_1|X_1V_2Q) \\ &= I(X_1; Y_1|V_1V_2Q), \end{aligned} \tag{115a}$$
$$R_{10}+R_{11} < I(X_1; Y_1|V_2Q), \tag{115b}$$
$$R_{20}+R_{11} < I(X_1V_2; Y_1|V_1Q), \tag{115c}$$
$$R_{10}+R_{11}+R_{20} < I(X_1V_2; Y_1|V_1Q), \tag{115d}$$
$$R_{20} < I(V_2; Y_1|X_1Q). \tag{115e}$$

This region is also included in (113). Therefore, when either condition (112e) or (112f) does not hold for a given distribution, the region (112) is included inside (113), i.e., destination 1 should ignore the relay to achieve higher rates. Since the final region is the union over all possible PDs of (112) and (113) for both users, we can drop (112e) and (112f) because they do not affect the final region after the maximization. This result can be seen as an extension of [7].

Before running FME to the system, we shall make same clarifications. First, let us define $\mathcal{R}_{\mathrm{CF}_3}(P_4)$ as the region obtained with the distribution P_4 when both users ignore the compression index, i.e., the HK inner bound. The regions $\mathcal{R}_{\mathrm{CF}_1}(P_4)$ and $\mathcal{R}_{\mathrm{CF}_2}(P_4)$ are the ones obtained when only the first or second user decodes the relay's message, respectively. $\mathcal{R}_{\mathrm{CF}_0}(P_4)$ corresponds to the region when both users decode the compression index.

Second, even though the expressions I_{ki} look rather complex, there exists an ordering between them analogous to I'_{ki} that allows us to reduce the number of bounds. In other words, the following inequalities hold,

$$I_{k1} \leq I_{k2} \leq I_{k4} \text{ and } I_{k1} \leq I_{k3} \leq I_{k4}. \tag{116}$$

To check this, take each term of I_{11} and I_{12} separately

$$\begin{aligned}
I_{11} &\leq I(X_1; Y_1\hat{Y}_3|V_1V_2X_3Q) \\
&= H(Y_1\hat{Y}_3|V_1V_2X_3Q) - H(Y_1\hat{Y}_3|X_1V_2X_3Q), && \text{(117a)} \\
I_{11} &\leq I(X_1X_3; Y_1|V_1V_2Q) - I_1 \\
&= H(Y_1|V_1V_2Q) - H(Y_1|X_1V_2X_3Q) - I_1, && \text{(117b)} \\
I_{12} &\leq I(X_1; Y_1\hat{Y}_3|V_2X_3Q) \\
&= H(Y_1\hat{Y}_3|V_2X_3Q) - H(Y_1\hat{Y}_3|X_1V_2X_3Q), && \text{(117c)} \\
I_{12} &\leq I(X_1X_3; Y_1|V_2Q) - I_1 \\
&= H(Y_1|V_2Q) - H(Y_1|X_1V_2X_3Q) - I_1. && \text{(117d)}
\end{aligned}$$

Since conditioning reduces entropy, we have that (117a) $\leq$ (117c) and (117b) $\leq$ (117d), which leads to $I_{11} \leq I_{12}$. The same reasoning applies for the other I_{ki} in (116).

Final Region $\mathcal{R}_{CF_3}$

After running FME to the system composed by (113) and its symmetric one for the second user, and letting $n \to \infty$, we obtain the region $\mathcal{R}^o_{\mathrm{CF}_3}(p)$:

$$\begin{aligned}
R_k &\leq \min\{I'_{k2}, I'_{k1} + I'_{l3}\}, \\
R_k + R_l &\leq \min\{I'_{k1} + I'_{l4}, I'_{k3} + I'_{l3}\}, \\
2R_k + R_l &\leq I'_{k1} + I'_{k4} + I'_{l3}.
\end{aligned}$$

This region has two redundant bounds as shown in [49]:

$$R_1 \leq I(X_1; Y_1|V_1V_2Q) + I(V_1X_2; Y_2|V_2Q), \tag{118a}$$
$$R_2 \leq I(X_1V_2; Y_1|V_1Q) + I(X_2; Y_2|V_1V_2Q). \tag{118b}$$

If we define $\mathcal{R}^c_{\text{CF}_3}(p)$ as the *compact* version of the *original* region $\mathcal{R}^o_{\text{CF}_3}(p)$, i.e., without the two redundant bounds, we can readily see that $\mathcal{R}^o_{\text{CF}_3}(p) \subseteq \mathcal{R}^c_{\text{CF}_3}(p)$ for a given distribution $p \in \mathcal{P}_4$ since $\mathcal{R}^c_{\text{CF}_3}(p)$ has fewer bounds.

If a pair of rates (R_1, R_2) belongs to $\mathcal{R}^c_{\text{CF}_3}(p)$ but not to $\mathcal{R}^o_{\text{CF}_3}(p)$, it is because (118) does not hold. Let us first assume that

$$R_1 > I(X_1; Y_1|V_1V_2Q) + I(V_1X_2; Y_2|V_2Q).$$

With this condition, $\mathcal{R}^c_{\text{CF}_3}(p)$ becomes:

$$\begin{aligned} R_1 &\leq I(X_1; Y_1|V_2Q), \\ R_2 &\leq I(V_2; Y_2|Q), \\ R_1 + R_2 &\leq I(X_1V_2; Y_1|Q), \end{aligned}$$

together with some additional bounds. We may compare this region with $\mathcal{R}^o_{\text{CF}_3}(p^*)$, where $p^* = \sum_{v_1} p$,

$$\begin{aligned} R_1 &\leq I(X_1; Y_1|V_2Q), \\ R_2 &\leq I(X_2; Y_2|Q), \\ R_1 + R_2 &\leq I(X_1V_2; Y_1|Q) + I(X_2; Y_2|V_2Q). \end{aligned}$$

It is clear that, when (118a) is violated, $\mathcal{R}^c_{\text{CF}_3}(p) \subseteq \mathcal{R}^o_{\text{CF}_3}(p^*)$.

Similarly, if (118b) does not hold, we see that $\mathcal{R}^c_{\text{CF}_3}(p) \subseteq \mathcal{R}^o_{\text{CF}_3}(p^{**})$, where $p^{**} = \sum_{v_2} p$. Therefore, in the general case,

$$\mathcal{R}^c_{\text{CF}_3}(p) \subseteq \mathcal{R}^o_{\text{CF}_3}(p) \cup \mathcal{R}^o_{\text{CF}_3}(p^*) \cup \mathcal{R}^o_{\text{CF}_3}(p^{**}).$$

Since we have already shown that $\mathcal{R}^o_{\text{CF}_3}(p) \subseteq \mathcal{R}^c_{\text{CF}_3}(p)$, when maximizing over all joint PDs, we have that $\mathcal{R}^o_{\text{CF}_3} = \mathcal{R}^c_{\text{CF}_3}$.

Final Regions $\mathcal{R}_{CF_1}$ and $\mathcal{R}_{CF_2}$

Now, we go to $\mathcal{R}^o_{\text{CF}_1}(p)$, where only the first user decodes the compression index. In this case, the region that is obtained after running FME is:

$$\begin{aligned} R_1 &\leq \min\{I_{12}, I_{11} + I'_{23}\}, \\ R_2 &\leq \min\{I'_{22}, I_{13} + I'_{21}\}, \\ R_1 + R_2 &\leq \min\{I_{11} + I'_{24}, I_{14} + I'_{21}, I_{13} + I'_{23}\}, \\ 2R_1 + R_2 &\leq I_{11} + I_{14} + I'_{23}, \\ R_1 + 2R_2 &\leq I_{13} + I'_{21} + I'_{24}. \end{aligned}$$

Here, we have another two redundant bounds:

$$R_1 \leq I_{11} + I(V_1X_2; Y_2|V_2Q), \tag{119a}$$
$$R_2 \leq I_{13} + I(X_2; Y_2|V_1V_2Q). \tag{119b}$$

Once again, for a given distribution $p \in \mathcal{P}_4$, we define $\mathcal{R}^o_{\mathrm{CF}_1}(p)$ as the original region with all the bounds and $\mathcal{R}^c_{\mathrm{CF}_1}(p)$ as the compact one without the redundant bounds. Since $\mathcal{R}^c_{\mathrm{CF}_1}(p)$ has fewer bounds, we can readily see that $\mathcal{R}^o_{\mathrm{CF}_1}(p) \subseteq \mathcal{R}^c_{\mathrm{CF}_1}(p)$.

If (119a) does not hold, $\mathcal{R}^c_{\mathrm{CF}_1}(p)$ becomes:

$$\begin{aligned} R_1 &\leq I_{12}, \\ R_2 &\leq I(V_2; Y_2|Q), \\ R_1 + R_2 &\leq I_{14}, \end{aligned}$$

together with some additional bounds. We may compare this region with $\mathcal{R}^o_{\mathrm{CF}_1}(p^*)$, where $p^* = \sum_{v_1} p$,

$$\begin{aligned} R_1 &\leq I_{12}, \\ R_2 &\leq I(X_2; Y_2|Q), \\ R_1 + R_2 &\leq I_{14} + I(X_2; Y_2|V_2Q). \end{aligned}$$

As we see, when (119a) is violated, $\mathcal{R}^c_{\mathrm{CF}_1}(p) \subseteq \mathcal{R}^o_{\mathrm{CF}_1}(p^*)$.

Since this region is not symmetric, we also need to see what happens when (119b) does not hold. In this case, $\mathcal{R}^c_{\mathrm{CF}_1}(p)$ becomes:

$$R_1 \leq I_{14} - I_{13}, \tag{120a}$$
$$R_2 \leq I(X_2; Y_2|V_1Q), \tag{120b}$$
$$R_1 + R_2 \leq I(V_1X_2; Y_2|Q), \tag{120c}$$

together with some additional bounds. Now, let us take $p^{**} = \sum_{v_2} p$ and calculate $\mathcal{R}^o_{\mathrm{CF}_1}(p^{**})$:

$$R_1 \leq I^*_{14}, \tag{121a}$$
$$R_2 \leq I(X_2; Y_2|V_1Q), \tag{121b}$$
$$R_2 \leq I^*_{13} + I(X_2; Y_2|V_1Q), \tag{121c}$$
$$R_1 + R_2 \leq I^*_{13} + I(V_1X_2; Y_2|Q) \tag{121d}$$

where

$$I^*_{13} \triangleq \min\{I(X_1; Y_1\hat{Y}_3|V_1X_3Q), I(X_1X_3; Y_1|V_1Q) - I(Y_3; \hat{Y}_3|X_1X_3Y_1Q)\},$$
$$I^*_{14} \triangleq \min\{I(X_1; Y_1\hat{Y}_3|X_3Q), I(X_1X_3; Y_1|Q) - I(Y_3; \hat{Y}_3|X_1X_3Y_1Q)\}.$$

We shall recall that the PD p is such that the rates R_1 and R_2 are nonnegative in $\mathcal{R}^c_{\mathrm{CF}_1}(p)$. However, this does not mean that I^*_{13} or I^*_{14} should be positive since they depend on p^{**}. If any of the two expressions is negative, $\mathcal{R}^c_{\mathrm{CF}_1}(p) \nsubseteq \mathcal{R}^o_{\mathrm{CF}_1}(p^{**})$, which is not what we are looking for. We first assume that both quantities are positive.

Let us define with a subscript a and b the first and second term of the minimums in the expressions I_{ki}, respectively. Then, if $I_{13} = I_{13a}$, the first rate in $\mathcal{R}^{c}_{\mathrm{CF}_1}(p)$ becomes:

$$R_1 \leq I_{14a} - I_{13a} = I(V_1; Y_1\hat{Y}_3|X_3Q) \leq I^*_{14a}, \tag{122a}$$

$$\begin{aligned} R_1 &\leq I_{14b} - I_{13a} \\ &= I(X_1V_2X_3; Y_1|Q) - I(Y_3; \hat{Y}_3|X_1V_2X_3Y_1Q) - I(X_1V_2; Y_1\hat{Y}_3|V_1X_3Q) \\ &= I(X_1V_2X_3; Y_1|Q) - I(Y_3; \hat{Y}_3|X_1V_2X_3Y_1Q) - I(X_1V_2; Y_1|V_1X_3Q) \\ &\quad - I(X_1V_2; \hat{Y}_3|V_1X_3Y_1Q) \\ &= I(V_1X_3; Y_1|Q) - I(X_1V_2Y_3; \hat{Y}_3|V_1X_3Y_1Q) \\ &= I(V_1X_3; Y_1|Q) - I(Y_3; \hat{Y}_3|V_1X_3Y_1Q) \leq I^*_{14b} \end{aligned} \tag{122b}$$

where in the last step we take into account that $\hat{Y}_3 \multimap (X_3Y_3Q) \multimap (X_1V_2)$. On the other hand, if $I_{13} = I_{13b}$, the first rate in $\mathcal{R}^{c}_{\mathrm{CF}_1}(p)$ becomes:

$$R_1 \leq I_{14b} - I_{13b} = I(V_1; Y_1|Q) \leq I^*_{14a}. \tag{123}$$

Also, in $\mathcal{R}^{o}_{\mathrm{CF}_1}(p^{**})$:

$$\begin{aligned} R_1 \leq I^*_{14b} &= I(X_1X_3; Y_1|Q) - I(Y_3; \hat{Y}_3|X_1X_3Y_1Q) \\ &= I(V_1; Y_1|Q) + I^*_{13b}. \end{aligned} \tag{124}$$

If we assume that $I^*_{13} \geq 0$, (122b) and (124) assure us that $I^*_{14} \geq 0$. Putting (120) through (124) together, we have shown that $\mathcal{R}^{c}_{\mathrm{CF}_1}(p) \subseteq \mathcal{R}^{o}_{\mathrm{CF}_1}(p^{**})$. However, if $I^*_{13} < 0$ we shall consider the case where the first user also ignores the compression index, i.e. $\mathcal{R}^{o}_{\mathrm{CF}_3}(p^{**})$,

$$R_1 \leq I(X_1; Y_1|Q), \tag{125a}$$

$$R_2 \leq I(X_2; Y_2|V_1Q), \tag{125b}$$

$$R_1 + R_2 \leq I(X_1; Y_1|V_1Q) + I(V_1X_2; Y_2|Q). \tag{125c}$$

The region in (120) looks smaller than (125), with the exception of the rate R_1 that we analyze in the sequel. If $I_{13} = I_{13a}$, in (120a) we have that,

$$\begin{aligned} R_1 &\leq I_{14} - I_{13} = \min\{I_{14a}, I_{14b}\} - I_{13a} \leq I_{14b} - I_{13a} \\ &= I(V_1X_3; Y_1|Q) - I(Y_3; \hat{Y}_3|V_1X_3Y_1Q) && \text{(126a)} \\ &= I(V_1X_3; Y_1|Q) - I(X_1; \hat{Y}_3|V_1X_3Y_1Q) - I(Y_3; \hat{Y}_3|X_1X_3Y_1Q) && \text{(126b)} \\ &< I(V_1X_3; Y_1|Q) - I(X_1; \hat{Y}_3|V_1X_3Y_1Q) - I(X_1X_3; Y_1|V_1Q) && \text{(126c)} \\ &\leq I(X_1X_3; Y_1|Q) - I(X_1; \hat{Y}_3|V_1X_3Y_1Q) - I(X_1X_3; Y_1|V_1Q) \\ &= I(V_1; Y_1|Q) - I(X_1; \hat{Y}_3|V_1X_3Y_1Q) \\ &\leq I(V_1; Y_1|Q), && \text{(126d)} \end{aligned}$$

where (126a) comes from (122b), (126b) is due to the Markov chain $\hat{Y}_3 \multimap (X_3Y_3Q) \multimap X_1$, and (126c) is due to the assumption $I^*_{13} < 0$, i.e. $I(X_1X_3; Y_1|V_1Q) < I(Y_3; \hat{Y}_3|X_1X_3Y_1Q)$.

On the other hand, if $I_{13} = I_{13b}$, we have already shown in (123) that $R_1 \leq I(V_1; Y_1|Q)$. Therefore, if $I^*_{13} < 0$, the region $\mathcal{R}^o_{\text{CF}_3}(p^{**})$ is larger than $\mathcal{R}^c_{\text{CF}_1}(p)$ when $R_2 > I_{13} + I(X_2; Y_2|V_1V_2Q)$. To sum up, in the general case,

$$\mathcal{R}^c_{\text{CF}_1}(p) \subseteq \mathcal{R}^o_{\text{CF}_1}(p) \cup \mathcal{R}^o_{\text{CF}_1}(p^*) \cup \mathcal{R}^o_{\text{CF}_1}(p^{**}) \cup \mathcal{R}^o_{\text{CF}_3}(p^{**}),$$

and since $\mathcal{R}^o_{\text{CF}_1}(p) \subseteq \mathcal{R}^c_{\text{CF}_1}(p)$, if we maximize over all joint possible joint distributions we obtain $\mathcal{R}^c_{\text{CF}_1} \cup \mathcal{R}^c_{\text{CF}_3} = \mathcal{R}^o_{\text{CF}_1} \cup \mathcal{R}^o_{\text{CF}_3}$.

The symmetric region $\mathcal{R}^o_{\text{CF}_2}(p)$ where only the second user decodes the compression index behaves similarly. We can redo the whole proof by simply swapping the subindices 1 and 2. Consequently, if we maximize over all joint possible joint distributions we have that $\mathcal{R}^c_{\text{CF}_2} \cup \mathcal{R}^c_{\text{CF}_3} = \mathcal{R}^o_{\text{CF}_2} \cup \mathcal{R}^o_{\text{CF}_3}$.

Final Region $\mathcal{R}_{CF_0}$

Finally, when both users decode the compression index, the region we obtain after running FME is,

$$\begin{aligned} R_k &\leq \min\{I_{k2}, I_{k1} + I_{l3}\}, \\ R_k + R_l &\leq \min\{I_{k1} + I_{l4}, I_{k3} + I_{l3}\}, \\ 2R_k + R_l &\leq I_{k1} + I_{k4} + I_{l3} \end{aligned}$$

where the redundant terms are

$$\begin{aligned} R_1 &\leq I_{11} + I_{23}, \\ R_2 &\leq I_{13} + I_{21}. \end{aligned}$$

We omit the complete proof for this region since it follows the same steps as the previous ones. The conclusion here is that the region $\mathcal{R}^c_{\text{CF}_0}(p)$, the one without the redundant terms, is larger than $\mathcal{R}^o_{\text{CF}_0}(p)$, and also,

$$\mathcal{R}^c_{\text{CF}_0}(p) \subseteq \mathcal{R}^o_{\text{CF}_0}(p) \cup \mathcal{R}^o_{\text{CF}_0}(p^*) \cup \mathcal{R}^o_{\text{CF}_1}(p^*) \cup \mathcal{R}^o_{\text{CF}_0}(p^{**}) \cup \mathcal{R}^o_{\text{CF}_2}(p^{**}).$$

Therefore, if we maximize over all possible joint distributions we have

$$\mathcal{R}^c_{\text{CF}_0} \cup \mathcal{R}^c_{\text{CF}_1} \cup \mathcal{R}^c_{\text{CF}_2} \cup \mathcal{R}^c_{\text{CF}_3} = \mathcal{R}^o_{\text{CF}_0} \cup \mathcal{R}^o_{\text{CF}_1} \cup \mathcal{R}^o_{\text{CF}_2} \cup \mathcal{R}^o_{\text{CF}_3}.$$

Since the region $\mathcal{R}_{\text{CF}_3}$ is a special case of $\mathcal{R}_{\text{CF}_0}$ in the maximization, we can eliminate it. The final region without redundant terms is (76) when both destinations decode the compression index, and the region (77) when one of them ignores it.

3.F PROOF OF PROPOSITION 3.1 (FULL DF CONSTANT GAP)

The comparison between the full DF inner bound (71) and the outer bound is complex mainly due to the different PDs in each bound

and the presence of the binning terms. However, as we see next, we can propose some simplifications to help us calculate the difference between the bounds.

First, let us assume the following set of auxiliary RVs,

$$V_1 = h_{21}X_1 + h_{23}X_3 + Z_2', \tag{127a}$$
$$V_2 = h_{12}X_2 + Z_1', \tag{127b}$$
$$V_3 = \frac{h_{23}}{\sqrt{1+S_{21}}}X_3 + Z_2'' \tag{127c}$$

where $S_{21} \triangleq |h_{21}|^2 P_1/N_2$, and Z_k' and Z_k'' are independent copies of Z_k. This choice fulfills the Markov chains in (70). Nonetheless, since it is a particular choice of variables, the region might be smaller than the optimal one.

Second, let us assume that X_1 and X_3 are independent. Then, the binning term becomes upper-bounded regardless of the channel coefficients,

$$I_b = \mathsf{C}\left[\frac{S_{23}}{1+S_{21}+S_{23}}\right] \leq \frac{1}{2} \text{ bit}.$$

We can reduce the achievable region (71) if we add $-I_b$ to (71c) and (71i) which render (71d) and (71h) redundant. We further shrink the region by replacing $-I_b$ with $-\frac{1}{2}$ which gives us,

$$R_1 \leq I(X_1; Y_3|X_3Q) \tag{128a}$$
$$R_1 \leq I(X_1X_3; Y_1|V_2Q) \tag{128b}$$
$$R_2 \leq I(X_2; Y_2|V_1V_3Q) - \frac{1}{2} \tag{128c}$$
$$R_1 + R_2 \leq I(X_1X_3; Y_1|V_1V_2V_3Q) + I(V_1X_2V_3; Y_2|Q) \tag{128d}$$
$$R_1 + R_2 \leq I(X_1; Y_3|V_1X_3Q) + I(V_1X_2V_3; Y_2|Q) - \frac{1}{2} \tag{128e}$$
$$R_1 + R_2 \leq I(X_1V_2X_3; Y_1|V_1V_3Q) + I(V_1X_2V_3; Y_2|V_2Q) \tag{128f}$$
$$R_1 + R_2 \leq I(X_1V_2X_3; Y_1|Q) + I(X_2; Y_2|V_1V_2V_3Q) - \frac{1}{2} \tag{128g}$$
$$\begin{aligned} 2R_1 + R_2 \leq\ & I(X_1X_3; Y_1|V_1V_2V_3Q) + I(X_1V_2X_3; Y_1|Q) \\ & + I(V_1X_2V_3; Y_2|V_2Q) \end{aligned} \tag{128h}$$
$$\begin{aligned} 2R_1 + R_2 \leq\ & I(X_1; Y_3|V_1X_3Q) + I(X_1V_2X_3; Y_1|Q) \\ & + I(V_1X_2V_3; Y_2|V_2Q) - \frac{1}{2} \end{aligned} \tag{128i}$$
$$\begin{aligned} R_1 + 2R_2 \leq\ & I(X_1V_2X_3; Y_1|V_1V_3Q) + I(X_2; Y_2|V_1V_2V_3Q) \\ & + I(V_1X_2V_3; Y_2|Q) \end{aligned} \tag{128j}$$

These bounds look similar to the following subset of the outer bound (66): (66a)–(66g), (66l), (66n), and (66r), which allows us to compare them. However, as the PDs present in the inner and outer bounds are different, we compare the expression of each bound in the Gaussian case since they only depend on the SNRs of the links.

