On Unconditionally Secure Commitment over Unreliable Noisy Channels

Thesis submitted to
Indian Institute of Technology Kharagpur
for the award of the degree

of

Dual degree(BTech + MTech)

by

Manideep Mamindlapally

under the supervision and guidance of

Professor Amitalok J Budkuley
(Department of Electronics and Electrical Communication Engineering)

Department of Electronics and Electrical Communication Engineering
INDIAN INSTITUTE OF TECHNOLOGY KHARAGPUR

April 2022

Department of Electronics & Electrical Communication Engg.
Indian Institute of Technology Kharagpur
Kharagpur, India-721302

Certificate

This is to certify that this thesis entitled **On Unconditionally Secure Commitment over Unreliable Noisy Channels** submitted by **Manideep Mamindlapally**, to the Indian Institute of Technology Kharagpur, towards partial requirements of fulfillment for the award of dual degree (Bachelors of Technology + Masters of Technology) in Electronics and Electrical Communication Engineering is a record of bona fide research work carried out under my supervision and guidance during the academic year 2021-22.

Prof. Amitalok J Budkuley
Department of Electronics and Electrical Communication Engineering
Indian Institute of Technology Kharagpur
India - 721302.

I.I.T. Kharagpur
April 2022

Declaration

I certify that

a. the work contained in the thesis is original and has been done by me under the guidance of my supervisor;

b. the work has not been submitted to any other institute for any other degree or diploma;

c. I have followed the guidelines provided by the Institute in preparing the thesis;

d. I have conformed to ethical norms and guidelines while writing the thesis;

e. whenever I have used materials (data, models, figures and text) from other sources, I have given due credit to them by citing them in the text of the thesis, and giving their details in the references, and taken permission from the copyright owners of the sources, whenever necessary.

f. Some of the content of this thesis has appeared in one or more published works, of which I am a co-author

Manideep Mamindlapally

Acknowledgements

I am grateful to my supervisor Prof. Amitalok J Budkuley(IIT Kharagpur) for providing this project opportunity. He has been very helpful throughout by clarifying doubts, conducting weekly meetings online and in many other ways. I would also thank other collaborators Anuj K Yadav(UG student IIT Patna), Pranav Joshi(IIT Kharagpur Alumnus) and Prof. Manoj Mishra(NISER Bhubaneshwar) who also participated actively in suggesting ideas which have been useful to the project and are also co-authors of some published papers arising out of this work.

Abstract

Commitment is a classic two-phase cryptographic protocol. Here a committer encrypts a string and sends it to the receiver in the *commit phase*. The string is then revealed in the *reveal phase* to the receiver; such a *verifier* then accepts the string only if it matches the original one. It is well known that noisy channels offer a valuable resource to realise *unconditionally-secure* or *information-theoretically* secure commitment.

The statistics of noisy channels, however, may be imprecisely characterised. Such *unreliable* noisy channels have been of active interest to the cryptographic community. In this work we study a wide range of unreliable channels; find out the regimes of parameters over which commitment is possible. We present new results for commitment throughput, i.e., *commitment capacity* for several such channels. Over discrete alphabet, we complete the study on elastic channels, reverse elastic channels, compound channels and unfair noisy channels. The results bring to the fore an the interplay between two forms of unreliability *compoundness* and *elasticity*. Motivated by the interesting trends that have come to light, we propose and study an even more generalised "asymmetric unfair noisy channels" for a wider perspective. We initiate a study over unreliable continuous channels too, by proposing and investigating commitment over "Gaussian unfair noisy channels."

Contents

Chapter 1

Introduction

1.1 What is commitment?

We start off by motivating the commitment problem with a coin toss example.

1.1.1 Coin toss example

Coin toss is a commonly used method to rule on some dispute between two conflicting parties without being partial to either of them. In a cricket match for example, the captains from both the teams want to decide who is to bat or bowl in the first innings. They do that with a coin toss. Usually the host team captain (the tosser T) brings a coin and tosses it into the air. The away team captain (the guesser G) guesses a choice "Heads" or "Tails" and shouts it out while the coin is still mid air. If the outcome matches the guess, G wins, else T wins. The winning captain then chooses whether to bat or bowl. The scheme works on the presumption that G has no hint or tool to predict the toss outcome. Now, imagine a highly sophisticated guesser G who is able to accurately determine the coin trajectory and so always guesses correctly. The above scheme fails to remain impartial in this case.

As an attempt towards resolving this issue, one may suggest G to make a guess before even T tosses the coin. But that puts T in a supremely advantageous position, who with his knowledge of the coin structure, can manipulate the outcome by launching the coin at one desired trajectory so that it lands excatly on the target side. This again compromises with the intended impartiality of the scheme.

Now, hear out another modified scheme. We ask G to *commit* to a choice "Heads" or "Tails", by whispering it to an umpire first, before T tosses the coin. Only after the toss is finished, G *reveals* his choice. T can verify that the revealed choice is indeed what G had committed to earlier by checking with the referee. This way T would not have any information on G's guess to base a target to manipulate the toss outcome to. Likewise G would also have no idea about the trajectory of the coin toss at the time when he *commits*. This assures the intended impartiality. Note here that we rely heavily on the trustworthiness of a third party, the umpire. Such a trusted thrid party may be not always be easy to establish in more complicated systems where a similar functionality is desired.

1.1.2 Commitment

In general, commitment is an interactive protocol that happens between two participants, a *committer*, say *Alice* and a *verifier*, say Bob. It takes place over two phases. In the first phase, the **commit phase**, *Alice commits* to a string, but keeps it hidden from *Bob*. Only in the second phase, the **reveal phase**, *Alice reveals* her string to *Bob* who later verifies. As a security guarantee *Bob* may want to flag out anytime *Alice* reveals a string different from what she has committed to, thus *binding* her to the committed string. We call this *bindingness*. *Concealment* is another guarantee which ensures that *Alice's* string remains hidden from *Bob* until the reveal phase. We will define these terms more formally later.

This functionality of commitment can find large applications. It is widely used as a cryptographic primitive in many practical tasks like sealed bid auctions [NS10], zero knowledge proofs [NS10], contract signing [EGL85] and secure multiparty computations [GMW87]. Modern technologies like blockchains also offer a great avenue to leverage the functionality offered by commitment [WSL+19].

1.2 Realisation of commitment: A literature survey

One way to realise commitment is by using an active trusted third party as discussed in the coin toss example above, but as already mentioned, such active trustworthiness is not an easy to procure, especially in complicated cryptosystems.

The earliest forms of commitment schemes, studied by Blum [Blu83], did not actually use any additional non-trivial resources beyond simple local computations and message exchanges between the two participants. However, the security of the schemes heavily relied on the assumption that the parties could not compute super-polynomial time-complex problems. In other words, these schemes were only *conditionally secure*. More precisely these schemes were either *conditionally concealing* or *computationally binding* or both. *Conditionally concealing* schemes assumed polynomial time bounds on computational power of Bob and were therefore secure from Alice's point of view. Analogously *conditionally binding* schemes required computational bounds on Alice and were therefore secure from Bob's point of view.

It was found in [DKS99], that without these computational bounds, commitment is actually impossible. The above schemes were therefore majorly flawed. Especially with the advent of quantum technologies, there is a possibility of efficient computation (in polynomial time) of certain problems that are so far thought to be super-polynomial time-complex, like finding integer factorisation and discrete logarithms of large numbers [Sho94].

It is pertinent to look for ways to realise commitment with security that is guaranteed beyond computational assumptions. Since, plain local-computations and message exchanges are not enough to realise *unconditionally secure* commitment [DKS99], the community began to look for other non-trivial resources that could help. Fortunately, *noisy channels* were found

to be very useful in this regard.

1.3 Commitment over noisy channels: A literature survey

Wyner's seminal work on wire-tap channels [Wyn78] first explored the potential of noisy channels for security. He was able to achieve *information theoretic* secure transmission of information using discrete memoryless noisy channels. It is to note that *information theoretic* from of security is not conditional on any computational assumptions. This inspired the community to explore noisy channels as a resource for other cryptographic protocols as well.

It is worth pointing out here that perfectly secure commitment is not possible even with the use of noisy channels. Inherently, perfect *concealing* guarantees for Alice would mean a compromise on *bindingness* guarantees for Bob and vice versa. The intuition with the use of noisy channels is that it probabilistically brings down the likelihood of failure of both *concealment* and *bindingness* guarantees to as small as needed. Markedly, this form of *information theoretic* security is not conditional on any computational assumptions. We discuss now the state of developments in *information theoretic* secure forms of commitment.

Inspired by [Wyn78], Crépeau et al. [CK88] were able to realise *information theoretic secure* commitment and another closely related cryptographic protocol, oblivious-transfer for the first time using binary symmetric channels(BSCs c.f. definition 3.5). They improved the results in [Cré97] by finding computationally efficient[1] ways to realise commitment. Winter et al. in [WNI03], characterised the notion of commitment *capacity* as the maximum number of bits that can be committed per use of the noisy channel. They also characterised the capacity expression for general alphabet discrete memoryless channels (DMCs). Recently in one of our works [MYMB21] we explored certain cost functions and restrictions associated with input symbols over noisy channels. We characterised commitment capacity over such *cost constrained* DMCs and found a dual expression for the same.

1.3.1 Commitment over unreliable noisy channels

Often times, the noisy channel resource may not have a perfect statistical characterisation. For instance, the cross over probability p of a binary symmetric channel (BSC(p)) may not be exactly known. More perniciously, one of the participants may have control over this value, and seeks to maliciously use it to their advantage. As an example, say two parties purchased a noisy channel box[2] with two access points, one for the sender and another for the receiver. The box is to take in messages from the sender and give it to the receiver after

[1]The computationally efficient notion of commitment schemes is that if the protocols can be executed in polynomial time steps as a function of input size. That said, the security of the scheme would still be secure against adversaries of any computational power

[2]This is a hypothetical example. By purchasing a noisy channel box, we emphasise that we use noise as a resource rather than as an obstacle, as is used in most reliable communication problems.

adding random noise of some given statistic. Due to some fault in manufacturing, say the box doesn't exactly perform according to the given statistic but is known to not vary too far away from it. Or one of the player knows how to tune the statistic but doesn't reveal it to the other, potentially to make some benefit out of this extra knowledge.

We call these imperfectly characterised channels in general as *unreliable noisy channels*, also referred to hereafter as simply *unreliable channels*. Damgård et al. [DKS99] initiated a systematic study of *unreliable channels* by introducing *unfair noisy channels*(UNCs). A UNC$[\gamma, \delta]$, $(0 < \gamma \leq \delta < \frac{1}{2})$ is essentially a BSC(p) where the transition probability p can belong to $[\gamma, \delta]$ interval. Additionally, a cheating party can also maliciously control this value p, by setting it to some value in the same interval, $[\gamma, \delta]$. [DKS99] characterised a regime of the parameters γ and δ for which where commitment is not possible over UNC$[\gamma, \delta]$. Crépeau et al. [CDN20] recently improved the result by finding an expression for the *commitment capacity i.e.,* the maximum commitment throughput over UNCs, for parameters within the possibility regime. The capacity expression was $\mathbb{C}_{UNC[\gamma,\delta]} = H_2(\gamma) - H_2(\frac{\delta-\gamma}{1-2\gamma})$.

In the current work, we emphasise primarily on two forms of unreliablility, *viz., compoundness* and *elasticity*. We study a class of compound BSC channels which model *compoundness* form of unreliability. A compound BSC is a BSC channel where the crossover probability is not precisely known but is said to be in some given real range. In this work we formulate the commitment capacity expression for compound BSCs [YMBM21] and also extend the result to general alphabet discrete compound channels [YMJB22]. The second form of unreliability, *elasticity* was first proposed earlier by Khurana et al. [KMS16] through elastic channels (ECs) and Reverse elastic channels(RECs). In essence, an elastic channel EC$[\gamma, \delta]$ behaves like a BSC(δ) except that a cheating receiver can control the channel by setting the crossover probability to some value in $[\gamma, \delta]$. It is the same in RECs, except that the sender has the power here rather than the receiver. Crepeau et al. [CDN20] characterised the commitment capacity expression of ECs to be $\mathbb{C}_{EC_{[\gamma,\delta]}} = H_2(\gamma)$. We find out the commitment capacity of RECs in [BJMY21, BJMY22a], to complete the picture.

There are some interesting trends in the behaviour of *elasticity* and *compoundness* in regard to commitment, which we address in [BJMY22a]. It is worth noting that UNCs model a combined form of unreliability of both *compoundness* and *elasticity*. While this combined form introduces an impossibility regime in UNCs, commitment is known to be always possible over ECs, RECs and compound channels. These trends motivated us to study a more general class of unreliable channels, which we called Asymmetric UNCs [BJMYon]. The framework of Asymmetric UNCs that we define specialises deftly to ECs, RECs and UNCs.

We discussed so far commitment over discrete alphabet channels. Nascimento et al. [NBSI08] studied commitment over continuous alphabet additive white gaussian noise(AWGN) channels. AWGN channels add a random gaussian variable as noise to an input from the real alphabet. One fascinating result is that non-trivial AWGN channels have infinite commitment capacity. Subsequently [OM08] showed a constructive commitment scheme over AWGN channels. In one of our works(in preparation) [BJMY22b], we present a class of unreliable gaussian channels called the Gaussian unfair noisy channels (Gaussian-UNCs). Gaussian-

UNCs add a zero-mean random gaussian noise with variance not precisely charecterised, but is known to be in some interval. We see that unlike AWGN channels, it is not apparent that Gaussian-UNCs have an infinite commitment capacity. In fact, we find Gaussian-UNCs have an impossibility regime where commitment is not possible at all, analogous to the UNCs of the binary alphabet. Furthermore, commitment has also been studied more generally over noisy quantum channels (for its reliable variants) [HW22]. As was with classical channels, commitment was also found to be impossible over noiseless quantum channels [LC97].

1.4 Contributions

For clarity purposes, we highlight here the important contributions of this thesis. Before that, it is worthwhile to recapitulate some important contributions of the previous thesis [Mam21] which is a direct precursor to the current work.

- In [MYMB21], we characterised cost constraints associated with noisy channels. As an extension to [WNI03], we found the commitment capacity expression and its dual over cost constrained DMCs.
- We studied commitment over compound BSCs [YMBM21] and characterised the capacity expression via an *achievability* and *converse* framework.

Through this thesis,

- We extend our past results on commitment over compound BSCs [YMBM21] to general discrete alphabet compound channels in [YMJB22]. Inspired by the methods used in [IMNW06], we propose a computationally efficient *capacity* rate achieving commitment protocol.
- Additionally, we look at cases when parties are *state-aware* (possibly in a one-sided manner), where a state-aware party(s) is one which knows a priori the exact compound state instantiated. We see that state-awareness at the committer can increase the commitment capacity of the compound-DMC.
- We study and characterise commitment capacity over RECs in [BJMY21, BJMY22a]. The result settles a recent conjecture in [CDN20].
- The results shed light upon an interesting interplay between the two forms of unreliability, viz., *compoundness* and *elasticity*. In particular, we show that unlike in UNCs (which combine both forms of unreliability) where the commitment capacity can be zero, capacity for binary channels with exclusively one form of unreliability have strictly positive commitment throughput.
- Motivated by these observations, we model a new more generalised form of unreliable BSCs, the Asymmetric-UNCs in [BJMYon]. We find a general impossibility result that encompasses all the variants BSC, EC, REC, and UNC. We also propose an achievability scheme over the possibility regime.

- We also propose an unreliable version of the AWGN channel, called the Gaussian-UNCs [BJMY22b]. Analogous to the UNCs [DKS99], Gaussian-UNCs also are found to have a parameter regime where commitment is impossible to realise.
- We also present partial achievability rate schemes over Gaussian UNCs. Unlike for AWGN channels [NBSI08], it is not apparent that non trivial Gaussian-UNCs have infinite capacity. The results bring a new perspective on the infinite capacity of the classical AWGN channels, as classical AWGN channels happen to be one special trivial Gaussian-UNC.

1.5 Thesis organisation

We first introduce preliminaries in chapter 2, then establish the commitment problem setup in chapter 3, where we also introduce different noise channel models along with the behaviours of different agents. We then discuss our results on compound channels and reverse elastic channels in chapters 5 and 6 respectively. Then we study commitment over Asymmetric-UNCs and Gaussian-UNCs. Lastly we conclude in chapter 9 and mention some past publications and references.

Chapter 2

Preliminaries

2.1 Notations

- We denote random variables by upper case letters (eg. X), the values they take by lower case letters (eg., x), and their alphabets by calligraphic letters (eg. $\mathcal{X}$). Unless stated otherwise, all sets are assumed to be finite.

- We denote random vectors and the accompanying values they take by boldface letters (e.g., $\mathbf{X} = (X_1, X_2, \cdots, X_n)$, $\mathbf{x} = (x_1, x_2, \cdots, x_n)$, resp.). Here n denotes the block length of communication.

- The set of real numbers, non-negative real numbers and real vectors (of length n) are denoted by $\mathbb{R}$, $\mathbb{R}_+$, and $\mathbb{R}^n$ respectively. The set of natural numbers is denoted by $\mathbb{N}$.

- For any natural number $a \in \mathbb{N}$, let $[a] := \{1, 2, \cdots, a\}$. Let $\mathbf{X}^i = (X_1, X_2, \cdots, X_i)$ and $\mathbf{X}_i^j = (x_i, X_{i+1}, \cdots, X_j)$ denote vectors.

- We denote the Hamming distance between two vectors, say $\mathbf{x}, \mathbf{x}' \in \mathcal{X}^n$ by $d_H(\mathbf{x}, \mathbf{x}') = \sum_{i=1}^n \mathbf{1}_{\{x_i \neq x_i'\}}$, where $\mathbf{1}_A$ denotes the indicator of A.

- Let P_X denote the distribution of $X \in \mathcal{X}$; $\mathcal{P}(\mathcal{X})$ denotes the simplex of probability distributions on set $\mathcal{X}$. Distributions for multiple random variables are similarly defined.

- Let $\mathcal{P}(\mathcal{X}|\mathcal{Y})$ denote the set of all conditional probability distributions on random variable $X \in \mathcal{X}$ conditioned on $Y \in \mathcal{Y}$. We denote by P_X, $P_{X|Y}$ and $P_{X,Y}$ the probability distribution on random variables $X \in \mathcal{X}$, conditional probability distribution on random variable $X \in \mathcal{X}$ conditioned on random variable $Y \in \mathcal{Y}$ and joint probability distribution on the pair of random variables $(x, Y) \in \mathcal{X} \times \mathcal{Y}$. For the latter, we denote the marginal distribution on random variable X by $[P_{X,Y}]_X$. Given P_X, $P_X^{(n)}$ denotes the n-fold memoryless extension of P_X.

- Let $\mathbb{P}(A)$ denote the probability of event A. Deterministic and random functions will be denoted by lower case letters (eg. f) and by upper case letters (e.g., F) respectively. Let $X \sim \text{Bernoulli}(p)$ denote a Bernoulli random variable X with parameter $p \in [0, 1]$.

Let $p*q := p(1-q)+(1-p)q$, where $p, q \in [0,1]$. Given $P_X, Q_X \in \mathcal{P}(\mathcal{X})$, let $||P_X - Q_X||$ denote the statistical (or variational) distance between P_X and Q_X.

2.2 Information quantities

We also need some information quantities to present our results; we begin by defining these useful information measures (see, for instance, [BB11, CK11] for details).

Given a discrete random variable $X \in \mathcal{X}$ and $\alpha \in [0,1) \cup (1,\infty)$, the *Renyi entropy of order* α is defined as:

$$H_\alpha(X) = \frac{1}{1-\alpha} \log \left(\sum_x (P_X(x))^\alpha \right).$$

The *max entropy* $H_0(X)$*, (Shannon) entropy* $H(X)$*, collision entropy* $H_c(X)$ *and min entropy* $H_\infty(X)$ are special cases of *Renyi entropy* of order α, where $\alpha = 0$, $\alpha \to 1$, $\alpha = 2$ and $\alpha \to \infty$ respectively:

$$\begin{aligned}
H_0(X) &= \log |\{x \in \mathcal{X} | P_X(x) > 0\}| \\
H(X) &= \lim_{\alpha \to 1} H_\alpha(X) = \sum_{x \in \mathcal{X}} P_X(x) \log \left(\frac{1}{P_X(x)} \right) \\
H_c(X) &= H_2(X) = -\log \left(\sum_{x \in \mathcal{X}} P_X(x)^2 \right) \\
H_\infty(X) &= \lim_{\alpha \to \infty} H_\alpha(X) = \min_x \log \left(\frac{1}{P_X(x)} \right)
\end{aligned}$$

Their conditional versions are defined as:

$$\begin{aligned}
H_0(X|Y) &= \max_y H_0(X|Y=y) \\
H(X|Y) &= \sum_{y \in \mathcal{Y}} P_Y(y) H(X|Y=y) \\
H_c(X|Y) &= \sum_{y \in \mathcal{Y}} P_Y(y) H_c(X|Y=y) \\
H_\infty(X|Y) &= \min_y H_\infty(X|Y=y)
\end{aligned}$$

The *min-entropy* is the Renyi entropy for order $\alpha \to \infty$,

$$H_\infty(X) = \lim_{\alpha \to \infty} H_\alpha(X) = \min_x \log \left(\frac{1}{P_X(x)} \right).$$

Its conditional version is given by. The *max-entropy* (i.e., Renyi entropy of order $\alpha \to 0$) is defined as

$$H_0(X) = \log |\{x \in \mathcal{X} | P_X(x) > 0\}|.$$

The *conditional max-entropy* is Similarly, the *collision entropy* (Renyi entropy of order $\alpha = 2$) and its conditional version are ,

$$H_c(X|Y) = \sum_{y \in \mathcal{Y}} P_Y(y) H_c(X|Y = y).$$

For $\epsilon \in [0, 1)$, the ϵ-smooth *max entropy*, ϵ-smooth *min entropy* and their conditional versions are given by:

$$\begin{aligned} H_0^\epsilon(X) &:= \min_{X' : ||P_{X'} - P_X|| \leq \epsilon} H_0(X') \\ H_\infty^\epsilon(X) &:= \max_{X' : ||P_{X'} - P_X|| \leq \epsilon} H_\infty(X') \\ H_0^\epsilon(X|Y) &:= \min_{X', Y' : ||P_{X',Y'} - P_{X,Y}|| \leq \epsilon} H_0(X'|Y') \\ H_\infty^\epsilon(X|Y) &:= \max_{X', Y' : ||P_{X',Y'} - P_{X,Y}|| \leq \epsilon} H_\infty(X'|Y') \end{aligned}$$

2.2.1 Chain Rules for smooth entropies

We now recapitulate some well known chain rules for these entropic notions.

Claim 2.1 (Min-entropy [VDTR13])**.** *For any $0 \leq \mu, \mu', \mu_1, \mu_2 < 1$ and any set of jointly distributed random variables (X, Y, W), we have*

$$\begin{aligned} H_\infty^{\mu+\mu'}(X, Y|W) &- H_\infty^{\mu'}(Y|W) \\ &\geq H_\infty^{\mu}(X|Y, W) && (2.1) \\ &\geq H_\infty^{\mu_1}(X, Y|W) - H_0^{\mu_2}(Y|W) - \log\left[\frac{1}{\mu - \mu_1 - \mu_2}\right] && (2.2) \end{aligned}$$

Claim 2.2 (Max-entropy [VDTR13, RW05])**.** *For any $0 \leq \mu, \mu', \mu_1, \mu_2 < 1$ and any set of jointly distributed random variables (X, Y, W), we have*

$$\begin{aligned} H_0^{\mu+\mu'}(X, Y|W) &- H_0^{\mu'}(Y|W) \\ &\leq H_0^{\mu}(X|Y, W) && (2.3) \\ &\leq H_0^{\mu_1}(X, Y|W) - H_\infty^{\mu_2}(Y|W) + \log\left[\frac{1}{\mu - \mu_1 - \mu_2}\right] && (2.4) \end{aligned}$$

2.2.2 Information quantities for continuous random variables

Let $X \in \mathcal{X}$ and $Y \in \mathbb{R}$ represent a discrete random variable and a continuous random variable respectively. For every $x \in \mathcal{X}$, the conditional probability density function (PDF) $f_{Y|X}(y|x)$ is assumed to be Riemann integrable. Then, the PDF of Y is given by

$$f_Y(y) = \sum_{x \in \mathcal{X}} P_X(x) f_{Y|X}(y|x)$$

is also Reimann Integrable.
Further, the conditional probability $P_{X|Y}(x|y)$ is given by

$$P_{X|Y}(x|y) = \frac{P_X(x) f_{Y|X}(y|x)}{f_Y(y)}$$

The conditional entropy of X given the random variable Y is given by:

$$H(X|Y) = -\int_{-\infty}^{\infty} f_Y(y) \left(\sum_{x \in \mathcal{X}} P_{X|Y}(x|y) \log(P_{X|Y}(x|y)) \right) dy$$

2.3 Useful definitions

Here are some definitions of certain structures which will be useful throughout this work.

Definition 2.1 (ξ-Univeral hash functions [CW79])**.** *Let $\mathcal{H}$ be a class of functions from $\mathcal{X}$ to $\mathcal{Y}$. $\mathcal{H}$ is said to be $\xi-$universal hash function, where $\xi \in \mathbb{N}$, if when $h \in \mathcal{H}$ is chosen uniformly at random, then $(h(x_1), h(x_2), ...h(x_\xi))$ is uniformly distributed over $\mathcal{Y}^\xi$, $\forall x_1, x_2, ...x_\xi \in \mathcal{X}$.*

Definition 2.2 (Strong randomness extractors [NZ96, DRS04a])**.** *A probabilistic polynomial time function of the form Ext: $\{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$ is an (n, k, m, ϵ)-strong extractor if for every probability distribution P_Z on $\mathcal{Z} = \{0,1\}^n$, and $H_\infty(Z) \geq k$, for random variables D (called 'seed') and M, distributed uniformly in $\{0,1\}^d$ and $\{0,1\}^m$ respectively, we have $||P_{Ext(Z;D),D} - P_{M,D}|| \leq \epsilon$.*

Chapter 3

Problem Setup

Now that we are equipped with all the necessary preliminaries, let us start our discussion on commitment in more detail. In this chapter we first define commitment in the context of its realisation over a general noisy channel. Then we will also look at the definitions of some unreliable channel models which we lightly introduced in chapter 1 (Section 1.3).

3.1 Definition of commitment

In the setup of commitment over noisy channels, we have two parties, a committer *Alice* and a verifier *Bob*. The commitment scheme itself involves two phases, the *commit phase* and *reveal phase*, each involving a series of steps that are prescribed for the parties to follow. *Alice* starts with a commit string c that she would commit to. *Alice* and *Bob* are capable of performing any computation and also have access to individual local randomness sources. As shown in figure 3.1, they share a two-way public authenticated noiseless link through which they can exchange messages publicly any number of times. There is also a one-way noisy channel (say $\mathcal{N}$) that goes from *Alice* to *Bob* that is used say n number of times. Crucially, the noisy channel, $\mathcal{N}$ is characterised by its behaviour when both the agents *Alice* and *Bob* are honest, and when either of them is cheating. We do not care about the case when both of them are cheating for reasons we will see later in the chapter. Honest agents adhere to all the steps dictated by the scheme never attempting to thwart the security guarantees, whereas cheating parties may try to deviate from the steps to suit to their advantage. Here is the formal definition of commitment for a given noisy channel and its stated behaviours over various natures of the agents.

Definition 3.1 (Commitment protocol over a noisy channel)**.** *An (n, R)-commitment protocol is a two way interactive protocol between the committer Alice and receiver Bob over two phases, viz., the* commit *phase followed by the* reveal *phase over a given noisy channel (say $\mathcal{N}$). The goal of the protocol is to allow commitment between Alice and Bob over a random string $C \in [2^{nR}]$ available to Alice.*

- **Commit phase:** *Given a uniformly random commit string $C \in [2^{nR}]$, Alice transmits $\mathbf{X} = (X_1, X_2, \cdots, X_n) \in \mathcal{X}^n$ over the given noisy channel. While the n-rounds of one-way communication takes place over the noisy channel $\mathcal{N}$, Alice and Bob also exchange*

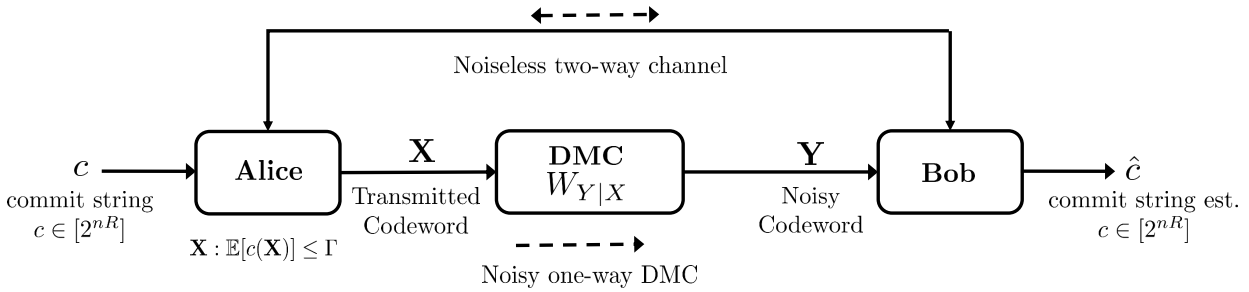

Figure 3.1: Commitment setup over a general noisy channel $\mathcal{N}$

messages over the public noiseless link (these messages are allowed to be arbitrarily many but assumed to be finite in size). Let M denote the entire collection of the exchanged messages (also called the transcript of the protocol) over the public channel at the end of commit phase. If K_A and K_B denote the sources of local randomnesses of Alice and Bob, Let V_A and V_B be their respective views, at the end of the commit phase; the view is the collection of all the random variables that a party has access to at the end *of the commit phase. Note that $V_A = (C, K_A, \mathbf{X}, M)$ and $V_B = (\mathbf{Y}, M, K_B)$. In general, the codewords sent by Alice in one round may depend on her view from all the previous rounds. The same is true for messages that are exchanged.*

- **Reveal phase:** *In this phase, communication between Alice and Bob occurs only over the two-way public authenticated noiseless channel. Initially, Alice reveals a pair comprising a commit string and a vector* [1]*, say $(\bar{c}, \bar{\mathbf{x}})$ to Bob, where $\bar{c} \in [2^{nR}]$ and $\bar{\mathbf{x}} \in \mathcal{X}^n$. Thereafter, Bob runs a test $T = T(\bar{c}, \bar{\mathbf{x}}, V_B)$, where the test output $T \in \{0, 1\}$. Here a test output of* 0 *indicates that Bob* rejects *the commit string $\bar{c}$ and a test output of* 1 *indicates that Bob* accepts *the commit string $\bar{c}$.*

We define R as the rate *of this (n, R) commitment protocol.*

We now define three key parameters of an (n, R) protocol. Let $\epsilon > 0$ be any arbitrary constant.

Definition 3.2 (ϵ-sound)**.** *An (n, R) protocol is said to be ϵ-sound if when* both *Alice and Bob are* honest *and execute the protocol,*

$$\mathbb{P}\left(T(C, \mathbf{X}, V_B) = 0\right) \leq \epsilon.$$

for any state of the channel that gets instantiated.

[1]Note that the pair $(\bar{c}, \bar{\mathbf{x}})$ may be the same pair that Alice used in the commit phase or a different one depending on her nature (honest or passively cheating or actively cheating).

Definition 3.3 (ϵ-concealing)**.** *An (n, R) protocol is said to be ϵ-concealing if for a honest Alice and under* any *strategy of Bob,*

$$I(C; V_B) \leq \epsilon.$$

for all the corresponding behaviours of the noisy channel.

Definition 3.4 (ϵ-binding)**.** *An (n, R) protocol is said to be ϵ-binding if for a honest Bob and under* any *strategy of Alice with an accompanying choice of $\mathbf{X} \in \{0,1\}^n$ during the commit phase, and for any two pairs $(\bar{c}, \bar{\mathbf{X}})$, $(\hat{c}, \hat{\mathbf{X}})$, where $\bar{c} \neq \hat{c}$, and $\bar{\mathbf{x}}, \hat{\mathbf{x}} \in \mathcal{X}^n$,*

$$\mathbb{P}\left(T(\bar{c}, \bar{\mathbf{x}}, V_B) = 1 \quad \& \quad T(\hat{c}, \hat{\mathbf{x}}, V_B) = 1\right) \leq \epsilon.$$

for all the corresponding behaviours of the noisy channel.

