# INFORMATION THEORETIC CRYPTANALYSIS AND RELIABLE COMMUNICATIONS UNDER CODEBOOK MISMATCH

by

Yücel Altuğ

B.S., Electrical and Electronics Engineering, Boğaziçi University, 2006

Submitted to the Institute for Graduate Studies in
Science and Engineering in partial fulfillment of
the requirements for the degree of
Master of Science

Graduate Program in Department of Electrical and Electronics Engineering

Boğaziçi University

2008

# ACKNOWLEDGEMENTS

First of all, I should faithfully state that I am grateful to my thesis supervisor Mehmet Kıvanç Mıhçak, for being an "optimum" (in approximately every sense) supervisor, a true friend and an elder brother, simultaneously. I owe to him almost everything I know about research.

I am also thankful to Süleyman Serdar Kozat and Hakan Deliç for their helpful comments and attendance to my thesis defense.

The gratitude from the bottom of my heart goes to, Nafiz Polat Ayerden, Mustafa Orhan Dirik, Muharrem Orkun Sağlamdemir, Cumhur Ozan Yalçın and Ömer Yetik simply for their *absolute* friendship, which I hope to enjoy throughout the rest of my life.

I want to express my sincere thanks to dear friends Sergül Aydöre, Özgur Dalkılıç, Onur Özyeşil (especially for the technical discussions and very insightful comments about the codebook mismatch problem) and Ekin Olcan Şahin.

Most importantly, I am indebted to my family for their true love, limitless support and endless patience.

# ABSTRACT

## INFORMATION THEORETIC CRYPTANALYSIS AND RELIABLE COMMUNICATIONS UNDER CODEBOOK MISMATCH

In this thesis, usage of typicality in two different concepts is investigated. In the first concept, a new approach on cryptanalysis is proposed where the goal is to explore the fundamental limits of a specific class of attacks against a particular cryptosystem. As a first step, the approach is applied on ABSG, which is an LFSR-based stream cipher where irregular decimation techniques are utilized. Consequently, under a set of mild assumptions, which are common in cryptanalysis, the tight lower bound on the algorithmic complexity of successful exhaustive search type Query-Based Key-Recovery attacks are derived where the proofs rely on the concept of typicality for single random variable. In the second concept, we define a new problem, which we called "codebook mismatch problem", which is a generalization of the traditional point-to-point to communication setup. Under independent identically distributed encoder codewords assumption, it is proven that the operational capacity of the system is equal to the information capacity of the system, defined as $\max_{p(x)} I(U;Y)$.

# ÖZET

## BİLGİ KURAMSAL KRİPTOANALİZ VE KOD REHBERİ UYUMSUZLUĞU DURUMUNDA GÜVENİLİR İLETİŞİM

Bu tezde, tipikalitenin iki farklı kavramda kullanılması incelenmiştir. Birinci kavramda, amacın hususi bir kriptosisteme karşı, belirli bir saldırı sınıfı içerisindeki saldırıların karmaşıklıkları üzerindeki temel sınırların keşfedilmesinin olduğu yeni bir yaklaşım önerilmiştir. Bir ilk adım olarak, yaklaşım düzensiz kısaltma tekniklerini kullanan, LFSR-tabanlıbir akım şifreleyicisi olan ABSG üzerinde tatbik edilmiştir. Sonuç olarak, kriptanalizde yaygın olan mutedil kabullenimler altında etraflıarama türünden sorgu temelli anahtar geri alma saldırılarının sıkı alt limiti çıkarılmıştır. İspatlar, tek rassal değişken için tipikalite kavramına dayanmaktadır. İkinci kavramda, yeni bir problem olan, geleneksel tek kullanıcılı iletişim düzeneğinin genellenmiş hali "kod rehberi uyumsuzluğu problemini" tanımladık. Bağımsız özdeş dağılmış kod kelimeleri kabullenimi altında, sistemin operasyonel kapasitesinin $\max_{p(x)} I(U;Y)$ olarak tanımlanan bilgi kapasitesine eşit olduğu gösterilmiştir.

# TABLE OF CONTENTS

# LIST OF FIGURES

# LIST OF TABLES

# LIST OF SYMBOLS

| | |
|---|---|
| $\oplus$ | Addition modulo 2 |
| $\lvert\mathcal{S}\rvert$ | Cardinality of set $\mathcal{S}$ |
| $\doteq$ | Equality to the first order in the exponent |
| $\mathrm{E}\left[\cdot\right]$ | Expectation operator |
| $\forall$ | For all |
| $\varnothing$ | Internal state sequence value where an output bit is generated |
| $\bigwedge$ | Logical "AND" operator |
| $\bigvee$ | Logical "OR" operator |
| $\bigcup$ | Union operator for sets |
| $\mathfrak{A}$ | Any QuBaR attack algorithm against ABSG |
| $\mathfrak{A}^E$ | Exhaustive search type QuBaR attack algorithm against ABSG |
| $\mathcal{A}$ | Algorithm $\mathcal{A}$ |
| $\mathcal{B}$ | Algorithm $\mathcal{B}$ |
| $\mathcal{C}$ | Encoder's codebook |
| $\tilde{\mathcal{C}}$ | Decoder's codebook |
| $\mathcal{C}\left(\mathfrak{A}\right)$ | Algorithmic complexity of QuBaR attack algorithm $\mathfrak{A}$ against ABSG |
| $\mathcal{C}_{ave}\left(\mathfrak{A}\right)$ | Average complexity of the QuBaR attack algorithm $\mathfrak{A}$ against ABSG |
| $\underline{\mathcal{C}}^E_{min}$ | To the first order in the exponent achievable lower bound on the complexity of any exhaustive search type QuBaR attack algorithm against ABSG |
| $\mathcal{E}$ | Error event |
| $\mathcal{M}$ | Recursive mapping $\mathcal{M}$ used in the definition of algorithm $\mathcal{A}$ |
| $\mathcal{S}^E$ | The class of exhaustive search type QuBaR attack algorithms against ABSG |
| $\mathcal{T}$ | Check algorithm in a QuBaR attack algorithm |
| $(\mathcal{X}, p(y\lvert x), \mathcal{Y}, p(u\lvert x), \mathcal{U})$ | Discrete memoryless codebook mismatched channel |
| $\mathcal{W}$ | Set of messages to be transmitted |

| | |
|---|---|
| $A_\epsilon^{(n)}(X)$ | Typical set with respect to distribution $p(x)$ |
| $C$ | Information capacity of the discrete memoryless i.i.d. codebook mismatched channel |
| $exp(L)$ | Complexity measure corresponding to "exponential complexity" |
| $G$ | A guess in a QuBaR attack algorithm |
| $H$ | Index of the $i$-th $\varnothing$ in the internal state sequence |
| $H(p)$ | Binary entropy function |
| $H(X)$ | Entropy of random variable $X$ |
| $H(X_1, X_2)$ | Joint entropy of random variables $X_1$ and $X_2$ |
| $H(X_1\|X_2)$ | Conditional entropy of random variable $X_1$ given $X_2$ |
| $I(X_1; X_2)$ | Mutual information between random variables $X_1$ and $X_2$ |
| $L$ | Degree of the generating LFSR's feedback polynomial |
| $poly(L)$ | Complexity measure corresponding to "polynomial complexity" |
| $P_e^{(n)}$ | Average probability of error |
| $p(u\|x)$ | Mismatch channel |
| $p(y\|x)$ | Communication channel |
| $Q$ | Random variable corresponding to the difference between two consecutive $\varnothing$'s in the internal state sequence |
| $\mathbf{u}^n(w)$ | Decoder's codeword corresponding to the message $w$ |
| $\hat{W}$ | Decoded message |
| $\mathbf{x}$ | Binary input sequence of ABSG algorithm |
| $\mathbf{x}^n(w)$ | Encoder's codeword corresponding to the message $w$ |
| $\mathbf{y}$ | Ternary internal state sequence of ABSG algorithm |
| $\lambda_i$ | Conditional probability of error corresponding to the message $i$ |
| $\lambda^{(n)}$ | Maximal probability of error |

# LIST OF ABBREVIATIONS

| | |
|---|---|
| AEP | Asymptotic Equipartition Property |
| BSG | Bit Search Generator |
| DMC | Discrete Memoryless Channel |
| DRM | Digital Rights Management |
| i.i.d. | Independent Identically Distributed |
| LFSR | Linear Feedback Shift Register |
| p.m.f. | Probability Mass Function |
| QuBaR | Query-Based Key-Recovery Attacks |
| SSG | Self Shrinking Generator |
| w.l.o.g. | Without Loss of Generality |

# 1. INTRODUCTION

## 1.1. Qualitative Introduction to AEP

Information theory, introduced by the seminal 1948 paper of Shannon [1], which states the fundamental performance limits of lossless source coding and the error-free communication, may be considered one of the most important improvements of the engineering sciences in the 20th century, since it forms the fundamentals of modern digital communication. Almost every information theorist agrees that the most important concept of information theory is *asymptotic equipartition property* (AEP) which is the fundamental crux of the proofs of both the achievability and the (weak) converse parts of capacity results of source and channel coding [2].

Qualitatively, the concept of information is formalized by the *entropy* (the choice of the name is not by accident) concept defined in [1], which is a measure of the *uncertainty* included in the event, for which it is defined.[1] With these explanations in mind, the concept of *typicality* (which will be used interchangeably with the term AEP throughout the rest of the thesis) may be best summarized by the quote of Thomas Cover (co-author of the standard textbook [2] of information theory): "Almost all events are almost equally surprising". Although this explanation may be counterintuitive at first glance for a person who does not study information theory before, taking into account the asymptotic nature of information theory and recalling law of large numbers makes the dissemination of the claim easier.

Before stating the AEP rigorously, we first want reader to take a short historical trip on ancestors of information theory and the evolution of different forms of AEP theorems.

[1] Of course, beside this qualitative explanation, there is an axiomatic development of the concept of entropy [1], which makes the choice of a logarithmic function (such as the entropy defined in the current way of information theory) a *must* instead of an *unjustified* choice, in order to satisfy the properties like *symmetry, normalization, continuity, grouping* that should be possessed by a measure of information.

The first known attempt to quantify the information is due to Nyquist. In [3] it is claimed that the transmission rate in a telegraph system is proportional to logarithm of the number of possible signal levels in a unit interval of transmission. Furthermore, the question of finding an *optimal* (in the sense of maximizing the transmission rate) code instead of Morse code is arisen.

Hartley, in his 1928 paper [4] introduced the formula[2] : $H = n \log s$, where $s$ is the number of possible states to choose from at each transmission, $n$ is the number of transmissions and $H$ is the "quantitative measure of information" from Hartley's point of view.

Note that neither Nyquist nor Hartley did not use the *probabilistic* nature of the problem of information transmission. The pioneer of introducing probability into the problem of information transmission is Wiener [5]. In his work, he introduced the concept of *differential entropy* for Gaussian random variables and did not consider the discrete random variables.

After these unsatisfactory attempts to quantify the information, Shannon formalized the concept of information in terms of his entropy definition (cf. Section 1.2) and stated the concept of typicality in his paper, provided the proof for i.i.d. random variables case and stated the result for stationary random processes. The generalization of the AEP theorem for stationary-ergodic random processes is due to McMillan (in addition to be the father of the modern name of the theorem, AEP, in information theory society) stated in [6] and independently to Breiman [7]. As a result, the AEP theorem is also termed as Shannon-McMillan-Breiman theorem in the literature. More detailed information regarding the history of information theory and specifically AEP may be found the excellent survey paper [8].

The importance of the typicality concept in information theory may be summarized by the following way: almost all theorems ever encountered in Shannon thoery[3]

[2]Note that this definition is a special case of Shannon's entropy and the two entities are equal for uniform distribution

[3]We refer to the problem of investigating the maximum achievable rates for different problems in

heavily relies on the concept of typicality in their proofs (both for achievability and converse parts). Of course, last decades' hot topic network information theory, which may be thought of as a generalization of the classical point-to-point communication to the case of multiple users case, also heavily uses the concept of typicality. For detailed surveys on network information theory, we refer the interested reader to [9, 10, 11].

To sum up, if one wants to prove a capacity result in an information theory related problem, then he/she most probably should use a kind of typicality argument.

## 1.2. Notation

In this chapter, we provide the notation used throughout the thesis. Boldface letters denote vectors; regular letters with subscripts denote individual elements of vectors. The vector $[a_1, a_2, \ldots, a_N]^T$ is compactly represented by $\mathbf{a}^N$. Furthermore, capital letters represent random variables and lowercase letters denote individual realizations of the corresponding random variable. The sequence of $\{a_1, a_2, \ldots, a_N\}$ is compactly represented by $\mathbf{a}_1^N$. Given $x \in \{0, 1\}$, $\bar{x}$ denotes the binary complement of $x$. The abbreviations "i.i.d.", "p.m.f." and "w.l.o.g." are shorthands for the terms "independent identically distributed", "probability mass function" and "without loss of generality", respectively.

For the discrete random variable $X$, corresponding p.m.f. is denoted by $p(x)$ by omitting subscript $X$, which should be evident from the context. E$[\cdot]$ denotes the expectation operator.

For discrete random variable $X$ defined on the discrete alphabet $\mathcal{X}$ with p.m.f. $p(x)$,

$$H(X) \stackrel{\triangle}{=} -\sum_{x \in \mathcal{X}} p(x) \log p(x), \text{[4]} \tag{1.1}$$

lossless source coding, lossy source coding (rate-distortion theory) and channel coding as Shannon theory for single encoder-decoder pair.

[4] All of the logarithms in the thesis is base 2.

denotes its *entropy*.

*Binary entropy* is defined as $H(p) \stackrel{\triangle}{=} -p\log p - (1-p)\log 1-p$, for $0 < p < 1$.

For discrete random variables $X_1, X_2$ defined on $\mathcal{X}_1 \times \mathcal{X}_2$ with joint p.m.f. $p(x_1, x_2)$,

$$H(X_1|X_2) \stackrel{\triangle}{=} -\sum_{x_1\in\mathcal{X}_1}\sum_{x_2\in\mathcal{X}_2} p(x_1,x_2)\log p(x_1|x_2), \tag{1.2}$$

$$H(X_1,X_2) \stackrel{\triangle}{=} -\sum_{x_1\in\mathcal{X}_1}\sum_{x_2\in\mathcal{X}_2} p(x_1,x_2)\log p(x_1,x_2), \tag{1.3}$$

$$I(X_1;X_2) \stackrel{\triangle}{=} -\sum_{x_1\in\mathcal{X}_1}\sum_{x_2\in\mathcal{X}_2} p(x_1,x_2)\log \frac{p(x_1,x_2)}{p(x_1)p(x_2)}, \tag{1.4}$$

denotes the *conditional entropy* or *equivocation* of $X_1$ given $X_2$, *joint entropy* of $X_1$ and $X_2$, and *mutual information* between $X_1$ and $X_2$, respectively.

Throughout the thesis, we say that "$a_n$ and $b_n$ are equal to the first order in the exponent" provided that $\lim_{n\to\infty}\frac{1}{n}\log\frac{a_n}{b_n} = 0$, which is denoted by $a_n \doteq b_n$ in our notation.

### 1.3. Quantitative Statement of AEP for Independent Random Variables

In this section, we review the concept of typicality (resp. joint typicality) for an i.i.d. sequence of random variables over a marginal (resp. joint) probability distribution and give AEP theorem for both cases. For the sake completeness and the beauty of the proofs, we include the full versions. Both definitions, theorems and proofs in this chapter are based on the ones given in [2].

We begin with the single random variable case:

**Definition 1.3.1** *The* typical set $A_\epsilon^{(n)}(X)$ *with respect to* $p(x)$ *is defined as:*

$$A_\epsilon^{(n)}(X) \stackrel{\triangle}{=} \left\{\mathbf{x}^n \in \mathcal{X}^n \ : \ \left|-\frac{1}{n}\log p(\mathbf{x}^n) - H(X)\right| < \epsilon\right\}. \tag{1.5}$$

Now we state the AEP for this case:

**Theorem 1.3.1** *(AEP) Given* $\{X_i\}_{i=1}^n$*, which are i.i.d. with distribution* $p(x)$*, and* $A_\epsilon^{(n)}(X)$ *is as defined in* (1.5)*, we have:*

*1.*

$$-\frac{1}{n}\log p\left(\mathbf{x}^n\right) \longrightarrow H(X), \text{in probability.} \tag{1.6}$$

*2.* $\Pr\left(A_\epsilon^{(n)}(X)\right) > 1-\epsilon$*, for* $n$ *sufficiently large.*

*3.* $|A_\epsilon^{(n)}(X)| \leq 2^{n(H(X)+\epsilon)}$.

*4.* $|A_\epsilon^{(n)}(X)| \geq (1-\epsilon)2^{(H(X)-\epsilon)}$*, for* $n$ *sufficiently large.*

**Proof:**

1. We have

$$\begin{aligned} -\frac{1}{n}\log p\left(\mathbf{x}^n\right) &= -\frac{1}{n}\sum_{i=1}^{n}\log p\left(x_i\right), & (1.7)\\ &\longrightarrow -\mathrm{E}\log p(x), \text{in probability} & (1.8)\\ &= H(X), & (1.9) \end{aligned}$$

   where (1.7) follows since functions of i.i.d. random variables are also i.i.d., (1.8) follows from law of large numbers and (1.9) follows from the definition of entropy. (1.9) concludes the proof of first item.

2. For any $\delta > 0$, there exists an $n_0$ such that for all $n > n_0$, we have

$$\Pr\left[\left|-\frac{1}{n}\log p\left(\mathbf{x}^n\right) - H(X)\right| < \epsilon\right] > 1-\delta, \tag{1.10}$$

   using (1.5) and (1.6) (recall the definition of convergence in probability). Choosing $\delta = \epsilon$ concludes the proof of this part.

3. We have

$$\begin{aligned} 1 &\geq \sum_{\mathbf{x}\in A_\epsilon^{(n)}(X)} p\left(\mathbf{x}^n\right), && (1.11)\\ &\geq \sum_{\mathbf{x}\in A_\epsilon^{(n)}(X)} 2^{-n(H(X)+\epsilon)}, && (1.12)\\ &= 2^{-n(H(X)+\epsilon)}|A_\epsilon^{(n)}(X)|, && (1.13) \end{aligned}$$

where (1.12) follows using (1.5). (1.13) concludes the proof of third item.

4. Using the result of second part, we have

$$\begin{aligned} 1-\epsilon &< \Pr\left(A_\epsilon^{(n)}(X)\right), && (1.14)\\ &\leq \sum_{\mathbf{x}^n\in A_\epsilon^{(n)}(X)} 2^{-n(H(X)-\epsilon)}, && (1.15)\\ &= 2^{-n(H(X)-\epsilon)}|A_\epsilon^{(n)}(X)|, && (1.16) \end{aligned}$$

where (1.15) follows using (1.5). (1.16) states the sought-after result. □

Next, we continue with the two random variables case, i.e. joint typicality.

**Definition 1.3.2** *The* jointly typical set *with respect to the distribution $p(x,y)$ is defined as:*

$$\begin{aligned} A_\epsilon^{(n)}(X,Y) \triangleq \Bigg\{ &(\mathbf{x}^n,\mathbf{y}^n)\in\mathcal{X}^n\times\mathcal{Y}^n \ : \ |-\frac{1}{n}\log p\left(\mathbf{x}^n\right)-H(X)|<\epsilon,\\ &|-\frac{1}{n}\log p\left(\mathbf{y}^n\right)-H(Y)|<\epsilon,\ |-\frac{1}{n}\log p\left(\mathbf{x}^n,\mathbf{y}^n\right)-H(X,Y)|<\epsilon,\Bigg\}, \end{aligned} \tag{1.17}$$

*where $p\left(\mathbf{x}^n,\mathbf{y}^n\right) \triangleq \prod_{i=1}^n p(x_i,y_i)$.*

**Theorem 1.3.2** *(Joint AEP) Let $(\mathbf{x}^n,\mathbf{y}^n)$ be realizations of random variables $X,Y$ jointly distributed with $p\left(\mathbf{x}^n,\mathbf{y}^n\right)=\prod_{i=1}^n p(x_i,y_i)$. Then, we have*

1. $\Pr\left[A_\epsilon^{(n)}(X,Y)\right] > 1-\epsilon$, *for sufficiently large* $n$.
2. $(1-\epsilon)2^{n(H(X,Y)-\epsilon)} \leq |A_\epsilon^{(n)}(X,Y)| \leq 2^{n(H(X,Y)+\epsilon)}$.
3. *If* $\left(\tilde{\mathbf{X}}^n, \tilde{\mathbf{Y}}^n\right) \sim p\left(\tilde{\mathbf{x}}^n\right) p\left(\tilde{\mathbf{y}}^n\right)$ *such that* $p\left(\tilde{\mathbf{x}}^n\right) = p\left(\mathbf{x}^n\right)$ *and* $p\left(\tilde{\mathbf{y}}^n\right) = p\left(\mathbf{y}^n\right)$, *then*

$$\Pr\left[\left(\tilde{\mathbf{X}}^n, \tilde{\mathbf{Y}}^n\right) \in A_\epsilon^{(n)}(X,Y)\right] \leq 2^{-n(I(X;Y)-3\epsilon)}. \tag{1.18}$$

*Also,*

$$\Pr\left[\left(\tilde{\mathbf{X}}^n, \tilde{\mathbf{Y}}^n\right) \in A_\epsilon^{(n)}(X,Y)\right] \geq (1-\epsilon)2^{-n(I(X;Y)+3\epsilon)}, \tag{1.19}$$

*for sufficiently large* $n$.

**Proof:**

1. Using similar arguments as in the proof of item (i) of Theorem 1.3.1 (independence, weak law of large numbers, convergence in probability), we conclude that for the given $\epsilon > 0$, there exists $n_1, n_2, n_3$ such that for all $n > n_1, n > n_2$ and $n > n_3$ we have

$$\Pr\left(|-\frac{1}{n}\log p\left(\mathbf{x}^n\right) - H(X)| \geq \epsilon\right) < \frac{\epsilon}{3}, \tag{1.20}$$

$$\Pr\left(|-\frac{1}{n}\log p\left(\mathbf{y}^n\right) - H(Y)| \geq \epsilon\right) < \frac{\epsilon}{3}, \tag{1.21}$$

$$\Pr\left(|-\frac{1}{n}\log p\left(\mathbf{x}^n, \mathbf{y}^n\right) - H(X,Y)| \geq \epsilon\right) < \frac{\epsilon}{3}, \tag{1.22}$$

   for sufficiently large $n$. Choosing $n > \max(n_1, n_2, n_3)$, the probability of the union of the sets in (1.20), (1.21) and (1.22) must be less than $\epsilon$, which establishes the result for the first item.
2. For the upper bound, we simply write

$$1 \geq \sum_{\mathbf{x}^n \in A_\epsilon^{(n)}(X,Y)} p\left(\mathbf{x}^n, \mathbf{y}^n\right), \tag{1.23}$$

$$\geq |A_\epsilon^{(n)}(X,Y)| 2^{-n(H(X,Y)+\epsilon)}, \tag{1.24}$$

where (1.24) follows using (1.17).