The reduced region (128) for the Gaussian case is,

$$R_1 \leq \mathsf{C}[S_{31}] \tag{129a}$$

$$R_1 \leq \mathsf{C}[G_2(S_{11}+S_{13})] \tag{129b}$$

$$R_2 \leq \mathsf{C}[G_1 S_{22}] - \frac{1}{2} \tag{129c}$$

$$R_1+R_2 \leq \mathsf{C}\left[G_2 \frac{S_{11}+S_{13}+\delta+S_{11}S_{23}/(1+S_{21})}{1+S_{21}+2S_{23}}\right] + \mathsf{C}[S_{21}+S_{22}+S_{23}] + \frac{1}{2}\log_2 G_1 \tag{129d}$$

$$R_1+R_2 \leq \mathsf{C}\left[\frac{S_{31}}{1+S_{21}}\right] + \mathsf{C}[S_{21}+S_{22}+S_{23}] + \frac{1}{2}\log_2 G_1 - \frac{1}{2} \tag{129e}$$

$$R_1+R_2 \leq \mathsf{C}\left[S_{12}+\frac{S_{11}+S_{13}+\delta+S_{11}S_{23}/(1+S_{21})}{1+S_{21}+2S_{23}}\right] + \mathsf{C}\left[S_{21}+S_{23}+\frac{S_{22}}{1+S_{12}}\right] + \frac{1}{2}\log_2 G_1 G_2 \tag{129f}$$

$$R_1+R_2 \leq \mathsf{C}[S_{11}+S_{12}+S_{13}] + \mathsf{C}\left[G_1\frac{S_{22}}{1+S_{12}}\right] + \frac{1}{2}\log_2 G_2 - \frac{1}{2} \tag{129g}$$

$$2R_1+R_2 \leq \mathsf{C}\left[G_2 \frac{S_{11}+S_{13}+\delta+S_{11}S_{23}/(1+S_{21})}{1+S_{21}+2S_{23}}\right] + \frac{1}{2}\log_2 G_1 G_2 + \mathsf{C}[S_{11}+S_{12}+S_{13}] + \mathsf{C}\left[S_{21}+S_{23}+\frac{S_{22}}{1+S_{12}}\right] \tag{129h}$$

$$2R_1+R_2 \leq \mathsf{C}\left[\frac{S_{31}}{1+S_{21}}\right] + \mathsf{C}[S_{11}+S_{12}+S_{13}] + \frac{1}{2}\log_2 G_1 G_2 - \frac{1}{2} + \mathsf{C}\left[S_{21}+S_{23}+\frac{S_{22}}{1+S_{12}}\right] \tag{129i}$$

$$R_1+2R_2 \leq \mathsf{C}\left[S_{12}+\frac{S_{11}+S_{13}+\delta+S_{11}S_{23}/(1+S_{21})}{1+S_{21}+2S_{23}}\right] + \mathsf{C}\left[G_1\frac{S_{22}}{1+S_{12}}\right] + \mathsf{C}[S_{21}+S_{22}+S_{23}] + \frac{1}{2}\log_2 G_1 G_2, \tag{129j}$$

where $\delta \triangleq \left(\sqrt{S_{11}S_{23}} \pm \sqrt{S_{13}S_{21}}\right)^2$ and

$$G_1 \triangleq \frac{1+2S_{21}+2S_{23}+S_{21}^2+2S_{21}S_{23}}{1+3S_{21}+3S_{23}+2S_{21}^2+4S_{21}S_{23}},$$

$$G_2 \triangleq \frac{1+S_{12}}{1+2S_{12}}.$$

To illustrate the procedure for bounding the gap, we show the single-rate gaps in the sequel. Consider,

$$\begin{aligned}\Delta_{R_1} &= (67a) - (129a)\\ &= \mathsf{C}[S_{11}+S_{31}] - \mathsf{C}[S_{31}]\\ &= \mathsf{C}\left[\frac{S_{11}}{1+S_{31}}\right] \leq \frac{1}{2},\end{aligned} \tag{130}$$

where the last inequality is due to $S_{31} \geq S_{11}$, otherwise, the gap would be unbounded. Additionally,

$$\begin{aligned}\Delta_{R_1} &= (67b) - (129b) \\ &= \mathsf{C}[S_{11} + S_{13}] + \frac{1}{2} - \mathsf{C}[G_2(S_{11} + S_{13})] \\ &\leq \frac{1}{2} - \frac{1}{2}\log_2 G_2 \leq 1, \end{aligned} \tag{131}$$

where the last two inequalities are due to $\frac{1}{2} \leq G_2 \leq 1$. For R_2 we have,

$$\begin{aligned}\Delta_{R_2} &= (67c) - (129c) \\ &= \mathsf{C}[S_{22}] - \mathsf{C}[G_1 S_{22}] + \frac{1}{2} \\ &\leq \frac{1}{2} - \frac{1}{2}\log_2 G_1 \leq 1, \end{aligned} \tag{132}$$

where the last two inequalities are due to $\frac{1}{2} \leq G_1 \leq 1$. In summary, if we compare the appropriate pair of bounds and we assume $S_{31} \geq S_{11}$, we obtain the following gaps

$$\begin{aligned} \Delta_{R_1} &\leq \frac{1}{2}, & \Delta_{R_1+R_2} &\leq 2, \\ \Delta_{R_1} &\leq 1, & \Delta_{R_1+R_2} &\leq 2, \\ \Delta_{R_2} &\leq 1, & \Delta_{2R_1+R_2} &\leq 3, \\ \Delta_{R_1+R_2} &\leq 2, & \Delta_{2R_1+R_2} &\leq 3, \\ \Delta_{R_1+R_2} &\leq 2, & \Delta_{R_1+2R_2} &\leq \frac{5}{2}. \end{aligned}$$

Therefore, the gap between the outer bound and the full DF inner bound, when $S_{31} \geq S_{11}$, is 1 bit per real dimension at most.

3.G PROOF OF PROPOSITION 3.2 (PARTIAL DF CONSTANT GAP)

The analysis of the gap for the partial DF scheme follows similar steps as the one for the full DF scheme. We enlarge the set of auxiliary RVs used in Appendix 3.F with

$$U_1 = h_{31}X_1 + Z_3'. \tag{133}$$

Then, we reduce the achievable region using the assumptions of independence between X_1 and X_3 and the upper bound in the binning term, which gives us,

$$R_1 \leq I(U_1; Y_3|X_3Q) + I(X_1; Y_1|V_1U_1V_2X_3Q), \tag{134a}$$
$$R_1 \leq I(X_1X_3; Y_1|V_2Q), \tag{134b}$$

$$R_2 \le I(X_2;Y_2|V_1V_3Q) - \frac{1}{2}, \tag{134c}$$
$$R_1 + R_2 \le I(X_1X_3;Y_1|V_1V_2V_3Q) + I(V_1X_2V_3;Y_2|Q), \tag{134d}$$
$$R_1 + R_2 \le I(U_1;Y_3|V_1X_3Q) + I(X_1;Y_1|V_1U_1V_2X_3Q) + I(V_1X_2V_3;Y_2|Q) - \frac{1}{2}, \tag{134e}$$
$$R_1 + R_2 \le I(X_1V_2X_3;Y_1|V_1V_3Q) + I(V_1X_2V_3;Y_2|V_2Q), \tag{134f}$$
$$R_1 + R_2 \le I(U_1;Y_3|V_1X_3Q) + I(X_1V_2;Y_1|V_1U_1X_3Q) + I(V_1X_2V_3;Y_2|V_2Q) - \frac{1}{2}, \tag{134g}$$
$$R_1 + R_2 \le I(X_1V_2X_3;Y_1|Q) + I(X_2;Y_2|V_1V_2V_3Q) - \frac{1}{2}, \tag{134h}$$
$$R_1 + R_2 \le I(U_1;Y_3|X_3Q) + I(X_1V_2;Y_1|V_1U_1X_3Q) + I(X_2;Y_2|V_1V_2V_3Q), \tag{134i}$$
$$2R_1 + R_2 \le I(X_1X_3;Y_1|V_1V_2V_3Q) + I(X_1V_2X_3;Y_1|Q) + I(V_1X_2V_3;Y_2|V_2Q), \tag{134j}$$
$$2R_1 + R_2 \le I(X_1X_3;Y_1|V_1V_2V_3Q) + I(X_1V_2;Y_1|V_1U_1X_3Q) + I(U_1;Y_3|X_3Q) + I(V_1X_2V_3;Y_2|V_2Q), \tag{134k}$$
$$2R_1 + R_2 \le I(U_1;Y_3|V_1X_3Q) + I(X_1;Y_1|V_1U_1V_2X_3Q) - \frac{1}{2} + I(X_1V_2X_3;Y_1|Q) + I(V_1X_2V_3;Y_2|V_2Q), \tag{134l}$$
$$R_1 + 2R_2 \le I(X_1V_2X_3;Y_1|V_1V_3Q) + I(X_2;Y_2|V_1V_2V_3Q) + I(V_1X_2V_3;Y_2|Q), \tag{134m}$$
$$R_1 + 2R_2 \le I(U_1;Y_3|V_1X_3Q) + I(X_1V_2;Y_1|V_1U_1X_3Q) - \frac{1}{2} + I(X_2;Y_2|V_1V_2V_3Q) + I(V_1X_2V_3;Y_2|Q). \tag{134n}$$

We can compare these bounds with a larger subset of the outer bound (66): (66a)–(66i), (66l)–(66n), and (66r)–(66s).

Half of the bounds in (134) are the same as in (128), while the other half –composed by the bounds (134a), (134e), (134g), (134i), (134k), (134l), and (134n)– have the following new terms:

$$I(U_1;Y_3|X_3Q) = \mathsf{C}[S_{31}] + \frac{1}{2}\log_2 G_{31},$$
$$I(U_1;Y_3|V_1X_3Q) = \mathsf{C}\left[\frac{S_{31}}{1+S_{21}}\right] + \frac{1}{2}\log_2 G_{32},$$
$$I(X_1;Y_1|V_1U_1V_2X_3Q) = \mathsf{C}\left[G_2\frac{S_{11}}{1+S_{21}+S_{31}}\right],$$
$$I(X_1V_2;Y_1|V_1U_1X_3Q) = \mathsf{C}\left[S_{12} + \frac{S_{11}}{1+S_{21}+S_{31}}\right] + \frac{1}{2}\log_2 G_2$$

where

$$G_{31} \triangleq \frac{1+S_{31}}{1+2S_{31}}, \quad \text{and} \quad G_{32} \triangleq \frac{1+S_{21}+S_{31}}{1+S_{21}+2S_{31}}.$$

Let us analyze only one of the gaps that change,

$$\begin{aligned}\Delta_{R_1} &= (67a) - (134a) = \mathsf{C}[S_{11} + S_{31}] - \mathsf{C}[S_{31}] \\ &\quad - \frac{1}{2}\log_2 G_{31} - \mathsf{C}\left[G_2 \frac{S_{11}}{1 + S_{21} + S_{31}}\right] \\ &\leq \mathsf{C}\left[\frac{S_{21}}{1 + S_{31}}\right] - \frac{1}{2}\log_2 G_{31} G_2 \leq \frac{3}{2}, \end{aligned} \tag{135}$$

where the last inequality is due to $S_{31} \geq S_{21}$, otherwise, the gap would be unbounded.

The gap between each pair of bounds in the inner and outer bound is,

$$\begin{aligned} \Delta_{R_1} &\leq \frac{3}{2}, & \Delta_{R_1+R_2} &\leq 2, \\ \Delta_{R_1} &\leq 1, & \Delta_{R_1+R_2} &\leq 2, \\ \Delta_{R_2} &\leq 1, & \Delta_{2R_1+R_2} &\leq 3, \\ \Delta_{R_1+R_2} &\leq 2, & \Delta_{2R_1+R_2} &\leq \frac{7}{2}, \\ \Delta_{R_1+R_2} &\leq \frac{5}{2}, & \Delta_{2R_1+R_2} &\leq \frac{7}{2}, \\ \Delta_{R_1+R_2} &\leq 2, & \Delta_{R_1+2R_2} &\leq \frac{5}{2}, \\ \Delta_{R_1+R_2} &\leq \frac{5}{2}, & \Delta_{R_1+2R_2} &\leq 3. \end{aligned}$$

In the previous calculations we assumed that $S_{31} \geq S_{21}$. Therefore, under this condition, the gap between the outer bound and the partial DF inner bound is 1.5 bits per real dimension at most.

3.H PROOF OF PROPOSITION 3.3 (CF CONSTANT GAP)

In this section, we show the constant gap result for the CF inner bound. As with the previous two schemes, we propose some simplifications to help in the analysis which, at the same time, reduce the region. First, we only take the region $\mathcal{R}_{\mathrm{CF}_0}$ (76) into account. This means that we force both end users to decode the compression index when we have already stated in the proof of the scheme that sometimes is better to ignore this message.

Second, the compressed channel observation of the relay is obtained by adding an independent Gaussian noise $Z \sim \mathcal{N}(0, N)$ to its channel output,

$$\hat{Y}_3 = Y_3 + Z.$$

Third, the random variables used in the scheme have the following structure. Given the independent RVs V_1, V_2, X_1', and X_2', all distributed according to $\mathcal{N}(0,1)$, we construct X_1 and X_2 as follows:

$$X_1 = \sqrt{\alpha_1 P_1} V_1 + \sqrt{\bar{\alpha}_1 P_1} X_1',$$
$$X_2 = \sqrt{\alpha_2 P_2} V_2 + \sqrt{\bar{\alpha}_2 P_2} X_2'$$

where $\alpha_i \in [0,1]$ and $\bar{\alpha}_i \triangleq 1 - \alpha_i$. Furthermore, inspired by [19] and taking into account the presence of the relay's compressed channel output, we choose the fixed power split strategy

$$\bar{\alpha}_1 \left(1 + S_{21} + \frac{S_{31}}{1+N}\right) = 1,$$
$$\bar{\alpha}_2 \left(1 + S_{12}\right) = 1.$$

The expression of the bounds (74) in the Gaussian case, where we assume $N_3 = 1$ for simplicity, can be found at the bottom of the next page.

We start by calculating the gap for the single rate $R_1 \leq I_{12a}$ with the bound (66a) from the outer bound:

$$\begin{aligned}
\Delta_{R_1} &= I(X_1; Y_1 Y_3 | X_2 X_3 Q) - I(X_1; Y_1 \hat{Y}_3 | V_2 X_3 Q) \\
&\leq \frac{1}{2}\log_2\{1 + S_{11} + S_{31}\} \\
&\quad - \frac{1}{2}\log_2\left\{\frac{(1+N)(1+S_{11}/2) + S_{31}}{1+N}\right\} && \text{(136a)} \\
&= \frac{1}{2}\log_2\left\{1 + \frac{(1+N)S_{11}/2 + NS_{31}}{(1+N)(1+S_{11}/2) + S_{31}}\right\} \\
&\leq \begin{cases} \frac{1}{2} + \mathsf{C}\left[\frac{N}{1+N}\right] & \text{if } S_{31} < S_{11} \\ \log_2 \frac{3}{2} + \mathsf{C}[N] & \text{if } S_{31} \geq S_{11} \end{cases} && \text{(136b)}
\end{aligned}$$

where in (136a) we have reduced the expression of the inner bound by adding $(1+N)\bar{\alpha}_2$ in the denominator and then, we apply the fixed power split strategy; and (136b) is obtained by eliminating either $(1+N)(1+S_{11}/2)$ or S_{31} from the denominator and taking into account that $S_{31} \lesseqgtr S_{11}$.

Next, we compare $R_1 \leq I_{12b}$ with the bound (66b):

$$\begin{aligned}
\Delta_{R_1} &= I(X_1 X_3; Y_1 | X_2 Q) - [I(X_1 X_3; Y_1 | V_2 Q) - I_1] \\
&\leq \frac{1}{2}\log_2\{1 + S_{11} + S_{13}\} + \frac{1}{2} \\
&\quad - \frac{1}{2}\log_2\left\{\frac{N(1 + S_{11} + S_{13})}{(1+N)(1+\bar{\alpha}_2 S_{12})}\right\} && \text{(137a)} \\
&\leq \frac{1}{2} + \frac{1}{2}\log_2\left\{\frac{2(1+N)}{N}\right\} \\
&= 1 + \mathsf{C}\left[\frac{1}{N}\right] && \text{(137b)}
\end{aligned}$$

where in (137a) we have already reduced the expression of the inner bound by eliminating the term $\bar{\alpha}_2 S_{12}$. If $S_{31} < S_{11}$, the gap for R_1 is dominated by (137b), since it is always greater than (136b), otherwise, the gap is the maximum of both.

Upper bounds on the gap of single rates and sum-rates can be derived using the expressions from the outer bound (66a)–(66c), (66f)–(66k), (66n)–(66q), and (66s)–(66t), and the assumption $S_{31} < S_{21}$ is needed for the gap to be bounded. These upper bounds on the gap

---

$$
\begin{aligned}
I_{11} = \min\Bigg\{ & \frac{1}{2}\log_2\left\{\frac{(1+N)(1+\bar{\alpha}_1 S_{11}+\bar{\alpha}_2 S_{12})+\bar{\alpha}_1 S_{31}(1+\bar{\alpha}_2 S_{12})}{(1+N)(1+\bar{\alpha}_2 S_{12})}\right\}, \\
& \frac{1}{2}\log_2\left\{\frac{N(1+\bar{\alpha}_1 S_{11}+\bar{\alpha}_2 S_{12}+S_{13})}{(1+N)(1+\bar{\alpha}_2 S_{12})}\right\}\Bigg\}, \\
I_{12} = \min\Bigg\{ & \frac{1}{2}\log_2\left\{\frac{(1+N)(1+S_{11}+\bar{\alpha}_2 S_{12})+S_{31}(1+\bar{\alpha}_2 S_{12})}{(1+N)(1+\bar{\alpha}_2 S_{12})}\right\}, \\
& \frac{1}{2}\log_2\left\{\frac{N(1+S_{11}+\bar{\alpha}_2 S_{12}+S_{13})}{(1+N)(1+\bar{\alpha}_2 S_{12})}\right\}\Bigg\}, \\
I_{13} = \min\Bigg\{ & \frac{1}{2}\log_2\left\{\frac{(1+N)(1+\bar{\alpha}_1 S_{11}+S_{12})+\bar{\alpha}_1 S_{31}(1+S_{12})}{(1+N)(1+\bar{\alpha}_2 S_{12})}\right\}, \\
& \frac{1}{2}\log_2\left\{\frac{N(1+\bar{\alpha}_1 S_{11}+S_{12}+S_{13})}{(1+N)(1+\bar{\alpha}_2 S_{12})}\right\}\Bigg\}, \\
I_{14} = \min\Bigg\{ & \frac{1}{2}\log_2\left\{\frac{(1+N)(1+S_{11}+S_{12})+S_{31}(1+S_{12})}{(1+N)(1+\bar{\alpha}_2 S_{12})}\right\}, \\
& \frac{1}{2}\log_2\left\{\frac{N(1+S_{11}+S_{12}+S_{13})}{(1+N)(1+\bar{\alpha}_2 S_{12})}\right\}\Bigg\}, \\
I_{21} = \min\Bigg\{ & \frac{1}{2}\log_2\left\{\frac{(1+N)(1+\bar{\alpha}_1 S_{21}+\bar{\alpha}_2 S_{22})+\bar{\alpha}_1 S_{31}(1+\bar{\alpha}_2 S_{22})}{(1+N)(1+\bar{\alpha}_1 S_{21})+\bar{\alpha}_1 S_{31}}\right\}, \\
& \frac{1}{2}\log_2\left\{\frac{N(1+\bar{\alpha}_1 S_{21}+\bar{\alpha}_2 S_{22}+S_{23})}{(1+N)(1+\bar{\alpha}_1 S_{21})+\bar{\alpha}_1 S_{31}}\right\}\Bigg\}, \\
I_{22} = \min\Bigg\{ & \frac{1}{2}\log_2\left\{\frac{(1+N)(1+\bar{\alpha}_1 S_{21}+S_{22})+\bar{\alpha}_1 S_{31}(1+S_{22})}{(1+N)(1+\bar{\alpha}_1 S_{21})+\bar{\alpha}_1 S_{31}}\right\}, \\
& \frac{1}{2}\log_2\left\{\frac{N(1+\bar{\alpha}_1 S_{21}+S_{22}+S_{23})}{(1+N)(1+\bar{\alpha}_1 S_{21})+\bar{\alpha}_1 S_{31}}\right\}\Bigg\}, \\
I_{23} = \min\Bigg\{ & \frac{1}{2}\log_2\left\{\frac{(1+N)(1+S_{21}+\bar{\alpha}_2 S_{22})+S_{31}(1+\bar{\alpha}_2 S_{22})}{(1+N)(1+\bar{\alpha}_1 S_{21})+\bar{\alpha}_1 S_{31}}\right\}, \\
& \frac{1}{2}\log_2\left\{\frac{N(1+S_{21}+\bar{\alpha}_2 S_{22}+S_{23})}{(1+N)(1+\bar{\alpha}_1 S_{21})+\bar{\alpha}_1 S_{31}}\right\}\Bigg\}, \\
I_{24} = \min\Bigg\{ & \frac{1}{2}\log_2\left\{\frac{(1+N)(1+S_{21}+S_{22})+S_{31}(1+S_{22})}{(1+N)(1+\bar{\alpha}_1 S_{21})+\bar{\alpha}_1 S_{31}}\right\}, \\
& \frac{1}{2}\log_2\left\{\frac{N(1+S_{21}+S_{22}+S_{23})}{(1+N)(1+\bar{\alpha}_1 S_{21})+\bar{\alpha}_1 S_{31}}\right\}\Bigg\}.
\end{aligned}
$$

were analyzed numerically, due to their complexity, and after cumbersome calculations the largest gap comes from the sum-rate:

$$\begin{aligned}\Delta_{R_1+R_2} &\leq \min\{(66h),(66k)\} - [\, I_{13} + I_{23}\,] \\ &\leq \max\{(66k) - [\, I_{13b} + I_{23a}\,],\ (66h) - [\, I_{13b} + I_{23b}\,]\} \\ &\leq 1 + \mathsf{C}\left[\frac{1}{N}\right] + \max\left\{\mathsf{C}[N] + \mathsf{C}\left[\frac{1+2N}{2+N}\right],\ 1+\mathsf{C}\left[\frac{1}{N}\right]\right\}.\end{aligned}$$

The value of N that minimizes this gap is $N \approx 1.81$, with the gap per real dimension being approximately 1.32 bits.

3.1 PROOF OF PROPOSITION 3.4 (LIMITED RELAYING BENEFIT)

Let us define $\mathcal{R}_{o'}(P_1)$ as the outer bound region composed by the bounds (66a), (66c), (66i)–(66k), (66q), and (66t). This new outer bound is analogous to the outer bound presented by Telatar and Tse [5] with the addition of the *antenna* Y_3. If the quality of the source-to-relay link is really low, this extra antenna does not provide much information and thus, both outer bounds should be within a constant gap. Since the gap between the HK inner bound and Telatar-Tse's outer bound is half a bit, it follows that HK scheme is within a constant gap to our outer bound under the aforementioned conditions.

We only show one of these gaps here, but all of them can be derived similarly. The expression for (66j) in the Gaussian case, i.e., (67j), is

$$\begin{aligned}(R_1+R_2)_{IS-IRC} &= I(X_1;Y_1Y_3|\underline{V_1}X_2X_3) + I(X_1X_2;Y_2Y_3|X_3) \\ &\leq \mathsf{C}\left[\frac{S_{11}+S_{31}}{1+S_{21}+S_{31}}\right] + \mathsf{C}[S_{21}+S_{22}+S_{31}(1+S_{22})]\,,\end{aligned} \tag{138}$$

while the analogous bound in Telatar-Tse's outer bound is

$$\begin{aligned}(R_1+R_2)_{IC} &= I(X_1;Y_1|V_1X_2) + I(X_1X_2;Y_2) \\ &= \mathsf{C}\left[\frac{S_{11}}{1+S_{21}}\right] + \mathsf{C}[S_{21}+S_{22}]\,.\end{aligned} \tag{139}$$

Then, we calculate the gap between (138) and (139)

$$\begin{aligned}\Delta_{ob} &= (R_1+R_2)_{IS-IRC} - (R_1+R_2)_{IC} \\ &= \mathsf{C}\left[\frac{2S_{31}}{1+S_{11}+S_{21}}\right] - \mathsf{C}\left[\frac{S_{31}}{1+S_{21}}\right] + \mathsf{C}\left[\frac{S_{31}}{1+\frac{S_{21}}{1+S_{22}}}\right] \\ &\leq \mathsf{C}\left[\frac{2S_{31}}{1+S_{11}+S_{21}}\right] + \mathsf{C}\left[\frac{S_{31}}{1+\frac{S_{21}}{1+S_{22}}}\right].\end{aligned}$$

The gap in this sum-rate can be upper bounded by 1 bit given that $S_{31} \leq S_{11}$ and $S_{31} \leq S_{21}/(1+S_{22})$. Further analysis of the other

bounds assures that the gap between outer bounds is half a bit per rate if $S_{31} \leq S_{11}/(1+S_{12})$ and $S_{31} \leq S_{21}/(1+S_{22})$ hold. Therefore, the use of the relay can improve the rate by at most 1 bit per real dimension compared to the HK scheme without the relay.

Part II

WIRETAP CHANNEL WITH GENERALIZED FEEDBACK

4

INTRODUCTION AND SETUP

4.1 INTRODUCTION

In recent years, there has been great interest in the study of the wiretap channel (WTC) [51] as a model for secure communications against eavesdroppers by harnessing the randomness present in the physical medium (see [3] and references therein). Application to secure wireless networks is extremely attractive, not only because the open nature of the medium makes communication devices particularly sensitive to eavesdropping, but also because randomness is abundantly available in such scenarios. As a matter of fact, the current theory of physical layer security indicates that securing part of the data can be provided at minimal –or even no– cost in the total throughput. A crucial observation behind this promising result is that unless the legitimate and the eavesdropper channels enjoy different statistical properties, which is often a nonrealistic assumption, secrecy cannot be guaranteed. Nevertheless, if both channels share the same statistical properties but some extra outdated side information is available at the transmitter, then the encoder can create the asymmetry required to ensure security (e.g. see [52, 53]).

As a matter of fact, this observation reveals one of the major limitations of the wiretap model whose performance strongly depends on the amount of outdated side information that may be available at the transmitter. Studying the impact on secrecy systems of different types of instantaneous information is therefore of both practical and theoretical interest.

In this work, we investigate the problem where a node, referred to as Alice, wishes to secretly communicate a message to another node, referred to as Bob, in presence of a passive eavesdropper, referred to as Eve. Alice can communicate with Bob using a general memoryless channel but Eve is listening this communication through another memoryless channel, whose statistical properties can be different or equal to Bob's channel. In addition, we assume that Alice observes general –may be noisy– outdated feedback, which is correlated to the channel outputs of Bob and Eve, referred to as "generalized feedback". It is worth mentioning that this feedback model is rich enough since it handles several different types of outdated side information

at the transmitter (e.g. models with delayed state-feedback and noisy feedback of the channel outputs) and thus provides the adequate framework to investigate the impact of the feedback model.