A rate $R > 0$ is said to be an *achievable rate* if for every $\epsilon > 0$ and every n sufficiently large, there exists an (n, R)-commitment protocol which satisfies all the security guarantees, i.e., the (n, R)-commitment protocol is ϵ-*sound*, ϵ-*concealing* and ϵ-*binding*. We define the *commitment capacity* or *capacity* of the given noisy channel $\mathcal{N}$ as the supremum of all achievable rates.

3.2 Noisy channel models

In chapter 1, we briefly looked at a few different noisy channels over which we will be studying commitment. Here we take a discourse into it by formally defining all the relevant noisy channels.

3.2.1 Reliable models

Let us start with the binary symmetric channels(BSCs).

Definition 3.5 (Binary symmetric channel)**.** *A binary symmetric channel BSC with parameter p s.t. $0 < p < 1$, also called BSC(p) is a channel which takes in a binary valued input and randomly outputs the input as is with probability $1 - p$ and the logical NOT of the input with probability p.*

A more general reliable noisy channel could be modelled by a discrete memoryless channel(DMC).

Definition 3.6 (Discrete memoryless channel)**.** *A discrete memoryless channel $W_{Y|X}$ is a channel that takes in an input, say x from a given alphabet space and gives out a random output from to the distribution $W_{Y|X=x}$ and independent of any previous inputs.*

3.2.2 Unreliable models

We look for more channels by modelling the forms of unreliability, *compoundness* or *elasticity*.

Definition 3.7 (Compound binary symmetric channel (Compound-BSC))**.** *A compound BSC with parameters $0 < \gamma < \delta < 1/2$, also called CBSC$[\gamma, \delta]$, is a noisy BSC where parties communicate over a $BSC(s)$, where $s \in [\gamma, \delta]$ and unknown to them.*

Compound-BSCs model *compoundness* from of unreliability. Now we look at *elasticity* form of unreliability.

Definition 3.8 (Elastic channel (EC))**.** *An elastic channel (EC) with parameters $0 < \gamma < \delta < 1/2$, also called EC$[\gamma, \delta]$, is a noisy BSC where*

(i) honest parties communicate over a classic $BSC(\delta)$,

(ii) only a cheating Bob can privately set the crossover probability to any value s in $[\gamma, \delta]$.

As one can see, while (*compoundness*) Compound-BSCs were symmetric in the agents Alice and Bob, ECs are certainly not. A malicious Bob has a lot more control over the channel than a malicious Alice can. We can also think of a channel model with a symmetrically opposite functionality where a malicious Alice can control the channel.

Definition 3.9 (Reverse elastic channel (REC))**.** *A reverse elastic channel (REC) with parameters $0 < \gamma < \delta < 1/2$, also called REC$[\gamma, \delta]$, is a noisy BSC where*

(i) honest parties communicate over a classic $BSC(\delta)$,

(ii) only a cheating Alice can privately set the crossover probability to any value $s \in [\gamma, \delta]$.

CBSCs and ECs, RECs model exclusive forms of unreliability where we have either *compoundness* or *elasticity*. Here is a channel model that has a combined form of unreliability.

Definition 3.10 (Unfair noisy channel (UNC))**.** *An unfair noisy channel (UNC) with parameters $0 < \gamma < \delta < 1/2$, also called UNC$[\gamma, \delta]$, is a noisy BSC where*

(i) honest parties communicate over a $BSC(s)$, where $s \in [\gamma, \delta]$ and unknown to them,

(ii) any cheating party can privately set s to a value in $[\gamma, \delta]$.

We can also define general alphabet versions of these unreliable channels in a similar manner. For one, let's look at a general compound DMC.

Definition 3.11 (Compound-discrete memoryless channel (Compound-DMC))**.** *A compound discrete memoryless channel (compound-DMC) is specified by the channel law given by the conditional distribution $W_{Y|X,s}$ and $s \in \mathcal{S}$, where $X \in \mathcal{X}$ and $Y \in \mathcal{Y}$ are the channel input and output, while $s \in \mathcal{S}$ ($\mathcal{S}$ is assumed to be a finite set) is the compound channel state. The set $\mathcal{S}$ is known* a priori *to all parties, whether honest or malicious, but the instantiated compound state $s \in \mathcal{S}$ is not known. We also denote the compound-DMC as $\{W_{Y|X,s}\}_{s \in \mathcal{S}}$.*

Remark 3.1. *A compound-DMC $\{W_{Y|X,s}\}_{s\in\mathcal{S}}$ can be essentially seen as a collection of DMCs indexed by $s \in \mathcal{S}$, i.e., $\{W^{(s)}_{Y|X}\}_{s\in\mathcal{S}}$.*

In chapter 5, we also look at certain variations of compound-DMCs bringing forth the concept of state awareness. One sided state aware channels are different from the Compound-DMCs of definition 3.11 in that, one of the parties gets to know the channel state s that gets instantiated, while the party agent still has no idea about s. It appears that two sided awareness is equivalent to a collection of simple DMC $\{W_{Y|X}\}_s$. We study them in more detail in chapter 5.

We also propose a new channel that models a general form of unreliability of elastic, reverse elastic and unfair noisy channels. We call that Asymmetric unfair noisy channels.

Definition 3.12 (Asymmetric unfair noisy channel (Asymmetric-UNC))**.** *An Asymmetric unfair noisy channel (A-UNC) with parameters $0 < \gamma_A, \gamma_B < \gamma < \delta < 1/2$, also called Asymmetric-UNC$[\gamma, \gamma_A, \gamma_B, \delta]$, is a noisy BSC where*

(i) honest parties communicate over a BSC(s), where $s \in [\gamma, \delta]$ and unknown to them,

(ii) a cheating sender can privately set s to a value in $[\gamma_A, \delta]$.

(iii) a cheating receiver can privately set s to a value in $[\gamma_B, \delta]$

3.2.3 Continuous channels

Here we look at some continuous alphabet noisy channels. The first is the AWGN channel. As the name suggests, this channel adds white Gaussian noise to the input.

Definition 3.13 (Additive white Gaussian noise channel)**.** *An additive white Gaussian noise channel (AWGN) with parameter $\sigma^2 > 0$, also called AWGN(σ^2) takes in an input from real alphabet and outputs after adding a random noise that comes from a zero mean Gaussian distribution with variance σ^2.*

We generalise this definition to model unreliability via Gaussian unfair noisy channels.

Definition 3.14 (Gaussian unfair noisy channels)**.** *A Gaussian unfair noisy channel (Gaussian-UNC) with parameters γ^2, δ^2 s.t. $0 < \gamma^2 \leq \delta^2$, also called Gaussian-UNC$[\gamma^2, \delta^2]$, is an AWGN where*

(i) honest parties communicate over an AWGN(s^2) where $s^2 \in [\gamma^2, \delta^2]$ and is unknown to them,

(ii) any cheating party can privately set s to a value in $\mathcal{S}$.

The elasticity of Gaussian-UNC$[\gamma^2, \delta^2]$ is $E := \delta^2 - \gamma^2$.

3.3 Behaviours of the participating agents

While we did indicate the differences in the "honest" and "cheating" behaviours while stating the security guarantees, we can think of more non-trivial behaviours while executing a general commitment scheme (of the form described in the section 3.1). Differentiating these behaviours would be crucial in analysing the results and proofs of later chapters. Honest agents adhere to all the steps dictated by the scheme never attempting to thwart the security guarantees, whereas cheating parties may try to deviate from the steps to suit to their advantage. Honest agents adhere to all the steps dictated by the scheme never attempting to thwart the security guarantees, whereas cheating parties may try to deviate from the steps to suit to their advantage. More specifically there are two kinds of cheating strategies, *active* and *passive*. A passively cheating party does not directly deviate from carrying out the laid out steps, but may attempt to gain knowledge of some variables which they are not meant to have access to. An actively cheating party on the other hand freely deviates from the prescribed steps in addition to his attempts to get hold of knowledge of extra variables. Moreover, both kinds of cheating parties may have an added ability to control certain parameters the channel, depending on its definition.

In the models that we study (in section 3.2), passive and active cheating strategies offer equal power in regard to control over the channel, and honest parties do not get any control. Although we do study certain state-awareness models (in section 5.5), where an honest party cannot directly control the channel, but may gain knowledge of the state that gets instantiated. Philosophically, it makes sense to study more complicated behaviours too, as long as the channel and the protocol are well defined. All the while, it is to be borne in mind that we offer security guarantees (in section 3.1 only to honest parties. More explicitly, we offer *bindingness* guarantees to an honest Bob, *concealment* to an honest Alice and *soundness* when both are honest. Philosophically, we do not seek to offer any guarantees when both the agents are cheating. For this reason, we do not also care about how the protocol plays out in such a case. Nor is it relevant to study the behaviour of the channel resources when both the agents are cheating, and so it is not a concern even if the channel is not well defined under that sub case.

Chapter 4

Review of prior work

In this chapter we present a summary of some relevant previous work. The points we make here will be helpful in understanding some results as we will be making some interesting analysis and comparisons in the later chapters. Let us start with some past results of commitment over reliable channels.

4.1 Commitment over general DMCs

[WNI03] characterises this expression for a class of non redundant DMCs.

Definition 4.1 (Non-redundant DMC)**.** *A discrete memoryless channel* $\{W_{Y|X}\}$ *is non-redundant if* $\forall x \in \mathcal{X}$ *and* $\forall P_X \in \mathcal{P}(\mathcal{X})$*, such that* $P_X(x) = 0$*,*

$$W_{Y|X}(\cdot|x) \neq \sum_{x' \in \mathcal{X}} P_X(x') W_{Y|X}(\cdot|x')$$

Theorem 4.1 (Commitment capacity of a DMC [WNI03])**.** *The commitment capacity of a non-redundant Discrete Memoryless Channel* $W_{Y|X}$ *over the input and output alphabet* $\mathcal{X}$*,* $\mathcal{Y}$*,* $\mathbb{C}_{DMC(W_{Y|X})}$ *is*

$$\mathbb{C}_{DMC(W_{Y|X})} = \max\{H(X|Y) : \text{ r.v.s } X, Y \text{ s.t. } Distr(Y|X) = W_{Y|X}\} \tag{4.1}$$

Every redundant DMC can be mapped to a non-redundant DMC by removing some redundant input symbols (those for which the equality in definition 4.1 gets satisfied). The commitment capacity of the obtained non-redundant DMC turns to be same as that of the original redundant DMC. So, using theorem 4.1, one can evaluate the capacity expression of any DMC.

Remark 4.1 (Commitment capacity of a BSC)**.** *The commitment capacity of a BSC*(p) *(*$0 < p < 1/2$*) can be found to be* $H_2(p)$ *by evaluating the capacity expression of general discrete memory channels from theorem 4.1.*

$$\mathbb{C}_{BSC(p)} = H_2(p) \tag{4.2}$$

As an extension to the result on DMCs, we study (in one of our earlier works [MYMB21]) commitment for certain *cost-constrained* DMCs.

4.1.1 Commitment over cost constrained DMCs

Often times, the input to a channel may have some restrictions. We model such behaviour via certain linear costs and cost constraints associated with each input symbol. For such *cost constrained* general DMCs that are non redundant.

Theorem 4.2 ([MYMB21]). *Let $W_{Y|X}$ be a (ρ_X, Γ)-non-trivial discrete memoryless channel. Then, the commitment capacity of $W_{Y|X}$ under the input constraint Γ, where $\Gamma \geq \min_x \rho_X(x)$, is given by*

$$\mathbb{C}_{DMC(W_{Y|X})}(\Gamma_X) = \max_{P_X : \mathbb{E}[\rho_X(X) \leq \Gamma]} H(X|Y) \tag{4.3}$$

The commitment capacity specializes to that of the (input) unconstrained capacity [WNI03] as $\mathcal{S}(\Gamma) = \mathcal{X}^n$ when input is unconstrained, i.e., all $\mathbf{x}$ are feasible vectors. The proofs of these theorems involves a converse upper bound and a capacity rate achieving commitment protocol built on a random binning codebook scheme. We have also a dual characterisation for the same capacity expression

Theorem 4.3 ([MYMB21]). *Let $W_{Y|X}$ be a (ρ_X, Γ)-non-trivial discrete memoryless channel. Then, for any $\Gamma \geq \min_{x \in \mathcal{X}} \rho_X(x)$,*

$$\mathbb{C}_{DMC}(\Gamma_X) = \min_{\gamma \geq 0} \max_{Q_Y} \log \left[\sum_{x \in \mathcal{X}} 2^{-D(W_{Y|X}(\cdot|x)||Q_Y(\cdot)) + \gamma(\Gamma - \rho_X(x))} \right]. \tag{4.4}$$

Furthermore, the maximizing distribution Q_Y is unique and $Q_Y = [P_X W_{Y|X}]_Y$, where P_X is any optimizer of (4.3).

The dual capacity characterization offers an alternate method to compute the commitment capacity. Given the channel law and the size of the input and output alphabets, one may prefer either of the two results depending on the computational and/or analytical tractability of the concomitant optimization problems. An interesting consequence of this result is that the unique optimizing output distribution, say $Q_Y^* \in \mathcal{P}(\mathcal{Y})$, is the output distribution corresponding to *every* input distribution that is an optimizer in (4.3).

4.1.2 Commitment over Compound-BSCs

In another of our works [YMBM21], we determined the commitment capacity of Compound BSCs defined in Definition 3.7.

Theorem 4.4 (Compound BSC commitment capacity [YMBM21]). *The commitment capacity of Compound-BSC$[\gamma, \delta]$ ($0 < \gamma \leq \delta < 1/2$)is*

$$\mathbb{C}_{C-BSC[\gamma,\delta]} = H_2(\gamma) \tag{4.5}$$

The proof of this is inspired by an approach in [CDN20], but with some notable differences. We find a converse upperbound and then present a computationally efficient scheme that achieves that rate bound.

4.1.3 Commitment over ECs

We also have a similar capacity expression for Elastic channels from [CDN20]. It turns out that the capacity of Elastic channel $\mathbb{C}_{EC[\gamma,\delta]}$ equals that of Compound BSC $\mathbb{C}_{C-BSC[\gamma,\delta]}$.

Theorem 4.5 (EC commitment capacity [CDN20]). *The commitment capacity of $EC[\gamma,\delta]$ $(0<\gamma\leq\delta<1/2)$is*

$$\mathbb{C}_{EC[\gamma,\delta]} = H_2(\gamma) \tag{4.6}$$

4.1.4 Commitment over UNCs

The capacity of UNCs [CDN20] was found to be

Theorem 4.6 (UNC commitment capacity [CDN20]). *The commitment capacity of $UNC[\gamma,\delta]$ $(0<\gamma\leq\delta<1/2)$ for $\delta\leq\gamma\circledast\gamma$ is*

$$\mathbb{C}_{UNC[\gamma,\delta]} = H_2(\gamma) - H_2\left(\frac{\delta-\gamma}{1-2\gamma}\right) \tag{4.7}$$

The proofs of theorems 4.5 and 4.6 also involve a similar achievability scheme involving two rounds of hash functions and a converse scheme involving similar information theoretic reduction techniques. Theorem 4.6 completes the study on UNCs along with the impossibility result of [DKS99].

Theorem 4.7 (Impossibility region for UNCs [DKS99]). *Commitment is not possible over a $UNC[\gamma,\delta]$ $(0<\gamma\leq\delta<1/2)$ with $\delta\geq\gamma\circledast\gamma$.*

By using slightly modified techniques, we study the capacity expression for UNCs in [BJMY22a, BJMY21]. We discuss the results more elaborately in chapter MM:sasa. Now let us review commitment over continuous channels.

4.2 Commitment over continuous channels

4.2.1 Commitment over AWGN channels

Here is Nascimento et al.'s infinite capacity result over AWGNs from [NBSI08]

Theorem 4.8 (Commitment capacity over AWGNs [NBSI08]). *The commitment capacity of a nontrivial AWGN channel i.e., $AWGN(\sigma^2)$ s.t. $\sigma^2>0$, is infinite irrespective of the input power constraint.*

$$\mathbb{C}_{AWGN(\sigma^2)} \to \infty \tag{4.8}$$

Chapter 5

Commitment over Compound-DMCs

We have from theorem 4.1, the capacity expression for general discrete memoryless channels. We also have from theorem 4.4, the capacity expression for Compound-BSCs. In this chapter we will expand upon these previous results. We start off by introducing the problem setup from chapter 3 specific to Compound-DMCs, for which we state our commitment capacity result and then prove it. Additionally we also discuss in detail the concept of state awareness which we lightly alluded to in section 3.3 and characterise commitment over those channels too using similar proofs.

5.1 Problem setup

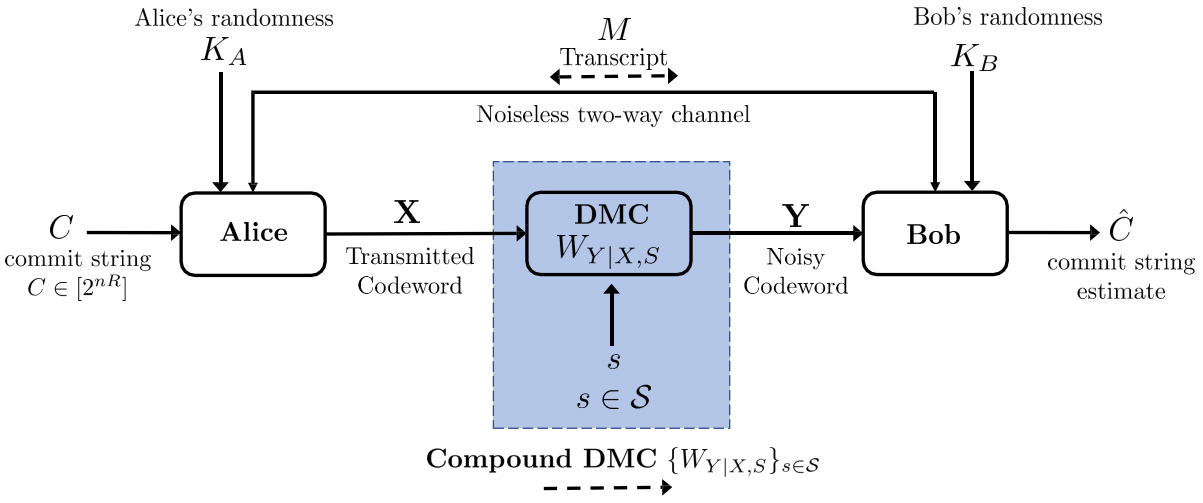

Figure 5.1: Commitment over a compound-DMC

In figure 5.1, we specialise the commitment problem setup of figure 3.1 to compound-DMC. We state the whole problem setup for completeness. Alice and Bob are two mutually distrustful parties who wish to *commit* on a random bit string $C \in [2^{nR}]$ (we specify $R > 0$

later); C is available to Alice. The two parties have access to a *compound*-discrete memoryless channel (Compound-DMC). Alice initiates n rounds of one-way communication with Bob over the Compound-DMC. Her transmitted *codeword* over the Compound-DMC is denoted by $\mathbf{X}$, $\mathbf{X} \in \mathbb{R}^n$. Bob observes the noisy version $\mathbf{Y}$ of the Alice's transmitted codeword $\mathbf{X}$. Notably the statistics of $\mathbf{Y}$ depend on the DMC $W_{Y|X,s}$ that gets instantiated from $\{W_{Y|X,s}\}_{s\in\mathcal{S}}$. Further, both Alice and Bob can privately randomize; let $K_A \in \mathcal{K}_A$ and $K_B \in \mathcal{K}_B$ denote the private randomness at Alice and Bob respectively. The parties also share a two-way, public authenticated noiseless public link. Any message transmitted over the bi-directional noiseless channel can have causal dependence on the information available to the parties at that instant.

A general (n, R) commitment protocol over a Compound-DMC$\{W_{Y|X,s}\}_{s\in\mathcal{S}}$ is of the form as in definition 3.1. Let us revise from definitions 3.2, 3.3 and 3.4, the accompanying security guarantees, viz., *soundness*, *concealment* and *bindingness.* in context to the Compound-DMCs.

- **ϵ-soundness:** An (n, R) protocol is said to be ϵ-sound if when *both* Alice and Bob are *honest* and execute the protocol,

$$\max_{s\in\mathcal{S}} \mathbb{P}\left(T(C, \mathbf{X}, V_B) = 0 | S = s\right) \leq \epsilon. \tag{5.1}$$

- **ϵ-concealing:** An (n, R) protocol is said to be ϵ-concealing if for a honest Alice and under *any* strategy of Bob,

$$\max_{s\in\mathcal{S}} I(C; V_B | S = s) \leq \epsilon. \tag{5.2}$$

- **$\epsilon-$bindingness:** An (n, R) protocol is said to be ϵ-binding if for a honest Bob and under *any* strategy of Alice with an accompanying choice of $\mathbf{X} \in \{0, 1\}^n$ during the commit phase, and for any two pairs $(\bar{c}, \bar{\mathbf{X}})$, $(\hat{c}, \hat{\mathbf{X}})$, where $\bar{c} \neq \hat{c}$, and $\bar{\mathbf{x}}, \hat{\mathbf{x}} \in \mathcal{X}^n$,

$$\max_{s\in\mathcal{S}} \mathbb{P}\left(T(\bar{c}, \bar{\mathbf{x}}, V_B) = 1 \quad \& \quad T(\hat{c}, \hat{\mathbf{x}}, V_B) = 1 \middle| S = s\right) \leq \epsilon. \tag{5.3}$$

A rate $R > 0$ is said to be an *achievable rate* if for every $\epsilon > 0$ and every n sufficiently large, there exists an (n, R)-commitment protocol which satisfies all the security guarantees, i.e., the (n, R)-commitment protocol is *ϵ-sound*, *ϵ-concealing* and *ϵ-binding*. We define the *commitment capacity* or *capacity* of the compound-DMC as the supremum of all achievable rates.

5.1.1 Non-redundant Compound-DMCs

Recall that information-theoretically secure commitment is impossible over noiseless channels [Blu83]. In fact, such channels belong to a larger class of DMCs called *trivial channels* [WNI03]. We now extend this notion to compound-DMCs. We first define the class of *non-redundant* compound-DMCs which help realize non-trivial commitment.

Definition 5.1 (Non-redundant compound-DMC)**.** *A compound discrete memoryless channel $\{W_{Y|X,S}\}_{s\in\mathcal{S}}$ is non-redundant if $\forall x \in \mathcal{X}$ and $\forall P_X \in \mathcal{P}(\mathcal{X})$, such that $P_X(x) = 0$, the following holds for every $s \in \mathcal{S}$:*

$$W_{Y|X,S}(\cdot|x,s) \neq \sum_{x'\in\mathcal{X}} P_X(x') W_{Y|X,S}(\cdot|x',s) \tag{5.4}$$

A redundant compound-DMC $\{W_{Y|X,S}\}_{s\in\mathcal{S}}$ can be transformed into a non-redundant compound-DMC by expurgating all *redundant* symbols $x \in \mathcal{X}$; these are symbols $x \in \mathcal{X}$ which violate the condition in Definition 5.1.

Definition 5.2 (Trivial compound DMC)**.** *A non-redundant compound-DMC $\{W_{Y|X,S}\}_{s\in\mathcal{S}}$ is* trivial *if*

$$W_{Y|X,S}(y|x,s) \cdot W_{Y|X,S}(y|x',s) = 0, \quad \forall y \in \mathcal{Y},$$

for every pair of non-redundant and distinct symbols $x, x' \in \mathcal{X}$, and for some state $s \in \mathcal{S}$.

Note that over a trivial compound-DMC, Bob can effectively infer Alice's input non-trivially, for some compound state $s \in \mathcal{S}$, upon observing the channel output; this makes concealment impossible over any commitment protocol. Therefore, commitment cannot be performed over a trivial compound-DMCs and their commitment capacity is zero.

5.2 Commitment capacity results

The main focus of our work in [YMJB22] has been to characterize the optimal commitment throughput over Compound-DMCs. The following theorem states the same.

Theorem 5.1 (Compound-DMC commitment capacity)**.** *The commitment capacity of a non-redundant Compound-DMC specified by $\{W_{Y|X,S}\}_{s\in\mathcal{S}}$ is is*

$$\mathbb{C} = \max_{P_X} \min_{s\in\mathcal{S}} H(X|Y) \tag{5.5}$$

In the next two sections we discuss a detailed proof of this theorem. The proof itself consists of two parts: an achievability and a converse. Our achievability protocol is inspired by [IMNW06]. In particular, we present a computationally-efficient scheme involving set exchanges and universal hash functions. Our converse follows from the work in [YMBM21] where compound-BSCs were studied (note that compound-BSCs belong to the class of Compound-DMCs). However, we *strengthen* that converse by analysing commitment schemes with a weaker concealment guarantee.[1]

We provide a computationally-efficient commitment scheme based on set exchange and universal hash function which achieves the commitment capacity. Note that the max (over P_X) and min (over $s \in \mathcal{S}$) cannot be interchanged in general. In fact, the alternate expression $\min_{s\in\mathcal{S}} \max_{P_X} H(X|Y)$ is generally larger (and hence, is a weaker upper bound); in fact, for Compound-DMCs with state-awareness, we can *upgrade* the commitment capacity to the larger value. We explore this next.

[1]Note that showing the commitment capacity rate upper bound by analysing commitment schemes with weaker security notions (in this case, for concealment, is a tighter rate upper bound as the bound continues to hold when the security guarantees are made stronger.

5.3 Converse proof

The general converse was presented in [YMBM21]. We give a quick summary of the converse for completeness. Let us consider a sequence of protocols $\{\mathscr{P}_n\}_{n\geq 1}$. We assume that every protocol $\mathscr{P}_n$ in this collection satisfies the three security criteria, viz., $\mathscr{P}_n$ is ϵ_n-sound, ϵ_n-concealing and ϵ_n-binding for every state $s \in \mathcal{S}$, where $\epsilon_n \geq 0$ and $\epsilon_n \to 0$ as $n \to \infty$.

Note that we strengthen our converse by proving that our rate upper bound holds even under a weaker notion of ϵ-concealment defined below:[2]

Definition 5.3 (weakly ϵ-concealing)**.** *An (n, R) protocol is said to be weakly ϵ'-concealing if for an honest Alice and under* any *strategy of Bob,*

$$\max_{s\in\mathcal{S}} I(C; V_B|S = s) \leq n\epsilon' \tag{5.6}$$

We now state a following claim which will be used in our converse.

Lemma 5.1. *For every $\mathscr{P}_n$, we have $\frac{1}{n}H(C|\mathbf{X}, V_B) \leq \epsilon''_n$, $\forall s \in \mathcal{S}$, where $\epsilon''_n \to 0$ as $n \to \infty$,*
.

The proof is presented in Appendix section A.1. Let us now bound the rate R. Consider the following:

$$\begin{aligned}
R &= \frac{1}{n}H(C|V_B) + \frac{1}{n}I(C; V_B) \\
&\overset{(a)}{\leq} \frac{1}{n}H(C|V_B) + \epsilon'_n \\
&\overset{(b)}{=} \frac{1}{n}H(C, \mathbf{X}|\mathbf{Y}_s, K_B, M) - \frac{1}{n}H(\mathbf{X}|\mathbf{Y}_s, K_B, M, C) + \epsilon'_n \\
&\overset{(c)}{\leq} \frac{1}{n}H(C, \mathbf{X}|\mathbf{Y}_s, K_B, M) + \epsilon'_n \\
&= \frac{1}{n}H(\mathbf{X}|\mathbf{Y}_s, K_B, M) + \frac{1}{n}H(C|\mathbf{X}, V_B) + \epsilon'_n \\
&\overset{(d)}{\leq} \frac{1}{n}H(\mathbf{X}|\mathbf{Y}_s) + \epsilon''_n + \epsilon'_n \\
&\leq \frac{1}{n}\sum_{i=1}^{n} H(X_i|Y_{s,i}) + \epsilon''_n + \epsilon'_n
\end{aligned} \tag{5.7}$$

Here

(a) follows from 5.6.

(b) follows from the chain rule of joint entropy and some manipulations

(c) follows from noting that conditional entropy is a non-negative quantity

(d) follows from the fact that conditioning reduces entropy and Lemma **??**

[2]This is the 'un-normalized' secrecy notion which was originally studied by Wyner [Wyn75] for wiretap channels and also called *weak secrecy* in literature.

Using the standard trick of introducing an independent time-sharing random variable distributed uniformly over the set $\{1, n\}$ and some manipulations, we can simplify (6.6) as follows

$$\begin{aligned} R &\leq \sum_{i=1}^{n} \frac{1}{n} H(X_i|Y_{s,i}) + \epsilon''_n + \epsilon'_n \\ &\leq H(X|Y_s) + \epsilon''_n + \epsilon'_n \end{aligned} \tag{5.8}$$

Note that (5.8) holds for every $s \in \mathcal{S}$. Furthermore, we know that $\epsilon'_n, \epsilon''_n \to 0$ as $n \to \infty$. Hence, it follows that

$$R \leq \min_{s \in \mathcal{S}} H(X|Y_s)$$

for some appropriate distribution P_X on X. We now optimize the distribution on $\mathcal{X}$ to get our bound:

$$R \leq \max_{P_X} \min_{s \in \mathcal{S}} H(X|Y_s) \tag{5.9}$$

This completes our converse proof.

5.4 Achievability proof

Outline: We present a computationally efficient scheme which involves a random set exchange between the two parties (over the noiseless two-way link) and a 2-universal hash function. Our scheme is inspired by commitment scheme for DMCs in [IMNW06]; we *robustify* it so as to be a commitment capacity-achieving over the compound-DMC.

5.4.1 Achievable scheme

The commit phase and the reveal phase are described as follows:

Commit Phase: Fix P_X and set the rate $R = \min_{s \in \mathcal{S}} H(X|Y) - \beta > 0$, where $\beta > 0$ is arbitrarily small constant. Alice wishes to commit to a string $c \in [2^{nR}]$ with Bob, and the parties proceed in the following manner:

(C1) Alice generates a random vector $\mathbf{X}$, generated i.i.d. with distribution P_X.

(C2) Alice sends $\mathbf{X}$ over the C-DMC. Bob receives a corrupted version $\mathbf{Y}$ of the transmitted vector $\mathbf{X}$.

(C3) Based on the received vector $\mathbf{Y} = \mathbf{y}$, Bob creates a list of all candidate transmitted vectors over the Compound-DMC[3]:

$$\mathcal{L}(\mathbf{y}) := \left\{ \mathbf{x} \in \mathcal{T}_{\delta}^{(n)}(P_X) : T_{\mathbf{x},\mathbf{y}} \in \bigcup_{s \in \mathcal{S}} \mathcal{T}_{\delta'}^{(n)}(P_X W_{Y|X,S}) \right\}.$$

[3]Here $\delta > 0$ is chosen appropriately small.

(C4) Bob chooses a random subset $\mathcal{J} \subseteq \{1, 2, \cdots, n\}$ consisting of $n\zeta$ elements (where we assume $n\zeta$ is integer and $\zeta > 0$); here $\mathcal{J}$ is chosen uniformly at random and sent to Alice over the two-way noiseless link.

(C5) Alice computes the subset of $\mathbf{X}$ restricted to the indices in $\mathcal{J}$; we denote this set by $\mathbf{X}_{|\mathcal{J}} := \{\mathbf{x}(i) : \forall i \in \mathcal{J}\}$ and sends it back to Bob over the noiseless link.

(C6) Alice chooses an extractor function Ext, uniformly at random from a 2-universal hash family $\mathcal{E} := \{\text{Ext} : \mathcal{X}^n \to \{0,1\}^{n(\min_s(H(X|Y))-\beta)}\}$, where $\beta > 0$ is a constant chosen appropriately. Alice sends $Z = c \oplus \text{Ext}(\mathbf{X})$ (where $\oplus$ denotes component-wise modulo-2 addition) and a description of Ext to Bob over the noiseless channel.

Reveal phase: All the announcements in the reveal phase are made over the public noiseless link:

(R1) Alice reveals the pair $(\tilde{c}, \tilde{\mathbf{x}})$ to Bob.

(R2) Bob accepts $\tilde{c}$, if the revealed pair passes following tests:

(T1) $\tilde{\mathbf{x}} \in \mathcal{L}(\mathbf{y})$

(T2) $\tilde{\mathbf{x}}_{|\mathcal{J}} = \mathbf{x}_{|\mathcal{J}}$

(T3) $\tilde{c} = \mathbf{z} \oplus \text{Ext}(\tilde{\mathbf{x}})$.