For the lower bound, we have (using the result of the first item)

$$\begin{aligned} 1-\epsilon &\leq \sum_{(\mathbf{x}^n,\mathbf{y}^n)\in A_\epsilon^{(n)}(X,Y)} p\left(\mathbf{x}^n,\mathbf{y}^n\right), && (1.25)\\ &\leq |A_\epsilon^{(n)}(X,Y)|2^{-n(H(X,Y)-\epsilon)}, && (1.26) \end{aligned}$$

where (1.26) follows (1.17).

3. We begin with first inequality.

From the statement, we have

$$\begin{aligned} \Pr\left[\left(\tilde{\mathbf{X}}^n,\tilde{\mathbf{Y}}^n\right)\right] &= \sum_{(\mathbf{x}^n,\mathbf{y}^n)\in A_\epsilon^{(n)}(X,Y)} p\left(\mathbf{x}^n\right)p\left(\mathbf{y}^n\right), && (1.27)\\ &\leq 2^{n(H(X,Y)+\epsilon)}2^{-n(H(X)-\epsilon)}2^{-n(H(Y)-\epsilon)}, && (1.28)\\ &= 2^{-n(I(X;Y)-3\epsilon)}, && (1.29) \end{aligned}$$

where (1.28) follows using (1.17). (1.29) states the first inequality of the third item.

Now, we continue with the second inequality

$$\begin{aligned} \Pr\left[\left(\tilde{\mathbf{X}}^n,\tilde{\mathbf{Y}}^n\right)\right] &= \sum_{(\mathbf{x}^n,\mathbf{y}^n)\in A_\epsilon^{(n)}(X,Y)} p\left(\mathbf{x}^n\right)p\left(\mathbf{y}^n\right), && (1.30)\\ &\geq (1-\epsilon)2^{n(H(X,Y)-\epsilon)}2^{n(H(X)+\epsilon)}2^{n(H(Y)+\epsilon)}, && (1.31)\\ &= (1-\epsilon)2^{-n(I(X;Y)+3\epsilon)}, \end{aligned}$$

where (1.31) using (1.17). Hence the theorem follows. □

## 1.4. Introduction to the Considered Problems

We basically investigated two "nearly-independent" concepts:

(i) First one is related to a cryptographic problem, where we introduce a (to the

best of our knowledge) novel approach to cryptanalysis. In our approach, the focus is jointly on a particular cryptosystem and a specific (sufficiently broad) class of attacks of interest at the same time. Then, under some mild conditions, the goal is to derive the *achievable fundamental performance limit* for the attacks within the considered class of interest against the cryptosystem at hand. The aforementioned limit should be "achievable", in the sense that it is necessary to provide an explicit attack construction of which performance coincides with the derived limit. Furthermore, the aforementioned limit should also necessarily be "fundamental", in the sense that within the considered specific class, there does not exist any attack of which performance is superior to the derived limit. The main concept employed in order to achieve this goal is Theorem 1.3.1 (cf. Chapter 2).

(ii) The other one is the introduction of a new "asymmetric codebook structure" concept in the classical point-to-point communication setup, of which theoretical and practical impacts are thoroughly explained in the following discussion, and as a first step "a memoryless" and "i.i.d." setup is investigated, for which the capacity is found where the main concept utilized in order to achieve this goal is Theorem 1.3.2 (cf. Chapter 3).

We begin our detailed discussion with the first problem mentioned above. Our proposed approach contrasts with the trend in conventional cryptanalysis, which can be outlined in two categories. In the first category, the focus is on the construction of a generic attack, which should be applicable (subject to slight modifications) to most cryptosystems; common examples include time-memory tradeoff attacks [12, 13], correlation attacks [14, 15], algebraic attacks [16, 17] and alike. The second category is conceptually on the opposite side of the spectrum. Here, given a particular cryptosystem, the focus is on the construction of a potentially-specialized attack, which is "tailored" specifically against the system at hand; hence, the resulting attack is not applicable to a broader class of cryptosystems in general. Although the approaches pursued in the aforementioned two attack categories are radically different, it is interesting to note that, for both of them the underlying fundamental goal is the same, which can be summarized as providing a "design advice" to the cryptosystem designer.

In practice, the cryptosystem designer is at first expected to test his/her proposed system against generic attacks (first category); thus, such attacks serve as a benchmark for the community of cryptosystem designers. Next, the cryptanalyst tests a proposed cryptosystem via constructing a cryptosystem-specific attack algorithm (second category). Both approaches are proven to be extremely valuable in practice since the first one provides a "unified approach" to cryptanalysis via providing some generic attack algorithms and the second one specifically tests the security of the considered cryptosystem and consequently yields its potential weaknesses. On the other hand, both categories of the conventional approach in cryptanalysis lack to provide fundamental performance bounds, i.e., the question of "what is the best that can be done?" goes unanswered. The main reason is that, for the first category, finding out a fundamental performance bound necessarily requires considering all possible cryptosystems, which is infeasible in practice; within the second category, providing a fundamental performance bound necessarily requires "describing" all possible cryptanalytic propositions (in a computational sense) and quantifying the resulting performances, which is again infeasible in practice.

In our proposed approach, we aim to derive "the best possible performance bound" [5] in a reasonably-confined setup. Intuitively, we "merge" the first and the second categories of the conventional cryptanalytic approach; we jointly focus on *both* a particular cryptosystem *and* a specific class of attacks, and subsequently aim to analytically quantify the fundamental, achievable performance bounds, i.e., specifically for a given cryptosystem, our goal is to find the achievable lower-bound on the complexity of a proposed class of attacks, under a set of mild assumptions. The main impact of this approach is that, it aims to provide an advice for the cryptanalyst, instead of the cryptosystem designer, in contrast with the conventional approach. If this resulting advice is "positive" (i.e., the fundamental achievable performance bound is of polynomial complexity), then the weakness of the analyzed cryptosystem is guaranteed (which can also be achieved via pursuing the second category of the conventional cryptanalytic approach). However, more interestingly, if the resulting advice is "negative" (i.e.,

[5]Note that, this approach is analogous to providing both achievability and converse proofs in classical information-theory problems. This connection will further be clarified throughout the thesis.

the fundamental achievable performance bound is of exponential complexity), then the considered class of attacks is *guaranteed* to be useless, which, in turn, directs a cryptanalyst to consider different classes of attacks, instead of experimenting with various attacks from the considered class via a (possibly educated) trial-and-error approach. Thus, the negative advice case (for which this thesis serves an exemplary purpose) constitutes the fundamental value of our approach. We believe that our efforts can be viewed as a contribution towards the goal of enhancing cryptanalytic approaches via incorporating a structural and procedural methodology.

In order to illustrate our approach, in this thesis we consider a class of Query-Based Key-Recovery attacks (of which precise definition is given in Section 2.2.2 of Chapter 2) targeted towards ABSG [18], which is an LFSR(linear feedback shift register)-based stream cipher that uses irregular decimation techniques. Recall that, within the class of stream ciphers, the usage of LFSRs is an attractive choice due to the implementation efficiency and favorable statistical properties of the LFSR output; however, security of LFSR-based stream ciphers is contingent upon applying additional non-linearities per the linear nature of LFSR [19]. An approach, which aims to achieve this task, is to use irregular decimation techniques to the LFSR output [18, 20, 21, 22]. The motivation lying behind the development of this approach is to render most conventional attacks useless (such as algebraic attacks). Shrinking [21] and self-shrinking generators (SSG) [22] are two important examples of this approach. In particular, in the literature SSG is well-known to be a very efficient algorithm and it has been shown to possess favorable security properties [23, 24, 25]. The bit-search generator (BSG) [20] and its variant ABSG [18] are newer algorithms, which also use irregular decimation techniques. In [26], it has been shown that the efficiency (output rate) of ABSG is superior to that of SSG and the security level of ABSG is at least the same level provided by SSG under a broad class of attacks. A detailed analysis of the statistical properties of ABSG and BSG algorithms has recently been presented in [27]. Since ABSG has been shown to be a state-of-the-art cryptosystem, in our developments we focus on it under a reasonable class of attacks and subsequently provide "negative advices" for the cryptanalyst in various setups of interest.

Next, we discuss the second problem we are interested in the thesis, namely "reliable communication under codebook mismatch" as promised at the beginning of this section. We first introduce the problem qualitatively in the following way: Consider the following setup for the error free transmission of information in a point-to-point (single encoder, single decoder) communication system where the encoder's and the decoder's codebooks are not perfectly matched, in other words they are not precisely the same as the other. We call this problem as "codebook mismatch problem" and the choice of the name will be more clear after the explanation provided next. To be more precise, at the codebook revealing case of traditional point-to-point communication setup, decoder does not receive the precise codebook of encoder, of which codewords will be the input to the communication channel, however receives a *perturbed*, yet *statistically related* version of them. We model this relation via a conditional distribution in a memoryless fashion. Lastly, both communicating parties know the statistical characterization of the encoder's codebook, the communication channel utilized during the communication phase and the aforementioned conditional distribution which models the statistical relation between the mismatched codebooks of the encoder and the decoder.[6] We defer the in depth definition of the problem to Chapter 3 and continue with comparing and contrasting the proposed scheme with the existing ones.

First of all, observe that the problem at hand may be thought as a variant of the classical *side information* problems of Shannon theory (e.g. [29, 30, 31, 32]) -which is not exactly the case for codebook mismatch- because of the similar "anti-symmetric" nature possessed by both the codebook mismatch and the traditional side information problems. First of all, let differentiate the problem at hand from the ones dealing with source coding (either lossless or lossy), by definition. Next, for the case of side information problems dealing with channel coding, observe that side information is about *the system parameters, and/or the noise corrupting the message*, but the codebooks employed in the system *always* shared between the parties, in other words either transmitter or receiver is *favored* by the usage of the provided side information which is not available to the other party, no matter whether this favorable situation turns out to

[6] As a result of these known quantities, statistical characterization of the decoder's codebook is also known at both sides.

increase the performance of the system or not. However, for the codebook mismatch problem at hand, there is *not* a shared codebook between the two communicating parties, as the name of the problem hints and the system parameters are precisely known by both the encoder and the decoder. After this much contrast with the vast body of the side information problems existing in the literature, we go on with the important and promising features of the codebook mismatch problem from both theoretical and practical aspects.

From a pure theoretical point of view, codebook mismatch problem is exciting, since it generalizes the classical approach of shared codebooks [1], to mismatched codebooks, which makes the latter a special case of the former.[7] By considering the fundamental importance of generalizing the existing concepts in mathematical sciences, such a generalization of Shannon's setup is an important merit possessed by codebook mismatch problem. Furthermore, this "antisymmetric phenomenon" may lead to other interesting problems (like capacity-rate problem mentioned below) which are important from a both theoretical (since it is very rare to see a new posed problem in Shannon theory) and practical point of view (of which main motivation is to provide a solution to a real life obstacle, see the discussion below), hence it is also very promising.

From a practical point of view, the most immediate impact of the codebook mismatch problem is on the topic of *robust signal hashing problem* [33], which aims to find a practical solution to the *content tracking with side information* problem where privacy is a major concern, which is an important phenomenon of the internet age, because with the vast dissemination of digital multimedia content over the internet, one of the major problems of the modern era is to determine "which signal has appeared where" in a reliable fashion. Consider a content owner who wants to know if anybody has used his/her signal(s) without getting the proper consent; in this scenario the content owner would like to keep track of such prohibited appearances. For various reasons, standard DRM (digital rights management) strategies fail to achieve this task since users may apply arbitrary quality-preserving modifications to the original

[7]Note that two system is equivalent if and only if the conditional probability distribution modelling the mismatch between the codebooks is a deterministic one-to-one mapping.

content. Information-hiding (also known as watermarking) [34, 35, 36] has been proposed as a countermeasure; however, one major problem with the watermarking-based protection mechanisms is that all targeted content need to be pre-processed (in order to embed content-owner information) before making it publicly available, which makes it practically useless for the cases where the valuable data has already been made public. In contrast with watermarking, "robust signal hashing" is another countermeasure which seems to bypass the aforementioned fundamental difficulty. In robust signal hashing, the goal is to extract perceptually-significant data (termed hash value) from signals, which are ideally approximately-invariant under perceptually-acceptable modifications. If this task is achieved, the extracted hash signals can potentially be used (as side information at the receiver side) to reliably decide whether a protected content has been used. A significant issue, regarding robust signal hashing, is that, given the hash values, it should be relatively difficult to obtain the original protected content. This is a valid concern from a privacy viewpoint, because the "content-trackers" (that utilize hash values) are usually thought to be third parties different from the content owners. We refer the interested reader to [33, 37, 38] for some practical robust signal hash algorithms proposed in the literature and [39] for a detection theoretic treatment of the problem. Therefore, codebook mismatch approach to robust signal hashing problem constitutes the fundamental limits for a given specific signal hashing algorithm, which is characterized by the conditional probability distribution employed to yield decoder's codebook, where the hash values are the decoder's codewords in the problem's setup. Hence, the aforementioned observation makes the problem at hand the pioneering work which aims to develop an information theoretic approach to the problem of robust signal hashing, which is a hot topic in signal processing society. Observe that instead of carrying out the maximization over the conditional distribution for a particular distribution on the encoder's codewords, we are also able to find the *asymptotically optimum* (in the sense of achieving the maximum error free transmission rate) robust signal hashing scheme; for which codebook mismatch problem constitutes its backbone. Obviously, robust signal hashing problem is not the only practical scheme codebook mismatch may be helpful, because of the *anti-symmetric* nature of it, which makes the codebook mismatch suitable for the situations where privacy is a concern, in other words within the class of communication problems where communicating parties

can not share a common codebook due to the nature of the problem, such as "public key watermarking" [40, 41, 42, 43] which is another hot topic both in signal processing and information theory society. The last possible practical scenario, for which the mismatched codebooks may be helpful is the situations, where the memory of the decoder is limited compared to encoder. For this situation, the mismatch between the codebooks, (which is very counter-intuitive from the 'orthodox-communication engineer" point of view) may be desirable, since this mismatch can be thought as a lossy-source coding. Again, by considering the codewords of the encoder's codebook as the realizations of the random variables to be compressed; and the corresponding codewords of the decoder's codebook as the reconstruction values of these random variables, we can define a new concept of "capacity-rate function" (an analogue to the rate-distortion counterpart of the Shannon theory), which constitutes the short term research topic of us which we aim to precisely state the problem and prove the results in a near future.

Next, we state the main results of the thesis below:

**Main Results:** Our main results for the problems (which are stated at the beginning of this section) considered in the thesis are summarized as follows:

(i) For the problem of characterizing optimal attacks against ABSG, (the former of the aforementioned problems) our contributions, which have been derived under a set of mild assumptions (specified in Sec. 2.2.1), are as follows:

- We show that breaking ABSG algorithm is equivalent to "guessing" a sequence of random variables, which are i.i.d. (independent identically distributed) with geometric distribution of parameter 1/2 using complexity theoretic notions (Theorem 2.2.1).
- In order to solve the problem mentioned in the previous item, we formulate a sufficiently broad class of attacks, termed as "Query-Based Key-Recovery attacks", which are quite generic by construction, and hence applicable for cryptanalysis for a wide range of cryptosystems (Definition 2.2.3).
- Within the class of attacks mentioned in the previous item, we concentrate on a practically-meaningful subset of them (termed "Exhaustive-Search

Type Query-Based Key-Recovery attacks") (Sec. 2.3); we derive a fundamental lower bound on the complexity of any successful attack in this subset (Theorem 2.3.2); this lower bound is proven to be achievable to the first order in the exponent (Theorem 2.3.1).

(ii) For the problem of reliable communication under codebook mismatch (a new posed problem, which is an important property itself, since such a new problem definition in Shannon theory is very rare), the second aforementioned problem, we deal with a special case, named as *discrete memoryless i.i.d. codebook mismatched channel* and derived following results:

- We find the maximum error free rate that can be asymptotically achieved for the communication system at hand. In other words, we find the operational capacity of the "codebook-mismatch problem" and state it as Theorem 3.2.1.
- We evaluate the information capacity (which turns out to be the operational capacity due to Theorem 3.2.1) of a specific discrete memoryless i.i.d. codebook mismatched channel, where both communication and mismatch channels are binary symmetric channels (BSC) by employing a new (to the best of our knowledge) concept of "circular Markovianity" (cf. Section 3.2.3) which is both elegant from a pure mathematical point of view and promising to be valuable in different problems of information theory, such as network information theory.

## 1.5. Organization of the Thesis

Chapter 2 devoted to the first problem considered in the thesis. In Section 2.1, we provide the relevant background material about ABSG algorithm under the consideration. Section 2.2 provides the assumptions we have employed throughout the chapter, the problem formulation and the definition of "Query-Based Key-Recovery" (QuBaR) attacks. In Section 2.3, we derive the tight (to the first order in the exponent) lower bound on the complexity of exhaustive-search type QuBaR attacks. Chapter 3 is about codebook mismatch problem. In Section 3.1 we rigorously state the problem considered in the chapter. In Section 3.2, we state the main result of the chapter of which forward statement's proof is given in Section 3.2.1 and converse statement's proof is given in

Section 3.2.2. Section 3.2.3, which illustrates the concept of codebook mismatch on a specific example concludes both the section and the chapter. Thesis ends with the concluding remarks stated in Chapter 4.

# 2. INFORMATION THEORETIC CRYPTANALYSIS

## 2.1. Background

Throughout this section, we use the notation that was introduced in [27] for the ABSG related concepts.

**Definition 2.1.1** *Given an infinite length binary sequence* $\mathbf{x} = \{x_n\}_{n=1}^{\infty}$ *which is an input to the ABSG algorithm, we define*

- $\mathbf{y} \triangleq \mathcal{A}(\mathbf{x})$*, where the sequence* $\mathbf{y}$ *represents the internal state of the ABSG algorithm and* $y_i \in \{\varnothing, 0, 1\}$*,* $1 \leq i < \infty$*. The action of algorithm* $\mathcal{A}$ *is defined via the recursive mapping* $\mathcal{M}$*:*

$$y_i = \mathcal{M}(y_{i-1}, x_i), \quad 1 \leq i < \infty, \tag{2.1}$$

*with the initial condition* $y_0 = \varnothing$*. The mapping* $\mathcal{M}$ *is defined in Table 2.1 .*

Table 2.1. Transition Table of algorithm $\mathcal{A}$

| $y_{i-1} \backslash x_i$ | 0 | 1 |
|---|---|---|
| $\varnothing$ | 0 | 1 |
| 0 | $\varnothing$ | 0 |
| 1 | 1 | $\varnothing$ |

- $\mathbf{z} \triangleq \mathcal{B}(\mathbf{y})$*, where the sequence* $\mathbf{z}$ *represents the output of the ABSG algorithm, such that the action of the algorithm* $\mathcal{B}$ *is given as follows:*

$$z_j = \begin{cases} y_{i-1}, & \text{if } y_i = \varnothing \text{ and } y_{i-2} = \varnothing, \\ \bar{y}_{i-1}, & \text{if } y_i = \varnothing \text{ and } y_{i-2} \neq \varnothing, \end{cases} \tag{2.2}$$

*where* $j \leq i$ *and* $i, j \in \mathbb{Z}^+$*.*

From Definition 2.1.1, we clearly deduce that the ABSG algorithm produces an output bit ($z_j$ denoting the $j$-th output bit) if and only if the value of the corresponding internal state variable ($y_i$ denoting the value of the internal state variable at time $i$) is $\varnothing$. The fact that $y_i \neq \varnothing$ for all $i$ is the reason of the mismatch between the input sequence indices (which are the same as the indices of the internal state variables) and the output sequence indices.

## 2.2. Problem Setup and Formulation

### 2.2.1. Assumptions and Preliminaries

Throughout this chapter, we consider the type of attacks, in which retrieving $L$ (where $L$ is the degree of the feedback polynomial of the generating LFSR) linear equations in terms of $\mathbf{x}_1^M$ is aimed. This type of attacks correspond to *key recovery attacks* to ABSG (assuming that the feedback polynomial of LFSR is known to the attacker, which is a common assumption in cryptanalysis). In particular, within the class of key recovery attacks, we concentrate on *query-based key recovery attacks* (abbreviated as ***"QuBaR attacks"*** in the rest of the chapter); QuBaR attacks shall be defined formally in Sec. 2.2.2. The following assumptions are made in this attack model:

**A1:** The length-$M$ input sequence $\mathbf{x}_1^M$ is assumed to be a realization of an i.i.d. Bernoulli process with parameter $1/2$.

**A2:** The length-$N$ output sequence $\mathbf{z}_1^N$ is assumed to be given to the attacker, where $N, M \in \mathbb{Z}^+$ (note that, this implies we necessarily have $M > N \geq 1$ due to Definiton 2.1.1).

**A3:** Explicit knowledge of the feedback polynomial of the generating LFSR is not used.

**A4:** The degree of the feedback polynomial of the generating LFSR, i.e., $L$, is sufficiently large.

Note that assumption A3 will be further clarified after we describe QuBaR attack model precisely. Further, from now on we denote the input sequence as $\mathbf{X}_1^M$ and the

corresponding internal state sequence as $\mathbf{Y}_1^M$ due to the stochastic nature of the input and hence the internal state sequences. Next, we continue with the following definitions.

**Definition 2.2.1** *The symbol $H_i$ denotes the index of the $i$-th $\varnothing$ in $\mathbf{Y}_1^M$, for $0 \leq i \leq N$.*

Note that, since we have $Y_0 = \varnothing$ with probability 1 by convention, we also use $H_0 = 0$ with probability 1 as the initial condition for $\{H_i\}$.

**Definition 2.2.2** *We define $Q_i \stackrel{\triangle}{=} H_i - H_{i-1} - 2$, for $1 \leq i \leq N$.*

**Remark 2.2.1** *For each $Q_i$ (regardless of its particular realization), the ABSG algorithm generates an output bit $z_i$. Thus, the number of output bits in the ABSG algorithm is precisely equal to the number of corresponding $\{Q_i\}$.*

Next, we state the following result regarding the distribution of $\{Q_i\}$, which will be heavily used throughout the rest of the chapter.

**Lemma 2.2.1** *Under assumptions A1 and A2, the random variables $\{Q_i\}$ are i.i.d. with geometric p.m.f. of parameter $1/2$:*

$$p\left(q_i\right) \stackrel{\triangle}{=} \Pr\left[Q_i = q_i | \mathbf{z}_1^N\right] = (1/2)^{q_i+1}, \text{ for } q_i \in \mathbb{N},\ 1 \leq i \leq N. \tag{2.3}$$

**Proof:** See Appendix A.

### 2.2.2. Problem Formulation

In this section, we provide an analytical formulation of the problem considered in this chapter. As the first step, we show that, under assumptions A1, A2, A3, and A4, all key recovery attacks to ABSG are equivalent to recovering the exact realizations of $\mathbf{Q}_1^N$, stated in Theorem 2.2.1[8] :

**Theorem 2.2.1** *Under the assumptions A1, A2, A3 and A4, the following three computational problems are equivalent in the sense of probabilistic polynomial time reducibility [44]:*

1. *Retrieving any $L$ independent linear equations in terms of $\mathbf{X}_1^M$.*
2. *Retrieving any $L$ consecutive bits from $\mathbf{X}_1^M$.*
3. *Correctly guessing $\mathbf{Q}_i^{\theta+i-1}$ for any positive integers $i$ and $\theta$ such that*

$$\sum_{j=i}^{\theta+i-1} (q_j + 2) \geq L, \tag{2.4}$$

*is satisfied.*

**Proof:** See Appendix B.

Next, we introduce the model for the query type attacks, namely *QuBaR attacks*, which are considered throughout the chapter. Qualitatively, a QuBaR attack consists of repeating the following procedure: For a cryptosystem that has a secret, generate a "guess", which aims to guess the secret itself, and subsequently "checks" whether the guess is equal to the secret or not; if the guess is equal to the secret, then terminate the procedure, else continue with another guess. The maximum number of guesses proposed in this procedure are limited by the complexity of the QuBaR attack, which is provided as an input parameter to the attack algorithm. Note that, if the task at hand is to guess i.i.d. random variables (which is the case for the third problem of Theorem 2.2.1), the

[8]For the random variable $Q_i$, its realization is denoted by $q_i$.