4.1.1 *Related Work*

There has been substantial work on the WTC with different feedback models, however, the capacity in the general case remains unresolved. Feedback, even partial, is known to increase the capacity of several multi-terminal networks with respect to the non-feedback case (e.g., broadcast [54] and multiple access channels [55]). The transmitter uses the feedback signal to provide the decoder with noisy functions of the channel noise or parameters, and the messages. This communication is accomplished by two fundamentally different classes of coding schemes: those based on block Markov (digital) coding [54,55], and those based on linear (analog) encoding [56], known as Schalkwijk-Kailath (SK) scheme, which perform well over additive Gaussian models.

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

Results based on the secret key approach are numerous, as it seems natural to use the feedback link (secure or not) to agree upon a key. In [9], the authors analyze the WTC with perfect output feedback only at the encoder and propose a scheme based on this approach. This scheme achieves the capacity of the *degraded*, i.e., $X \multimap Y \multimap Z$, and *reversely degraded*, i.e., $X \multimap Z \multimap Y$, WTC with perfect output feedback. The case of parallel channels, i.e., $Y \multimap X \multimap Z$, is studied in [57], where secrecy capacity is found when one of the channels is *more capable* than the other. A similar model to [9], where the feedback link is in fact a secure rate-limited channel from Bob to Alice, is presented in [58]. In contrast to the previous schemes, the key is here created with *fresh* randomness that Bob sends.

The use of state-feedback as a means to generate a key has also been analyzed, either when it is known only by the legitimate users [59] or by all the nodes in the network [60]. The authors of [59] propose

a lower bound for the general discrete memoryless WTC with state information at both the encoder and decoder, which is tight in several scenarios, e.g., when Bob is *less noisy* than Eve, or when Eve is less noisy than Bob and the channel is independent of the state. Additionally, in [60], the authors study a communication scenario where an encoder transmits private messages to several receivers through a broadcast erasure channel, and the receivers feedback (publicly) their channel states. Capacity is characterized based on linear complexity two-phase schemes: in the first phase appropriate secret keys are generated which are exploited during the second phase to encrypt each message.

Indeed, the generation of the secret key is a problem in and of itself [61, 62]. Two models exist that tackle this issue: the "source model", when the generation is based on the common randomness present in correlated sources, and the "channel model", when the common randomness is due to the correlation between inputs and outputs of the channel. The authors of [8] study the first model, where two nodes generate common randomness with the aid of a third "helper" node, all of them connected by noiseless rate-limited links. This common randomness may be kept secret from a fourth passive node that acts as an eavesdropper. More recently, [63] investigates the situation where there is no helper node, the users communicate over a WTC, and a public discussion channel may or may not be available. On the other hand, [64] analyzes key agreement over a multiple access channel, i.e., the channel model. Here the receiver can actively send feedback, through a noiseless or noisy link, to increase the size of the shared key.

Results based on the "feedback-dependent codebook" approach, however, are not that numerous to the best of our knowledge. Early work in [65] studies the multiple access channel with generalized feedback and secrecy constraints. There, the authors propose lower bounds based on compress-and-forward (CF) to increase the transmission rates to levels that are no longer decodable by the cooperating encoders. State-feedback can also be used to prevent the eavesdropper from decoding the transmitted codeword. In [52, 53], it is shown that state-feedback of either the legitimate channel, the eavesdropper's channel or both, increases the secure degrees of freedom (SDoF) of the two-user Gaussian multiple-input multiple-output (MIMO) WTC.

The destination can also take part in concealing the information present in the channel. Active feedback in a half-duplex fashion is used in [66], where communication is split in two phases. In the first one, the destination sends a random codeword which cannot be decoded by the eavesdropper. On top of this "interference sequence", the codeword to be transmitted in the second phase is superimposed. This scheme achieves positive secrecy rates in the MIMO WTC even when the eavesdropper has more antennas than the source. In [67],

the modulo-additive WTC with a full-duplex destination node is investigated. The authors propose a scheme where the legitimate receiver injects noise in the backward (feedback) channel, effectively eliminating any correlation between the message sent and the eavesdropper's observation. This scheme achieves the full capacity of the point-to-point (PtP) channel in absence of the wiretapper, i.e., full secrecy can be guaranteed at no rate cost.

A similar conclusion is also drawn in [10], where the authors analyze an additive white Gaussian noise (AWGN) channel with perfect output feedback from the legitimate receiver. They propose a SK-based coding scheme which achieves the full capacity of the AWGN channel in absence of the wiretapper, as long as the eavesdropper only has access to a noisy feedback signal.

A closely related topic to the one addressed in this part of the thesis is the WTC with *noncausal* side-information available to the parties. The model where the side-information is only available at the encoder is studied in [68], where an inner bound based on Gelfand and Pinsker's strategy for channels with state [69] is introduced. An extension to this model, with both the encoder and legitimate decoder having access to correlated side-information, is investigated in [70]. More recently, the authors of [71] analyze a slightly different scenario where the state affecting the legitimate decoder's channel is not equal to the one affecting the eavesdropper's channel. These channel states are correlated and the encoder only knows the state of the legitimate decoder's channel.

4.1.2 *Our Contribution*

In this work, we present two different inner bounds on the capacity of the memoryless wiretap channel with generalized feedback (WCGF), using the two different approaches mentioned earlier. We first derive an inner bound that is based on the use of joint source-channel coding, which introduces time dependencies between the noisy functions and the channel inputs through different blocks. We then introduce a second inner bound based on the secret key approach, where the feedback link is used to generate a key that encrypts the message partially or completely. These new bounds extend several existing bounds that were obtained for special classes of networks and feedback models. Our results can be seen as a generalization and thus unification of several results in the field.

Moreover, as a side result, we derive an inner bound on secret key agreement for the same channel model. The channel is used both as a source of correlated randomness and as a means of communication, i.e., there is no parallel public noiseless channel used by the terminals.

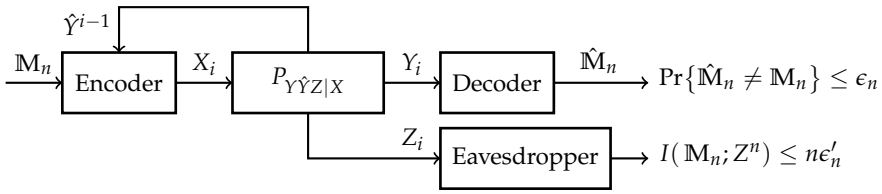


Figure 16.: Wiretap channel with generalized feedback.

4.2 PROBLEM DEFINITION

We consider the WCGF, where a source wants to transmit a message $\mathbb{M}_n \in \mathcal{M}_n$ securely to a destination with the aid of a feedback signal while an eavesdropper is present in the channel. The WCGF, depicted in Fig. 16, is modeled as a memoryless channel defined by a conditional probability distribution (PD)

$$p(y\hat{y}z|x) : \mathcal{X} \longmapsto \mathcal{Y} \times \hat{\mathcal{Y}} \times \mathcal{Z}, \tag{140}$$

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

Definition 4.1. *A* secrecy rate *R is said to be achievable for this channel if for every $(\epsilon_n, \epsilon'_n) > 0$ there exists a block length n, $\|\mathcal{M}_n\| \geq 2^{n(R-\epsilon_n)}$, randomized encoder functions $enc_i : (\mathcal{M}_n, \hat{\mathcal{Y}}^{i-1}) \mapsto \mathcal{X}_i$, and a decoder function $dec : \mathcal{Y}^n \mapsto \mathcal{M}_n$, such that*

$$\frac{1}{\|\mathcal{M}_n\|} \sum_{m \in \mathcal{M}_n} \Pr\Big\{ dec(Y^n) \neq m \,|\, X^n = \{enc_i(m, \hat{Y}^{i-1})\}_{i=1}^n \Big\} \leq \epsilon_n,$$
$$\text{and } I(\mathbb{M}_n; Z^n) \leq n\epsilon'_n,$$

where ϵ_n and ϵ'_n are sequences that $(\epsilon_n, \epsilon'_n) \to 0$ as $n \to \infty$.

The secrecy capacity C_{sf} *of the WCGF is the supremum of all achievable secrecy rates.*

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

Given the strictly causal nature of the feedback link, for each time slot i, the encoder uses its past observations to generate a symbol $\varphi_i(\hat{Y}^{i-1})$ that sends through the channel. After n time slots, both the encoder and the legitimate decoder generate a secret key, i.e., $K_n = \psi_a(\hat{Y}^n)$ and $\hat{K}_n = \psi_b(Y^n)$, where $K_n, \hat{K}_n \in \mathcal{K}_n$.

Definition 4.2. *A* secret key *of rate R_k is said to be achievable for this channel if for every $(\epsilon_n, \epsilon'_n) > 0$ there exists a block length n, $\|\mathcal{K}_n\| \geq 2^{n(R_k - \epsilon_n)}$, functions $\psi_a(\cdot)$ and $\psi_b(\cdot)$ such that the preceding steps can be fulfilled and*

$$\begin{aligned} &\Pr\{K_n \neq \hat{K}_n\} \leq \epsilon_n, \\ &\text{and } I(K_n; Z^n) \leq n\epsilon'_n, \end{aligned}$$

where ϵ_n and ϵ'_n are sequences that $(\epsilon_n, \epsilon'_n) \to 0$ as $n \to \infty$.

The secret key capacity *of the WCGF is the supremum of all achievable secret key rates.*

5

WIRETAP CHANNEL WITH GENERALIZED FEEDBACK

We present the two proposed inner bounds in Sections 5.1 and 5.2, while their proofs are deferred to Appendices 5.A and 5.C. In Section 5.3, we investigate special cases of these results while summary and discussion are relegated to Section 5.4.

5.1 INNER BOUND BASED ON JOINT SOURCE-CHANNEL CODING

We first introduce a coding scheme based on a joint source-channel coding (JSCC) strategy where the codewords sent convey both digital and analog information.

Theorem 5.1 (JSCC inner bound). *A lower bound on the secrecy capacity of the WCGF is given by all rates satisfying:*

$$\begin{aligned} R \leq \max_{p\in\mathcal{P}_1} \sup_{b\geq 1} \frac{1}{b}\Bigg[& I(U_1;Y^b) - I(U_1;Z^b) \\ & + \sum_{j=2}^{b} \min\Big\{ I(U_j;Y_j^b|U^{j-1}Y^{j-1}) - I(U_j;X^{j-1}\hat{Y}^{j-1}|U^{j-1}Y^{j-1}), \\ & \qquad I(U_j;Y^b|U^{j-1}) - I(U_j;Z^b|U^{j-1}) \Big\} \Bigg], \end{aligned} \tag{141}$$

where all admissible input PDs $\mathcal{P}_1$ factor as

$$p(u^b x^b y^b \hat{y}^b z^b) = \prod_{j=1}^{b} p(u_j|u^{j-1}x^{j-1}\hat{y}^{j-1})\, p(x_j|u^j x^{j-1}\hat{y}^{j-1})\, p(y_j\hat{y}_j z_j|x_j). \tag{142}$$

Proof. The transmission is split into b blocks and, in each block, the codeword $U_{[j]}^n$ sent carries both digital and analog information, the latter through the correlation with sequences from past blocks. The proof is relegated to Appendix 5.A. □

The expression of the bound (141) is rather complex, thus, we propose next a simpler scheme with less variables involved.

Corollary 5.1. *A lower bound on the secrecy capacity of the WCGF is given by all rates satisfying:*

$$R \leq \max_{p \in \mathcal{P}_2} \left[I(UV;Y) - \max\{I(V;X\hat{Y}|U), I(UV;Z)\} \right], \tag{143}$$

where all admissible input PDs $\mathcal{P}_2$ factor as

$$p(uvxy\hat{y}z) = p(ux)p(y\hat{y}z|x)p(v|ux\hat{y}).$$

Proof. It suffices to choose an arbitrarily large b in the JSCC scheme and a particular choice of random variables (RVs). See Appendix 5.B for details. □

Remark 5.1. *The achievable rate (143) can be independently derived using a simpler block Markov scheme.*

Remark 5.2. *If we set $V = \emptyset$, we recover the achievable rate of the WTC without feedback.*

5.2 INNER BOUND BASED ON KEY GENERATION

We now introduce a coding scheme that employs the feedback link to generate a secret key shared between the legitimate users simultaneously with the transmission. The key is later used to encrypt at the bit level the message to be sent.

Let $\mathcal{P}_3$ be the set of all PDs that factor as

$$p(quxvty\hat{y}z) = p(qu)p(x|u)p(y\hat{y}z|x)p(t|v)p(v|ux\hat{y}), \tag{144}$$

and let $\mathcal{P}_4$ be the subset in $\mathcal{P}_3$ with $Q = \emptyset$.

For any $p \in \mathcal{P}_3$, let R_{KG_1} be the set of all nonnegative rates satisfying:

$$\begin{aligned} R_{KG_1} \leq\ & I(U;Y) - I(U;Z|Q) - \max\{I(Q;Y),\ I(V;X\hat{Y}|UY)\} \\ & + I(V;Y|UT) - I(V;Z|UT) - I(U;T|QZ), \end{aligned} \tag{145a}$$

$$R_{KG_1} \leq I(U;Y) - \max\{I(Q;Y),\ I(V;X\hat{Y}|UY)\}, \tag{145b}$$

whereas, for any $p' \in \mathcal{P}_4$, let R_{KG_2} be the set of all nonnegative rates satisfying:

$$R_{KG_2} \leq I(V;Y|UT) - I(V;Z|UT) \tag{146a}$$

$$R_{KG_2} \leq I(U;Y) - I(V;X\hat{Y}|UY). \tag{146b}$$

Theorem 5.2 (KG inner bound). *A lower bound on the secrecy capacity of the WCGF is given by the region:*

$$R \leq \max \left\{ \max_{p \in \mathcal{P}_3} R_{KG_1}, \max_{p' \in \mathcal{P}_4} R_{KG_2} \right\}.$$

Proof. In this scheme, the transmission is split into several blocks and the transmitted message in each block is encrypted fully (R_{KG_2}) or partially (R_{KG_1}). The codeword V^n is used to convey a description of the feedback signal $\hat{Y}^n$ from the previous block, and therefore, allows both end users to *generate* the secret key during transmission. In R_{KG_1}, the description is sent in part by Q^n and the rest, by U^n, thus the presence of the maximum in (145). See Appendix 5.C for further details. □

Remark 5.3. *If we set $Q = T = V = \emptyset$, we recover the achievable rate of the WTC without feedback.*

5.2.1 *Key Agreement Inner Bound*

The scheme presented in Theorem 5.2, in the absence of a message, may be used by the legitimate users to agree upon a secret key. This key could later be employed to encrypt the transmission or part of it on a higher layer.

Corollary 5.2. *A lower bound on the secret key capacity of the WCGF is given by all rates satisfying:*

$$R_k \leq \max_{p \in \mathcal{P}_4} \left[I(V;Y|UT) - I(V;Z|UT) \right], \tag{147}$$

subject to

$$I(V; X\hat{Y}|UY) \leq I(U;Y). \tag{148}$$

Proof. This corollary is a special case of the strategy R_{KG_2}, where there is no message to be transmitted, i.e., $R = 0$, and we are only interested on generating a secret key, i.e., $R_k \leq \bar{S}_2$.

The codeword U^n only carries the indices used by the destination to reconstruct the sequences T^n and V^n. The inequality (148) corresponds to the cost of transmitting these indices. Additionally, the purpose of the codeword T^n is to extract most of the common randomness between Z^n and $(Y^n\hat{Y}^n)$, and it is assumed that the eavesdropper can obtain it. The secret key is thus the remaining uncertainty in V^n that the eavesdropper cannot resolve from its own observation Z^n.

See Appendix 5.C.7 for details, specially the bounds (247). □

5.3 APPLICATION EXAMPLES TO SOME CHANNEL AND FEEDBACK MODELS

In this section, we show how both the JSCC and KG scheme contain several other strategies as special cases with the appropriate choice of joint PD.

5.3.1 *Wiretap Secret Key Capacity*

We first analyze the situation where two terminals connected through a noiseless rate-limited channel, and which have access to correlated i.i.d. sources, want to generate a shared key. This key must be concealed from an eavesdropper which is also connected to the noiseless public channel and has access to a correlated source.

The channel model (140) encompasses this situation. Let us take the following set of variables:

$$\hat{Y} = \hat{Y}_s \tag{149}$$
$$Y = (Y_s X) \tag{150}$$
$$Z = (Z_s X), \tag{151}$$

where $H(X) = R$, i.e., both the legitimate receiver and the eavesdropper have access to the noiseless rate-limited channel. Moreover, the correlated sources available to the nodes $(\hat{Y}_s Y_s Z_s)$ are independent of the channel input X, i.e., $p(x y_s \hat{y}_s z_s) = p(x)p(y_s \hat{y}_s z_s)$.

Theorem 5.3 ([8, Thm. 2.6]). *In this scenario, the* secret key capacity *of the WTC with a public noiseless channel of rate R is given by*

$$\mathrm{C}_{wsk} = \max_{p(y_s \hat{y}_s z_s) p(v|\hat{y}_s) p(t|v)} [I(V;Y_s|T) - I(V;Z_s|T)], \tag{152}$$

subject to

$$I(V;\hat{Y}_s) - I(V;Y_s) < R, \tag{153}$$

and is achieved by the scheme of Corollary 5.2.

Proof. Since both end users have access to X, the following set of auxiliaries is optimal

$$Q = \varnothing \tag{154}$$
$$U = X, \tag{155}$$

and (VT) independent of X, since it does not affect the correlated sources. The joint PD is $p(x)p(y_s \hat{y}_s z_s)p(v|\hat{y}_s)p(t|v)$, and therefore (147) and (148) become (152) and (153).

The converse can be found in [8]. □

5.3.2 *Wiretap Channel with Perfect Output Feedback*

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

Theorem 5.4 ([9, Thm. 1]). *In this model, the KG scheme presented in Theorem 5.2 achieves all the rates satisfying*

$$R \leq \max_{p(ux)p(yz|x)} \min \left\{ |I(U;Y) - I(U;Z)|^+ + H(Y|UZ),\, I(U;Y) \right\}. \tag{156}$$

where $|a|^+ = \max\{a, 0\}$.

Proof. With the following choice of RVs:

$$V = Y \tag{157}$$
$$T = Q = \emptyset, \tag{158}$$

the rate R_{KG_1} (145) becomes

$$R_{KG_1} \leq \min\{I(U;Y) - I(U;Z) + H(Y|UZ),\, I(U;Y)\}, \tag{159}$$

while the rate R_{KG_2} (146) becomes

$$R_{KG_2} \leq \min\{H(Y|UZ),\, I(U;Y)\}. \tag{160}$$

Therefore, the union of both regions can be written as (156). □

Remark 5.4. *The secrecy capacity results for the* degraded *and* reversely degraded *WTC with perfect output feedback [9, Cor. 1 and 2] also apply here.*

Remark 5.5. *If we set $V = Y$ in the rate expression of Corollary 5.1, which given the perfect feedback seems to be the maximizing PD, we obtain*

$$R \leq \max_{p(ux)p(yz|x)} \min \left\{ I(U;Y) - I(U;Z) + H(Y|UZ),\, I(U;Y) \right\}, \tag{161}$$

which is strictly below (156) if $I(U;Y) < I(U;Z)$.

5.3.3 *Wiretap Channel with Casual State Information*

In [59], the authors analyze a WTC affected by a random state S, i.e., $p(yz|xs)p(s)$, when the state is available causally only at the encoder and the legitimate decoder, i.e., $\hat{Y} = S$ and $Y = (YS)$.

Theorem 5.5 ([59, Thm. 1]). *In this model, the KG scheme presented in Theorem 5.2 achieves all the rates satisfying*

$$R \leq \max \Bigg\{ \max_{p(u)u'(u,s)p(x|u's)} \min\{I(U;YS) - I(U;ZS) + H(S|Z), \\ I(U;YS)\}, \\ \max_{p(u)p(x|us)} \min\{H(S|ZU),\, I(U;Y|S)\} \Bigg\}. \tag{162}$$

Proof. First, we make the choice of RVs:

$$V = S \tag{163}$$
$$T = Q = \emptyset. \tag{164}$$

Second, since the state is known causally at the encoder, i.e., s^i is present at time slot i, we can modify step 4) from the encoding process (Section 5.C.2) in the following way. For R_{KG_1}, after the encoder has chosen the codeword to transmit in block j, i.e., $u^n(\underline{r}_j)$, it computes $u'_i = u'(u_i(\underline{r}_j), s_i)$ and transmits a randomly generated symbol x_i according to $p(x_i|u'_i s_i)$ for each time slot $i \in [1:n]$. The rate (145) becomes

$$\begin{aligned} R_{KG_1} &\leq I(U;YS) - I(U;Z) + H(S|ZU) \\ &= I(U;YS) - I(U;ZS) + H(S|Z) \qquad (165a) \\ R_{KG_1} &\leq I(U;YS). \qquad (165b) \end{aligned}$$

For R_{KG_2}, we proceed similarly but without the inclusion of the function $u'(\cdot)$ between the codeword $u^n(\underline{r}_j)$ and the generation of x_i. The rate (146) becomes

$$R_{KG_2} \leq I(S;YS|U) - I(S;Z|U) = H(S|ZU) \tag{166a}$$
$$R_{KG_2} \leq I(U;YS) = I(U;Y|S). \tag{166b}$$

Therefore, the final expression for the rate is (162). □

Remark 5.6. *The secrecy capacity result for* less noisy *WTC with state information available causally or noncausally at the encoder and decoder [9, Thm. 3] also applies here.*

5.3.4 *Erasure WTC with State-Feedback (KG scheme)*

In [60, Corollary 1], the authors analyze an erasure WTC with public state-feedback from the legitimate receiver; therefore, both the encoder and the eavesdropper know if there was an erasure or not at the legitimate end. Moreover, the channels experience independent

erasures, i.e., $p(yz|x) = p(y|x)p(z|x)$. In this scenario, secrecy capacity is shown to be

$$C_{sf} = (1-\delta)\delta_E \frac{1-\delta\delta_E}{1-\delta\delta_E^2}, \tag{167}$$

where δ denotes the erasure probability of the legitimate receiver and δ_E, the one of the eavesdropper. In the sequel, we see that the KG scheme is not able to achieve this capacity.

We add the RV $S = \mathbb{1}\{Y = e\}$, respectively $S_E = \mathbb{1}\{Z = e\}$, to indicate the erasure events and, since the feedback from the legitimate user is public, we give this information to the eavesdropper. We analyze each term of (145) and (146) separately. We start with R_{KG_1}. First,

$$\begin{aligned}
&I(U;Y|Q) - I(U;Z|Q) + I(V;Y|UT) - I(V;Z|UT) - I(U;T|QZ) \\
&\quad\le I(U;Y|Q) - I(U;Z|Q) + I(V;Y|UT) - I(V;Z|UT) && \text{(168a)} \\
&\quad= I(U;YS|Q) - I(U;ZS_ES|Q) + I(V;YS|UT) - I(V;ZS_ES|UT) \\
&\quad= I(U;Y|QS) - I(U;ZS_E|QS) + I(V;Y|UTS) - I(V;ZS_E|UTS) \\
&\quad= I(U;Y|QS) - I(U;Z|QSS_E) + I(V;Y|UTS) - I(V;Z|UTSS_E) && \text{(168b)} \\
&\quad= I(U;X|Q,S=0)(1-\delta) - I(U;X|QS)(1-\delta_E) \\
&\qquad + I(V;X|UT,S=0)(1-\delta) - I(V;X|UTS)(1-\delta_E) && \text{(168c)} \\
&\quad= I(U;X|Q)(\delta_E-\delta) + I(V;X|UT,S=0)(1-\delta)\delta_E \\
&\qquad - I(V;X|UT,S=1)(1-\delta_E)\delta && \text{(168d)} \\
&\quad\le I(U;X|Q)(\delta_E-\delta) + I(V;X|UT,S=0)(1-\delta)\delta_E \\
&\quad\le I(U;X)(\delta_E-\delta) + H(X|UT,S=0)(1-\delta)\delta_E \\
&\quad\le I(U;X)(\delta_E-\delta) + H(X|U)(1-\delta)\delta_E, && \text{(168e)}
\end{aligned}$$

where in (168b) we note that the erasure event S_E is independent of the inputs $(QUVT)$ and the erasure S; in (168c) we use the fact that $Y = X$ ($Z = X$) when $S = 0$ ($S_E = 0$); and in (168d) we note that S is independent of $(Q\,UX)$. Second,

$$\begin{aligned}
&I(U;Y) - I(U;Z|Q) + I(V;Y|UT) - I(V;Z|UT) - I(U;T|QZ) \\
&- I(V;X\hat{Y}|UY) \\
&\qquad\le I(U;Y) - I(U;Z|Q) + I(V;Y|UT) - I(V;Z|UT), && \text{(169)}
\end{aligned}$$

which is always above (168a). Third,

$$I(U;Y|Q) = I(U;X|Q)(1-\delta) \le I(U;X)(1-\delta). \tag{170}$$

And fourth,

$$I(U;Y) - I(V;X\hat{Y}|UY) = I(U;X)(1-\delta) - I(V;X|U,S=1)\delta, \tag{171}$$

which is always above (170).