Else he abots the protocol and outputs a 0.

5.4.2 Analysis of security guarantees

We now present an outline of our analysis. The soundness of our protocol follows from standard Chernoff bound. The protocol satisfies the bindingness guarantee too. To see this, note that for a cheating Alice to pass the Bob's typicality test (T1), she must reveal a $\tilde{\mathbf{x}}$ such that the $d_H(\mathbf{x}, \tilde{\mathbf{x}}) \leq q\sqrt{n}$ (for some constant $q > 0$) so that $\tilde{\mathbf{x}}$. However, the random set exchange (via set $\mathcal{J}$ and $\mathbf{X}_{|\mathcal{J}}$) between Alice and Bob over the noiseless link binds Alice to her specific choice of the transmitted vector $\mathbf{x}$. Any cheating attempt by revealing a different vector $\tilde{\mathbf{x}}$ is detected by Bob with high probability. This is because the set exchange makes it essentially impossible for Alice to find a vector $\tilde{\mathbf{x}}$ within the Hamming sphere (of radius proportional to $\sqrt{n}$) with same randomly chosen symbols (as $\mathbf{x}$) at $n\zeta$ locations such that it passes Bob's second test (T2). For concealment, the protocol needs to detect cheating strategy by Bob with high probability. Toward this, in the protocol, Alice uses a 2-Universal hash function Ext and computes $\text{Ext}(\mathbf{X})$; which is a nearly (uniformly) random string of size nR bits (where R is the rate of our commitment protocol), and hence, equals the length of Alice's commit string. Alice uses $\text{Ext}(\mathbf{X})$ as a secret key to encrypt the commit string c using one-time pad encryption, and sends the encrypted output to Bob over the C-DMC. This results in perfectly hiding the commit string from Bob in the commit phase thereby guaranteeing concealment. Also, note that Bob's third test (where Bob checks for compatibility of Alice's revealed string $\tilde{c}$ and $\tilde{\mathbf{x}}$ via the extractor function Ext) is important as it

helps detect a cheating Alice if she tries to behave maliciously and reveals an arbitrary $\tilde{c}$ such that $\tilde{c} \neq c$ with an $\tilde{\mathbf{x}}$ which is same as the transmitted vector $\mathbf{x}$, therefore, she will be caught. We now present a more detailed security analysis of our (n, R)-commitment protocol.

5.4.2.1 *ϵ-sound*

For honest Alice and Bob, the commitment protocol is ϵ-sound if:

$$\mathbb{P}(T(C, \mathbf{X}, \mathbf{Y}, J, \mathbf{X}_{|J}, Z, \text{Ext}) = 1) \geq 1 - \epsilon$$

where we assume that Alice and Bob are honest. Observe that due to Chernoff bound, $\mathbf{X} \in \mathcal{L}(\mathbf{Y})$ with high probability; this is Bob's test (T1). Conditioned on $\mathbf{X} \in \mathcal{L}(\mathbf{Y})$, note that the outcome of Bob's next two deterministic tests, viz. (T2) and (T3) are guaranteed to accept the string. Hence, we can conclude that the protocol is $\epsilon-$sound for n sufficiently large. Further, it can be written as:

$$\mathbb{P}((T_1(\mathbf{X}, \mathbf{Y}) = 1) \cap (T_2(\mathbf{X}, J, \mathbf{X}_{|J}) = 1) \cap (T_3(C, \mathbf{X}, Z, \text{Ext}) = 1)) \geq 1 - \epsilon$$

The above equations can be further re-written as:

$$\mathbb{P}(T_1(\mathbf{X}, \mathbf{Y}) = 1).\mathbb{P}(T_2(\mathbf{X}, J, \mathbf{X}_{|J}) = 1 | T_1 = 1).$$
$$\mathbb{P}(T_3(C, \mathbf{X}, Z, \text{Ext}) = 1 | T_1 = 1, T_2 = 1) \geq 1 - \epsilon$$

Note that the test T_2 and T_3 are deterministic and the revelations made by an honest Alice will always pass both T_2 and T_3. Therefore $\mathbb{P}(T_2(\mathbf{X}, J, \mathbf{X}_{|J}) = 1 | T_1 = 1) = 1$ and $\mathbb{P}(T_3(C, \mathbf{X}, Z, \text{Ext}) = 1 | T_1 = 1, T_2 = 1) = 1$.
The soundness criteria can then be simplified to:

$$\mathbb{P}(T_1(\mathbf{X}, \mathbf{Y}) = 1) \geq 1 - \epsilon$$
$$\mathbb{P}(\mathbf{X} \in \mathcal{L}(\mathbf{y})) \geq 1 - \epsilon$$

We analyse the complementary event $\{\mathbf{X} \notin \mathcal{L}(\mathbf{Y})\}$. Using standard chernoff bounds, we show that $\mathbb{P}(\mathbf{X} \notin \mathcal{L}(\mathbf{Y}))$ is exponentially decreasing as $n \to \infty$.

5.4.2.2 *ϵ-concealing*

For an honest Alice and a malicious Bob, the protocol is ϵ-concealing if it satisfies the *capacity-based* secrecy [DPP98], i.e., $I(C; V_B) \leq \epsilon$. We use the privacy amplification lemma to show that the specified protocol guarantees concealment even in the worst-case scenario of the compound DMC, for an honest Alice. We first make the following claim without proof which lower bounds the conditional collision entropy (thereby allowing us to use the privacy amplification lemma).

Claim 5.1. *For every $Y = y, \mathcal{J} = j$ and $\mathbf{X}_{|\mathcal{J}} = r$, where $j \subseteq [n]$, $r \in \mathcal{X}^{|\mathcal{J}|}$, the conditional collision entropy*

$$H_c(\mathbf{X}|\mathbf{Y} = y, \mathcal{J} = j, \mathbf{X}_{|J} = \mathbf{x}_{|j}) \geq n(\min_s H(X|Y_s) - \zeta') \tag{5.10}$$

where $\zeta' > 0$ is a constant and $\zeta' < \beta$.

The proof has been discussed in Appendix section A.2. We now state the privacy amplification lemma [BBCM95]; which uses the Claim 5.1.

Lemma 5.2 (Privacy Amplification Lemma)**.** *Let P_{AB} be an arbitrary probability distribution for $A \in \mathcal{A}$, $B \in \mathcal{B}$ and b be a realization of B. Suppose, the conditional collision entropy $H_c(A|B = b)$ is at least c. Let G be chosen uniformly at random from a 2-universal hash family $\mathcal{G} : \mathcal{X}^n \to \{0,1\}^r$. Then,*

$$H(G(A)|G, B = b) \geq r - \frac{2^{r-c}}{\ln 2} \tag{5.11}$$

We make the following correspondence in privacy amplification lemma: $A \leftrightarrow \mathbf{X}$, $G \leftrightarrow \epsilon$ and $B \leftrightarrow Y, \mathcal{J}, \mathbf{X}_{|\mathcal{J}}$.
From Claim 5.1 and Lemma 5.2, we have:

$$\begin{aligned} H(\epsilon(\mathbf{X})|\mathbf{Y}, \mathcal{J}, &\mathbf{X}_{|\mathcal{J}}, \epsilon) \geq \\ &n(\min_s(H(X|Y)) - \beta) - \frac{2^{n(\zeta'-\beta)}}{\ln 2} \end{aligned} \tag{5.12}$$

Using the above result, we can upper bound the mutual information $I(C : V_B)$:

$$\begin{aligned} I(C; V_B) &= I(C; \mathbf{Y}, \mathcal{J}, \mathbf{X}_{|\mathcal{J}}, Z, \text{Ext}) \\ &\overset{(b)}{=} I(C; Z|\mathbf{Y}, J, \mathbf{X}_{|J}, \text{Ext}) \\ &\overset{(c)}{=} H(C|\mathbf{Y}, J, \mathbf{X}_{|J}, \text{Ext}) - H(Z|C, \mathbf{Y}, J, \mathbf{X}_{|J}, \epsilon) \\ &\overset{(d)}{\leq} H(C) - H(Z|C, \mathbf{Y}, J, \mathbf{X}_{|J}, \epsilon) \\ &\overset{(e)}{\leq} H(C) - H(\epsilon(\mathbf{X})|C, \mathbf{Y}, J, \mathbf{X}_{|J}, \epsilon) \\ &\leq H(C) - H(\epsilon(\mathbf{X})|\mathbf{Y}, J, \mathbf{X}_{|J}, \epsilon) \\ &\overset{(a)}{\leq} \frac{2^{n(\zeta'-\beta)}}{\ln 2} \\ &\overset{(b)}{\leq} \epsilon_n \end{aligned}$$

where, $\epsilon_n \to 0$ as $n \to \infty$. Here (a) follows from several manipulations and the (5.12) while b follows from noting that $\zeta' < \beta$. Here,

(a) follows from noting that $V_B = \{\mathbf{Y}, J, \mathbf{X}_J, Z, \text{Ext}\}$.

(b) follows from chain rule of mutual Information and noting that C is independent of $\mathbf{Y}, J, \mathbf{X}_J, \text{Ext}$.

(c) follows from expressing mutual information in terms of entropy.

(d) Note that conditioning reduces entropy.

(e) Given C, knowing Z is equivalent to knowing $\text{Ext}(\mathbf{X})$.

(f) follows from noting that $\text{Ext}(\mathbf{X}) \leftrightarrow \mathbf{Y}, J, X_{|J}, \text{Ext} \leftrightarrow C$ is a markov chain.

(g) follows from (5.12).

(h) follows from noting that $\zeta' > 0$ and $\beta > 0$ are chosen such that $\zeta' < \beta$.

This completes our proof of concealment.

5.4.2.3 *ϵ-binding*

Let a cheating Alice transmit vector $\mathbf{x}$ (note that for cheating successfully, she seeks to reveal a different vector $\tilde{\mathbf{x}}$ in the reveal phase). Let Bob receive $\mathbf{y}$. Given that $\mathbf{x} \in \mathcal{L}(\mathbf{y})$ and using the fact that the channel is a non-redundant compound channel, Alice needs to find a vector $\tilde{\mathbf{x}}$ which lies within the n-dimensional hamming sphere centered at $\mathbf{x}$ of radius $\sqrt{n}$ such that $\tilde{\mathbf{x}} \in \mathcal{L}(\mathbf{y})$. However, the probability to find such a $\tilde{\mathbf{x}}$ which has similar $n\zeta$ randomly chosen symbols as $\mathbf{x}$ is vanishing in block length n. Thus, Alice cannot find an $\tilde{\mathbf{x}}$ which would satisfy Bob's second test thereby ensuring that our protocol is ϵ-binding.

5.5 Commitment capacity of Compound-DMCs under state awareness

In [YMJB22], we also study commitment over compound-DMCs under state-awareness at either and/or both parties. Crucially, we assume that a state-aware party knows the compound state $s \in \mathcal{S}$ exactly but cannot control it (such a control, for instance, is possible in UNCs and channels with elasticity).

5.5.1 Case I: Only committer is state-aware

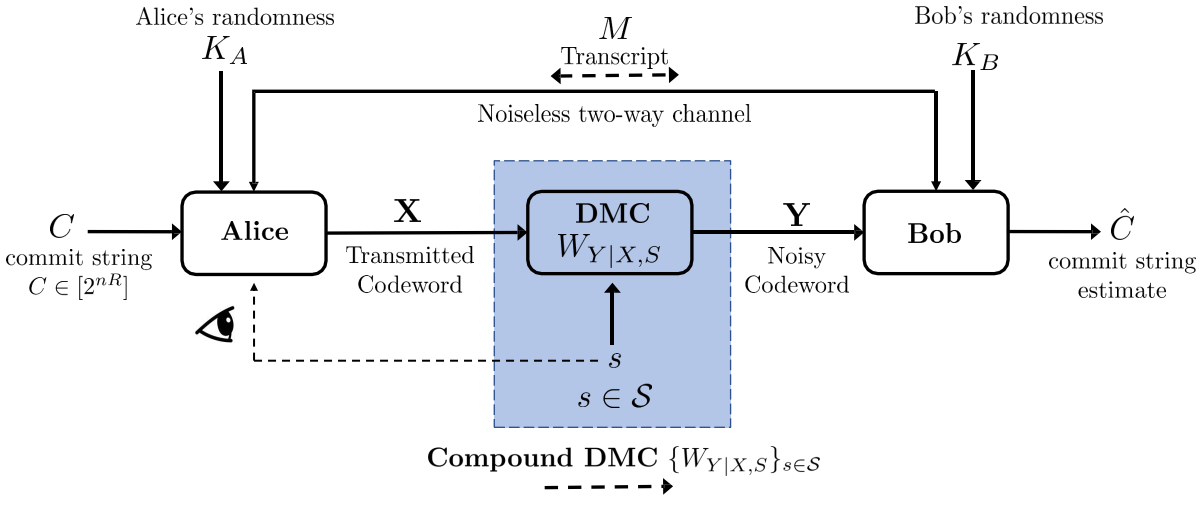

Figure 5.2: Commitment over a Compound-DMC when only committer Alice is state-aware

Fig 5.2 depicts the problem setup when only Alice is state-aware while Bob remains oblivious to the instantiated state. The following theorem specifies the commitment capacity for this configuration.

Theorem 5.2. *The commitment capacity of the a non-redundant compound-DMC* $\{W_{Y|X,S}\}_{s\in\mathcal{S}}$ *when only the committer Alice is state-aware is given by*

$$\mathbb{C} = \min_{s} \max_{P_X} H(X|Y_s).$$

5.5.2 Case II: Only receiver is state-aware

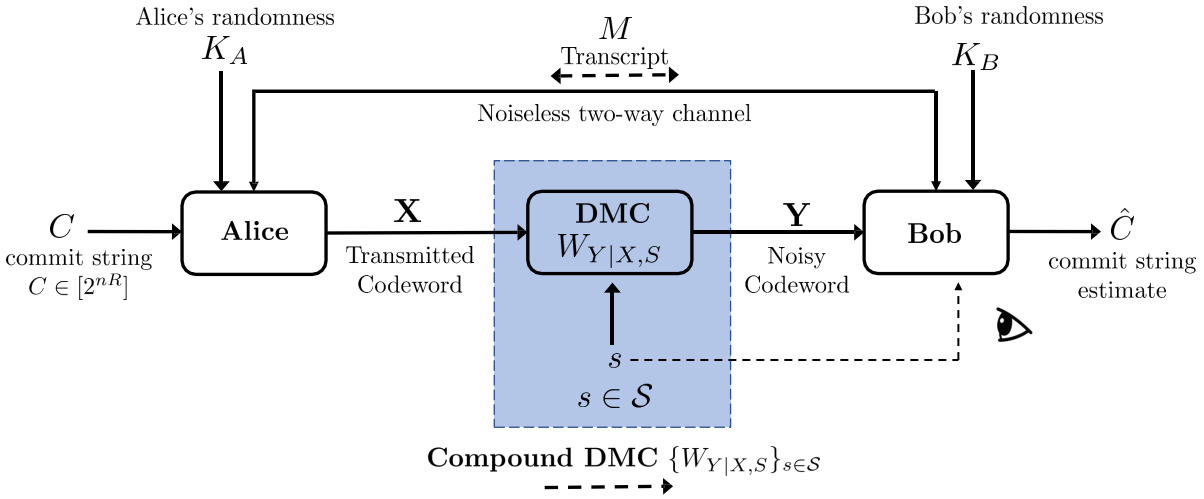

Figure 5.3: Commitment over a Compound-DMC when only receiver Bob is state-aware

Here we depict the setup where only receiver Bob is state-aware in Fig 5.3. Our result for this configuration is stated next.

Theorem 5.3. *The commitment capacity of a non-redundant compound-DMC* $\{W_{Y|X,S}\}_{s\in\mathcal{S}}$ *when only the receiver Bob is state-aware is given by*

$$\mathbb{C} = \max_{P_X} \min_{s\in\mathcal{S}} H(X|Y),$$

and equals the commitment capacity of that C-DMC under no state-awareness at either party.

5.5.3 Case III: Both committer and receiver are state-aware

Fig 5.4 depicts the scenario when both Alice and Bob are state-aware and know the instantiated state precisely.

Theorem 5.4. *The commitment capacity of a non-redundant compound-DMC* $\{W_{Y|X,S}\}_{s\in\mathcal{S}}$ *when both committer Alice and receiver Bob are state-aware is given by*

$$\mathbb{C} = \min_{s\in\mathcal{S}} \max_{P_X} H(X|Y),$$

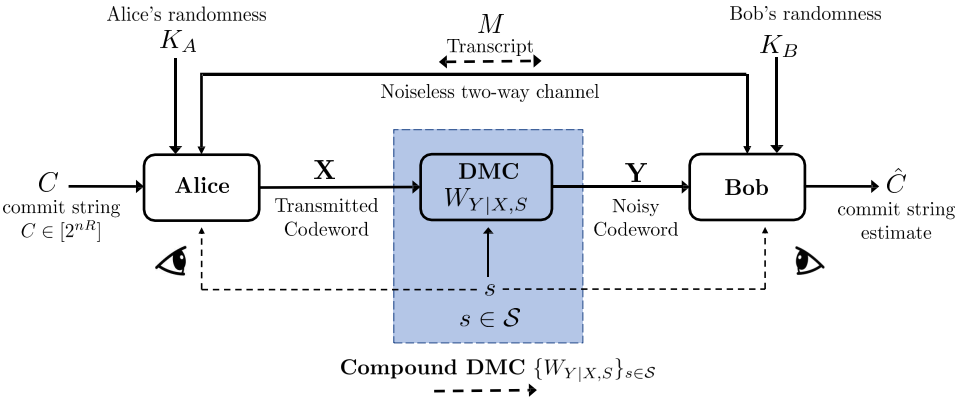

Figure 5.4: Commitment over a C-DMC when both committer Alice and receiver Bob are state-aware

As pointed out in section 3.2, a Compound-DMC with two sided awareness is not different from a DMC of some arbitrary state getting instantiated. The converse for the larger commitment capacity expression when committer Alice is state-aware follows largely along the lines of the converse when no party is state-aware but differs in some key aspects. The specific differences are outlined here.

The *weaker* rate upper bound for the compound-DMC when committer Alice is state-aware can be derived by appropriately tweaking the analysis. In particular, our converse for that model will proceed along the lines of the above converse until (5.8) to get the following rate bound:

$$R \leq H(X|Y_s) + \epsilon_n'' + \epsilon_n'.$$

Now we proceed differently by optimizing first the input distribution P_X:

$$R \leq \max_{P_X} H(X|Y_s) + \epsilon_n'' + \epsilon_n'.$$

The above rate bound is a valid, though weaker bound, and holds for every state $s \in \mathcal{S}$. Thus, optimizing over the choice of $s \in \mathcal{S}$ and letting $n \to \infty$, we get

$$R \leq \min_{s\in\mathcal{S}} \max_{P_X} H(X|Y_s).$$

One can immediately conclude that the commitment throughput over a C-DMC when both parties are state-aware equals the commitment capacity of the *worst-case* DMC induced via the state $s \in \mathcal{S}$; here worst-case is to be understood in terms of *commitment throughput*. Interestingly, from the above results, one can immediately conclude that committer-side state-awareness (recall that state-awareness does not allow the party to control the channel state) can sometimes help increase the commitment throughput over a compound-DMC. On the other hand, only receiver-side state-awareness has no effect on the commitment throughput (w.r.t. the original C-DMC under no state-awareness assumptions). However, note that state-awareness need not always increase commitment capacity. A classic example

is the class of compound-BSCs, where one can easily verify that both expressions, viz., $\min_{s\in\mathcal{S}} \max_{P_X} H(X|Y)$ and $\max_{P_X} \min_{s\in\mathcal{S}} H(X|Y)$, evaluate to the same value $H(\gamma)$ which equals the commitment capacity of the CBSC$[\gamma, \delta]$ [YMBM21]. As such, the commitment capacity over a CBSC$[\gamma, \delta]$ is invariant to state-awareness at either committer Alice and/or receiver Bob. In fact, more generally, one can extend this invariance of commitment capacity under state-awareness to a wider class of appropriately *degraded* noisy channels [GK11]; we leave this exploration as future work.

Chapter 6

Commitment over RECs

In this chapter we will look at another of our main results (published in [BJMY21], [BJMY22a]), the commitment capacity over RECs, which were defined earlier in Definition 3.9. First let us reformulate the problem setup for commitment from figure 3.1 over reverse elastic channels.

6.1 Problem setup

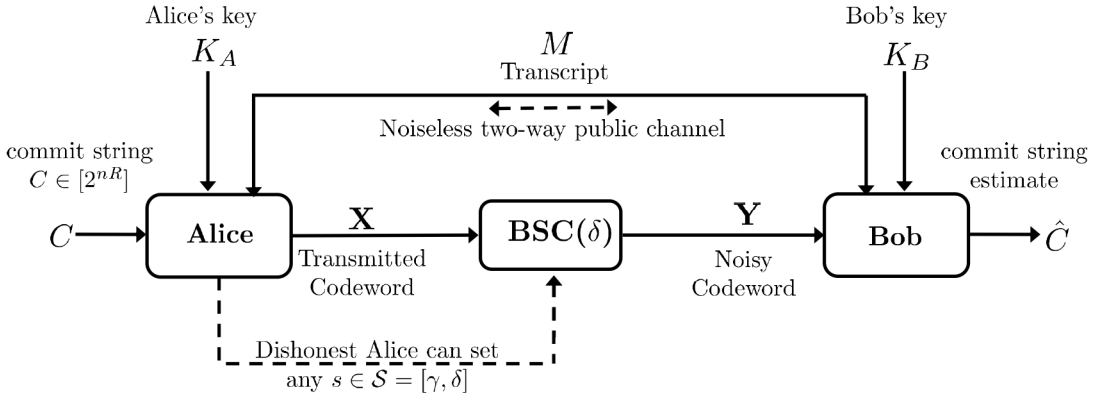

Figure 6.1: The problem setup: commitment over an REC$[\gamma, \delta]$

In figure 6.1, we specialise the commitment problem setup of figure 3.1 to RECs. The problem comprises two mutually distrustful parties, the *committer* Alice and the *receiver* Bob. Alice seeks to commit to a bit string $C \in [2^{nR}]$, where rate $R > 0$ is specified later. They have access to a one-way (Alice-to-Bob) noisy REC$[\gamma, \delta]$, where $0 < \gamma < \delta < 1/2$ (cf. Definition 3.9). Apart from the REC$[\gamma, \delta]$, Alice and Bob can also communicate over a two-way noiseless authenticated public channel. Alice makes n uses of REC$[\gamma, \delta]$. Let $\mathbf{X}$ denote her channel input; Bob receives its noisy version $\mathbf{Y}$. Both Alice and Bob can privately randomize. Alice's key $K_A \in \mathcal{K}_A$ and Bob's key $K_B \in \mathcal{K}_B$ are independent and generated privately via random experiments; these model the randomness in Alice's and Bob's actions and/or transmissions in the protocol. At any point in time, any message

transmitted by individual parties can depend causally on the information available to them. We have an (n, R)-commitment protocol $\mathscr{P}$, following the procedure in definition 3.1. The security guarantees for $\mathscr{P}$ in the context of commitment are as follows.

- **ϵ-soundness:** Protocol $\mathscr{P}$ is said to be ϵ-sound if for an honest Alice and an honest Bob,
$$\max_{c\in[2^{nR}]} \mathbb{P}\big(T(c, \mathbf{X}, V_B) = 0\big) \leq \epsilon. \tag{6.1}$$

- **ϵ-concealing:** Protocol $\mathscr{P}$ is said to be ϵ-concealing if for an *honest* Alice, under any strategy of Bob,
$$I(C; V_B) \leq \epsilon. \tag{6.2}$$

- **$\epsilon-$bindingness:** Protocol $\mathscr{P}$ is said to be ϵ-binding if for an honest Bob, and any strategy of Alice
$$\max_{s\in[\gamma,\delta]} \mathbb{P}\Big(T(\bar{c}, \bar{\mathbf{x}}, V_B) = 1 \quad \& \quad T(\hat{c}, \hat{\mathbf{x}}, V_B) = 1 \Big| S = s\Big) \leq \epsilon \tag{6.3}$$
for any two pairs $(\bar{c}, \bar{\mathbf{x}})$, $(\hat{c}, \hat{\mathbf{x}})$, $\bar{c} \neq \hat{c}$ and $\bar{\mathbf{x}}, \hat{\mathbf{x}} \in \{0, 1\}^n$.

A rate $R \in [0, 1]$ is said to be *achievable* if for every $\epsilon > 0$, there exists for every n sufficient large, an (n, R)-commitment protocol which is ϵ- sound, ϵ-concealing and ϵ-binding. The supremum of all achievable rates is defined as the *commitment capacity* of the REC$[\gamma, \delta]$, denoted by $\mathbb{C}_{REC[\gamma,\delta]}$.

6.2 Commitment capacity results

The principal contribution of our work in [BJMY21, BJMY22a] is the commitment capacity characterization of the REC$[\gamma, \delta]$.

Theorem 6.1 (REC commitment capacity)**.** *The commitment capacity of the REC$[\gamma, \delta]$, where $0 < \gamma < \delta < 1/2$, is*
$$\mathbb{C}_{REC} = H(\delta) - H(\kappa), \tag{6.4}$$
where $\kappa := \frac{\delta-\gamma}{1-2\gamma}$ and $\delta = \gamma * \kappa$.

Our result proves the conjecture stated in [CDN20] on RECs. A key contribution of our work is the matching rate upper bound (see Section 6.3). Although our converse analysis is inspired by the approach in [CDN20] for UNCs, it has some novel differences. Crucially, we prove our converse under complete generality, unlike the one for UNCs in [CDN20]. In that work, the authors impose a condition where the Markov chain $M \leftrightarrow \mathbf{Y} \leftrightarrow \mathbf{X}$ holds; this is restrictive and commitment protocols in general need not satisfy such a condition (this limitation is also pointed out in [CDN20]). Additionally, for the specific cheating strategy of Alice, the authors leverage a degraded channel structure over the UNC; such a structure is not available over the REC which necessitates a different approach. See Sec. 6.3 for the detailed converse proof.

Our achievability commitment protocol follows Damgård et al.'s construction [DKS99]. In particular, our presentation is inspired by [CDN20]; however, we analyse a soundness criterion where *every* commit string $c \in [2^{nR}]$ is accepted with a probability of at least $1-\epsilon$. This is *stronger* than the corresponding criterion in [CDN20] where on average (over $C \in [2^{nR}]$) soundness is guaranteed. [1] We refine the choice of the protocol parameters for the given REC and analyse soundness, concealment and bindingness (see Section 6.4) of the protocol. An interesting consequence of this work is that even when the malicious party is *adaptively* allowed to set potentially different values $s_i \in [\gamma, \delta]$ for $i \in [n]$, there is essentially no benefit to the said party as no further commitment rate degradation is possible (this is also seen in UNCs; see [DKS99] for instance).

6.3 Converse proof

Consider a sequence of protocols $\{\mathscr{P}\}_{n\geq 1}$. Here every protocol $\mathscr{P}_n$ is ϵ_n-sound, ϵ_n-concealing and ϵ_n-binding, where $\epsilon_n \to 0$ as $n \to \infty$.

Alice's 'achievable' strategy: We analyse the following specific active cheating strategy by Alice, feasible for the REC$[\gamma, \delta]$:[2] If the scheme for active cheating strategies, it would work for passive strategies as well. Alice sets the REC$[\gamma, \delta]$ to a BSC(s), $s \in [\gamma, \delta]$. Correspondingly, she also sets up a 'private' BSC(κ_s), where $\kappa_s := \frac{\delta - s}{1-2s} \geq 0$; we denote the output of this private BSC(κ_s) as Z (the dependence on $s \in \mathcal{S}$ is implicit). Note that essentially the channel from Z to Y (via X) is always[3] a BSC(δ). We show later that Alice's rate-minimizing choice s^* equals γ which results in the tight rate bound we seek.[4]

Such a cheating Alice sends $\mathbf{X}$ over the BSC(s) to Bob, and privately generates $\mathbf{Z}$ by passing $\mathbf{X}$ through the private channel BSC(κ_s); given that the pair $(\mathbf{Z}, \mathbf{Y})$ are 'compatible' over the BSC(δ), we have $\mathbb{P}\big(T(C, \mathbf{Z}, V_B) = 0\big) \leq \epsilon_n$, where T is Bob's test. Let us denote $\tilde{Z} := (Y, Z)$, and let $\tilde{\mathbf{Z}} := (\mathbf{Y}, \mathbf{Z})$.

We now state two useful lemmas used later in our analysis.

Lemma 6.1. *For every $\mathscr{P}_n$ which is ϵ_n-sound and ϵ_n-binding, $H(C|\mathbf{Z}, \mathbf{Y}, K_B, M) \leq n\epsilon'_n$, where $\epsilon'_n(\epsilon_n) \to 0$ as $\epsilon_n \to 0$.*

The proof of this lemma appears in Appendix B.1. Note that our converse holds in full generality (see proof details later); this is quite unlike in the converse for UNCs [CDN20] where the authors require that commitment protocols satisfy the Markov chain $M \leftrightarrow \mathbf{Y} \leftrightarrow \mathbf{X}$, thereby restricting the validity of the rate upper bound to those protocols only.

[1] It is known that for some problems such a change in the criterion can lead to different notions of 'capacity' (see, for instance, [LN98]). However, commitment capacity remains the same for both *average* and *maximal* soundness criteria here.

[2] Note that fixing such a strategy gives us an upper bound on rate; in our case, this bound will prove tight.

[3] This follows from noting that $\kappa_s \otimes s = \kappa_s(1-s) + (1-\kappa)s$ equals δ for every $s \in [\gamma, \delta]$.

[4] Another rate bound, for instance, can be obtained by assessing the case when Alice is 'honest', and sets $s = \delta$. However, it is not hard to argue that the resulting rate bound $R \leq H(\delta)$ will only be 'weak'.

Let $\tilde{\mathbf{Z}}^i := (\tilde{Z}_1, \tilde{Z}_2, \cdots, \tilde{Z}_i)$ and let $\hat{\mathbf{Y}}^i := (Y_i, Y_{i+1}, \cdots, Y_n)$. The following lemma is stated without proof (the proof follows directly from [CK78]).

Lemma 6.2 ([CK78]). *Let $W := (K_B, M)$. Then,*

$$I(C; \tilde{\mathbf{Z}}|W) - I(C; \mathbf{Y}|W) = \sum_{i=1}^{n} [I(C; \tilde{Z}_i|W, \tilde{\mathbf{Z}}^{i-1}, \hat{\mathbf{Y}}^{i+1}) - I(C; Y_i|W, \tilde{\mathbf{Z}}^{i-1}, \hat{\mathbf{Y}}^{i+1})]. \tag{6.5}$$

We now bound the rate R of the commitment protocol $\mathscr{P}_n$:

$$\begin{aligned}
nR &= H(C) \\
&= H(C|V_B) + I(C; V_B) \\
&\overset{(a)}{\leq} H(C|\mathbf{Y}, K_B, M) + \epsilon_n \\
&\overset{(b)}{=} H(C|\mathbf{Y}, K_B, M) - H(C|\mathbf{Y}, \mathbf{Z}, K_B, M) \\
&\quad + H(C|\mathbf{Y}, \mathbf{Z}, K_B M) + \epsilon \\
&\overset{(c)}{\leq} H(C|\mathbf{Y}, K_B, M) - H(C|\mathbf{Y}, \mathbf{Z}, K_B, M) + n\epsilon'_n + \epsilon_n \\
&\overset{(d)}{=} I(C; \mathbf{Y}, \mathbf{Z}|K_B, M) - I(C; \mathbf{Y}|K_B, M) + n\epsilon'_n + \epsilon_n \\
&\overset{(e)}{=} I(C; \tilde{\mathbf{Z}}|K_B, M) - I(C; \mathbf{Y}|K_B, M) + n\epsilon'_n + \epsilon_n \\
&\overset{(f)}{\leq} \sum_{i=1}^{n} [I(C; \tilde{Z}_i|K_B, M, \tilde{Z}^{i-1}, \hat{Y}^{i+1}) - I(C; Y_i|K_B, M, \tilde{Z}^{i-1}, \hat{Y}^{i+1})] + n\epsilon'_n + \epsilon_n
\end{aligned} \tag{6.6}$$

where we have

(a) as $\mathscr{P}_n$ is ϵ_n-concealing, and from the definition of V_B.