QuBaR attack model is intuitively obviously reasonable. Furthermore, recall that most of the cryptanalysis against symmetric key cryptography may be modeled in this way (e.g., time-memory attacks, correlation attacks, algebraic attacks and alike). Next, we formally present the general form of QuBaR attack algorithms.

**Definition 2.2.3** *Assuming the existence of a "check algorithm" $\mathcal{T}(G)$ for a "guess" $G$ (the output of $\mathcal{T}(G)$ is 1 if and only if the guess $G$ is equal to the secret), a QuBaR attack algorithm, of complexity $\mathcal{C}$, executes the following steps:*

Table 2.2. QuBaR Attack Algorithm

| |
|---|
| For $k = 1$ to $\mathcal{C}$ |
| **1.** Generate a guess $G_k$. |
| **2.** Compute $\mathcal{T}(G_k)$. |
| **3.** If $\mathcal{T}(G_k) = 1$, then terminate and output the secret given by $G_k$. |
| end |

Next, we introduce the particular "guess" structure (together with the accompanying relevant definitions) which aims to find $\mathbf{Q}_i^{\theta+i-1}$ so as to solve the third computational problem of Theorem 2.2.1.

**Definition 2.2.4** *An* ABSG-guess *is a triplet defined as $G \triangleq \{i, \theta, \mathbf{q}_i^{\theta+i-1}\}$, such that $2\theta + \beta \geq L$, where $\beta \triangleq \sum_{j=0}^{\theta-1} q_{i+j}$, $i \geq 1$ and $i + \theta - 1 \leq N$.*

The Bernoulli random variable, $\mathcal{T}(G_k)$, indicates the success probability of guess $G_k$ and is heavily used throughout the rest of the chapter, where $G_k \triangleq \left(i_k, \theta_k, \mathbf{q}_{i_k}^{\theta_k+i_k-1}\right)$

is the ABSG-guess of a QuBaR attack (against ABSG) at step $k$. Note that, at each step $k$, the "guessed" values $\mathbf{q}_{i_k}^{\theta_k+i_k-1}$ themselves depend on $k$, which is not explicitly stated (unless otherwise specified) for the sake of notational convenience; this should be self-understood from the context.

**Remark 2.2.2** *Note that, the probability of having a successful QuBaR attack* after precisely $K$ steps *is equal to* $\Pr\left[\mathcal{T}\left(G_1\right)=0,\ \ \mathcal{T}\left(G_2\right)=0,\ldots\mathcal{T}\left(G_{K-1}\right)=0,\mathcal{T}\left(G_K\right)=1\right]$ *which is* not *equal to* $\Pr\left(\mathcal{T}\left(G_K\right)=1\right)$ *(the latter being equal to the marginal successful guess probability at step $K$). Moreover, neither of these expressions is the success probability of any QuBaR attack with a specified complexity, which will formally be defined in (2.7). Observe that our formulation allows the usage of* potentially correlated guesses $\{G_k\}$ *which aims to make the approach as generic as possible.*

**Corollary 2.2.1** *Per Lemma 2.2.1 and Definition 2.2.4, we have*

$$\Pr\left[\mathcal{T}\left(G_k\right)=1\right]=\Pr\left[\mathbf{Q}_{i_k}^{i_k+\theta_k-1}=\mathbf{q}_{i_k}^{i_k+\theta_k-1}\,|\,\mathbf{z}_1^N\right]=\prod_{j=i_k}^{i_k+\theta_k-1}\left(\frac{1}{2}\right)^{q_j+1}=\left(\frac{1}{2}\right)^{\beta_k+\theta_k},\tag{2.5}$$

*where* $\beta_k\stackrel{\triangle}{=}\sum_{j=0}^{\theta_k-1}q_{i_k+j}$.

The following corollary, which is a direct consequence of Theorem 2.2.1, is one of the key results of the chapter.

**Corollary 2.2.2** *All QuBaR-type attacks against ABSG are probabilistic polynomial time reducible to the QuBaR algorithm (defined in Definition 2.2.3) which uses ABSG-guesses defined in Definition 2.2.4 and aims to find* $\mathbf{Q}_i^{\theta+i-1}$ *satisfying (2.4) for any* $i,\theta\in\mathbb{Z}^+$.

**Definition 2.2.5** *From now on, we call an arbitrary "ABSG-Guess", $G$, simply as*

*"guess". Further, for the sake of notational convenience, we use*

$$\mathfrak{A} = \{G_k\}_{k=1}^{\mathcal{C}(\mathfrak{A})} \tag{2.6}$$

*for any attack algorithm $\mathfrak{A}$ mentioned in Corollary 2.2.2, where $\mathcal{C}(\mathfrak{A})$ denotes the (algorithmic) complexity of $\mathfrak{A}$ (i.e., number of guesses applied within $\mathfrak{A}$). Accordingly, the success probability of any $\mathfrak{A}$ is given by*

$$Pr_{succ}(\mathfrak{A}) \stackrel{\triangle}{=} \Pr\left[\vee_{k=1}^{\mathcal{C}(\mathfrak{A})}\mathcal{T}(G_k) = 1\right] = 1 - \Pr\left[\wedge_{k=1}^{\mathcal{C}(\mathfrak{A})}\mathcal{T}(G_k) = 0\right]. \tag{2.7}$$

Hence, as far as QuBaR attacks against ABSG are concerned, w.l.o.g., in this chapter we focus on the ones specified in Corollary 2.2.2, which aim to solve the third computational problem of Theorem 2.2.1. In particular, in the rest of the chapter, we explore the fundamental limits of the aforementioned QuBaR attacks (denoted by $\mathfrak{A}$) under various setups of interest.

**Remark 2.2.3**

*(i)* *Measure of QuBaR Complexity in Terms of L: At the first glance, it may look reasonable to evaluate the complexity of a QuBaR attack in terms of the length of its input, which is $N$ since the input is $\mathbf{z}_1^N$. Note that, this is a common practice in complexity theory. However, when we confine the setup as the application of a QuBaR attack to the ABSG algorithm (prior to which there exists a LFSR whose length-$L$ initial state is unknown), then it would be more reasonable to evaluate the complexity of a QuBaR attack in terms of $L$ for this case (since we eventually aim to find $L$ consecutive bits of $\mathbf{X}_1^M$; see Theorem 2.2.1). This is precisely the approach we pursue in this chapter, i.e., the analysis of the resulting QuBaR attack complexity is given as a function of $L$.*

*(ii)* *Time Complexity Lower Bound for QuBaR: As far as the complexity analysis of QuBaR attacks against ABSG are concerned, in our developments we treat $\mathcal{C}(\mathfrak{A})$*

*as the time complexity (of an algorithm $\mathfrak{A}$) and carry out the analysis accordingly. In other words, the complexities of guess and check algorithms are not explicitly taken into account in the analysis. The reason is that the quantity $\mathcal{C}(\mathfrak{A})$ constitutes the fundamental complexity of any QuBaR attack against ABSG, since in practice complexities of both guess and check algorithms may be considered as poly$(L)$ complexity (cf. item (v) in this remark). Next, observe that $\mathcal{C}(\mathfrak{A})$ is indeed a lower bound on the time complexity of any QuBaR attack*[9] *. In particular, in the following sections, using information theoretic arguments we derive lower bounds on $\mathcal{C}(\mathfrak{A})$ (for different setups of interest) and subsequently prove that these bounds are achievable to the first order in the exponent. This amounts to showing that these bounds are tight and indeed optimal, i.e., exponentially tight minima in the sense of time complexity.*

*(iii)* *Data Complexity Upper Bound for QuBaR: As far as the data complexity in the QuBaR attack analysis is concerned, consider the following arguments: Using Definition 2.2.4 and denoting the relevant parameters of the $k$-th ABSG-guess $G_k = \left(i_k, \theta_k, \mathbf{q}_{i_k}^{\theta_k+i_k-1}\right)$ by $\left(\theta_k, \beta_k = \sum_{j=0}^{\theta_k-1} q_{i_k+j}\right)$, we observe that at each iteration step $k$, a "meaningful" ABSG-guess operates in the range of $2\theta_k + \beta_k = poly(L)$ (due to the "valid guess" constraint of $2\theta_k + \beta_k \geq L$ for each guess $G_k$); otherwise, e.g., given a QuBaR attack for which $2\theta_k + \beta_k = exp(L)$, a "better" attack can obviously be found with high probability (via omitting some $\{Q_j\}$ in the guess-based search)*[10] *. Since, for each $k$, the value of $\theta_k$ is equal to the number of "guessed" output bits (per Remark 2.2.1), we see that the number of "guessed" output bits is poly$(L)$. Thus, the overall data complexity of a successful QuBaR attack algorithm $\mathfrak{A}$ against ABSG is at most $\mathcal{C}(\mathfrak{A}) \cdot poly(L)$. As we mentioned in item (ii) above, we will show that at optimality $\mathcal{C}(\mathfrak{A})$ is $exp(L)$. Hence, poly$(L)$ vanishes to the first order in the exponent, which implies that $\mathcal{C}(\mathfrak{A})$ is also a tight (to the first order in the exponent) upper bound on data complexity at optimality.*

*(iv)* *Algorithmic Complexity Lower Bound for QuBaR: In parts (ii) and (iii) above,*

[9] Note that this bound is tight to the first order in the exponent for the case when $\mathcal{C}(\mathfrak{A})$ is $exp(L)$ (which is the case at optimality) and both guess and check algorithms are $poly(L)$ (which is the case in practice), which justifies taking $\mathcal{C}(\mathfrak{A})$ as the time complexity.

[10] We will soon show that at optimality, the data complexity of an individual guess within the QuBaR attack algorithm is $\mathcal{O}(L)$ which justifies this argument.

*we stress that for an optimal QuBaR attack algorithm* $\mathfrak{A}$ *against ABSG,* $\mathcal{C}(\mathfrak{A})$ *forms a lower (resp. upper) bound on the time (resp. data) complexity of* $\mathfrak{A}$*. Following the general convention in cryptanalysis, we use the term "algorithmic complexity" as the maximum of time complexity and data complexity. At optimality, we have following cases:* ***a)*** *Time complexity is greater than data complexity, which implies that* $\mathcal{C}(\mathfrak{A})$ *is a lower bound on algorithmic complexity.* ***b)*** *Time complexity is equal to data complexity,* $\mathcal{C}(\mathfrak{A})$ *is the algorithmic complexity.* ***c)*** *Data complexity is greater than time complexity, which constitutes the contradiction of* $\mathcal{C}(\mathfrak{A}) > \mathcal{C}(\mathfrak{A})$*, hence impossible.*

*Therefore, we conclude that at optimality,* $\mathcal{C}(\mathfrak{A})$ *forms a lower bound on the algorithmic complexity. Thus, throughout the rest of the chapter, we focus on* $\mathcal{C}(\mathfrak{A})$ *and develop arguments on its value at asymptotic optimality for large* $L$*. Further, we will show that at optimality the value of* $\mathcal{C}(\mathfrak{A})$ *is achieved to the first order in the exponent.*

*(v)* *Practical Implementation Approaches to QuBaR Algorithms: As far as practical attacks are concerned, existence of a polynomial-time guess generation algorithm is obvious. Furthermore, a polynomial-time check algorithm, which corresponds to the procedure of initiating a LFSR (whose feedback polynomial is assumed to be known) with the corresponding "guessed and retrieved"* $L$ *consecutive bits of* $\mathbf{X}_1^M$*, generating sufficiently many output bits and comparing them with the original output bits, constitutes a practical approach.*

*(vi)* *Relationship Of QuBaR Attacks With State-Of-The-Art Attack Algorithms: We see that QuBaR attacks are analogous to "first type of attacks" described in [26], which "aim to exploit possible weaknesses of compression component introduced by ABSG". However, note that, QuBaR attacks* do not *use explicit knowledge of the feedback polynomial of the generating LFSR, (recall the structure of algorithm* $\mathcal{T}$*) which is a direct consequence of the assumption A3.*

## 2.3. Optimum Exhaustive-Search Type QuBaR Attacks Against ABSG

In this section, we deal with "exhaustive-search" type QuBaR attacks which are formally defined in Definition 2.3.1. Qualitatively, given the output sequence $\mathbf{z}_1^N$, an exhaustive-search type QuBaR attack aims to correctly identify $\theta$-many $\{Q_i\}$ (equivalently at least $L$ consecutive bits of $\mathbf{X}_1^M$ per Theorem 2.2.1) beginning from *an arbitrarily-chosen, fixed index*, subject to constraint (2.4) [11] . Since the attacker is confined to initiate the guesses beginning from a fixed index for exhaustive-search attacks, in practice this can be thought to be equivalent to a scenario where the attacker uses only a *single portion* of the observed output sequence $\mathbf{z}_1^N$.

First theorem of this section, namely Theorem 2.3.1, proves the existence of an exhaustive-search type QuBaR attack with success probability of $1-\epsilon$ (for any $\epsilon > 0$) with algorithmic complexity $2^{2L/3}$ (in particular, with time complexity $2^{2L/3}$ and data complexity $L/3$) under the assumptions mentioned in Section 2.2.1. The second theorem of this section, namely Theorem 2.3.2, proves that the algorithmic complexity of the best (in the sense of $\mathcal{C}$) exhaustive-search type QuBaR algorithm under the assumptions A1, A2, A3, A4 is lower-bounded by $2^{2L/3}$ (to the first order in the exponent). Hence, as a result of these two theorems, we show that the overall algorithmic complexity of the best exhaustive-search attack against ABSG has complexity $2^{2L/3}$ to the first order in the exponent (argued in Corollary 2.3.1). Note that, in [26] Gouget et. al. mention the existence of an exhaustive-search attack (under i.i.d. Bernoulli 1/2 input assumption) of complexity $\mathcal{O}\left(2^{2L/3}\right)$ without providing the details of the attack. Our main novelty in this section is that, we provide a rigorous proof about the existence of such an attack (Theorem 2.3.1, which is analogous to the "achievability"-type proofs in traditional lossless source coding) and further show that this is the best (to the first order in the exponent) in the sense of algorithmic complexity under some certain assumptions, specifically within the class of exhaustive-search QuBaR attacks (Theorem 2.3.2, which is analogous to the "converse"-type proofs in traditional lossless source coding). As a result, the developments in this section can be considered to be analogous

[11] In contrast with exhaustive-search attacks, a generalized version, where we focus on identifying $\theta$-many $\{Q_i\}$, possibly beginning from arbitrarily-chosen, multiple indices, which constitutes the topic of Section V of [28], which is not included in the thesis, since it does not use the concept of typicality.

to those of source coding by Shannon [1]; see Remark 2.3.3 for a further discussion on this subject. Theorem 2.3.3 concludes the section, which characterizes some necessary conditions of the optimal exhaustive-search type QuBaR attacks against ABSG.

We begin our developments with the formal definition of exhaustive-search type QuBaR attacks.

**Definition 2.3.1** *The class of exhaustive-search type QuBaR attacks against ABSG are defined as*

$$\mathcal{S}^E \triangleq \{\mathfrak{A}^E = \{G_k\}_{k=1}^{\mathcal{C}(\mathfrak{A}^E)} : \forall k, i_k = 1\}, \tag{2.8}$$

*where each k-th guess* $G_k = \left(i_k, \theta_k, \mathbf{q}_{i_k}^{\theta_k+i_k-1}\right)$ *is subject to (2.4) (see Definition 2.2.4).*

**Remark 2.3.1** *Exhaustive-search type attacks constitute an important class of attacks in cryptanalysis. They essentially determine the "effective size" of the key space of any cipher. In case of ABSG, as we mentioned at the beginning of this section, since the exhaustive-search type QuBaR attack uses a single portion of the output sequence, they form a basic choice for practical cryptanalysis via QuBaR attacks in situations where a limited amount (poly* $(L)$*) of output data are available to the attacker.*

Thus, at each $k$-th step, via guess $G_k$ an exhaustive-search type QuBaR attack aims to correctly identify $\theta_k$-many $\{Q_i\}$ subject to (2.4) beginning from a fixed index $i_k$, equivalently at least $L$ consecutive bits of $\mathbf{X}_1^M$ beginning from the index $i'_k$ (in general $i'_k \neq i_k$ due to the "decimation" nature of ABSG). As we specified in Definition 2.3.1, in our developments w.l.o.g. we use $i_k = 1$ (which in turn implies having $i'_k = 1$ as well).

**Theorem 2.3.1** (Achievability - Exhaustive-Search) *Under the assumptions A1, A2, A3, A4, mentioned in Section 2.2.1, there exists an exhaustive-search type QuBaR at-*

*tack algorithm* $\mathfrak{A}^E_{ach,opt}$ *against ABSG with* $\mathcal{C}\left(\mathfrak{A}^E_{ach,opt}\right) = 2^{2L/3}$ *such that* $\Pr_{succ}\left(\mathfrak{A}^E_{ach,opt}\right) > 1-\epsilon$, *for any* $\epsilon > 0$. *Further,* $\mathcal{C}_{ave}\left(\mathfrak{A}^E_{ach,opt}\right) = \frac{1}{2}\left(2^{2L/3}+1\right)$ *where* $\mathcal{C}_{ave}\left(\mathfrak{A}^E_{ach,opt}\right)$ *is the* expected complexity *of* $\mathfrak{A}^E_{ach,opt}$ *over the probability distribution induced by* $\mathbf{q}$.

**Proof:** See Appendix C.

**Remark 2.3.2** *An inspection of the proof of Theorem 2.3.1 reveals that (as promised in Remark 2.2.3) the overall data complexity of the proposed attack algorithm* $\mathfrak{A}^E_{ach,opt}$ *is* $L/3$ *which certainly implies that each guess is of data complexity* $\mathcal{O}(L)$. *Furthermore, the overall time complexity of* $\mathfrak{A}^E_{ach,opt}$ *is* $\mathcal{O}\left(2^{2L/3}\right)$ *assuming that the contribution of the generation of each guess is poly* $(L)$ *(which is reasonable in practice). Note that, the time and data complexity of the proposed attack* $\mathfrak{A}^E_{ach,opt}$ *used in the proof of Theorem 2.3.1 coincides with the one mentioned in [26].*

Next, we prove the converse counterpart of Theorem 2.3.1, namely derive a lower bound on the algorithmic complexity of any exhaustive-search type QuBaR attack with an inequality constraint on the success probability.

**Theorem 2.3.2** (Converse - Exhaustive-Search) *Under the assumptions A1, A2, A3, A4, and for any* $\mathfrak{A}^E \in \mathcal{S}^E$ *with* $\Pr_{succ}\left(\mathfrak{A}^E\right) > \frac{1}{2}$, *we necessarily have* $\mathcal{C}\left(\mathfrak{A}^E\right) > \underline{\mathcal{C}}^E_{min} \triangleq 2^{2L/3}\left(\frac{1}{2} - \frac{6}{L}\right)$.

**Proof:** See Appendix D.

**Corollary 2.3.1** *After some straightforward algebra, it can be shown that*

$$\mathcal{C}\left(\mathfrak{A}^E_{ach,opt}\right) \doteq \mathcal{C}_{ave}\left(\mathfrak{A}^E_{ach,opt}\right) \doteq \underline{\mathcal{C}}^E_{min} \tag{2.9}$$

*in* $L$. *Thus, Theorems 2.3.1 and 2.3.2 show that, under the assumptions mentioned in Section 2.2.1, the* tight *lower bound (to the first order in the exponent) on the*

*algorithmic complexity of any exhaustive-search type QuBaR attack against ABSG is* $2^{2L/3}$.

Following remark provides the promised discussion at the beginning of the section, which interprets the relationship between the result proved in this section (namely, Theorems 2.3.1 and 2.3.2) and the traditional lossless source coding of information theory.

**Remark 2.3.3** *Observe that for the exhaustive-search setup, the problem is "somewhat dual" of the lossless source coding problem. Intuitively, the concept of cryptographic compression (which is also termed as "decimation" in this chapter) aims to produce a sequence of random variables, such that the sequence is as long as possible with the highest entropy possible so as to render cryptographic attacks useless as much as possible (which amounts to making the decimation operation "non-invertible" in practice). On the other hand, in lossless source coding, the goal is to produce an output sequence which is as short as possible while maintaining "exact invertibility" (which amounts to "lossless" decoding). Hence, it is not surprising that, from the cryptanalyst's point of view, usage of concepts from lossless source coding may be valuable. To be more precise, the cryptanalyst aims to identify a set of* highly-probable *sequences (each of which is a collection of i.i.d. random variables from a known distribution), of which cardinality is as small as possible, thereby maximizing the chances of a successful guess with the least number of trials. As a result, the usage of the concept of* typicality *fits naturally within this framework. In particular, typicality is the essence of the proof of the converse theorem (Theorem 2.3.2), which states a fundamental lower bound on the complexity of all possible exhaustive-search type QuBaR attacks.* The outcome of "converse" states a negative result (which is unknown for the case of stream ciphers to the best of our knowledge) within a reasonable attack class in cryptanalysis by construction. *This observation contributes to a significant portion of our long-term goal, which includes construction of a unified approach to cryptanalysis of stream ciphers. In particular, our future research includes focusing on specific cryptosystems and quantifying fundamental bounds on the performance of attacks (within a pre-specified reasonable class) against*

*these systems.*

Following theorem characterizes some important necessary conditions for an optimal exhaustive-search type QuBaR attack against ABSG, subject to an equality constraint on the success probability. Thus, these results are important in practice since they provide some guidelines in construction of optimal or near-optimal exhaustive-search type QuBaR attacks.

**Theorem 2.3.3** *Given an optimal (in the sense of minimizing* $\mathcal{C}\left(\mathfrak{A}_{opt}^{E}\right)$ *subject to an equality constraint on the success probability) exhaustive-search type QuBaR attack (denoted by* $\mathfrak{A}_{opt}^{E}$*) against ABSG, we have the following necessary conditions:*

*(i) The corresponding guesses are* prefix-free.

*(ii) The corresponding "success events"* $\left\{\mathcal{T}\left(G_i\right)=1\right\}_{i=1}^{\mathcal{C}\left(\mathfrak{A}_{opt}^{E}\right)}$ *are* disjoint.