Therefore, the rate R_{KG_1} is upper-bounded by

$$R_{KG_1} \leq \max_{p \in \mathcal{P}_3} \min\{I(U;X)(\delta_E - \delta) + H(X|U)(1-\delta)\delta_E,\, I(U;X)(1-\delta)\},$$

which is achievable with the following set of auxiliary RVs

$$T = Q = \emptyset \text{ and } V = \begin{cases} X & \text{if } S = 0 \\ \emptyset & \text{if } S = 1. \end{cases} \tag{172}$$

Taking $H(X|U) = \beta, \beta \in [0,1]$, the bound becomes

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

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

$$R_{KG_1} \leq (1-\delta)\delta_E \frac{1-\delta}{1-\delta\delta_E}, \text{ for } \beta = \frac{1-\delta_E}{1-\delta\delta_E}. \tag{173}$$

We can proceed similarly with the rate R_{KG_2} and, with the choice of RVs (172), we obtain

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

or equivalently

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

whose maximization gives

$$R_{KG_2} \leq (1-\delta)\delta_E \frac{1}{1+\delta_E}, \text{ for } \beta = \frac{1}{1+\delta_E}. \tag{174}$$

Therefore, the rate given by Theorem 5.2 is

$$R \leq (1-\delta)\delta_E \max\left\{\frac{1-\delta}{1-\delta\delta_E}, \frac{1}{1+\delta_E}\right\}. \tag{175}$$

This rate is always below capacity (167) as depicted in Fig. 17.

5.3.5 *Erasure WTC with State-Feedback (JSCC scheme)*

Theorem 5.6 ([60, Cor. 1]). *The JSCC scheme presented in Theorem 5.1 achieves the secrecy capacity* (167).

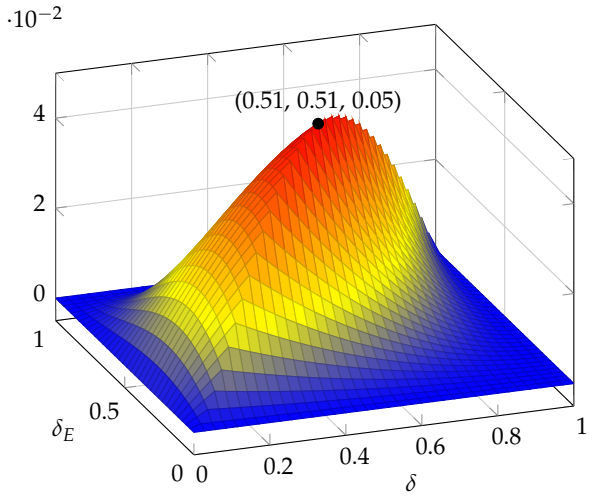


Figure 17.: Gap in bits between C_{sf} and the rate achieved by the KG scheme.

Proof. In a similar way as [60, 72], we divide the transmission in two phases; in the first phase, the legitimate users agree on a key which is then used to secure the second phase.

During the first phase, which comprises b' blocks, Alice sends random bits. Bob correctly receives $b'(1-\delta)$ bits on average, out of which $b'(1-\delta)\delta_E$ are erasures for Eve. Since Alice knows which bits were received by Bob, they can calculate the same $K = b'[(1-\delta)\delta_E - \epsilon']$ linear combinations of these bits. For large enough b', treating K as integer has a negligible loss. Hence, the resulting K bits are concatenated to form the key X^K.

Alice encrypts the sequence of N bits to transmit W^N using the key X^K, i.e., $W'^N = [W^K \oplus X^K, W_{K+1}^N]$. Then, the encrypted message gets encoded using a generator matrix G, i.e., $W''^N = W'^N G$. This $N \times N$ matrix is publicly known and full-rank. The resulting bits are sent sequentially and, as long as Bob experiences an erasure, the previous bit is repeated. This strategy forces the input variables in the JSCC scheme to be chosen as

$$U_j = \begin{cases} W^N & \text{if } j = b'+1 \\ \emptyset & \text{otherwise} \end{cases} \tag{176}$$

$$X_j = \begin{cases} X \sim \text{Bern}(1/2) & \text{if } j \in [1:b'] \\ f(X^K, W^N, S_{b'+1}^{j-1}) & \text{if } j \in [b'+1:b] \end{cases} \tag{177}$$

where $S_{b'+1}^{j-1}$ is the state-feedback from the previous blocks of the second phase. This choice of input PD simplifies the rate (141) as

$$bR \leq I(W^N; Y^b S^b) - I(W^N; Z^b S_E^b S^b), \tag{178}$$

where $S = \mathbb{1}\{Y = e\}$ and $S_E = \mathbb{1}\{Z = e\}$.

If the length of the key is $K = M + M^{3/4}$, where

$$M = N\frac{1-\delta_E}{1-\delta\delta_E},$$

the proposed scheme assures that the second term vanishes for sufficiently large N, or equivalently, sufficiently large b since $N = bR$. We refer the reader to [72] for the complete proof. Hence,

$$\begin{aligned}
bR &\leq I(W^N; Y^b S^b) \\
&= \sum_{j=1}^{b} I(W^N; Y_j S_j | Y^{j-1} S^{j-1}) \\
&= \sum_{j=b'+1}^{b} I(W^N; Y_j | Y^{j-1} S^{j-1} S_j) && \text{(179a)} \\
&= \sum_{j=b'+1}^{b} I(W^N; X_j | Y^{j-1} S^{j-1}, S_j = 0)(1-\delta) \\
&= \sum_{j=b'+1}^{b} I(W^N; X_j | X^K S_{b'+1}^{j-1})(1-\delta) && \text{(179b)} \\
&= \sum_{j=b'+1}^{b} [H(X_j | X^K S_{b'+1}^{j-1}) - H(X_j | W^N X^K S_{b'+1}^{j-1})](1-\delta) \\
&= (1-\delta)(b-b'). && \text{(179c)}
\end{aligned}$$

where (179a) is due to W^N being independent of the channel outputs in the first phase and the present state; where in (179b) X^K is a deterministic function of $(Y^{b'} S^{b'})$ and $X_j \multimap (X^K S_{b'+1}^{j-1}) \multimap (Y^{j-1} S^{b'} S_j)$ forms a Markov chain; and (179c) follows from $H(X_j | X^K S_{b'+1}^{j-1}) = H(X_j) = 1$ since W'^N is independent of X^K given that $W_i \sim \text{Bern}(1/2)$ for $i \in [1:N]$ and $H(X_j | W^N X^K S_{b'+1}^{j-1}) = 0$ according to (177).

The length of the first phase can be calculated as follows,

$$\begin{aligned}
&b'[(1-\delta)\delta_E - \epsilon'] \\
&\quad = M + M^{3/4} \\
&\quad = N\frac{1-\delta_E}{1-\delta\delta_E} + \left(N\frac{1-\delta_E}{1-\delta\delta_E}\right)^{3/4} \\
&\quad = (1-\delta)(b-b')\frac{1-\delta_E}{1-\delta\delta_E} + \left((1-\delta)(b-b')\frac{1-\delta_E}{1-\delta\delta_E}\right)^{3/4}, && \text{(180)}
\end{aligned}$$

where the last equality comes from the most restrictive condition for the rate $N = bR = (1-\delta)(b-b')$. If we divide (180) by b at the same time that $b \to \infty$ and we choose an arbitrarily small ϵ', we have that

$$\frac{b'}{b}(1-\delta)\delta_E = (1-\delta)\left(1-\frac{b'}{b}\right)\frac{1-\delta_E}{1-\delta\delta_E}, \tag{181}$$

or equivalently,

$$\frac{b'}{b} = \frac{1-\delta_E}{1-\delta\delta_E^2}. \tag{182}$$

The achievable rate (179c) for the JSCC scheme is therefore

$$R \leq (1-\delta)\delta_E \frac{1-\delta\delta_E}{1-\delta\delta_E^2}, \tag{183}$$

which is capacity-achieving. □

Remark 5.7. *The capacity result obtained by the JSCC scheme is valid for* weak secrecy*, i.e.,* $I(\mathbb{M}_n; Z^n) \leq n\epsilon'_n$*, whereas the capacity result in [60, Cor. 1] is also valid for* strong secrecy*, i.e.,* $I(\mathbb{M}_n; Z^n) \leq \epsilon'_n$.

5.3.6 *AWGN Wiretap Channel with Perfect Output Feedback*

In [10], the authors analyze the Gaussian WTC with perfect output feedback at the encoder, i.e., $\hat{Y} = Y$, and noisy feedback at the eavesdropper. This model can be succinctly described as follows,

$$Y_j = X_j + N_j \tag{184}$$

$$Z_j = \begin{bmatrix} \bar{Z}_j \\ \bar{Y}_j \end{bmatrix} = \begin{bmatrix} X_j + M_j \\ Y_j + S_j \end{bmatrix}, \tag{185}$$

where Y_j, $\bar{Z}_j$, and $\bar{Y}_j$ are the legitimate receiver's and the eavesdropper's output, and the noisy feedback at time j, respectively. The encoder's signal X_j has an average power constraint P, and N_j, M_j, and S_j are arbitrarily correlated additive white Gaussian noise terms with zero means and variances σ_N^2, σ_M^2, and σ_S^2, respectively.

Theorem 5.7 ([10, Thm. 5.1])**.** *The secrecy capacity of this model is given by*

$$C_{sf} = \frac{1}{2}\log\left(1 + \frac{P}{\sigma_N^2}\right), \tag{186}$$

provided that the eavesdropper has access to the noisy feedback $\bar{Y}$ *only, and it is achieved by the JSCC scheme.*

Proof. Fix the following joint PD in the JSCC scheme

$$U_j = \begin{cases} \alpha_1\theta & \text{if } j = 1 \\ \varnothing & \text{if } j \in [2:b] \end{cases} \tag{187}$$

$$X_j = \begin{cases} U_1 & \text{if } j = 1 \\ f_j(X_{j-1}, Y_{j-1}) & \text{if } j \in [2:b] \end{cases} \tag{188}$$

where $\alpha_1 = \alpha \triangleq \sqrt{1 + P/\sigma_N^2}$ and $\theta \sim \mathcal{U}[-0.5, 0.5]$ is a continuous RV. The functions $f_j(\cdot)$ in (188) are defined as follows,

$$X_j = \begin{cases} h_2\alpha_1\left(Y_1 - X_1\right) & \text{if } j = 2 \\ \dfrac{h_j}{h_{j-1}}\left[X_{j-1} + \alpha_{j-1}h_{j-1}\left(Y_{j-1} - X_{j-1}\right)\right] & \text{if } j \in [3:b], \end{cases} \tag{189}$$

where $\alpha_j \triangleq \sqrt{P/\sigma_N^2}\,\alpha^{j-1}$ and $h_j \triangleq -\alpha_j / \sum_{l=1}^{j-1}\alpha_l^2$ are parameters similar to those of the SK scheme, such that $X_j = h_j \sum_{l=1}^{j-1}\alpha_l N_l$. Therefore, for every $j \in [2:b]$, X_j is independent of the original message X_1 and is a deterministic function of X_{j-1} and Y_{j-1}. We refer the reader to [10] for additional details.

The achievable rate (141) can therefore be written as

$$bR < I(U_1; Y^b) - I(U_1; \bar{Z}^b \bar{Y}^b), \tag{190}$$

and we analyze each term in the sequel.

The first term,

$$\begin{aligned}
I(U_1;Y^b) &= I(X_1;Y^b) \\
&= I(X_1Y_1;Y_2^b) + h(Y_1|Y_2^b) - h(Y_1|X_1) \\
&\geq \sum_{l=2}^{b} I(X_1Y_1;Y_l|Y_2^{l-1}) + h(X_1+N_1|Y_2^bN_1) - h(X_1+N_1|X_1) && \text{(191a)} \\
&= \sum_{l=2}^{b} \Big[h(Y_l|Y_2^{l-1}) - h(Y_l|X_1Y^{l-1})\Big] + h(X_1) - h(N_1) && \text{(191b)} \\
&= \sum_{l=2}^{b} \Big[h(Y_l) - h(Y_l|X^lY^{l-1})\Big] + \log|\alpha_1| - h(N_1) && \text{(191c)} \\
&= \sum_{l=2}^{b} [h(X_l+N_l) - h(N_l)] + \log|\alpha_1| - h(N_1) \\
&= (b-1)\frac{1}{2}\log\left(1+\frac{P}{\sigma_N^2}\right) + \log|\alpha_1| - h(N_1). && \text{(191d)}
\end{aligned}$$

where inequality (191a) is due to the additional conditioning in the differential entropy; where in (191b) we note that N_1 and X_2^b (subsequently Y_2^b) are independent of X_1; where in (191c) we use some properties of this scheme, namely, Y_l is independent of Y_2^{l-1} and X_l is a deterministic function of $(X_{l-1}Y_{l-1})$, and that $h(X_1) = \log|\alpha_1|$; and where in (191d) we note that for $l \in [2:b]$ $X_l \sim \mathcal{N}(0,P)$ and is independent of N_l.

We upper-bound the second term in a similar way as [10],

$$\begin{aligned}
I(U_1;\bar{Z}^b\bar{Y}^b) &= I(\theta;\bar{Z}^b\bar{Y}^b) \\
&\leq I(\theta;\bar{Z}^b\bar{Y}^bN^b) \\
&= h(\theta) - h(\theta|\bar{Z}^b\bar{Y}^bN^b) \\
&= h(\theta) - h(\theta|\alpha_1\theta+M_1, \alpha_1\theta+S_1, S_2^b, M_2^b, N^b) && \text{(192a)} \\
&= h(\theta) - h(\theta|\alpha_1\theta+M_1, \alpha_1\theta+S_1, N_1) && \text{(192b)} \\
&= I(\theta;\alpha_1\theta+M_1, \alpha_1\theta+S_1, N_1) \\
&= I(\theta;\boldsymbol{A}\theta+\boldsymbol{B}) && \text{(192c)} \\
&\leq \frac{1}{2}\log\det\left(\boldsymbol{I}+\frac{1}{12}\boldsymbol{A}\boldsymbol{A}^T\mathbb{E}[\boldsymbol{B}\boldsymbol{B}^T]^{-1}\right), && \text{(192d)}
\end{aligned}$$

where in (192a) we use the sequence N^b to form X_2^b and subtract it from $(\bar{Z}^b\bar{Y}^b)$; where (192b) follows since $(S_2^bM_2^bN_2^b)$ is independent

of $(\theta S_1 M_1 N_1)$ due to the channel memorylessness; where in (192c) we define $\boldsymbol{A} \triangleq [0, \alpha_1, \alpha_1]^T$ and $\boldsymbol{B} \triangleq [N_1, M_1, S_1]^T$; and where (192d) follows from the fact that the mutual information is maximized for a Gaussian input distribution with the same variance as θ, which is uniform.

The expression in (192d) has a finite value as long as

$$\rho_{NM}^2 + \rho_{NS}^2 + \rho_{MS}^2 - 2\rho_{NM}\rho_{NS}\rho_{MS} - 1 \neq 0, \tag{193}$$

where ρ_{NM}, ρ_{NS}, ρ_{MS} are the correlation coefficients between the corresponding noises. If this condition is fulfilled, the following is an achievable rate for this particular choice of variables

$$R \leq \left(\frac{b-1}{b}\right)\frac{1}{2}\log\left(1 + \frac{P}{\sigma_N^2}\right) + \frac{1}{b}\big[\log|\alpha_1| - h(N_1) - I(\theta; \boldsymbol{A}\theta + \boldsymbol{B})\big],$$

which tends to (186) as $b \to \infty$. □

5.3.7 *AWGN Wiretap Channel with Noisy Feedback*

We now modify the previous model to consider the situation where the encoder has access to a noisy feedback from the legitimate user. The channel can therefore be modeled as

$$Y_j = X_j + N_j \tag{194}$$
$$Z_j = X_j + M_j \tag{195}$$
$$\hat{Y}_j = Y_j + S_j = X_j + N_j + S_j, \tag{196}$$

where Y_j, Z_j and $\hat{Y}_j$ are the legitimate output, the eavesdropper's observation and the noisy feedback present at the encoder at time j, respectively. Additionally, N_j, S_j and M_j are additive white jointly Gaussian noises and their covariance matrix is

$$\boldsymbol{C} \triangleq \begin{bmatrix} \sigma_N^2 & \rho\sigma_N\sigma_S & \rho_N\sigma_N\sigma_M \\ \rho\sigma_N\sigma_S & \sigma_S^2 & \rho_S\sigma_S\sigma_M \\ \rho_N\sigma_N\sigma_M & \rho_S\sigma_S\sigma_M & \sigma_M^2 \end{bmatrix}. \tag{197}$$

Theorem 5.8. *A lower bound on the secrecy capacity for this channel is given by*

$$\begin{aligned} R &\leq \frac{1}{b}\Big[I(U^b; Y^b) - I(U^b; Z^b)\Big] \\ &= \frac{1}{2b}\left[\log\frac{\det(\boldsymbol{C}_{Y^b})}{\det(\boldsymbol{C}_{Y^b|U^b})} - \log\frac{\det(\boldsymbol{C}_{Z^b})}{\det(\boldsymbol{C}_{Z^b|U^b})}\right], \end{aligned} \tag{198}$$

where the matrices are defined in (204)–(207).

Proof. As seen in Section 5.3.6, Theorem 5.1 recovers the SK scheme with a special choice of RVs. Moreover, with independent U_j's across blocks, we fall back to a transmission with i.i.d. codewords (as in Corollary 5.1). We join these two options as follows,

$$U_j = \begin{cases} \sqrt{\beta}\alpha_1\theta + \sqrt{\bar{\beta}}U'_1 & \text{if } j = 1 \\ \sqrt{\bar{\beta}}U'_j & \text{if } j \in [2:b] \end{cases} \tag{199}$$

$$X_j = \begin{cases} U_1 & \text{if } j = 1 \\ X_j^{\text{SK}} + U_j & \text{if } j \in [2:b], \end{cases} \tag{200}$$

where $U'_j \sim \mathcal{N}(0, P)$, $\theta \sim \mathcal{N}(0, P/\alpha_1^2)$, $\bar{\beta} = 1 - \beta$, and $\beta \in [0, 1]$ is an optimization parameter. The variables U'_j convey new information in each block, whereas the X_j^{SK} allow the decoding of θ as in the SK scheme. The definition of the variables X_j^{SK} differs from (189) due to the presence of the variables U'_j and the noisy feedback,

$$X_j^{\text{SK}} \triangleq \begin{cases} h_2\alpha_1\left(\hat{Y}_1 - X_1\right) & \text{if } j = 2 \\ \dfrac{h_j}{h_{j-1}}\left[X_{j-1}^{\text{SK}} + \alpha_{j-1}h_{j-1}\left(\hat{Y}_{j-1} - X_{j-1}\right)\right] & \text{if } j \in [3:b], \end{cases} \tag{201}$$

where $h_j \triangleq -\alpha_j\left(\sum_{l=1}^{j-1}\alpha_l^2\right)^{-1}$, $\alpha_1 = \alpha$, $\alpha_j = \gamma\alpha^{j-1}$ for $j \in [2:b]$,

$$\gamma = \sqrt{\frac{\beta P}{\sigma_N^2 + 2\rho\sigma_N\sigma_S + \sigma_S^2}}, \text{ and } \alpha = \sqrt{1+\gamma^2}. \tag{202}$$

The choice of variables (199)–(201), which is in accordance with the joint PD (142), and the parameters (202) verify the power constraint $\mathbb{E}[X_j^2] = P$ and allow us to write

$$X_j^{\text{SK}} = h_j \sum_{l=1}^{j-1} \alpha_l(N_l + S_l). \tag{203}$$

Since the variables U'_j are independent between each other, for a given number of blocks b the rate (141) becomes (198). The elements of the matrix $\boldsymbol{C}_{Y^b}$ are as follows,

$$\boldsymbol{C}_{Y^b}(j,j) = P + \sigma_N^2 \tag{204a}$$

$$\boldsymbol{C}_{Y^b}(1,j) = \boldsymbol{C}_{Y^b}(j,1) = -\gamma\alpha^{2-j}(\sigma_N^2 + \rho\sigma_N\sigma_S), \text{ for } j \neq 1 \tag{204b}$$

$$\boldsymbol{C}_{Y^b}(j,l) = \gamma^2\alpha^{j-l}(\sigma_S^2 + \rho\sigma_N\sigma_S), \text{ for } j \neq l \neq 1, \tag{204c}$$

and similarly

$$\boldsymbol{C}_{Z^b}(j,j) = P + \sigma_M^2 \tag{205a}$$

$$\boldsymbol{C}_{Z^b}(1,j) = \boldsymbol{C}_{Z^b}(j,1) = -\gamma\alpha^{2-j}\sigma_M(\rho_N\sigma_N + \rho_S\sigma_S), \text{ for } j \neq 1 \tag{205b}$$

$$\boldsymbol{C}_{Z^b}(j,l) = \gamma^2\alpha^{j-l}\left[\sigma_N^2 + 2\rho\sigma_N\sigma_S + \sigma_S^2 - \sigma_M(\rho_N\sigma_N + \rho_S\sigma_S)\right], \text{ for } j \neq l \neq 1. \tag{205c}$$

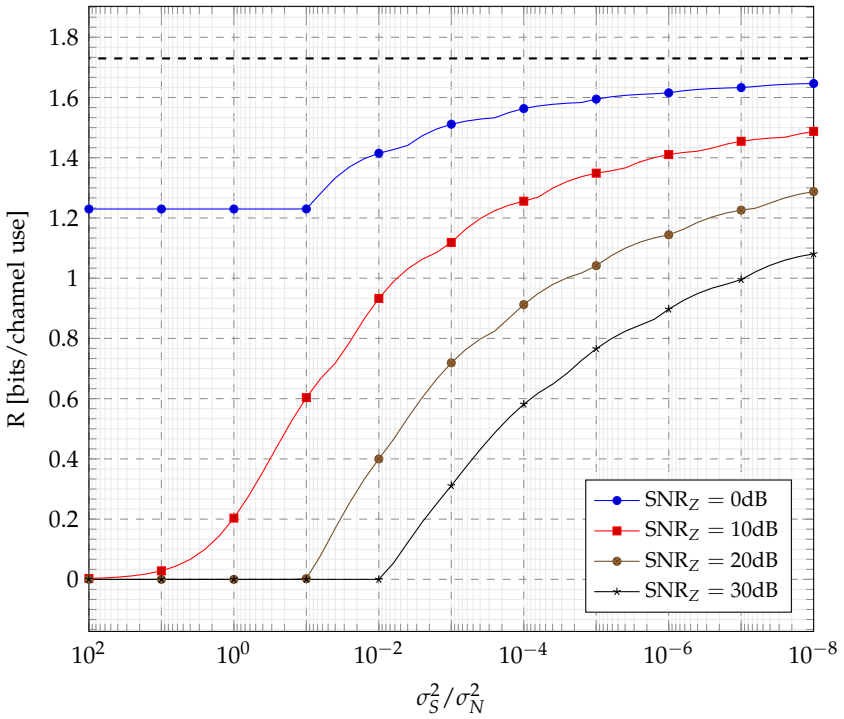


Figure 18.: Achievable rate by the JSCC scheme for $\mathrm{SNR}_Y = P/\sigma_N^2$ ($= 10\mathrm{dB}$) and different values of $\mathrm{SNR}_Z = P/\sigma_M^2$, with respect to the feedback noise variance. The dashed line is the channel capacity without the eavesdropper.

Finally,

$$\boldsymbol{C}_{Y^b|U^b} = \boldsymbol{C}_{Y^b} - \mathrm{diag}(P, \bar{\beta}P, \ldots, \bar{\beta}P), \text{ and} \tag{206}$$

$$\boldsymbol{C}_{Z^b|U^b} = \boldsymbol{C}_{Z^b} - \mathrm{diag}(P, \bar{\beta}P, \ldots, \bar{\beta}P). \tag{207}$$

□

Discussion

The expression (198) cannot be calculated in closed form so we proceed numerically. In Fig. 18, we plot the maximum achievable rate attained by the JSCC scheme according to (198) with respect to the fractional feedback noise variance σ_S^2/σ_N^2 for different values of SNR at the eavesdropper. As expected, the smaller the noise present in the feedback, the larger the achievable rate by the scheme. Moreover, as the feedback becomes noisier, the achievable rate falls back to the WTC rate, i.e. $I(X;Y) - I(X;Z)$, which is zero when the eavesdropper has a better channel. Remarkably, thanks to the feedback, the achievable rate is nonzero even in unfavorable scenarios where the eavesdropper experiences a much better channel than the legitimate user.

