Beyond the Csiszár-Körner Bound: Best-Possible Wiretap Coding via Obfuscation

Yuval Ishai* Alexis Korb† Paul Lou‡ Amit Sahai§

March 2022

Abstract

A *wiretap coding scheme* (Wyner, Bell Syst. Tech. J. 1975) enables Alice to reliably communicate a message m to an honest Bob by sending an encoding c over a noisy channel ChB, while at the same time hiding m from Eve who receives c over another noisy channel ChE.

Wiretap coding is clearly impossible when ChB is a *degraded* version of ChE, in the sense that the output of ChB can be simulated using only the output of ChE. A classic work of Csiszár and Korner (IEEE Trans. Inf. Theory, 1978) shows that the converse does not hold. This follows from their full characterization of the channel pairs $(\mathsf{ChB}, \mathsf{ChE})$ that enable information-theoretic wiretap coding.

In this work, we show that in fact the converse *does* hold when considering *computational security*; that is, wiretap coding against a computationally bounded Eve is possible *if and only if* ChB is not a degraded version of ChE. Our construction assumes the existence of virtual black-box (VBB) obfuscation of specific classes of "evasive" functions that generalize fuzzy point functions, and can be heuristically instantiated using indistinguishability obfuscation. Finally, our solution has the appealing feature of being *universal* in the sense that Alice's algorithm depends only on ChB and not on ChE.

*Technion. Email: yuvali@cs.technion.ac.il

†UCLA. Email: alexiskorb@cs.ucla.edu.

‡UCLA. Email: pslou@cs.ucla.edu.

§UCLA. Email: sahai@cs.ucla.edu.

Contents

1 Introduction **1**
- 1.1 Our Contributions . . . 2
- 1.2 Related Works . . . 4

2 Technical Overview **4**

3 Preliminaries **10**
- 3.1 Channel Definitions . . . 11

4 Wiretap Channels **13**
- 4.1 Wiretap Channel Definitions . . . 13
- 4.2 Ideal Obfuscation Model . . . 14
- 4.3 Wiretap Feasibility in the Information Theoretic Setting . . . 15
- 4.4 Rate and General Message Spaces . . . 18

5 Constructing Bounded Query Secure Wiretap Coding Schemes in the Ideal Obfuscation Model **18**
- 5.1 Construction . . . 18
- 5.2 Correctness . . . 20
- 5.3 Security . . . 21

6 Universal Coding Schemes **33**
- 6.1 Our Construction is a Universal Coding Scheme in the Ideal Oracle Model . . . 33
- 6.2 Universal Coding Schemes in the Information Theoretic Setting . . . 34

7 Instantiating the Oracle via Obfuscation **34**
- 7.1 Obfuscation Definitions . . . 34
- 7.2 Fuzzy Point Function Obfuscation for the BSC-BEC Case . . . 36
- 7.3 Generalized Fuzzy Point Function Obfuscation . . . 39
- 7.4 Construction from $i\mathcal{O}$ . . . 42

8 Acknowledgments **44**

9 References **45**

A [CK78] and [MW00] Definitions **46**
- A.1 [CK78] Definitions . . . 47
- A.2 [MW00] Definitions . . . 47

B Main Theorem Additional Proofs **48**

C Proof of Theorem 4.17 **51**
- C.1 Background Information . . . 52
- C.2 Proof . . . 55

1 Introduction

The wiretap channel, first introduced by Wyner [Wyn75], captures a unidirectional communication setting in which Alice transmits an encoding of a message across two discrete memoryless channels: a main channel (Bob's channel) for the intended receiver Bob and an eavesdropping channel (Eve's channel) for an adversarial receiver Eve. Two conditions are desired: correctness and security. Informally, correctness guarantees that Bob can decode the message with overwhelming probability, and security requires that Eve learn essentially nothing about the message. The wiretap coding problem is then to find a (randomized) encoding algorithm that satisfies both conditions. The wiretap coding question represents a basic and fundamental question regarding secure transmission over noisy channels, and indeed Wyner's work has been incredibly influential: Google Scholar reports that the literature citing [Wyn75] surpasses 7000 papers, and Wyner's work is considered *the* foundational work on using noisy channels for cryptography. Much of the interest in this question comes from its relevance to physical layer security, a large area of research that exploits physical properties of communication channels to enhance communication security through coding and signal processing. See, e.g., [PS17] for a survey.

The classic work of Csiszár and Korner [CK78] completely characterized the pairs of channels for which wiretap coding is possible information theoretically. Roughly speaking, their work defined a notion of one channel being *less noisy* than the other, and they proved that wiretap coding is possible information theoretically if and only if Eve's channel is *not* less noisy than Bob's channel.

To illustrate this, let's consider a specific case: suppose that Bob's channel is a binary symmetric channel, flipping each bit that Alice sends with probability $p = 0.1$; at the same time, suppose Eve's channel is a binary erasure channel, erasing each bit that Alice sends (i.e., replacing it with $\perp$) with probability ϵ. Then, it turns out [Nai10] that Bob's channel is less noisy than Eve's channel if and only if $\epsilon > 0.36 = 4p(1-p)$, and thus by [CK78], information-theoretic wiretap coding is only possible under this condition.

A new feasibility result for wiretap coding. In cryptography, we often take for granted that assuming adversaries to be computationally bounded should lead to improved feasibility results. Indeed, we have seen this many times especially in the early history of cryptography: from re-usable secret keys for encryption [BM84, Yao82] to the feasibility of secure multi-party computation with a dishonest majority [GMW87]. However, despite the popularity of Wyner's work, no improvement over [CK78] in terms of feasibility against computationally bounded adversaries has been obtained in *over 40 years*.

Nevertheless, in this work, we ask: is it possible to obtain new feasibility results for wiretap coding for computationally bounded eavesdroppers?

Taking a fresh look at this scenario, we observe that if $\epsilon \leq 0.2 = 2p$, then wiretap coding is completely impossible: If $\epsilon \leq 0.2 = 2p$, then Eve can simulate Bob's channel. For example, if $\epsilon = 0.2 = 2p$, then Eve can assign each $\perp$ that Eve receives uniformly to $\{0, 1\}$, and this would exactly yield a binary symmetric channel with flip probability $p = 0.1$, thus exactly simulating the distribution received by Bob. Since wiretap coding is non-interactive, if Bob can recover the message with high probability, then so can Eve, violating security. Indeed, whenever Eve can efficiently simulate Bob's channel, we say that Bob's channel is a *degraded* version of Eve's channel. When this is true, wiretap coding is clearly impossible, even for efficient eavesdroppers Eve.

In our main result, we show that assuming secure program obfuscation for simple specific classes of functionalities (as we describe in more detail below), the above limitation presents the *only* obstacle to feasibility of wiretap coding against computationally bounded eavesdroppers. In particular, for the scenario described above, we show that wiretap coding is possible whenever

$\epsilon > 0.2 = 2p$, even though [CK78, Nai10] showed that information-theoretic wiretap coding is impossible for $\epsilon < 0.36 = 4p(1-p)$. More generally, we show that wiretap coding is possible whenever Bob's channel is *not* a degraded version of Eve's channel. We now describe our results in more detail.

1.1 Our Contributions

Let ChB represent Bob's channel, and let ChE represent Eve's channel. Observe that the input alphabets for the channels ChB and ChE must be identical; we will denote this input alphabet by $\mathcal{X}$, and consider 1-bit messages for simplicity[1].

We first consider an oracle-based model in which a wiretap coding scheme consists of two algorithms:

- $\mathrm{Enc}(1^\lambda, m)$: The (randomized) encoder takes as input a security parameter λ and a message bit $m \in \{0,1\}$. The output of Enc consists of: (1) a string $c \in \mathcal{X}^*$, and (2) a circuit describing a function f. The string c is transmitted over channels ChB and ChE to Bob and Eve respectively. However, both Bob and Eve are granted oracle access to f.
- $\mathrm{Dec}^f(y)$: The deterministic decoder is a polynomial-time oracle algorithm with oracle access to f. Dec^f takes as input the string y received by Bob over his channel.

We obtain our main result in two steps. In our first and primary step, we prove:

Theorem 1.1 (Informal)**.** *For any pair of discrete memoryless channels* $(\mathsf{ChB}, \mathsf{ChE})$ *where* ChB *is not a degraded version of* ChE*, there exist PPT encoding and decoding algorithms* $(\mathrm{Enc}, \mathrm{Dec}^{(\cdot)})$ *which achieve:*

- ***Correctness****: For all messages* $m \in \{0,1\}$*,*
$$\Pr[\mathrm{Dec}^f(1^\lambda, \mathsf{ChB}(c)) = m \mid (f,c) \leftarrow \mathrm{Enc}(1^\lambda, m)] \geq 1 - \mathsf{negl}(\lambda)$$
- ***Security****: For all computationally unbounded adversaries* $\mathcal{A}^{(\cdot)}$ *that are allowed to make polynomially many queries to their oracle,*
$$\Pr[\mathcal{A}^{f_b}(1^\lambda, \mathsf{ChE}(c_b)) = b \mid (f_b, c_b) \leftarrow \mathrm{Enc}(1^\lambda, b)] \leq \frac{1}{2} + \mathsf{negl}(\lambda)$$
where b *is uniformly distributed over* $\{0,1\}$*.*

Theorem 1.1 can be viewed as an unconditional construction using an *ideal obfuscation* of the oracle f. Our use of obfuscation in this context was inspired by the recent work of Agrawal et al. [AIK+21], which used ideal obfuscation to obtain a new feasibility result for secure computation using unidirectional communication over noisy channels (see Section 1.2 for comparison and more related work).

In our second step, we show how to bootstrap from Theorem 1.1 to obtain wiretap coding in the plain model secure against computationally bounded adversaries, via a suitable form of cryptographic program obfuscation. More concretely, we use the notion of virtual black-box (VBB) obfuscation for *evasive circuits* [BBC+14], for a specific class of evasive circuits that we call generalized fuzzy point functions, and with a very simple kind of auxiliary information that corresponds to the message that Eve receives when Alice transmits a uniformly random message (see Section 7 for details). Using this kind of obfuscation, we obtain the following result in the plain model:

[1] In the computational setting, any wiretap coding scheme for 1-bit messages can be bootstrapped into one that encodes long messages with rate achieving the capacity of ChB via the use of a standard hybrid encryption technique. (See the full version or the supplementary material.)