*(iii) We have*

$$Pr_{succ}\left(\mathfrak{A}_{opt}^{E}\right)=\Pr\left(\vee_{k=1}^{\mathcal{C}\left(\mathfrak{A}_{opt}^{E}\right)}\left[\mathcal{T}\left(G_k\right)=1\right]\right)=\sum_{k=1}^{\mathcal{C}\left(\mathfrak{A}_{opt}^{E}\right)}\Pr\left(\mathcal{T}\left(G_k\right)=1\right). \tag{2.10}$$

*(iv) The corresponding "success events"* $\left\{\mathcal{T}\left(G_i\right)=1\right\}_{i=1}^{\mathcal{C}\left(\mathfrak{A}_{opt}^{E}\right)}$ *satisfy*

$$(i>j)\quad\Longrightarrow\quad\left[\Pr\left(\mathcal{T}\left(G_i\right)=1\right)\leq\Pr\left(\mathcal{T}\left(G_j\right)=1\right)\right], \tag{2.11}$$

*for any* $i\neq j$*, such that,* $i,j\in\left\{1,\ldots,\mathcal{C}\left(\mathfrak{A}_{opt}^{E}\right)\right\}$.

**Proof:** See Appendix E.

# 3. RELIABLE COMMUNICATION UNDER CODEBOOK MISMATCH

In this chapter, our major concern is determining the maximum (asymptotically) error-free rate for a communication system, for which the encoder's and decoder's codebooks are not the same one.

To be more precise, prior to the beginning of the communication between two communicating parties, encoder generates its codebook. Then, at the "codebook revealing phase" of the classical Shannon theory, decoder receives *only* a "perturbed", yet correlated version of the encoder's original codebook[12] , of which codewords will be input to the "communication channel" at the communication phase, and the statistical dependence between the two codebooks is assumed to be known at both encoder and decoder side in addition to the statistical characterization of the encoder's codebook at the decoder side. After the encoding step of the communication phase, encoder transmits the corresponding codeword over the communication channel and at the decoding step, decoder uses its *perturbed* codebook in order to perform detection in addition to the knowledge of the statistical characterization of the communication channel, statistical characterization of the perturbation of its codebook with the encoder's codebook and the statistical characterization of the encoder's codebook.

## 3.1. Problem Statement

After the qualitative explanation provided above, we state the precise definition of the communication system to be investigated. The aforementioned communication system consists of two parts: *discrete-memoryless codebook mismatched channel* (cf. Definition 3.1.1) and $\left(2^{nR}, n\right)$ *mismatched code* (cf. Definition 3.1.2).

**Definition 3.1.1** *A* discrete memoryless codebook mismatched channel*,*

[12] We concentrate on the special case of i.i.d. codewords case in Section 3.2.2 and derive the capacity result

*$(\mathcal{X}, p(y|x), \mathcal{Y}, p(u|x), \mathcal{U})$ consists of three finite sets $\mathcal{X}, \mathcal{Y}, \mathcal{U}$ and two independent collections of probability mass functions $p(y|x)$ and $p(u|x)$ defined over $\mathcal{Y} \times \mathcal{X}$ and $\mathcal{U} \times \mathcal{X}$, respectively. Note that $p(y|x)$ is the so-called communication channel (which is assumed to be known by both the encoder and the decoder), of which output is received by the decoder at the communication phase and $p(u|x)$ the so-called "mismatch channel" which models the stochastic dependence between the codewords of the encoder's and decoder's codebooks.*[13]

**Definition 3.1.2** *A* $\left(2^{nR}, n\right)$ mismatched code *for the channel* $(\mathcal{X}, p(y|x), \mathcal{Y}, p(u|x), \mathcal{U})$ *consists of the following:*

*(i) A message set,* $\mathcal{W} \triangleq \left\{1, \ldots, 2^{nR}\right\}$.

*(ii) An encoding function,* $f : \mathcal{W} \to \mathcal{X}^n$ *yielding the encoder's codewords* $\{\mathbf{x}^n(w)\}_{w=1}^{2^{nR}}$, *which constitutes the encoder's codebook,* $\mathcal{C} \in \mathcal{X}^{2^{nR} \times n}$, *which is defined as* $\mathcal{C} \triangleq [\mathbf{x}^n(w)]$.

*(iii) A decoding function,* $g : \mathcal{Y}^n \to \mathcal{W} \cup \{0\}$, *which is the rule that assigns a decision (including a null (*0*) decision, too) to every received sequence.*

*Note that, although it is not explicitly stated in the definition of the decoder function, decoder side* only *(in addition to the knowledge of the statistics of the communication and mismatch channels and the encoder's codebook) uses the so-called "decoder's codebook" (which is created prior to the communication phase, with the help of mismatch channel),* $\tilde{\mathcal{C}} \in \mathcal{U}^{2^{nR} \times n}$, *which is defined as* $\tilde{\mathcal{C}} \triangleq [\mathbf{u}^n(w)]$, *where* $u_i(w)$ *is the mismatch channel output corresponding to* $x_i(w)$, *for all* $i \in \{1, \ldots, n\}$, $w \in \left\{1, \ldots, 2^{nR}\right\}$.

**Remark 3.1.1**

*(i) First of all, note that there is a one-to-one correspondence between messages* $\mathcal{W}$ *and* $\{\mathbf{x}^n(w)\}_{w=1}^{2^{nR}}$ *at the encoder side, which is characterized by* $f(\cdot)$ *defined in*

[13] In fact, we use the term "channel" with a slight abuse of notation for this case, because there is no shared codebook between two sides for this "channel" (cf. item (iii)) of Remark 3.1.1), however our purpose is to stress the probabilistic nature of this structure and (except the "no-shared-codebook" point) its essentially same nature with the communication channel.

*item (ii) of Definition 3.1.2. Furthermore, a similar one-to-one correspondence between* $\mathcal{W}$ *and* $\{\mathbf{u}^n(W)\}_{w=1}^{2^{nR}}$ *exists at the decoder side.*

*(ii) We restate the following fact again: (because it will be crucial in proof of the converse theorem) The generation of the encoder's codebook,* $\mathcal{C}$*, and the construction of the decoder's codebook,* $\tilde{\mathcal{C}}$ *via mismatch channel* $p(u|x)$ *occurs* prior to sending the codeword $\mathbf{x}^n(w)$ corresponding to the message $w \in \mathcal{W}$.

*(iii) Note there is* not *a shared codebook between two parties for the mismatch channel, in other words decoder* only *observes output of this channel* without *knowledge of any additional information, except the statistical characterization of the channel.*

*(iv) Observe that, since communication and mismatch channels are independent, we conclude that* $U \leftrightarrow X \leftrightarrow Y$ *forms a Markov chain, i.e.*

$$p(u, x, y) = p(x)p(u|x)p(y|x). \tag{3.1}$$

The block diagram representation of the communication system described above (which we call discrete codebook mismatched channel) is given in Figure 3.1 below.

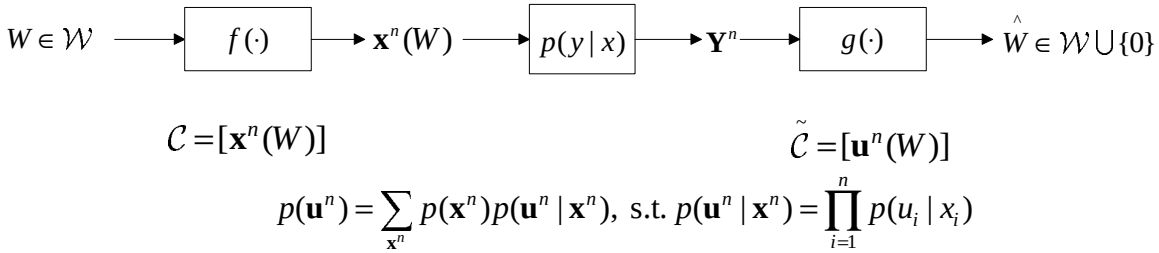


Figure 3.1. The Block Diagram Representation of the Discrete Codebook Mismatched Channel.

### 3.2. Discrete-Memoryless Codebook Mismatched Channel, I.I.D. Case

In this section, we deal with the communication system defined in Section 3.1 under the following assumption: the codewords of encoder's codebook, $\mathcal{C}$, are i.i.d. random variables with any arbitrary distribution $p(x)$. Under this assumption, we call the system as *the discrete memoryless i.i.d. codebook mismatched channel*. Our fundamental result is Theorem 3.2.1. Section 3.2.1 contains achievability result, while Section 3.2.2 is devoted to the converse of Theorem 3.2.1. Section 3.2 concludes with

the evaluation of the capacity of a special case, for which both communication and mismatch channels are binary symmetric channels, which is the topic of Section 3.2.3.

Before proceeding further, we define the information capacity of the discrete memoryless i.i.d. codebook mismatched channel, which will be shown to be the operational capacity of the system:

**Definition 3.2.1** *For any given $p(y|x)$ defined on $\mathcal{Y} \times \mathcal{X}$ and $p(u|x)$ defined on $\mathcal{U} \times \mathcal{X}$,* information capacity *of the discrete codebook mismatched channel, under the assumption of i.i.d. codewords is defined as*

$$C \stackrel{\triangle}{=} \max_{p(x)} I(U;Y), \tag{3.2}$$

*where $p(u,y) \stackrel{\triangle}{=} \sum_x p(x)p(y|x)p(u|x)$ (cf. (3.1)).*

The main result of this section is the following theorem:

**Theorem 3.2.1** *(Mismatched Channel Coding Theorem) For a discrete memoryless i.i.d. codebook mismatched channel, all rates below capacity $C$ are achievable. Specifically, for every rate $R < C$, there exists a sequence of $\left(2^{nR}, n\right)$ mismatched codes with maximum probability of error goes to 0 for sufficiently large $n$.*

*Conversely, any sequence of $\left(2^{nR}, n\right)$ mismatched codes with asymptotically vanishing maximum error probability should necessarily satisfy $R \leq C$.*

Before proceeding further, we state following lemmata which will be helpful in both achievability and converse theorems.

**Lemma 3.2.1** *Given* $p(x) = \prod_{i=1}^{n} p(x_i)$*, we have*

$$p\left(\mathbf{x}^n|\mathbf{u}^n\right) = \prod_{i=1}^{n} p(x_i|u_i), \tag{3.3}$$

*where* $p(x|u) \stackrel{\triangle}{=} \frac{p(x)p(u|x)}{\sum_x p(x)p(u|x)}$.

**Proof:** See Appendix F.

**Lemma 3.2.2** *Given* $p(x) = \prod_{i=1}^{n} p(x_i)$*, we have*

$$p\left(\mathbf{y}^n|\mathbf{u}^n\right) = \prod_{i=1}^{n} p(y_i|u_i), \tag{3.4}$$

*where* $p(y|u) \stackrel{\triangle}{=} \frac{\sum_x p(x)p(y|x)p(u|x)}{\sum_x p(x)p(u|x)}$.

**Proof:** See Appendix G.

**Lemma 3.2.3**

$$\Pr\left(\tilde{\mathcal{C}}\right) = \prod_{i=1}^{n} \prod_{w=1}^{2^{nR}} p(u_i(w)), \tag{3.5}$$

*where* $p(u) \stackrel{\triangle}{=} \sum_x p(x)p(u|x)$.

**Proof:** See Appendix H.

### 3.2.1. Achievability

The main result of this section is the following theorem.

**Theorem 3.2.2** *(Achievability) For every rate $R < C$, there exists a sequence of $(2^{nR}, n)$ mismatched codes with maximum probability of error goes to zero for sufficiently large $n$.*

**Proof:** We use standard random coding arguments.

**Encoding:**

(i) Generation of Codebooks: Fix $p(x)$ and reveal to both sides. Generate the encoder codebook $\mathcal{C} \stackrel{\triangle}{=} [x_i(w)]$, such that $x_i(w)$ are i.i.d. realizations of $X$ of which distribution is $p(x)$ for all $i \in \{1, \ldots, n\}$, $w \in \mathcal{W}$. Constitute the decoder's codebook, $\tilde{\mathcal{C}} \stackrel{\triangle}{=} [u_i(w)]$, via mismatch channel, such that as if each $x_i(w)$ is input to $p(u|x)$, and $u_i(w)$ is the output of the mismatch channel.

(ii) Choose a message uniformly from $\mathcal{W}$, i.e. $\Pr(W = w) = \frac{1}{2^{nR}}$ for all $w \in \mathcal{W}$. Suppose $w \in \mathcal{W}$ is the message chosen; then $\mathbf{x}^n(w)$ is transmitted over communication channel $p(y|x)$ resulting in $\mathbf{y}^n$, such that $p(\mathbf{y}^n) = \prod_{i=1}^{n} p(y_i|x_i(w))$ (recall the memoryless property of the communication channel).

**Decoding:**

(i) Decide the unique $\hat{W} \in \mathcal{W}$, such that $\left(\mathbf{u}^n(\hat{W}), \mathbf{y}^n\right) \in A_\epsilon^{(n)}(U, Y)$, where $A_\epsilon^{(n)}(U, Y)$ is the $\epsilon$-typical set defined on $p(u, y)$, which is defined in the statement of the theorem. Note that since $\mathbf{x}^n(w)$'s are i.i.d. $\{u_i(w), y_i\}_{i=1}^{n}$ pairs are independent from each other where $\mathbf{y}^n$ is the communication channel output corresponding to the message $w \in \mathcal{W}$.

If such a $\hat{W} \in \mathcal{W}$ is not unique or does not exist, then declare $g(\mathbf{y}^n) = 0$. Error event is defined in the following way:

$$\mathcal{E} \stackrel{\triangle}{=} \left\{\hat{W} \neq W\right\}. \tag{3.6}$$

**Analysis of Probability of Error:**

Now, we state following definitions, which will be used throughout the chapter.

We begin with the *conditional probability of error*, $\lambda_i$, is defined as:

$$\lambda_i \stackrel{\triangle}{=} \Pr\left(g\left(\mathbf{y}^n\right) \neq i | \mathbf{u}^n = \mathbf{u}^n(i)\right) = \sum_{\mathbf{y}^n} p\left(\mathbf{y}^n | \mathbf{u}^n(i)\right) 1_{(g(\mathbf{y}^n) \neq i)}, \tag{3.7}$$

where $1_{(\cdot)}$ is the standard indicator function.

Next, the *maximal probability of error*, $\lambda^{(n)}$, is defined as:

$$\lambda^{(n)} \stackrel{\triangle}{=} \max_{i \in \mathcal{W}} \lambda_i. \tag{3.8}$$

Last, the *average probability of error*, $P_e^{(n)}$, is defined as:

$$P_e^{(n)} \stackrel{\triangle}{=} \frac{1}{2^{nR}} \sum_{i=1}^{2^{nR}} \lambda_i, \tag{3.9}$$

Next, we define the $\epsilon$-typical set $A_\epsilon^{(n)}(U,Y)$ (from now on $A_\epsilon^{(n)}$ for the sake of simplicity) defined on i.i.d. (recall Lemma 3.2.1 and 3.2.2) $(\mathbf{u}^n, \mathbf{y}^n)$ with $p\left(\mathbf{u}^n, \mathbf{y}^n\right) = \prod_{i=1}^n p(u_i, y_i)$:

$$A_\epsilon^{(n)} \stackrel{\triangle}{=} \left\{ (\mathbf{u}^n, \mathbf{y}^n) \ : \ | -\frac{1}{n} \log p\left(\mathbf{u}^n\right) - H(U)| < \epsilon, | -\frac{1}{n} \log p\left(\mathbf{y}^n\right) - H(Y)| < \epsilon, \right.$$
$$\left. | -\frac{1}{n} \log p\left(\mathbf{u}^n, \mathbf{y}^n\right) - H(U,Y)| < \epsilon \right\} \tag{3.10}$$

Next, using the uniform distribution assumption on $W$, we have

$$P_e^{(n)} = \Pr\left(W \neq g\left(\mathbf{y}^n\right)\right). \tag{3.11}$$

Recalling (3.6) and using (3.11) we have following average probability of error averaged over all possible decoder codebooks[14] :

$$\begin{aligned} P_e^{(n)} &= \Pr\left(\mathcal{E}\right), && (3.12)\\ &= \sum_{\tilde{\mathcal{C}}} \Pr\left(\tilde{\mathcal{C}}\right) P_e^{(n)}\left(\tilde{\mathcal{C}}\right), && (3.13)\\ &= \frac{1}{2^{nR}} \sum_{w=1}^{2^{nR}} \sum_{\tilde{\mathcal{C}}} \Pr\left(\tilde{\mathcal{C}}\right) \lambda_w\left(\tilde{\mathcal{C}}\right), && (3.14)\\ &= \sum_{\tilde{\mathcal{C}}} \Pr\left(\tilde{\mathcal{C}}\right) \lambda_1\left(\tilde{\mathcal{C}}\right), && (3.15)\\ &= \Pr\left(\mathcal{E}|W=1\right), && (3.16) \end{aligned}$$

where (3.15) follows since decoder's codebook generation is symmetric, which is guaranteed by Lemma 3.2.3.

Next, we define following events:

$$\mathcal{E}_i \stackrel{\triangle}{=} \left\{(\mathbf{u}^n(i), \mathbf{y}^n) \in A_\epsilon^{(n)}\right\}, \tag{3.17}$$

for $i \in \left\{1, \ldots, 2^{nR}\right\}$, where $\mathbf{y}^n$ is the output of the communication channel when $W = 1$ is the case.

Using (3.16) and (3.17) we have:

$$\begin{aligned} \Pr\left(\mathcal{E}|W=1\right) &= \Pr\left(\mathcal{E}_1^c \cup \bigcup_{j=2}^{2^{nR}} \mathcal{E}_j | W=1\right), && (3.18)\\ &\leq \Pr\left(\mathcal{E}_1^c|W=1\right) + \sum_{j=2}^{2^{nR}} \Pr\left(\mathcal{E}_j|W=1\right). && (3.19) \end{aligned}$$

[14]Recall that since the marginal probability of $\tilde{\mathcal{C}}$ is the result of averaging the joint distribution of $\mathcal{C}$ and $\tilde{\mathcal{C}}$ over $\mathcal{C}$, (cf. Lemma 3.2.3) we equivalently average out the conditional probability of error expression over the two codebooks of the system, since the probability space of $\tilde{\mathcal{C}}$ is jointly induced by the mismatch channel and the probability space of $X$.

Next, we bound the probabilities in (3.19):

$$\Pr\left(\mathcal{E}_1^c|W=1\right) \leq \epsilon, \tag{3.20}$$

$$\Pr\left(\mathcal{E}_j|W=1\right) \leq 2^{-n(I(U;Y)-3\epsilon)}, \tag{3.21}$$

for any $\epsilon > 0$ and sufficiently large $n$, where (3.20) follows since $\Pr\left(A_\epsilon^{(n)}\right) > 1-\epsilon$ (cf. Theorem 1.3.2) and (3.21) follows since $\mathbf{u}^n(i)$ and $\mathbf{u}^n(1)$ are independent for $i \neq 1$ (cf. Lemma 3.2.3), hence using the joint-typicality result (cf. Theorem 1.3.2).

Using (3.20) and (3.21) in (3.19) yields,

$$\begin{aligned}
\Pr\left(\mathcal{E}|W=1\right) &\leq \epsilon + \sum_{j=2}^{2^{nR}} 2^{-n(I(U;Y)-3\epsilon)}, && (3.22)\\
&= \epsilon + 2^{nR}2^{-n(I(U;Y)-3\epsilon)}, && (3.23)\\
&= \epsilon + 2^{-n(I(U;Y)-R-3\epsilon)}, && (3.24)\\
&\leq 2\epsilon, && (3.25)
\end{aligned}$$

for any $\epsilon > 0$ and sufficiently large $n$, where (3.25) follows since $I(U;Y) - R > 3\epsilon$ (recall the statement of the theorem). This concludes that $P_e^{(n)} \leq 2\epsilon$ for any $\epsilon > 0$ for sufficiently large $n$. Further, applying the standard procedure for finding a $\left(2^{nR}, n\right)$-codes with $\lambda^{(n)} \leq 4\epsilon$ (cf. [2] pp. 203–204) given a code with $P_e^{(n)} \leq 2\epsilon$, for the case of $\left(2^{nR}, n\right)$ mismatched code, we conclude the proof, since $\epsilon > 0$ may be arbitrarily small for sufficiently large $n$. □

### 3.2.2. Converse

In this section, we provide the converse of Theorem 3.2.1, which is stated below:

**Theorem 3.2.3** *(Converse) For any $\left(2^{nR}, n\right)$ codes with i.i.d. $x_i(w)$ with $P_e^{(n)} \to 0$, we have $R < C$.*

**Proof:** First of all, observe that since the maximal probability of error is greater than its average counter part, to prove the statement in the theorem concludes the converse statement of Theorem 3.2.1.

Next, since the decoder uses only $\tilde{\mathcal{C}}$ (in other words has only access to $\{\mathbf{u}^n(i)\}_{i=1}^{2^{nR}}$) in order to make its decision upon receiving $\mathbf{Y}^n$ we conclude that $U \leftrightarrow W \leftrightarrow Y \leftrightarrow \hat{W}$. Furthermore, note that there is a one-to-one correspondence between $\mathcal{W}$ and $\{\mathbf{u}^n(i)\}_{i=1}^{2^{nR}}$, which is the "encoding function from the decoder's side" and hence implies that $W \leftrightarrow U \leftrightarrow Y \leftrightarrow \hat{W}$ also forms a Markov chain.