(b) by adding and subtracting $H(C|\mathbf{Y}, \mathbf{Z}, K_B, M)$

(c) from Lemma 6.1

(d) by adding and subtracting $H(C|K_B, M)$

(e) from the definition of $\tilde{\mathbf{Z}}$

(f) from Lemma 6.2.

To proceed from (6.6), let us define an independent random variable $L \sim \text{Unif}([n])$. Also, let $U := (K_B, M, \tilde{\mathbf{Z}}^{L-1}, \hat{\mathbf{Y}}^{L+1}, L)$ $V := (U, C)$. Observe that U depends only on $\tilde{Z}_i$, $i < L$, and and Y_j, $j > L$. Furthermore, Y_L is a trivially degraded version of $\tilde{Z}_L = (Y_L, Z_L)$. Thus, we have the following Markov chain: $U \leftrightarrow V \leftrightarrow X \leftrightarrow \tilde{Z} \leftrightarrow Y$.

We now use these facts to simplify (6.6) as follows:

$$\begin{aligned}
R &\overset{(a)}{\leq} \sum_{i=1}^{n} \mathbb{P}(L=i)[I(C;\tilde{Z}_L|K_B,M,\tilde{Z}^{L-1},\hat{Y}^{L+1},L=i) \\
&\quad - I(C;Y_L|K_B,M,\tilde{Z}^{L-1},\hat{Y}^{L+1},L=i)] + \epsilon'_n + \tilde{\epsilon}_n \\
&\overset{(b)}{=} I(C;\tilde{Z}|U) - I(C;Y|U) + \epsilon'_n + \tilde{\epsilon}_n \\
&\overset{(c)}{=} I(V;\tilde{Z}|U) - I(V;Y|U) + \epsilon'_n + \tilde{\epsilon}_n \\
&\overset{(d)}{=} I(V;\tilde{Z}) - I(U;\tilde{Z}) - I(V;Y) - I(U;Y) + \epsilon'_n + \tilde{\epsilon}_n \\
&\overset{(e)}{=} I(X;\tilde{Z}) - I(X;Y) - [I(X;\tilde{Z}|V) - I(X;Y|V)] \\
&\qquad\qquad - [I(U;\tilde{Z}) - I(U;Y)] + \epsilon'_n + \tilde{\epsilon}_n \\
&\overset{(f)}{\leq} I(X;\tilde{Z}) - I(X;Y) + \epsilon'_n + \tilde{\epsilon}_n
\end{aligned} \tag{6.7}$$

where we have

(a) from definition of L, and letting $\tilde{\epsilon}_n := \frac{\epsilon_n}{n}$.

(b) from noting that $U = (K_B, M, \tilde{\mathbf{Z}}^{L-1}, \hat{\mathbf{Y}}^{L+1}, L)$ and letting $X := X_L$, $Y := Y_L$ and $\tilde{Z} := \tilde{Z}_L$.

(c) from noting that $V = (U, C)$.

(d) from the chain rule of mutual information

(e) from the Markov chains $V \leftrightarrow X \leftrightarrow \tilde{Z}$ and $V \leftrightarrow X \leftrightarrow Y$, and non-negativity of the trailing two terms in brackets.

(f) from the Markov chain $X \leftrightarrow \tilde{Z} \leftrightarrow Y$ as Y is a degraded version of $\tilde{Z}$.

Note that (6.7) holds $\forall s \in [\gamma, \delta]$. Letting $n \to \infty$ and optimizing Alice's choice $s \in [\gamma, \delta]$ (recall her cheating strategy), we have

$$\begin{aligned}
R &\leq \min_{s\in[\gamma,\delta]} I(X;YZ) - I(X;Y) \\
&\overset{(a)}{\leq} \max_{P_X} \min_{s\in[\gamma,\delta]} I(X;YZ) - I(X;Y) \\
&\overset{(b)}{=} H(\delta) - H\left(\frac{\delta-\gamma}{1-2\gamma}\right) \\
&\overset{(c)}{=} \mathbb{C}_{REC},
\end{aligned}$$

where (a) follows by optimizing the input distribution P_X, and (b) follows by optimizing the expression $I(X;YZ) - I(X;Y) = H(X|Y) - H(X|YZ)$ which occurs at input $X \sim$ Bernoulli(1/2) and $s^* = \gamma$; the optimum value equals $H(\delta) - H(\frac{\delta-\gamma}{1-2\gamma})$. Finally, (c) follows from (6.4).

6.4 Achievability proof

Following [DKS99], our protocol utilizes two rounds of random hash exchange challenges and a strong randomness extractor based on 2-universal hash functions; our presentation is inspired by [CDN20]. The two rounds[5] of hash challenges essentially *bind* Alice to her choice in the commit phase thereby ensuring Bob's test T can detect any cheating attempt by Alice during the reveal phase. The strong randomness extractor extracts a secret key (note that the leftover hash lemma [DRS04a] allows us to quantify the size of this key). This key is then XOR-ed with the commit string c to realize a *one-time pad* scheme, which conceals the committed string against Bob in the commit phase.

6.4.1 Achievabile scheme

Here are the details of our protocol. The rate $R := H(\delta) - H(\kappa) - \beta_3$, where the choice of $\beta_3 > 0$ is specified later. Let $\mathcal{G}_1 := \{g_1 : \{0,1\}^n \to \{0,1\}^{n(H(\kappa)+\beta_1)}\}$ be a $4n$-universal hash family, where $\kappa := \frac{\delta-\gamma}{1-2\gamma}$ and $\beta_1 > 0$ is a small enough constant. Let $\mathcal{G}_2 := \{g_2 : \{0,1\}^n \to \{0,1\}^{n\beta_2}\}$ be a $2-$universal hash family, where $\beta_2 > 0$ is a small enough constant. Let $\mathcal{E} := \{\text{ext} : \{0,1\}^n \to \{0,1\}^{nR}\}$ be a $2-$universal hash family, where $\beta_3 > 0$ is chosen such that $\beta_3 > \beta_1 + \beta_2$.[6] We now describe the commit and reveal phases:

Commit Phase: For Alice to commit string $c \in [2^{nR}]$, the protocol proceeds as follows:

(C1) Given c, Alice sends $\mathbf{X} \sim \text{Bernoulli}(1/2)$ independent and identically distributed (i.i.d.) over the $\text{REC}[\gamma, \delta]$; Bob receives $\mathbf{Y}$.

(C2) Bob chooses a hash function $G_1 \sim \text{Unif}(\mathcal{G}_1)$, and sends the description of G_1 to Alice over the noiseless link.

(C3) Alice computes $G_1(\mathbf{X})$ and sends it to Bob over the noiseless link.

(C4) Bob picks another hash function $G_2 \sim \text{Unif}(\mathcal{G}_2)$, and sends its description to Alice over the noiseless link.

(C5 Alice computes the hash $G_2(\mathbf{X})$ and sends it over the noiseless link to Bob.

(C6) Alice chooses an extractor function $\text{Ext} \sim \text{Unif}(\mathcal{E})$ and sends[7] $Q = c \oplus \text{Ext}(\mathbf{X})$ and the description of Ext to Bob over the noiseless link.

Reveal phase: Alice proceeds as follows:

(R1) Having received $\mathbf{Y} = \mathbf{y}$, Bob creates list $\mathcal{L}(\mathbf{y})$ of vectors given by:[8]

$$\mathcal{L}(\mathbf{y}) := \{\mathbf{x} \in \{0,1\}^n : n(\delta - \alpha_1) \leq d_H(\mathbf{x}, \mathbf{y}) \leq n(\delta + \alpha_1)\}.$$

[5] We need two rounds of hash challenge to circumvent a non-trivial rate loss that arises in the single hash challenge due to the *birthday paradox*; see [CDN20] where it is discussed in detail.

[6] Note that R can be made arbitrarily close to $\mathbb{C}_{REC}$.

[7] In the following expression, operator $\oplus$ denotes component-wise XOR.

[8] Here the parameter $\alpha_1 > 0$ is chosen appropriately small.

(R2) Alice announces $(\tilde{c}, \tilde{\mathbf{x}})$ to Bob over the noiseless link.

(R3) Bob accepts $\tilde{c}$ if all the following four conditions are satisfied: (i) $\tilde{\mathbf{x}} \in \mathcal{L}(\mathbf{y})$, (ii) $g_1(\tilde{\mathbf{x}}) = g_1(\mathbf{x})$, (iii) $g_2(\tilde{\mathbf{x}}) = g_2(\mathbf{x})$ and (iv) $\tilde{c} = q \ \oplus \text{ext}(\tilde{\mathbf{x}})$. Else, he rejects $\tilde{c}$ and outputs '0'.

6.4.2 Analysis of security guarantees

We now analyse and prove the security guarantees in detail for the above defined (n, R)-commitment scheme:

6.4.2.1 $\epsilon-$*sound*

For our protocol to be ϵ-sound, it is sufficient to show that $\mathbb{P}(\mathbf{X} \notin \mathcal{L}(\mathbf{Y})) \leq \epsilon$ when both the parties, Alice and Bob, are honest; the proof of this fact follows from classic Chernoff bounds. We skip the details.

6.4.2.2 ϵ*-concealing*

It is known that a positive rate commitment protocol is $\epsilon-$concealing, where $\epsilon > 0$ is *exponentially decreasing* in blocklength n, if it satisfies the *capacity-based secrecy* (cf. [DPP98, Def. 3.2]) and vice versa. We use a well established relation between *capacity-based secrecy* and the *bias-based secrecy* (cf. [DPP98, Th. 4.1]) to prove that our protocol is ϵ-concealing.

To begin, we prove that our protocol satisfies bias-based secrecy by essentially proving the perfect secrecy of the key $\text{Ext}(\mathbf{X})$; here we crucially use the *leftover hash* lemma. Several versions of this lemma exists (cf. [ILL89,DRS04a,HILL99] for instance); we use the following:

Lemma 6.3. *Let $\mathcal{G} = \{G : \{0,1\}^n \to \{0,1\}^l\}$ be a family of universal hash functions. Then, for any hash function G chosen uniformly at random from $\mathcal{G}$, and W*

$$\|(P_{G(W),G} - P_{U_l,G})\| \leq \frac{1}{2}\sqrt{2^{-H_\infty(W)}2^l}$$

where $U_l \sim Unif\big(\{0,1\}^l\big)$.

We then establish the following lower bound:

Lemma 6.4. *For any $\epsilon_1 > 0, \zeta > 0$ and n sufficiently large,*

$$\begin{aligned} &H_\infty^{\epsilon_1}(\mathbf{X}|\mathbf{Y}, G_1(\mathbf{X}), G_1, G_2(\mathbf{X}), G_2) \\ &\quad \geq n(H(\delta) - \zeta - H(\kappa) - \beta_1 - \beta_2) - \log(\epsilon_1^{-1}) \end{aligned} \tag{6.8}$$

The proof appears in Appendix B.2. Next, we use Lemma 8.1 to show that the distribution of the secret key $\text{Ext}(\mathbf{X})$ is statistically close to a uniform distribution thereby achieving bias-based secrecy. Let us fix $\epsilon_1 := 2^{-n\alpha_2}$, where $\alpha_2 > 0$ is an arbitrary small constant. We

make the following correspondence in Lemma 8.1: $G \leftrightarrow \text{Ext}$, $W \leftrightarrow \mathbf{X}$ and $l \leftrightarrow nR$ to get the following:

$$\begin{aligned}
&\|P_{\text{Ext}(\mathbf{X}),\text{Ext}} - P_{U_l,\text{Ext}}\| \\
&\overset{(a)}{\leq} \frac{1}{2}\sqrt{2^{-H_\infty(\mathbf{X})}2^{nR}} \\
&\overset{(b)}{\leq} \frac{1}{2}\sqrt{2^{-H_\infty(\mathbf{X}|\mathbf{Y},G_1(\mathbf{X}),G_1,G_2(\mathbf{X}),G_2)}2^{nR}} \\
&\overset{(c)}{\leq} \frac{1}{2}\sqrt{2^{-n(H(\delta)-\zeta-H(\kappa)-\beta_1-\beta_2-\alpha_2)}2^{n(H(\delta)-H(\kappa)-\beta_3))}} \\
&= \frac{1}{2}\sqrt{2^{n(\zeta+\beta_1+\beta_2+\alpha_2-\beta_3))}} \\
&\overset{(d)}{\leq} 2^{-n\alpha_3}
\end{aligned} \tag{6.9}$$

where, $\alpha_3 > 0$ and n is sufficiently large. Here,

(a) follows directly from the leftover hash lemma (cf. Lemma 8.1)

(b) follows from the fact that conditional min-entropy bounds min-entropy.

(c) follows from (A.6) and noting that the choice of 2-universal hash function Ext is random and uniform from the set $\mathcal{E} : \{0,1\}^n \to \{0,1\}^{n(H(\delta)-H(\kappa)-\beta_3)}$.

(d) follows from noting that β_3 is chosen such that $\zeta + \beta_1 + \beta_2 + \alpha_2 - \beta_3 < 0$; here, we note that α_2 is an arbitrarily chosen (small enough) constant, and $\zeta > 0$ can be made arbitrarily small for n sufficiently large. As such, a choice of $\beta_3 > \beta_1 + \beta_2$ is sufficient.

From (8.23) and Lemma 8.1, it follows that we can extract $n(H(\delta) - H(\kappa) - \beta_3)$ almost uniformly random bits which proves the security of the secret key; this guarantees that our commitment protocol satisfies bias-based secrecy (cf. [DPP98, Def. 3.1]). Recall from our discussion earlier (see also [DPP98, Th. 4.1]) that bias-based secrecy under *exponentially decaying* statistical distance, as in (8.23), implies capacity-based secrecy; hence, it follows that for n sufficiently large, $I(C; V_B) \leq \epsilon$ and our protocol is ϵ-concealing.

6.4.2.3 *ϵ-binding*

Let us assume that a dishonest Alice sets the crossover probability of the REC$[\gamma, \delta]$ to $s \in [\gamma, \delta]$; let us define $\kappa_s := \frac{\delta - s}{1-2s}$. Note that $\kappa = \kappa_\gamma = \frac{\delta-\gamma}{1-2\gamma}$. Let $\mathbf{X} = \mathbf{x}$ be the transmitted bit string and $\mathbf{Y} = \mathbf{y}$ be the bit string received by Bob's over the BSC(s). Alice can cheat successfully by confusing Bob in the reveal phase only if she can find two distinct bit strings $\mathbf{x}'$ and $\tilde{\mathbf{x}}$ such that (i) $\mathbf{x}', \tilde{\mathbf{x}} \in \mathcal{L}(\mathbf{y})$, and (ii) $\mathbf{x}'$, $\tilde{\mathbf{x}}$ pass the two rounds of sequential random hash exchange challenge (w.r.t hash functions $G_1(\cdot)$ and $G_2(\cdot)$). Let $\mathcal{A}$ denote all such candidate vectors that appear in Bob's list (*prior* to the hash challenges) that Alice can use to confuse Bob; the following claim shows that $\mathcal{A}$ can be exponentially large.

Claim 6.1. *Given any $\eta > 0$, for n sufficiently large*

$$|\mathcal{A}| \leq 2^{n(H(\kappa)+\eta)} \tag{6.10}$$

The proof appears in Appendix B.2.1. Note that, essentially, we can conclude that the choice of $s = \gamma$ is the 'best' choice for a cheating Alice (such a choice maximizes $|\mathcal{A}|$), i.e., Alice can be no worse than when it fixes the REC to a BSC(γ). We will choose $0 < \eta < \beta_1$ later (cf. Claim 8.5).

We now show that our choice of hash functions $G_1(\cdot)$ and $G_2(\cdot)$ allows us to essentially 'trim' down this set $\mathcal{A}$ of 'confusable' vectors all the way down to none. Recall that Alice's choice in the commit phase is $\mathbf{x}$. For a given hash value $h_1 \in \{0,1\}^{n(H(\kappa)+\beta_1)}$ sent by Alice, let

$$I_i(h_1) := \begin{cases} 1 & \text{if } G_1(\mathbf{x}_i) = G_1(\mathbf{x}) = h_1 \\ 0 & \text{otherwise.} \end{cases} \tag{6.11}$$

Also, let

$$I(h_1) := \sum_{i=1}^{|\mathcal{A}|} I_i(h_1) \tag{6.12}$$

denotes the total number of hash collisions with hash value h_1. Then, the following holds when $0 < \eta < \beta_1$:

Claim 6.2. $\mathbb{P}\left(\exists h_1 \in \{0,1\}^{n(H(\kappa)+\beta_1)} : I(h_1) > 8n+1\right) \to 0$ *exponentially in* n *as* $n \to \infty$.

This implies that the size of the 'confusable' set *after* the first hash challenge via G_1 for any h_1 is larger that $8n+1$ with exponentially small probability (in block length n).

Conditioned on the event $I(h_1) < 8n+1, \forall h_1$, which occurs with high probability (w.h.p.), we now analyse the size of the 'confusable' set *after* the second hash challenge via G_2; let $\mathcal{F}_{h_1}$ denote this set of 'confusable' vectors after the second hash challenge for a given h_1. We prove the following claim (proof in Appendix B.3.1):

Claim 6.3. *For every* $h_1 \in \{0,1\}^{n(H(\kappa)+\beta_1)}$*, we have for* n *sufficiently large*

$$\begin{aligned} &\mathbb{P}\left(\exists \mathbf{x} \neq \mathbf{x}' \in \mathcal{F}_{h_1} : G_2(\mathbf{x}) = G_2(\mathbf{x}') \middle| I(h_1) \leq 8n+1\right) \\ &\quad \leq 2^{-n\frac{\beta_2}{2}} \end{aligned} \tag{6.13}$$

As (6.13) holds for every h_1, and noting that[9] $\beta_2 > 0$, we now choose n large enough to prove that our commitment protocol is $\epsilon-$binding.

6.5 Key Observations

From our result in Theorem 6.1 and the corresponding results for ECs and UNCs (cf. [CDN20]), we can establish that $\mathbb{C}_{EC[\gamma,\delta]} > \mathbb{C}_{REC[\gamma,\delta]} > \mathbb{C}_{UNC[\gamma,\delta]}$ for any specified γ, δ values. Refer Fig. 6.2 where we plot the capacities of these *unreliable* channels along with the BSC(δ).

Remark 6.1 (Positive commitment throughput)**.** *Unlike UNC*$[\gamma,\delta]$ *which may have zero commitment capacity (this occurs when* $\delta \geq \gamma * \gamma := 2\gamma(1-\gamma)$*, see [CDN20]), an REC*$[\gamma,\delta]$ *always exhibits positive commitment capacity for the specified range of parameters. Note that the same is true for an EC*$[\gamma,\delta]$ *whose capacity is* $\mathbb{C}_{EC[\gamma,\delta]} = H(\gamma) > 0$ *[CDN20].*

[9]Recall that $\beta_2 > 0$ is a fixed parameter in our protocol.

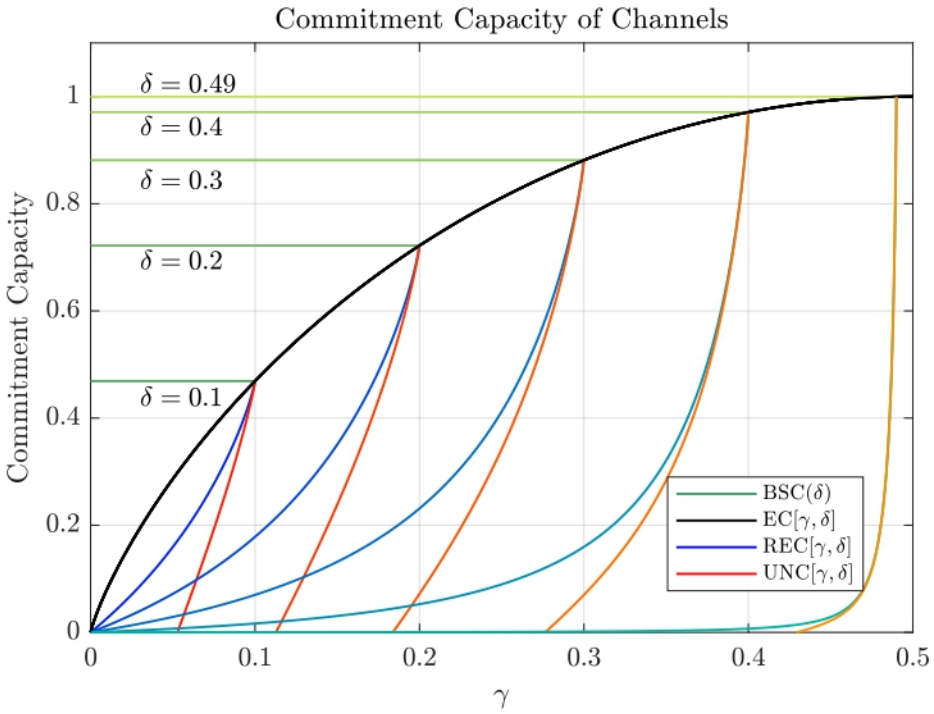

Figure 6.2: Variation of commitment capacities (w.r.t. γ) for different channels. Curves are presented for different values of $\delta \in (0, 1/2)$.

The following is a key takeaway from this work: commitment throughput over RECs is strictly lower than that over ECs (under identical γ, δ parameters) when parties can malicious alter the channel characteristics. This fact reveals an interesting *asymmetry* in commitment over such unreliable channels with *one-sided elasticity*, i.e., channels which afford elasticity (i.e., capability to alter the channel) to exactly one of the cheating parties exclusively. Essentially, a cheating *committer* Alice *always* degrades the commitment throughput more than a cheating *receiver* Bob. This is in stark contrast to the *symmetric* scenario under *honest-but-curious* parties which lack malicious channel control; the REC (as well as EC) essentially defaults to a classic BSC(δ) here. For such *honest-but-curious* adversaries, RECs and ECs offer identical commitment throughput.

Figure 6.3 illustrates the asymmetry in the commitment capacity for the RECs and the ECs more succinctly; in figure 6.3 we present the joint 'equal-capacity' contours for RECs and ECs. As can be seen in Fig. 6.3, for a fixed $\delta \in (0, 1/2)$, a cheating receiver in EC[γ, δ] requires considerably 'larger' receiver-side elasticity, characterized by a lower γ (the axes plot a normalized value of γ w.r.t. δ), to effect the same degradation of the commitment throughput than a cheating committer in an REC[γ, δ]. Furthermore, as δ increases, one can observe that the skew in the asymmetry, which essentially characterizes the committer-

receiver 'mismatch' in 'elastic-capabilities', is more pronounced.

Seen from another perspective, for a fixed $\delta \in (0, 1/2)$, the *gap* in the commitment capacity $\Omega_\delta(\gamma) := \mathbb{C}_{EC[\gamma,\delta]} - \mathbb{C}_{REC[\gamma,\delta]}$ is strictly positive (note that $0 < \gamma < \delta < 1/2$), though it is *not* a constant (see Fig. 6.2). Furthermore, this gap $\Omega_\delta(\cdot)$ increases as δ increases in the range $(0, 1/2)$; it can be shown that $\Omega_\delta(\gamma)$ is concave in γ (for fixed δ), and $\Omega_\delta(\gamma)$ is maximized when $\gamma \otimes \gamma = \delta$, i.e., for a unique optimizer $\gamma^*(\delta) = \frac{1-\sqrt{1-2\delta}}{2}$. It is pertinent to note that $\gamma^*(\delta)$ is exactly the value for which the corresponding UNC$[\gamma^*, \delta]$ has zero capacity.

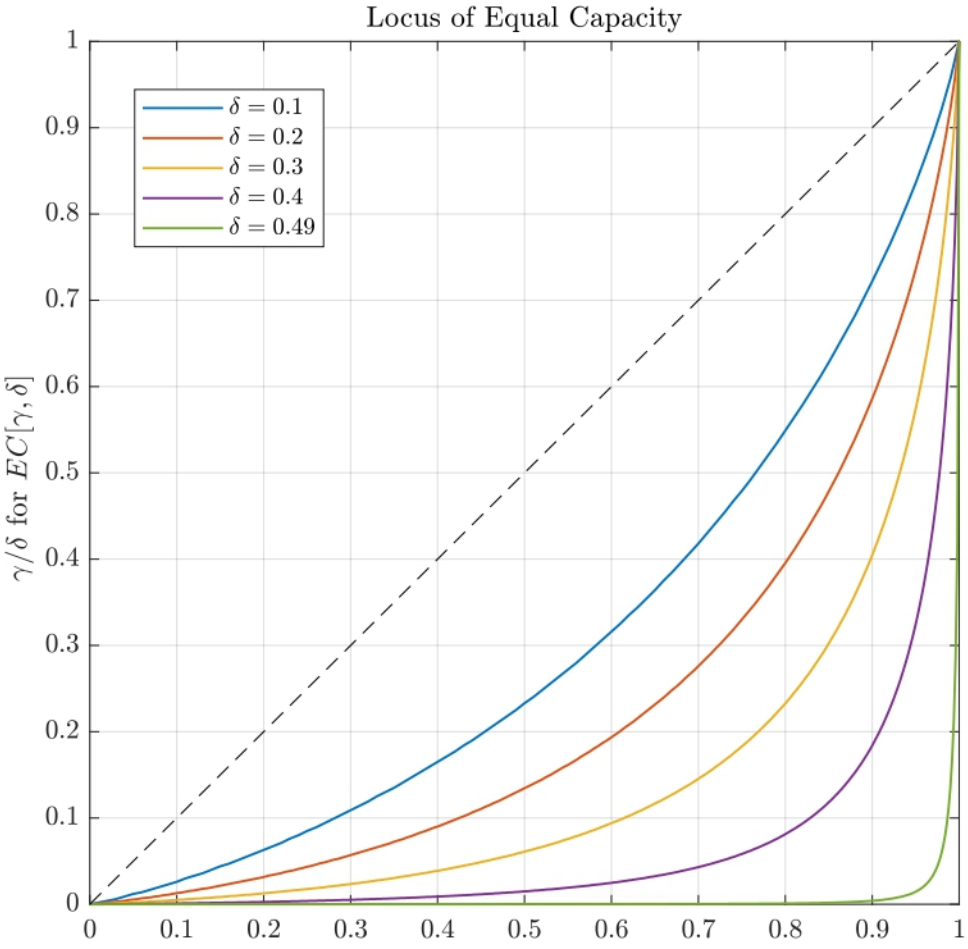

Figure 6.3: The EC$[\gamma, \delta]$ versus REC$[\gamma, \delta]$ commitment capacity contour plotted when those capacities are identical. Curves are presented for different values of $\delta \in (0, 1/2)$.

Chapter 7

Commitment over Asymmetric UNCs

Here we study commitment over a more general unreliable channel model that encompasses all the works on elastic channels, reverse elastic channels and unfair noisy channels.

7.1 Problem setup

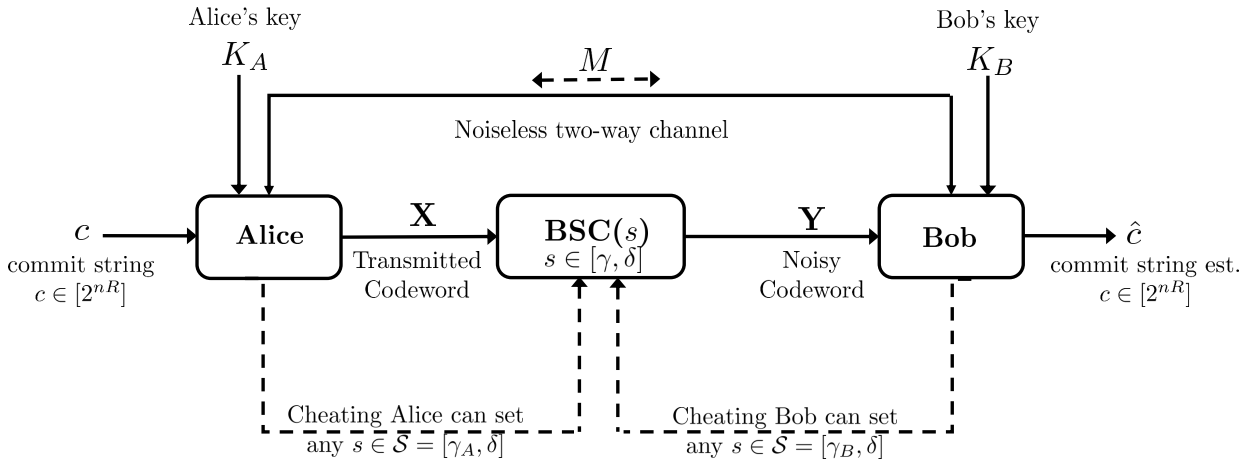

Figure 7.1: The problem setup: commitment over a Asymmetric-UNC$[\gamma^2, \delta^2]$

The commitment problem over an Asymmetric-UNC$[\gamma, \gamma_A, \gamma_B, \delta]]$ is depicted in Fig. 8.1. Here two mutually distrustful parties, the *committer* Alice and the *receiver* Bob seek to realize commitment over Alice's random bit string $C \in [2^{nR}]$, where $R > 0$ is specified later. Alice and Bob have access to a one-way (from Alice to Bob) noisy channel, viz., a Asymmetric-UNC$[\gamma, \gamma_A, \gamma_B, \delta]]$, where $0 < \gamma_A, \gamma_B \leq \gamma < \delta < 1/2$ (cf. Definition 3.12). Apart from the Asymmetric-UNC$[\gamma, \gamma_A, \gamma_B, \delta]]$, Alice and Bob can also communicate over a two-way *noiseless*, *authenticated* and *public* channel. Alice makes n uses of Asymmetric-UNC$[\gamma, \gamma_A, \gamma_B, \delta]$. Let $\mathbf{X}$ denote her transmission on the channel. Bob receives a noisy version $\mathbf{Y}$ of Alice's transmission $\mathbf{X}$. We assume that both Alice and Bob can privately randomize.

We denote by $K_A \in \mathcal{K}_A$ and $K_B \in \mathcal{K}_B$, Alice's and Bob's random keys respectively. These are independent and privately generated keys. Note that the keys essentially represent the randomness in Alice's and Bob's actions and/or transmissions. At any point in time, any message transmitted by individual parties can depend causally on the information available to them. Say $\mathscr{P}$ is an $(n, R)-$commitment protocol (from definition 3.1) over an Asymmetric-UNC$[\gamma, \gamma_A, \gamma_B, \delta]$. The security features corresponding are

- **ϵ-soundness:** Protocol $\mathscr{P}$ is said to be ϵ-sound if for an honest Alice and an honest Bob,
$$\max_{s\in[\gamma,\delta]} \max_{c\in[2^{nR}]} \mathbb{P}\big(T(c, \mathbf{X}, V_B) = 0 \Big| S = s\big) \leq \epsilon. \tag{7.1}$$
- **ϵ-concealing:** Protocol $\mathscr{P}$ is said to be ϵ-concealing if for an *honest* Alice, under any strategy of Bob,
$$\max_{s\in[\gamma_B,\delta]} I(C; V_B \Big| S = s) \leq \epsilon. \tag{7.2}$$
- **$\epsilon-$bindingness:** Protocol $\mathscr{P}$ is said to be ϵ-binding if for an honest Bob, and any strategy of Alice
$$\max_{s\in[\gamma_A,\delta]} \mathbb{P}\Big(T(\bar{c}, \bar{\mathbf{x}}, V_B) = 1 \quad \& \quad T(\hat{c}, \hat{\mathbf{x}}, V_B) = 1 \Big| S = s\Big) \leq \epsilon \tag{7.3}$$
for any two pairs $(\bar{c}, \bar{\mathbf{x}})$, $(\hat{c}, \hat{\mathbf{x}})$, $\bar{c} \neq \hat{c}$ and $\bar{\mathbf{x}}, \hat{\mathbf{x}} \in \{0, 1\}^n$.

A rate $R \in [0, 1]$ is said to be *achievable* if for every $\epsilon > 0$, there exists for every n sufficient large, an (n, R)-commitment protocol which is ϵ- sound, ϵ-concealing and ϵ-binding.

7.2 Impossibility and achievability results

We find that commitment is not possible over Asymmetric-UNCs of certain parameters.

Theorem 7.1 (Impossibility over Asymmetric-UNCs)**.** *For a Asymmetric-UNC$[\gamma, \gamma_A, \gamma_B, \delta]$, the commitment capacity $\mathbb{C}_{A-UNC} = 0$ if $\delta \geq \gamma_A * \gamma_B$.*

This result conclusively identifies sufficient conditions for impossibility of even *single-bit* commitment over Asymmetric-UNCs. See Section 7.3 for the proof.