Theorem 1.2 (Informal)**.** *Assume that $\mathcal{O}$ is a secure evasive function obfuscation scheme for the class of generalized fuzzy point functions. Then, for any pair of discrete memoryless channels* $(\mathsf{ChB}, \mathsf{ChE})$ *where* ChB *is not a degraded version of* ChE*, there exist PPT encoding and decoding algorithms* $(\mathrm{Enc}, \mathrm{Dec})$ *which achieve:*

- ***Correctness****: For all messages $m \in \{0,1\}$,*

$$\Pr[\mathrm{Dec}(1^\lambda, \mathcal{O}(f), \mathsf{ChB}(c)) = m \mid (f, c) \leftarrow \mathrm{Enc}(1^\lambda, m)] \geq 1 - \mathsf{negl}(\lambda)$$

- ***Security****: For all computationally bounded adversaries $\mathcal{A}$,*

$$\Pr[\mathcal{A}(1^\lambda, \mathcal{O}(f_b), \mathsf{ChE}(c_b)) = b \mid (f_b, c_b) \leftarrow \mathrm{Enc}(1^\lambda, b)] \leq \frac{1}{2} + \mathsf{negl}(\lambda)$$

where b is uniformly distributed over $\{0,1\}$.

Note that since $\mathcal{O}(f)$ can be made public to both Bob and Eve, it can be communicated by using a standard encoding scheme for ChB, with no security requirements.

On instantiating obfuscation. We conjecture that indistinguishability obfuscation (iO) provides a secure realization of the obfuscation needed in our wiretap coding scheme. The recent work of [JLS21] provides a construction of iO from well-studied hardness assumptions, and thus gives a conservative and explicit candidate realization. We provide several arguments in favor of our conjecture (see Section 7 for details regarding all the points below):

- First, we stress that VBB obfuscation for *evasive* circuit families is not known to be subject to any impossibility results, under any hardness assumptions, even wildly speculative ones. This is because the notion of evasiveness that we consider is *statistical* in the following sense: even a computationally unbounded Eve, that can make any polynomially bounded number of queries to our oracle, cannot find an input z to the oracle f such that $f(z) = 1$. This property rules out all known techniques for proving impossibility of obfuscation that we are aware of (c.f. [BGI+01, GK05]). But in fact, our situation is even further away from impossibility results because we obfuscate simple distributions of evasive functions that generalize random fuzzy point functions, and only need to leak a simple auxiliary information about the obfuscated function.
- Furthermore, in fact, the work of [BMSZ16] gives a construction of VBB obfuscation for evasive circuits from multilinear maps, which is designed to be immune to all known attacks on multilinear map candidates, and has never been successfully attacked.
- Finally, indistinguishability obfuscation is a "best-possible obfuscation" [GR07], and therefore, roughly speaking, if *any* way exists to securely realize the ideal oracle in our construction to achieve wiretap coding, then using iO must also yield secure wiretap coding.

Optimal-rate wiretap coding. We stress that the problem of achieving asymptotically optimal *rate* follows almost immediately from our solution to the feasibility question above. This is because the feasibility solution can be used to transmit a secret key, and then the encrypted message can be transmitted using any reliable coding scheme to Bob. The security of encryption will ensure that even if Eve learns the ciphertext, because she is guaranteed not to learn the encryption key due to our solution to the feasibility problem above, the (computationally bounded) Eve cannot learn anything about the message. Using standard Rate 1 symmetric key encryption, therefore, we achieve asymptotic wiretap coding rate equal to the capacity of Bob's channel, regardless of the quality of Eve's channel.

Universal wiretap coding. An appealing feature of our solution to the wiretap problem is that it gives a *universal* encoding, meaning that (Enc, Dec) depend only on the main channel ChB and not on the eavesdropper's channel ChE. This is not possible in the information-theoretic regime.

1.2 Related Works

Our work was inspired by the recent work of Agrawal et al. [AIK$^+$21], who proposed a similar obfuscation-based approach for establishing a feasibility result for secure *computation* over unidirectional noisy channels. In contrast to our work, the use of ideal obfuscation in [AIK$^+$21] applies to more complex functions that are not even "evasive" in the standard sense. We stress that beyond inspiration and a common use of obfuscation, there is no other technical overlap between [AIK$^+$21] and our work.

Another closely related line of work studies the notion of fuzzy extractors, introduced by Dodis et al. [DORS08]. A fuzzy extractor can be used to encode a message m in a way that: (1) any message m' which is "close" to m (with respect to some metric) can be used to decode m, and (2) if m has sufficiently high min-entropy, its encoding hides m. The possibility of constructing strong forms of computational fuzzy extractors from strong forms of fuzzy point function obfuscation was discussed by Canetti et al. [CFP$^+$21] and Fuller et al. [FMR20]. The wiretap coding problem can be loosely cast as a variant of fuzzy extractors where the metric is induced by the main channel ChB and security should hold with respect to a specific entropic source defined by the eavesdropper's channel ChE. The latter relaxation makes the notion of obfuscation we need qualitatively weaker.

Various extensions to the wiretap setting have been studied in the information theoretic setting, and we discuss a very limited subset here that relate most closely to our work. Further generalizations were made by Liang et al's [LKP09] introduction of the compound wiretap channel, in which there are finitely many honest receiver and finitely many eavesdroppers, modeling a transmitter's uncertainty about the receiver's channel and the eavesdropper's channel. The upper and lower bounds on secrecy capacity of the compound wiretap channel suggest the impossibility of positive rate universal encodings. Maurer [Mau93] showed that a public channel and *interaction* between the transmitter and honest receiver circumvent the necessity of ChE being not less noisy than ChB for security. We stress that the focus of our paper is the non-interactive case, without any feedback channels. Nair [Nai10] studied information-theoretic relationships between BSC and BEC channels.

Bellare et al. [BTV12] introduced stronger security notions for wiretap coding than the notions that existed within the information theoretic community. In particular, they introduced an information theoretic notion of semantic security, which we also achieve in our work. They also provided an efficient information-theoretic encoding and decoding scheme for many channels that achieves correctness, semantic security, and rate achieving the Csiszár-Korner bound. Previously, most works on wiretap coding had only proven the existence of wiretap encoding and decoding schemes, and not provided explicit constructions.

2 Technical Overview

In the wiretap setting, we consider two discrete memoryless channels (DMCs): $\mathsf{ChB} : \mathcal{X} \to \mathcal{Y}$ from Alice to the intended receiver Bob, and $\mathsf{ChE} : \mathcal{X} \to \mathcal{Z}$ from Alice to an eavesdropper Eve. Alice's goal is to transmit an encoding of a message $m \in \mathcal{M} = \{0, 1\}$ across both channels so that Bob can decode m with high probability and Eve learns negligible information about m. Our goal is to build an encoder and a decoder that satisfies these requirements.

Definition 2.1 (Discrete Memoryless Channel (DMC))**.** *We define a discrete memoryless channel*

(DMC) $\mathsf{ChW} : \mathcal{X} \to \mathcal{Y}$ *to be a randomized function from input alphabet* $\mathcal{X}$ *to output alphabet* $\mathcal{Y}$*. We associate* ChW *with its stochastic matrix* $P_W = [p_W(y|x)]_{x\in\mathcal{X},y\in\mathcal{Y}}$*.*

Warmup: The $\mathsf{BSC}_{0.1}$-$\mathsf{BEC}_{0.3}$ Wiretap Setting. We first consider a simple example. Consider a wiretap setting in which Alice has a $\mathsf{BSC}_{0.1}$ between her and Bob and a $\mathsf{BEC}_{0.3}$ between her and Eve. Alice wishes to send $m \in \{0,1\}$ to Bob, but not to Eve. First observe that on a uniform random input distribution, Eve's information about the input is greater than Bob's information. Indeed, Eve's $\mathsf{BEC}_{0.3}$ channel has greater capacity than Bob's $\mathsf{BSC}_{0.1}$ channel. In fact, it can be proven [CK78, Nai10] that in the information theoretic setting with these channel parameters, then there does not exist any encoding scheme that Alice can use to encode her message so that Bob can decode with high probability but Eve cannot.

Acknowledging this obstacle, how can we favor Bob's decoding probability and disadvantage Eve in the computational setting? A simple observation is that on a uniform random input $r \in \{0,1\}^n$ to the channels, then Bob's output distribution is different from Eve's output distribution. Indeed, for large enough n, Bob's $\mathsf{BSC}_{0.1}$'s output r_B should contain approximately 10% bit flips relative to r, whereas Eve's $\mathsf{BEC}_{0.3}$ output r_E should contain approximately 30% erasures.

Now, suppose Bob and Eve both had access to an oracle that outputs m on binary inputs containing approximately 10% bit flips relative to r and outputs $\perp$ on all other inputs. Then, Bob can decode m by simply sending his received output r_B to the oracle. However, in order to learn m, Eve must be able to guess a $\widehat{r}_B$ that has 10% bit flips relative to r. It is simple to observe that Eve's best strategy for guessing such an $\widehat{r}_B$ is to generate it from her channel output r_E by replacing each erasure in r_E with a uniformly random bit. But observe that with high probability this $\widehat{r}_B$ will contain roughly 15% bit flips relatives to r. Thus, with high probability, Eve cannot generate a $\widehat{r}_B$ with only 10% bit flips, so she cannot learn m.

This motivates our use of the ideal obfuscation model in which Alice, in addition to specifying a string r to send across both channels can also specify an oracle f which is perfectly transmitted to Bob and Eve who get bounded access to the oracle. In this model, we can achieve secure wiretap coding schemes. To encode $m \in \{0,1\}$, Alice picks a random string r that will be sent across both channels and specifies the oracle mentioned above which is perfectly transmitted to Bob and Eve. By the above argument, this encoding satisfies both correctness and security.