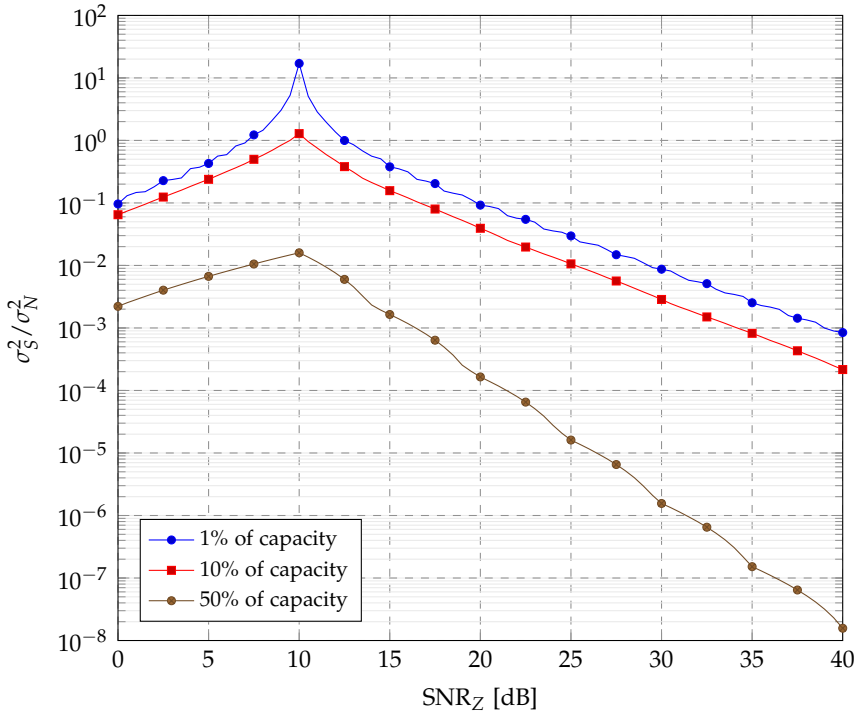


Figure 19.: Maximum admissible fractional feedback noise σ_S^2/σ_N^2 to attain a percentage of the point-to-point channel capacity, with respect to the eavesdropper's SNR.

As mentioned previously, the capacity of the Gaussian WTC with perfect output feedback is equal to the capacity of the PtP channel without the eavesdropper. A noisy feedback, on the other hand, imposes a penalty in the achievable rate of the proposed scheme as seen in Fig. 18. The feedback quality is in direct relation to the achievable rate, thus, a normal question to ask is how noisy the feedback may be in order to attain a certain percentage φ of the PtP channel capacity with respect to the secrecy capacity without feedback. In other words, if R is the rate achieved by (198), C_{spf} is the secrecy capacity with perfect feedback (186), and C_s is the secrecy capacity without feedback, the aforementioned percentage φ is defined as

$$\varphi = \frac{R - \mathrm{C}_s}{\mathrm{C}_{spf} - \mathrm{C}_s}. \tag{208}$$

In Fig. 19, we plot the maximum admissible fractional feedback noise σ_S^2/σ_N^2 for three different values of φ.

A particular behavior is seen in the curves of Fig. 19. When the eavesdropper has a better channel than the legitimate user, the feedback noise variance needed to achieve a certain percentage of PtP capacity decreases logarithmically with increasing eavesdropper's SNR. On the other hand, when the eavesdropper has a worse channel, since the capacity without feedback is nonzero, the behavior is reversed.

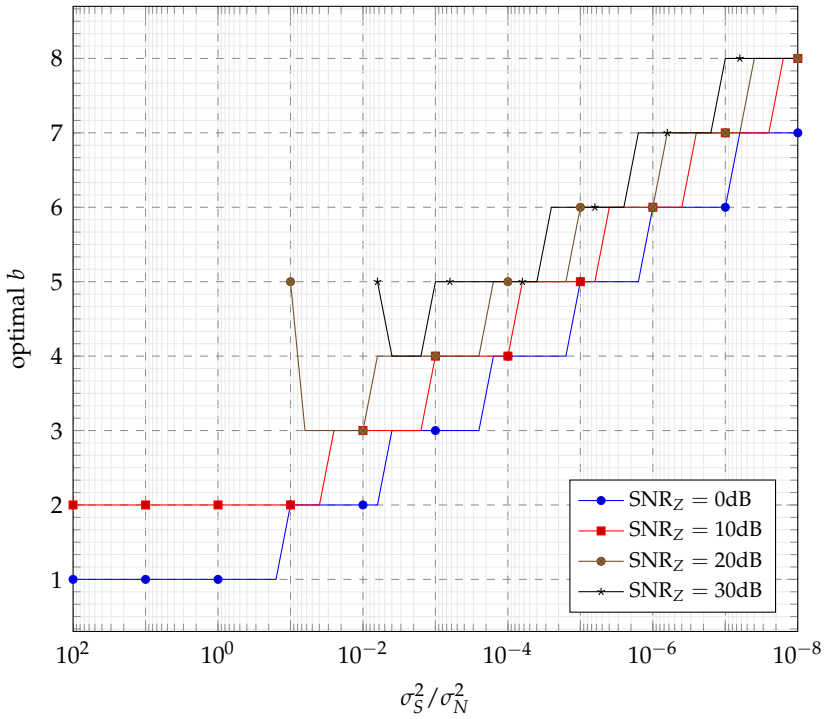


Figure 20.: Optimal number of blocks in the JSCC scheme for $\text{SNR}_Y = P/\sigma_N^2$ (= 10dB) and different values of $\text{SNR}_Z = P/\sigma_M^2$, with respect to the feedback noise variance.

The maximal feedback noise variance needed to increase the rate over the non-feedback rate decreases logarithmically with decreasing eavesdropper's SNR.

It is worth mentioning that the maximization of (198) involves not only the parameter β but also the number of blocks b used, as seen in Fig. 20. Given the recursive nature of the SK scheme, the presence of noise in the feedback is destructive for the system. To prevent this, less blocks are used as the feedback becomes noisier. If the legitimate user has a better channel than the eavesdropper, eventually, the optimal number of blocks is one and the feedback is completely ignored. Inversely, if the eavesdropper has a better channel, the feedback is always needed and the optimal number of blocks never reaches one. In this case, due to the behavior of (198), the maximization produces a larger optimal value of b when the rate is almost zero.

The behavior of the optimal β is almost binary, taking primarily the values 0 or 1. Whenever the feedback is used, i.e. optimal $b \geq 2$, $\beta = 1$, and when optimal $b = 1$, $\beta = 0$. The transition occurs in a very small interval of σ_S^2/σ_N^2 where the achievable rate barely varies. Therefore, for practical considerations β should be seen as a binary parameter.

5.4 SUMMARY AND CONCLUDING REMARKS

In this part of the thesis, we have proposed two achievable schemes for the WCGF. Each scheme follows a different approach in securing the communication: either by generating a secret key that encrypts the transmitted message or by "aligning" the codewords in a way that is beneficial for the legitimate receiver. We have shown how several previous results for different channel and feedback models can be achieved with these schemes. Additionally, we analyzed the Gaussian model with noisy feedback and obtained nonzero rates even when the eavesdropper experiences a better channel than the legitimate user.

In the analysis of the erasure WTC with state-feedback, we showed that the scheme of Theorem 5.2 is suboptimal (Section 5.3.4), while the scheme of Theorem 5.1, is not (Section 5.3.5). However, in another model, Theorem 5.2 achieves a higher rate than Corollary 5.1 (see Remark 5.5), which is derived from Theorem 5.1. Since the evaluation of Theorem 5.1 is cumbersome, we are not able to conclude that Theorem 5.2 is actually better than Theorem 5.1 in this model. Nevertheless, it may seem that both approaches are complementary to each other. This analysis is the focus of ongoing work.

Finally, we presented an inner bound on secret key agreement for the channel model, which recovers the well-known capacity result of [8].

APPENDIX

5.A PROOF OF THEOREM 5.1

The whole transmission is divided into b blocks of n time slots, and we employ joint source-channel coding to convey the message to be sent and the feedback from previous blocks. This strategy allows thus the transmission of both digital and analog information.

5.A.1 *Codebook Generation*

Let us define the quantities

$$\bar{R}_j = I(U_j; Z^b|U^{j-1}) - \bar{\epsilon}_j, \tag{209}$$

$$\tilde{R}_j = \max\left\{I(U_j; X^{j-1}\hat{Y}^{j-1}|U^{j-1}),\, I(U_j; Z^b|U^{j-1})\right\} + \tilde{\epsilon}_j, \tag{210}$$

and fix the following joint PD

$$\begin{aligned} &p(u^n_{[1:b]}x^n_{[1:b]}y^n_{[1:b]}\hat{y}^n_{[1:b]}z^n_{[1:b]}) \\ &= \prod_{j=1}^{b} p(u^n_{[j]}x^n_{[j]}|u^n_{[1:j-1]}x^n_{[1:j-1]}\hat{y}^n_{[1:j-1]})p(y^n_{[j]}\hat{y}^n_{[j]}z^n_{[j]}|x^n_{[j]}) \\ &= \prod_{j=1}^{b}\prod_{i=1}^{n} p(u_{i[j]}x_{i[j]}|u_{i[1:j-1]}x_{i[1:j-1]}\hat{y}_{i[1:j-1]})p(y_{i[j]}\hat{y}_{i[j]}z_{i[j]}|x_{i[j]}) \end{aligned} \tag{211}$$

Then, for each block, proceed as follows:

1. For block 1, generate 2^{nbR} subcodebooks $\mathcal{C}(m)$, each one with $2^{n\bar{R}_1}$ i.i.d. sequences $u^n_1(m,k_1)$, where $m \in [1:2^{nbR}]$ and $k_1 \in [1:2^{n\bar{R}_1}]$, according to the PD

$$p(u^n_1) = \prod_{i=1}^{n} p(u_{i[1]}).$$

2. For block $j \in [2:b]$ and given the sequence of codewords $u^n_{[1:j-1]}(m,k^{j-1}) = \left(u^n_1(m,k_1), u^n_2(m,k^2), \ldots u^n_{j-1}(m,k^{j-1})\right)$, generate $2^{n\tilde{R}_j}$ conditionally independent sequences $u^n_j(m,k^{j-1},k_j) \equiv u^n_j(m,k^j)$, where $k_j \in [1:2^{n\tilde{R}_j}]$, according to the PD

$$p(u^n_j|u^n_{[1:j-1]}(m,k^{j-1})) = \prod_{i=1}^{n} p(u_{i[j]}|u_{i[1:j-1]}(m,k^{j-1})).$$

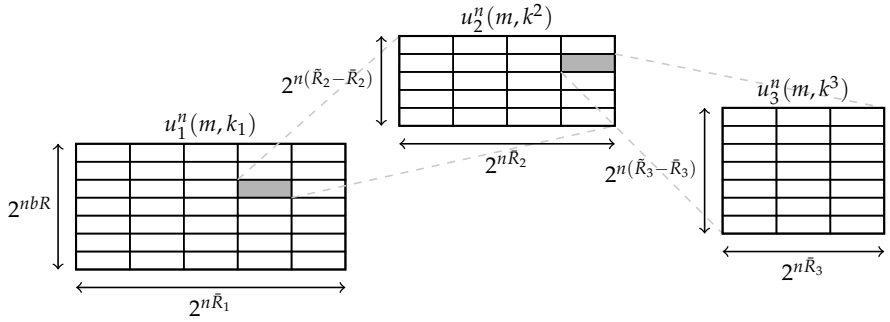


Figure 21.: Schematic representation of the codebooks for the first three blocks.

3. For block $j \in [2 : b]$, partition the set $[1 : 2^{n\tilde{R}_j}]$ into $2^{n[\tilde{R}_j - \tilde{R}_j]}$ bins and index each bin associated with k_j as $l_j = \mathcal{B}(k_j)$, where $l_j \in [1 : 2^{n[\tilde{R}_j - \tilde{R}_j]}]$. There are $2^{n\tilde{R}_j}$ codewords in each bin l_j.

An schematic representation of the codebook construction for the first three blocks is found in Fig. 21.

5.A.2 *Encoding*

1. In block 1, let m be the message to be sent. The encoder chooses randomly and uniformly a codeword from the subcodebook $\mathcal{C}(m)$, i.e., $u_1^n(m,k_1)$. It then sends the associated jointly typical sequence $x_1^n(m,k_1)$ that is randomly generated according to the conditional PD

$$p(x_1^n|u_1^n(m,k_1)) = \prod_{i=1}^{n} p(x_{i[1]}|u_{i[1]}(m,k_1)).$$

2. For block $j \in [2 : b]$, given the past codewords and feedback sequences, the encoder looks for an index $k_j \equiv \hat{k}$ such that

$$\begin{aligned}\big(u_1^n(m,k_1),\dots,u_{j-1}^n(m,k^{j-1}),u_j^n(m,k^{j-1},\hat{k}),x_1^n(m,k_1),\dots,\\ x_{j-1}^n(m,k^{j-1}),\hat{y}_1^n,\dots,\hat{y}_{j-1}^n\big) \in T_{\delta'}^n(U^jX^{j-1}\hat{Y}^{j-1}).\end{aligned}$$

If $\delta' \leq \tilde{\epsilon}_j$, the existence of at least one such index is guaranteed by the size of $\tilde{R}_j$. If several indices are found, choose one randomly and uniformly.

The encoder then sends the associated jointly typical sequence $x_j^n(m,k^j)$ that is randomly generated according to the conditional PD

$$\begin{aligned}&p(x_j^n|u_{[1:j]}^n(m,k^j),x_{[1:j-1]}^n(m,k^{j-1}),\hat{y}_{[1:j-1]}^n)\\ &\qquad=\prod_{i=1}^{n} p(x_{i[j]}|u_{i[1:j]}(m,k^j),x_{i[1:j-1]}(m,k^{j-1}),\hat{y}_{i[1:j-1]}).\end{aligned}$$

5.A.3 *Decoding*

The legitimate decoder waits until the last block is received and performs joint decoding of all the sequences, i.e., it looks for the unique index $m \equiv \hat{m}$ such that,

$$\left(u_1^n(\hat{m}, k_1), u_2^n(\hat{m}, k^2), \ldots, u_b^n(\hat{m}, k^b), y_1^n, y_2^n, \ldots, y_b^n\right) \in T_\delta^n(U^b Y^b),$$

for some k^b. The probability of error in the decoding of m can be made arbitrarily small if,

$$bR + \bar{R}_1 + \sum_{j=2}^{b} \tilde{R}_j < I(U^b; Y^b) - \delta. \tag{212}$$

Therefore, as $n \to \infty$, the achievable rate is,

$$\begin{aligned}
bR &< \sum_{j=1}^{b} I(U_j; Y^b | U^{j-1}) - \bar{R}_1 - \sum_{j=2}^{b} \tilde{R}_j \\
&= I(U_1; Y^b) - I(U_1; Z^b) + \sum_{j=2}^{b} \left[I(U_j; Y^b | U^{j-1}) - \tilde{R}_j \right] \\
&= I(U_1; Y^b) - I(U_1; Z^b) + \sum_{j=2}^{b} \min\Big\{ I(U_j; Y^b | U^{j-1}) \\
&\qquad - I(U_j; X^{j-1}\hat{Y}^{j-1} | U^{j-1}), I(U_j; Y^b | U^{j-1}) - I(U_j; Z^b | U^{j-1}) \Big\} \\
&= I(U_1; Y^b) - I(U_1; Z^b) + \sum_{j=2}^{b} \min\Big\{ I(U_j; Y_j^b | U^{j-1} Y^{j-1}) \\
&\qquad - I(U_j; X^{j-1}\hat{Y}^{j-1} | U^{j-1} Y^{j-1}),\ I(U_j; Y^b | U^{j-1}) - I(U_j; Z^b | U^{j-1}) \Big\},
\end{aligned}$$

where the last equality is due to $U_j \multimap (U^{j-1} X^{j-1} \hat{Y}^{j-1}) \multimap Y^{j-1}$ being a Markov chain.

5.A.4 *Information Leakage Rate*

Let us denote with $\mathbb{M}$, L_j and K_j the RV associated with the transmitted message m, the bin index $l_j = \mathcal{B}(k_j)$, and the codeword index k_j in block j, respectively.

Consider the following,

$$\begin{aligned}
&H(\mathbb{M} | Z_{[1:b]}^n) \\
&\quad = H(\mathbb{M} L_2^b | Z_{[1:b]}^n) - H(L_2^b | \mathbb{M} Z_{[1:b]}^n) \\
&\quad = H(\mathbb{M} L_2^b U_{[1:b]}^n | Z_{[1:b]}^n) - H(U_{[1:b]}^n | \mathbb{M} L_2^b Z_{[1:b]}^n) - H(L_2^b | \mathbb{M} Z_{[1:b]}^n) \\
&\quad \geq H(U_{[1:b]}^n | Z_{[1:b]}^n) - H(U_{[1:b]}^n | \mathbb{M} L_2^b Z_{[1:b]}^n) - H(L_2^b | \mathbb{M} Z_{[1:b]}^n) \qquad (213a) \\
&\quad \geq H(U_{[1:b]}^n | Z_{[1:b]}^n) - H(U_{[1:b]}^n | \mathbb{M} L_2^b Z_{[1:b]}^n) - \sum_{j=2}^{b} n(\tilde{R}_j - \bar{R}_j) \qquad (213b)
\end{aligned}$$

$$\geq H(U^n_{[1:b]}|Z^n_{[1:b]}) - H(U^n_{[1:b]}|Y^n_{[1:b]}) - H(U^n_{[1:b]}|\mathbb{M}L^b_2 Z^n_{[1:b]}) - \sum_{j=2}^{b} n(\tilde{R}_j - \bar{R}_j) \tag{213c}$$

$$= I(U^n_{[1:b]}; Y^n_{[1:b]}) - I(U^n_{[1:b]}; Z^n_{[1:b]}) - H(U^n_{[1:b]}|\mathbb{M}L^b_2 Z^n_{[1:b]}) + nI(U^b_2; Z^b|U_1) - \sum_{j=2}^{b} n(\tilde{R}_j + \bar{\epsilon}_j),$$

$$\geq n\Big[I(U^b; Y^b) - I(U_1; Z^b) - \sum_{j=2}^{b}(\tilde{R}_j + \bar{\epsilon}_j) - b(\eta_1 + \eta_2)\Big], \tag{213d}$$

where (213a) is due to $H(\mathbb{M}L^b_2|U^n_{[1:b]}Z^n_{[1:b]}) \geq 0$; where (213b) is due to $H(L^b_2|\mathbb{M}Z^n_{[1:b]}) \leq H(L^b_2) \leq \sum_{j=2}^{b} n(\tilde{R}_j - \bar{R}_j)$; where (213c) is due to $H(U^n_{[1:b]}|Y^n_{[1:b]}) \geq 0$; and (213d) stems from the following two lemmas.

Lemma 5.1. *Given the encoding process of Section 5.A.2,*

$$I(U^n_{[1:b]}; Y^n_{[1:b]}) - I(U^n_{[1:b]}; Z^n_{[1:b]}) \geq n\Big[I(U^b; Y^b) - I(U^b; Z^b) - b\eta_1\Big]. \tag{214}$$

Proof. See Appendix 5.D. □

Lemma 5.2. *Given the encoding process of Section 5.A.2,*

$$H(U^n_{[1:b]}|\mathbb{M}L^b_2 Z^n_{[1:b]}) \leq bn\eta_2. \tag{215}$$

Proof. See Appendix 5.E. □

Now, according to (212),

$$H(\mathbb{M}) = bnR < n\Big[I(U^b; Y^b) - \bar{R}_1 - \sum_{j=2}^{b}\tilde{R}_j - \delta\Big].$$

Therefore, the information leakage rate is upper-bounded by,

$$I(\mathbb{M}; Z^n_{[1:b]}) \leq n\Big[b(\eta_1 + \eta_2) - \delta + \sum_{j=1}^{b}\bar{\epsilon}_j\Big].$$

which guarantees that the message is hidden from the eavesdropper asymptotically.

5.B PROOF OF COROLLARY 5.1

Let us fix the special choice of RVs

$$U_j = \begin{cases} \bar{U}_j \sim p(\bar{u}_j) & \text{if } j = 1 \\ (\bar{U}_j \bar{V}_{j-1}) \sim p(\bar{u}_j)p(\bar{v}_{j-1}|\bar{u}_{j-1}\bar{x}_{j-1}\hat{y}_{j-1}) & \text{if } j \in [2:b] \end{cases}$$
$$X_j = \bar{X}_j \sim p(\bar{x}_j|\bar{u}_j), \qquad \forall\, j \in [1:b]$$

where the distributions are the same for each block. Then, the joint PD (211) becomes

$$\begin{aligned}
&p(\bar{u}^n_{[1:b]}\bar{v}^n_{[1:b-1]}\bar{x}^n_{[1:b]}y^n_{[1:b]}\hat{y}^n_{[1:b]}z^n_{[1:b]}) \\
&\quad= \left[\prod_{j=1}^{b-1} p(\bar{u}^n_j\bar{x}^n_j)p(\bar{v}^n_j|\bar{u}^n_j\bar{x}^n_j\hat{y}^n_j)p(y^n_j\hat{y}^n_jz^n_j|\bar{x}^n_j)\right] p(\bar{u}^n_b\bar{x}^n_b)p(y^n_b\hat{y}^n_bz^n_b|\bar{x}^n_b) \\
&\quad= \prod_{i=1}^{n}\left[\prod_{j=1}^{b-1} p(\bar{u}_{i[j]}\bar{x}_{i[j]})p(\bar{v}_{i[j]}|\bar{u}_{i[j]}\bar{x}_{i[j]}\hat{y}_{i[j]})p(y_{i[j]}\hat{y}_{i[j]}z_{i[j]}|\bar{x}_{i[j]})\right]\times \\
&\qquad\qquad p(\bar{u}_{i[b]}\bar{x}_{i[b]})p(y_{i[b]}\hat{y}_{i[b]}z_{i[b]}|\bar{x}_{i[b]}),
\end{aligned}$$

where we see that each block is now independent of the others.

The achievable rate (212) can be written as

$$\begin{aligned}
bR < I(U^b;Y^b) - I(U_1;Z^b) - \sum_{j=2}^{b}\max\Big\{&I(U_j;X^{j-1}\hat{Y}^{j-1}|U^{j-1}), \\
&I(U_j;Z^b|U^{j-1})\Big\},
\end{aligned} \tag{216}$$

and we analyze each term separately in the sequel.

The first one,

$$\begin{aligned}
&I(U^b;Y^b) \\
&\quad= I(\bar{U}^b\bar{V}^{b-1};Y^b) \\
&\quad= \sum_{j=1}^{b-1} I(\bar{U}_j\bar{V}_j;Y^b|\bar{U}^{j-1}\bar{V}^{j-1}) + I(\bar{U}_b;Y^b|\bar{U}^{b-1}\bar{V}^{b-1}) \\
&\quad= \sum_{j=1}^{b-1} I(\bar{U}_j\bar{V}_j;Y_j) + I(\bar{U}_b;Y_b) && \text{(217a)} \\
&\quad= (b-1)I(\bar{U}\bar{V};Y) + I(\bar{U};Y), && \text{(217b)}
\end{aligned}$$

where (217a) is due to the independence between blocks; and (217b) follows from having the same distribution in each block. The same applies to the second term of (216),

$$I(U_1;Z^b) = I(\bar{U}_1;Z^b) = I(\bar{U}_1;Z_1) = I(\bar{U};Z). \tag{218}$$

The third term,

$$\begin{aligned}
&I(U_j;X^{j-1}\hat{Y}^{j-1}|U^{j-1}) \\
&\quad= I(\bar{U}_j\bar{V}_{j-1};\bar{X}^{j-1}\hat{Y}^{j-1}|\bar{U}^{j-1}\bar{V}^{j-2}) \\
&\quad= I(\bar{V}_{j-1};\bar{X}^{j-1}\hat{Y}^{j-1}|\bar{U}^{j-1}\bar{V}^{j-2}) + I(\bar{U}_j;\bar{X}^{j-1}\hat{Y}^{j-1}|\bar{U}^{j-1}\bar{V}^{j-1}) \\
&\quad= I(\bar{V}_{j-1};\bar{X}_{j-1}\hat{Y}_{j-1}|\bar{U}_{j-1}) \\
&\quad= I(\bar{V};\bar{X}\hat{Y}|\bar{U}), && \text{(219)}
\end{aligned}$$

where we have again used the fact that blocks are independent and follow the same distribution. Similarly, the last term of (216),

$$\begin{aligned} &I(U_j; Z^b|U^{j-1}) \\ &\quad= I(\bar{U}_j\bar{V}_{j-1}; Z^b|\bar{U}^{j-1}\bar{V}^{j-2}) \\ &\quad= I(\bar{V}_{j-1}; Z^b|\bar{U}^{j-1}\bar{V}^{j-2}) + I(\bar{U}_j; Z^b|\bar{U}^{j-1}\bar{V}^{j-1}) \\ &\quad= I(\bar{V}_{j-1}; Z_{j-1}|\bar{U}_{j-1}) + I(\bar{U}_j; Z_j) \\ &\quad= I(\bar{V}; Z|\bar{U}) + I(\bar{U}; Z) \\ &\quad= I(\bar{U}\bar{V}; Z). \end{aligned} \tag{220}$$

Therefore, the achievable rate by the JSCC scheme with this particular choice of joint PD is

$$\begin{aligned} R < \frac{b-1}{b}\left[I(\bar{U}\bar{V}; Y) - \max\{I(\bar{V}; \bar{X}\hat{Y}|\bar{U}),\, I(\bar{U}\bar{V}; Z)\}\right] \\ + \frac{1}{b}\left[I(\bar{U}; Y) - I(\bar{U}; Z)\right], \end{aligned} \tag{221}$$

which tends to (143) as $b \to \infty$.