Remark 7.1. *Our converse in inspired in spirit by the one for binary UNCs in [DKS99]. A key fact used in the converse is the classic result of impossibility of commitment over noiseless links (even when parties can privately randomize). Our proof of the converse continues to use this same approach. A crucial part of our proof involves analysing a 'more restrictive' channel model called the Passive AUNC$[\gamma_A, \gamma_B, \delta]$ with identical parameters as in the Asymmetric-UNC$[\gamma, \gamma_A, \gamma_B, \delta]$ (see Sec 7.3). We show via a sequence of reductions that Passive AUNC$[\gamma_A, \gamma_B, \delta]$ can be simulated noiselessly, and thus, should preclude commitment. We then leverage this result to show that, as a consequence, commitment is impossible over a Asymmetric-UNC$[\gamma, \gamma_A, \gamma_B, \delta]$.*

Theorem 7.2 (Achievability result over Asymmetric-UNCs)**.** *For Asymmetric-UNC*$[\gamma, \gamma_A, \gamma_B, \delta]$ *with* $\delta < \gamma_A * \gamma_B$*, the commitment capacity* $\mathbb{C}_{AUNC} \geq H_2(\frac{\delta-\gamma_A}{1-2\gamma_A})$

The above inequality evaluates with equality for UNCs, ECs and RECs. Both the results also fully characterise the possibility regime of commitment as the Capacity lowerbound of theorem 7.2 just reaches zero on the boundary of impossibility regime of theorem 7.1, $\delta = \gamma_A * \gamma_B$. That said, a complete information theoretic rate upperbound still remains an open problem.

7.3 Impossibility proof

Claim 7.1. *No* ϵ_1-*sound,* ϵ_2-*concealing,* ϵ_3-*binding* $k-$*bit commitment scheme is possible over noiseless channels for*

$$\epsilon_2 < k(1 - \epsilon_1 - 2^k\epsilon_3) - 2\sqrt{\epsilon_1 + 2^k\epsilon_3}. \tag{7.4}$$

The proof is in Appendix C.1. Let us now define a channel called Passive-AUNC, which is a slightly modified version of the AUNC channel which we studied earlier.

Definition 7.1 (Passive-AUNC)**.** *A Passive AUNC*$[\gamma_A, \gamma_B, \delta]$ *(*$\gamma_A, \gamma_B \leq \delta$*) behaves like a regular BSC*(δ) *when both the users are honest. However a cheating Alice or Bob can get extra side information that can reduce the noise to* γ_A *or* γ_B *respectively from their point of view.*

We will first show that commitment is impossible over Passive-AUNC over some parameter regimes. It follows from here that commitment is not possible over Asymmetric-UNCs as well. Towards the first part we show this claim

Claim 7.2. *A Passive AUNC*$[\gamma_A, \gamma_B, \delta]$ *can be realised noiselessly when* $\delta \geq \gamma_A \circledast \gamma_B$*.*

Proof. We present here a protocol `SimAUNC` that for given γ_A, γ_B and δ, can realise the functionality of n uses of a Passive AUNC$[\gamma_A, \gamma_B, \delta]$ for any given channel input $\mathbf{x} \in [0,1]^n$.

`SimAUNC`$\{\gamma_A, \gamma_B, \delta\}(\mathbf{x})\{$
  Define θ s.t. $\gamma_A \circledast \gamma_B \circledast \theta = \delta$
  Alice passes $\mathbf{x}$ through a local BSC(γ_B) to get $\mathbf{x}_1$
  Alice passes $\mathbf{x}_1$ through a local BSC(θ) to get $\mathbf{x}_2$
  Alice sends $\mathbf{x}_1$, $\mathbf{x}_2$ to Bob noiselessly
  Bob passes $\mathbf{x}_2$ through a local BSC(γ_A) to get $\mathbf{x}^*$
  Ask Alice, Bob to forget $\mathbf{x}_1$, $\mathbf{x}_2$
  Return the resulting views V_A and V_B
$\}$

Here $\mathbf{x}, \mathbf{x}_1, \mathbf{x}_2, \mathbf{x}^* \in [0,1]^n$. To understand how `SimAUNC` correctly realises the functionality of a Passive AUNC, let us analyse over a case by case basis. It is to note here that while honest parties faithfully forget the values of $\mathbf{x}_1$ and $\mathbf{x}_2$, passively cheating parties continue to remember them, but not affecting the protocol in any other way. An actively cheating party on the other hand may change the variables where ever possible involved in the protocol to his/her advantage.

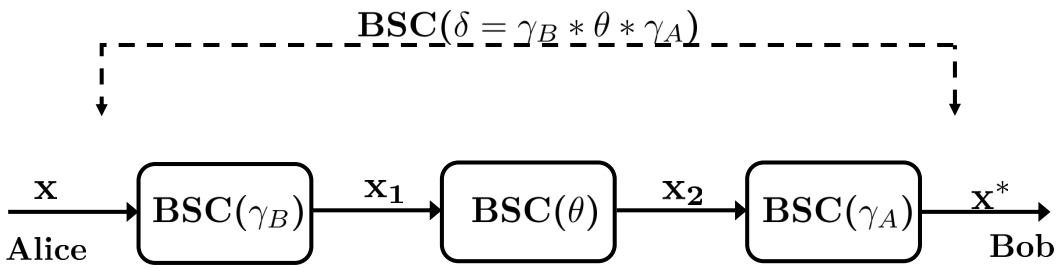

Figure 7.2: Channel structure in $\texttt{SimAUNC}\{\gamma_A, \gamma_B, \delta\}(\mathbf{x})$ and how it simulates the behaviour of a Passive-AUNC$[\gamma_A, \gamma_B, \delta]$ with input $\mathbf{x}$.

(a) **when Alice is honest and Bob is honest:** Here, Alice and Bob follow all the steps in `SimUNC` exactly. For input $\mathbf{x}$, at the end of `SimUNC`, Alice's and Bob's views are $V_A = (\mathbf{x})$, $V_B = (\mathbf{x}^*)$ respectively. It follows from figure 7.2 that the channel between $\mathbf{x}$ and $\mathbf{x}^*$ is a BSCδ. This exactly corresponds to the channel behaviour when an honest Alice sends over $\mathbf{x}$ through Passive AUNC$[\gamma_A, \gamma_B, \delta]$ to an honest Bob. (see Def. 7.1).

(b) **when Alice is passively cheating and Bob is honest:** A passively cheating Alice remembers the values of $\mathbf{x}_1$ and $\mathbf{x}_2$ in addition to that of $\mathbf{x}$, resulting in $V_A = (\mathbf{x}, \mathbf{x}_1, \mathbf{x}_2)$ and $V_B = (\mathbf{x}^*)$. From figure 7.2, the extra knowledge of $\mathbf{x}_2$ brings down Alice's uncertainty of $\mathbf{x}^*$ to BSC(γ_A) in what is otherwise a BSC(δ) as is observed from an honest Bob's perspective. This corresponds to the behaviour of a Passive AUNC$[\gamma_A, \gamma_B, \delta]$ whose channel input is $\mathbf{x}$.

(c) **when Alice is actively cheating and Bob is honest:** Consider a cheating behaviour of Alice who, for input string $\mathbf{x}$, modifies the values of $\mathbf{x}_1$ and $\mathbf{x}_2$ to say $\mathbf{y}_1$ and $\mathbf{y}_2'$ respectively, before sending them over to Bob. This results in views $V_A = (\mathbf{x}, \mathbf{y}_1, \mathbf{y}_2)$ and $V_B = (\mathbf{y}^*)$. This corresponds to the behaviour of a Passive AUNC$[\gamma_A, \gamma_B, \delta]$ whose channel input is changed by actively cheating Alice to some $\mathbf{y}$, s.t. $\mathbf{y}$, $\mathbf{y}_2$ are $\gamma_A \circledast \theta$ typical i.e., $d_H(\mathbf{y}, \mathbf{y}_2) \in [n(\gamma_A \circledast \theta) - \nu, n(\gamma_A \circledast \theta) + \nu]$ for small enough ν.

(d) **when Alice is honest and Bob is passively cheating:** The analysis is similar to the second case, except that here a cheating Bob passively cheats to gain a view of $V_B = (\mathbf{x}_1, \mathbf{x}_2, \mathbf{x}^*)$ while Alice's view is simply $V_A = (\mathbf{x})$. This results in Bob bringing down his noise to γ_B flipping error, while Alice still observes BSC(δ).

(e) **when Alice is honest and Bob is actively cheating:** In `SimAUNC` Bob doesn't have any active cheating opportunity because there are no parts of the protocol which he can actively change to modify the outcome. The same is true over Passive AUNCs as well.

We do not analyse the behaviour of `SimUNC` when both the agents are cheating, because the behaviour of Passive AUNC is not defined for this case. Moreover, this is not relevant in the context of commitment as there are no security guarantees associated with this case. □

Remark 7.2. *From claims 7.1 and* **??** *we can conclude that there exists no $\epsilon-$sound, $\epsilon-$concealing, and $\epsilon-$binding $k-$bit commitment scheme over a Passive AUNC$[\gamma_A, \gamma_B, \delta]$ for $\delta \geq \gamma_A \circledast \gamma_B$.*

Claim 7.3. *If for a given ϵ, there exists no $\epsilon-$sound, $\epsilon-$concealing, $\epsilon-$binding commitment protocol over a Passive-AUNC$[\gamma_A, \gamma_B, \delta]$, then there exists no such protocol over an Asymmetric-UNC$[\gamma_A, \gamma_B, \delta]$.*

Proof. We will prove the contrapositive of this statement. We take a commitment protocol $\mathscr{P}$ that is $\epsilon-$*sound,* $\epsilon-$*concealing,* $\epsilon-$*binding* over a Asymmetric-UNC$[\gamma_A, \gamma_B, \delta]$. Then we show that $\mathscr{P}$ satisfies the security guarantees over Passive-AUNC$[\gamma_A, \gamma_B, \delta]$ as well. Let c, $\mathbf{x}$, $\mathbf{y}(s)$ $V_A(s)$, $V_B(s)$ be the commit string, sent codeword, received codeword, and view variables respectively as defined in Definition 3.1, as functions of the channel state s that is instantiated. Let us define new view variables V'_A and V'_B when the same protocol $\mathscr{P}$ is carried out over a Passive-AUNC$[\gamma_A, \gamma_B, \delta]$. We have from the soundness criterion of Definition 3.2 of $\mathscr{P}$, that when both Alice and Bob are honest,

$$\mathbb{P}(T(c, \mathbf{x}, V_B(s)) \neq 1) \leq \epsilon \qquad \forall s \in [\gamma, \delta] \tag{7.5}$$

$$\Rightarrow (T(c, \mathbf{x}, V'_B) \neq 1) \leq \epsilon \tag{7.6}$$

This is true because for the honest-honest case, $V'_B = (\mathbf{y}(s = \delta), M)$ evaluates to a special case of $V_B(s = \delta)$. From the concealment criterion of definition 3.3, for an honest Alice,

$$I(C, V_B(s)) \leq \epsilon \qquad \forall s \in [\gamma_B, \delta] \tag{7.7}$$

$$\Rightarrow I(C, V'_B) \leq \epsilon \tag{7.8}$$

To prove the correctness of above, let's look at the view V'_B when Bob is honest, and when he is cheating separately. When he is honest V'_B simply evaluates to $V_B(s = \delta)$ as above. Now when Bob is cheating, consider a case when Alice send $\mathbf{x}$ over Passive-AUNC and Bob receives some $\mathbf{z}$ as the output, but is also able to tap into the channel to get an intermediary output $\mathbf{y}$ that equates to $\mathbf{y}(s = \gamma_B)$. We have $V'_B = (\mathbf{y}, \mathbf{z}, M)$. Because of the Markov chain dependence $\mathbf{x} - \mathbf{y} - \mathbf{z}$, $I(C, V'_B) = I(C, (\mathbf{y}, \mathbf{z}, M)) = I(C, (\mathbf{y}, M))$ which is same as $I(C, V_B(s))$ for $s = \gamma_B$ from (7.7). From the bindingness criterion of Definition **??**, for an honest Bob, under any cheating strategy of Alice

$$\mathbb{P}\left(T(c_1, \mathbf{x}_1, V_B(s)) = 1 \;\&\; T(c_2, \mathbf{x}_2, V_B(s)) = 1\right) \leq \epsilon$$
$$\forall c_1, c_2 \in \mathcal{C}, c_1 \neq c_2, \mathbf{x}_1, \mathbf{x}_2 \in \mathcal{X}^n, s \in [\gamma_A, \delta] \tag{7.9}$$

$$\Rightarrow \mathbb{P}\left(T(c_1, \mathbf{x}'_1, V'_B) = 1 \;\&\; T(c_2, \mathbf{x}'_2, V'_B) = 1\right) \leq \epsilon$$
$$\forall c_1, c_2 \in \mathcal{C}, c_1 \neq c_2, \mathbf{x}_1, \mathbf{x}_2 \in \mathcal{X}^n \tag{7.10}$$

Observing in a case by case basis over Passive Gaussian UNC we have $V'_B = (\mathbf{y}(s = \delta, M))$ when Alice is honest and $V'_B = (\mathbf{y}(s = \gamma_A, M))$ when Alice is cheating. They evaluate

to $V_B(s)$ for $s = \delta$ and $s = \gamma_A$ respectively. So we can substitute them in (7.9) to get (7.10). Since T and V_B anyways do not depend on V'_A, (8.14) holds for any behaviour of Alice. From (7.6), (7.8) and (7.10), protocol $\mathscr{P}$ is $\epsilon-$*sound,* $\epsilon-$*concealing,* $\epsilon-$*binding* over a Passive Gaussian UNC$[\gamma^2, \delta^2]$ also. □

From Remark 7.2 and claim 7.3, we can say that for small enough ϵ i.e., ϵ less than $k^2/(1 + k + k2^k + 2^{\frac{k+1}{2}})^2)$, and for $\delta^2 > 2\gamma^2$, there exists no $k-$bit commitment protocol over a Asymmetric-UNC$[\gamma, \gamma_A, \gamma_B, \delta]$ (over any number of uses of the channel) that is $\epsilon-$*sound,* $\epsilon-$*concealing,* $\epsilon-$*binding* i.e., there exists no *achievable* protocol.

7.4 Achievabilty idea

Our achievability scheme is inspired by the work of Damgård et al. [DKS99]. It involves the use of two rounds of random hash exchange challenge from Bob to Alice, and a strong randomness extractor based on 2-Universal hash function. The two rounds of hash challenge binds Alice and therefore prevents her from cheating successfully. The first hash challenge brings down the number of confusable bit strings ($\mathbf{x}'$) that Alice can use to confuse Bob in the reveal phase from exponential to polynomial many in block-length n, the second hash exchange further brings down the number of such bit strings to 1. The strong randomness extractor is used to extract the left over randomness via a secret key (note that the generalized left over hash lemma [DRS04b] allows us to quantify the size of such a key) of length same as that of the committed bit string. This key is then XOR-ed with the commit string c, which results in a *one-time pad* and ensures the perfect secrecy of the committed bit string (c) against Bob in the commit phase.

Let $\mathcal{G}_1$ be a $4n$-universal hash family such that $\mathcal{G}_1 := \{g_1 : \{0,1\}^n \to \{0,1\}^{n(H(\kappa_A)+\beta_1)}\}$, where $\kappa_A := \frac{\delta-\gamma_A}{1-2\gamma_A}$ and $\beta_1 > 0$ is a small enough constant. Further, let $\mathcal{G}_2$ be a $2-$universal hash family such that $\mathcal{G}_2 := \{g_2 : \{0,1\}^n \to \{0,1\}^{n\beta_2}\}$, where $\beta_2 > 0$ is a small enough constant. Let $\mathcal{E}$ be a $2-$universal hash family such that $\mathcal{E} := \{ext : \{0,1\}^n \to \{0,1\}^{n(H(\gamma_B)-H(\kappa_A)-\beta_3)}\}$, where $\beta_3 > 0$ is a constant chosen such that $\beta_3 > \beta_1 + \beta_2$.
We now describe the commit phase and the reveal phase as follows:

• *Commit Phase:* Alice wants to commit to a bit string $c \in [2^{nR}]$. The users proceed as follows in the commit phase:

(C1). Given the commit string c, Alice sends $\mathbf{X} \sim$ Bernoulli(1/2) independent and identically distributed (i.i.d.) over the Asymmetric-UNC$[\gamma, \gamma_A, \gamma_B, \delta]$. Bob receives the corrupted string $\mathbf{Y}$.

(C2). Having received $\mathbf{Y} = \mathbf{y}$, Bob determines the list $\mathcal{L}(\mathbf{y})$ of bit strings given by:[1]

$$\mathcal{L}(\mathbf{y}) := \{\mathbf{x} \in \{0,1\}^n : n(\gamma - \alpha_1) \leq d_H(\mathbf{x}, \mathbf{y}) \leq n(\delta + \alpha_1)\}.$$

[1]Here the parameter $\alpha_1 > 0$ is chosen appropriately small.

(C3). Bob selects a $4n-$universal hash function $G_1 \sim \text{Unif}(\mathcal{G}_1)$, and sends the description of G_1 to Alice over the two-way noiseless channel.

(C4). Alice computes the hash value $G_1(\mathbf{X})$ and sends it to Bob over the two-way noiseless channel.

(C5). Now, Bob chooses a $2-$universal hash function $G_2 \sim \text{Unif}(\mathcal{G}_2)$, and sends its description to Alice over the noiseless channel.

(C6). Alice computes the hash value $G_2(\mathbf{X})$ and sends it over the two-way noiseless channel to Bob.

(C7). Alice chooses a $2-$universal hash function $\text{Ext} \sim \text{Unif}(\mathcal{E})$ and sends $Q = c \oplus \text{EXT}(\mathbf{X})$ and the description of EXT to Bob over the noiseless link. [2]

- *Reveal phase:* The users proceed in the following manner:

(R1). Alice announces $(\tilde{c}, \tilde{\mathbf{x}})$ to Bob over the two-way noiseless channel.

(R2). Bob accepts $\tilde{c}$ if all the following four tests result an accept i.e., $(\text{T} = 1)$:

T1: (i) $\tilde{\mathbf{x}} \in \mathcal{L}(\mathbf{y})$,
T2: (ii) $g_1(\tilde{\mathbf{x}}) = g_1(\mathbf{x})$,
T3: (iii) $g_2(\tilde{\mathbf{x}}) = g_2(\mathbf{x})$,
T4: (iv) $\tilde{c} = q \ \oplus \text{ext}(\tilde{\mathbf{x}})$.
Otherwise, Bob rejects the revealed bit string $\tilde{c}$ and outputs '0'.

We skip the analysis of the proofs.

7.4.1 Note on Asymmetric UNCs over other regimes

The rate expression we achieved for Asymmetric-UNCs is highly dependent on the assumption that $\gamma_A, \gamma_B < \gamma$. Over other parameter regimes, the condition for concealment and bindingness guarantees dictate the size of hash functions and randomness extractors that we choose. Accordingly the rate differs. The exact values of the rates of different protocols that are possible are $H_2(\gamma)$, $H_2(\gamma_B)$, $H_2(\gamma_B - \kappa_A)$, $H_2(\gamma - \kappa)$ ($\kappa = \frac{\delta-\gamma}{1-2\gamma}$, $\kappa_A = \frac{\delta-\gamma_A}{1-2\gamma_A}$). At any time it is the protocol with rate corresponding to the minimum of these values, that is achievable. In the above case, $\gamma_A, \gamma_B < \gamma$, there is clearly only one minima $H_2(\gamma_B - \kappa_A)$. Moreover, the achievable region of this rate and the impossibility region of theorem 7.1 exactly span the entire space. But if one of the other terms mentioned turns out to be the minimum rate, there would still remain a gap in the analysis of our impossibility and achievability proofs.

[2] In the following expression, operator $\oplus$ denotes component-wise XOR.

Chapter 8

Commitment over Gaussian UNCs

In this chapter we present the last of our principal results. We study commitment on an unreliable variant of continuous AWGN channels, through Gaussian-UNCs [BJMY22b]. We find an impossibility regime for commitment over Gaussian-UNCs. Over the possibility regime, we present positive throughput schemes for different power constraint values. We start off by discussing the problem setup.

8.1 Problem setup

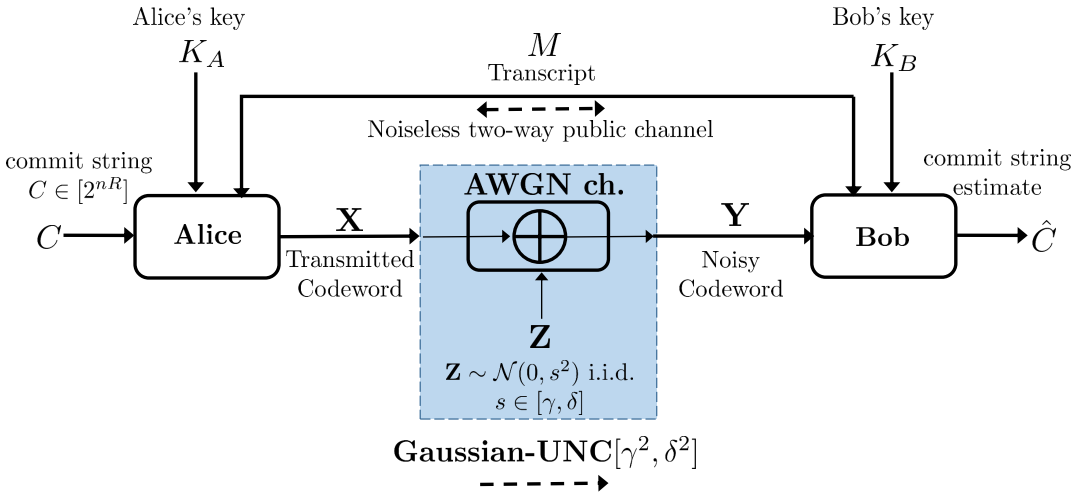

Figure 8.1: The problem setup: commitment over a Gaussian UNC$[\gamma^2, \delta^2]$

We build upon the problem setup from figure 3.1 for over Gaussian-UNCs. Markedly, we would be characterising power constraints on the channel's input alphabet. Figure 8.1 specialises the setup. In our problem, two mutually distrustful parties, *committer* Alice and *receiver* Bob employ a Gaussian-UNC$[\gamma^2, \delta^2]$ to realize commitment over a random string $C \in [2^{nR}]$ available to Alice (we specify $R > 0$ later). Alice and Bob have access to a one-way Gaussian-UNC$[\gamma^2, \delta^2]$ with elasticity E at both Alice and Bob (henceforth only referred to as

elasticity) where $E := \delta^2 - \gamma^2$, for $0 < \gamma \leq \delta$, and $\gamma, \delta \in \mathbb{R}^+$.[1] Separately, as is common in such cryptographic primitives, we also assume that Alice and Bob can interact over a two-way link that is noiseless and where the interaction is public and fully authenticates the transmitting party. To commit to her random string C, Alice uses the Gaussian-UNC$[\gamma^2, \delta^2]$ channel n times and transmits over it her encrypted data $\mathbf{X} = (X_1, X_2, \cdots, X_n) \in \mathbb{R}^n$; Bob receives a noisy version $\mathbf{Y} \in \mathbb{R}^n$ of Alice's transmission $\mathbf{X}$. Alice has an input power constraint $P > 0$, i.e., Alice can only transmit vectors $\mathbf{X} \in \mathcal{S}(P)$, where $\mathcal{S}(P) := \{\mathbf{x} \in \mathbb{R}^n : \|\mathbf{x}\| \leq \sqrt{nP}\}$, thus yielding a signal to elasticity ratio (SER) defined as SER:= $\frac{P}{E}$. We allow private randomization at both Alice and Bob via their respective keys $K_A \in \mathcal{K}_{\mathcal{A}}$ and $K_B \in \mathcal{K}_{\mathcal{B}}$. At any point in time, Alice and Bob can also exchange messages over the public, noiseless link; let M denote the entire collection of messages exchanged. We call M the *transcript* of the protocol. It is important to note that we assume that any point in time during the protocol, the transmissions of Alice and/or Bob can depend *causally* on the information previously available to them.

An $(n, R)-$commitment protocol $\mathscr{P}$ from definition 3.1 over Gaussian-UNCs is studied for the following characteristics.

- **ϵ-soundness:** A protocol $\mathscr{P}$ is $\epsilon-$sound if, for an honest Alice and an honest Bob,

$$\mathbb{P}\left(T(C, \mathbf{X}, V_B) \neq 1\right) \leq \epsilon. \tag{8.1}$$

- **ϵ-concealing:** A protocol $\mathscr{P}$ is $\epsilon-$concealing if, for an honest Alice and under any strategy of Bob,

$$I(C; V_B) \leq \epsilon. \tag{8.2}$$

- **$\epsilon-$bindingness:** A protocol $\mathscr{P}$ is $\epsilon-$binding if, for an honest Bob and under any strategy of Alice,

$$\mathbb{P}\Big(T(\bar{c}, \bar{\mathbf{x}}, V_B) = 1 \quad \& \quad T(\hat{c}, \hat{\mathbf{x}}, V_B) = 1\Big) \leq \epsilon \tag{8.3}$$

  for any two pairs $(\bar{c}, \bar{\mathbf{x}})$, $(\hat{c}, \hat{\mathbf{x}})$, $\bar{c} \neq \hat{c}$, and $\bar{\mathbf{x}}, \hat{\mathbf{x}} \in \mathcal{S}(P)$.

A rate R is said to be *achievable* if for every $\epsilon > 0$ there exists for every $n \in \mathbb{N}$ sufficiently large a protocol $\mathscr{P}$ such that $\mathscr{P}$ is $\epsilon-$sound, $\epsilon-$concealing and $\epsilon-$binding. The supremum of all achievable rates is called the commitment capacity $\mathbb{C}_{GUNC}$ of the Gaussian-UNC$[\gamma^2, \delta^2]$.

8.2 Impossibility and achievability results

We first present an impossibility result.

[1] We require the strict inequality $\gamma > 0$ as otherwise a malicious Alice can force the Gaussian-UNC$[\gamma^2, \delta^2]$ always to an AWGN channel with variance 0, i.e., a *noiseless* channel. It is well known that a noiseless channel precludes commitment [Blu83].

Theorem 8.1 (Impossibility over Gaussian-UNCs)**.** *For a Gaussian UNC*$[\gamma^2, \delta^2]$*, the commitment capacity* $\mathbb{C} = 0$ *if* $\delta^2 \geq 2\gamma^2$.

This result conclusively identifies sufficient conditions for impossibility of even *single-bit* commitment over Gaussian UNCs. See Section 8.3 for the proof.

Remark 8.1. *Our converse in inspired in spirit by the one for binary UNCs in [DKS99]. A key fact used in the converse is the classic result of impossibility of commitment over noiseless links (even when parties can privately randomize). Our proof of the converse continues to use this same approach. A crucial part of our proof involves analysing a 'more restrictive' channel model called the Passive-Gaussian UNC*$[\gamma^2,\delta^2]$ *with identical parameters as in the Gaussian UNC*$[\gamma^2,\delta^2]$ *(see Sec 8.3). We show via a sequence of reductions that Passive-Gaussian UNC*$[\gamma^2,\delta^2]$ *can be simulated noiselessly, and thus, should preclude commitment. We then leverage this result to show that, as a consequence, commitment is impossible over a Gaussian UNC*$[\gamma^2,\delta^2]$ *.*

An interesting aspect of our impossibility result is that Alice's power constraint P *plays no role; commitment is seen to be impossible if the* elasticity $E = \delta^2 - \gamma^2$ *is 'large enough', i.e.,* $E \geq \gamma^2$*. This result is similar in 'flavour' to that over the binary UNCs (cf. [DKS99] for details).*

Having understood the impossibility regime (when $\delta^2 \geq 2\gamma^2$), we now flip the question and seek to explore positive-rate commitment schemes. Interestingly, unlike our impossibility result, Alice's input constraint P plays a crucial role. Furthermore, we notice that there is a stark difference in our achievability results when $P > E$ and when $P \leq E$. This motivates us to define the notion of *signal-to-elasticity ratio (SER)*, where $SER := P/E$ for a Gaussian UNC$[\gamma^2, \delta^2]$. We now state our first result. Note that all the following theorems are stated without proof here (see extended draft for proof details).

Theorem 8.2. *Let* $P > E$ *and hence, the* $SER > 1$*. Then, positive-rate commitment is possible, i.e.,* $\mathbb{C} > 0$ *if:*

$$\delta^2 \leq \left(1 + \frac{P}{P + \gamma^2}\right) \gamma^2. \tag{8.4}$$

Furthermore, $\mathbb{C}$ *is lower bounded by :*

$$\mathbb{C}_{G-UNC} \geq \frac{1}{2} \log \left(\frac{P}{\delta^2 - \gamma^2}\right) - \frac{1}{2} \log \left(1 + \frac{P}{\gamma^2}\right). \tag{8.5}$$

We present only a brief overview of our achievability protocol. See the extended draft for details.

Remark 8.2. *The proof of this theorem uses a novel approach but crucially borrows ideas both from the protocol of Crepeau* et al. *[DKS99, CDN20] for binary UNCs as well as that of Nascimento* et al. *[NBSI08] for classic AWGN channels. The 'skeleton' of our protocol uses an error correcting code with certain minimum distance guarantee (similar to [NBSI08]). However, to handle adversaries who may benefit from the channel elasticity available, we 'robustify' our protocol by using an appropriate hash function challenge mechanism inspired*

by the protocols in [DKS99, CDN20]. Note that this is not required in classic AWGN channels which lack elasticity. The specific choice of the protocol parameters (viz., the error correcting code rate, the range of the universal hash functions and the randomness extractors, etc..) needs careful consideration. While the soundness of our protocol follows from Chernoff bounding, the concealment and bindingness are more tricky. For concealment, we utilize a well known equivalence between the so-called bias-based *security and* capacity-based *security [DPP98]; here, the leftover hash lemma [NBSI08] is crucially used. The bindingness analysis follows from the hash function challenges Bob offers to Alice; careful concentration bounds need to be established. An important part in this analysis requires us to get a good bound on the number of 'confusable' codewords that a cheating Alice may seek to reveal. Here we use results on spherical codes to get the appropriate bound on the cardinality of the 'confusable' codewords.*

The above result holds for the regime when the $SER > 1$. Interestingly, for extremely large values of SER, the 'possibility' bound 'shifts' (as a function of P) towards the impossibility bound of Theorem 8.1. In fact, in the limit $P \to \infty$, the two bounds meet exactly, thereby allowing us to characterize precisely the positive commitment rate, i.e., $\mathbb{C} > 0$, threshold.

Theorem 8.3. *Fix $\gamma^2, \delta^2 < \infty$ and let $P \to \infty$. Then commitment is possible if and only if $\delta^2 \leq 2\gamma^2$.*

The proof of this result simply follows from Theorem 8.1 and by taking the limit $P \to \infty$ for the threshold in (8.4) (for fixed γ^2, δ^2) from Theorem 8.2. Having presented results for $SER > 1$, we now present achievability results for the regime where $0 < SER < 1$. Note that commitment is impossible when $SER = 0$.

Theorem 8.4. *Let $P \leq E$ and hence, the $SER \leq 1$. Then, positive-rate commitment is possible if the following holds:*

$$\delta^2 \leq \left(1 + \frac{P}{P + \gamma^2}\right) \tilde{\gamma}^2. \tag{8.6}$$

where $\tilde{\gamma}^2 := \delta^2 - P$. Furthermore, the commitment capacity $\mathbb{C}$ is lower bounded by the following expression:

$$\mathbb{C}_{G-UNC} \geq \frac{1}{2} \log \left(\frac{P}{\delta^2 - \tilde{\gamma}^2}\right) - \frac{1}{2} \log \left(1 + \frac{P}{\gamma^2}\right). \tag{8.7}$$

Remark 8.3. *The condition for positive rate commitment for this scenario is different from that in Theorem 8.2. A low SER where Alice's power P is no larger than the channel elasticity allows malicious parties significant ascendance. However, this ascendance is not symmetric. Thus, while Bob can benefit from effecting an AWGN channel with variance γ^2 (when malicious) such is not the case for Alice. In fact, in her case, it is seen that the most effective use of channel elasticity is to induce an AWGN channel with variance $\tilde{\gamma}^2 > \gamma^2$. This comes about from a malicious Alice's interest in maximizing her 'confusable' set of codewords. For details, refer the extended draft.*

An important take away from the achievability results for both the scenarios, *viz.,* when $SER > 1$ and when $SER \leq 1$, is that the 'finiteness' of commitment capacity of Gaussian UNCs is owing to the underlying channel elasticity E. This fact is particularly stark when, for fixed $P > 0$, one allows the channel elasticity to vanish, i.e., $E = 0$. In this case, the commitment capacity lower bound (see Theorem 8.2) suggests that commitment rate is infinite, which is exactly what is known for classical AWGN channels that exhibit $E = 0$. We capture this alternate perspective on the infinite commitment rate of classical AWGN channels in the following corollary.