Handling all Non-Degraded Channels. Now, consider the case where Bob's channel $\mathsf{ChB} : \mathcal{X} \to \mathcal{Y}$ and Eve's channel $\mathsf{ChE} : \mathcal{X} \to \mathcal{Z}$ are arbitrary channels with the same input domain $\mathcal{X}$ with the sole restriction that ChB is not a degradation of ChE. We first build intuition about channel degradation.

Definition 2.2 (Channel Degradation)**.** *We say that channel* ChB *is a degradation of channel* ChE *if there exists a channel* ChS *such that*

$$\mathsf{ChB} = \mathsf{ChS} \circ \mathsf{ChE}$$

where $\circ$ *denotes channel concatenation, that is* $(\mathsf{ChS} \circ \mathsf{ChE})(x) = \mathsf{ChS}(\mathsf{ChE}(x))$*.*

Observe that if ChB is a degradation of ChE, then secure wiretap coding schemes are impossible even in the computational setting since then there exists a ChS such that $\mathsf{ChB} = \mathsf{ChS} \circ \mathsf{ChE}$, which means Eve can simulate Bob's output by running her channel output through ChS and learn everything that Bob learns.

On the other hand, if ChB is not a degradation of ChE, then this means that for every channel ChS, there exists an $x^* \in \mathcal{X}$ and $y^* \in \mathcal{Y}$ such that

$$|p_B(y^* \mid x^*) - p_{E \cdot S}(y^* \mid x^*)| > 0$$

where $p_B(y^* \mid x^*) = \Pr[\mathsf{ChB}(x^*) = y^*]$ and $p_{E \cdot S}(y^* \mid x^*) = \Pr[\mathsf{ChS}(\mathsf{ChE}(x^*)) = y^*]$. In fact, by using properties of continuity and compactness, we can prove that there is a constant $d > 0$ such that for every ChS, there exists an $x^* \in \mathcal{X}$ and $y^* \in \mathcal{Y}$ such that

$$|p_B(y^* \mid x^*) - p_{E \cdot S}(y^* \mid x^*)| \geq d$$

Now, define the following notation.

Definition 2.3. *Let $\mathcal{X}$ and $\mathcal{Y}$ be any two discrete finite sets and $n \in \mathbb{N}$. For $r \in \mathcal{X}^n$ and $s \in \mathcal{Y}^n$ and for any $x \in \mathcal{X}$ and $y \in \mathcal{Y}$, we define the fraction of x's in r that are y's in s to be*

$$\textsc{Ratio}_{x \to y}(r, s) = \frac{|i \in [n] : r_i = x, s_i = y|}{|i \in [n] : r_i = x|}.$$

If $|i \in [n] : r_i = x| = 0$, then we define $\textsc{Ratio}_{x \to y}(r, s) = 0$.

Fix any $\mathsf{ChS} : \mathcal{Z} \to \mathcal{Y}$ and let x^* and y^* be defined as above. Consider sending a uniform random string $r \in \mathcal{X}^n$ through ChB and $\mathsf{ChS} \circ \mathsf{ChE}$. By a Chernoff bound, we expect that with high probability, $\textsc{Ratio}_{x^* \to y^*}(r, \mathsf{ChB}(r))$ should be close to $p_B(y^* \mid x^*)$ and $\textsc{Ratio}_{x^* \to y^*}(r, \mathsf{ChS}(\mathsf{ChE}(r)))$ should be close to $p_{E \cdot S}(y^* \mid x^*)$. But since $p_{E \cdot S}(y^* \mid x^*)$ and $p_B(y^* \mid x^*)$ differ by a constant, we expect $\textsc{Ratio}_{x^* \to y^*}(r, \mathsf{ChS}(\mathsf{ChE}(r)))$ to differ by a constant from $p_B(y^* \mid x^*)$ with high probability.

Thus, $\textsc{Ratio}_{x^* \to y^*}$ forms a distinguisher between ChB and $\mathsf{ChS} \circ \mathsf{ChE}$. Therefore, we can define the following function which outputs m with high probability on an input sampled from $\mathsf{ChB}(r)$ and outputs m with negligible probability on an input sampled from $\mathsf{ChS}(\mathsf{ChE}(r))$ for any channel ChS.[2]

$h_{m,r,\mathsf{ChB},n}(r_B)$:

If for all $x \in \mathcal{X}$ and $y \in \mathcal{Y}$, $|\textsc{Ratio}_{x \to y}(r, r_B) - p_B(y \mid x)| \leq n^{-\frac{1}{3}}$, output m.

Else, output $\perp$.

In fact, since we are considering the ratios of all pairs $(x, y) \in \mathcal{X} \times \mathcal{Y}$, the same observation holds for the following function.

$f_{m,r,\mathsf{ChB},n}(r_B)$:

If for all $x \in \mathcal{X}$ and $y \in \mathcal{Y}$, $\textsc{Ratio}_{x \to y}(r, r_B) \leq p_B(y \mid x) + n^{-\frac{1}{3}}$, output m.

Else, output $\perp$.

Construction Overview. We now describe our coding scheme for wiretap channel $(\mathsf{ChB}, \mathsf{ChE})$. Our encoder $\mathrm{Enc}_{\mathsf{ChB}}$ takes a security parameter 1^λ and a message $m \in \mathcal{M}$ and outputs a description of a circuit computing some function f and a string $r \in \mathcal{X}^n$. Our decoder $\mathrm{Dec}^{(\cdot)}$ takes as input a security parameter 1^λ and a string in $\mathcal{Y}^n$ and outputs some message in $\mathcal{M}$. The string r is sent across both channels, and both Bob and Eve obtain bounded oracle access to f.

[2] A slight caveat is that this holds only when r contains sufficiently many of each $x \in \mathcal{X}$, but this occurs with overwhelming probability over the choice of r.

$\mathrm{Enc}_{\mathsf{ChB}}(1^\lambda, m)$:

1. Let $n = \lambda$
2. Sample $r \leftarrow \mathcal{X}^n$.
3. Define $f_{m,r,\mathsf{ChB},n} : \mathcal{Y}^n \to \{\mathcal{M}, \perp\}$ where

   $f_{m,r,\mathsf{ChB},n}(r_B)$:

   If for all $x \in \mathcal{X}$ and $y \in \mathcal{Y}$, $\textsc{Ratio}_{x\to y}(r, r_B) \leq p_B(y \mid x) + n^{-\frac{1}{3}}$, output m. Here, $p_B(y \mid x) = \Pr[\mathsf{ChB}(x) = y]$.

   Else, output $\perp$.
4. Output $(f_{m,r,\mathsf{ChB},n}, r)$.

$\mathrm{Dec}^f_{\mathsf{ChB}}(1^\lambda, r_B)$:

1. Output $f(r_B)$.

For convenience, we define R to be a uniform random input over $\mathcal{X}^n$, $R_E = \mathsf{ChE}(R)$, and $R_B = \mathsf{ChB}(R)$.

Correctness holds since Bob can decode with high probability since $f_{m,r,\mathsf{ChB},n}$ on $\mathsf{ChB}(r)$ will output m with high probability.

Security Overview. Now consider security. Intuitively, since r is independent of the message bit b, then Eve should only be able to learn b if she can generate a guess $\widehat{r}_B$ such that $f_{b,r,\mathsf{ChB},n}(\widehat{r}_B) = b$. Consider a strategy g that given input $r_E \leftarrow \mathsf{ChE}(r)$ from Eve's channel seeks to produce an output $\widehat{r}_B$ that maximizes the probability that $f_{b,r,\mathsf{ChB},n}(g(r_E)) = b$. We say that g wins if this occurs and b is output.

If strategy g is to send Eve's channel output r_E through some discrete memoryless channel ChS (i.e. $g(r_E) = \mathsf{ChS}(r_E)$), then by our previous discussion on non-degraded channels, there exists some $x^* \in \mathcal{X}$ and $y^* \in \mathcal{Y}$ such that with high probability, $\textsc{Ratio}_{x^*\to y^*}(r, g(\mathsf{ChE}(r)))$ differs from $p_B(y^* \mid x^*)$ by at least a constant. Thus, such a g would only win with negligible probability.

However, Eve can choose any arbitrary strategy g. Nevertheless, we can still prove that any strategy g has only a negligible chance of winning. To do so, we show through a series of hybrids that any strategy g is only polynomially better than a strategy $\textsc{Eve}_3$, where $\textsc{Eve}_3$'s strategy is to apply a DMC independently to each symbol of r_E. Then, we can use the non-degraded condition to show that $\textsc{Eve}_3$'s probability of success on a single query to the oracle is negligible, and thus that any g's probability of success on a single query to the oracle is negligible. This hybrid argument is the main technical argument in our work, and it is summarized below.

The hybrid argument: Proving g has a negligible chance of winning. We first observe that an arbitrary strategy g cannot perform better than an optimal strategy g^* defined as follows:

Definition 2.4. *For any m, we say that a strategy $g^* : \mathcal{Z}^n \to \mathcal{Y}^n$ for guessing $\widehat{r}_B$ is optimal if*

$$g^* = \arg\max_g \left(\Pr_{R,\mathsf{ChE}}[f_{m,R,\mathsf{ChB},n}(g(R_E)) = m] \right).$$

Now, consider any deterministic optimal strategy. (Observe that there always exists an optimal g^* that is deterministic since g^* can arbitrarily break ties in the maximum.)

Our first step is to simplify our function g^* by a symmetrization argument. We observe that our definition of evaluation function $f_{m,r,\mathsf{ChB},n}$ on input $\widehat{r}_B$ considers only the mapping ratios $\textsc{Ratio}_{x\to y}(r,\widehat{r}_B)$ for all $x \in \mathcal{X}, y \in \mathcal{Y}$ from r to $\widehat{r}_B$. An immediate consequence of this recollection is that the probability of success for Eve when the input string is r and the guessed string is $\widehat{r}_B = g^*(r_E)$ is permutation-invariant. That is, for every permutation $\pi \in S_n$, the probability of succeeding on $\widehat{r}_B$ when the input string is r is equivalent to the probability of succeeding on $\pi(\widehat{r}_B)$ when the input string is $\pi(r)$ because

$$\textsc{Ratio}_{x\to y}(r,\widehat{r}_B) = \textsc{Ratio}_{x\to y}(\pi(r),\pi(\widehat{r}_B)).$$

Thus, since r is uniformly random, then we have $\Pr[R = \pi(r)] = \Pr[R = r]$, so morally an optimal g^*'s success probability on r_E and $\pi(r_E)$ should be the same. This is formally seen by a symmetrization argument regarding the equivalence relation we define below.