**Remark 3.2.1**

*(i) To state the fact that "$W \leftrightarrow U \leftrightarrow Y \leftrightarrow \hat{W}$ forms a Markov chain" (which is the most crucial part of the converse) from another way, note that decoder estimates $W \in \mathcal{W}$ (the actual transmitted message) using $\mathbf{Y}^n$, which is the situation in the original point-to-point communication, so far. The difference for the mismatched codebook case under investigation (as apparent from the name) arises due to the "mismatched codebook" of the decoder, $\tilde{\mathcal{C}} = \{\mathbf{u}^n(i)\}_{i=1}^{2^{nR}}$, which is the only codeword set available at decoder side and has the aforementioned one-to-one relation with message set (cf. Remark 3.1.1). Combining these facts altogether yields the Markov chain structure between $W \leftrightarrow U \leftrightarrow Y \leftrightarrow \hat{W}$.*

*(ii) Note that the aforementioned fact also has an intuitive (yet not so rigorous) explanation: from the decoder side, the* only *channel between encoder and decoder is $p(\mathbf{y}^n|\mathbf{u}^n)$ with the* shared *(an hypothetical channel, depends on the choice of $p(x)$) codebooks $\tilde{\mathcal{C}}$ at both encoder and decoder, since there's a one-to-one relation between $w, \mathbf{x}^n(w), \mathbf{u}^n(w)$), recalling the formation of the decoder's codebook. Therefore, although the encoder sends $\mathbf{x}^n(w)$ using the original communication channel ($p(y|x)$), the effective situation from the decoder side is the encoder sends $\mathbf{u}^n(w)$ using the hypothetical channel $p(\mathbf{y}^n|\mathbf{u}^n)$. The channel $p(\mathbf{y}^n|\mathbf{u}^n)$ is* known *at decoder's side (since both $p(x)$, $p(y|x)$ and $p(u|x)$ is known); therefore, the problem transforms to the classical point-to-point communication variant.*

*(iii) The meaning of the hypothetical channel $p(\mathbf{y}^n|u^n)$ mentioned in item (ii) above can be explained as follows: since the received $\mathbf{y}^n$ is due to $\mathbf{x}^n(w)$ through the channel $p(y|x)$, and the corresponding $\mathbf{u}^n(w)$ is due to $\mathbf{x}^n(w)b$; hence the dependence of $\mathbf{y}^n$ to $\mathbf{u}^n(w)$ is over $\mathbf{x}^n(w)$; therefore decoder in some sense "finds out" $\mathbf{x}^n(w)$ first (through the usage of $p(\mathbf{x}^n|\mathbf{u}^n)$) (which can be calculated, since $p(x)$ and $p(u|x)$ is available at the decoder), and then decides on $\hat{W}$ using $p(y|x)$ and the "found out" $\mathbf{x}^n(w)$ mentioned above.*

Further, recalling (3.4) we know that $p(y|u)$ is memoryless. Keeping this facts in mind, we continue with following arguments:

$$\begin{aligned}
nR &= H(W), && (3.26)\\
&= I(\hat{W};W) + H(W|\hat{W}), && (3.27)\\
&\leq I(\mathbf{U}^n;\mathbf{Y}^n) + \left(1 + nRP_e^{(n)}\right), && (3.28)\\
&= H\left(\mathbf{Y}^n\right) - \sum_{i=1}^{n} H\left(Y_i|U_i\right) + \left(1 + nRP_e^{(n)}\right), && (3.29)\\
&\leq \left(1 + nRP_e^{(n)}\right) + \sum_{i=1}^{n} \left(H(Y_i) - H(Y_i|U_i)\right), && (3.30)\\
&= \left(1 + nRP_e^{(n)}\right) + \sum_{i=1}^{n} I(U_i;Y_i), && (3.31)
\end{aligned}$$

where (3.26) follows since $W$ is uniformly distributed over $\mathcal{W}$, (3.28) follows using Fano's inequality [2], (3.29) follows using (3.4), (3.30) follows since $\sum_{i=1}^{n} H(Y_i) \leq H\left(\mathbf{Y}^n\right)$ and (3.31) follows using definition of mutual information.

Next, we aim to upper bound the second term of the RHS of (3.31)

$$\begin{aligned}
I(U;Y) &= \sum_{u,y} p(u,y) \log \frac{p(y|u)}{p(y)} && (3.32)\\
&= \sum_{u,y} \sum_{x} p(x)p(u|x)p(y|x) \log \frac{\frac{\sum_x p(x)p(y|x)p(u|x)}{\sum_x p(x)p(u|x)}}{\sum_x p(x)p(y|x)}, && (3.33)
\end{aligned}$$

where (3.33) follows using (3.1). Note that the only variable of (3.33) is $p(x)$, hence we conclude that

$$I(U_i;Y_i) \leq \max_{p(x)} I(U;Y) = C, \text{ for all } (U_i,Y_i) \text{ pairs.} \tag{3.34}$$

Using (3.34) in (3.31), we have

$$\begin{aligned} R &\leq \frac{1}{n} + RP_e^{(n)} + C, &(3.35)\\ &\leq \epsilon + C, &(3.36) \end{aligned}$$

for any $\epsilon > 0$ and sufficiently large $n$, where (3.36) follows since $P_e^n \to 0$ (cf. recall the statement of the theorem) and $1/n \leq \epsilon$ for sufficiently large $n$. Hence (3.36) implies $R < C$, which is the desired result. □

### 3.2.3. Binary Symmetric Communication and Mismatch Channel Case

In this section, we consider a specific example of the discrete codebook mismatched channel with i.i.d. codewords, which is shown in Figure 3.1. To be more precise, we consider the case for which $\mathcal{X} = \mathcal{Y} = \mathcal{U} = \{0,1\}$, both communication and codebook channels are binary symmetric channels with crossover probabilities $p_1$ and $p_2$, respectively, i.e.

$$Y \stackrel{\triangle}{=} X \oplus Z_1, \tag{3.37}$$

where $\Pr(Z_1 = 1) = p_1$ and $\Pr(Z_1 = 0) = 1 - p_1$ and similarly

$$U \stackrel{\triangle}{=} X \oplus Z_2, \tag{3.38}$$

where $\Pr(Z_2 = 1) = p_2$ and $\Pr(Z_2 = 0) = 1 - p_2$, where $\oplus$ denotes addition modulo 2 and w.l.o.g. we assume that $p_1, p_2 < 1/2$.

**Theorem 3.2.4** *For the BSC case of the discrete codebook mismatched channel with i.i.d. codewords, the capacity is given by*

$$C = 1 - H(p_1 + p_2(1 - 2p_1)), \tag{3.39}$$

*where capacity is only achieved for the case of Bernoulli* $1/2$ *distributed* $X$*, i.e.* $Pr\,(X = 1) = Pr\,(X = 0) = 1/2$.

**Proof:** First of all, we define the auxiliary random variable $V$ in the following way:

$$V \stackrel{\triangle}{=} X \oplus Z_1 \oplus Z_2. \tag{3.40}$$

Next, we prove following lemma:

**Lemma 3.2.4** $U \leftrightarrow V \leftrightarrow Y$ *forms a Markov chain, i.e.*

$$p(u, y|v) = p(u|v)p(y|v). \tag{3.41}$$

**Proof:** First of all, observe that we have $U = V \oplus Z_1$ and $Y = V \oplus Z_2$ (cf. (3.37) and (3.38))

$$\begin{aligned} \Pr\left(U = u|V = v\right) &= \Pr\left(Z_1 = u \oplus v\right), & (3.42)\\ \Pr\left(Y = y|V = v\right) &= \Pr\left(Z_2 = y \oplus v\right), & (3.43) \end{aligned}$$

for all $u, v, y \in \{0, 1\}$.

Furthermore, we also have

$$\begin{aligned} \Pr\left(U=u, Y=y|V=v\right) &= \Pr\left(Z_1=u\oplus v, Z_2=y\oplus v\right), && (3.44)\\ &= \Pr\left(Z_1=u\oplus v\right)\Pr\left(Z_2=y\oplus v\right), && (3.45) \end{aligned}$$

for all $u, v, y \in \{0, 1\}$, where (3.44) follows using (3.37) and (3.38) and (3.45) follows since $Z_1$ and $Z_2$ are independent. Combining (3.42), (3.43) and (3.45) we conclude that $p(u, y|v) = p(u|v)p(y|v)$, which is the sought-after result. □

Next, observe that from the definition of auxiliary random variable $V$ (cf. (3.40)) we have $X \leftrightarrow U \leftrightarrow V$ forms a Markov chain, i.e.

$$p(x, v|u) = p(x|u)p(v|u), \tag{3.46}$$

and $X \leftrightarrow Y \leftrightarrow V$ forms a Markov chain, i.e.

$$p(x, v|y) = p(x|y)p(v|y). \tag{3.47}$$

Furthermore, combining (3.1) and (3.41) yields following "circular Markov chain" structure between $X, Y, V, U$ which helps to visualize the situation at hand better and is the first of its kind, to the best of our knowledge.

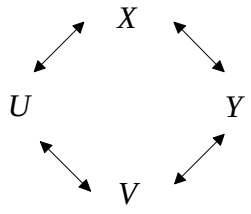


Figure 3.2. The *circular Markov chain structure* of random variables $X, Y, V, U$ defined for the binary symmetric communication and mismatch channels of Section 3.2.3.

Now, let's evaluate the following expression from two different way using the chain rule for mutual information:

$$\begin{aligned} I(U,Y;V) &= I(V;U) + I(V;Y|U), && (3.48)\\ &= I(V;Y) + I(V;U|Y). && (3.49) \end{aligned}$$

Next, define $A \stackrel{\triangle}{=} I(U;Y) - I(U;V|Y)$ and $B \stackrel{\triangle}{=} I(V;Y) - I(V;Y|U)$. Using the definition of mutual information, we have

$$\begin{aligned} A &= H(U) - H(U|Y) - H(U|Y) + H(U|V,Y), && (3.50)\\ &= I(U;Y) - I(U;Y|V), && (3.51)\\ &= I(U;Y), && (3.52) \end{aligned}$$

where (3.52) follows since $U \leftrightarrow V \leftrightarrow Y$ forms a Markov chain (cf. (3.41)).

Further, again using definition of mutual information, we have

$$\begin{aligned} B &= H(V) - H(V|Y) - H(V|U) + H(V|U,Y), && (3.53)\\ &= H(V) + H(V|U,Y) - H(p_1) - H(p_2), && (3.54) \end{aligned}$$

where (3.54) follows using (3.37), (3.38) and (3.40).

Now, we should find a way to evaluate $H(V|U,Y)$. Keeping this goal in mind, we continue with following development.

Using chain rule for entropy, we have

$$\begin{aligned} H(X,U,Y,V) &= H(U,Y|X,V) + H(X,V), && (3.55)\\ &= H(X,V|U,Y) + H(U,Y), && (3.56) \end{aligned}$$

Next, we continue with evaluating individual terms in (3.55) and (3.56).

$$H(U,Y|X,V) = H(U|X,V) + H(Y|X,V), \quad (3.57)$$
$$H(X,V) = H(V|X) + H(X), \quad (3.58)$$

where (3.57) (resp.(3.58) ) follows using (3.46) (chain rule for joint entropy).

Further, we have

$$H(X,V|U,Y) = H(X|U,Y) + H(V|U,Y), \quad (3.59)$$
$$= H(X,U,Y) - H(U,Y) + H(V|U,Y), \quad (3.60)$$
$$= H(U,Y|X) + H(X) - H(U,Y) + H(V|U,Y), \quad (3.61)$$
$$= H(U|X) + H(Y|X) + H(X) - H(U,Y) + H(V|U,Y), \quad (3.62)$$

where (3.59) follows using (3.47), (3.60) and (3.61) follows using chain rule for entropy, (3.62) follows using (3.1).

Now, it is time to sum up things. Using (3.57) and (3.58) in (3.55), using (3.62) in (3.56) and equating these two expressions yields:

$$H(V|U,Y) = H(U|X,V) + H(Y|X,V) + H(V|X) - H(U|X) - H(Y|X), \quad (3.63)$$
$$= H(U|X,V) + H(Y|X,V) + H(V|X) - H(p_1) - H(p_2), \quad (3.64)$$

where (3.64) follows using (3.37) and (3.38).

Now, we evaluate the remaining terms in (3.64). First of all, observe that we have (using definition of auxiliary random variable $V$)

$$p(v = k|x = k) = 1 - p_1 - p_2 + 2p_1p_2, \quad (3.65)$$
$$p(v = k|x = \bar{k}) = p_1 + +p_2 - 2p_1p_2. \quad (3.66)$$

Using this result in $H(V|X)$ expression yields:

$$H(V|X) = H(p_1 + p_2 - 2p_1p_2). \tag{3.67}$$

Next, we deal with first and second equations of the RHS of (3.64)

$$\begin{aligned}
H(U|X,V) &= H(X,U,V) - H(X,V), && (3.68)\\
&= H(X,V|U) + H(U) - H(X,V), && (3.69)\\
&= H(X|U) + H(V|U) + H(U) - H(V|X) - H(X), && (3.70)\\
&= H(X,U) + H(V|U) - H(V|X) - H(X), && (3.71)\\
&= H(U|X) + H(V|U) - H(V|X), && (3.72)\\
&= H(p_2) + H(p_1) - H(p_1 + p_2 - 2p_1p_2), && (3.73)
\end{aligned}$$

where (3.68) and (3.69) follows using chain rule for entropy, (3.70) follows using (3.46), (3.71) and (3.72) follows using chain rule for entropy, (3.73) using (3.37), (3.38) and (3.67).

Similarly,

$$\begin{aligned}
H(Y|X,V) &= H(X,Y,V) - H(X,V), && (3.74)\\
&= H(X,V|Y) + H(Y) - H(X,V), && (3.75)\\
&= H(X|Y) + H(V|Y) + H(U) - H(V|X) - H(X), && (3.76)\\
&= H(X,Y) + H(V|Y) - H(V|X) - H(X), && (3.77)\\
&= H(Y|X) + H(V|Y) - H(V|X), && (3.78)\\
&= H(p_1) + H(p_2) - H(p_1 + p_2 - 2p_1p_2), && (3.79)
\end{aligned}$$

where (3.74) and (3.75) follows using chain rule for entropy, (3.76) follows using (3.47), (3.77) and (3.78) follows using chain rule for entropy, (3.79) using (3.37), (3.38) and (3.67).

Finally, using (3.67), (3.73) and (3.79) in (3.64) yields:

$$H(V|U,Y) = H(p_1) + H(p_2) - H(p_1 + p_2 - 2p_1p_2), \tag{3.80}$$

Now, plugging (3.80) in (3.49) yields:

$$\begin{aligned} I(U;Y) &= H(V) - H(p_1 + p_2 - 2p_1p_2), && (3.81)\\ &\leq 1 - H(p_1 + p_2(1-2p_1)), && (3.82) \end{aligned}$$

where equality in equation (3.82) is achieved if and only if $V$ is Bernoulli $1/2$, which is the case if and only if $X$ is Bernoulli $1/2$. This concludes the proof of theorem. $\square$

**Remark 3.2.2** *Note that for $0 < p_2, p_1 < 1/2$, we have*

$$p_1 < p_1 + p_2(1-2p_1) < (1-p_1), \tag{3.83}$$

*where the LHS of* (3.83) *follows since $1 - 2p_1 > 0$ and the RHS of* (3.83) *follows since*

$$\begin{aligned} [p_1 + p_2(1-2p_1) < (1-p_1)] &\Leftrightarrow [2p_1(1-p_2) < (1-p_2)], && (3.84)\\ &\Leftrightarrow [1/2 > p_1]. && (3.85) \end{aligned}$$

*Now, since binary entropy function is monotonic increasing (resp. decreasing) for $0 \leq p \leq 1/2$ (resp. $1/2 \leq p \leq 1$) and is further symmetric around $p = 1/2$, we conclude that the capacity of BSC case of codebook mismatch setup (cf.* (3.39)*) is strictly less than the "original Shannon type" counterpart (which is a special case of the setup at hand with $p_2 = 0$) for $0 < p_2, p_1 < 1/2$. To be more precise, we have*

$$1 - H(p_1 + p_2(1-2p_1)) < 1 - H(p_1), \tag{3.86}$$

*for* $0 < p_2, p_1 < 1/2$.

*Furthermore, observe that for* $p_2 = 0$ *case,* $1 - H(p_1 + p_2(1 - 2p_1)) = 1 - H(p_1)$, *which is the capacity of the case of "perfectly matched codebooks". Moreover, for* $p_2 = 1/2$ *case,* $1 - H(p_1 + p_2(1 - 2p_1)) = 1 - H(1/2) = 0$ *regardless of the value of* $p_1$ *which is also obvious, since this case corresponds to "perfectly mismatched codebooks", which implies that it is not possible to transmit any information, since decoder does not have a meaningful codebook.*

# 4. CONCLUSIONS

In this thesis, our main approach is to investigate the usage of typicality in two different contexts.

In the first one, we introduce a novel approach to cryptanalysis. We aim to explore *fundamental performance limits* within a specified class of attacks of interest, targeted towards breaking a particular cryptosystem. As a first step, we illustrate our approach via considering the class of "Query-Based Key-Recovery" (QuBaR) attacks against ABSG, which is an LFSR-based stream cipher constructed via irregular decimation techniques. In order to achieve this task, we rely on the following assumptions (which are quite common in conventional cryptanalysis): The input sequence to ABSG is assumed to be an independent identically distributed Bernoulli process with probability 1/2; the attacker has access to the output sequence of ABSG; an explicit knowledge of the generating LFSR's feedback polynomial is not used; and the degree of the feedback polynomial (denoted by $L$) of the generating LFSR is sufficiently large. Using these assumptions, we show that breaking ABSG is equivalent to determine the exact realizations of a sequence of random variables, which are proven to be independent identically distributed with geometric distribution of parameter 1/2. Next, we investigate a setup of interest, in which we concentrate on the "Exhaustive-Search Type QuBaR" attacks (which form a subset of general-case QuBaR attacks, such that the starting index of all guesses in any element of this set is constrained to be equal to unity). Here, using the typicality notion, we prove that the tight lower bound (to the first order in the exponent) on the algorithmic complexity of any successful Exhaustive-Search Type QuBaR attack is $2^{2L/3}$. Our result can be viewed as a "negative advice" to the cryptanalyst (contrary to the conventional trend in cryptanalysis, where the general goal is to deduce a "negative design advice" to the cryptosystem designer) in terms of QuBaR attacks against ABSG under the aforementioned assumptions.

In the second one, we introduced the new concept of *reliable communication under codebook mismatch* of which novel, anti-symmetric nature is very exciting from both

theoretical and practical point of view. For this problem and under the assumption of i.i.d. encoder codewords, we show the operational capacity of the system is equal to the information capacity of the system, which is given as $\max_{p(x)} I(U;Y)$. We illustrate the concept by considering the special case where both communication and mismatch channels are binary symmetric channels with crossover probabilities $p_1$ and $p_2$, respectively. In order to find the information capacity, we employ a circular markov chain structure, which deserves to be mentioned here, because of its interesting nature.

# APPENDIX A: PROOF OF LEMMA 2.2.1

First, note that each output bit $Z_i = z_i$ (for $1 \leq i \leq N$) is produced by a *block* of input bits from the input sequence $\mathbf{X}_1^M$. In order to identify the $i$-th input block that generates $Z_i$ (for $1 \leq i \leq N$), we define

$$A_i \stackrel{\triangle}{=} 1 + \sum_{j=1}^{i-1} [Q_j + 2] = H_{i-1} - H_0 + 1 = H_{i-1} + 1, \tag{I-1}$$

$$B_i \stackrel{\triangle}{=} \sum_{j=1}^{i} [Q_j + 2] = H_i - H_0 = H_i, \tag{I-2}$$

where we used $H_0 = 0$ as the initial condition. Hence, we note that the input block $\mathbf{X}_{A_i}^{B_i}$ produces the $i$-th output bit $Z_i = z_i$ which is given per assumption A2. Further, from the definition of the algorithm $\mathcal{B}$ (see Definition 2.1.1), we have

$$\Pr\left(X_{A_i+1} = z_i \,|\, Z_i = z_i\right) = 1. \tag{I-3}$$

Next, note that the statement of the lemma is *equivalent to*

$$\Pr\left(\mathbf{Q}_1^N = \mathbf{q}_1^N \,|\, \mathbf{Z}_1^N = \mathbf{z}_1^N\right) = \prod_{i=1}^{N} \left[\Pr\left(Q_i = q_i \,|\, \mathbf{Z}_1^N = \mathbf{z}_1^N\right)\right] = \prod_{i=1}^{N} \left(\frac{1}{2}\right)^{q_i+1}. \tag{I-4}$$

Thus, it is necessary and sufficient to show (I-4) to prove Lemma 2.2.1. In order to show (I-4), we use proof by induction.

- Step 1: We would like to show

$$\Pr\left(Q_1 = q_1 \,|\, \mathbf{Z}_1^N = \mathbf{z}_1^N\right) = \left(\frac{1}{2}\right)^{q_1+1}. \tag{I-5}$$

Since the value of $Q_1$ depends only on the first output bit, we have

$$\Pr\left(Q_1 = q_1 \,|\, \mathbf{Z}_1^N = \mathbf{z}_1^N\right) = \Pr\left(Q_1 = q_1 \,|\, Z_1 = z_1\right). \tag{I-6}$$

Next,

$$\begin{aligned}
\Pr\left(Q_1 = 0 \,|\, Z_1 = z_1\right) &= \Pr\left(X_1 = z_1, X_2 = z_1 \,|\, Z_1 = z_1\right), && \text{(I-7)}\\
&= \Pr\left(X_1 = z_1 \,|\, Z_1 = z_1\right), && \text{(I-8)}\\
&= \frac{1}{2}, && \text{(I-9)}
\end{aligned}$$

where (I-7) follows from the definition of the mapping $\mathcal{M}(\cdot,\cdot)$ (Table 2.1), (I-8) follows from (I-3), (I-9) follows from assumption A1. Also, for $q_1 > 0$,

$$\begin{aligned}
&\Pr\left(Q_1 = q_1 \,|\, Z_1 = z_1\right)\\
=\ &\Pr\left(X_1 = \bar{z}_1, X_2 = z_1, \ldots, X_{q_1+1} = z_1, X_{q_1+2} = \bar{z}_1 \,|\, Z_1 = z_1\right), && \text{(I-10)}\\
=\ &\Pr\left(X_1 = \bar{z}_1, X_3 = z_1, \ldots, X_{q_1+1} = z_1, X_{q_1+2} = \bar{z}_1 \,|\, Z_1 = z_1\right), && \text{(I-11)}\\
=\ &\left(\frac{1}{2}\right)^{q_1+1} && \text{(I-12)}
\end{aligned}$$

where (I-10) follows from the definition of the mapping $\mathcal{M}$ (Table 2.1), (I-11) follows from (I-3), (I-12) follows from assumption A1. Combining (I-9) and (I-12), we get (I-5).