Corollary 8.1. *For a fixed $P > 0$, the commitment capacity of a Gaussian UNC with vanishing channel elasticity E approaches infinity.*

8.3 Impossibility proof

We first start by showing that commitment is impossible over noiseless channels in Claim 8.1. We then define a channel called 'Passive-Gaussian UNC$[\gamma^2, \delta^2]$', which we show can be simulated noiselessly over the regime $\delta^2 \geq 2\gamma^2$ through claim 8.2. This implies that commitment can't be realised over such Passive-Gaussian UNCs. We build upon this result and show in claim 8.3 that it further implies that commitment is not possible over Gaussian UNCs as well. This completes our proof. It is to note that, in this section we analyse seperately the two different cheating behaviours of users - 'active' and 'passive'(discussed earlier in section 3.3).

Claim 8.1. *No ϵ_1-sound, ϵ_2-concealing, ϵ_3-binding $k-$bit commitment scheme is possible over noiseless channels for*

$$\epsilon_2 < k(1 - \epsilon_1 - 2^k\epsilon_3) - 2\sqrt{\epsilon_1 + 2^k\epsilon_3}. \tag{8.8}$$

The proof is included in Appendix C.1. This claim shows that commitment is impossible with vanishing soundness, concealment and bindingness parameters over a noiseless channel. Let us look at a modified version of the Gaussian-UNCs.

Definition 8.1 (Passive-Gaussian UNC)**.** *A Passive-Gaussian UNC$[\gamma^2, \delta^2]$ is an AWGN(δ^2) channel when both the users are honest. However, a cheating party can get some extra side information which can bring down the noise variance to $\gamma^2 \leq \delta^2$ from his/her point of view.*

Crucially since there is no chance of channel control, a passively cheating party and an 'honest but curious' party behave alike over Passive-GaussianUNC. By proving that commitment is impossible over this channel, we show that it follows that commitment is impossible over Gaussian UNCs as well. Towards the first part, we first claim this result.

Claim 8.2. *A Passive-Gaussian UNC$[\gamma^2, \delta^2]$ can be realised noiselessly when $\delta^2 \geq 2\gamma^2$.*

Proof. We present here a protocol `SimGUNC` that for given γ and δ, can realise the functionality of n uses of a Passive-Gaussian UNC$[\gamma^2, \delta^2]$ for any given channel input $\mathbf{x} \in \mathbb{R}^n$.
`SimGUNC`$\{\gamma^2, \delta^2\}(\mathbf{x})\{$
Define $\theta := \sqrt{\delta^2 - 2\gamma^2}$

Alice passes $\mathbf{x}$ through a local AWGN(γ^2) to get $\mathbf{x}_1$
Alice passes $\mathbf{x}_1$ through a local AWGN(θ^2) to get $\mathbf{x}_2$
Alice sends $\mathbf{x}_1$, $\mathbf{x}_2$ to Bob noiselessly
Bob passes $\mathbf{x}_2$ through a local AWGN(γ^2) to get $\mathbf{x}^*$
Ask Alice, Bob to forget $\mathbf{x}_1$, $\mathbf{x}_2$
Return the resulting views V_A and V_B
}

`SimGUNC` here involves only noiseless interactions between Alice and Bob. Here $\mathbf{x}, \mathbf{x}_1, \mathbf{x}_2, \mathbf{x}^* \in \mathbb{R}^n$. To understand how `SimGUNC` correctly realises the functionality of a Passive-Gaussian UNC, let us analyse over a case by case basis. It is to note here that while honest parties faithfully forget the values of $\mathbf{x}_1$ and $\mathbf{x}_2$, passively cheating parties continue to remember them, but not affecting the protocol in any other way. An actively cheating party on the other hand may change the variables where ever possible involved in the protocol to his/her advantage. A crucial fact used here is that addition of two independent zero mean gaussian variables is another zero mean gaussian with variance that is the sum of the variances of the addends.

(a) **when Alice is honest and Bob is honest:** Here, Alice and Bob follow all the steps in `SimGUNC` exactly. For input $\mathbf{x}$, at the end of `SimGUNC`, Alice's and Bob's views are $V_A = (\mathbf{x})$, $V_B = (\mathbf{x}^*)$ respectively. It follows from Fig. 8.2 that the channel between $\mathbf{x}$ and $\mathbf{x}^*$ is an AWGN(δ^2). This exactly corresponds to the channel behaviour when an honest Alice sends over $\mathbf{x}$ through Passive-Gaussian UNC$[\gamma^2, \delta^2]$ to an honest Bob. (see defnition 8.1).

(b) **when Alice is passively cheating and Bob is honest:** A passively cheating Alice remembers the values of $\mathbf{x}_1$ and $\mathbf{x}_2$ in addition to that of $\mathbf{x}$, resulting in $V_A = (\mathbf{x}, \mathbf{x}_1, \mathbf{x}_2)$ and $V_B = (\mathbf{x}^*)$. From Fig 8.2, the extra knowledge of $\mathbf{x}_2$ brings down Alice's uncertainty of $\mathbf{x}^*$ to AWGN(γ^2) in what is otherwise an AWGN(δ^2) as is observed from an honest Bob's perspective. This corresponds to the behaviour of a Passive AUNC$[\gamma^2, \delta^2]$ whose channel input is $\mathbf{x}$.

(c) **when Alice is actively cheating and Bob is honest:** Consider a cheating behaviour of Alice who, for input string $\mathbf{x}$, modifies the values of $\mathbf{x}_1$ and $\mathbf{x}_2$ to say $\mathbf{y}_1$ and $\mathbf{y}_2'$ respectively, before sending them over to Bob. This results in views $V_A = (\mathbf{x}, \mathbf{y}_1, \mathbf{y}_2)$ and $V_B = (\mathbf{y}^*)$. This corresponds to the behaviour of a Passive-Gaussian UNC$[\gamma_A, \gamma_B, \delta]$ whose channel input is changed by the actively cheating Alice to some $\mathbf{y} \in \mathbb{R}^n$, s.t. $\mathbf{y}$, $\mathbf{y}_2$ are $\gamma^2 + \theta^2$ typical i.e., $||\mathbf{y}, \mathbf{y}_2|| \in [\sqrt{n(\gamma^2 + \theta^2) - \nu}, \sqrt{n(\gamma^2 + \theta^2) + \nu}]$ for small enough ν. In lose terms $\mathbf{y}$, $\mathbf{y}_2$ are separated by an AWGN($\gamma^2 + \theta^2$).

(d) **when Alice is honest and Bob is passively cheating:** The analysis is similar to the second case, except that here a cheating Bob passively cheats to gain a view of $V_B = (\mathbf{x}_1, \mathbf{x}_2, \mathbf{x}^*)$ while Alice's view is simply $V_A = (\mathbf{x})$. This results in Bob bringing down his noise to AWGN(γ^2), while Alice still observes an AWGN(δ^2).

(e) **when Alice is honest and Bob is actively cheating:** In `SimGUNC` Bob doesn't have any active cheating opportunity because there are no parts of the protocol which he

can actively change to modify the outcome; which is the same case for Passive-Gaussian UNCs as well.

We do not analyse the behaviour of `SimGUNC` when both the agents are cheating, because the behaviour of Passive-Gaussian UNC is not defined for this case. Moreover, this is not relevant in the context of commitment as there are no security guarantees associated with this case. □

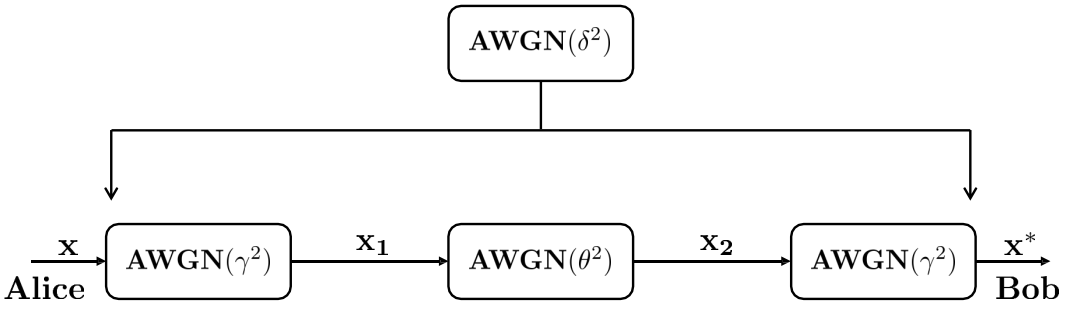

Figure 8.2: Channel structure in $\texttt{SimGUNC}\{\gamma^2, \delta^2\}(\mathbf{x})$ and how it simulates the behaviour of a Passive-Gaussian UNC$[\gamma^2, \delta^2]$ with input $\mathbf{x}$.

Remark 8.4. *From claims 8.1 and 8.2, we can conclude that there exists no $\epsilon-$sound, $\epsilon-$concealing, $\epsilon-$binding $k-$bit commitment scheme over a Passive-Gaussian UNC$[\gamma^2, \delta^2]$ when $\delta^2 \geq 2\gamma^2$, for small enough ϵ. (More precisely[2] for $\epsilon < \left(\frac{k}{1+k+k2^k+2^{\frac{k+1}{2}}}\right)^2$).*

Claim 8.3. *Let $\epsilon > 0$. If there exists no $\epsilon-$sound, $\epsilon-$concealing, $\epsilon-$binding commitment protocol over a Passive-Gaussian UNC$[\gamma^2, \delta^2]$, then there exists no such protocol over a Gaussian UNC$[\gamma^2, \delta^2]$.*

Proof. We will prove the contrapositive of this statement. We take a commitment protocol $\mathscr{P}$ that is *$\epsilon-$sound, $\epsilon-$concealing, $\epsilon-$binding* over a Gaussian UNC$[\gamma^2, \delta^2]$. Then we show that $\mathscr{P}$ satisfies the security guarantees over Passive Gaussian UNC$[\gamma^2, \delta^2]$ as well. Let c, $\mathbf{x}$, $\mathbf{y}(s)$ $V_A(s)$, $V_B(s)$ be the commit string, sent codeword, received codeword, and view variables respectively as defined in Definition 3.1, but as functions of the channel state s that is instantiated. Let us define new view variables V'_A and V'_B when the same protocol $\mathscr{P}$ is carried out over a Passive Gaussian UNC. We have from the soundness criterion of Definition 3.2 of $\mathscr{P}$, that when both Alice and Bob are honest,

$$\mathbb{P}(T(c, \mathbf{x}, V_B(s)) \neq 1) \leq \epsilon \qquad \forall s \in [\gamma^2, \delta^2] \tag{8.9}$$

$$\Rightarrow (T(c, \mathbf{x}, V'_B) \neq 1) \leq \epsilon \tag{8.10}$$

[2]This bound cannot be improved by increasing the number of channel uses.

This is true because for the honest-honest case, $V_B' = (\mathbf{y}(s = \delta^2), M)$ evaluates to a special case of $V_B(s = \delta^2)$. From the concealment criterion of definition 3.3, for an honest Alice,

$$I(C, V_B(s)) \leq \epsilon \qquad \forall s \in [\gamma^2, \delta^2] \tag{8.11}$$
$$\Rightarrow I(C, V_B') \leq \epsilon \tag{8.12}$$

To prove the correctness of above, let's look at the view V_B' when Bob is honest, and when he is cheating separately. When he is honest V_B' simply evaluates to $V_B(s = \delta^2)$ as above. Now when Bob is cheating, consider a case when Alice send $\mathbf{x}$ over Passive Gaussian UNC and Bob receives some $\mathbf{z}$ as the output, but is also able to tap into the channel to get an intermediary output $\mathbf{y}$ that equates to $\mathbf{y}(s = \gamma^2)$. We have $V_B' = (\mathbf{y}, \mathbf{z}, M)$. Because of the Markov chain dependence $\mathbf{x} - \mathbf{y} - \mathbf{z}$, $I(C, V_B') = I(C, (\mathbf{y}, \mathbf{z}, M)) = I(C, (\mathbf{y}, M))$ which is same as $I(C, V_B(s))$ for $s = \gamma^2$ from (8.11). From the bindingness criterion of Definition 3.4, for an honest Bob, under any cheating strategy of Alice

$$\mathbb{P}\left(T(c_1, \mathbf{x}_1, V_B(s)) = 1 \;\&\; T(c_2, \mathbf{x}_2, V_B(s)) = 1\right) \leq \epsilon$$
$$\forall c_1, c_2 \in \mathcal{C}, c_1 \neq c_2, \mathbf{x}_1, \mathbf{x}_2 \in \mathcal{X}^n, s \in [\gamma^2, \delta^2] \tag{8.13}$$
$$\Rightarrow \mathbb{P}\left(T(c_1, \mathbf{x}_1', V_B') = 1 \;\&\; T(c_2, \mathbf{x}_2', V_B') = 1\right) \leq \epsilon$$
$$\forall c_1, c_2 \in \mathcal{C}, c_1 \neq c_2, \mathbf{x}_1, \mathbf{x}_2 \in \mathcal{X}^n \tag{8.14}$$

Observing in a case by case basis over Passive Gaussian UNC we have $V_B' = (\mathbf{y}(s = \delta^2, M))$ when Alice is honest and $V_B' = (\mathbf{y}(s = \gamma^2, M))$ when Alice is cheating. They evaluate to $V_B(s)$ for $s = \delta^2$ and $s = \gamma^2$ respectively. So we can substitute them in (8.13) to get (8.14). Since T and V_B anyways do not depend on V_A', (8.14) holds for any behaviour of Alice. From (8.10), (8.12) and (8.14), protocol $\mathscr{P}$ is $\epsilon-$*sound,* $\epsilon-$*concealing,* $\epsilon-$*binding* over a Passive Gaussian UNC$[\gamma^2, \delta^2]$ also. □

From Remark 8.4 and claim 8.3, we can say that for small enough ϵ (for ϵ less than $k^2/(1 + k + k2^k + 2^{\frac{k+1}{2}})^2$), and for $\delta^2 \geq 2\gamma^2$, there exists no $k-$bit commitment protocol over a Gaussian UNC$[\gamma^2, \delta^2]$ (over any number of uses of the channel) that is $\epsilon-$*sound,* $\epsilon-$*concealing,* $\epsilon-$*binding* i.e., there exists no *achievable* protocol.

8.4 Achievability proof

We first present an overview of our achievability protocol following which we present the actual protocol and then the security analysis within the possibility regime ($\delta^2 < 2\gamma^2$). Our protocol uses ideas from [DKS99, NBSI08, CDN20]; however, the specific protocol we present for the Gaussian UNCs is novel to the best of our knowledge.

In our scheme, Alice first generates a random bit string $U^m \in \{0, 1\}^m$ toward committing string $C \in [2^{nR}]$. Alice then uses an error correcting code, say $\mathcal{C} = (\psi, \phi)$ where $\mathcal{C} \subseteq \mathbb{R}^n$ here ($\mathcal{C}$ is known to both parties) to encode this bit string U^m to codeword $\mathbf{X} = \psi(U^m)$ and sends $\mathbf{X}$ over the Gaussian UNC$[\gamma^2, \delta^2]$ to Bob. Our error correcting code $\mathcal{C}$ is a spherical code comprising *equi-normed* codewords (where all codewords reside on the surface of a n-dimensional Euclidean ball). Bob receives a noisy version $\mathbf{Y}$ of the transmitted codeword

$\mathbf{X}$. We choose the rate $\bar{R}(\mathcal{C})$ of the error correcting code $\mathcal{C}$ sufficiently 'large'; this ensures that upon receiving a noisy observation $\mathbf{Y}$ of the transmitted codeword $\mathbf{X}$, Bob decodes a 'large' list $\mathcal{L}(\mathbf{Y}) \subseteq \mathcal{C}$ of codewords which are 'typical' w.r.t the observation $\mathbf{Y}$ (here typicality is w.r.t. the underlying Gaussian UNC[γ^2,δ^2]). Recall however that a cheating Alice can privately change the noise variance in the Gaussian UNC[γ^2,δ^2] such an action can 'enlarge' her set of spoofing codewords that she can present, if dishonest, in the reveal phase. To restrict Alice's potential dishonest behaviour, our protocol employs the classic hash-challenge approach (inspired by [DKS99]). In particular, Bob initiates a *two-round* hash challenge with Alice[3] which essentially *bind* Alice to her choice of U^m (remember U^m has a one-to-one mapping with $\mathbf{X}$ via the codebook $\mathcal{C}$) in the commit phase thereby ensuring Bob's test T can detect any cheating attempt by Alice during the reveal phase. Essentially, the first hash challenge reduces the number of confusable strings that Alice can use to confuse Bob in the reveal phase from exponential to polynomial many in block-length n; the second hash challenge further brings down the number of such bit strings to 1 (this precludes the possibility of Bob being confused between two different bit string, say $U_1^m, U_2^m \in \{0,1\}^m$, thereby guaranteeing the binding guarantee). The strong randomness extractor extracts a secret key (note that the leftover hash lemma [DRS04a] allows us to quantify the size of this key). This key is then XOR-ed with the commit string c to realize a *one-time pad* scheme, which conceals the committed string against Bob in the commit phase.

8.4.1 Achievable protocol for $SER > 1$

We now present our commitment protocol. Recall that when $SER > 1$ for the Gaussian UNC[γ^2,δ^2] i.e., given elasticity $E = \delta^2 - \gamma^2$ of the Gaussian UNC[γ^2,δ^2] we have $P > E$, or $P > \delta^2 - \gamma^2$. Alice and Bob fix an error correcting code $\mathcal{C} \subseteq \mathbb{R}^n$ comprising an encoder $\psi : \{0,1\}^m \to \mathbb{R}^n$ and decoder $\phi : \mathbb{R}^n \to \{0,1\}^m \bigcup \{0\}$ with rate $\bar{R} := \frac{1}{2}\log(\frac{1}{1-\left(1-\frac{\hat{d}}{2}\right)^2}) - \tilde{\beta}$ where $d_{\min}(\mathcal{C}) = n\hat{d}P$ is the minimum distance of the code $\mathcal{C}$. The commitment rate of the protocol is

$$R = \frac{1}{2}\log\left(\frac{P}{E}\right) - \frac{1}{2}\log\left(1 + \frac{P}{\gamma^2}\right) - \beta_3. \tag{8.15}$$

It can be noted that our choice of R is greater than zero only when $SER > 1$ i.e., $P > E$. This expression for R is therefore chosen only for $SEER > 1$. Let $\mathcal{G}_1 := \{g_1 : \{0,1\}^m \to \{0,1\}^{n(\bar{R}+\frac{1}{2}\log(\frac{E}{P})+\beta_1)}\}$ be a $4n$-universal hash family, where $E := \delta^2 - \gamma^2$ and $\beta_1 > 0$ is a small enough constant. Let $\mathcal{G}_2 := \{g_2 : \{0,1\}^m \to \{0,1\}^{m\beta_2}\}$ be a $2-$universal hash family, where $\beta_2 > 0$ is a small enough constant. Let $\mathcal{E} := \{\text{ext} : \{0,1\}^n \to \{0,1\}^{nR}\}$ be a $2-$universal hash family, where $\beta_3 > 0$ is chosen such that $\beta_3 > \beta_1 + \beta_2$.[4] Here are the commit and reveal phases of our protocol:

Commit Phase: Alice seeks to commit to string $C \in [2^{nR}]$ and proceeds as follows:

[3]We need two rounds of hash challenge to circumvent a non-trivial rate loss that arises in the single hash challenge due to the *birthday paradox*; see [CDN20] where it is discussed in detail.

[4]Note that R can be made arbitrarily close to $\mathbb{C}_{REC}$.

(C1) Given C, Alice first generates $U^m = (U_1, U_2, \cdots, U_m) \sim$ Bernoulli(1/2) independent and identically distributed (i.i.d.) bits.

(C2) Using code $\mathcal{C} = (\psi, \phi)$, Alice picks the codeword $\mathbf{X} = \psi(U^m)$ and sends it over the Gaussian UNC[γ^2,δ^2] Let Bob receive $\mathbf{Y}$ over the noisy channel.

(C3) Bob creates a list $\mathcal{L}(\mathbf{y})$ of codewords in $\mathcal{C}$ given by:[5]

$$rCl\mathcal{L}(\mathbf{y}) := \{\mathbf{x} \in \mathcal{C} : n(\gamma^2 - \alpha_1) \leq \|\mathbf{x} - \mathbf{y}\|^2 \leq n(\delta^2 + \alpha_1)\}. \tag{8.16}$$

(C4) Bob now initiates the two rounds of hash challenges for Alice. Bob first chooses his hash function $G_1 \sim$ Unif$(\mathcal{G}_1)$. Bob sends the description of G_1 to Alice over the two-way noiseless link.

(C5) Using G_1, Alice computes the hash $G_1(U^m)$ and sends the hash value, say $\bar{g}_1$, to Bob over the noiseless link.

(C6) Next, Bob initiates the second round of hash exchange by choosing another hash function $G_2 \sim$ Unif$(\mathcal{G}_2)$, and sends the description of G_2 to Alice over the noiseless link.

(C7) Once again, Alice locally computes the hash value $G_2(\mathbf{X})$ and sends the hash value, $\bar{g}_2$ to Bob over the noiseless link.

(C8) Alice now chooses an extractor function $\texttt{Ext} \sim$ Unif$(\mathcal{E})$ and sends[6] the value $Q = C \oplus \texttt{Ext}(U^m)$ along with the exact choice of the function $\texttt{Ext}$ to Bob over the noiseless link.

Reveal phase: The following operations comprise the reveal phase:

(R1) Alice announces $(\tilde{c}, \tilde{u}^m)$ to Bob over the noiseless link.

(R2) Bob determines the codeword $\tilde{\mathbf{x}} = \tilde{\mathbf{x}}(\tilde{u}^m) = \psi(\tilde{u}^m)$.

(R3) Bob accepts $\tilde{c}$ if all the following four conditions are simultaneously satisfied:

(i) $\tilde{\mathbf{x}} \in \mathcal{L}(\mathbf{y})$, where $\mathbf{y}$ is Bob's observation at the end of the commit phase,

(ii) $g_1(\tilde{u}^m) = \bar{g}_1$,

(iii) $g_2(\tilde{u}^m) = \bar{g}_2$,

(iv) $\tilde{c} = q \ \oplus \texttt{ext}(\tilde{u}^m)$.

Else, he rejects $\tilde{c}$ and outputs '0'.

[5]Here the parameter $\alpha_1 > 0$ is chosen appropriately small.

[6]The operator $\oplus$ here denotes component-wise XOR.

8.4.1.1 Positivity of rate R of our protocol $\mathscr{P}$:

We first show that the rate $R > 0$ when $\delta^2 < \left(1 + \frac{P}{P+\gamma^2}\right)\gamma^2$, i.e., $(\delta^2 - \gamma^2) < \frac{P\gamma^2}{P+\gamma^2}$. Toward proving rate positivity, let us assume that $(\delta^2 - \gamma^2) = \frac{P\gamma^2}{P+\gamma^2} - \eta$, for some $\eta > 0$. Recall that the rate of the commitment protocol is

$$R = \frac{1}{2}\log\left(\frac{P}{E}\right) - \frac{1}{2}\log\left(1 + \frac{P}{\gamma^2}\right) - \beta_3 \tag{8.17}$$

$$\stackrel{(a)}{=} \frac{1}{2}\log\left(\frac{P}{\delta^2 - \gamma^2}\right) - \frac{1}{2}\log\left(1 + \frac{P}{\gamma^2}\right) - \beta_3 \tag{8.18}$$

$$= \frac{1}{2}\log\left(\frac{P}{\delta^2 - \gamma^2}\right) - \frac{1}{2}\log\left(\frac{P+\gamma^2}{\gamma^2}\right) - \beta_3 \tag{8.19}$$

$$= \frac{1}{2}\log\left(\frac{\frac{P\gamma^2}{(P+\gamma^2)}}{\delta^2 - \gamma^2}\right) - \beta_3 \tag{8.20}$$

Given $\eta > 0$, for $\beta_3 = \beta_3(\eta) > 0$ small enough, it follows that $R > 0$. We now analyse and prove the security guarantees in detail for the above defined (n, R)-commitment scheme:

8.4.1.2 $\epsilon-$soundness analysis

For our protocol to be ϵ-sound, we essentially need to show that when both parties are honest, Bob accepts $\tilde{C} = C$ with high probability (w.h.p.). Since Alice is honest, it follows directly that it is sufficient to show that $\mathbb{P}\left(\mathbf{X} \notin \mathcal{L}(\mathbf{Y})\right) \leq \epsilon$ for n large enough. This is because, conditioned on the event $\{\mathbf{X} \in \mathcal{L}(\mathbf{Y})\}$, the rest of the three conditions, viz., (a) $g_1(\tilde{u}^m) = \bar{g}_1$, (b) $g_2(\tilde{u}^m) = \bar{g}_2$, and (c) $\tilde{c} = q \ \oplus \texttt{ext}(\tilde{u}^m)$ *deterministically* hold true when Alice and Bob are both honest. The proof of the fact that $\mathbb{P}\left(\mathbf{X} \notin \mathcal{L}(\mathbf{Y})\right) \leq \epsilon$ for n sufficiently large follows from classic Chernoff bound for additive Gaussian channels.

8.4.1.3 $\epsilon-$concealment analysis

Our approach uses the classic left-over hash lemma to show that the 2-universal hash function can be used as a strong randomness extractor to extract the 'residual' randomness in the transmitted codeword $\mathbf{X}$ and hence U^m (recall that $\mathbf{X} = \psi(U^m)$). It is well known that a positive rate commitment protocol is $\epsilon-$concealing, where $\epsilon > 0$ is *exponentially decreasing* in block length n, if it satisfies the *capacity-based secrecy* notion (cf. [DPP98, Def. 3.2]) and vice versa. We use a well established relation between *capacity-based secrecy* and the *bias-based secrecy* (cf. [DPP98, Th. 4.1]) to prove that our protocol is ϵ-concealing.

To begin, we prove that our protocol satisfies bias-based secrecy by essentially proving the perfect secrecy of the key $\texttt{Ext}(\mathbf{X})$; here we crucially use the *leftover hash* lemma. Several versions of this lemma exists (cf. [ILL89, DRS04a] for instance); we use the following:

Lemma 8.1. *Let $\mathcal{G} = \{g : \{0,1\}^n \to \{0,1\}^l\}$ be a family of universal hash functions. Then, for any hash function G chosen uniformly at random from $\mathcal{G}$, and W*

$$\|(P_{G(W),G} - P_{U_l,G})\| \leq \frac{1}{2}\sqrt{2^{-H_\infty(W)}2^l}$$

where $U_l \sim \mathit{Unif}\big(\{0,1\}^l\big)$.

We seek to lower bound $H_\infty(U^m)$. Toward this, we seek to analyse the conditional min-entropy of U^m conditioned on the view of Bob (this quantity lower bounds the min-entropy of interest). However, owing to the continuous alphabet of Bob's observation over the channel $\mathbf{Y}$, we need to take a 'discretization approach' to first "quantize" the channel output, say via $\mathbf{Y}^\Delta$, and then calculate the conditional min-entropy over such a quantized (and discrete) variable $\mathbf{Y}^\Delta$. This is important since min-entropy and conditional min-entropy (as well as their smooth "versions") do not posses the properties we seek when the variables are continuous.

Our treatment follows [NBSI08, CT91]. Let Y be a continuous random variable in $\mathbb{R}$ and $\Delta > 0$ be some constant. Then, from the mean value theorem, there exists a y_k such that

$$f_Y(y_k) = \frac{1}{\Delta}\int_{\Delta k}^{\Delta(k+1)} f_Y(y)dy$$

Let X be a discrete random variable in $\mathcal{X}$. Given a $x \in \mathcal{X}$, the conditional PDF of y given x is:

$$f_{Y|X}(y_k|x) = \frac{1}{\Delta}\int_{\Delta k}^{\Delta(k+1)} f_{Y|X}(y|x)dy$$

Let Y^Δ represent the quantized version of the continuous random variable Y, which takes value y_k for every $Y \in [\Delta k, \Delta(k+1)]$, with probability $P_{Y^\Delta}(y_k) = f_Y(y_k)\Delta$. Further, the joint probability distribution of the random variables XY^Δ is given as:

$$P_{XY^\Delta}(x, y_k) = P_X(x)P_{Y^\Delta|X}(y_k|x) = P_X(x)f_{Y|X}(y_k|x)\Delta$$

The quantized version of the conditional min-entropy is given by:

$$H_\infty(X|Y^\Delta) = \inf_{x,y_k}(-\log(P_{X|Y^\Delta}(x|y_k))) = \inf_{x,y_k}\log\left(\frac{f_Y(y_k)\Delta}{P_X(x)f_{Y|X}(y_k|x)\Delta}\right)$$

Now, for the string U^m, note that for quantization via $\Delta > 0$, we have

$$H_\infty(U^m|\mathbf{Y}, G_1(U^m), G_1, G_2(U^m), G_2) = \lim_{\Delta\to 0} H_\infty(U^m|\mathbf{Y}^\Delta, G_1(U^m), G_1, G_2(U^m), G_2)$$

where $\mathbf{Y}^\Delta$ is the vector of all quantised Y^Δ. Furthermore, from the definition of smooth-min-entropy, we know that

$$H_\infty(U^m|\mathbf{Y}^\Delta, G_1(U^m), G_1, G_2(U^m), G_2) = \lim_{\epsilon_1\to 0} H_\infty^{\epsilon_1}(U^m|\mathbf{Y}^\Delta, G_1(U^m), G_1, G_2(U^m), G_2)$$

To proceed, let us first lower bound $H_\infty^{\epsilon_1}(U^m|\mathbf{Y}^\Delta, G_1(U^m), G_1, G_2(U^m), G_2)$ for a given $\epsilon_1 > 0$ (we specify the choice of ϵ_1 later). Crucially, our lower bound will not depend on the quantization parameter Δ; this allows us to immediately extend the same lower bound to the limiting quantity: $\lim_{\Delta\to 0} H_\infty^{\epsilon_1}(U^m|\mathbf{Y}^\Delta, G_1(U^m), G_1, G_2(U^m), G_2)$. We now state the following lemma:

Lemma 8.2. *For any $\epsilon_1 > 0, \delta' > 0$ and n sufficiently large,*

$$H_\infty^{\epsilon_1}(U^m|\mathbf{Y}^\Delta, G_1(U^m), G_1, G_2(U^m), G_2) \geq n\left(\frac{1}{2}\log\left(\frac{P}{E}\right) - \frac{1}{2}\left(\log\left(1+\frac{P}{\gamma^2}\right)\right) - \beta_1 - \beta_2\right) - \log(\epsilon_1^{-1}) - n\delta' \tag{8.21}$$

The proof appears in Appendix C.2.

Since the lower bound does not depend on $\Delta > 0$, the following lemma is straight forward. Note the change to the continuous random vector $\mathbf{Y}$ (instead of $\mathbf{Y}^\Delta$ as in the previous lemma) as part of Bob's view.