Definition 2.5. *For $r_E \in \mathcal{Z}^n$, we define the weight of r_E as*

$$\mathsf{wt}(r_E) = (N_{z_1}(r_E), \ldots, N_{z_{|\mathcal{Z}|}}(r_E))$$

where $\mathcal{Z} = \{z_1, \ldots, z_{|\mathcal{Z}|}\}$ and $N_{z_i}(r_E) = |i \in [n] \mid r_{Ei} = z_i|$. We define an equivalence relation EQWT *on $\mathcal{Z}^n \times \mathcal{Z}^n$ by*

$$\begin{aligned}\textsc{Eqwt} &= \{(r_E, {r_E}') \in \mathcal{Z}^n \times \mathcal{Z}^n \mid \mathsf{wt}(r_E) = \mathsf{wt}({r_E}')\} \\ &= \{(r_E, {r_E}') \in \mathcal{Z}^n \times \mathcal{Z}^n \mid \exists \pi \in S_n,\ r_E = \pi({r_E}')\}.\end{aligned}$$

Let $r_{Ew,0}$ denote the lexicographically first vector in the equivalence class $\{r_E \in \mathcal{Z}^n \mid \mathsf{wt}(r_E) = w\}$.

Then since g^* performs equally well on all permutations of r_E, we can create a new optimal deterministic strategy $\textsc{Eve}_0$ which behaves in a structured manner on all strings r_E from the same equivalence class. Importantly, $\textsc{Eve}_0$ has the nice property that for any permutation π, then $\pi(\textsc{Eve}_0(r_E)) = \textsc{Eve}_0(\pi(r_E))$.

$\textsc{Eve}_0(r_E)$:
Given optimal deterministic strategy g^*.

1. Let $w = \mathsf{wt}(r_E)$. Let $r_{Ew,0}$ be the lexicographically first vector in $\mathcal{Z}^n$ of weight w.
2. Let permutation $\sigma \in S_n$ be such that $\sigma(r_{Ew,0}) = r_E$.
3. Output $\widehat{r}_B = \sigma(g^*(\sigma^{-1}(r_E))) = \sigma(g^*(r_{Ew,0}))$.

Now, consider a probabilistic $\textsc{Eve}_1$ that on input $r_E \in \mathcal{Z}^n$ deviates slightly from the deterministic $\textsc{Eve}_0$. For any $z \in \mathcal{Z}$, $y \in \mathcal{Y}$, and input $r_E \in \mathcal{Z}^n$, observe that $\textsc{Eve}_0$ will map some deterministically chosen subset of size $k_{z,y}$ of the y's in r_E to be a z in $\widehat{r}_B$. Instead, we will have $\textsc{Eve}_1$ map a random subset of size k_{zy} of the y's in r_E to be a z in $\widehat{r}_B$. By a similar symmetrization argument and the construction of $\textsc{Eve}_0$, then $\textsc{Eve}_1$'s probability of success is equal to that of $\textsc{Eve}_0$.

$\textsc{Eve}_1(r_E)$:

1. For each $y \in \mathcal{Y}$ and $z \in \mathcal{Z}$, compute $k_{z,y} = N_z(r_E) \cdot \textsc{Ratio}_{z \to y}(r_E, \textsc{Eve}_0(r_E))$.
2. Start with $S = [n]$.
   For each $y \in \mathcal{Y}$ and $z \in \mathcal{Z}$
   (a) Pick a random set $S_{z,y} \subset S \cap \{i \in [n] \mid r_{E,i} = z\}$ such that $|S_{z,y}| = k_{z,y}$.
   (b) Set $\widehat{r}_{B,i} = y$ for all $i \in S_{z,y}$.
   (c) Set $S = S \backslash S_{z,y}$.
3. Output $\widehat{r}_B$.

Now, we relax the necessity of requiring that exactly $k_{z,y}$ of the z's in r_E map to y's in $\widehat{r}_B$. This relaxation is done by defining a set of stochastic matrices that model a DMC. In particular, we use the probabilistic strategy of $\textsc{Eve}_1$ to define a set of DMCs Ch_{r_E} where $p_{r_E}(z \mid y) = \textsc{Ratio}_{z \to y}(r_E, \textsc{Eve}_1(r_E))$ (which is also equal to $\textsc{Ratio}_{z \to y}(r_{Ew,0}, \textsc{Eve}_0(r_{Ew,0}))$ by definition of $\textsc{Eve}_1$). We then define a new strategy $\textsc{Eve}_2$ which on input r_E applies the corresponding channel Ch_{r_E} on each symbol of r_E to get $\widehat{r}_B$. Then $\textsc{Eve}_2$ acts identically to $\textsc{Eve}_1$ whenever each of the ratios $\textsc{Ratio}_{z \to y}(r_E, \textsc{Eve}_2(r_E))$ hit their expected value. We prove that this happens with probability at least $\frac{1}{\mathsf{poly}(n)}$, so therefore, $\textsc{Eve}_2$ wins at least inverse polynomially as often as $\textsc{Eve}_1$.

$\textsc{Eve}_2(r_E)$:

1. Define a channel Ch_{r_E} from $\mathcal{Z}$ to $\mathcal{Y}$ by stochastic matrix
$$P_{r_E} = [p_{r_E}(y \mid z)]_{z \in \mathcal{Z}, y \in \mathcal{Y}} = [\textsc{Ratio}_{z \to y}(r_E, \textsc{Eve}_0(r_E))]_{z \in \mathcal{Z}, y \in \mathcal{Y}}$$
2. For $i \in [n]$, set $\widehat{r}_{Bi} = \mathsf{Ch}_{r_E}(r_{Ei})$.
3. Output $\widehat{r}_B$.

Although $\textsc{Eve}_2$'s strategy is to apply a channel Ch_{r_E} to each symbol of her input r_E, the choice of channel she applies is dependent on which r_E she received. However, it turns out that there are only polynomially many possible channels that $\textsc{Eve}_2$ may construct. In particular, the set of channels that $\textsc{Eve}_2$ can construct is in bijective correspondence with the equivalence classes $\textsc{Eqwt}$. To see this, observe that for any permutation π, $\mathsf{Ch}_{r_E} = \mathsf{Ch}_{\pi(r_E)}$ because $\textsc{Eve}_0(\pi(r_E)) = \pi(\textsc{Eve}_0(r_E))$. Thus, the total number of possible channels that $\textsc{Eve}_2$ may apply to r_E is bounded by the number of equivalence classes of $\textsc{Eqwt}$, which is polynomial in size. We define Ch_w to be equal to Ch_{r_E} for any r_E of weight w.

Thus, instead of having $\textsc{Eve}_2$ choose a channel based on r_E's weight, we define a new strategy that randomly selects the channel before seeing r_E. In particular, we construct an $\textsc{Eve}_3$ which in addition to getting input r_E also gets an independently chosen random input w that defines which channel Ch_w that $\textsc{Eve}_3$ should apply to r_E.

$\textsc{Eve}_3(w, r_E)$:

1. Let $r_{Ew,0} \in \mathcal{Z}^n$ be the lexicographically first vector in $\mathcal{Z}^n$ of weight w.

2. Define a channel Ch_w from $\mathcal{Z}$ to $\mathcal{Y}$ by stochastic matrix

$$P_w = [p_{Y|Z}(y \mid z)]_{z\in\mathcal{Z},y\in\mathcal{Y}} = [\textsc{Ratio}_{z\to y}(r_{Ew,0}, \textsc{Eve}_0(r_{Ew,0}))]_{z\in\mathcal{Z},y\in\mathcal{Y}}$$

3. For $i \in [n]$, set $\widehat{r}_{Bi} = \mathsf{Ch}_w(r_{Ei})$.

4. Output $\widehat{r}_B$.

Now, if the randomly chosen w equals $\mathsf{wt}(r_E)$, then $\textsc{Eve}_3$ acts identically to $\textsc{Eve}_2$. But since there are only polynomially many weight vectors, an independently chosen random w equals $\mathsf{wt}(r_E)$ with probability $\frac{1}{\mathsf{poly}(n)}$. Thus, the probability that $\textsc{Eve}_3$ succeeds given a random w is only polynomially worse than the probability that $\textsc{Eve}_2$ succeeds.

However, for any weight w, it is now the case that $\textsc{Eve}_3$ applies an input-independent channel to each symbol of r_E. Thus, we can now apply the non-degraded condition to prove that $\textsc{Eve}_3$'s probability of success is negligible for any input weight w. This then implies that any arbitrary strategy g has a negligible probability of winning.

3 Preliminaries

Throughout, we will use λ to denote a security parameter.

Notation

- We say that a function $f(\lambda)$ is negligible in λ if $f(\lambda) = \lambda^{-\omega(1)}$, and we denote it by $f(\lambda) = \mathsf{negl}(\lambda)$.
- We say that a function $g(\lambda)$ is polynomial in λ if $g(\lambda) = p(\lambda)$ for some fixed polynomial p, and we denote it by $g(\lambda) = \mathsf{poly}(\lambda)$.
- For $n \in \mathbb{N}$, we use $[n]$ to denote $\{1, \ldots, n\}$.
- If R is a random variable, then $r \leftarrow R$ denotes sampling r from R. If T is a set, then $i \leftarrow T$ denotes sampling i uniformly at random from T.
- Let S_n denote the symmetric group on n letters.