5.C PROOF OF THEOREM 5.2

The encoder splits the transmission in b blocks of n time slots, during which it transmits $b-1$ messages of rate R. The region R_{KG_1} is obtain by the joint use of Wyner's wiretap scheme and an encryption key generated through the feedback link, whereas R_{KG_2} only relies on the aforementioned encryption key. If the eavesdropper is able to decode everything the legitimate decoder can, the second scheme obtains higher rates. In the sequel, we show the proof for R_{KG_1}, while the proof of R_{KG_2} is relegated to the end.

5.C.1 *Codebook Generation*

Let us define the quantities

$$S_1 = I(T; UX\hat{Y}|Q) + \epsilon_1 \tag{222a}$$
$$\tilde{S}_1 = I(T; UX\hat{Y}|Q) - I(T; UY|Q) + \epsilon_1 + \tilde{\epsilon}_1 \tag{222b}$$
$$S_2 = I(V; X\hat{Y}|UT) + \epsilon_2 \tag{222c}$$
$$\tilde{S}_2 = I(V; X\hat{Y}|UT) - I(V; Y|UT) + \epsilon_2 + \tilde{\epsilon}_2 \tag{222d}$$
$$\bar{S}_2 = I(V; Y|UT) - I(V; Z|UT) \tag{222e}$$
$$R_1 + R_f = I(U; TZ|Q) - \epsilon', \tag{222f}$$

and fix the joint distribution (144) that achieves the maximum in R_{KG_1}. Then, for each block, create independent codebooks as follows:

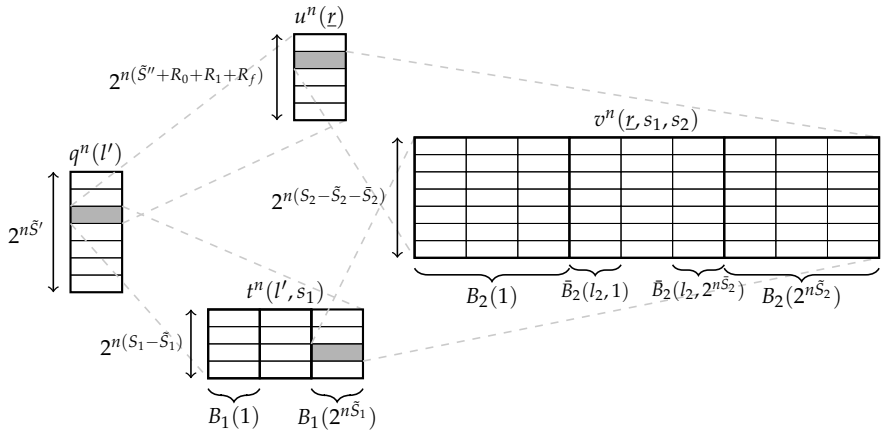


Figure 22.: Schematic representation of the codebook. The index s_1 in the bins and sub-bins of $v^n(\cdot)$ is not shown to improve readability.

1. Generate $2^{n\tilde{S}'}$ i.i.d. sequences $q^n(l')$, where $l' \in [1 : 2^{n\tilde{S}'}]$, according to the PD

$$p(q^n) = \prod_{i=1}^{n} p(q_i).$$

2. For each seq. $q^n(l')$, generate $2^{n(\tilde{S}''+R_0+R_1+R_f)}$ conditionally independent sequences $u^n(\underline{r}) \equiv u^n(l', l'', m_0, m_1, l_f)$, where $l'' \in [1 : 2^{n\tilde{S}''}]$, $m_0 \in [1 : 2^{nR_0}]$, $m_1 \in [1 : 2^{nR_1}]$, and $l_f \in [1 : 2^{nR_f}]$, according to the PD

$$p(u^n|q^n(l')) = \prod_{i=1}^{n} p(u_i|q_i(l')).$$

3. For each seq. $q^n(l')$, generate 2^{nS_1} conditionally independent sequences $t^n(l', s_1)$, where $s_1 \in [1 : 2^{nS_1}]$, according to the PD

$$p(t^n|q^n(l')) = \prod_{i=1}^{n} p(t_i|q_i(l')).$$

Distribute the sequences uniformly at random in $2^{n\tilde{S}_1}$ equal-size bins $B_1(l_1)$, which is possible since $\tilde{S}_1 \leq S_1$.

4. For each pair $(u^n(\underline{r}), t^n(l', s_1))$, generate 2^{nS_2} conditionally independent sequences $v^n(\underline{r}, s_1, s_2)$, where $s_2 \in [1 : 2^{nS_2}]$, according to the PD

$$p(v^n|u^n(\underline{r}), t^n(l', s_1)) = \prod_{i=1}^{n} p(v_i|u_i(\underline{r}), t_i(l', s_1)).$$

Distribute the sequences uniformly at random in $2^{n\tilde{S}_2}$ equal-size bins $B_2(s_1, l_2)$ and the sequences in each bin in $2^{n\bar{S}_2}$ equal-size sub-bins $\bar{B}_2(s_1, l_2, k)$. This binning process is feasible if

$$\tilde{S}_2 \leq S_2, \tag{223a}$$
$$\bar{S}_2 \leq S_2 - \tilde{S}_2, \tag{223b}$$

which holds under (222) as long as $I(V;Z|UT) \leq I(V;Y|UT)$.

See Fig. 22 for details.

5.C.2 *Encoding*

In block 1, the encoder chooses a codeword $u^n(\underline{r}_1)$ uniformly at random. It then transmits the associated jointly typical sequence $x^n(\underline{r}_1)$ that is randomly generated according to the conditional PD

$$p(x^n|u^n(\underline{r}_1)) = \prod_{i=1}^{n} p(x_i|u_i(\underline{r}_1)).$$

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

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

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

where $\delta' < \epsilon$. If more than one index is found, choose the smallest one. The probability of not finding such an index is arbitrarily small as $n \to \infty$.

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

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

where $\delta' < \epsilon$. If more than one index is found, choose the smallest one. The probability of not finding such an index is arbitrarily small as $n \to \infty$.

3. Let $t^n(l'_{j-1}, s_{1(j-1)}) \in B_1(l_{1(j-1)})$ and $v^n(\underline{r}_{j-1}, s_{1(j-1)}, s_{2(j-1)}) \in \bar{B}_2(s_{1(j-1)}, l_{2(j-1)}, k_{j-1})$, and define the following two mappings. First, let $(l'_j, l''_j) = M_l(l_{1(j-1)}, l_{2(j-1)})$, such that $M_l(\cdot)$ is invertible. Second, let $k'_{j-1} = M_k(k_{j-1})$, where $k'_{j-1} \in [1 : 2^{nR_1}]$ and $M_k(\cdot)$ is not necessarily invertible. These two functions can be defined if

$$\tilde{S}' + \tilde{S}'' = \tilde{S}_1 + \tilde{S}_2, \tag{224a}$$
$$R_1 \leq \bar{S}_2. \tag{224b}$$

4. In order to transmit the message $m_j = (m_{0j}, m_{1j})$, the encoder chooses uniformly at random a value $l_{fj} \in [1 : 2^{nR_f}]$ and selects the codeword $u^n(l'_j, l''_j, m_{0j}, m'_{1j}, l_{fj}) = u^n(\underline{r}_j)$, where $m'_{1j} = m_{1j} \oplus k'_{j-1}$. It then transmits the associated jointly typical sequence $x^n(\underline{r}_j)$, generated on the fly.

5.C.3 *Decoding*

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

1. The legitimate decoder looks for the unique set of indices $\underline{r}_j = (l'_j, l''_j, m_{0j}, m'_{1j}, l_{fj}) \equiv (\hat{l}', \hat{l}'', \hat{m}_0, \hat{m}'_1, \hat{l}_f)$ such that

$$\left(q^n(\hat{l}'), u^n(\hat{l}', \hat{l}'', \hat{m}_0, \hat{m}'_1, \hat{l}_f), y^n_j\right) \in T^n_\delta(QUY).$$

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

$$\tilde{S}'' + R_0 + R_1 + R_f < I(U; Y|Q) - \delta, \tag{225a}$$
$$\tilde{S}' + \tilde{S}'' + R_0 + R_1 + R_f < I(U; Y) - \delta. \tag{225b}$$

2. Compute $(l_{1(j-1)}, l_{2(j-1)}) = M_l^{-1}(l'_j, l''_j)$.

3. The legitimate decoder looks for the unique index $s_{1(j-1)} \equiv \hat{s}_1$ such that $t^n(l'_{j-1}, \hat{s}_1) \in B_1(l_{1(j-1)})$ and

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

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

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

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

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

5. The legitimate decoder then recovers the key $k'_{j-1} = M_k(k_{j-1})$ since $v^n(\underline{r}_{j-1}, s_{1(j-1)}, s_{2(j-1)}) \in \bar{B}_2(s_{1(j-1)}, l_{2(j-1)}, k_{j-1})$, and with this key, it decrypts the message, i.e., $m_j = (m_{0j}, m'_{1j} \oplus k'_{j-1})$.

5.C.4 *Key Leakage*

Let us denote with L_{1j} the RV associated with the bin index of codeword $T^n_{[j]}$ in block j, and L_{2j} and K_j the RVs associated with the bin and sub-bin index of codeword $V^n_{[j]}$ in block j, respectively.

Remark 5.8. *Owing to the encoding process, the variables L_{1j}, L_{2j} and $K'_j = M_k(K_j)$ are the sole responsible for the correlation between blocks, the latter through $\mathbb{M}_{1(j+1)} \oplus K'_j$. This fact is used in many of the subsequent Markov chains.*

Consider the following,

$$
\begin{aligned}
&H(K^{b-1}|Z^n_{[1:b]}) \\
&\quad \geq H(K^{b-1}|Z^n_{[1:b]}L_1^{b-1}L_2^{b-1}) \\
&\quad = \textstyle\sum_{j=1}^{b-1} H(K_j|Z^n_{[1:b]}L_1^{b-1}L_2^{b-1}K^{j-1}) \\
&\quad \geq \textstyle\sum_{j=1}^{b-1} H(K_j|U^n_{[j]}Z^n_{[j:b]}L_{1j}^{b-1}L_{2j}^{b-1}) && \text{(226a)} \\
&\quad \geq \textstyle\sum_{j=1}^{b-1} H(K_j|U^n_{[j]}Z^n_{[j]}L_{1j}L_{2j}, \mathbb{M}_{1(j+1)} \oplus K'_j) && \text{(226b)} \\
&\quad \geq \textstyle\sum_{j=1}^{b-1} H(K_j|U^n_{[j]}Z^n_{[j]}T^n_{[j]}L_{2j}, \mathbb{M}_{1(j+1)} \oplus K'_j) \\
&\quad = \textstyle\sum_{j=1}^{b-1} \Big[H(K_jV^n_{[j]}|U^n_{[j]}Z^n_{[j]}T^n_{[j]}L_{2j}, \mathbb{M}_{1(j+1)} \oplus K'_j) \\
&\qquad\qquad - H(V^n_{[j]}|U^n_{[j]}Z^n_{[j]}T^n_{[j]}L_{2j}K_j)\Big] && \text{(226c)}
\end{aligned}
$$

where (226a) is due to the fact that $(Z^n_{[1:j-1]}L_1^{j-1}L_2^{j-1}K^{j-1}) \multimap U^n_{[j]} \multimap (Z^n_{[j:b]}L_{1j}^{b-1}L_{2j}^{b-1}K_j)$ is a Markov chain since $U^n_{[j]}$ contains the indices $(L_{1(j-1)}L_{2(j-1)}K'_{j-1})$, see Remark 5.8; and where (226b) is due to $(Z^n_{[j+1:b]}L^b_{1(j+1)}L^b_{2(j+1)}) \multimap (L_{1j}L_{2j}, \mathbb{M}_{1(j+1)} \oplus K'_j) \multimap (K_jU^n_{[j]}Z^n_{[j]})$, see Remark 5.8.

The first term in (226c) can be lower-bounded as follows,

$$
\begin{aligned}
&H(V^n_{[j]}|U^n_{[j]}Z^n_{[j]}T^n_{[j]}L_{2j}, \mathbb{M}_{1(j+1)} \oplus K'_j) \\
&\quad = H(V^n_{[j]}|U^n_{[j]}Z^n_{[j]}T^n_{[j]}) - I(V^n_{[j]}; L_{2j}|U^n_{[j]}Z^n_{[j]}T^n_{[j]}) \\
&\qquad - I(V^n_{[j]}; \mathbb{M}_{1(j+1)} \oplus K'_j|U^n_{[j]}Z^n_{[j]}T^n_{[j]}L_{2j}) \\
&\quad \geq H(V^n_{[j]}|U^n_{[j]}Z^n_{[j]}T^n_{[j]}) - H(L_{2j}) - I(K'_j; \mathbb{M}_{1(j+1)} \oplus K'_j) && \text{(227a)} \\
&\quad \geq H(V^n_{[j]}|U^n_{[j]}Z^n_{[j]}T^n_{[j]}) - n\tilde{S}_2 && \text{(227b)} \\
&\quad \geq H(V^n_{[j]}|U^n_{[j]}Z^n_{[j]}T^n_{[j]}) - H(V^n_{[j]}|U^n_{[j]}X^n_{[j]}\hat{Y}^n_{[j]}T^n_{[j]}) - n\tilde{S}_2 \\
&\quad = I(V^n_{[j]}; X^n_{[j]}\hat{Y}^n_{[j]}|U^n_{[j]}T^n_{[j]}) - I(V^n_{[j]}; Z^n_{[j]}|U^n_{[j]}T^n_{[j]}) - n\tilde{S}_2 \\
&\quad \geq n[\, I(V; X\hat{Y}|UT) - I(V; Z|UT) - \eta - \tilde{S}_2\,] && \text{(227c)} \\
&\quad = n[\, I(V; Y|UT) - I(V; Z|UT) - \eta'\,] \\
&\quad = n(\, \bar{S}_2 - \eta'\,) && \text{(227d)}
\end{aligned}
$$

where (227a) is due to $\mathbb{M}_{1(j+1)} \oplus K'_j \multimap K'_j \multimap (V^n_{[j]} U^n_{[j]} Z^n_{[j]} T^n_{[j]} L_{2j})$; (227b) is due to $H(L_{2j}) \leq n\tilde{S}_2$, and $H(\mathbb{M}_{1(j+1)} \oplus K'_j) = H(\mathbb{M}_{1(j+1)})$ since $\mathbb{M}_{1(j+1)}$ is uniformly distributed on $[1 : 2^{nR_1}]$ and independent of K'_j; and where (227c) stems from the following lemma.

Lemma 5.3. *Given the encoding process of Section 5.C.2,*

$$I(V^n; X^n \hat{Y}^n | U^n T^n) - I(V^n; Z^n | U^n T^n) \geq n[\, I(V; X\hat{Y}|UT) - I(V; Z|UT) - \eta \,]. \quad (228)$$

Proof. The proof is analogous to the one of Lemma 5.1, therefore it is not presented. □

The second term in (226c) can be upper-bounded using Fano's inequality, as in Lemma 5.2, since $S_2 - \tilde{S}_2 - \bar{S}_2 < I(V; Z|UT)$, i.e.,

$$H(V^n_{[j]} | U^n_{[j]} Z^n_{[j]} T^n_{[j]} L_{2j} K_j) \leq n\epsilon_n, \quad (229)$$

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

Therefore, joining (226c), (227d) and (229), we obtain

$$\begin{aligned} I(K^{b-1}; Z^n_{[1:b]}) &= H(K^{b-1}) - H(K^{b-1} | Z^n_{[1:b]}) \\ &\leq n(b-1)\bar{S}_2 - n(b-1)(\bar{S}_2 - \eta'') \\ &= n(b-1)\eta'', \end{aligned}$$

and the key is asymptotically secure.

5.C.5 *Information Leakage Rate*

We now proceed to bound the information leakage of the $b-1$ messages $\mathbb{M}^b = (\mathbb{M}^b_0, \mathbb{M}^b_1)$. Consider first,

$$\begin{aligned} &I(\mathbb{M}^b_0; Z^n_{[1:b]}) \\ &\quad = \textstyle\sum_{j=2}^{b} I(\mathbb{M}_{0j}; Z^n_{[1:b]} | \mathbb{M}^{j-1}_0) \\ &\quad \leq \textstyle\sum_{j=2}^{b} I(\mathbb{M}_{0j}; Z^n_{[1:b]} T^n_{[j]} \mathbb{M}^{j-1}_0 L_{1(j-1)} L_{2(j-1)} K'_{j-1}) \\ &\quad = \textstyle\sum_{j=2}^{b} \Big[I(\mathbb{M}_{0j}; Z^n_{[j]} T^n_{[j]} | L_{1(j-1)} L_{2(j-1)} K'_{j-1}) \\ &\qquad\qquad + I(\mathbb{M}_{0j}; Z^n_{[j+1:b]} | Z^n_{[j]} T^n_{[j]} L_{1(j-1)} L_{2(j-1)} K'_{j-1}) \Big], \end{aligned} \quad (230)$$

where the last equality is due to the fact that $(L_{1(j-1)} L_{2(j-1)} K'_{j-1})$ is independent of $\mathbb{M}_{0j}$ and that $(Z^n_{[1:j-1]} \mathbb{M}^{j-1}_0) \multimap (L_{1(j-1)} L_{2(j-1)} K'_{j-1}) \multimap (\mathbb{M}_{0j} Z^n_{[j:b]})$ is a Markov chain, see Remark 5.8. The first term in (230) corresponds to the information leakage in block j of the message $\mathbb{M}_{0j}$ given the indices $(L'_j L''_j)$, which is upper-bounded by $n\eta_1$ thanks to (222f). The conditioning over K'_{j-1} does not affect this term because

$Z_{[j]}^n$ is only correlated to $\mathbb{M}_{1j} \oplus K'_{j-1}$ which is independent of K'_{j-1}, given that $\mathbb{M}_{1j}$ is uniformly distributed on $[1 : 2^{nR_1}]$ and independent of K'_{j-1}.

The second term in (230) can be bounded as follows

$$\begin{aligned}
&I(\mathbb{M}_{0j}; Z_{[j+1:b]}^n | Z_{[j]}^n T_{[j]}^n L_{1(j-1)} L_{2(j-1)} K'_{j-1}) \\
&\quad \le I(\mathbb{M}_{0j} L_{1(j-1)} L_{2(j-1)} K'_{j-1} Z_{[j]}^n; Z_{[j+1:b]}^n | T_{[j]}^n) \\
&\quad \le I(U_{[j]}^n Z_{[j]}^n; Z_{[j+1:b]}^n | T_{[j]}^n) && \text{(231a)} \\
&\quad \le I(U_{[j]}^n Z_{[j]}^n; L_{1j} L_{2j}, \mathbb{M}_{1(j+1)} \oplus K'_j | T_{[j]}^n) && \text{(231b)} \\
&\quad = I(U_{[j]}^n Z_{[j]}^n; L_{2j} | T_{[j]}^n) + I(U_{[j]}^n Z_{[j]}^n; \mathbb{M}_{1(j+1)} \oplus K'_j | T_{[j]}^n L_{2j}) \\
&\quad \le I(U_{[j]}^n Z_{[j]}^n; L_{2j} | T_{[j]}^n) + I(K'_j; \mathbb{M}_{1(j+1)} \oplus K'_j) && \text{(231c)} \\
&\quad = I(U_{[j]}^n Z_{[j]}^n; L_{2j} | T_{[j]}^n), && \text{(231d)}
\end{aligned}$$

where (231a) is due to the Markov chain $(\mathbb{M}_{0j} L_{1(j-1)} L_{2(j-1)} K'_{j-1}) \multimap U_{[j]}^n \multimap (T_{[j]}^n Z_{[j:b]}^n)$, since $U_{[j]}^n$ hides the indices $(\mathbb{M}_{0j} L_{1(j-1)} L_{2(j-1)} K'_{j-1})$, and the data processing inequality; (231b) is due to $(U_{[j]}^n Z_{[j]}^n T_{[j]}^n) \multimap (L_{1j} L_{2j}, \mathbb{M}_{1(j+1)} \oplus K'_j) \multimap Z_{[j+1:b]}^n$, see Remark 5.8; where (231c) is due to the Markov chain $\mathbb{M}_{1(j+1)} \oplus K'_j \multimap K'_j \multimap (U_{[j]}^n Z_{[j]}^n T_{[j]}^n L_{2j})$; and (231d) is due to $H(\mathbb{M}_{1(j+1)} \oplus K'_j) = H(\mathbb{M}_{1(j+1)})$ since $\mathbb{M}_{1(j+1)}$ is uniformly distributed on $[1 : 2^{nR_1}]$ and independent of K'_j.

In order to bound (231d), we make use of the following two lemmas.

Lemma 5.4 ([51, Lemma 2.5]). *Consider a discrete RV X taking on the mass points $x_1, \ldots, x_m$ and with probability mass function satisfying*

$$\frac{\Pr\{X = x_i\}}{\Pr\{X = x_j\}} \le 2 \cdot 2^{\delta}, \quad \forall i, j \in [1 : m]. \tag{232}$$

Then

$$H(X) \ge \log m - \delta - 1. \tag{233}$$

Lemma 5.5. *Given the encoding process of Section 5.C.2, the probability of the index L_{2j} can be bounded as follows*

$$\frac{2^{-n\eta/2}}{\beta} \le \Pr\left\{L_{2j} = l | U_{[j]}^n T_{[j]}^n Z_{[j]}^n\right\} \le \frac{2^{n\eta/2}}{\beta}, \tag{234}$$

where β is a normalization constant independent of the value of L_{2j}.

Proof. See Appendix 5.F. □

Lemma 5.5 allows us to write,

$$\frac{\Pr\left\{L_{2j} = l_1 | U_{[j]}^n T_{[j]}^n Z_{[j]}^n\right\}}{\Pr\left\{L_{2j} = l_2 | U_{[j]}^n T_{[j]}^n Z_{[j]}^n\right\}} \le 2^{n\eta} = 2 \cdot 2^{n\eta - 1}, \tag{235}$$

$\forall l_1, l_2 \in [1 : 2^{n\tilde{S}_2}]$. Therefore, according to Lemma 5.4,

$$H(L_{2j}|U^n_{[j]}T^n_{[j]}Z^n_{[j]}) \geq n(\tilde{S}_2 - \eta), \tag{236}$$

and

$$\begin{aligned} I(U^n_{[j]}Z^n_{[j]}; L_{2j}|T^n_{[j]}) &\leq H(L_{2j}) - H(L_{2j}|U^n_{[j]}T^n_{[j]}Z^n_{[j]}) \\ &\leq n\tilde{S}_2 - n(\tilde{S}_2 - \eta) \\ &= n\eta, \end{aligned} \tag{237}$$

which let us bound (231d), and in turn, (230),

$$I(\mathbb{M}^b_0; Z^n_{[1:b]}) \leq \sum_{j=2}^{b}(n\eta_1 + n\eta) = n(b-1)\eta_3. \tag{238}$$

Now consider,

$$\begin{aligned} &I(\mathbb{M}^b_1; Z^n_{[1:b]}|\mathbb{M}^b_0) \\ &\quad= \textstyle\sum_{j=2}^{b} I(\mathbb{M}_{1j}; Z^n_{[1:b]}|\mathbb{M}^b_0\mathbb{M}^{j-1}_1) \\ &\quad\leq \textstyle\sum_{j=2}^{b} I(\mathbb{M}_{1j}; U^n_{[j-1]}T^n_{[j-1:j]}Z^n_{[1:b]}|\mathbb{M}^b_0\mathbb{M}^{j-1}_1) \\ &\quad= \textstyle\sum_{j=2}^{b} \Big[I(\mathbb{M}_{1j}; U^n_{[j-1]}T^n_{[j-1]}Z^n_{[1:j-1]}|\mathbb{M}^b_0\mathbb{M}^{j-1}_1) \\ &\qquad\qquad + I(\mathbb{M}_{1j}; T^n_{[j]}Z^n_{[j]}|\mathbb{M}^b_0\mathbb{M}^{j-1}_1U^n_{[j-1]}T^n_{[j-1]}Z^n_{[1:j-1]}) \\ &\qquad\qquad + I(\mathbb{M}_{1j}; Z^n_{[j+1:b]}|\mathbb{M}^b_0\mathbb{M}^{j-1}_1U^n_{[j-1]}T^n_{[j-1:j]}Z^n_{[1:j]})\Big]. \end{aligned} \tag{239}$$

The first term in (239) is zero due to the independence between $\mathbb{M}_{1j}$ and $(U^n_{[j-1]}T^n_{[j-1]}Z^n_{[1:j-1]}\mathbb{M}^b_0\mathbb{M}^{j-1}_1)$, while the second term can be upper-bounded as follows

$$\begin{aligned} &I(\mathbb{M}_{1j}; T^n_{[j]}Z^n_{[j]}|\mathbb{M}^b_0\mathbb{M}^{j-1}_1U^n_{[j-1]}T^n_{[j-1]}Z^n_{[1:j-1]}) \\ &\quad\leq I(\mathbb{M}_{1j}; \mathbb{M}_{1j} \oplus K'_{j-1}|\mathbb{M}^b_0\mathbb{M}^{j-1}_1U^n_{[j-1]}T^n_{[j-1]}Z^n_{[1:j-1]}) && \text{(240a)} \\ &\quad\leq I(\mathbb{M}^b_0\mathbb{M}^j_1Z^n_{[1:j-2]}; \mathbb{M}_{1j} \oplus K'_{j-1}|U^n_{[j-1]}T^n_{[j-1]}Z^n_{[j-1]}) \\ &\quad\leq I(\mathbb{M}^b_0\mathbb{M}^j_1Z^n_{[1:j-2]}; K'_{j-1}|U^n_{[j-1]}T^n_{[j-1]}Z^n_{[j-1]}) + n\eta_4 && \text{(240b)} \\ &\quad= n\eta_4. && \text{(240c)} \end{aligned}$$

where (240a) is due to the Markov chain $\mathbb{M}_{1j} \multimap (\mathbb{M}_{1j} \oplus K'_{j-1}) \multimap (T^n_{[j]}Z^n_{[j]})$; where in (240b) $H(\mathbb{M}_{1j} \oplus K'_{j-1}|U^n_{[j-1]}T^n_{[j-1]}Z^n_{[j-1]}) = nR_1$ due to $\mathbb{M}_{1j}$ being independent of $(K'_{j-1}U^n_{[j-1]}T^n_{[j-1]}Z^n_{[j-1]})$, and similar to (236), $H(K'_{j-1}|U^n_{[j-1]}T^n_{[j-1]}Z^n_{[j-1]}) \geq n(R_1 - \eta_4)$ due to a quasi uniform distribution; and where (240c) is due to the Markov chain $K'_{j-1} \multimap (U^n_{[j-1]}T^n_{[j-1]}Z^n_{[j-1]}) \multimap (\mathbb{M}^b_0\mathbb{M}^j_1Z^n_{[1:j-2]})$.