- Step 2: We assume that

$$\Pr\left(\mathbf{Q}_1^{n-1} = \mathbf{q}_1^{n-1} \,|\, \mathbf{Z}_1^N = \mathbf{z}_1^N\right) = \prod_{i=1}^{n-1}\left[\Pr\left(Q_i = q_i \,|\, \mathbf{Z}_1^N = \mathbf{z}_1^N\right)\right] = \prod_{i=1}^{n-1}\left(\frac{1}{2}\right)^{q_i+1}. \tag{I-13}$$

- Step 3: Given (I-13) we want to show that

$$\Pr\left(\mathbf{Q}_1^{n} = \mathbf{q}_1^{n} \,|\, \mathbf{Z}_1^N = \mathbf{z}_1^N\right) = \prod_{i=1}^{n}\left[\Pr\left(Q_i = q_i \,|\, \mathbf{Z}_1^N = \mathbf{z}_1^N\right)\right] = \prod_{i=1}^{n}\left(\frac{1}{2}\right)^{q_i+1}. \tag{I-14}$$

Note that, given (I-13), (I-14) is equivalent to

$$\Pr\left(Q_n = q_n \,|\, \mathbf{Q}_1^{n-1} = \mathbf{q}_1^{n-1}, \mathbf{Z}_1^N = \mathbf{z}_1^N\right) = \Pr\left(Q_n = q_n \,|\, \mathbf{Z}_1^N = \mathbf{z}_1^N\right) = \left(\frac{1}{2}\right)^{q_n+1}, \tag{I-15}$$

using Bayes rule. Now,

$$\begin{aligned}
& \Pr\left(Q_n = 0 \,|\, \mathbf{Q}_1^{n-1} = \mathbf{q}_1^{n-1}, \mathbf{Z}_1^N = \mathbf{z}_1^N\right) \\
= \;& \Pr\left(X_{A_n} = z_n, X_{A_n+1} = X_{B_n} = z_n \,|\, \mathbf{Q}_1^{n-1} = \mathbf{q}_1^{n-1}, \mathbf{Z}_1^N = \mathbf{z}_1^N\right), && \text{(I-16)} \\
= \;& \Pr\left(X_{A_n} = z_n \,|\, \mathbf{Q}_1^{n-1} = \mathbf{q}_1^{n-1}, \mathbf{Z}_1^N = \mathbf{z}_1^N\right), && \text{(I-17)} \\
= \;& \Pr\left(X_{A_n} = z_n \,|\, \mathbf{Z}_1^N = \mathbf{z}_1^N\right) = \Pr\left(Q_n = 0 \,|\, \mathbf{Z}_1^N = \mathbf{z}_1^N\right), && \text{(I-18)} \\
= \;& \Pr\left(X_{A_n} = z_n \,|\, Z_n = z_n\right) = \frac{1}{2} && \text{(I-19)}
\end{aligned}$$

where (I-16) follows from the definition of the mapping $\mathcal{M}(\cdot,\cdot)$ (Table 2.1), (I-17) follows from (I-3), (I-18) and (I-19) follow from assumption A1 [15] . On the other hand, for $q_n > 0$, we have

$$\begin{aligned}
& \Pr\left(Q_n = q_n \,|\, \mathbf{Q}_1^{n-1} = \mathbf{q}_1^{n-1}, \mathbf{Z}_1^N = \mathbf{z}_1^N\right) \\
= \;& \Pr\left(X_{A_n} = \bar{z}_n, X_{A_n+1} = z_n, \ldots, X_{B_n} = \bar{z}_n \,|\, \mathbf{Q}_1^{n-1} = \mathbf{q}_1^{n-1}, \mathbf{Z}_1^N = \mathbf{z}_1^N\right), && \text{(I-20)} \\
= \;& \Pr\left(X_{A_n} = \bar{z}_n, X_{A_n+2} = z_n, \ldots, X_{B_n} = \bar{z}_n \,|\, \mathbf{Q}_1^{n-1} = \mathbf{q}_1^{n-1}, \mathbf{Z}_1^N = \mathbf{z}_1^N\right), && \text{(I-21)} \\
= \;& \Pr\left(X_{A_n} = \bar{z}_n, X_{A_n+2} = z_n, \ldots, X_{B_n} = \bar{z}_n \,|\, \mathbf{Z}_1^N = \mathbf{z}_1^N\right), && \text{(I-22)} \\
= \;& \Pr\left(X_{A_n} = \bar{z}_n, X_{A_n+2} = z_n, \ldots, X_{B_n} = \bar{z}_n \,|\, Z_n = z_n\right) = \left(\frac{1}{2}\right)^{q_n+1}, && \text{(I-23)}
\end{aligned}$$

where (I-20) follows from the definition of the mapping $\mathcal{M}(\cdot,\cdot)$ (Table 2.1), (I-21) follows from (I-3), (I-22) and (I-23) follow from assumption A1 (see the discussion in the footnote). Combining (I-18), (I-19), (I-22), (I-23), we get (I-15), and equivalently (I-14), which completes the proof.

□

[15] Since $\mathbf{X}$ is an i.i.d. Bernoulli 1/2 process, the value of $\Pr\left(X_{A_n} = z_n \,|\, Z_n = z_n\right)$ is independent of the particular value of $A_n$ and that is why it is equal to 1/2.

# APPENDIX B: PROOF OF THEOREM 2.2.1

The equivalence of the first and second problems is shown in [26]. In order to prove the theorem, we proceed with proving the equivalence of the second and third problems.

First, we show that the third problem reduces to the second problem in $poly\,(L)$ time: Since we know $\mathbf{z}_1^N$ and $\mathbf{Q}_i^{\theta+i-1}$ per assumption, we construct $L$ consecutive bits of $\mathbf{X}_1^M$ via using Definition 2.1.1 in the following way. We are given $\mathbf{Q}_i^{i+\theta-1} = \mathbf{q}_i^{i+\theta-1}$ such that (2.4) holds. Then, we apply the following algorithm:

1. For each $j = i, i+1, \ldots, \theta+i-1$ do:
   (a) If $q_j = 0$, generate $B_j = \{z_j, z_j\}$.
   (b) If $q_j > 0$, generate $B_j = \left\{\bar{z}_j, z_j^{q_j}, \bar{z}_j\right\}$
2. Concatenate $\{B_j\}_{j=i}^{\theta+i-1}$ thereby forming the desired $\mathbf{X} = \mathbf{x}$ sequence.

Note that, the condition (2.4) ensures that the resulting $\mathbf{X} = \mathbf{x}$ sequence $\{B_i, B_{i+1}, \ldots, B_{\theta+i-1}\}$ is of length at least $L$. Furthermore, from the definition of the ABSG algorithm, the resulting $\mathbf{X} = \mathbf{x}$ sequence is unique and necessarily the correct one. Obviously, this algorithm runs in $poly\,(L)$ time, which completes the proof for this case.

Next, we proceed with showing that the second problem can be reduced to the third problem via an algorithm in probabilistic polynomial time. First, note the following Lemma.

**Lemma II-1** *Under the assumptions A1, A2, A3, and A4, for any $n \in \mathbb{Z}^+$, we have*

$$\Pr\left[\wedge_{l=0}^{poly(L)} Y_{n+l} \neq \varnothing\right] \leq \epsilon, \tag{II-1}$$

*for any $\epsilon > 0$ for $L$ sufficiently large.*

**Proof:** First, under the given assumptions, we note the following fundamental results from [27]:

- For any $n \in \mathbb{Z}^+$,

$$\Pr\left(Y_n = \varnothing\right) = \frac{1}{3} + \frac{2}{3}\left(-\frac{1}{2}\right)^n. \tag{II-2}$$

- $\{Y_n\}$ form a Markovian process with memory-1:

$$\Pr\left(Y_n | \mathbf{Y}_1^{n-1} = \mathbf{y}_1^{n-1}\right) = \Pr\left(Y_n | Y_{n-1} = y_{n-1}\right), \tag{II-3}$$

  for any $n \in \mathbb{Z}^+$.

- For any $n \in \mathbb{Z}^+$,

$$\Pr\left(Y_n \neq \varnothing | Y_{n-1} \neq \varnothing\right) = \frac{1}{2}. \tag{II-4}$$

Hence, for any $\epsilon > 0$ we have

$$\begin{aligned}
\Pr\left[\wedge_{l=0}^{poly(L)} Y_{n+l} \neq \varnothing\right] &= \Pr\left(Y_n \neq \varnothing\right) \prod_{l=1}^{poly(L)} \Pr\left(Y_{n+l} \neq \varnothing | \wedge_{k=0}^{l-1} Y_{n+k} \neq \varnothing\right), && \text{(II-5)}\\
&= \Pr\left(Y_n \neq \varnothing\right) \prod_{l=1}^{poly(L)} \Pr\left(Y_{n+l} \neq \varnothing | Y_{n+l-1} \neq \varnothing\right), && \text{(II-6)}\\
&= \left[\frac{2}{3} - \frac{2}{3}\left(-\frac{1}{2}\right)^n\right] \cdot \left(\frac{1}{2}\right)^{poly(L)-1}, && \text{(II-7)}\\
&\leq \epsilon && \text{(II-8)}
\end{aligned}$$

where (II-5) follows from Bayes rule, (II-6) follows from (II-3), (II-7) follows from (II-2) and (II-4), (II-8) follows from the fact that the first term in (II-7) is constant in $L$ and the second term is exponentially decaying in $L$ whence $\epsilon$ can be made arbitrarily small for sufficiently large $L$. □

Now, since $Y_n \in \{0, 1, \varnothing\}$ (i.e., there are constant possibilities for $Y_n$), without loss of generality, we assume that $Y_n$ is known. Since we are also given $\mathbf{X}_{n+1}^{n+L}$ for some $n \in \mathbb{Z}^+$, this also means we know $\mathbf{Y}_n^{n+L}$ (via successively applying $\mathcal{M}(Y_{n+l-1}, X_{n+l})$ for $l = 1, 2, \ldots, L$). Next, consider the following situations:

1. $\underline{Y_n = Y_{n+L} = \varnothing}$:

   In this case, w.l.o.g. we choose $h_{i-1} = n$ for some $i$. Next, let $K$ denote the number of $\varnothing$'s within the sequence $\mathbf{Y}_n^{n+L}$ (which is necessarily $\geq 2$ per assumption) and assign $\theta = K - 1$. Next, let $h_{i+j-2}$ denote the index of the $j$-th $\varnothing$ within the sequence $\mathbf{Y}_n^{n+L}$, where $1 \leq j \leq K = \theta + 1$ (implying $h_{i+K-2} = h_{i+\theta-1} = n + L$). Accordingly, assign $q_j = h_j - h_{j-1} - 2$ for all $j \in \{i, i+1, \ldots, i+\theta-1\}$. Note that, all these $\{h_j\}$ (equivalently $\{q_j\}$) are known since $\mathbf{Y}_n^{n+L}$ is known. Consequently, this means we have identified $\mathbf{Q}_i^{i+\theta-1} = \mathbf{q}_i^{i+\theta-1}$ such that

   $$\sum_{j=i}^{\theta+i-1} (q_j + 2) = \sum_{j=i}^{\theta+i-1} (h_j - h_{j-1}) = h_{\theta+i-1} - h_i = L, \tag{II-9}$$

   satisfying the constraint (2.4). Further, note that the operations performed within this procedure constitute an algorithm, which is in deterministic polynomial time (implying it is also in probabilistic polynomial time).

2. $\underline{Y_n = \varnothing \text{ and } Y_{n+L} \neq \varnothing}$:

   In this case, since $Y_{n+L} \neq \varnothing$, we aim to identify some $Y_{n+L+L'} = \varnothing$ for $L' > 0$ with high probability in polynomial time. To achieve this task, we consider the sequence $\{Y_{n+L+k}\}$ for $k > 0$. Now, note that as we increment $k$, after $poly(L)$ steps we necessarily need to come across a $\varnothing$ with high probability (the probability of *not* coming across a $\varnothing$ is exponentially small in $L$ per Lemma II-1). Thus, we have $Y_n = Y_{n+L''} = \varnothing$ where $L'' = L + L' > L$. Next, applying algorithmic steps analogous to the ones in Situation 1 (i.e., beginning from $Y_n = Y_{n+L''} = \varnothing$), we identify $\mathbf{Q}_i^{i+\theta-1} = \mathbf{q}_i^{i+\theta-1}$ such that

   $$\sum_{j=i}^{\theta+i-1} (q_j + 2) = \sum_{j=i}^{\theta+i-1} (h_j - h_{j-1}) = h_{\theta+i-1} - h_i = L'' > L, \tag{II-10}$$

satisfying the constraint (2.4). Further, note that the operations performed within this procedure constitute an algorithm, which is in probabilistic polynomial time.

3. $\underline{Y_n \neq \varnothing \text{ and } Y_{n+L} = \varnothing}$:

   Our overall goal is to identify (via using an algorithm, which is in probabilistic polynomial time) $Y_{n+L} = Y_{n+L'''} = \varnothing$ such that $L''' - L > L$. In that case, we would be able to apply algorithmic steps analogous to the ones in Situation 1 (i.e., beginning from $Y_{n+L} = Y_{n+L'''} = \varnothing$) and identify $\mathbf{Q}_i^{i+\theta-1} = \mathbf{q}_i^{i+\theta-1}$ such that

$$\sum_{j=i}^{\theta+i-1} (q_j + 2) = \sum_{j=i}^{\theta+i-1} (h_j - h_{j-1}) = h_{\theta+i-1} - h_i = L''' - L > L, \qquad \text{(II-11)}$$

   satisfying the constraint (2.4). Next, we show that, beginning from $Y_{n+L}$, we are able to find some $Y_{n+L'''} = \varnothing$ such that $L''' > 2L$ via a probabilistic polynomial time algorithm. To see this, first consider the sequence $\{Y_{n+L+k}\}$ for $k > 0$ (as we did in Situation 2). Following Lemma II-1 and using similar arguments to Situation 2, we see that as we increment $k$ by $poly\,(L)$, we necessarily come across a $\varnothing$ with high probability. Next, we apply this step $L/2$ times; at each step, we increment $k$ by $poly\,(L)$ and at each step, we see a $\varnothing$ with probability $1 - \epsilon$ where $\epsilon$ is exponentially small in $L$ per Lemma II-1. Thus, as a result of incrementing $k$ by a total of $\frac{L}{2} \cdot poly\,(L)$ (which is again $poly\,(L)$), we observe $L/2$ $\varnothing$'s with sufficiently high probability, which makes this procedure an algorithm in probabilistic polynomial time. On the other hand, observing $L/2$ $\varnothing$'s guarantee us to identify some $L'''$ such that $L''' > 2L$ since the gap between two $\varnothing$'s is at least 2 due to the definition of the ABSG algorithm. As a result, we see that we can identify $Y_{n+L'''} = \varnothing$ such that $L''' - L > L$ via an algorithm which is in probabilistic polynomial time, which was our initial goal.

4. $\underline{Y_n \neq \varnothing \text{ and } Y_{n+L} \neq \varnothing}$:

   This is straightforward via applying an approach analogous to the Situation 3 above. Again, we begin from $Y_{n+L}$, consider the sequence $Y_{n+L+k}$ for $k > 0$, increment $k$ in blocks of length $poly\,(L)$; the only difference is that this time we use $\frac{L}{2} + 1$ blocks (each of which is $poly\,(L)$) instead of $\frac{L}{2}$. As a result, we are guaranteed to identify $Y_{n+L''''} = Y_{n+L'''''} = \varnothing$ such that $L'''' - L'''' > L$ via an

algorithm which is in probabilistic polynomial time; the rest is obvious.

Thus, the proof of the (probabilistic polynomial time) reduction of the second problem to the third one is completed. Hence the proof of Theorem 2.2.1. □

# APPENDIX C: PROOF OF THEOREM 2.3.1

For the sake of clarity, throughout this section we use the notation $G_k\left(i_k, \theta_k, \left(\mathbf{q}_{i_k}^{\theta_k+i_k-1}\right)_k\right)$ (instead of $G_k\left(i_k, \theta_k, \mathbf{q}_{i_k}^{\theta_k+i_k-1}\right)$) to denote a particular guess $G_k$.

Choosing $n \stackrel{\triangle}{=} L/3$, first we define the typical set (cf. (1.5)) $A_\epsilon^{(n)}$ with respect to $p(q)$ (given by (2.3)):

$$A_\epsilon^{(n)} \stackrel{\triangle}{=} \left\{\mathbf{q}_1^n \,:\, \left|-\frac{1}{n}\log p\left(\mathbf{q}_1^n\right) - H(Q)\right| \leq \epsilon\right\}, \tag{III-1}$$

where (using logarithm with base-2)

$$H(Q) = -\sum_{q=0}^{\infty} p(q)\log p(q) = 2.$$

At this point, we also restate the two fundamental results regarding typical sets which are given in Theorem 1.3.1:

$$(1-\epsilon)\,2^{n(H(Q)-\epsilon)} \;\leq\; \left|A_\epsilon^{(n)}\right| \;\leq\; 2^{n(H(Q)+\epsilon)}, \tag{III-2}$$

$$\Pr\left(\mathbf{q}_1^n \in A_\epsilon^{(n)}\right) > 1-\epsilon, \tag{III-3}$$

for any $\epsilon > 0$, for sufficiently large $n$.

Next, we propose the following construction for the attack $\mathfrak{A}_{ach,opt}^E$:

**1.** Index all $\mathbf{q}_1^n \in A_\epsilon^{(n)}$ and accordingly let $\left(\mathbf{q}_1^n\right)_k$ denote the $k$-th element where $k \in \left\{1, 2, \ldots, \left|A_\epsilon^{(n)}\right|\right\}$. Let $q_{i,k}$ denote the $i$-th element of $\left(\mathbf{q}_1^n\right)_k$ for $i \in \{1, 2, \ldots, n\}$.

**2.** At each $k$-th step of the QuBaR attack, choose $G_k = \left(i_k = 1, \theta_k = n = \frac{L}{3}, \left(\mathbf{q}_1^n\right)_k\right)$; $k \in \left\{1, 2, \ldots, \left|A_\epsilon^{(n)}\right|\right\}$.

Note that, this attack qualifies as a "QuBaR attack against ABSG" only if all of the aforementioned guesses satisfy the constraint (2.4). To see that this is satisfied for arbitrarily small $\epsilon$, we observe (noting that $\beta_k = \sum_{i=1}^{n} q_{i,k}$)

$$\left| -\frac{1}{n} \log p\left( \left( \mathbf{q}_1^n \right)_k \right) - H\left( Q \right) \right| = \left| \left( 1 + \frac{\beta_k}{\theta_k} \right) - 2 \right| \leq \epsilon, \tag{III-4}$$

where the equality follows from (2.3), the definition of $\beta_k$ and using $\theta_k = n$, the inequality follows from (III-1). Furthermore, using $\theta_k = n = L/3$, after straightforward algebra (III-4) can be shown to be equivalent to

$$L\left( 1 - \frac{\epsilon}{3} \right) \leq 2\theta_k + \beta_k \leq L\left( 1 + \frac{\epsilon}{3} \right). \tag{III-5}$$

Since we can choose $\epsilon$ arbitrarily small, the aforementioned attack qualifies as a QuBaR attack against ABSG as $\epsilon \to 0$.

Next, (III-3) implies that for large $n$ (equivalently for large $L$) $\Pr_{succ}\left( \mathfrak{A}_{ach,opt}^{E} \right) = \Pr\left( \mathbf{q}_1^n \in A_\epsilon^{(n)} \right)$ can be made arbitrarily close to 1 since we can choose $\epsilon$ arbitrarily small. Thus, $\Pr_{succ}\left( \mathfrak{A}_{ach,opt}^{E} \right) \to 1$ as $L \to \infty$ and $\epsilon \to 0$. Furthermore, for large $L$ the algorithmic complexity is at most $\left| A_\epsilon^{(n)} \right|$ which can be made arbitrarily close to $2^{2L/3}$ per (III-2) since $n = L/3$, $H\left( Q \right) = 2$ and we can choose $\epsilon$ arbitrarily small. Thus, the algorithmic complexity is at most $2^{2L/3}$ as $L \to \infty$, $\epsilon \to 0$. Recalling that for sufficiently small $\epsilon$, all elements of $A_\epsilon^{(n)}$ are equiprobable (since $\beta_k \in \mathbb{N}, \theta_k \in \mathbb{Z}^+$) with $2^{-(\theta_k + \beta_k)}\big|_{\theta_k = \beta_k = L/3}$, we immediately see that the expected algorithmic complexity is $\frac{1}{2}\left( 2^{2L/3} + 1 \right)$. Note that in the proposed attack, $i_k = 1$ and $\theta_k = n = L/3$ for all $k$ which implies that the corresponding data complexity is $L/3$. $\square$

# APPENDIX D: PROOF OF THEOREM 2.3.2

First of all, since $L$ is sufficiently large (per assumption A4), we assume w.l.o.g. $L$ is divisible by 6. Our fundamental goal is to characterize the algorithmic complexity of the optimal attacks subject to a lower bound on the success probability of the attack. Thus, we aim to analytically identify

$$\mathfrak{A}_{opt}^{E} \triangleq \arg \min_{\mathfrak{A}^{E} \in \mathcal{S}_{p}^{E}} \mathcal{C}\left(\mathfrak{A}^{E}\right), \tag{IV-1}$$

where

$$\mathcal{S}_{p}^{E} \triangleq \left\{ \mathfrak{A}^{E} \ : \ \mathfrak{A}^{E} \in \mathcal{S}^{E} \text{ and } \Pr\left( \vee_{k=1}^{\mathcal{C}\left(\mathfrak{A}^{E}\right)} \left[ \mathcal{T}\left(G_{k}\right) = 1 \right] \right) > \frac{1}{2} \right\} \subseteq \mathcal{S}^{E}, \tag{IV-2}$$

i.e., $\mathcal{S}_{p}^{E}$ is a "probabilistically-constrained" subset of $\mathcal{S}^{E}$ for which the success probability is strictly bounded away from $1/2$. In our terminology, we denote the quantity of $\Pr\left( \vee_{k=1}^{\mathcal{C}(\mathfrak{A})} \left[ \mathcal{T}\left(G_{k}\right) = 1 \right] \right)$ as the *success probability of algorithm* $\mathfrak{A}$. Our problem is to characterize

$$\mathcal{C}_{min}^{E} \triangleq \mathcal{C}\left(\mathfrak{A}_{opt}^{E}\right), \tag{IV-3}$$

in particular, we aim to achieve this goal via quantifying a lower bound on it.

Our proof approach can be summarized as follows: Since it is not a straightforward task to solve the optimization problem (IV-1), we proceed with a simpler problem. We define a set $\tilde{\mathcal{S}}_{p}^{E}$, such that $\mathcal{S}_{p}^{E} \subseteq \tilde{\mathcal{S}}_{p}^{E} \subseteq \mathcal{S}^{E}$, and accordingly proceed with minimizing $\mathcal{C}\left(\mathfrak{A}^{E}\right)$ over all $\mathfrak{A}^{E} \in \tilde{\mathcal{S}}_{p}^{E}$. The set $\tilde{\mathcal{S}}_{p}^{E}$ is defined in such a way that carrying out the aforementioned optimization problem is more tractable over this set. At the last step, we conclude the proof via deriving a lower bound on the minimum algorithmic complexity over $\tilde{\mathcal{S}}_{p}^{E}$, which also forms a lower bound on $\mathcal{C}_{min}^{E}$ since $\mathcal{S}_{p}^{E} \subseteq \tilde{\mathcal{S}}_{p}^{E}$.

We proceed with defining the set

$$\tilde{\mathcal{S}}_p^E \stackrel{\triangle}{=} \left\{ \mathfrak{A}^E \ : \ \mathfrak{A}^E \in \mathcal{S}^E \text{ and } \sum_{k=1}^{\mathcal{C}\left(\mathfrak{A}^E\right)} \Pr\left(\mathcal{T}\left(G_k\right)=1\right) > \frac{1}{2} \right\}. \tag{IV-4}$$

In our terminology, we denote the quantity of $\sum_{k=1}^{\mathcal{C}(\mathfrak{A})} \Pr\left(\mathcal{T}\left(G_k\right)=1\right)$ as the *cumulative success probability of algorithm* $\mathfrak{A}$. Note that, success probability is always upper-bounded by cumulative success probability for any algorithm $\mathfrak{A}$; i.e., we have

$$\Pr\left(\vee_{k=1}^{\mathcal{C}(\mathfrak{A})}\left[\mathcal{T}\left(G_k\right)=1\right]\right) \leq \sum_{k=1}^{\mathcal{C}(\mathfrak{A})} \Pr\left(\mathcal{T}\left(G_k\right)=1\right), \tag{IV-5}$$

due to the union bound, which implies $\mathcal{S}_p^E \subseteq \tilde{\mathcal{S}}_p^E \subseteq \mathcal{S}^E$. Next, we define the optimization problem (which is "alternate" to (IV-1))

$$\tilde{\mathfrak{A}}_{opt}^E \stackrel{\triangle}{=} \arg \min_{\mathfrak{A}^E \in \tilde{\mathcal{S}}_p^E} \mathcal{C}\left(\mathfrak{A}^E\right), \tag{IV-6}$$

and accordingly

$$\tilde{\mathcal{C}}_{min}^E \stackrel{\triangle}{=} \mathcal{C}\left(\tilde{\mathfrak{A}}_{opt}^E\right). \tag{IV-7}$$

In order to quantify the solution of (IV-6), for the sake of convenience we define

$$\mathcal{G}\left(\theta,\alpha\right) \stackrel{\triangle}{=} \left\{ \mathbf{q}_1^\theta \ : \ \forall i,\, q_i \geq 0,\, \theta \in \mathbb{Z}^+,\, \alpha \in \mathbb{N},\, \sum_{i=1}^{\theta} q_i = \beta = L - 2\theta + \alpha \right\}, \tag{IV-8}$$

for any given $\theta \in \mathbb{Z}^+$ and $\alpha \in \mathbb{N}$. Observe that $\{\mathcal{G}\left(\theta,\alpha\right)\}$ are clearly disjoint for different pairs of $\{(\theta,\alpha)\}$. Further, note that, by construction, $\mathbf{q} \in \mathcal{G}\left(\theta,\alpha\right)$ for some $\theta \in \mathbb{Z}^+$, $\alpha \in \mathbb{N}$ implies (2.4) since $2\theta + \beta = L + \alpha \geq L$; thus, any guess $G = \left(1, \theta, \mathbf{q}_1^\theta\right)$ where $\mathbf{q}_1^\theta \in \mathcal{G}\left(\theta,\alpha\right)$ for some $\theta \in \mathbb{Z}^+$, $\alpha \in \mathbb{N}$ is a valid ABSG-guess. Furthermore, any valid guess $G$ necessarily corresponds to a $\mathbf{q} \in \mathcal{G}\left(\theta,\alpha\right)$ for some unique pair $(\theta,\alpha)$.