Lemma 8.3. *For any $\epsilon_1 > 0, \delta' > 0$ and n sufficiently large,*

$$H_\infty^{\epsilon_1}(U^m|\mathbf{Y}, G_1(U^m), G_1, G_2(U^m), G_2) \geq n\left(\frac{1}{2}\log\left(\frac{P}{E}\right) - \frac{1}{2}\left(\log\left(1+\frac{P}{\gamma^2}\right)\right) - \beta_1 - \beta_2\right) - \log(\epsilon_1^{-1}) - n\delta' \tag{8.22}$$

Next, we use Lemma 8.1 to show that the distribution of the secret key $\text{Ext}(\mathbf{X})$ is statistically close to a uniform distribution thereby achieving bias-based secrecy. Let us fix $\epsilon_1 := 2^{-n\alpha_2}$, where $\alpha_2 > 0$ is an arbitrary small constant. We make the following correspondence in Lemma 8.1: $G \leftrightarrow \text{Ext}$, $W \leftrightarrow U^m$ and $l \leftrightarrow nR$ to get the following:

$$\begin{aligned}
&\|P_{\text{Ext}(U^m),\text{Ext}} - P_{U_l,\text{Ext}}\| \\
&\overset{(a)}{\leq} \frac{1}{2}\sqrt{2^{-H_\infty(U^m)}2^{nR}} \\
&\overset{(b)}{\leq} \frac{1}{2}\sqrt{2^{-H_\infty(U^m|\mathbf{Y}^\Delta, G_1(U^m), G_1, G_2(U^m), G_2)}2^{nR}} \\
&\overset{(c)}{\leq} \frac{1}{2}\sqrt{2^{-n\left(\frac{1}{2}\log\left(\frac{P}{E}\right) - \frac{1}{2}\left(\log\left(1+\frac{P}{\gamma^2}\right)\right) - \beta_1 - \beta_2 - \alpha_2 - \delta'\right)}2^{n\left(\frac{1}{2}\log\left(\frac{P}{E}\right) - \frac{1}{2}\left(\log\left(1+\frac{P}{\gamma^2}\right)\right) - \beta_3\right)}} \\
&= \frac{1}{2}\sqrt{2^{n(\beta_1+\beta_2+\alpha_2+\delta'-\beta_3))}} \\
&\overset{(d)}{\leq} 2^{-n\alpha_3}
\end{aligned} \tag{8.23}$$

where, n is sufficiently large so that $\delta' > 0$ is negligibly small such that $\alpha_3 > 0$. Here,

(a) follows directly from Lemma 8.1.

(b) follows as conditional min-entropy (under any $\Delta > 0$ sufficiently small) lower bounds min-entropy. This also holds under the limit $\Delta \to 0$.

(c) follows from the definition of R (cf. (8.15)) and Lemma 8.3

(d) follows from noting that β_3 is chosen such that $\delta' + \beta_1 + \beta_2 + \alpha_2 - \beta_3 < 0$; here, we note that α_2 is an arbitrarily chosen (small enough) constant, and $\delta' > 0$ can be made arbitrarily small for n sufficiently large. As such, a choice of $\beta_3 > \beta_1 + \beta_2$ is sufficient.

From (8.23) and Lemma 8.1, it follows that $n\left(\frac{1}{2}\log\left(\frac{P}{E}\right) - \frac{1}{2}\left(\log\left(1+\frac{P}{\gamma^2}\right)\right) - \beta_3\right)$ almost uniformly random bits can be extracted which proves the security of the secret key; this guarantees that our commitment protocol satisfies bias-based secrecy (cf. [DPP98, Def. 3.1]).

To conclude the concealment analysis, recall from our discussion earlier (see also [DPP98, Th. 4.1]) that bias-based secrecy under *exponentially decaying* statistical distance, as in (8.23), implies capacity-based secrecy. Since we have already shown that the protocol satisfies bias-based secrecy with exponentially decaying security parameter, hence, the protocol satisfies capacity-based secrecy. In particular, for n sufficiently large, $I(C;V_B) \leq \epsilon$ and our protocol is ϵ-concealing.

8.4.1.4 $\epsilon-$bindingness analysis

To analyse binding, we analyse the scenario where a potentially dishonest Alice seeks to confuse Bob between two (or more) different commit bit strings in $\{0,1\}^m$, say $\bar{u}^m$ and $\tilde{u}^m$ (i.e., Bob's test accepts two different commit strings). We seek to show that w.h.p our commitment protocol precludes any such possibility.

To begin, a cheating Alice seeks to maximize the set of potential bit strings in $\{0,1\}^m$ that would appear potential candidates in the list $\mathcal{L}(\mathbf{y})$ generated by Bob. Toward the same, a cheating Alice employs the following strategy: she first picks up a vector $\mathbf{x} \in \mathcal{S}(0, \sqrt{n(P-\gamma^2)})$ in the commit phase. Next, she privately fixes the variance of the Gaussian UNC[γ^2,δ^2] to the lowest value possible, i.e., γ^2. Let us define $E_s := \delta^2 - s^2$. Note that $E = E_\gamma = \delta^2 - \gamma^2$. Let $\mathbf{X} = \mathbf{x}$ be the transmitted vector and $\mathbf{Y} = \mathbf{y}$ be the bit string received by Bob's over the BSC(s). Note that a cheating Alice need not transmit a codeword, however $\mathbf{x} \in \mathcal{S}(P)$, i.e., the transmitted vector needs to satisfy the transmit power constraint P. Alice can cheat successfully by confusing Bob in the reveal phase only if she can find two *distinct* length-m binary strings, say $\bar{u}^m$ and $\tilde{u}^m$ such that (i) if $\psi(\bar{u}^m) = \bar{\mathbf{x}}$ and $\psi(\tilde{u}^m) = \tilde{\mathbf{x}}$ then $\mathbf{x}', \tilde{\mathbf{x}} \in \mathcal{L}(\mathbf{y})$, and (ii) $\bar{u}^m$ and $\tilde{u}^m$ pass the two rounds of sequential random hash exchange challenge (w.r.t hash functions $G_1(\cdot)$ and $G_2(\cdot)$). Let $\mathcal{A}$ denote all codewords in $\mathcal{C}$ corresponding to such length-m bit strings. Then, the following claim shows that $\mathcal{A}$ can be exponentially large.

Claim 8.4. *Given any $\eta > 0$, for n sufficiently large,*

$$|\mathcal{A}| \leq 2^{n(\bar{R}+\frac{1}{2}\log(\frac{E}{P})+\eta)}. \tag{8.24}$$

The proof appears in Appendix C.3. Note that, essentially, we can conclude that the choice of $s = \gamma^2$ is the 'best' choice for a cheating Alice (such a choice maximizes $|\mathcal{A}|$), i.e., Alice can be no worse than when it privately fixes the Gaussian UNC[γ^2,δ^2] o an AWGN channel with variance γ^2. We will choose $0 < \eta < \beta_1$ later (cf. Claim 8.5).

We now show that our choice of hash functions $G_1(\cdot)$ and $G_2(\cdot)$ allows us to essentially 'trim' down this set $\mathcal{A}$ of 'confusable' vectors all the way down to none. Recall that Alice's choice in the commit phase is $\mathbf{x}$. For a given hash value $h_1 \in \{0,1\}^{n(\bar{R}+\frac{1}{2}\log(\frac{E}{P})+\beta_1)}$ sent by

Alice, let

$$I_i(h_1) := \begin{cases} 1 & \text{if } G_1(u_i^m) = h_1 \\ 0 & \text{otherwise.} \end{cases} \tag{8.25}$$

$I_i(h_1)$ is an indicator random variable which identifies if u_i^m has a *hash-collision* under G_1 with the hash value h_1. Also, let

$$I(h_1) := \sum_{i=1}^{|\mathcal{A}|} I_i(h_1) \tag{8.26}$$

denotes the total number of hash collisions with hash value h_1. Then, the following holds when $0 < \eta < \beta_1$:

Claim 8.5. $\mathbb{P}\left(\exists h_1 \in \{0,1\}^{n(\bar{R}+\frac{1}{2}\log(\frac{E}{P})+\beta_1)} : I(h_1) > 8n+1\right) \to 0$ *exponentially in* n *as* $n \to \infty$.

The proof appears in Appendix C.4. This implies that the size of the 'confusable' set *after* the first hash challenge via G_1 for any h_1 is larger that $8n+1$ with exponentially small probability (in block length n). Conditioned on the event $I(h_1) < 8n+1$, $\forall h_1$, which occurs with high probability (w.h.p.), we now analyse the size of the 'confusable' set *after* the second hash challenge via G_2; let $\mathcal{F}_{h_1}$ denote this set of 'confusable' vectors after the second hash challenge for a given h_1. We prove the following claim (proof in Appendix C.5):

Claim 8.6. *For every* $h_1 \in \{0,1\}^{n(\bar{R}+\frac{1}{2}\log(\frac{E}{P})+\beta_1)}$, *we have for* n *sufficiently large*

$$rCl\mathbb{P}\left(\exists \mathbf{x} \neq \mathbf{x}' \in \mathcal{F}_{h_1} \colon G_2(u^m) = G_2(u'^m) \middle| I(h_1) \leq 8n+1\right) \leq 2^{-n\frac{\beta_2}{2}} \tag{8.27}$$

As the above claim holds for every h_1, and noting that[7] $\beta_2 > 0$, we now choose n large enough to conclude that our commitment protocol is $\epsilon-$binding.

8.4.2 Achievable protocol for $SER < 1$

The protocol would be same as the one proposed in the previous section for $SER \leq 1$ case except that the value of R is chosen to be

$$R = \frac{1}{2}\log\left(\frac{P}{\delta^2 - \tilde{\gamma}^2}\right) - \frac{1}{2}\log\left(1 + \frac{P}{\gamma^2}\right) - \beta_3 \tag{8.28}$$

When $\delta^2 \leq \left(1 + \frac{P}{P+\gamma^2}\right)\tilde{\gamma}^2$, the expression for R would bclearly evaluate to be positive. The analysis for soundness would follow from a similar Chernoff bound argument as was with the previous case. The proof for concealment and bindingness varies slightly as the choice of hash functions and randomness extractors would be different. We skip the details here.

[7]Recall that $\beta_2 > 0$ is a fixed parameter in our protocol.

Chapter 9

Conclusion

In a short summary this thesis explains the commitment problem and explores its realisation over noisy channels. We revise some noisy channel models from some previous studies and their related results. Through chapter 5, we look at an unreliable general class of channels, the Compound-DMCs and find a commitment capacity expression for the same. While studying the state-awareness models, a non trivial observation we make is that, state awareness at Alice's end seemingly has a lower converse bound expression than Alice not being state aware. While Bob being aware of the state doesn't degrade the capacity. However, at least for reduction to Compound-BSCs, these two expressions evaluate to the same capacity value, as is also apparent in our earlier work [YMBM21]. In chapter 6, we study the commitment capacity expression over RECs. This along with the capacity expressions we had from earlier for ECs, UNCs and CBSCs aloow us to observe some interesting trends in commitment capacity plots. We observe an interplay between the two forms of unreliability *compoundness* and *elasticity*. While channels with exclusively one form of unreliability, Compound-BSCs (*compoundness*) and ECs, RECs (*elasticity*) have positive commitment throughputs for all values of parameters γ, δ; channel with combined form of unreliability, UNC has positive commitment throughput only for $\delta < \gamma * \gamma$ from its capacity expression in (4.7). Our results also shed light on asymmetry in the effect of one-sided elasticity on commitment throughput. This has interesting consequences as a similar one-sided elasticity exhibits no such asymmetry when parties are only honest-but-curious (and not malicious).

With a motivation to better understand these trends, we looked at the Asymmetric-UNCs. We completely characterised the possibility region of commitment. We conjecture that the capacity expression actually evaluates to the lower bound in theorem 7.2. An information theoretic converse proof should fully settle the commitment characterisation over the assumed parameter ranges. Outside the assumed ranges, though there is a gap between the impossibility regime and the achievable protocols' regime.

Over Gaussian-UNCs too we were able to fully characterise the commitment possibility regime unconstrained inputs and for $SER > 1$. This is a surprise considering AWGN channels have infinite capacity for even the tightest power constraints (that are greater than zero). Moreover, our achievable schemes also indicate that even within the possibility regime, the throughputs are finite over non-trivial Gaussian-UNCs.

9.1 Future Scopes

With these observations we have in mind to extend our study to the following in the future.

- We seek to extend this study to completely study the asymmetric-UNCs and extend to more general channel models as well.
- There is some gap in the achievability and impossibility analysis of Asymmetric-AUNCs over regimes where γ is less than one of γ_A, γ_B. An information theoretic converse is also still open.
- There is also a gap between the possibility and impossibility characterisations of the Gaussian-UNCs for when $SER < 1$. We would like to fill that in too.
- Quantum bit commitment is another area we would like to explore. [LC97] showed that commitment is impossible over noiseless quantum channels. However, several weaker variants have been studied and found to show positive throughput in [BCH$^+$08]. Unreliable versions of noisy quantum channels could also be explored.

Chapter 10

Publications

(J) denotes a journal publication and (C) denotes a conference proceeding. (*) denotes that the author names are in alphabetical order.

List of works from this thesis **under preperation:**

(J) Mamindlapally, M., Yadav, A.K., Mishra, M. and Budkuley, A.J., 2021, July. Commitment capacity under cost constraints. In 2021 IEEE Transactions on Information Theory. IEEE.

(J) Yadav, A.K., Mamindlapally, M., Budkuley, A.J. and Mishra, M., 2021, July. Commitment over Compound Binary Symmetric Channels. In 2021 IEEE Transactions on Communications. IEEE.

(C)* Budkuley, A.J., Joshi, P., Mamindlapally, M. and Yadav, A.K., 2021. On the (Im)possibility of Commitment over Gaussian Unfair Noisy Channels. In 2022 IEEE Information Theory Workshop (ITW). IEEE.

(C)* Budkuley, A.J., Joshi, P., Mamindlapally, M. and Yadav, A.K., 2021. On the (Im)possibility of Commitment over Asymmetric Unfair Noisy Channels.

List of works from this thesis **published:**

(J)* A. J. Budkuley, P. Joshi, M. Mamindlapally and A. K. Yadav, "On Reverse Elastic Channels and the Asymmetry of Commitment Capacity Under Channel Elasticity," in IEEE Journal on Selected Areas in Communications, vol. 40, no. 3, pp. 862-870, March 2022, doi: 10.1109/JSAC.2022.3142304.

(C) A. K. Yadav, M. Mamindlapally, P. Joshi and A. J. Budkuley, "On Commitment over General Compound Channels," 2022 14th International Conference on COMmunication Systems & NETworkS (COMSNETS), 2022, pp. 488-496, doi: 10.1109/COMSNETS53615.2022.9668465.

(C)* A. J. Budkuley, P. Joshi, M. Mamindlapally and A. K. Yadav, "On the Commitment Capacity of Reverse Elastic Channels," 2021 IEEE Information Theory Workshop (ITW), 2021, pp. 1-6, doi: 10.1109/ITW48936.2021.9611485.

Here are two releavant published works of the author from his earlier **(bachelor) thesis [Mam21]:**

(C) A. K. Yadav, M. Mamindlapally, A. J. Budkuley and M. Mishra, "Commitment over Compound Binary Symmetric Channels," 2021 National Conference on Communications (NCC), 2021, pp. 1-6, doi: 10.1109/NCC52529.2021.9530060.

(C) M. Mamindlapally, A. K. Yadav, M. Mishra and A. J. Budkuley, "Commitment Capacity under Cost Constraints," 2021 IEEE International Symposium on Information Theory (ISIT), 2021, pp. 3208-3213, doi: 10.1109/ISIT45174.2021.9518204.

Bibliography

[BB11] Matthieu Bloch and João Barros. *Physical-Layer Security: From Information Theory to Security Engineering*. Cambridge University Press, Cambridge, 2011.

[BBCM95] Charles H Bennett, Gilles Brassard, Claude Crkpeau, and Ueli M Maurer. Generalized privacy amplification. *IEEE TRANSACTIONS ON INFORMATION THEORY*, 41(6):1915, 1995.

[BCH+08] Harry Buhrman, Matthias Christandl, Patrick Hayden, Hoi-Kwong Lo, and Stephanie Wehner. Possibility, impossibility, and cheat sensitivity of quantum-bit string commitment. *Physical Review A*, 78(2):022316, 2008.

[BJMY21] Amitalok J Budkuley, Pranav Joshi, Manideep Mamindlapally, and Anuj Kumar Yadav. On the commitment capacity of reverse elastic channels. In *2021 IEEE Information Theory Workshop (ITW)*, pages 1–6. IEEE, 2021.

[BJMY22a] Amitalok J Budkuley, Pranav Joshi, Manideep Mamindlapally, and Anuj Kumar Yadav. On reverse elastic channels and the asymmetry of commitment capacity under channel elasticity. *IEEE Journal on Selected Areas in Communications*, 2022.

[BJMY22b] Amitalok J Budkuley, Pranav Joshi, Manideep Mamindlapally, and Anuj Kumar Yadav. On the (im)possibility of comitment over gaussian unfair noisy channels. In preparation for ITW2022.

[BJMYon] Amitalok J Budkuley, Pranav Joshi, Manideep Mamindlapally, and Anuj Kumar Yadav. On the (im)possibility of comitment over asymmetric unfair noisy channels. In preparation.

[Blu83] Manuel Blum. Coin flipping by telephone a protocol for solving impossible problems. *ACM SIGACT News*, 15(1):23–27, January 1983.

[BR94] Mihir Bellare and John Rompel. Randomness-efficient oblivious sampling. In *Proceedings 35th Annual Symposium on Foundations of Computer Science*, pages 276–287. IEEE, 1994.

[CDN20] Claude Crépeau, Rafael Dowsley, and A. C. A. Nascimento. On the commitment capacity of unfair noisy channels. *IEEE Transactions on Information Theory*, 66(6):3745–3752, 2020.

[CK78] Imre Csiszár and Janos Korner. Broadcast channels with confidential messages. *IEEE transactions on information theory*, 24(3):339–348, 1978.

[CK88] Claude Crépeau and Joe Kilian. Achieving oblivious transfer using weakened security assumptions. In *[Proceedings 1988] 29th Annual Symposium on Foundations of Computer Science*, pages 42–52. IEEE Computer Society, 1988.

[CK11] Imre Csiszár and János Körner. *Information theory: coding theorems for discrete memoryless systems*. Cambridge University Press, 2011.

[Cré97] Claude Crépeau. Efficient cryptographic protocols based on noisy channels. In *International Conference on the Theory and Applications of Cryptographic Techniques*, pages 306–317. Springer, 1997.

[CT91] T.M. Cover and J.A. Thomas. *Elements of Information Theory*. Wiley, New York, 1991.

[CW79] J. Lawrence Carter and Mark N. Wegman. Universal classes of hash functions. *Journal of Computer and System Sciences*, 18(2):143–154, April 1979.

[DKS99] Ivan Damgård, Joe Kilian, and Louis Salvail. On the (im) possibility of basing oblivious transfer and bit commitment on weakened security assumptions. In *International Conference on the Theory and Applications of Cryptographic Techniques*, pages 56–73. Springer, 1999.

[DPP98] Ivan B Damgard, Torben P Pedersen, and Birgit Pfitzmann. Statistical secrecy and multibit commitments. *IEEE Transactions on Information Theory*, 44(3):1143–1151, 1998.

[DRS04a] Yevgeniy Dodis, Leonid Reyzin, and Adam Smith. Fuzzy extractors: How to generate strong keys from biometrics and other noisy data. In *International conference on the theory and applications of cryptographic techniques*, pages 523–540. Springer, 2004.

[DRS04b] Yevgeniy Dodis, Leonid Reyzin, and Adam Smith. Fuzzy extractors: How to generate strong keys from biometrics and other noisy data. In *International conference on the theory and applications of cryptographic techniques*, pages 523–540. Springer, 2004.

[EGL85] Shimon Even, Oded Goldreich, and Abraham Lempel. A randomized protocol for signing contracts. *Communications of the ACM*, 28(6):637–647, 1985.

[GK11] Abbas El Gamal and Young-Han Kim. *Network Information Theory*. Cambridge University Press, 2011.

[GMW87] O. Goldreich, S. Micali, and A. Wigderson. How to play ANY mental game. In *Proceedings of the nineteenth annual ACM symposium on Theory of computing*, STOC '87, pages 218–229, New York, NY, USA, January 1987. Association for Computing Machinery.

[HILL99] Johan Håstad, Russell Impagliazzo, Leonid A Levin, and Michael Luby. A pseudorandom generator from any one-way function. *SIAM Journal on Computing*, 28(4):1364–1396, 1999.

[HW22] Masahito Hayashi and Naqueeb Ahmad Warsi. Commitment capacity of classical-quantum channels. *arXiv preprint arXiv:2201.06333*, 2022.

[ILL89] Russell Impagliazzo, Leonid A Levin, and Michael Luby. Pseudo-random generation from one-way functions. In *Proceedings of the twenty-first annual ACM symposium on Theory of computing*, pages 12–24, 1989.

[IMNW06] Hideki Imai, Kirill Morozov, A. C. A. Nascimento, and Andreas Winter. Efficient protocols achieving the commitment capacity of noisy correlations. In *2006 IEEE International Symposium on Information Theory*, pages 1432–1436, 2006.

[KMS16] Dakshita Khurana, Hemanta K Maji, and Amit Sahai. Secure computation from elastic noisy channels. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 184–212. Springer, 2016.

[LC97] Hoi-Kwong Lo and Hoi Fung Chau. Is quantum bit commitment really possible? *Physical Review Letters*, 78(17):3410, 1997.

[LN98] A. Lapidoth and P. Narayan. Reliable communication under channel uncertainty. 44:2148–2177, 1998.

[Mam21] Manideep Mamindlapally. *Unconditionally secure commitment problem.* PhD thesis, 2021.

[MYMB21] Manideep Mamindlapally, Anuj Kumar Yadav, Manoj Mishra, and Amitalok J Budkuley. Commitment capacity under cost constraints. In *2021 IEEE International Symposium on Information Theory (ISIT)*, pages 3208–3213. IEEE, 2021.

[NBSI08] A. C. A. Nascimento, J. Barros, S. Skludarek, and H. Imai. The Commitment Capacity of the Gaussian Channel Is Infinite. *IEEE Transactions on Information Theory*, 54(6):2785–2789, June 2008.

[NS10] Mehrdad Nojoumian and Douglas R Stinson. Unconditionally secure first-price auction protocols using a multicomponent commitment scheme. In *International Conference on Information and Communications Security*, pages 266–280. Springer, 2010.

[NZ96] Noam Nisan and David Zuckerman. Randomness is linear in space. *Journal of Computer and System Sciences*, 52(1):43–52, 1996.

[OM08] Frédérique Oggier and Kirill Morozov. A practical scheme for string commitment based on the gaussian channel. In *2008 IEEE Information Theory Workshop*, pages 328–332. IEEE, 2008.

[RW05] Renato Renner and Stefan Wolf. Simple and tight bounds for information reconciliation and privacy amplification. In Bimal Roy, editor, *Advances in Cryptology - ASIACRYPT 2005*, pages 199–216, Berlin, Heidelberg, 2005. Springer Berlin Heidelberg.

[Sho94] Peter W Shor. Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings 35th annual symposium on foundations of computer science*, pages 124–134. Ieee, 1994.

[VDTR13] Alexander Vitanov, Frédéric Dupuis, Marco Tomamichel, and Renato Renner. Chain rules for smooth min- and max-entropies. *IEEE Transactions on Information Theory*, 59(5):2603–2612, 2013.

[WNI03] Andreas Winter, A. C. A. Nascimento, and Hideki Imai. Commitment capacity of discrete memoryless channels. In *IMA International Conference on Cryptography and Coding*, pages 35–51. Springer, 2003.

[WSL+19] Licheng Wang, Xiaoying Shen, Jing Li, Jun Shao, and Yixian Yang. Cryptographic primitives in blockchains. *Journal of Network and Computer Applications*, 127:43–58, 2019.

[Wyn75] Aaron D Wyner. The wire-tap channel. *Bell system technical journal*, 54(8):1355–1387, 1975.

[Wyn78] Aaron D. Wyner. The rate-distortion function for source coding with side information at the decoder-ii: General source. *Information and Control*, 38:60–80, 1978.

[YMBM21] Anuj Kumar Yadav, Manideep Mamindlapally, Amitalok J Budkuley, and Manoj Mishra. Commitment over compound binary symmetric channels. In *2021 National Conference on Communications (NCC)*, pages 1–6. IEEE, 2021.

[YMJB22] Anuj Kumar Yadav, Manideep Mamindlapally, Pranav Joshi, and Amitalok J Budkuley. On commitment over general compound channels. In *2022 14th International Conference on COMmunication Systems & NETworkS (COMSNETS)*, pages 488–496. IEEE, 2022.

Appendix A

Appendix Compound-DMCs

A.1 Proof of lemma 5.1

Proof of lemma. Recall that V_B denotes the view of Bob at the end of commit phase.

Let us define[1] $\tilde{c} := \arg\max_{c\in[2^{nR}]} T(\tilde{c}, \mathbf{X}, V_B)$. We now bound $\mathbb{P}(\hat{C} \neq C)$, where $\hat{C} = \hat{C}(V_B, \mathbf{X}) = \tilde{c}$. As the code is ϵ_n-binding for every $s \in \mathcal{S}$, we know that $\forall s \in \mathcal{S}$

$$\mathbb{P}\left(T(\bar{c}, \bar{\mathbf{X}}, V_B) = 1 \quad \& \quad T(\hat{c}, \hat{\mathbf{X}}, V_B) = 1 \middle| \, s\right) \leq \epsilon_n \tag{A.1}$$

for any two distinct $(\bar{c}, \bar{\mathbf{X}})$ and $(\hat{c}, \hat{\mathbf{X}})$. For the given decoder, we have

$$\begin{aligned}\mathbb{P}(\hat{C} \neq C) &= \mathbb{P}(\hat{C} = 0) + \mathbb{P}(\hat{C} \neq C | C \neq 0) \\ &\leq \epsilon_n + \epsilon_n \\ &= 2\epsilon_n. \end{aligned} \tag{A.2}$$

where in the penultimate inequality, the first part follows from noting that $\mathscr{P}_n$ is ϵ_n-binding, and the second part follows from the fact that conditioned on $\mathscr{P}_n$ being ϵ_n-binding, the probability that $\hat{C}$ is different from C is at most ϵ_n due to $\mathscr{P}_n$ being ϵ_n-sound.

We now use Fano's inequality (cf. [GK11]) to bound the conditional entropy.

$$\frac{1}{n} H(C|\mathbf{X}, V_B) \leq \frac{1}{n}\left(1 + \mathbb{P}(\hat{C} \neq C) nR\right) \tag{A.3}$$

$$\leq \frac{1}{n} + 2\epsilon_n R$$

$$\leq \epsilon_n'' \tag{A.4}$$

where $\epsilon_n'' \to 0$ as $n \to \infty$. This completes the proof of the lemma. □

[1] Although Bob's test T is a randomized test, it can be shown that one can construct from T a deterministic test with essentially the same soundness and bindingness performance (cf. []). Hence, for the rest of the converse, we consider that Bob's test is a deterministic function; as such, $\tilde{c}$ is well defined for such a deterministic test.

A.2 Proof of claim 5.1

Proof. Recall that the collision entropy can be bounded from below by min-entropy. Therefore, we have the following equation:

$$\begin{aligned} & H_c(\mathbf{X}|\mathbf{Y}=\mathbf{y}, J=j, \mathbf{X}_{|J}=\mathbf{x}_{|j}) \\ & \quad \geq H_\infty(\mathbf{X}|\mathbf{Y}=\mathbf{y}, J=j, \mathbf{X}_{|J}=\mathbf{x}_{|j}) \\ & \quad \geq \min_{\mathbf{y},j,\mathbf{x}_{|j}} H_\infty(\mathbf{X}|\mathbf{Y}=\mathbf{y}, J=j, \mathbf{X}_{|J}=\mathbf{x}_{|j}) \\ & \quad = H_\infty(\mathbf{X}|\mathbf{Y}, J, \mathbf{X}_{|J}) \end{aligned} \tag{A.5}$$

Therefore, we begin by establishing a lower bound on conditional min-entropy using chain rules on it's smooth version.

$$\begin{aligned} & H_\infty^{\epsilon_1}(\mathbf{X}|\mathbf{Y}, J, \mathbf{X}_{|J}) \\ & \quad \overset{(a)}{\geq} H_\infty(\mathbf{X}, \mathbf{X}_{|J}|\mathbf{Y}, J) - H_0(\mathbf{X}_{|J}|\mathbf{Y}, J) - \log(\epsilon_1^{-1}) \\ & \quad \overset{(b)}{=} H_\infty(\mathbf{X}|\mathbf{Y}, J) + H_\infty(\mathbf{X}_{|J}|\mathbf{Y}, J, \mathbf{X}) \\ & \qquad\quad - H_0(\mathbf{X}_{|J}|\mathbf{Y}, J) - \log(\epsilon_1^{-1}) \\ & \quad \overset{(c)}{=} H_\infty(\mathbf{X}|\mathbf{Y}, J) - H_0(\mathbf{X}_{|J}|\mathbf{Y}, J) - \log(\epsilon_1^{-1}) \\ & \quad \overset{(d)}{=} H_\infty(\mathbf{X}|\mathbf{Y}) - H_0(\mathbf{X}_{|J}|\mathbf{Y}, J) - \log(\epsilon_1^{-1}) \\ & \quad \overset{(e)}{\geq} (H(\mathbf{X}|\mathbf{Y}) - \xi') - H_0(\mathbf{X}_{|J}|\mathbf{Y}, J) - \log(\epsilon_1^{-1}) \\ & \quad \overset{(f)}{\geq} n(\min_s H(X|Y_s) - \xi) - n\zeta - \log(\epsilon_1^{-1}) \\ & \quad \overset{(g)}{=} n(\min_s H(X|Y_s) - \xi - \zeta - \kappa') \\ & \quad \overset{(h)}{=} n(\min_s H(X|Y_s) - \zeta') \end{aligned} \tag{A.6}$$

Here,

(a) follows from the chain rule for smooth min-entropy; see Claim C.1 and substitute $\mu = \epsilon_1$, $\mu_1 = 0$ and $\mu_2 = 0$ in (C.3).

(b) from the chain rule for min-entropy; see Claim C.1 and and substitute $\mu = 0$ and $\mu' = 0$ in (C.2).

(c) follows from the fact that $\mathbf{X}_{|J}$ is deterministic function of $\mathbf{X}$ and J.

(d) follows due to the Markov chain $\mathbf{X} \leftrightarrow \mathbf{Y} \leftrightarrow J$.

(e) follows from [NBSI08, Th. 1] which allows us to lower bound $H_\infty(\mathbf{X}|\mathbf{Y})$ using $H(\mathbf{X}|\mathbf{Y})$ for a large n.

(f) follows from noting that the worst-case scenario channel law is $\min_s H(X|Y_s)$ and from the fact that $\mathbf{X}_{|J} \in \mathcal{X}^{n\zeta}$.

(g) follows from setting $\epsilon = 2^{-\kappa' n}$, where $\kappa' > 0$ for sufficiently large n.

(h) Noting that κ' can be arbitrarily small for sufficiently large n, and $\zeta' = \xi + \zeta$.

Therefore, from (A.5) and (A.6) we have the required lower bound on the conditional collision entropy. □

Appendix B

Appendix RECs

B.1 Proof of lemma 6.1

Proof. We use the fact that $\mathscr{P}_n$ is ϵ_n-sound and ϵ_n-binding in this proof; furthermore, we can show that every protocol $\mathscr{P}_n$ can essentially recover the commit string under a 'noisy' version $\mathbf{Z}$ of $\mathbf{X}$ coupled with $\mathbf{Y}$ (we use Fano's inequality here).

Let us define[1] $\hat{c}(\mathbf{Z}, V_B) := \arg\max_{c\in[2^{nR}]} T(c, \mathbf{Z}, V_B)$. Here we crucially use the fact that for Alice's assumed cheating strategy where she fixes the channel to Bob as BSC(s), $s \in [\gamma, \delta]$, the effective channel from Z to Y is a BSC with crossover probability $\kappa_s \otimes s = \delta$ under every $s \in [\gamma, \delta]$.

We now bound $\mathbb{P}(\hat{C} \neq C)$, where $\hat{C} = \hat{c}(\mathbf{Z}, V_B)$. As the code is ϵ_n-binding, it follows that

$$\mathbb{P}\left(T(\bar{c}, \bar{\mathbf{X}}, V_B) = 1 \quad \& \quad T(\hat{c}, \hat{\mathbf{X}}, V_B) = 1\right) \leq \epsilon_n$$

for any two distinct $(\bar{c}, \bar{\mathbf{X}})$ and $(\hat{c}, \hat{\mathbf{X}})$ such that $\bar{c} \neq \hat{c}$. Furthermore, as the code is ϵ_n-sound,

$$\mathbb{P}\left(T(c, \mathbf{Z}, V_B) = 1\right) \geq 1 - \epsilon_n.$$

where we crucially use the fact that Z to Y is a BSC(δ) channel. Note that for the converse, we assume an *averaged* (over commit strings C) soundness criterion, where we replace the 'max' in (8.1) with an average over C.[2] Thus, for the given decoder, we then have

$$\begin{aligned}\mathbb{P}(\hat{C} \neq C) &= \mathbb{P}(\hat{C} = 0) + \mathbb{P}(\hat{C} \neq C | \hat{C} \neq 0) \\ &\leq \epsilon_n + \epsilon_n \\ &\leq 2\epsilon_n.\end{aligned}$$

where in the penultimate inequality, the first part follows from noting that $\mathscr{P}_n$ is ϵ_n-binding, and the second part follows from the fact that conditioned on $\mathscr{P}_n$ being ϵ_n-binding, the probability that $\hat{C} = \hat{C}(\mathbf{Z}, V_B)$ is different from C is at most ϵ_n due to $\mathscr{P}_n$ being ϵ_n-sound.