The third term in (239) is upper-bounded as follows

$$\begin{aligned} & I(\mathbb{M}_{1j}; Z^n_{[j+1:b]} | \mathbb{M}^b_0 \mathbb{M}^{j-1}_1 U^n_{[j-1]} T^n_{[j-1:j]} Z^n_{[1:j]}) \\ & \quad \leq I(\mathbb{M}_{1j}; L_{1j} L_{2j}, \mathbb{M}_{1(j+1)} \oplus K'_j | \mathbb{M}^b_0 \mathbb{M}^{j-1}_1 U^n_{[j-1]} T^n_{[j-1:j]} Z^n_{[1:j]}) \\ & \quad \leq I(\mathbb{M}^b_0 \mathbb{M}^j_1 U^n_{[j-1]} T^n_{[j-1]} Z^n_{[1:j]}; L_{1j} L_{2j}, \mathbb{M}_{1(j+1)} \oplus K'_j | T^n_{[j]}) \\ & \quad \leq I(U^n_{[j]} Z^n_{[j]}; L_{1j} L_{2j}, \mathbb{M}_{1(j+1)} \oplus K'_j | T^n_{[j]}) \\ & \quad \leq n\eta_2, \end{aligned} \tag{241}$$

where the last inequality is bounded exactly as (231b). Thus, (239) is upper-bounded as

$$I(\mathbb{M}^b_1; Z^n_{[1:b]} | \mathbb{M}^b_0) \leq \sum_{j=2}^{b} (n\eta_4 + n\eta_2) = n(b-1)\eta_5. \tag{242}$$

Finally, the total information leakage rate is

$$I(\mathbb{M}^b_0 \mathbb{M}^b_1; Z^n_{[1:b]}) = I(\mathbb{M}^b_0; Z^n_{[1:b]}) + I(\mathbb{M}^b_1; Z^n_{[1:b]} | \mathbb{M}^b_0) \leq n(b-1)\eta_6, \tag{243}$$

which assures that the eavesdropper has no knowledge of the messages asymptotically.

5.C.6 *Sufficient Conditions (R_{KG_1})*

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

$$I(V; Z|UT) \leq I(V; Y|UT) \tag{244a}$$
$$\tilde{S}' + \tilde{S}'' = \tilde{S}_1 + \tilde{S}_2 = I(V; X\hat{Y}|UY) + \epsilon_1 + \epsilon_2 + \tilde{\epsilon}_1 + \tilde{\epsilon}_2 \tag{244b}$$
$$R_1 \leq \bar{S}_2 = I(V; Y|UT) - I(V; Z|UT) \tag{244c}$$
$$\tilde{S}'' + R_0 + R_1 + R_f < I(U; Y|Q) - \delta \tag{244d}$$
$$\tilde{S}' + \tilde{S}'' + R_0 + R_1 + R_f < I(U; Y) - \delta \tag{244e}$$
$$R_1 + R_f = I(U; Z|Q) + I(U; T|QZ) - \epsilon'. \tag{244f}$$

After applying Fourier-Motzkin elimination (FME) to this system, we obtain the bounds on the rate (145) subject to the conditions

$$I(V; Z|UT) \leq I(V; Y|UT) \tag{245a}$$
$$I(U; TZ|Q) \leq I(U; Y|Q) \tag{245b}$$
$$I(V; X\hat{Y}|UY) + I(U; TZ|Q) \leq I(U; Y). \tag{245c}$$

Nonetheless, these conditions are redundant after the maximization process. If for a certain PD, condition (245a) is not satisfied, then, R_{KG_1} with $T = V = \emptyset$ attains a higher value. Similarly, if either (245b) or (245c) does not hold for a certain PD, then, R_{KG_2} with $Q = \emptyset$ attains a higher value.

5.C.7 *Inner Bound* R_{KG_2}

This second strategy tackles the situation where the eavesdropper experiences a better channel than the legitimate receiver and can therefore decode everything sent by the encoder. In R_{KG_1}, when either the condition (245b) or (245c) is not satisfied, the rate of the unencrypted message (R_0) is negative. Therefore, in this second strategy the message is encrypted completely. The proof is similar to the one of R_{KG_1} and we only point out the differences in the sequel.

Codebook Generation

Since the eavesdropper is able to decode everything, there is no need for the codeword $q^n(\cdot)$ as a lower layer for $u^n(\cdot)$, which in turn makes the bit recombination $(l'_j, l''_j) = M_l(l_{1(j-1)}, l_{2(j-1)})$ unnecessary. Additionally, since the encoder cannot send the message without encrypting it, $R_0 = 0$ and $R_f = 0$, and the condition (222f) disappears. We therefore take the joint PD (144) with $Q = \emptyset$ and build the codebooks for each block as in Section 5.C.1 without $q^n(\cdot)$ and with $t^n(\cdot)$ superimposed over $u^n(\cdot)$. The quantities (222) are modified as follows:

$$S_1 = I(T; X\hat{Y}|U) + \epsilon_1 \tag{246a}$$

$$\tilde{S}_1 = I(T; X\hat{Y}|U) - I(T; UY|Q) + \epsilon_1 + \tilde{\epsilon}_1 \tag{246b}$$

Encoding and Decoding

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

Key and Information Leakage

The proof for the key secrecy is untouched while the one for the information leakage is simplified. Since there is no unencrypted message, i.e., $R_0 = 0$ the upper-bounding of $I(\mathbb{M}_0^b; Z_{[1:b]}^n)$ becomes trivial and the condition (222f) is no longer necessary.

Final Expression

The sufficient conditions in this second strategy for the encoder to transmit a message uniformly distributed in $[1 : 2^{nR}]$, $R = R_{KG_2}$, while concealing it from the eavesdropper are

$$I(V; Z|UT) \leq I(V; Y|UT) \tag{247a}$$

$$\tilde{S}_1 + \tilde{S}_2 = I(V; X\hat{Y}|UY) + \epsilon_1 + \epsilon_2 + \tilde{\epsilon}_1 + \tilde{\epsilon}_2 \tag{247b}$$
$$R \leq \bar{S}_2 = I(V; Y|UT) - I(V; Z|UT) \tag{247c}$$
$$\tilde{S}_1 + \tilde{S}_2 + R < I(U; Y) - \delta, \tag{247d}$$

which gives us (146) after applying FME to the system (247).

5.D PROOF OF LEMMA 5.1

Consider,

$$\begin{aligned} &I(U^n_{[1:b]}; Y^n_{[1:b]}) - I(U^n_{[1:b]}; Z^n_{[1:b]}) \\ &\quad = H(Y^n_{[1:b]}) - H(Y^n_{[1:b]}|U^n_{[1:b]}) - H(Z^n_{[1:b]}) + H(Z^n_{[1:b]}|U^n_{[1:b]}), \end{aligned} \tag{248}$$

where we bound each term independently. First,

$$\begin{aligned} H(Y^n_{[1:b]}) &= -\sum_{y^n_{[1:b]} \in \mathcal{Y}^n_{[1:b]}} p(y^n_{[1:b]}) \log p(y^n_{[1:b]}) \\ &\geq -\sum_{y^n_{[1:b]} \in T^n_\delta(Y^b)} p(y^n_{[1:b]}) \log p(y^n_{[1:b]}) \\ &\geq \sum_{y^n_{[1:b]} \in T^n_\delta(Y^b)} p(y^n_{[1:b]}) n[H(Y^b) - b\eta_2] && \text{(249a)} \\ &\geq (1-\eta_1) n[H(Y^b) - b\eta_2] && \text{(249b)} \\ &\geq n[H(Y^b) - b\eta_3], && \text{(249c)} \end{aligned}$$

where (249a) and (249b) follow from Lemma A.3 and A.1, respectively; and where in (249c) $\eta_3 \geq \eta_2 - \eta_1[H(Y^b)/b - \eta_2]$. Second,

$$\begin{aligned} H(Y^n_{[1:b]}|U^n_{[1:b]}) &= \sum_{i=1}^n H(Y_{i[1:b]}|U^n_{[1:b]} Y^{i-1}_{[1:b]}) \\ &\leq \sum_{i=1}^n H(Y_{i[1:b]}|U_{i[1:b]}) && \text{(250a)} \\ &= nH(Y^b|U^b), && \text{(250b)} \end{aligned}$$

where (250a) is due to the fact that conditioning reduces the entropy; and (250b) stems from the variables being identically distributed, see (211). Similarly,

$$\begin{aligned} H(Z^n_{[1:b]}) &= \sum_{i=1}^n H(Z_{i[1:b]}|Z^{i-1}_{[1:b]}) \\ &\leq \sum_{i=1}^n H(Z_{i[1:b]}) \\ &= nH(Z^b). && \text{(251)} \end{aligned}$$

And finally,

$$\begin{aligned} H(Z^n_{[1:b]}|U^n_{[1:b]}) &= -\sum_{(u^n_{[1:b]}z^n_{[1:b]})\in\mathcal{U}^n_{[1:b]}\times\mathcal{Z}^n_{[1:b]}} p(u^n_{[1:b]}z^n_{[1:b]})\log p(z^n_{[1:b]}|u^n_{[1:b]}) \\ &\geq -\sum_{(u^n_{[1:b]}z^n_{[1:b]})\in T^n_\delta(U^bZ^b)} p(u^n_{[1:b]}z^n_{[1:b]})\log p(z^n_{[1:b]}|u^n_{[1:b]}) \\ &\geq (1-\eta_4)n[H(Z^b|U^b)-b\eta_5] \\ &\geq n[H(Z^b|U^b)-b\eta_6], \end{aligned} \tag{252}$$

where the steps are analogous to those of (249a)–(249c). Putting (248)–(252) together we obtain (214):

$$I(U^n_{[1:b]};Y^n_{[1:b]}) - I(U^n_{[1:b]};Z^n_{[1:b]}) \geq n\Big[I(U^b;Y^b) - I(U^b;Z^b) - b\eta\Big].$$

5.E PROOF OF LEMMA 5.2

To analyze $H(U^n_{[1:b]}|\mathbb{M}L^b_2Z^n_{[1:b]})$ we resort to Fano's inequality. Let $g(\cdot)$ be the decoder function at the eavesdropper and $\hat{U}^n_{[1:b]} = g(Z^n_{[1:b]})$ the estimated codewords, then $P^{(n)}_{e,Z} = \Pr\Big\{\hat{U}^n_{[1:b]} \neq U^n_{[1:b]}\Big\}$. Conditioned on the message $\mathbb{M}$ and the bin indices L^b_2, the uncertainty in the codewords $U^n_{[1:b]}$ is given by the position inside the bins, that we denote S^b. Since each $S_j \in [1 : 2^{n\bar{R}_j}]$, we bound the conditional entropy as follows,

$$H(U^n_{[1:b]}|\mathbb{M}L^b_2Z^n_{[1:b]}) \leq 1 + P^{(n)}_{e,Z}\sum_{j=1}^{b} n\bar{R}_j \leq bn\epsilon_n, \tag{253}$$

where ϵ_n denotes a sequence such that $\epsilon_n \to 0$ as $n \to \infty$. The second inequality is true as long as $P^{(n)}_{e,Z} \to 0$ as $n \to \infty$, and we prove this in the sequel.

For ease of notation and until the end of the proof, we define $U^n_{[1:b]}(s^b)$ as the set of codewords indexed by the true indices $(\mathbb{M}, L^b_2)$. Then, the eavesdropper makes an error in any of the following events:

$$\begin{aligned} \mathcal{E}_{1,Z} &= \Big\{\Big(U^n_{[1:b]}(S^b), Z^n_{[1:b]}\Big) \notin T^n_\delta(U^bZ^b)\Big\}, \\ \mathcal{E}_{2,Z} &= \Big\{\Big(U^n_{[1:b]}(s^b), Z^n_{[1:b]}\Big) \in T^n_\delta(U^bZ^b) \text{ for some } s^b \neq S^b\Big\}. \end{aligned}$$

And we can bound its probability of error as

$$P^{(n)}_{e,Z} \leq \Pr\{\mathcal{E}_{1,Z}\} + \Pr\{\mathcal{E}_{2,Z}\}. \tag{254}$$

By the law of large numbers, the first term tends to zero as $n \to \infty$. On the other hand, given the codebook generation of Section 5.A.1,

i.e., for any $j \in [1:b]$ the codewords U_j^b are superimposed over U^{j-1}, the second term in the r.h.s. of (254) can be made arbitrarily small if,

$$\sum_{j=t}^{b} \bar{R}_j \leq I(U_j^b; Z^b | U^{j-1}),\ \forall t \in [1:b]. \tag{255}$$

Since this is verified by the definition of $\bar{R}_j$ (209), then, we are able to bound $P_{e,Z}^{(n)}$ and thus, the uncertainty over $U_{[1:b]}^n$ in (253).

5.F PROOF OF LEMMA 5.5

Let us define the event

$$\mathcal{E}(V^n(\underline{r}, s_1, s_2)) = \big\{(V^n(\underline{r}, s_1, s_2), T^n(l', s_1), Q^n(l'), U^n(\underline{r}), Z^n) \in T_\delta^n(VTQUZ)\big\}, \tag{256}$$

whose probability can be bounded as,

$$p_{\mathcal{E}_1} = 2^{-n[I(V;Z|UT)+\delta']} \leq \Pr\{\mathcal{E}(V^n(\underline{r}, s_1, s_2))\} \leq 2^{-n[I(V;Z|UT)-\delta]} = p_{\mathcal{E}_2}. \tag{257}$$

The probability $\Pr\{L_2 = l | U^n T^n Z^n\}$ is the probability of finding at least one jointly typical sequence in the bin l, i.e.,

$$\Pr\{L_2 = l | U^n T^n Z^n\} = \frac{1}{\beta} \Pr\left\{ \bigcup_{V^n(\underline{r}, s_1, s_2) \in B_2(s_1, l)} \mathcal{E}(V^n(\underline{r}, s_1, s_2)) \right\}, \tag{258}$$

where $\beta = \Pr\Big\{\bigcup_{V^n(\underline{r}, s_1, s_2)} \mathcal{E}(V^n(\underline{r}, s_1, s_2))\Big\}$.

With a little abuse of notation, let us define the set of sequences $V^n(\underline{r}, s_1, s_2) \in B_2(s_1, l)$ as $\{V^n(1), \ldots, V^n(2^{n(S_2 - \tilde{S}_2)})\}$, and rename the event (256) as $\mathcal{E}(V^n(k))$ with $k \in [1 : 2^{n(S_2 - \tilde{S}_2)}]$. Then, the probability (258) can be written as follows,

$$\Pr\{L_2 = l | U^n T^n Z^n\} = \frac{1}{\beta} \sum_{k=1}^{2^{n(S_2 - \tilde{S}_2)}} \Pr\{\mathcal{E}(V^n(k))\} \prod_{k'=1}^{k-1} \Big(1 - \Pr\big\{\mathcal{E}(V^n(k'))\big\}\Big).$$

Using the lower and upper bounds (257), we can bound the probability as follows,

$$\begin{aligned} \Pr\{L_2 = l | U^n T^n Z^n\} &\geq \frac{1}{\beta} \sum_{k=1}^{2^{n(S_2 - \tilde{S}_2)}} p_{\mathcal{E}_1} (1 - p_{\mathcal{E}_2})^{k-1} \\ &= \frac{p_{\mathcal{E}_1} / p_{\mathcal{E}_2}}{\beta} [1 - (1 - p_{\mathcal{E}_2})^{2^{n(S_2 - \tilde{S}_2)}}], \end{aligned} \tag{259}$$

$$\begin{aligned} \Pr\{L_2 = l | U^n T^n Z^n\} &\leq \frac{1}{\beta} \sum_{k=1}^{2^{n(S_2 - \tilde{S}_2)}} p_{\mathcal{E}_2} (1 - p_{\mathcal{E}_1})^{k-1} \\ &= \frac{p_{\mathcal{E}_2} / p_{\mathcal{E}_1}}{\beta} [1 - (1 - p_{\mathcal{E}_1})^{2^{n(S_2 - \tilde{S}_2)}}]. \end{aligned} \tag{260}$$

If $-\log p_{\mathcal{E}_2} < n(S_2 - \tilde{S}_2)$, i.e., $I(V;Z|UT) - \delta < I(V;Y|UT) - \tilde{\epsilon}$, the terms in brackets in (259) and (260) tend to 1 as $n \to \infty$, thus,

$$\frac{p_{\mathcal{E}_1}/p_{\mathcal{E}_2}}{\beta} \leq \Pr\{L_2 = l|U^n T^n Z^n\} \leq \frac{p_{\mathcal{E}_2}/p_{\mathcal{E}_1}}{\beta}.$$

If $\delta + \delta' = \eta/2$, $p_{\mathcal{E}_1}/p_{\mathcal{E}_2} = 2^{-n\eta/2}$ and we recover (234).

Part III

CONCLUSIONS AND APPENDICES

6

CONCLUSIONS AND PERSPECTIVES

In this chapter, we revisit the motivation behind our work and the contributions we made. We then present some perspective about possible future work.

6.1 GENERAL COMMENTS & CONCLUSIONS

In this thesis, we investigated two relevant aspects of future wireless networks, namely interference mitigation through user cooperation and secure transmission through physical layer security. To that end, we conducted an information theoretical study of two basic models: the interference relay channel (IRC) and the wiretap channel with generalized feedback (WCGF).

Interference Relay Channel

In the first part of the thesis, we investigated a class of IRCs where the relay can only observe one of the sources and, additionally, the channel outputs are injective semideterministic functions of the channel inputs. For this particular model, we derived a novel outer bound that is a nontrivial extension of Telatar and Tse's outer bound for the interference channel (IC). The most relevant contribution here is the modelization of the interference signals, a key step in order to obtain an outer bound in single-letter form. Furthermore, we presented two inner bounds, which combine the (partial) decode-and-forward (DF) and compress-and-forward (CF) relaying strategies with the scheme of Han and Kobayashi for the IC to deal with interference. These schemes were fairly novel by themselves, e.g., the introduction of *partial* DF and the use of different decoding strategies in CF, but the main contribution here is the development of inner bounds that resemble the outer bound. These bounds allowed us to characterize within a constant gap the capacity region of the Gaussian class of IRCs studied. Moreover, we determined a regime in the SNR of the source-to-relay link which gives a bounded increase in achievable rates independently of any other channel parameter. This last result

is of paramount importance when the time comes to plan the infrastructure of next-generation cellular networks.

We have to account also for some shortcomings in our analysis in this first part of the thesis. The main premise was to extend Telatar and Tse's work to the IRC in order to characterize its capacity region within a constant gap. In a general setting, where the relay observes both sources, this proved to be particularly challenging. The addition of the relay's input correlates the interference signals present in the injective semideterministic model, which is not the case in the injective semideterministic IC (IS-IC). The resulting outer bound in this general scenario was cumbersome, which prevented us from gaining any insight into the problem. By eliminating the link between one of the sources and the relay, a solution found in the literature, we could substantially simplify the outer bound and later compare it to the inner bounds. Nonetheless, even though the model is now simpler, the outer bound is still composed of 20 different bounds; in contrast, Telatar and Tse's outer bound only has 7. Indeed, this issue reveals the complexity of dealing simultaneously with relaying and interference, both of them open problems by themselves.

Wiretap Channel with Generalized Feedback

The second part of the thesis focused on understanding the benefit and the way of employing feedback in physical layer security, through the analysis of the WCGF. For this purpose, we derived two different inner bounds based on the two different approaches found in the literature. The first of these methods, though not the most popular one, takes advantage of the feedback signal to create codebooks that "align" the codeword to be sent in a way that is detrimental to the eavesdropper's decoding. Our first inner bound was based on this approach and the use of joint source-channel coding (JSCC). On the other hand, the second method employs the feedback signal as a source of common randomness between the legitimate users, with which they agree on a secret key. Based on this approach, we developed a second inner bound and, as a side result, we obtained an inner bound on secret key agreement for the same channel model. Both inner bounds successfully recovered previous results found in the literature for specific channel and feedback models. However, neither of them appears to be more general than the other because each scheme failed to recover all the results taken into consideration. Based on these findings we believe that both approaches are complementary and a unified inner bound would be more general. Nonetheless, we cannot prove this conjecture without actually deriving the unified scheme.

Once more, there were a few downsides in our work in the second part of the thesis, of which we address two in the sequel. First of

all, the complexity of the multi-letter expression in the JSCC scheme made any insight rather difficult to obtain. As a matter of fact, the maximizing probability distribution (PD) could only be found in two examples due to similarities between the schemes. We thus resorted to a simplified version of the JSCC inner bound, i.e., Corollary 5.1, that helped us gain some perspective on the problem but failed to obtain any relevant capacity result. The derivation of the KG inner bound was a response to this issue. Second, the proposed achievable schemes were shown to fulfill the *weak secrecy* condition, i.e., $I(\mathbb{M}_n; Z^n) \leq n\epsilon_n$, rather than the *strong secrecy* one, i.e., $I(\mathbb{M}_n; Z^n) \leq \epsilon_n$. Therefore, one of the previous results in the literature, which was developed considering strong secrecy, is not actually included as a special case of our schemes. A different proof, e.g., based on channel resolvability [11], should be carried out to properly include the aforementioned result.

6.2 DISCUSSION & FUTURE WORK

A Ph.D. thesis is carried out during a finite period of time and, as in any work with a time constraint, several possible research paths remain unexplored. We shall address some of them in this section.

Interference Relay Channel

The most challenging and compelling extension to this work is the generalization of the injective semideterministic IRC (IS-IRC) to the case where the relay observes the two sources. In this general IRC, the relay's channel input is correlated to the channel inputs of both sources, i.e., $p(x_1x_2x_3) = p(x_1)p(x_2)p(x_3|x_1x_2)$. Therefore, X_3 becomes simultaneously desired signal and interference for each decoder, and the model in Fig. 13 is no valid anymore. Most importantly, the interference signal S_k is no longer independent of the input X_j, i.e., $p(s_1s_2|x_1x_2x_3) = p(s_1|x_1x_3)p(s_2|x_2x_3)$, cf., (62). We show next how this issue prevents us from single-letterizing the outer bound the way we did.

Consider the following derivation of the outer bound for the *general* model just described, cf., (78b).

$$\begin{aligned} n(R_1 - \epsilon_n) &\leq I(X_1^n; Y_1^n) \\ &\leq I(X_1^n X_3^n; Y_1^n) \\ &= H(Y_1^n) - H(Y_1^n|X_1^n X_3^n) \\ &= H(Y_1^n) - \boxed{H(S_2^n|X_1^n X_3^n)}, \end{aligned} \tag{261}$$

where in (261) we take into account the IS-IRC model. Also consider the following, cf., (82b),

$$
\begin{aligned}
n(R_2 - \epsilon_n) &\leq I(X_2^n; Y_2^n) \\
&\leq I(X_2^n; Y_2^n | X_1^n) \\
&\leq I(X_2^n X_3^n; Y_2^n V_2^n | X_1^n) \\
&= I(X_2^n X_3^n; V_2^n | X_1^n) + I(X_2^n X_3^n; Y_2^n | X_1^n V_2^n) \\
&= H(V_2^n | X_1^n) - H(V_2^n | X_2^n X_3^n) + I(X_2^n X_3^n; Y_2^n | X_1^n V_2^n) \qquad \text{(262a)} \\
&= \boxed{H(S_2^n | X_1^n)} - H(Y_1^n | X_1^n X_2^n X_3^n) + I(X_2^n X_3^n; Y_2^n | V_2^n X_1^n), \qquad \text{(262b)}
\end{aligned}
$$

where in (262a) we use the Markov chain $X_1^n \multimap (X_2^n X_3^n) \multimap V_2^n$; and in (262b) we take into account the IS-IRC model, i.e., $H(Y_1^n | X_1^n X_2^n X_3^n) = H(S_2^n | X_1^n X_2^n X_3^n) = H(S_2^n | X_2^n X_3^n) = H(V_2^n | X_2^n X_3^n)$. We see here that the boxed terms in (261) and (262b) are not equal, consequently, the sum of these two multi-letter single rates does not give a single-letter sum-rate. A new technique to derive outer bounds for the general model is therefore needed.