Definition 3.1 (Max Norm of a Matrix)**.** *Let A by any $n \times m$ matrix. We define the max norm to be the maximal magnitude of any entry and denote it with*

$$\|A\|_{\max} = \max_{i,j} |A_{i,j}| .$$

Lemma 3.2 (Chernoff Bound)**.** *Let $X_1, \ldots, X_n$ be independent random variables taking values in $\{0, 1\}$, and let $X = \sum_{i=1}^{n} X_i$ and $\mathbb{E}[X] = \mu$. Then a two-sided Chernoff bound for $0 \le \delta \le 1$ is*

$$\Pr\left[|X - \mu| \ge \delta\mu\right] \le 2 \cdot \exp\left(-\frac{\delta^2\mu}{3}\right)$$

And a one sided Chernoff bound for $0 \le \delta \le 1$ is

$$\Pr[X \ge (1+\delta)\mu] \le \exp\left(\frac{-\delta^2\mu}{3}\right)$$

Remark 3.3. As a reminder, computationally bounded adversaries are described as non-uniform polynomial-time throughout the paper but can be equivalently given as a family of polynomial-size circuits.

3.1 Channel Definitions

Definition 3.4 (Discrete Memoryless Channel (DMC))**.** *We define a discrete memoryless channel (DMC)* $\mathsf{ChW} : \mathcal{X} \to \mathcal{Y}$ *to be a randomized function from input alphabet* $\mathcal{X}$ *to output alphabet* $\mathcal{Y}$*. We associate* ChW *with its stochastic matrix*

$$P_W = [p_W(y|x)]_{x \in \mathcal{X}, y \in \mathcal{Y}}$$

For $x \in \mathcal{X}$*, we use* $\mathsf{ChW}(x)$ *to denote a random variable over* $\mathcal{Y}$ *such that for* $y \in \mathcal{Y}$*,*

$$\Pr[\mathsf{ChW}(x) = y] = p_W(y|x)$$

For $n \in \mathbb{N}$ *and* $r = (r_1, \ldots, r_n) \in \mathcal{X}^n$*, we define*

$$\mathsf{ChW}(r) = \mathsf{ChW}(r_1) \ldots \mathsf{ChW}(r_n)$$

Notation If ChE is a channel, we may use $\Pr_{\mathsf{ChE}}$ to denote the probability over the randomness of ChE. Similarly, if f is a randomized function, we may use $\Pr_f$ to denote the probability over the randomness of f.

Definition 3.5 (Binary Symmetric Channel (BSC))**.** *A binary symmetric channel with crossover probability* p (BSC_p) *is a DMC with binary input and binary output such that on input bit* b*, it outputs* $1 - b$ *with probability* p *and* b *otherwise.*

Definition 3.6 (Binary Erasure Channel (BEC))**.** *A binary erasure channel with erasure probability* ϵ (BEC_ϵ) *is a DMC with binary input and output* $\{0, 1, \perp\}$ *such that on input bit* b*, it outputs* $\perp$ *(i.e. erases the bit) with probability* ϵ *and* b *otherwise.*

3.1.1 Less Noisy and Channel Degradation

Definition 3.7 (Less Noisy, [CK78])**.** *Channel* ChE *is less noisy than channel* ChB *if for every Markov chain* $V \to X \to YZ$ *such that* $p_{Y|X}(y|x)$ *corresponds to* ChB *and* $p_{Z|X}(z|x)$ *correspond to* ChE *then*

$$I(V; Z) \geq I(V; Y).$$

Definition 3.8 (Channel Degradation)**.** *We say that channel* ChB *is a degradation of channel* ChE *if there exists a channel* ChS *such that*

$$\mathsf{ChB} = \mathsf{ChS} \circ \mathsf{ChE}$$

where $\circ$ *denotes channel concatenation, that is* $(\mathsf{ChS} \circ \mathsf{ChE})(x) = \mathsf{ChS}(\mathsf{ChE}(x))$*.*

Definition 3.9 (Channel Degradation Equivalent Definition)**.** *Equivalently, we say that channel* $\mathsf{ChB} : \mathcal{X} \to \mathcal{Y}$ *is a degradation of channel* $\mathsf{ChE} : \mathcal{X} \to \mathcal{Z}$ *if there exists a stochastic matrix* $P_S = [p_S(y \mid z)]_{z \in \mathcal{Z}, y \in \mathcal{Y}}$ *such that*

$$P_B = P_E \cdot P_S$$

where $P_B = [p_B(y \mid x)]_{x \in \mathcal{X}, y \in \mathcal{Y}}$ *is the stochastic matrix of* ChB *and* $P_E = [p_E(z \mid x)]_{x \in \mathcal{X}, z \in \mathcal{Z}}$ *is the stochastic matrix of* ChE*.*

Consider two channels ChB and ChE. To better understand the relationship between less noisy and channel degradation, consider a concrete example where ChB is a BSC_p and ChE is a BEC_ϵ.

Theorem 3.10 (Imported from [Nai10], claim 4)**.** *Let* ChB *be a* BSC_p *for* $p \in [0, \frac{1}{2})$ *and let* ChE *be a* BEC_ϵ*. Then the following holds:*

1. *If* $0 \leq \epsilon \leq 2p$*, then* ChB *is a degradation of* ChE*.*
2. *If* $2p < \epsilon \leq 4p(1-p)$*, then* ChE *is less noisy than* ChB*, but* ChB *is not a degradation of* ChE*.*

We remark that ChE may have higher capacity than ChB but may still not be considered less noisy than ChB, e.g. $(\mathsf{ChB}, \mathsf{ChE}) = (\mathsf{BSC}_{0.1}, \mathsf{BEC}_{0.4})$. Additionally, there are many channels where ChE is not less noisy than ChB, but ChB is not a degradation of ChE, e.g. $(\mathsf{ChB}, \mathsf{ChE}) = (\mathsf{BSC}_{0.1}, \mathsf{BEC}_{0.3})$.

3.1.2 Limiting Channel Degradation

We also prove that if channel ChB is not a degradation of channel ChE then there is a constant separation between the probability distribution of ChB and the distribution of any channel formed by concatenating ChE with some other channel.

Definition 3.11 (Limiting Channel Degradation)**.** *We say that channel* ChB *is a limiting degradation of channel* ChE *if there exists a sequence of stochastic matrices* $(P_{S,1}, P_{S,2}, P_{S,3}, \ldots)$ *such that*

$$\lim_{i \to \infty} \|P_B - P_E \cdot P_{S,i}\|_{\max} = 0$$

where $P_B = [p_B(y \mid x)]_{x \in \mathcal{X}, y \in \mathcal{Y}}$ *is the stochastic matrix of* ChB *and* $P_E = [p_E(z \mid x)]_{x \in \mathcal{X}, z \in \mathcal{Z}}$ *is the stochastic matrix of* ChE*.*

Lemma 3.12 (Channel Degradation is equivalent to Limiting Channel Degradation)**.** *Channel* ChB *is a degradation of channel* ChE *if and only if* ChB *is a limiting degradation of* ChE

Proof. One direction is immediate: if channel ChB is a degradation of channel ChE, then ChB is a limiting degradation of ChE.

For the other direction, proceed by contrapositive. We show that if channel ChB is not a degradation of channel ChE, then ChB is not a limiting degradation of ChE. Let $\mathsf{ChB} : \mathcal{X} \to \mathcal{Y}$ and $\mathsf{ChE} : \mathcal{X} \to \mathcal{Z}$ be channels such that ChB is not a degradation of ChE. Let P_B and P_E be the stochastic matrices of ChB and ChE respectively. Let T be the set of all stochastic matrices from $\mathcal{Z}$ to $\mathcal{Y}$. Observe that T is a compact set: The set of stochastic matrices T is defined by finitely many constraints, each of which define either a closed halfspace ($0 \leq M_{ij} \leq 1$) or a hyperplane ($\sum_i M_{ij} = 1$) for $M \in T$. The finite intersection of these constraints forms a closed convex polytope which is indeed compact. We consider the metric given by the max norm $\|\cdot\|_{\max}$. Let $\delta_{B,E} : T \to [0, 1]$ be such that $\delta_{B,E}(P_S) = \|P_B - P_E \cdot P_S\|_{\max}$. Then observe that $\delta_{B,E}$ is a continuous function since it is a composition of two continuous functions. Now, consider any converging sequence in $[0, 1]$

$$(\delta_{B,E}(P_{S,1}), \delta_{B,E}(P_{S,2}), \delta_{B,E}(P_{S,3}), \ldots)$$

Then note that T equipped with the max norm metric is sequentially compact so the corresponding sequence $(P_{S,1}, P_{S,2}, P_{S,3}, \ldots)$ has a converging subsequence $(P_{S,i_1}, P_{S,i_2}, P_{S,i_3}, \ldots)$ such that $\lim_{j \to \infty} P_{S,i_j} = P_S{}^*$ for some stochastic matrix $P_S{}^* \in T$. Since $\delta_{B,E}$ is continuous, $\lim_{j \to \infty} \delta_{B,E}(P_{S,i_j}) = \delta_{B,E}(P_S{}^*)$. Since channel ChB is not a degradation of channel ChE and $P_S{}^*$ is a stochastic matrix, then $\|P_B - P_E \cdot P_S{}^*\|_{\max} = \delta_{B,E}(P_S{}^*) > 0$. But all converging subsequences of a converging sequence converge to the same limit; therefore the converging sequence

$$(\delta_{B,E}(P_{S,1}), \delta_{B,E}(P_{S,2}), \delta_{B,E}(P_{S,3}), \ldots)$$

converges to $\delta_{B,E}(P_S{}^*) > 0$. Therefore no converging sequence can have limit 0, so ChB is not a limiting degradation of ChE. □

Lemma 3.13. *If channel* ChB *is not a degradation of channel* ChE*, then there exists a constant* $d > 0$ *such that for all stochastic matrices* $P_S = [p_S(y \mid z)]_{z\in\mathcal{Z},y\in\mathcal{Y}}$*,*

$$\|P_B - P_E \cdot P_S\|_{\max} \geq d$$

where $P_B = [p_B(y \mid x)]_{x\in\mathcal{X},y\in\mathcal{Y}}$ *is the stochastic matrix of* ChB *and* $P_E = [p_E(z \mid x)]_{x\in\mathcal{X},z\in\mathcal{Z}}$ *is the stochastic matrix of* ChE*.*