[1] Although Bob's test T is a randomized test, it can be shown that one can construct from T a deterministic test with essentially the same soundness and bindingness performance. Hence, for the rest of the converse, we consider that Bob's test is a deterministic function; as such, $\hat{c}$ is well defined for such a deterministic test.

[2] This is a stronger converse as impossibility under the *average* criterion implies impossibility over the *maximal* criterion in (8.1).

We now use Fano's inequality (cf. [GK11]) to bound the conditional entropy.

$$\begin{aligned} H(C|\mathbf{Z}, V_B) &\leq 1 + \mathbb{P}(\hat{C} \neq C)nR \\ &\leq n\epsilon'_n \end{aligned}$$

where $\epsilon'_n(\epsilon) := \frac{1}{n} + 2\epsilon_n R \to 0$ as $\epsilon_n \to 0$. □

B.2 Proof of lemma 8.2

Proof. Before we start with the proof, we recap (without proof) a few well known results.

Claim B.1 (Min-entropy [VDTR13])**.** *For any $0 \leq \mu, \mu', \mu_1, \mu_2 < 1$ and any set of jointly distributed random variables (X, Y, W), we have*

$$\begin{aligned} H_\infty^{\mu+\mu'}(X, Y|W) - H_\infty^{\mu'}(Y|W) & \\ \geq H_\infty^{\mu}(X|Y, W) & \quad \text{(B.1)} \\ \geq H_\infty^{\mu_1}(X, Y|W) - H_0^{\mu_2}(Y|W) - \log\left[\frac{1}{\mu - \mu_1 - \mu_2}\right] & \quad \text{(B.2)} \end{aligned}$$

Claim B.2 (Max-entropy [VDTR13, RW05])**.** *For any $0 \leq \mu, \mu', \mu_1, \mu_2 < 1$ and any set of jointly distributed random variables (X, Y, W), we have*

$$\begin{aligned} H_0^{\mu+\mu'}(X, Y|W) - H_0^{\mu'}(Y|W) & \\ \leq H_0^{\mu}(X|Y, W) & \quad \text{(B.3)} \\ \leq H_0^{\mu_1}(X, Y|W) - H_\infty^{\mu_2}(Y|W) + \log\left[\frac{1}{\mu - \mu_1 - \mu_2}\right] & \quad \text{(B.4)} \end{aligned}$$

Now consider the following for any $\epsilon_1 > 0$:

$$
\begin{aligned}
& H_\infty^{\epsilon_1}(\mathbf{X}|\mathbf{Y}, G_1(\mathbf{X}), G_1, G_2(\mathbf{X}), G_2) \\
& \overset{(a)}{\geq} H_\infty(\mathbf{X}, G_1(\mathbf{X}), G_2(\mathbf{X})|\mathbf{Y}, G_1, G_2) \\
& \qquad - H_0(G_1(\mathbf{X}), G_2(\mathbf{X})|\mathbf{Y}, G_1, G_2) - \log(\epsilon_1^{-1}) \\
& \overset{(b)}{=} H_\infty(\mathbf{X}|\mathbf{Y}, G_1, G_2) + H_\infty(G_1(\mathbf{X}), G_2(\mathbf{X})|\mathbf{Y}, G_1, G_2, \mathbf{X}) \\
& \qquad - H_0(G_1(\mathbf{X}), G_2(\mathbf{X})|\mathbf{Y}, G_1, G_2) - \log(\epsilon_1^{-1}) \\
& \overset{(c)}{=} H_\infty(\mathbf{X}|\mathbf{Y}, G_1, G_2) \\
& \qquad - H_0(G_1(\mathbf{X}), G_2(\mathbf{X})|\mathbf{Y}, G_1, G_2) - \log(\epsilon_1^{-1}) \\
& \overset{(d)}{=} H_\infty(\mathbf{X}|\mathbf{Y}) - H_0(G_1(X), G_2(X)|\mathbf{Y}, G_1, G_2) - \log(\epsilon_1^{-1}) \\
& \overset{(e)}{\geq} H_\infty(\mathbf{X}|\mathbf{Y}) - H_0(G_1(\mathbf{X})|G_2(\mathbf{X}), \mathbf{Y}, G_1, G_2) \\
& \qquad - H_0(G_2(\mathbf{X})|\mathbf{Y}, G_1, G_2) - \log(\epsilon_1^{-1}) \\
& \overset{(f)}{\geq} (H(\mathbf{X}|\mathbf{Y}) - \zeta') - H_0(G_1(\mathbf{X})|G_2(\mathbf{X}), \mathbf{Y}, G_1, G_2) \\
& \qquad - H_0(G_2(\mathbf{X})|\mathbf{Y}, G_1, G_2) - \log(\epsilon_1^{-1}) \\
& \overset{(g)}{\geq} n(H(\delta) - \zeta) - n(H(\kappa) + \beta_1 + \beta_2) - \log(\epsilon_1^{-1}) \\
& = n(H(\delta) - \zeta - H(\kappa) - \beta_1 - \beta_2) - \log(\epsilon_1^{-1})
\end{aligned} \tag{B.5}
$$

where we have

(a) from the chain rule for smooth min-entropy; see Claim C.1 and substitute $\mu = \epsilon_1$, $\mu_1 = 0$ and $\mu_2 = 0$ in (C.3).

(b) from the chain rule for min-entropy; see Claim C.1 and substitute $\mu = 0$ and $\mu' = 0$ in (C.2).

(c) from the fact that $G_1(\mathbf{X})$ and $G_2(\mathbf{X})$ are deterministic functions of G_1, G_2 and $\mathbf{X}$.

(d) by the Markov chain $\mathbf{X} \leftrightarrow \mathbf{Y} \leftrightarrow (G_1, G_2)$.

(e) from the chain rule for max-entropy; see Claim C.2 and substitute $\mu = 0$ and $\mu' = 0$ in (C.4).

(f) from [NBSI08, Th. 1] which allows us to lower bound $H_\infty(\mathbf{X}|\mathbf{Y})$ in terms of $H(\mathbf{X}|\mathbf{Y})$ (via an appropriate smooth-min-entropy quantity); here $\zeta > 0$ can be made arbitrarily small for n sufficiently large

(g) by noting that the crossover probability is δ and from definition of max-entropy (also noting that the range of G_1 and G_2 is $\{0,1\}^{n(H(\kappa)+\beta_1)}$ and $\{0,1\}^{n\beta_2}$ respectively).

□

B.2.1 Proof of claim 8.4

Proof. From the definition of $\mathcal{A}$, we have

$$\begin{aligned} |\mathcal{A}| &\overset{(a)}{\leq} 2^{n(H(\kappa_s)+\eta)} \\ &\overset{(b)}{\leq} 2^{n(H(\kappa)+\eta)} \end{aligned} \tag{B.6}$$

where

(a) follows from noting that an honest Bob will accept a vector $\mathbf{x}'$ if $d_H(\mathbf{x}'\mathbf{y}) \in [n(\delta - \alpha_1), n(\delta+\alpha_1)]$; since Alice has fixed the REC$[\gamma, \delta]$ to a BSC(s), the total number of such vectors are at most $2^{n(H(\kappa_s)+\eta)}$, where $\eta > 0$ choice can be arbitrary, for n sufficiently large.

(b) follows from noting that $\kappa_s \leq \kappa = \frac{\delta-\gamma}{1-2\gamma} < 1/2$.

This concludes the proof of the claim.

B.3 Proof of claim 8.5

Recall that $G_1 \sim \text{Unif}\,(\mathcal{G}_1)$. Then,

$$\begin{aligned} \mathbf{E}_{G_1}[I(h_1)] &\overset{(a)}{\leq} \sum_{i=1}^{|\mathcal{A}|} 2^{-(n(H(\kappa)+\beta_1))} \\ &\overset{(b)}{\leq} 2^{n(\eta-\beta_1)} \\ &\overset{(c)}{\leq} 2^{-n\tilde{\beta}_1} \end{aligned} \tag{B.7}$$

which is independent of h_1. Here (a) follows from the definition of $\mathcal{G}_1$, (b) follows from Claim 8.4 and noting that $\beta_1 > \eta$; letting $\tilde{\beta}_1 := \beta_1 - \eta > 0$ gives us (c). Note that for n sufficiently large, we have $\mathbb{E}[I(h_1)] \leq 1$, $\forall h_1$.

We now need the following result by Rompel [BR94] to proceed:

Lemma B.1 ([BR94])**.** *Let $X_1, X_2, X_3....X_m \in [0,1]$ be k-wise independent random variables, where k is an even and positive integer. Let $X := \sum_{i=1}^m X_i$, $\mu := \mathbf{E}[X]$, and $\Delta > 0$ be a constant. Then,*

$$\mathbb{P}\left(|X-\mu| > \Delta\right) < O\left(\left(\frac{k\mu + k^2}{\Delta^2}\right)^{k/2}\right) \tag{B.8}$$

We now make the following correspondence: $k \leftrightarrow 4n$, $\Delta \leftrightarrow 2k = 8n$. Then, using the

union bound, we get:

$$\begin{aligned}
&\mathbb{P}\left(\exists h_1 \in \{0,1\}^{n(H(\kappa)+\beta_1)} : I(h_1) > 8n+1\right) && \text{(B.9)}\\
&\leq \sum_{h_1 \in \{0,1\}^{n(H(\kappa)+\beta_1)}} \mathbb{P}\left(I(h_1) > 8n+1\right) && \text{(B.10)}\\
&\overset{(a)}{\leq} 2^{n(H(\kappa)+\beta_1)} O\Big(\Big(\frac{k\mu+k^2}{\Delta^2}\Big)^{k/2}\Big)\\
&\overset{(b)}{\leq} 2^{n(H(\kappa)+\beta_1)} O\Big(\Big(\frac{1+k}{4k}\Big)^{k/2}\Big)\\
&< 2^{n(H(\kappa)+\beta_1)} O(2^{-k/2})\\
&= 2^{n(H(\kappa)+\beta_1)} O(2^{-n}) && \text{(B.11)}
\end{aligned}$$

where we have

(a) from Lemma C.2

(b) by noting that for n sufficiently large, $\mu = \mathbb{E}[I(h_1)] \leq 1$, $\forall h_1$, and making the correspondence $\Delta \leftrightarrow 2k$.

Now note that (C.16) tends to zero exponentially fast as we have $(H(\kappa)+\beta_1) < 1$. This completes the proof of claim. □

B.3.1 Proof of claim 8.6

Proof. Recall the definition of $\mathcal{F}_{h_1}$, and let $\mathcal{F} := \max_{h_1} \mathcal{F}_{h_1}$. Note that $|\mathcal{F}| \leq 8n+1$. Noting that $G_2 \sim \text{Unif}(\mathcal{G}_2)$, where $\mathcal{G}_2 = \{g_2 : \{0,1\}^n \to \{0,1\}^{n\beta_2}\}$, we have for every $h_1 \in \{0,1\}^{n(H(\kappa)+\beta_1)}$,

$$\begin{aligned}
&\mathbb{P}\left(\exists \mathbf{x} \neq \mathbf{x}' \in \mathcal{F}_{h_1} : G_2(\mathbf{x}) = G_2(\mathbf{x}') \middle| I(h_1) \leq 8n+1\right)\\
&\overset{(a)}{\leq} \binom{\mathcal{F}}{2} \mathbb{P}\left(G_2(\mathbf{x}) = G_2(\mathbf{x}')\right)\\
&\overset{(b)}{\leq} \binom{8n+1}{2} 2^{-n\beta_2}\\
&< (8n+1)(8n) 2^{-n\beta_2}\\
&\leq 2^{-n\frac{\beta_2}{2}} \qquad \text{for } n \text{ large enough} && \text{(B.12)}
\end{aligned}$$

where (a) follows from the definition of $\mathcal{F}$, and using the union bound (on distinct pairs of vectors in $\mathcal{F}$); we get (b) from the definition of $\mathcal{G}_2$. This completes the proof of the claim. □

Appendix C

Appendix Asymmetric-UNCs and Gaussian-UNCs

C.1 Proof of claim 8.1

Proof. Consider any general commitment protocol from Definition **??**, realised using a noiseless channel. Let's say we have Alice's commit string c, exchanged messages m, and codeword $\mathbf{x}$ which Bob receives noiselessly as $\mathbf{y} = \mathbf{x}$. This would mean that, at the end of the commit phase, Alice and Bob's views are $V_A = (c, \mathbf{x}, m)$ and $V_B = (\mathbf{x}, m)$, respectively. Let Alice reveal some $\tilde{c}$, $\tilde{\mathbf{x}}$, after which Bob performs a test $T(\tilde{c}, \tilde{\mathbf{x}}, V_B)$. Clearly, it is possible to formulate a test that fails for $\tilde{\mathbf{x}} \neq \mathbf{x}$, because Bob's View V_B contains $\mathbf{x}$. Let's therefore take such a test T. Now, consider an event E,

$$
\begin{aligned}
E &= \{T(c, \mathbf{x}, V_B) = 1\} \bigcap_{c' \neq c \in \mathcal{C}} \{T(c', \mathbf{x}, V_B) = 0\} \\
\Rightarrow \neg E &= \{T(c, \mathbf{x}, V_B) = 0\} \bigcup_{c' \neq c \in \mathcal{C}} \{T(c', \mathbf{x}, V_B) = 1\} \\
\Rightarrow \mathbb{P}[\neg E] &= \mathbb{P}[T(c, \mathbf{x}, V_B) = 0] \\
&\quad + \sum_{c' \neq c \in \mathcal{C}} \mathbb{P}\big[T(c', \mathbf{x}, V_B) = 1 | T(c, \mathbf{x}, V_B) = 1\big] \\
&\leq \epsilon_1 + |\mathcal{C}|\epsilon_3 \qquad \text{(C.1)}
\end{aligned}
$$

The last step follows from the ϵ_1-soundness and ϵ_3-bindingness property of the protocol. Also observe that if the event E were true, Bob could directly estimate Alice's string c with certainty, by simply performing the test T over all strings in $\mathcal{C}$. Now,

$$
\begin{aligned}
H(C|V_B) &\leq H(C, E|V_B) \\
&= H(E|V_B) + H(C|V_B, E) \\
&\leq H(E) + \mathbb{P}[E] \cdot H(C|V_B, E = \text{True}) \\
&\quad + \mathbb{P}(\neg E) \cdot H(C|V_B, E = \text{False}) \\
&\leq 2\sqrt{\epsilon_1 + |\mathcal{C}|\epsilon_3} + 0 + (\epsilon_1 + |\mathcal{C}|\epsilon_3) \log |\mathcal{C}|
\end{aligned}
$$

Now,

$$\begin{aligned}\Rightarrow I(C;V_B) &= H(C) - H(C|V_B)\\ &\geq (1-\epsilon_1-|\mathcal{C}|\epsilon_3)\log|\mathcal{C}| - 2\sqrt{\epsilon_1+|\mathcal{C}|\epsilon_3}\\ \epsilon_2 &\geq (1-\epsilon_1-|\mathcal{C}|\epsilon_3)\log|\mathcal{C}| - 2\sqrt{\epsilon_1+|\mathcal{C}|\epsilon_3}\end{aligned}$$

The reduction of $H(E)$ follows from its upperbound $H_2(\epsilon_1+|\mathcal{C}|\epsilon_3)$ from (C.1) and a general upperbound on binary entropy function $H_2(p)$ for general $p\in[0,1]$, $H_2(p)\leq 2\ln 2\sqrt{p(1-p)}\leq 2\sqrt{p}$. □

C.2 Proof of lemma 8.2

First, we recap (without proof) a few well known results.

Claim C.1 (Min-entropy [VDTR13]). *For any $\mu,\mu',\mu_1,\mu_2\in[0,1)$ and any set of jointly distributed random variables (X,Y,W), we have*

$$\begin{aligned}rCl \qquad H_\infty^{\mu+\mu'}(X,Y|W) - H_\infty^{\mu'}(Y|W) &\\ \geq H_\infty^{\mu}(X|Y,W) &\qquad \text{(C.2)}\\ \geq H_\infty^{\mu_1}(X,Y|W) - H_0^{\mu_2}(Y|W) - \log\left[\frac{1}{\mu-\mu_1-\mu_2}\right] &\qquad \text{(C.3)}\end{aligned}$$

Claim C.2 (Max-entropy [VDTR13, RW05]). *For any $\mu,\mu',\mu_1,\mu_2\in[0,1)$ and any set of jointly distributed random variables (X,Y,W), we have*

$$\begin{aligned}rCl \qquad H_0^{\mu+\mu'}(X,Y|W) - H_0^{\mu'}(Y|W) &\\ \leq H_0^{\mu}(X|Y,W) &\qquad \text{(C.4)}\\ \leq H_0^{\mu_1}(X,Y|W) - H_\infty^{\mu_2}(Y|W) + \log\left[\frac{1}{\mu-\mu_1-\mu_2}\right] &\qquad \text{(C.5)}\end{aligned}$$

Now consider the following for any $\epsilon_1 > 0$:

$$
\begin{aligned}
& H_\infty^{\epsilon_1}(U^m|\mathbf{Y}^\Delta, G_1(U^m), G_1, G_2(U^m), G_2) \\
& \overset{(a)}{\geq} H_\infty(U^m, G_1(U^m), G_2(U^m)|\mathbf{Y}^\Delta, G_1, G_2) \\
& \qquad - H_0(G_1(U^m), G_2(U^m)|\mathbf{Y}^\Delta, G_1, G_2) - \log(\epsilon_1^{-1}) \\
& \overset{(b)}{=} H_\infty(U^m|\mathbf{Y}^\Delta, G_1, G_2) + H_\infty(G_1(U^m), G_2(U^m)|\mathbf{Y}^\Delta, G_1, G_2, U^m) \\
& \qquad - H_0(G_1(U^m), G_2(U^m)|\mathbf{Y}^\Delta, G_1, G_2) - \log(\epsilon_1^{-1}) \\
& \overset{(c)}{=} H_\infty(U^m|\mathbf{Y}^\Delta, G_1, G_2) \\
& \qquad - H_0(G_1(U^m), G_2(U^m)|\mathbf{Y}^\Delta, G_1, G_2) - \log(\epsilon_1^{-1}) \\
& \overset{(d)}{=} H_\infty(U^m|\mathbf{Y}^\Delta, G_1, G_2) - H_0(G_1(U^m), G_2(U^m)|\mathbf{Y}^\Delta, G_1, G_2) - \log(\epsilon_1^{-1}) \\
& \overset{(e)}{\geq} H_\infty(U^m|\mathbf{Y}^\Delta, G_1, G_2) - H_0(G_1(U^m)|G_2(U^m), \mathbf{Y}^\Delta, G_1, G_2) \\
& \qquad - H_0(G_2(U^m)|\mathbf{Y}^\Delta, G_1, G_2) - \log(\epsilon_1^{-1}) \\
& \overset{(f)}{\geq} H_\infty(U^m|\mathbf{Y}^\Delta, G_1, G_2) - n\left(\bar{R} + \frac{1}{2}\log\left(\frac{E}{P}\right) + \beta_1\right) - n\beta_2 - \log(\epsilon_1^{-1}) \qquad \text{(C.6)}
\end{aligned}
$$

(a) from the chain rule for smooth min-entropy; see Claim C.1 and substitute $\mu = \epsilon_1$, $\mu_1 = 0$ and $\mu_2 = 0$ in (C.3).

(b) from the chain rule for min-entropy; see Claim C.1 and substitute $\mu = 0$ and $\mu' = 0$ in (C.2).

(c) from the fact that $G_1(U^m)$ and $G_2(U^m)$ are deterministic functions of G_1, G_2 and U^m. The quantity
$H_\infty(G_1(U^m), G_2(U^m)|\mathbf{Y}^\Delta, G_1, G_2, U^m) = 0$ irrespective of $\mathbf{Y}^\Delta$.

(d) by the Markov chain $\mathbf{X} \leftrightarrow \mathbf{Y} \leftrightarrow (G_1, G_2)$.

(e) from the chain rule for max-entropy; see Claim C.2 and substitute $\mu = 0$ and $\mu' = 0$ in (C.4).

(f) by noting that the range of G_1 is $\{0,1\}^{n(\bar{R}+\frac{1}{2}\log(\frac{E}{P})+\beta_1)}$ and range of G_2 is $\{0,1\}^{m\beta_2}$.

We now lower bound the first term in (C.6), i.e., $H_\infty(U^m|\mathbf{Y}^\Delta, G_1, G_2)$. Here is the lemma with the lower bound.

Lemma C.1. *For any $\delta' > 0$ small enough and n sufficiently large, we have*

$$H_\infty(U^m|\mathbf{Y}^\Delta, G_1, G_2) \geq H(U^m) - I(U^m; \mathbf{Y}) - n\delta'. \qquad \text{(C.7)}$$

Proof. To prove this result, we first recap the following known result which relates conditional smooth-min-entropy and conditional (Shannon) entropy. We use the specific version in [NBSI08] (cf. [NBSI08, Thm. 1]).

Theorem C.1 ([NBSI08]). *Let P_{V^n,W^n} be a distribution over finite alphabets $\mathcal{V}^n \times \mathcal{W}^n$. Then, for any constants $\delta', \epsilon' > 0$ and n sufficiently large, we have*

$$H_\infty^{\epsilon'}(U^n|V^n) \geq H(U^n|V^n) - n\delta'. \tag{C.8}$$

We now simplify $H_\infty(U^m|\mathbf{Y}^\Delta, G_1, G_2)$ as follows:

$$\begin{aligned} H_\infty(U^m|\mathbf{Y}^\Delta, G_1, G_2) &\overset{(a)}{=} \lim_{\epsilon'\to 0} H_\infty^{\epsilon'}(U^m|\mathbf{Y}^\Delta, G_1, G_2) \\ &\overset{(b)}{\geq} \lim_{\epsilon'\to 0} H(U^m|\mathbf{Y}^\Delta, G_1, G_2) - n\delta' \\ &= H(U^m|\mathbf{Y}^\Delta, G_1, G_2) - n\delta' \\ &\overset{(c)}{=} H(U^m) - I(U^m; \mathbf{Y}^\Delta, G_1, G_2) - n\delta' \end{aligned} \tag{C.9}$$

where

1. follows from the definition of smooth-min-entropy.
2. follows from Theorem C.1.
3. follows from chain rule of mutual information.

Let us now simplify $I(U^m; \mathbf{Y}^\Delta, G_1, G_2)$ in (C.9) as $\Delta \to 0$. Note that

$$\begin{aligned} \lim_{\Delta\to 0} I(U^m; \mathbf{Y}^\Delta, G_1, G_2) &\overset{(a)}{=} I(U^m; \mathbf{Y}, G_1, G_2) \\ &\overset{(b)}{=} I(U^m; \mathbf{Y}) + I(U^m; G_1, G_2|\mathbf{Y}) \\ &\overset{(c)}{=} I(U^m; \mathbf{Y}). \end{aligned} \tag{C.10}$$

where

(a) follows from definition of $\mathbf{Y}^\Delta$ and the mutual information $I(U^m; \mathbf{Y}^\Delta, G_1, G_2)$ and their limiting values (as $\Delta \to 0$) .

(b) follows from the chain rule of mutual information

(c) follows from the Markov chain $U^m \leftrightarrow \mathbf{X} \leftrightarrow \mathbf{Y} \leftrightarrow (G_1, G_2)$.

Putting together (C.9) and (C.10), we have (C.7). This completes the proof of the lemma. □

Coming back to the main proof of Lemma 8.2, let us now simplify (C.6) as follows:

$$
\begin{aligned}
& H_{\infty}^{\epsilon_1}(U^m|\mathbf{Y}^{\Delta}, G_1(U^m), G_1, G_2(U^m), G_2) \\
& \overset{(a)}{\geq} (H(U^m) - I(U^m;\mathbf{Y}) - n\delta') - n\left(\bar{R} + \frac{1}{2}\log\left(\frac{E}{P}\right) + \beta_1\right) - n\beta_2 - \log(\epsilon_1^{-1}) \\
& \overset{(b)}{\geq} H(U^m) - I(\mathbf{X};\mathbf{Y}) - n\left(\bar{R} + \frac{1}{2}\log\left(\frac{E}{P}\right) + \beta_1\right) - n\beta_2 - \log(\epsilon_1^{-1}) - n\delta' \\
& \overset{(c)}{\geq} H(U^m) - n\mathbb{C}_{AWGN}(\gamma^2) - n\left(\bar{R} + \frac{1}{2}\log\left(\frac{E}{P}\right) + \beta_1\right) - n\beta_2 - \log(\epsilon_1^{-1}) - n\delta' \\
& \overset{(d)}{=} n\bar{R} - n\left(\frac{1}{2}\log\left(1 + \frac{P}{\gamma^2}\right)\right) - n\left(\bar{R} + \frac{1}{2}\log\left(\frac{E}{P}\right) + \beta_1\right) - n\beta_2 - \log(\epsilon_1^{-1}) - n\delta' \\
& = n\left(\bar{R} - \frac{1}{2}\log\left(1 + \frac{P}{\gamma^2}\right)\right) - n\left(\bar{R} + \frac{1}{2}\log\left(\frac{E}{P}\right) + \beta_1\right) - n\beta_2 - \log(\epsilon_1^{-1}) - n\delta' \\
& \overset{(e)}{=} n\left(\frac{1}{2}\log\left(\frac{P}{E}\right) - \frac{1}{2}\log\left(1 + \frac{P}{\gamma^2}\right)\right) - n\left(\beta_1 + \beta_2\right) - \log(\epsilon_1^{-1}) - n\delta'
\end{aligned}
\tag{C.11}
$$

(a) follows from Lemma C.1.

(b) follows from the Markov chain $U^m \leftrightarrow \mathbf{X} \leftrightarrow \mathbf{Y}$ and the data processing inequality.

(c) follows from noting that $I(\mathbf{X};\mathbf{Y}) \leq n\mathbb{C}_{AWGN}(\gamma^2)$ where $\mathbb{C}_{AWGN}(\gamma^2) := \frac{1}{2}\log\left(1 + \frac{P}{\gamma^2}\right)$ is the capacity of an AWGN channel with noise variance γ^2 under input power constraint P. Note that we need to allow the possibility that a cheating Bob may privately fix an AWGN channel where the variance may take any value in the range $[\gamma^2, \delta^2]$.

(d) follows from noting that $H(U^m) = n\bar{R}$ and substituting for $\mathbb{C}_{AWGN}(\gamma^2)$.

(e) follows from cancelling the term $n\bar{R}$ and rearranging the terms.

C.3 Proof of claim 8.4

From the definition of $\mathcal{A}$, we have

$$\begin{aligned} |\mathcal{A}| &\overset{(a)}{\leq} 2^{n(H(E_s)+\eta)} \\ &\overset{(b)}{\leq} 2^{n(H(E)+\eta)} \end{aligned} \tag{C.12}$$

where

(a) follows from noting that an honest Bob will accept a vector $\mathbf{x}'$ if $d_H(\mathbf{x}'\mathbf{y}) \in [n(\delta - \alpha_1), n(\delta+\alpha_1)]$; since Alice has fixed the REC$[\gamma, \delta]$ to a BSC(s), the total number of such vectors are at most $2^{n(H(E_s)+\eta)}$, where $\eta > 0$ choice can be arbitrary, for n sufficiently large.

(b) follows from noting that $E_s \leq E = \frac{\delta-\gamma}{1-2\gamma} < 1/2$.

C.4 Proof of claim 8.5

The proof of this claim follows by standard concentration techniques. We first bound the expected number of hash-collisions $\mathbf{E}_{G_1}[I(h_1)]$ for a given hash value h_1. In particular, we show that for n large enough, the expected number of such collisions $\mathbf{E}_{G_1}[I(h_1)] < 1$. We now concentrate using this expected value and identify the 'bad' hash values, say h', where the expected number of hash collisions $\mathbf{E}_{G_1}[I(h')]$ exceeds the average value by a 'non-trivial' amount. As $G_1 \sim \text{Unif}\,(\mathcal{G}_1)$, we have $\mathbf{E}_{G_1}[I(h_1)] \leq \sum_{i=1}^{|\mathcal{A}|} 2^{-(n(H(E)+\beta_1))} \leq 2^{n(\eta-\beta_1)}$, where the final inequality follows from Claim 8.4 and noting that $\beta_1 > \eta$. We set $\tilde{\beta}_1 := \beta_1 - \eta > 0$ to get $\mathbf{E}_{G_1}[I(h_1)] \leq 2^{-n\tilde{\beta}_1}$. Hence, for n sufficiently large, we have $\mathbb{E}[I(h_1)] \leq 1$, $\forall h_1$. We need the following result to proceed:

Lemma C.2 ([BR94]). *Let $X_1, X_2, X_3 .... X_m \in [0,1]$ be k-wise independent random variables, where k is an even and positive integer. Let $X := \sum_{i=1}^{m} X_i$, $\mu := \mathbf{E}[X]$, and $\Delta > 0$ be a constant. Then,*

$$\mathbb{P}\left(|X - \mu| > \Delta\right) < O\left(\left(\frac{k\mu + k^2}{\Delta^2}\right)^{k/2}\right) \tag{C.13}$$

We make the following correspondence: $k \leftrightarrow 4n$, $\Delta \leftrightarrow 2k = 8n$. Then, using the union

bound, we get:

$$\begin{aligned}
&\mathbb{P}\left(\exists h_1 \in \{0,1\}^{n(H(E)+\beta_1)} : I(h_1) > 8n+1\right) && \text{(C.14)}\\
&\leq \sum_{h_1 \in \{0,1\}^{n(H(E)+\beta_1)}} \mathbb{P}\left(I(h_1) > 8n+1\right) && \text{(C.15)}\\
&\overset{(a)}{\leq} 2^{n(H(E)+\beta_1)} O\Big(\Big(\frac{k\mu + k^2}{\Delta^2}\Big)^{k/2}\Big)\\
&\overset{(b)}{\leq} 2^{n(H(E)+\beta_1)} O\Big(\Big(\frac{1+k}{4k}\Big)^{k/2}\Big)\\
&< 2^{n(H(E)+\beta_1)} O(2^{-k/2})\\
&= 2^{n(H(E)+\beta_1)} O(2^{-n}) && \text{(C.16)}
\end{aligned}$$

where we have

(a) from Lemma C.2

(b) by noting that for n sufficiently large, $\mu = \mathbb{E}[I(h_1)] \leq 1$, $\forall h_1$, and making the correspondence $\Delta \leftrightarrow 2k$.

Now note that (C.16) tends to zero exponentially fast as we have $(H(E) + \beta_1) < 1$.

C.5 Proof of claim 8.6

Recall the definition of $\mathcal{F}_{h_1}$, and let $\mathcal{F} := \max_{h_1} \mathcal{F}_{h_1}$. Note that $|\mathcal{F}| \leq 8n + 1$. Noting that $G_2 \sim \text{Unif}(\mathcal{G}_2)$, where $\mathcal{G}_2 = \{g_2 : \{0,1\}^n \to \{0,1\}^{n\beta_2}\}$, we have for every $h_1 \in \{0,1\}^{n(H(E)+\beta_1)}$,

$$\begin{aligned}
&\mathbb{P}\left(\exists \mathbf{x} \neq \mathbf{x}' \in \mathcal{F}_{h_1} : G_2(\mathbf{x}) = G_2(\mathbf{x}') \middle| I(h_1) \leq 8n+1\right)\\
&\overset{(a)}{\leq} \binom{\mathcal{F}}{2} \mathbb{P}\left(G_2(\mathbf{x}) = G_2(\mathbf{x}')\right)\\
&\overset{(b)}{\leq} \binom{8n+1}{2} 2^{-n\beta_2}\\
&\leq 2^{-n\frac{\beta_2}{2}} \qquad \text{for } n \text{ large enough,} && \text{(C.17)}
\end{aligned}$$

where (a) follows from the definition of $\mathcal{F}$, and using the union bound (on distinct pairs of vectors in $\mathcal{F}$); we get (b) from the definition of $\mathcal{G}_2$.