Next, using (2.5) observe that

$$p\left(\mathbf{q}_1^\theta\right) = 2^{-(\theta+\beta)}\big|_{\beta=L-2\theta+\alpha} = 2^{-(L-\theta+\alpha)}, \tag{IV-9}$$

for any $\mathbf{q}_1^\theta \in \mathcal{G}\left(\theta,\alpha\right)$; i.e., given a pair $(\theta,\alpha)$, all elements of $\mathcal{G}\left(\theta,\alpha\right)$ are equally likely with probability $2^{-(L-\theta+\alpha)}$.

Going back to (IV-6), since we are trying to achieve a cumulative success probability strictly greater than $1/2$ using elements from *disjoint* sets $\{\mathcal{G}\left(\theta,\alpha\right)\}$, the optimal strategy is clearly to use the *sorted* elements $\mathbf{q}_1^\theta \in \mathcal{G}\left(\theta,\alpha\right)$ with respect to their success probabilities, specified in (IV-9) [16] . Thus, algorithmically the optimal solution consists of trying the guess with largest marginal success probability first, and then the most probable guess in the remaining ones, and so on.

Next, we aim to characterize the aforementioned sorting process and analyze the minimum number of elements needed to achieve a cumulative success probability strictly greater than $1/2$. Since all elements of $\mathcal{G}\left(\theta,\alpha\right)$ are equally likely (cf. (IV-9)), the problem of sorting individual sequences reduces to the problem of sorting the sets $\{\mathcal{G}\left(\theta,\alpha\right)\}$ in non-increasing order with respect to (IV-9). The total number of elements in these sorted sets of $\{\mathcal{G}\left(\theta,\alpha\right)\}$ such that the total probability exceeds $1/2$ amounts to the sought result $\tilde{\mathcal{C}}_{min}^{E}$. As a result, we should solve the following sorting problem:

**Sorting Problem I:** Sort over $(\theta,\alpha)$, with respect to the cost function $L-\theta+\alpha$, in non-decreasing order, such that

$$(\theta,\alpha) \in \mathcal{S}_{E,F} \stackrel{\triangle}{=} \left\{(\theta,\alpha) \;:\; \theta \in \mathbb{Z}^+,\; \alpha \in \mathbb{N},\; \beta = L-2\theta+\alpha \geq 0\right\}. \tag{IV-10}$$

Since this sorting needs to be done over $(\theta,\alpha)$, our next task is to characterize the feasible set $\mathcal{S}_{E,F}$ over which the sorting will be carried out.

[16] This problem is trivially equivalent to the problem of obtaining a pre-specified amount of cake with minimum number of slices, where the slice sizes are fixed, but not necessarily uniform.

First of all, notice that from the definition of $\mathcal{G}(\theta, \alpha)$ (cf. (IV-8)), we have

$$2\theta - \alpha \leq L, \tag{IV-11}$$

since $\beta = L - 2\theta + \alpha \geq 0$. Next, we define

$$B \triangleq L - \theta + \alpha, \tag{IV-12}$$

as our cost function in the aforementioned Sorting Problem I. Note that, for any $\mathbf{q} \in \mathcal{G}(\theta, \alpha)$, $\Pr(\mathbf{Q} = \mathbf{q}) = 2^{-(\theta+\beta)} = 2^{-B}$; i.e., for any guess $G(i, \theta, \mathbf{q})$, its success probability is equal to $2^{-B}$ where $B$ is computed via (IV-12) using the corresponding $\theta$ and $\alpha$. This means that, for any given guess $G(\cdot)$, its marginal success probability, $\Pr(\mathcal{T}(G) = 1)$ is directly determined by the corresponding value of $B$.

Next, our goal is to find an alternate re-parameterized expression for (IV-10) in terms of $B$ and $L$ since $B$ is our cost function in Sorting Problem I. Now, using (IV-12) in (IV-11) and noting that $\alpha \in \mathbb{N}$ yields

$$\alpha \in \{0, 1, \ldots, 2B - L\}. \tag{IV-13}$$

which also implies that $B \geq L/2$ since $\alpha \geq 0$. As a side result, this accordingly implies the following upper bound on the marginal success probability of any valid guess:

$$\Pr[\mathcal{T}(G(i, \theta, \mathbf{q})) = 1] = 2^{-B}\big|_{B=\theta+\beta} \leq 2^{-L/2}, \tag{IV-14}$$

for any $G(i, \theta, \mathbf{q}) \in \mathcal{G}(\theta, \alpha)$ and for some $\alpha \in \mathbb{N}$.

Next, per (IV-12), each value of $\alpha$ uniquely determines $\theta$ in terms of $B$ via

$$\theta = L - B + \alpha. \tag{IV-15}$$

Using (IV-15) in (IV-13), we have

$$\theta \in \{L-B, L-B+1, \ldots, B\}, \tag{IV-16}$$

which also implies that $B \leq L-1$ since $\theta \geq 1$. Combining these observations, we find out the following equivalent expression to (IV-10):

$$(\theta, \alpha) \in \mathcal{S}_{E,F} = \bigcup_{B=\frac{L}{2}}^{L-1} \{(L-B, 0), (L-B+1, 1), \ldots, (B-1, 2B-L-1), (B, 2B-L)\}, \tag{IV-17}$$

where we effectively did a re-parameterization using $B$. Note that, this re-parameterization allows us to see that, given a fixed $B$, all $\{\mathcal{G}(\theta, \alpha)\}$ such that

$$(\theta, \alpha) \in \{(L-B, 0), (L-B+1, 1), \ldots, (B-1, 2B-L-1), (B, 2B-L)\}, \tag{IV-18}$$

are equivalent to each other in terms of their success probabilities, $2^{-B}$. Using this observation and (IV-17), we conclude that Sorting Problem I is equivalent to to the following one:

**Sorting Problem II:** Sort over $(B, \alpha)$ with respect to $B$ in non-decreasing order, such that

$$(B, \alpha) \in \{(B, \alpha) \ : \ \alpha \in \{0, 1, \ldots, 2B-L\}, \ B \in \{L/2, \ldots, L-1\}\}. \tag{IV-19}$$

Note that, the corresponding values of $\theta$ in (IV-19) are given by (IV-15).

Following is one of the solutions to Sorting Problem II:

$$\{(B, \alpha)\} = \{(L/2, 0), (L/2+1, 0), (L/2+1, 1), (L/2+1, 2), \ldots, (L-1, L-2)\}. \tag{IV-20}$$

Note that all solutions to Sorting Problem II are equivalent to each other in terms of the resulting complexity. In particular, for a given $B$, we follow the strategy of varying $\alpha$ in increasing order, beginning from 0, ending in $2B - L$ as illustrated in (IV-20).

Next, we concentrate on the range of $L/2 \leq B < 2L/3$ and analyze the corresponding cumulative success probability (denoted by $P_1$) of the aforementioned strategy (cf. (IV-20)), i.e.,

$$P_1 \stackrel{\triangle}{=} \sum_{B=\frac{L}{2}}^{\frac{2L}{3}-1} \sum_{\alpha=0}^{2B-L} \Pr\left(\mathcal{G}\left(\theta,\alpha\right)|_{\theta=L-B+\alpha}\right). \tag{IV-21}$$

Next, we derive an upper bound on $P_1$ which will be used in the subsequent computations.

**Lemma IV-1** *The cumulative success probability in the range of $L/2 \leq B < 2L/3$ (i.e., $P_1$) is upper-bounded by*

$$P_1 \leq \sum_{\theta=\frac{L}{3}+1}^{\frac{2L}{3}-1} \sum_{\alpha=0}^{\theta-\frac{L}{3}-1} \Pr\left(\mathcal{G}\left(\theta,\alpha\right)\right). \tag{IV-22}$$

**Proof:** From (IV-21), we see that $P_1$ is defined in the $(B,\alpha)$ space (where $B = L - \theta + \alpha$), over the set

$$\Lambda \stackrel{\triangle}{=} \left\{(B,\alpha) \ : \ \frac{L}{2} \leq B \leq \frac{2L}{3} - 1,\, 0 \leq \alpha \leq 2B - L\right\}, \tag{IV-23}$$

i.e., $P_1 = \sum_{(B,\alpha)\in\Lambda} \Pr\left(\mathcal{G}\left(\theta,\alpha\right)\right)|_{\theta=L-B+\alpha}$. Next, we proceed with deriving a set $\tilde{\Lambda}$. The purpose of using this set is to transform the summation indexes to corresponding $(\theta,\alpha)$ for each $(B,\alpha) \in \tilde{\Lambda}$. Now we show that $\tilde{\Lambda}$ is a superset of $\Lambda$.This is done in four steps.

1. First, recall that

$$\alpha \geq 0. \tag{IV-24}$$

2. Second, observe that

$$\left[B \leq \frac{2L}{3} - 1\right] \implies \left[L - \theta + \alpha \leq \frac{2L}{3} - 1\right] \tag{IV-25}$$

$$\implies \left[\alpha \leq \theta - \frac{L}{3} - 1\right] \tag{IV-26}$$

3. Third, note that (IV-26) is equivalent to

$$\theta \geq \frac{L}{3} + \alpha + 1 \tag{IV-27}$$

Using (IV-24) in (IV-27) implies

$$\theta \geq \frac{L}{3} + 1 \tag{IV-28}$$

4. Fourth, using $B \leq \frac{2L}{3} - 1$ in $\alpha \leq 2B - L$ (cf. (IV-23)) implies

$$\alpha \leq \frac{L}{3} - 2. \tag{IV-29}$$

Also, using (IV-12) we have

$$[\alpha \leq 2B - L = L - 2\theta + 2\alpha] \implies \left[\theta \leq \frac{L}{2} + \frac{\alpha}{2}\right]. \tag{IV-30}$$

Using (IV-29) in (IV-30) yields

$$\theta \leq \frac{2L}{3} - 1. \tag{IV-31}$$

Now, defining

$$\tilde{\Lambda} \stackrel{\triangle}{=} \left\{ (B,\alpha) \ : \ \text{corresponding } (\theta,\alpha) \text{ satisfies } \frac{L}{3}+1 \leq \theta \leq \frac{2L}{3}-1,\, 0 \leq \alpha \leq \theta - \frac{L}{3} - 1 \right\}, \tag{IV-32}$$

and using (IV-24), (IV-26), (IV-28), (IV-31), we conclude that $\Lambda \subseteq \tilde{\Lambda}$, which implies (IV-22). □

Next, we proceed with providing an upper bound on the right hand side of (IV-22), which will be shown to be $\mathcal{O}\left(L^{-1}\right)$, i.e., diminishing in $L$, the length of the generator polynomial of the LFSR[17] . In order to achieve this task, we heavily use the concept of "typical set" (cf. (III-1)). Note that, using (IV-9) and $H(Q) = 2$, (III-1) can be shown to be equivalent to

$$A_{\epsilon}^{(\theta)} = \left\{ \mathbf{q}_1^{\theta} \ : \ 1-\epsilon \leq \frac{\beta}{\theta} \leq 1+\epsilon \right\}. \tag{IV-33}$$

In the following lemma, we show that all guesses $\{\mathcal{G}(\theta,\alpha)\}$ included in the summation of the right hand side of (IV-22) are necessarily "atypical" (i.e., belong to the complement of the corresponding typical set).

**Lemma IV-2** *For any $\theta \in \mathbb{Z}^+$, such that $\theta > L/3$, and for all $\alpha \in \mathbb{N}$, such that $0 \leq \alpha \leq \theta - \frac{L}{3}$, we have $\mathcal{G}(\theta,\alpha) \subseteq [A_{\epsilon}^{(\theta)}]^{(c)}$ for all $\epsilon \in \left(0, \frac{2}{\theta}\right)$, where $[A_{\epsilon}^{(\theta)}]^{(c)}$ denotes the complement of the typical set $A_{\epsilon}^{(\theta)}$.*

**Proof:** First of all, note that (cf. (IV-8)), we have

$$\left[\mathbf{q}_1^{\theta} \in \mathcal{G}(\theta,\alpha)\right] \Rightarrow \left[\frac{\beta}{\theta} = \left(\frac{L}{\theta} - 2\right) + \frac{\alpha}{\theta}\right]. \tag{IV-34}$$

[17]This result, in turn, implies that an optimal QuBaR attack which uses the solution to the Sorting Problem II for $\theta > L/3$ has a negligible cumulative success probability, i.e., negligible success probability.

Hence, for any $\mathbf{q}_1^\theta \in \mathcal{G}(\theta,\alpha)$ such that $\theta > L/3$ and $0 \le \alpha \le \theta - \frac{L}{3}$ , we have

$$\begin{aligned} -\frac{1}{\theta}\log p\left(\mathbf{q}_1^\theta\right) - H(Q) &= \frac{\theta+\beta}{\theta} - 2, && \text{(IV-35)}\\ &= \frac{L-\theta+\alpha}{\theta} - 2 = \frac{L+\alpha}{\theta} - 3, && \text{(IV-36)}\\ &\le \frac{2L}{3\theta} - 2, && \text{(IV-37)}\\ &\le \frac{2L}{L+3} - 2 = -\frac{6}{L+3} < 0, && \text{(IV-38)} \end{aligned}$$

where (IV-35) follows from the fact that $p\left(\mathbf{q}_1^\theta\right) = 2^{-(\theta+\beta)}$ and $H\left(Q\right) = 2$, (IV-36) follows using (IV-34) in (IV-35), (IV-37) follows since $\alpha \le \theta - L/3$, (IV-38) follows since $\theta \ge \frac{L}{3} + 1$. Note that (IV-38) implies

$$\left| -\frac{1}{\theta}\log p\left(\mathbf{q}_1^\theta\right) - H(Q) \right| \ge \frac{6}{L+3}. \qquad \text{(IV-39)}$$

Now, since $\theta \ge \frac{L}{3} + 1$ (equivalently $\frac{2}{\theta} \le \frac{6}{L+3}$), we have $\epsilon < \frac{6}{L+3}$ for all $\epsilon \in \left(0, \frac{2}{\theta}\right)$. Using this in (IV-39), the claim follows. □

Next, we provide an upper bound on the right hand side of (IV-22) using Lemma IV-2. For all $\epsilon_\theta \in \left(0, \frac{2}{\theta}\right)$, we have

$$\begin{aligned} \sum_{\theta=\frac{L}{3}+1}^{\frac{2L}{3}-1} \sum_{\alpha=0}^{\theta-\frac{L}{3}-1} \Pr\left(\mathcal{G}\left(\theta,\alpha\right)\right) &\le \sum_{\theta=\frac{L}{3}+1}^{\frac{2L}{3}-1} \Pr\left(\left[A_{\epsilon_\theta}^\theta\right]^{(c)}\right), && \text{(IV-40)}\\ &\le \sum_{\theta=\frac{L}{3}+1}^{\frac{2L}{3}-1} \epsilon_\theta, && \text{(IV-41)}\\ &\le \left(\frac{L}{3}-1\right)\left(\max_{\frac{L}{3}+1\le\theta\le\frac{2L}{3}-1} \epsilon_\theta\right), && \text{(IV-42)} \end{aligned}$$

where (IV-40) follows from Lemma IV-2 and the fact that, for any given $\theta$, $\{\mathcal{G}\left(\theta,\alpha\right)\}$ are disjoint by construction, (IV-41) follows from (III-3). Now, choosing $\epsilon_\theta = \frac{1}{\theta^2}$ for all

$\theta$, and using (IV-42) in (IV-22), we have

$$P_1 \leq \left(\frac{L}{3}-1\right)\left(\max_{\frac{L}{3}+1\leq\theta\leq\frac{2L}{3}-1}\frac{1}{\theta^2}\right) = \frac{L/3-1}{(L/3+1)^2} < \frac{3}{L}. \tag{IV-43}$$

Thus, for any $\delta_1 > 0$, there exists a sufficiently large $L$ (per assumption A4), where

$$P_1 < \delta_1. \tag{IV-44}$$

Note that, for the optimal strategy, which uses the ordering mentioned in (IV-20), (IV-43) and (IV-44) imply that the range of $\frac{L}{2} \leq B \leq \frac{2L}{3} - 1$ is not sufficient to achieve every given cumulative success probability strictly greater than $1/2$, since $\delta_1$ can be made arbitrarily small. Therefore, we necessarily need to include guesses with $B = 2L/3$ in the optimal structure to achieve a cumulative success probability strictly greater than $1/2$.

Next, we proceed with quantifying the contribution to the cumulative success probability for the case of $B = 2L/3$. In this case, for the optimal strategy, since $\theta = L - B + \alpha$ and $0 \leq \alpha \leq 2B - L$ for a given value of $B$, the corresponding $(\theta, \alpha)$ pairs are of the form $\left\{\left(\frac{L}{3}+\alpha, \alpha\right)\right\}_{0\leq\alpha\leq L/3}$. Thus, for the case of $B = 2L/3$, the total contribution to the cumulative success probability is given by

$$\Pr\left(\mathcal{G}(L/3, 0)\right) + \sum_{\alpha=1}^{L/3} \Pr\left(\mathcal{G}(L/3+\alpha, \alpha)\right). \tag{IV-45}$$

Note that, the right hand side of (IV-45) is "atypical" per Lemma IV-2; accordingly, we will show that the only significant contribution to the cumulative success probability is due to the left hand side of (IV-45) since it includes terms within the corresponding typical set.

Next, we provide an upper bound on the right hand side of (IV-45). Defining $P_2 \stackrel{\triangle}{=} \sum_{\alpha=1}^{L/3} \Pr\left(\mathcal{G}(L/3+\alpha,\alpha)\right)$, for all $\epsilon_\theta \in \left(0, \frac{2}{\theta}\right)$, we have

$$\begin{aligned} P_2 &= \sum_{\theta=\frac{L}{3}+1}^{2L/3} \Pr\left(\mathcal{G}(\theta,\theta-L/3)\right), && \text{(IV-46)} \\ &\leq \sum_{\theta=\frac{L}{3}+1}^{2L/3} \Pr\left(\left[A_{\epsilon_\theta}^{\theta}\right]^c\right), && \text{(IV-47)} \\ &\leq \left(\frac{L}{3}\right)\left(\max_{L/3+1\leq\theta\leq 2L/3} \epsilon_\theta\right), && \text{(IV-48)} \end{aligned}$$

where (IV-46) follows from using $\theta = (L-B+\alpha)|_{B=2L/3}$, (IV-47) follows from Lemma IV-2, (IV-48) follows using (III-3). Choosing $\epsilon_\theta = \frac{1}{\theta^2}$ for all $\theta$ in (IV-48), we have

$$P_2 \leq \frac{L/3}{(L/3+1)^2} < \frac{3}{L}. \tag{IV-49}$$

Thus, for any $\delta_2 > 0$, there exists a sufficiently large $L$ (per assumption A4), where

$$P_2 < \delta_2. \tag{IV-50}$$

Since $\delta_1$ (resp. $\delta_2$) in (IV-44) (resp. (IV-50)) can be made arbitrarily small, we necessarily need to use guesses from the set $\mathcal{G}\left(\frac{L}{3},0\right)$ in order to achieve a cumulative success probability strictly greater than $1/2$.

Next, consider the case of $(\theta,\alpha) = \left(\frac{L}{3},0\right)$: Note that, for any $\mathbf{q}_1^{L/3} \in \mathcal{G}\left(\frac{L}{3},0\right)$, we have

$$p\left(\mathbf{q}_1^{L/3}\right) = 2^{-(2L/3)}. \tag{IV-51}$$

Per (IV-33), (IV-51) implies that $\mathcal{G}\left(\frac{L}{3},0\right) \subseteq A_\epsilon^{(L/3)}$ for any $\epsilon > 0$. Furthermore, after some straightforward algebraic manipulations, it can be shown that, for $0 < \epsilon < \frac{3}{L}$, we

have $A_\epsilon^{(L/3)} \subseteq \mathcal{G}\left(\frac{L}{3}, 0\right)$; therefore we have

$$\mathcal{G}\left(\frac{L}{3}, 0\right) = A_\epsilon^{(L/3)} \text{ for } 0 < \epsilon < \frac{3}{L}. \tag{IV-52}$$

In fact, (IV-52) constitutes the fundamental crux of the converse proof. This observation implies that, using sufficiently many guesses from the set $\mathcal{G}\left(\frac{L}{3}, 0\right)$ is both necessary (since $\delta_1$ and $\delta_2$ may be arbitrarily small) and sufficient (since for $0 < \epsilon < \frac{3}{L}$, we have $\Pr\left(\mathcal{G}\left(\frac{L}{3}, 0\right)\right) = \Pr\left(A_\epsilon^{(L/3)}\right) > 1-\epsilon$) to achieve a cumulative success probability strictly greater than $1/2$ for large $L$ (per Assumption A4).

Now, let

$$P_1 + P_2 + P_3 > 1/2, \tag{IV-53}$$

denote the cumulative success probability of optimal attack in the set $\tilde{\mathcal{S}}_p^E$, where $P_3$ denotes the contribution to the cumulative success probability by the guesses from $\mathcal{G}\left(\frac{L}{3}, 0\right)$[18] . Using (IV-43) and (IV-49) in (IV-53), we have

$$P_3 > \frac{1}{2} - \frac{6}{L}. \tag{IV-54}$$

Next, let $\mathcal{C}'$ denote the number of sequences used from the set $\mathcal{G}\left(\frac{L}{3}, 0\right)$. Using (IV-51), we have

$$\mathcal{C}' = P_3/2^{-2L/3}. \tag{IV-55}$$

[18]Note that, w.l.o.g. we assume that, at step $B = 2L/3$, the proposed optimal attack uses guesses from the set $\mathcal{G}\left(\frac{L}{3}, 0\right)$ *in the end* (i.e., after applying guesses from the sets $\left\{\mathcal{G}\left(\frac{L}{3} + \alpha, \alpha\right)\right\}_{\alpha=1}^{L/3}$ of which contributions to the cumulative success probability is denoted by $P_2$). Since our strategy is to "lower-bound" the number of guesses from the set $\mathcal{G}\left(\frac{L}{3}, 0\right)$ and declare the resulting value as a lower bound on the overall complexity, $\tilde{\mathcal{C}}_{min}$, this approach maintains the validity of our result.