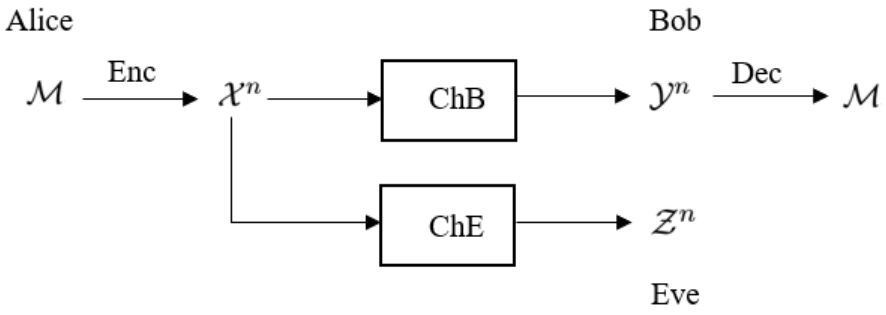
Proof. The non-existence of such d would imply that channel ChB is a limiting degradation of channel ChE. But by Lemma 3.12, this would imply that ChB is a degradation of ChE which is a contradiction. □

4 Wiretap Channels

4.1 Wiretap Channel Definitions

A wiretap channel [Wyn75, CK78] is defined by two discrete memoryless channels $(\mathsf{ChB}, \mathsf{ChE})$ with the same input domain $\mathcal{X}$ where $\mathsf{ChB} : \mathcal{X} \to \mathcal{Y}$ is the main channel and $\mathsf{ChE} : \mathcal{X} \to \mathcal{Z}$ is the eavesdropper channel. We characterize ChB by its stochastic matrix $P_B = [p_B(y \mid x)]_{x\in\mathcal{X},y\in\mathcal{Y}}$ and ChE by its stochastic matrix $P_E = [p_E(z \mid x)]_{x\in\mathcal{X},z\in\mathcal{Z}}$. Throughout, we will use $\mathcal{X}, \mathcal{Y}, \mathcal{Z}$ to denote respectively the input alphabet of ChB and ChE, the output alphabet of ChB, and the output alphabet of ChE. We use $\mathcal{M}$ to denote the message space.

Definition 4.1 (Wiretap Coding Scheme: Syntax)**.** *A wiretap coding scheme* Π *for wiretap channel* $(\mathsf{ChB}, \mathsf{ChE})$ *and message space* $\mathcal{M}$ *is a pair of algorithms* $(\mathrm{Enc}, \mathrm{Dec})$*.* Enc *is a randomized encoding algorithm that takes as input a security parameter* 1^λ*, a message* $m \in \mathcal{M}$*, and outputs a finite length encoding in* $\mathcal{X}^n$ *where* $n = n(\lambda)$*.* Dec *is a deterministic decoding algorithm that takes as input a security parameter* 1^λ*, and a string from* $\mathcal{Y}^n$ *and outputs a message in* $\mathcal{M}$*.*



A wiretap coding scheme satisfies correctness if Bob can decode the output of ChB on an encoding of a message. Security holds if Eve when given the output of ChE on the encoding of the message cannot learn the message. Similarly to [BTV12][3], we use the standard notion of semantic security [GM84]. For simplicity, we only consider the case when $\mathcal{M} = \{0, 1\}$. However, we can easily generalize our definition to consider larger families of message spaces (see Definition 4.19).

[3]Our security definition corresponds to requiring the distinguishing advantage Adv^{ds} of [BTV12] to be negligible. [BTV12] define a separate notion for semantic security, but prove that the two definitions are equivalent.

Definition 4.2 (Statistically Secure Wiretap Coding Scheme)**.** *A wiretap coding scheme* $\Pi = (\mathrm{Enc}, \mathrm{Dec})$ *is a statistically secure wiretap coding scheme for wiretap channel* $(\mathsf{ChB}, \mathsf{ChE})$ *and message space* $\mathcal{M} = \{0,1\}$ *if there exist negligible functions* $\epsilon(\lambda), \mu(\lambda)$ *such that*

- ***Correctness****: For all messages* $m \in \{0,1\}$*,*

$$\Pr[\mathrm{Dec}(1^\lambda, \mathsf{ChB}(\mathrm{Enc}(1^\lambda, m))) = m] \geq 1 - \epsilon(\lambda)$$

- ***Security****: For all adversaries* $\mathcal{A}$*,*

$$\Pr[\mathcal{A}(1^\lambda, \mathsf{ChE}(\mathrm{Enc}(1^\lambda, b))) = b] \leq \frac{1}{2} + \mu(\lambda)$$

  where b *is uniformly distributed over* $\{0,1\}$*.*

We may similarly refer to a finite scheme Π_0 *(with a fixed* λ*) as being* ϵ_0*-correct and* μ_0*-secure.*

Definition 4.3 (Computationally Secure Wiretap Coding Scheme)**.** $\Pi = (\mathrm{Enc}, \mathrm{Dec})$ *is a computationally secure wiretap coding scheme if* Enc *and* Dec *are PPT algorithms, and if it satisfies the above definition except that we only require security against non-uniform polynomial-time adversaries* $\mathcal{A}$*.*

Notation We say that a wiretap channel $(\mathsf{ChB}, \mathsf{ChE})$ admits a statistically (resp. computationally) secure wiretap coding scheme if there exists a statistically (resp. computationally) secure wiretap coding scheme for $(\mathsf{ChB}, \mathsf{ChE})$.

We can also consider a finite version of Definition 4.2 where both error parameters are fixed to constants.

Definition 4.4. *A wiretap coding scheme* $\Pi = (\mathrm{Enc}, \mathrm{Dec})$ *is a* δ*-statistically secure wiretap coding scheme for wiretap channel* $(\mathsf{ChB}, \mathsf{ChE})$ *and message space* $\mathcal{M} = \{0,1\}$ *if*

- ***Rate****: For all* $m \in \{0,1\}, |\mathrm{Enc}(b)| = c$ *for some constant* c*.*

- ***Correctness****: For all* $m \in \{0,1\}$*,*

$$\Pr[\mathrm{Dec}(\mathsf{ChB}(\mathrm{Enc}(m))) = m] \geq \delta$$

- ***Security****: For all adversaries* $\mathcal{A}$*,*

$$\Pr[\mathcal{A}(\mathsf{ChE}(\mathrm{Enc}(b))) = b] \leq \frac{1}{2} + (1 - \delta)$$

  where b *is uniformly distributed over* $\{0,1\}$*.*

4.2 Ideal Obfuscation Model

Similarly to the recent use of obfuscation in [AIK+21], it is convenient to describe and analyze our constructions in an ideal obfuscation model in which the sender can give a receiver (either Bob or Eve) bounded query access to an oracle. In this model, the encoding function outputs both an encoding of m and a description $\hat{f}$ of a circuit computing a deterministic function f. (We will typically abuse notation by using f to denote both the function and its description.) The receiver Bob and the adversary Eve are both given oracle access to f. In addition, though we require Eve to only make polynomially many queries to the oracle f, we allow Eve to be otherwise unbounded by default (see Remark 4.7 below for a relaxed definition variant). We will later consider the question of instantiating the ideal obfuscation primitive in the plain model under concrete cryptographic assumptions (see Section 7).

Definition 4.5 (Wiretap Coding Scheme in the Ideal Obfuscation Model: Syntax)**.** *A wiretap coding scheme* Π *for wiretap channel* $(\mathsf{ChB}, \mathsf{ChE})$ *and message space* $\mathcal{M}$ *in the ideal obfuscation model is a pair of algorithms* $(\mathrm{Enc}, \mathrm{Dec}^{(\cdot)})$*.* Enc *is a randomized encoding algorithm that takes as input a security parameter* 1^λ *and a message* $m \in \mathcal{M}$*, and outputs a finite length encoding in* $\mathcal{X}^n$ *where* $n = n(\lambda)$ *and a description* $\hat{f}$ *of a circuit computing some deterministic function* f*.* $\mathrm{Dec}^{(\cdot)}$ *is a deterministic decoding algorithm with polynomially bounded access to an oracle. It takes as input a security parameter* 1^λ*, a string from* $\mathcal{Y}^n$*, and outputs a message in* $\mathcal{M}$*.*

Definition 4.6 (Bounded Query Secure Wiretap Coding Scheme in the Ideal Obfuscation Model)**.** *A wiretap coding scheme* $\Pi = (\mathrm{Enc}, \mathrm{Dec}^{(\cdot)})$ *is a bounded query secure wiretap coding scheme in the ideal obfuscation model for wiretap channel* $(\mathsf{ChB}, \mathsf{ChE})$ *and message space* $\mathcal{M} = \{0,1\}$ *if* Enc *and* $\mathrm{Dec}^{(\cdot)}$ *are PPT algorithms which satisfy*

- ***Correctness****: For all messages* $m \in \{0,1\}$*,*

$$\Pr[\mathrm{Dec}^f(1^\lambda, \mathsf{ChB}(c)) = m \mid (f,c) \leftarrow \mathrm{Enc}(1^\lambda, m)] \geq 1 - \mathsf{negl}(\lambda)$$

- ***Security****: For every polynomial query bound* $q(\lambda)$ *and (computationally unbounded) adversary* $\mathcal{A}^{(\cdot)}$ *that makes at most* $q(\lambda)$ *queries to its oracle* f*,*

$$\Pr[\mathcal{A}^{f_b}(1^\lambda, \mathsf{ChE}(c_b)) = b \mid (f_b, c_b) \leftarrow \mathrm{Enc}(1^\lambda, b)] \leq \frac{1}{2} + \mathsf{negl}(\lambda)$$

  where b *is uniformly distributed over* $\{0,1\}$*.*

Remark 4.7 (Computationally bounded adversaries)**.** Definition 4.6 only bounds the number of queries made by $\mathcal{A}$ but does not otherwise bound its computational complexity. This makes our main feasibility results stronger. One may also consider a relaxed variant of the definition in which $\mathcal{A}$ is computationally bounded, as in Definition 4.3. This relaxation can be used for bootstrapping from a low-rate wiretap coding scheme in the ideal obfuscation model to a high-rate *computationally secure* scheme (with a "small" oracle f) via a hybrid encryption technique (see Remark 4.18).