Another interesting future work is the development of better inner bounds for the IRC. Both DF and CF achieve capacity within half a bit for the Gaussian relay channel (RC), while the Han-Kobayashi scheme achieves capacity within half a bit per dimension of the Gaussian IC, independent of any channel parameter. However, our results show that each proposed relaying strategy achieves the capacity region of the Gaussian IRC within a constant gap only in specific SNR regimes. Additionally, the gap is larger than the sum of the gaps for the RC and IC. Whether there exists a single coding scheme that achieves the constant gap in all SNR regimes is still an open question. This could be a shortcoming of the outer bound, the inner bounds, or the maximization carried out in them.

There are also some attractive problems related to this model, for example, the IRC with state, i.e., $p(y_1 y_2 y_3 | x_1 x_2 x_3 s) p(s)$. We could consider the situation where the state is only known at the relay, or even, the state is the only observation the relay has from the channel. This model would give useful insight into the particular scenario where the purpose of the relay is not to forward the messages from the base stations (BSs) but rather help the users cope with an external interference to the cellular system. In another interesting model, the relay receives feedback from the destinations. The relay could use this information jointly with its own channel observation to improve its decoding capabilities and, hence, the overall achievable rates. This model is attractive for future generation cellular networks, where users might belong simultaneously to macro and femto cells, and their feedback is restricted to the small cell in order to save energy and avoid interference.

Wiretap Channel with Generalized Feedback

Two possible extensions to the second part of the thesis are the development of a unified inner bound that recovers all the previous results from the literature, and the use of strong secrecy. However, achieving these two goals together might be a colossal task given the complexity each one of them separately has.

A more compelling future work, however, is to provide an outer bound for the WCGF. All our capacity results were based on outer bounds found in the literature, thus we did not develop one of our own. We are currently looking into new channel models for which one of our schemes might achieve capacity, hence a new outer bound is necessary. It is unlikely that this new outer bound will be tight in the general case, but it might be under some particular conditions. The key agreement problem should also be studied for additional channel models, for which we will need to derive specific outer bounds.

Given the similarities between the source encoder with feedback and the relay's encoding functions, another interesting topic of study is the relation between our work and the wiretap channel (WTC) with a relay, e.g., [73]. Moreover, in an effort to fully unify the work in the two parts of this thesis, the IRC with secrecy constraints is worth investigating, e.g., see [74] for secrecy in the IC. The complexity of this last problem is such that a whole Ph.D. could be devoted to it.

A

STRONGLY TYPICAL SEQUENCES AND DELTA-CONVENTION

Following [75], we use in this paper *strongly typical sets* and the so-called *Delta-Convention*. Some useful facts are recalled here. Let X and Y be random variables on some finite sets $\mathcal{X}$ and $\mathcal{Y}$, respectively. We denote by $p_{X,Y}$ (resp. $p_{Y|X}$, and p_X) the joint probability distribution of (X,Y) (resp. conditional distribution of Y given X, and marginal distribution of X).

Definition A.1 (Number of occurrences)**.** *For any sequence $x^n \in \mathcal{X}^n$ and any symbol $a \in \mathcal{X}$, notation $N(a|x^n)$ stands for the number of occurrences of a in x^n.*

Definition A.2 (Typical seq.)**.** *A sequence $x^n \in \mathcal{X}^n$ is called* (strongly) δ-typical *w.r.t. X (or simply* typical *if the context is clear) if*

$$\left|\frac{1}{n}N(a|x^n) - p_X(a)\right| \leq \delta \text{ for each } a \in \mathcal{X} ,$$

and $N(a|x^n) = 0$ for each $a \in \mathcal{X}$ such that $p_X(a) = 0$. The set of all such sequences is denoted by $T^n_\delta(X)$.

Definition A.3 (Conditionally typical sequence)**.** *Let $x^n \in \mathcal{X}^n$. A sequence $y^n \in \mathcal{Y}^n$ is called* (strongly) δ-typical (w.r.t. Y) given x^n *if for each $a \in \mathcal{X}$, $b \in \mathcal{Y}$*

$$\left|\frac{1}{n}N(a,b|x^n,y^n) - \frac{1}{n}N(a|x^n)p_{Y|X}(b|a)\right| \leq \delta,$$

and, $N(a,b|x^n,y^n) = 0$ for each $a \in \mathcal{X}$, $b \in \mathcal{Y}$ such that $p_{Y|X}(b|a) = 0$. The set of all such sequences is denoted by $T^n_\delta(Y|x^n)$.

Delta-Convention [75]. *For any sets $\mathcal{X}$, $\mathcal{Y}$, $\exists$ a sequence $\{\delta_n\}_{n\in\mathbb{N}^*}$ such that the lemmas stated below hold.*[1] *From now on, typical sequences are understood with $\delta = \delta_n$. Typical sets are still denoted by $T^n_\delta(\cdot)$.*

1 As a matter of fact, $\delta_n \to 0$ and $\sqrt{n}\,\delta_n \to \infty$ as $n \to \infty$.

Lemma A.1 ([75, Lemma 1.2.12]). *There exists a sequence* $\eta_n \xrightarrow[n\to\infty]{} 0$ *such that*

$$p_X(T_\delta^n(X)) \geq 1 - \eta_n \, .$$

Lemma A.2 ([75, Lemma 1.2.13]). *There exists a sequence* $\eta_n \xrightarrow[n\to\infty]{} 0$ *such that, for each* $x^n \in T_\delta^n(X)$,

$$\left| \frac{1}{n} \log \| T_\delta^n(X) \| - H(X) \right| \leq \eta_n \, ,$$
$$\left| \frac{1}{n} \log \| T_\delta^n(Y|x^n) \| - H(Y|X) \right| \leq \eta_n \, .$$

Lemma A.3 (Asymptotic equipartition property). *There exists a sequence* $\eta_n \xrightarrow[n\to\infty]{} 0$ *such that, for each* $x^n \in T_\delta^n(X)$ *and each* $y^n \in T_\delta^n(Y|x^n)$,

$$\left| -\frac{1}{n} \log p_X(x^n) - H(X) \right| \leq \eta_n \, ,$$
$$\left| -\frac{1}{n} \log p_{Y|X}(y^n|x^n) - H(Y|X) \right| \leq \eta_n \, .$$

Lemma A.4 (Joint typicality lemma [1]). *For each* $x^n \in T_\delta^n(X)$, *there exists a sequence* $\eta_n \xrightarrow[n\to\infty]{} 0$ *such that*

$$\left| -\frac{1}{n} \log p_Y(T_\delta^n(Y|x^n)) - I(X;Y) \right| \leq \eta_n .$$

Proof.

$$\begin{aligned} p_Y(T_\delta^n(Y|x^n)) &= \sum_{y^n \in T_\delta^n(Y|x^n)} p_Y(y^n) \\ &\overset{(a)}{\leq} \| T_\delta^n(Y|x^n) \| \, 2^{-n[H(Y)-\alpha_n]} \\ &\overset{(b)}{\leq} 2^{n[H(Y|X)+\beta_n]} \, 2^{-n[H(Y)-\alpha_n]} \\ &= 2^{-n[I(X;Y)-\beta_n-\alpha_n]} \, , \end{aligned}$$

where

- step (a) follows from $T_\delta^n(Y|x^n) \subset T_\delta^n(Y)$ and Lemma A.3, for some sequence $\alpha_n \xrightarrow[n\to\infty]{} 0$,
- step (b) from Lemma A.2, for some sequence $\beta_n \xrightarrow[n\to\infty]{} 0$.

The reverse inequality $p_Y(T_\delta^n(Y|x^n)) \geq 2^{-n[I(X;Y)+\beta_n+\alpha_n]}$ can be proved following similar argument. □

BIBLIOGRAPHY

[1] A. El Gamal and Y.-H. Kim, *Network Information Theory*. Cambridge University Press, 2011.

[2] C. Kosta, B. Hunt, A. U. Quddus, and R. Tafazolli, "On Interference Avoidance Through Inter-Cell Interference Coordination (ICIC) Based on OFDMA Mobile Systems," *IEEE Communications Surveys and Tutorials*, vol. 15, no. 3, pp. 973–995, 2013.

[3] R. Bassily, E. Ekrem, X. He, E. Tekin, J. Xie, M. Bloch, S. Ulukus, and A. Yener, "Cooperative Security at the Physical Layer: A Summary of Recent Advances," *IEEE Signal Processing Magazine*, vol. 30, no. 5, pp. 16–28, 2013.

[4] G. Bassi, P. Piantanida, and S. Yang, "Capacity to Within a Constant Gap for a Class of Interference Relay Channels," in *Proc. 51st Annual Allerton Conf. Commun., Control, Comput.*, Oct. 2013, pp. 1300–1306.

[5] E. Telatar and D. Tse, "Bounds on the Capacity Region of a Class of Interference Channels," in *Information Theory (ISIT), 2007 IEEE International Symposium on*, Jun. 2007, pp. 2871–2874.

[6] X. Wu and L.-L. Xie, "On the Optimal Compressions in the Compress-and-Forward Relay Schemes," *IEEE Transactions on Information Theory*, vol. 59, no. 5, pp. 2613–2628, May 2013.

[7] A. Behboodi and P. Piantanida, "Mixed Noisy Network Coding and Cooperative Unicasting in Wireless Networks," *IEEE Transactions on Information Theory*, vol. 61, no. 1, pp. 189–222, Jan. 2015.

[8] I. Csiszár and P. Narayan, "Common Randomness and Secret Key Generation with a Helper," *IEEE Transactions on Information Theory*, vol. 46, no. 2, pp. 344–366, Mar. 2000.

[9] R. Ahlswede and N. Cai, "Transmission, Identification and Common Randomness Capacities for Wire-Tape Channels with Secure Feedback from the Decoder," in *General Theory of Information Transfer and Combinatorics*. Springer Berlin Heidelberg, 2006, vol. 4123, pp. 258–275.

[10] D. Gündüz, D. R. Brown, and H. V. Poor, "Secret Communication with Feedback," in *Information Theory and Its Applications, 2008. ISITA 2008. International Symposium on*, Dec. 2008, pp. 1–6.

[11] M. R. Bloch and J. N. Laneman, "Strong Secrecy From Channel Resolvability," *IEEE Transactions on Information Theory*, vol. 59, no. 12, pp. 8077–8098, Dec. 2013.

[12] E. C. Van Der Meulen, "Three-terminal Communication Channels," *Advances in Applied Probability*, vol. 3, no. 1, pp. 120–154, 1971.

[13] T. M. Cover and A. El Gamal, "Capacity Theorems for the Relay Channel," *IEEE Transactions on Information Theory*, vol. 25, no. 5, pp. 572–584, Sep. 1979.

[14] R. Ahlswede, "The Capacity Region of a Channel with Two Senders and Two Receivers," *The Annals of Probability*, vol. 2, no. 5, pp. 805–814, Oct. 1974.

[15] T. S. Han and K. Kobayashi, "A New Achievable Rate Region for the Interference Channel," *IEEE Transactions on Information Theory*, vol. 27, no. 1, pp. 49–60, Jan. 1981.

[16] H. Sato, "On the Capacity Region of a Discrete Two-User Channel for Strong Interference (Corresp.)," *IEEE Transactions on Information Theory*, vol. 24, no. 3, pp. 377–379, May 1978.

[17] M. H. M. Costa and A. A. El Gamal, "The Capacity Region of the Discrete Memoryless Interference Channel with Strong Interference (Corresp.)," *IEEE Transactions on Information Theory*, vol. 33, no. 5, pp. 710–711, Sep. 1987.

[18] A. B. Carleial, "Interference Channels," *IEEE Transactions on Information Theory*, vol. 24, no. 1, pp. 60–70, Jan. 1978.

[19] R. H. Etkin, D. Tse, and H. Wang, "Gaussian Interference Channel Capacity to Within One Bit," *IEEE Transactions on Information Theory*, vol. 54, no. 12, pp. 5534–5562, Dec. 2008.

[20] O. Sahin and E. Erkip, "Achievable Rates for the Gaussian Interference Relay Channel," in *IEEE Global Telecommunications Conference, 2007. GLOBECOM '07*, Nov. 2007, pp. 1627–1631.

[21] C. E. Shannon, "Communication Theory of Secrecy Systems," *Bell System Technical Journal*, vol. 28, no. 4, pp. 656–715, 1949.

[22] A. D. Wyner, "The Wire-Tap Channel," *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, 1975.

[23] I. Csiszár and J. Körner, "Broadcast Channels with Confidential Messages," *IEEE Transactions on Information Theory*, vol. 24, no. 3, pp. 339–348, May 1978.

[24] G. Kramer, M. Gastpar, and P. Gupta, "Cooperative Strategies and Capacity Theorems for Relay Networks," *IEEE Transactions on Information Theory*, vol. 51, no. 9, pp. 3037–3063, Sep. 2005.

[25] A. Avestimehr, S. Diggavi, and D. Tse, "Wireless Network Information Flow: A Deterministic Approach," *IEEE Transactions on Information Theory*, vol. 57, no. 4, pp. 1872–1905, Apr. 2011.

[26] W. Chang, S.-Y. Chung, and Y. H. Lee, "Gaussian Relay Channel Capacity to Within a Fixed Number of Bits," *arXiv:1011.5065 [cs, math]*, Nov. 2010. [Online]. Available: http://arxiv.org/abs/1011.5065

[27] S. H. Lim, Y.-H. Kim, A. El Gamal, and S.-Y. Chung, "Noisy Network Coding," *IEEE Transactions on Information Theory*, vol. 57, no. 5, pp. 3132–3152, May 2011.

[28] Y. Tian and A. Yener, "The Gaussian Interference Relay Channel: Improved Achievable Rates and Sum Rate Upperbounds Using a Potent Relay," *IEEE Transactions on Information Theory*, vol. 57, no. 5, pp. 2865–2879, May 2011.

[29] A. Chaaban and A. Sezgin, "On the Generalized Degrees of Freedom of the Gaussian Interference Relay Channel," *IEEE Transactions on Information Theory*, vol. 58, no. 7, pp. 4432–4461, Jul. 2012.

[30] B. Kang, S.-H. Lee, S.-Y. Chung, and C. Suh, "A New Achievable Scheme for Interference Relay Channels," in *Information Theory (ISIT), 2013 IEEE International Symposium on*, Jul. 2013, pp. 2419–2423.

[31] I. Marić, R. Dabora, and A. J. Goldsmith, "Relaying in the Presence of Interference: Achievable Rates, Interference Forwarding, and Outer Bounds," *IEEE Transactions on Information Theory*, vol. 58, no. 7, pp. 4342–4354, Jul. 2012.

[32] O. Sahin and E. Erkip, "On Achievable Rates for Interference Relay Channel with Interference Cancelation," in *Conference Record of the Forty-First Asilomar Conference on Signals, Systems and Computers, 2007. ACSSC 2007*, Nov. 2007, pp. 805–809.

[33] S. Rini, D. Tuninetti, and N. Devroye, "Outer Bounds for the Interference Channel with a Cognitive Relay," in *2010 IEEE Information Theory Workshop (ITW)*, Aug. 2010, pp. 1–5.

[34] O. Sahin, O. Simeone, and E. Erkip, "Interference Channel With an Out-of-Band Relay," *IEEE Transactions on Information Theory*, vol. 57, no. 5, pp. 2746–2764, May 2011.

[35] Y. Tian and A. Yener, "Symmetric Capacity of the Gaussian Interference Channel With an Out-of-Band Relay to Within 1.15

Bits," *IEEE Transactions on Information Theory*, vol. 58, no. 8, pp. 5151–5171, Aug. 2012.

[36] P. Razaghi, S.-N. Hong, L. Zhou, W. Yu, and G. Caire, "Two Birds and One Stone: Gaussian Interference Channel With a Shared Out-of-Band Relay of Limited Rate," *IEEE Transactions on Information Theory*, vol. 59, no. 7, pp. 4192–4212, Jul. 2013.

[37] L. Zhou and W. Yu, "Incremental Relaying for the Gaussian Interference Channel With a Degraded Broadcasting Relay," *IEEE Transactions on Information Theory*, vol. 59, no. 5, pp. 2794–2815, May 2013.

[38] O. Simeone, E. Erkip, and S. Shamai, "On Codebook Information for Interference Relay Channels With Out-of-Band Relaying," *IEEE Transactions on Information Theory*, vol. 57, no. 5, pp. 2880–2888, May 2011.

[39] A. Høst-Madsen, "Capacity Bounds for Cooperative Diversity," *IEEE Transactions on Information Theory*, vol. 52, no. 4, pp. 1522–1544, Apr. 2006.

[40] V. M. Prabhakaran and P. Viswanath, "Interference Channels With Source Cooperation," *IEEE Transactions on Information Theory*, vol. 57, no. 1, pp. 156–186, Jan. 2011.

[41] ——, "Interference Channels With Destination Cooperation," *IEEE Transactions on Information Theory*, vol. 57, no. 1, pp. 187–209, Jan. 2011.

[42] I.-H. Wang and D. Tse, "Interference Mitigation Through Limited Transmitter Cooperation," *IEEE Transactions on Information Theory*, vol. 57, no. 5, pp. 2941–2965, May 2011.

[43] ——, "Interference Mitigation Through Limited Receiver Cooperation," *IEEE Transactions on Information Theory*, vol. 57, no. 5, pp. 2913–2940, May 2011.

[44] I. Marić, R. D. Yates, and G. Kramer, "Capacity of Interference Channels With Partial Transmitter Cooperation," *IEEE Transactions on Information Theory*, vol. 53, no. 10, pp. 3536–3548, Oct. 2007.

[45] M. Cardone, D. Tuninetti, R. Knopp, and U. Salim, "New Outer Bounds for the Interference Channel with Unilateral Source Cooperation," in *Information Theory (ISIT), 2014 IEEE International Symposium on*, Jun. 2014, pp. 1426–1430.

[46] V. S. Annapureddy and V. V. Veeravalli, "Gaussian Interference Networks: Sum Capacity in the Low-Interference Regime and New Outer Bounds on the Capacity Region," *IEEE Transactions on Information Theory*, vol. 55, no. 7, pp. 3032–3050, Jul. 2009.

[47] G. Kramer, "Outer Bounds on the Capacity of Gaussian Interference Channels," *IEEE Transactions on Information Theory*, vol. 50, no. 3, pp. 581–586, Mar. 2004.

[48] H.-F. Chong, M. Motani, and H. K. Garg, "A Comparison of Two Achievable Rate Regions for the Interference Channel," in *UCSD-ITA*, Feb. 2006. [Online]. Available: http://ita.ucsd.edu/workshop/06/talks/papers/276.pdf

[49] H.-F. Chong, M. Motani, H. K. Garg, and H. El Gamal, "On The Han-Kobayashi Region for the Interference Channel," *IEEE Transactions on Information Theory*, vol. 54, no. 7, pp. 3188–3195, Jul. 2008.

[50] G. Bassi, P. Piantanida, and S. Yang, "Constant-Gap Results and Cooperative Strategies for a Class of Interference Relay Channels," in *Information Theory (ISIT), 2014 IEEE International Symposium on*, Jun. 2014, pp. 1421–1425.

[51] Y. Liang, H. V. Poor, and S. S. (Shitz), *Information Theoretic Security*, ser. Foundations and Trends in Communications and Information Theory. Hanover, MA, USA: Now Publishers Inc., 2008, vol. 5, no. 4–5.

[52] S. Yang, M. Kobayashi, P. Piantanida, and S. Shamai, "Secrecy Degrees of Freedom of MIMO Broadcast Channels With Delayed CSIT," *IEEE Transactions on Information Theory*, vol. 59, no. 9, pp. 5244–5256, Sep. 2013.

[53] R. Tandon, P. Piantanida, and S. Shamai, "On Multi-User MISO Wiretap Channels with Delayed CSIT," in *Information Theory (ISIT), 2014 IEEE International Symposium on*, June 2014, pp. 211–215.

[54] G. Dueck, "Partial Feedback for Two-Way and Broadcast Channels," *Problems of Information and Control*, vol. 46, no. 1, pp. 1–15, 1980.

[55] T. Cover and C. Leung, "An Achievable Rate Region for the Multiple-Access Channel with Feedback," *IEEE Transactions on Information Theory*, vol. 27, no. 3, pp. 292–298, May 1981.

[56] J. Schalkwijk and T. Kailath, "A Coding Scheme for Additive Noise Channels with Feedback – Part I: No Bandwidth Constraint," *IEEE Transactions on Information Theory*, vol. 12, no. 2, pp. 172–182, Apr. 1966.

[57] B. Dai, A. H. Vinck, Y. Luo, and Z. Zhuang, "Capacity Region of Non-degraded Wiretap Channel with Noiseless Feedback," in *Information Theory (ISIT), 2012 IEEE International Symposium on*, Jul. 2012, pp. 244–248.

[58] E. Ardestanizadeh, M. Franceschetti, T. Javidi, and Y.-H. Kim, "Wiretap Channel With Secure Rate-Limited Feedback," *IEEE Transactions on Information Theory*, vol. 55, no. 12, pp. 5353–5361, Dec. 2009.

[59] Y.-K. Chia and A. El Gamal, "Wiretap Channel With Causal State Information," *IEEE Transactions on Information Theory*, vol. 58, no. 5, pp. 2838–2849, May 2012.

[60] L. Czap, V. M. Prabhakaran, C. Fragouli, and S. N. Diggavi, "Secret Communication over Broadcast Erasure Channels with State-Feedback," 2014. [Online]. Available: http://arxiv.org/abs/1408.1800

[61] R. Ahlswede and I. Csiszár, "Common Randomness in Information Theory and Cryptography—Part I: Secret Sharing," *IEEE Transactions on Information Theory*, vol. 39, no. 4, pp. 1121–1132, Jul. 1993.

[62] U. M. Maurer, "Secret Key Agreement by Public Discussion from Common Information," *IEEE Transactions on Information Theory*, vol. 39, no. 3, pp. 733–742, May 1993.

[63] A. Khisti, S. N. Diggavi, and G. W. Wornell, "Secret-Key Generation Using Correlated Sources and Channels," *IEEE Transactions on Information Theory*, vol. 58, no. 2, pp. 652–670, Feb. 2012.

[64] S. Salimi, M. Skoglund, J. D. Golic, M. Salmasizadeh, and M. R. Aref, "Key Agreement over a Generalized Multiple Access Channel Using Noiseless and Noisy Feedback," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 9, pp. 1765–1778, Sep. 2013.

[65] E. Ekrem and S. Ulukus, "Effects of Cooperation on the Secrecy of Multiple Access Channels with Generalized Feedback," in *Information Sciences and Systems, 2008. CISS 2008. 42nd Annual Conference on*, Mar. 2008, pp. 791–796.

[66] T. T. Kim and H. V. Poor, "Secure Communications With Insecure Feedback: Breaking the High-SNR Ceiling," *IEEE Transactions on Information Theory*, vol. 56, no. 8, pp. 3700–3711, Aug. 2010.

[67] L. Lai, H. El Gamal, and H. V. Poor, "The Wiretap Channel With Feedback: Encryption Over the Channel," *IEEE Transactions on Information Theory*, vol. 54, no. 11, pp. 5059–5067, Nov. 2008.

[68] Y. Chen and A. H. Vinck, "Wiretap Channel With Side Information," *IEEE Transactions on Information Theory*, vol. 54, no. 1, pp. 395–402, Jan. 2008.

[69] S. I. Gelfand and M. S. Pinsker, "Coding for Channel with Random Parameters," *Problems of Control and Information Theory*, vol. 9, no. 1, pp. 19–31, 1980.

[70] W. Liu and B. Chen, "Wiretap Channel With Two-Sided Channel State Information," in *Conference Record of the 41st Asilomar Conference on Signals, Systems and Computers, 2007. ACSSC 2007*, Nov. 2007, pp. 893–897.

[71] H. G. Bafghi, B. Seyfe, M. Mirmohseni, and M. R. Aref, "On The Achievable Rate Region of a New Wiretap Channel With Side Information," 2012. [Online]. Available: http://arxiv.org/abs/1204.0173

[72] L. Czap, V. M. Prabhakaran, C. Fragouli, and S. N. Diggavi, "Secret Message Capacity of Erasure Broadcast Channels with Feedback," in *Information Theory Workshop (ITW), 2011 IEEE*, Oct. 2011, pp. 65–69.

[73] L. Lai and H. El Gamal, "The Relay-Eavesdropper Channel: Cooperation for Secrecy," *IEEE Transactions on Information Theory*, vol. 54, no. 9, pp. 4005–4019, Sep. 2008.

[74] O. O. Koyluoglu and H. El Gamal, "Cooperative Encoding for Secrecy in Interference Channels," *IEEE Transactions on Information Theory*, vol. 57, no. 9, pp. 5682–5694, Sep. 2011.

[75] I. Csiszár and J. Körner, *Information Theory: Coding Theorems for Discrete Memoryless Systems*. Akadémiai Kiado, Budapest, 1982.