Combining (IV-54) and (IV-55) yields

$$\left[\mathcal{C}' > 2^{2L/3}\left(\frac{1}{2} - \frac{6}{L}\right)\right] \implies \left[\mathcal{C}\left(\tilde{\mathfrak{A}}_{opt}^{E}\right) > 2^{2L/3}\left(\frac{1}{2} - \frac{6}{L}\right)\right], \tag{IV-56}$$

since $\mathcal{C}\left(\tilde{\mathfrak{A}}_{opt}^{E}\right) > \mathcal{C}'$. Next, using $\mathcal{S}_p^E \subseteq \tilde{\mathcal{S}}_p^E$ yields

$$\mathcal{C}_{min}^{E} = \mathcal{C}\left(\mathfrak{A}_{opt}^{E}\right) \geq \tilde{\mathcal{C}}_{min}^{E} = \mathcal{C}\left(\tilde{\mathfrak{A}}_{opt}^{E}\right) > 2^{2L/3}\left(\frac{1}{2} - \frac{6}{L}\right), \tag{IV-57}$$

where $\mathfrak{A}_{opt}^{E}$ and $\tilde{\mathfrak{A}}_{opt}^{E}$ have been defined in (IV-1) and (IV-13), respectively. Hence, the claim finally follows. □

# APPENDIX E: PROOF OF THEOREM 2.3.3

For the sake of clarity, we use the notation $G_k\left(i_k=1,\theta_k,\left(\mathbf{q}_{i_k}^{\theta_k+i_k-1}\right)_k\right)$ (instead of $G_k\left(i_k=1,\theta_k,\mathbf{q}_{i_k}^{\theta_k+i_k-1}\right)$) throughout the proof in this section.

(i) First of all, note that letting $\mathfrak{A}_{opt}^{E}=\{G_k\}_{k=1}^{\mathcal{C}\left(\mathfrak{A}_{opt}^{E}\right)}$ denote the optimal exhaustive-search type QuBaR attack against ABSG with success probability $\Pr_{succ}\left(\mathfrak{A}_{opt}^{E}\right)$, the claim is equivalent to the following statement:
For any $i\neq j; i,j\in\{1,\ldots,\mathcal{C}\left(\mathfrak{A}_{opt}^{E}\right)\}$ (assuming $\theta_j>\theta_i$ w.l.o.g.), we have $\left(\mathbf{q}_1^{\theta_i}\right)_i\neq\left(\mathbf{q}_1^{\theta_i}\right)_j$. Suppose to the contrary, we have $\left(\mathbf{q}_1^{\theta_i}\right)_i=\left(\mathbf{q}_1^{\theta_i}\right)_j$ for some $i\neq j; i,j\in\{1,\ldots,\mathcal{C}\left(\mathfrak{A}_{opt}^{E}\right)\}$ where w.l.o.g. $\theta_j>\theta_i$. Given $\mathfrak{A}_{opt}^{E}$, we construct an exhaustive-search type QuBaR attack $\tilde{\mathfrak{A}}^{E}$ via eliminating $G_j$ from $\mathfrak{A}_{opt}^{E}$, i.e., $\tilde{\mathfrak{A}}^{E}\triangleq\{\tilde{G}_k\}_{k=1}^{\mathcal{C}\left(\mathfrak{A}_{opt}^{E}\right)-1}$ where $\tilde{G}_k=G_k$ for $k\in\{1,\ldots,j-1\}$ and $\tilde{G}_k=G_{k+1}$ for $k\in\{j,\ldots,\mathcal{C}\left(\mathfrak{A}_{opt}^{E}\right)-1\}$. Next, note that

$$\left[\Pr\left(\vee_{k=1}^{\mathcal{C}\left(\mathfrak{A}_{opt}^{E}\right)}\left[\mathcal{T}\left(G_k\right)=1\right]\right)=\Pr\left(\vee_{1\leq k\leq\mathcal{C}\left(\mathfrak{A}_{opt}^{E}\right),k\neq j}\left[\mathcal{T}\left(G_k\right)=1\right]\right)\right]\quad\Longleftarrow\quad\left[\left(\mathcal{T}\left(G_j\right)=1\right)\Rightarrow\left(\mathcal{T}\left(G_i\right)=1\right)\right]\tag{V-1}$$

If $G_j$ is a correct guess, then all $\left(\mathbf{q}_1^{\theta_j}\right)_j$ are correct, which implies $\left(\mathbf{q}_1^{\theta_i}\right)_j$ are necessarily correct as well since $\theta_i<\theta_j$. Further, this implies that $\left(\mathbf{q}_1^{\theta_i}\right)_i$ are correct as well per the contradiction assumption. Hence, this proves the left hand side of (V-1); thus, the right hand side of (V-1) is true as well. This, in turn, is equivalent to $\Pr_{succ}\left(\mathfrak{A}_{opt}^{E}\right)=\Pr_{succ}(\tilde{\mathfrak{A}}^{E})$ which yields the promised contradiction ($\mathcal{C}\left(\tilde{\mathfrak{A}}^{E}\right)=\mathcal{C}\left(\mathfrak{A}_{opt}^{E}\right)-1$) since $\mathfrak{A}_{opt}^{E}$ is an optimal exhaustive-search type QuBaR attack for the given success probability $\Pr_{succ}\left(\mathfrak{A}_{opt}^{E}\right)$; hence the proof the first statement of Theorem 2.3.3.

(ii) Suppose not; then this means that there exists some $i,j\in\left\{1,2,\ldots,\mathcal{C}\left(\mathfrak{A}_{opt}^{E}\right)\right\}$, $i\neq j$, such that $\Pr\left[\left(\mathcal{T}\left(G_i\right)=1\right)\cap\left(\mathcal{T}\left(G_j\right)=1\right)\right]>0$. This implies that there is some realization $\tilde{\mathbf{q}}$ of $\mathbf{Q}$ with non-zero probability such that the events of $\left(\mathcal{T}\left(G_i\right)=1\right)$ and $\left(\mathcal{T}\left(G_j\right)=1\right)$ both occur at the same time. In other words,

there exists some $\tilde{\mathbf{q}}$ with $\Pr\left(\mathbf{Q}=\tilde{\mathbf{q}}\right)>0$ such that $\left(\mathbf{q}_1^{\theta_i}\right)_i=\tilde{\mathbf{q}}_1^{\theta_i}$ and $\left(\mathbf{q}_1^{\theta_j}\right)_j=\tilde{\mathbf{q}}_1^{\theta_j}$. However, this implies that $\left(\mathbf{q}_1^{\theta_i}\right)_i$ is a prefix of $\left(\mathbf{q}_1^{\theta_j}\right)_j$ (assuming w.l.o.g. $\theta_i<\theta_j$). Hence contradiction (per the first statement of Theorem 2.3.3) and the proof of the second statement of Theorem 2.3.3.

(iii) This statement is the direct consequence of the first and second statements of the theorem.

(iv) First recall that, at optimality $\mathcal{C}\left(\mathfrak{A}_{opt}^E\right)$ is the smallest possible value (given the success probability $\Pr_{succ}\left(\mathfrak{A}_{opt}^E\right)$). This observation and (2.10) clearly imply that the optimal strategy consists of "sorted" guesses (in descending order) with respect to the probabilities $\{\Pr\left(\mathcal{T}\left(G_k\right)=1\right)\}$ of the corresponding success events $\{\left(\mathcal{T}\left(G_k\right)=1\right)\}$ since the success probability $\Pr_{succ}\left(\mathfrak{A}_{opt}^E\right)$ is fixed.

□

# APPENDIX F: PROOF OF LEMMA 3.2.1

First of all, note that

$$p\left(\mathbf{x}^n|\mathbf{u}^n\right) = \frac{p\left(\mathbf{x}^n,\mathbf{u}^n\right)}{p\left(\mathbf{u}^n\right)}, \tag{VI-1}$$

$$= \frac{\prod_{i=1}^n p(x_i)p(u_i|x_i)}{p\left(\mathbf{u}^n\right)}, \tag{VI-2}$$

where (VI-2) follows since $p\left(\mathbf{x}^n\right) = \prod_{i=1}^n p(x_i)$ and the DMC nature of $p(u|x)$.

Next, we deal with $p\left(\mathbf{u}^n\right)$:

$$p\left(\mathbf{u}^n\right) = \sum_{\mathbf{x}^n} p\left(\mathbf{x}^n\right) p\left(\mathbf{u}^n|\mathbf{x}^n\right), \tag{VI-3}$$

$$= \sum_{\mathbf{x}^n} \prod_{i=1}^n p(x_i)p(u_i|x_i), \tag{VI-4}$$

$$= \sum_{x_1} p(x_1)p(u_1|x_1) \cdot \ldots \cdot \sum_{x_n} p(x_n)p(u_n|x_n), \tag{VI-5}$$

$$= \prod_{i=1}^n \sum_{x_i} p(x_i)p(u_i|x_i), \tag{VI-6}$$

where (VI-4) follows since $p\left(\mathbf{x}^n\right) = \prod_{i=1}^n p(x_i)$ and the DMC nature of $p(u|x)$.

Using (VI-6) in (VI-2) yields:

$$p\left(\mathbf{x}^n|\mathbf{u}^n\right) = \frac{\prod_{i=1}^n p(x_i)p(u_i|x_i)}{\prod_{i=1}^n} \sum_{x_i} p(x_i)p(u_i|x_i), \tag{VI-7}$$

$$= \prod_{i=1}^n \left(\frac{p(x_i)p(u_i|x_i)}{\sum_{x_i} p(x_i)p(u_i|x_i)}\right), \tag{VI-8}$$

$$= \prod_{i=1}^n p(x_i|u_i), \tag{VI-9}$$

where (VI-9) follows using the definition of $p(x|u)$ given in the statement of the lemma. Hence the result follows. □

# APPENDIX G: PROOF OF LEMMA 3.2.2

First of all, we have

$$
\begin{aligned}
p\left(\mathbf{y}^n|\mathbf{u}^n\right) &= \frac{\sum_{\mathbf{x}^n} p\left(\mathbf{y}^n, \mathbf{u}^n, \mathbf{x}^n\right)}{p\left(\mathbf{u}^n\right)}, && \text{(VII-1)}\\
&= \frac{\sum_{\mathbf{x}^n} p\left(\mathbf{y}^n|\mathbf{x}^n, \mathbf{u}^n\right) p\left(\mathbf{x}^n|\mathbf{u}^n\right) p\left(\mathbf{u}^n\right)}{p\left(\mathbf{u}^n\right)}, && \text{(VII-2)}\\
&= \sum_{\mathbf{x}^n} p\left(\mathbf{y}^n|\mathbf{x}^n\right) p\left(\mathbf{x}^n|\mathbf{u}^n\right), && \text{(VII-3)}\\
&= \sum_{\mathbf{x}^n} \left( \prod_{i=1}^{n} p(y_i|x_i) p(x_i|u_i) \right), && \text{(VII-4)}\\
&= \sum_{x_1} p(y_1|x_1) p(x_1|u_1) \cdot \ldots \cdot \sum_{x_n} p(y_n|x_n) p(x_n|u_n), && \text{(VII-5)}\\
&= \prod_{i=1}^{n} \sum_{x_i} p(y_i|x_i) p(x_i|u_i), && \text{(VII-6)}\\
&= \prod_{i=1}^{n} \sum_{x_i} \frac{p(y_i|x_i, u_i) p(x_i|u_i) p(u_i)}{p(u_i)}, && \text{(VII-7)}\\
&= \prod_{i=1}^{n} \sum_{x_i} \frac{p(y_i, u_i, x_i)}{p(u_i)}, && \text{(VII-8)}\\
&= \prod_{i=1}^{n} p(y_i|u_i), && \text{(VII-9)}
\end{aligned}
$$

where (VII-3) follows from (3.1), (VII-4) follows from (3.3) and DMC property of communication channel,$p(y|x)$, (VII-7) follows using (3.1). (VII-9) is the desired result, hence the proof. □

# APPENDIX H: PROOF OF LEMMA 3.2.3

First, note that we have

$$\Pr(\mathcal{C}) = \prod_{i=1}^{n}\prod_{w=1}^{2^{nR}} p(x_i(w)), \tag{VIII-1}$$

$$\Pr\left(\tilde{\mathcal{C}}|\mathcal{C}\right) = \prod_{i=1}^{n}\prod_{w=1}^{2^{nR}} p(u_i(w)|x_i(w)), \tag{VIII-2}$$

where both (VIII-1) and (VIII-2) follows from the definition of encoder's and decoder's codebooks, respectively.

Combining (VIII-1) and (VIII-2) yields:

$$\Pr\left(\tilde{\mathcal{C}}\right) = \sum_{\mathcal{C}}\prod_{i=1}^{n}\prod_{w=1}^{2^{nR}} p(x_i(w))p(u_i(w)|x_i(w)), \tag{VIII-3}$$

$$= \sum_{x_1(1)} p(x_1(1))p(u_1(1)|x_1(1)) \cdot \ldots$$

$$\cdot \sum_{x_n(2^{nR})} p(x_n(2^{nR}))p(u_n(2^{nR})|x_n(2^{nR})), \tag{VIII-4}$$

$$= \prod_{w=1}^{2^{nR}}\prod_{i=1}^{n}\sum_{x_i(w)} p(x_i(w))p(u_i(w)|x_i(w)), \tag{VIII-5}$$

$$= \prod_{w=1}^{2^{nR}}\prod_{i=1}^{n} p(u_i(w)), \tag{VIII-6}$$

where $p(u_i(w)) \stackrel{\triangle}{=} \sum_{x_i(w)} p(x_i(w))p(u_i(w)|x_i(w))$ as in the statement of the theorem. Hence, (VIII-6) is the desired result, which concludes the proof. □

# REFERENCES


1. Shannon, C. E., "A Mathematical Theory of Communication," *Bell Syst. Tech. J.*, vol. 27, pp. 379–423, 623–656, 1948.

2. Cover, T. M. and J. A. Thomas, *Elements of Information Theory*, 2nd Edition, New York: Wiley, 2006.

3. Nyquist, H., "Certain factors affecting telegraph speed," *Bell Syst. Tech. J.*, vol. 3, pp. 324-352, Apr. 1924.

4. Hartley, R. V. L., "Transmission of Information," *Bell Syst. Tech. J.*, vol. 7, pp. 535, July 1928.

5. Wiener, N., *Extrapolation, Interpolation and Smoothing of Stationary Time Series*, New York: Wiley, 1949.

6. McMillan, B., "The basic theorems of information theory," *Ann. Math. Statist.*, vol. 24, pp. 196-219, June 1953.

7. Breiman, L., "The individual ergodic theorems of information theory," *Ann. Math. Statist.*, vol. 28, pp. 809-811, 1957.

8. Verdu, S., "Fifty Years of Shannon Theory", *IEEE Trans. Inf. Theory*, vol. IT–44, no. 6, Oct 1998.

9. Ahslwede, R., "Multi-way communication channels," in Proc. 2nd Int. Symp. Inform. Theory (Tsahkadsor, Armenian S.S.R.), pp. 23–52, 1971. (Publishing House of the Hungarian Academy of Sciences, 1973.)

10. Van der Meulen, E. C., "A survey of multi-way channels in information theory: 1961-1976," *IEEE Trans. Inf. Theory*, vol. IT-23, no. 2, Jan. 1977.

11. El Gamal, A. and T. M. Cover, "Multiple user information theory," in *Proc. IEEE,* vol. 68, pp. 1466–1483, Dec. 1980.

12. Hellman, M., "A cryptanalytic time-memory trade-off," *IEEE Trans. Inf. Theory,* vol. IT–26, no. 4, pp. 401–406, Jul. 1980.

13. Biryukov, A. and A. Shamir, "Cryptanalytic time/memory/data tradeoffs for stream ciphers," *Asiacrypt 2000*, Lecture Notes in Computer Science, Berlin: Springer-Verlag, 2000, vol. 1976, pp. 1–13.

14. Siegenthaler, T., "Decrypting a Class of Stream Ciphers Using Ciphertext Only", *IEEE Trans. Comput.*, vol. 34, no. 1, pp. 81–85, Jan. 1985.

15. Meier, W. and O. Staffelbach, "Fast Correlation Attacks on Certain Stream Ciphers", *Journal of Cryptology*, vol. 1, pp. 159–176, 1989.

16. Courtois, N. and W. Meier, "Algebraic Attacks on Stream Ciphers with Linear Feedback", *Advances in Cryptology– EUROCRYPT 2003,* Lecture Notes in Computer Science, Berlin: Springer-Verlag, 2003, vol. 2656, pp. 345–359.

17. Courtois, N., "Fast Algebraic Attacks on Stream Ciphers with Linear Feedback", *Advances in Cryptology– CRYPTO 2003,* Lecture Notes in Computer Science, Berlin: Springer-Verlag, 2003, vol. 2729, pp. 177–194, 2003.

18. Gouget, A., H. Sibert, C. Berbain, N. Courtois, B. Debraize and C. Mitchell, "Analysis of the Bit-Search Generator and Sequence Compression Techniques" in *Fast Software Encryption–FSE 2005,* Lecture Notes in Computer Science, Berlin: Springer-Verlag, 2005, vol. 3557, pp. 196–214.

19. Golomb, S. W., *Shift Register Sequences*, Revised Edition, Aegean Park Press, 1982.

20. Gouget, A. and H. Sibert, "The Bit-Search Generator" in *The State of the Art of Stream Ciphers: Workshop Record, Brugge, Belgium, October 2004*, pp. 60–68, 2004.

21. Coppersmith, D., H. Krawczyk and Y. Mansour, "The Shrinking Generator" in *Advances in Cryptology–CRYPTO'93,* Lecture Notes in Computer Science, Berlin: Springer-Verlag, 1993, vol. 773, pp. 22–39.

22. Meier, W. and O. Staffelbach, "The Self-Shrinking Generator" in *Advances in Cryptology– EUROCRYPT'94,* Lecture Notes in Computer Science, Berlin: Springer-Verlag, 1994, vol. 905, pp. 205–214.

23. Mihaljevic, M., "A Faster Cryptanalysis of the Self-Shrinking Generator" in *First Australasian Conference on Information Security and Privacy ACISP'96,* Lecture Notes in Computer Science, Berlin: Springer-Verlag, 1996, vol. 1172, pp. 182–189.

24. Zenner, E., M. Krause, and S. Lucks, "Improved Cryptanalysis of the Self-Shrinking Generator" in *Australasian Conference on Information Security and Privacy ACISP'01,* Lecture Notes in Computer Science, Berlin: Springer-Verlag, 2001, vol. 2119, pp. 21–35.

25. Hell, M. and T. Johansson, "Two New Attacks on the Self-Shrinking Generator," *IEEE Trans. Inf. Theory,* vol. IT–52, no. 8, pp. 3837–3843, Aug. 2006.

26. Gouget, A. and H. Sibert, "How to Strengthen Pseudo-random Generators by Using Compression," in *Advances in Cryptology–EUROCRYPT 2006,* Lecture Notes in Computer Science, Berlin: Springer-Verlag, 2006, vol. 4004, pp. 129–146.

27. Altuğ, Y., N. P. Ayerden, M. K. Mıhçak and E. Anarım, "A Note on the Periodicity and the Output Rate of Bit Search Type Generators," *IEEE Trans. Inf. Theory,* vol. IT–54, no. 2, pp. 666–679, Feb. 2008.

28. Altuğ, Y. and M. K. Mıhçak, "Towards Exploring Fundamental Limits of System-Specific Cryptanalysis Within Limited Attack Classes: Application to ABSG," submitted to *IEEE Trans. Inf. Theory.*

29. Shannon, C. E., "Channels with Side Information at the Transmitter," *IBM J. Res. Dev.*, pp. 289–293, 1958.

30. Wyner, A. D., "On Source Coding with Side Information at the Decoder," *IEEE Trans. Inf. Theory,* vol. IT–21, no. 3, pp. 294–300, 1975.

31. Wyner, A. D. and J. Ziv, "The Rate Distortion Function for Source Coding with Side Information at the Receiver," *IEEE Trans. Inf. Theory,* vol. IT–22, no. 1, pp. 1–11, 1976.

32. Costa, M. H. M., "Writing on the Dirty Paper," *IEEE Trans. Inf. Theory,* vol. IT-29, no. 3, pp. 439–441, 1983.

33. Venkatesan, R., S. M. Koon, M. H. Jakubowski, P. Moulin, "Robust image hashing", in *Proc. IEEE Int. Conf. Image Processing, vol. 3,* pp. 664-666, 2000.

34. Cox, I. J., M. L. Miller and A. L. McKellips, "Watermarking as communications with side information", *Proc. IEEE*, vol. 87, No. 7, pp. 1127–1141, July 1999.

35. Petitcolas, F. A. P., R. J. Anderson and M. G. Kuhn, "Information hiding-a survey", *Proc. IEEE*, vol. 87, No. 7, pp. 1062–1078, July 1999.

36. Moulin, P. and R. Koetter, "Data-Hiding Codes," (tutorial paper), *Proc. IEEE*, Vol. 93, No. 12, pp. 2083–2127, Dec. 2005.

37. Mihcak, M. K. and R. Venkatesan, "A Perceptual Audio Hashing Algorithm: A Tool For Robust Audio Identification and Information Hiding," in *Proceedings of 4th International Information Hiding Workshop*, 2001.

38. Kozat, S. S., R. Venkatesan and M. K. Mihcak, "Robust Hashing via Matrix Invariances," in *Proceedings of IEEE International Conference on Image Processing (ICIP)*, 2004.

39. Mıhçak, M. K., Y. Altuğ and N. P. Ayerden, "On Minimax Optimal Linear Transforms for Detection with Side Information in Gaussian Setup", *IEEE Communications Letters,* vol. 12, no. 3, Mar. 2008.

40. Eggers, J., J. Su and B. Girod, "Public keywatermarking by eigenvectors of linear transforms,' in *Proc. Eur. Signal Process. Conf.* Tampere, Finland, Sept. 2000.

41. Kirovski, D., H. S. Malvar and Y. Yacobi, "A Dual Watermarking and Fingerprinting System," *IEEE Multimedia,* vol. 11, no. 3, pp. 59–73, Mar. 2004.

42. Moulin, P. and J. A. O'Sullivan, "Information–Theoretic Analysis of Information Hiding,"*IEEE Trans. Inf. Theory,* vol. IT–49, no. 3, pp. 563–593.

43. Somekh–Baruch, A. and N. Merhav, "On the capacity game of public watermarking systems," *IEEE Trans. Inf. Theory,* vol. IT–50, no. 3, pp. 511–524, Mar. 2004.

44. Goldreich, O., *Foundations of Cryptography, Volume 1*, Cambridge University Press, 2001.