4.3 Wiretap Feasibility in the Information Theoretic Setting

We will prove the following characterization of the wiretap feasibility region in the information theoretic setting:

Theorem 4.8. ChE *is not less noisy than* ChB *if and only if there exist a statistically secure wiretap coding scheme for* $(\mathsf{ChB}, \mathsf{ChE})$*.*

In fact, we will prove a stronger claim (Theorem 4.17) relating the definitions of wiretap security from prior work to our definitions. As historically information theorists have focused more on obtaining the maximal achievable rate R for the encoding function Enc than on achieving strong notions of cryptographic security, their definitions of security are framed differently from the typical cryptographic definitions. This disconnect was addressed in [BTV12], who bridged the gap between the information theoretic and cryptographic communities and proposed new security definitions for the wiretap channel.

We now define the following in terms of the correctness and security requirements of [CK78].

Definition 4.9 (CK Rate-R Wiretap Coding Family [CK78])**.** *A family of wiretap encoder-decoder pairs* $\{(\mathrm{Enc}_n, \mathrm{Dec}_n)\}_{n\in\mathbb{N}}$ *is a rate-*R *information theoretic wiretap coding family for a wiretap channel* $(\mathsf{ChB}, \mathsf{ChE})$ *and message family* $\{\mathcal{M}_n\}_{n\in\mathbb{N}}$ *if each* Enc_n *outputs an encoding of length* n *such that*

- ***Message Rate*** *R:*
$$\lim_{n\to\infty} \frac{1}{n} \log |\mathcal{M}_n| = R$$
- ***Correctness****: For all $m \in \mathcal{M}_n$,*
$$\Pr[\mathrm{Dec}_n(\mathsf{ChB}(\mathrm{Enc}_n(m))) = m] \geq 1 - \epsilon_n$$
where
$$\lim_{n\to\infty} \epsilon_n = 0$$
- ***Security****:*
$$\lim_{n\to\infty} \frac{1}{n} I(M_n; \mathsf{ChE}(\mathrm{Enc}_n(M_n))) = 0$$
where M_n is uniform over $\mathcal{M}_n$.

We denote the set of all achievable rate pairs as $\mathcal{R}$.

We define secrecy capacity as the maximum rate of such an encoding.

Definition 4.10 (Secrecy Capacity)**.** *The secrecy capacity C_s of a wiretap channel $(\mathsf{ChB}, \mathsf{ChE})$, is the maximum of the rates R of any CK rate-R wiretap coding family for wiretap channel $(\mathsf{ChB}, \mathsf{ChE})$ for any message family $\{\mathcal{M}_n\}_{n\in\mathbb{N}}$.*

Furthermore, [CK78] completely characterized the region in which positive rate CK wiretap coding schemes are possible.

Theorem 4.11 ([CK78])**.** *$C_s > 0$ if and only if ChE is not less noisy than ChB.*

Note that if $C_s = 0$, then no positive rate encoding can satisfy both correctness and security.

Additionally, [MW00] show that the security requirement can be strengthened to the following:

Definition 4.12 (CK Rate-R Wiretap Coding Family with Strong Secrecy [CK78, MW00])**.** *This is the same as the definition of a CK Rate-R wiretap coding family except that we replace the security requirement with the following:*

- ***Strong Security****:*
$$\lim_{n\to\infty} I(M_n; \mathsf{ChE}(\mathrm{Enc}_n(M_n))) = 0$$
where M_n is uniform over $\mathcal{M}_n$.

We can then define the strong secrecy capacity.

Definition 4.13 (Strong Secrecy Capacity (Adapted from [MW00]))**.** *The strong secrecy capacity $\overline{C_s}$ of a wiretap channel $(\mathsf{ChB}, \mathsf{ChE})$, is the maximum of the rates R of any CK rate-R wiretap coding family with strong secrecy for wiretap channel $(\mathsf{ChB}, \mathsf{ChE})$ for any message family $\{\mathcal{M}_n\}_{n\in\mathbb{N}}$.*

Theorem 4.14 (Equivalence of Strong and Weak Secrecy Capacity (Imported from [MW00]))**.** *For all wiretap channels $(\mathsf{ChB}, \mathsf{ChE})$, we have $C_s = \overline{C_s}$.*

Remark 4.15. The definition of C_s above is written differently from the definition in [CK78]. However, it is equivalent and follows easily from the definitions used in [CK78]. The definitions of C_s and $\overline{C_s}$ are similar, but slightly different from the definitions used in [MW00]. However, Theorem 4.14 still holds with respect to our definitions. We provide a short explanation of these two facts in Appendix A.

As observed by [BTV12], both the correctness and security definitions of [CK78] are weaker than our definitions and are insufficient for cryptographic purposes[4]. Thus, [BTV12] defined several new notions of security including the semantic security definition we use. They also prove that this semantic security definition implies an information theoretic security notion.

Theorem 4.16 ([BTV12])**.** *The semantic security requirement of Definition 4.2 of a statistically secure wiretap coding scheme implies that* $I(M; \mathsf{ChE}(\mathrm{Enc}(1^\lambda, M))) = \mathsf{negl}(\lambda)$ *where* M *is uniform over* $\mathcal{M} = \{0,1\}$.

We now prove the following theorem which implies Theorem 4.8.

Theorem 4.17. *The following are equivalent:*

1. ChE *is not less noisy than* ChB*. (Definition 3.7)*
2. $C_s > 0$ *(Definition 4.10)*
   i.e. There exists a CK Rate-R wiretap coding family for $(\mathsf{ChB}, \mathsf{ChE})$ *with positive rate R. (Definition 4.9)*
3. $\overline{C_s} > 0$ *(Definition 4.13)*
   i.e. There exists a CK Rate-R wiretap coding family with strong secrecy for $(\mathsf{ChB}, \mathsf{ChE})$ *with positive rate R. (Definition 4.12)*
4. *There exists a* 0.99*-statistically secure wiretap coding scheme for* $(\mathsf{ChB}, \mathsf{ChE})$*. (Definition 4.4)*
5. *There exists a statistically secure wiretap coding scheme for* $(\mathsf{ChB}, \mathsf{ChE})$*. (Definition 4.2)*
6. *There exists a statistically secure wiretap coding scheme for general message spaces for* $(\mathsf{ChB}, \mathsf{ChE})$ *with a positive constant rate. (Definition 4.19. See Section 4.4 below for the definition.)*

Proof. The theorem follows from the relations below.

- $1 \iff 2$. This follows from Theorem 4.11.
- $2 \iff 3$. This follows from Theorem 4.14.
- $6 \Rightarrow 5$. A statistically secure wiretap coding scheme for general message spaces can be easily transformed into one for a binary message spaces by ignoring all but the first bit of the message from the general message space.
- $5 \Rightarrow 2$. This proof can be found in Appendix C.
- $3 \Rightarrow 4$. This proof can be found in Appendix C.
- $4 \Rightarrow 6$. This proof can be found in Appendix C.

□

[4] As the growth rate of the correctness and security functions is not specified, correctness would be satisfied even if the probability of correct decryption is $1 - \frac{1}{\log(n)}$ and security would be satisfied even if $\lim_{n\to\infty} I(M_n; \mathsf{ChE}(\mathrm{Enc}_n(M_n))) = \log(n)$. Even when using the strong secrecy definition of [MW00, Mau94], security is defined only with respect to a uniformly random message distribution.

4.4 Rate and General Message Spaces

Previously, we only considered the case when $\mathcal{M} = \{0,1\}$. This means that any secure wiretap coding scheme must be rate 0.

Remark 4.18. When the adversary is computationally bounded, and potentially has oracle access, we note that any computationally secure wiretap coding scheme can be made optimal rate, meaning rate asymptotically approaching Bob's channel's capacity. This is achieved by using the computationally secure wiretap coding scheme to share a secret key between Alice and Bob and then subsequently using a PRG to build a stream cipher between Alice and Bob. The ciphertext must then be sent across Bob's channel; therefore the maximal rate is given by the capacity.

Unfortunately, in the information theoretic setting, we cannot improve rate in the same manner. Thus, we define a notion of secure wiretap coding schemes for general message spaces.

Definition 4.19 (Statistically Secure Wiretap Coding Schemes for General Message Spaces)**.** *A wiretap coding scheme* $\Pi = (\mathrm{Enc}, \mathrm{Dec})$ *is a secure wiretap coding scheme for wiretap channel* $(\mathsf{ChB}, \mathsf{ChE})$ *and a polytime computable message length* $\ell(\lambda)$ *if there exist negligible functions* $\epsilon(\lambda), \mu(\lambda)$ *such that*

- ***Correctness****: For all messages* $m \in \{0,1\}^{\ell(\lambda)}$*,*

$$\Pr[\mathrm{Dec}(1^\lambda, \mathsf{ChB}(\mathrm{Enc}(1^\lambda, m))) = m] \geq 1 - \epsilon(\lambda)$$

- ***Security****: For all adversaries* $\mathcal{A}$ *and all messages* $m_0 \neq m_1 \in \{0,1\}^{\ell(n)}$*,*

$$\Pr[\mathcal{A}(1^\lambda, m_0, m_1, \mathsf{ChE}(\mathrm{Enc}(1^\lambda, m_b))) = b] \leq \frac{1}{2} + \mu(\lambda)$$

  where b *is uniformly distributed over* $\{0,1\}$*.*

Similarly, we can define this in the computational setting and in the ideal obfuscation model.

Remark 4.20. Our main result of Theorem 5.3 still holds with respect to this general definition with only notational changes in the proofs.

5 Constructing Bounded Query Secure Wiretap Coding Schemes in the Ideal Obfuscation Model

5.1 Construction

We consider the setting of a $(\mathsf{ChB}, \mathsf{ChE})$ wiretap channel where the main channel $\mathsf{ChB} : \mathcal{X} \to \mathcal{Y}$ is not a degradation of the eavesdropping channel $\mathsf{ChE} : \mathcal{X} \to \mathcal{Z}$. For the entirety of this section, we will characterize ChB by its stochastic matrix $P_B = [p_B(y \mid x)]_{x \in \mathcal{X}, y \in \mathcal{Y}}$ and channel ChE by its stochastic matrix $P_E = [p_E(z \mid x)]_{x \in \mathcal{X}, z \in \mathcal{Z}}$. We let $\mathcal{M} = \{0,1\}$.

Let λ be a security parameter, and let $n = \lambda$. Our encoding of a message $m \in \mathcal{M}$ will specify a codeword and an oracle. The codeword will be a random string $r \in \mathcal{X}^n$ which will be sent across the two channels. We define

- R: uniform random variable over $\mathcal{X}^n$
- $R_B := \mathsf{ChB}(R)$

- $R_E := \mathsf{ChE}(R)$

The oracle, which is transmitted perfectly to both parties, will output the message m if it receives an input which is "typical" for R_B conditioned on $R = r$ (notationally $R_{B|R=r}$) and will output $\perp$ otherwise. We will define typicality in terms of the expected number of x's in r that should turn into y's in $R_{B|R=r}$ for each pair $(x, y) \in \mathcal{X} \times \mathcal{Y}$ as specified by Bob's channel probability matrix P_B. The receiver Bob should be able to recover m simply by sending his received value of R_B to the oracle. Thus, the decoder will simply output the value of the oracle on its input. Security holds if the eavesdropper Eve cannot create a "typical" channel value for $R_{B|R=r}$ given only $R_{E|R=r}$. To specify this more formally, we first define the following:

Definition 5.1. *Let $\mathcal{X}$ be any discrete finite set and $n \in \mathbb{N}$. For any $r \in \mathcal{X}^n$ and $x \in \mathcal{X}$, we define the number of x's in r to be*

$$N_x(r) = |\{i \in [n] : r_i = x\}|$$

Definition 5.2. *Let $\mathcal{X}$ and $\mathcal{Y}$ be any two discrete finite sets and $n \in \mathbb{N}$. For $r \in \mathcal{X}^n$ and $s \in \mathcal{Y}^n$ and for any $x \in \mathcal{X}$ and $y \in \mathcal{Y}$, we define the fraction of x's in r that are y's in s to be*

$$\textsc{Ratio}_{x \to y}(r, s) = \frac{|i \in [n] : r_i = x, s_i = y|}{N_x(r)}.$$

If $N_x(r) = 0$, then we define $\textsc{Ratio}_{x \to y}(r, s) = 0$.

We now describe our wiretap encoder-decoder pair $(\mathrm{Enc}_{\mathsf{ChB}}, \mathrm{Dec}_{\mathsf{ChB}})$ for main channel ChB.

$\mathrm{Enc}_{\mathsf{ChB}}(1^\lambda, m)$:

1. Let $n = \lambda$
2. Sample $r \leftarrow \mathcal{X}^n$.
3. Define $f_{m,r,\mathsf{ChB},n} : \mathcal{Y}^n \to \{\mathcal{M}, \perp\}$ where

   $f_{m,r,\mathsf{ChB},n}(r_B)$:

   If for all $x \in \mathcal{X}$ and $y \in \mathcal{Y}$, $\textsc{Ratio}_{x \to y}(r, r_B) \leq p_B(y \mid x) + n^{-\frac{1}{3}}$, output m.
   Else, output $\perp$.

4. Output $(f_{m,r,\mathsf{ChB},n}, r)$.

$\mathrm{Dec}^f_{\mathsf{ChB}}(1^\lambda, r_B)$:

1. Output $f(r_B)$.

We then prove that our coding scheme gives us both correctness and security.

Theorem 5.3. *If $(\mathsf{ChB}, \mathsf{ChE})$ is a wiretap channel where ChB is not a degradation of ChE, then $(\mathrm{Enc}_{\mathsf{ChB}}, \mathrm{Dec}^{(\cdot)}_{\mathsf{ChB}})$ achieves*

- ***Correctness**: For all messages $m \in \{0, 1\}$,*

$$\Pr[\mathrm{Dec}^{f_{m,r,\mathsf{ChB},n}}_{\mathsf{ChB}}(1^\lambda, \mathsf{ChB}(r)) = m \mid (f_{m,r,\mathsf{ChB},n}, r) \leftarrow \mathrm{Enc}_{\mathsf{ChB}}(1^\lambda, m)] \geq 1 - \mathsf{negl}(\lambda)$$

- ***Security**: For every polynomial query bound $q(\lambda)$ and (computationally unbounded) adversary $\mathcal{A}^{(\cdot)}$ that makes at most $q(\lambda)$ queries to its oracle,*

$$\Pr[\mathcal{A}^{f_{b,r,\mathsf{ChB},n}}(1^\lambda, \mathsf{ChE}(r)) = b \mid (f_{b,r,\mathsf{ChB},n}, r) \leftarrow \mathrm{Enc}_{\mathsf{ChB}}(1^\lambda, b)] \leq \frac{1}{2} + \mathsf{negl}(\lambda)$$

where b is uniformly distributed over $\{0,1\}$.

Proof. Correctness follows by Theorem 5.8, and security follows by Theorem 5.34 which are proven below. □

Since $\mathrm{Enc}_{\mathsf{ChB}}$ and $\mathrm{Dec}^{(\cdot)}_{\mathsf{ChB}}$ are PPT, we get the following corollary.

Corollary 5.4. *If $(\mathsf{ChB}, \mathsf{ChE})$ is a wiretap channel where ChB is not a degradation of ChE, then $(\mathrm{Enc}_{\mathsf{ChB}}, \mathrm{Dec}^{(\cdot)}_{\mathsf{ChB}})$ is a bounded query secure wiretap coding scheme in the ideal obfuscation model.*

Remark 5.5. Theorem 5.3 and Corollary 5.4 hold even if we modify $f_{m,r,\mathsf{ChB},n}$ to have binary output domain by outputting 0 in place of $\perp$. Correctness still holds since the probability that the decoder using the original function outputs $\perp$ is negligible, so changing $\perp$ to 0 results in at most a negligible change in correctness. For security, observe that by outputting 0 instead of $\perp$, Eve gets strictly less information as she cannot tell whether an observed 0 from the oracle is an indicator of failure to receive the message bit or is the message bit itself.

5.2 Correctness

Correctness follows by a simple Chernoff bound over each set of symbols $x \in \mathcal{X}$ in R. However, for the Chernoff bound to apply, we need R to have a sufficient number of each symbol in $\mathcal{X}$. By an additional Chernoff bound, this occurs with overwhelming probability over R.

Definition 5.6. *Let* $\textsc{Good} = \{r \in \mathcal{X}^n \mid \forall x \in \mathcal{X}, N_x(r) \geq \frac{n}{2|\mathcal{X}|}\} \subset \mathcal{X}^n$.
Observe that for all $r \in \textsc{Good}$ and $x \in \mathcal{X}$, then $N_x(r) = \Theta(n)$.

Lemma 5.7. $\Pr[R \in \textsc{Good}] \geq 1 - \mathsf{negl}(\lambda)$

Proof. We defer the proof to Appendix B. □

Now, we apply a Chernoff bound and a union bound to get correctness.

Theorem 5.8. *For all messages $m \in \{0,1\}$,*

$$\Pr\left[\mathrm{Dec}^{f_{m,r,\mathsf{ChB},n}}_{\mathsf{ChB}}(1^\lambda, \mathsf{ChB}(r)) = m \mid (f_{m,r,\mathsf{ChB},n}, r) \leftarrow \mathrm{Enc}_{\mathsf{ChB}}(1^\lambda, m)\right] \geq 1 - \mathsf{negl}(\lambda)$$

Proof. By definition of $\mathrm{Enc}_{\mathsf{ChB}}$ and $\mathrm{Dec}^{(\cdot)}_{\mathsf{ChB}}$,

$$\begin{aligned}
&\Pr\left[\mathrm{Dec}^{f_{m,r,\mathsf{ChB},n}}_{\mathsf{ChB}}(1^\lambda, \mathsf{ChB}(r)) = m \mid (f_{m,r,\mathsf{ChB},n}, r) \leftarrow \mathrm{Enc}_{\mathsf{ChB}}(1^\lambda, m)\right] \\
&= \Pr[f_{m,r,\mathsf{ChB},n}(\mathsf{ChB}(r)) = m \mid r \leftarrow R\ ] \\
&= \Pr\left[\forall x \in \mathcal{X}, y \in \mathcal{Y},\ \textsc{Ratio}_{x\to y}(R, \mathsf{ChB}(R)) \leq p_B(y|x) + n^{-\frac{1}{3}}\right] \\
&= 1 - \Pr\left[\exists x \in \mathcal{X}, y \in \mathcal{Y},\ \textsc{Ratio}_{x\to y}(R, \mathsf{ChB}(R)) > p_B(y|x) + n^{-\frac{1}{3}}\right]
\end{aligned}$$

Thus, since $\Pr[R \notin \textsc{Good}] \leq \mathsf{negl}(\lambda)$ by Lemma 5.7, it suffices to prove that for all $r \in \textsc{Good}$,

$$\Pr\left[\exists x \in \mathcal{X}, y \in \mathcal{Y},\ \textsc{Ratio}_{x\to y}(r, \mathsf{ChB}(r)) > p_B(y|x) + n^{-\frac{1}{3}}\right] \leq \mathsf{negl}(\lambda)$$

Fix any $r \in \textsc{Good}$, $x \in \mathcal{X}$, and $y \in \mathcal{Y}$. For all $i \in [n]$, define

$$V_i = \begin{cases} 1 \text{ if } r_i = x \text{ and } (\mathsf{ChB}(r))_i = y \\ 0 \text{ else} \end{cases}$$

Let $S_x = \{i \in [n] \mid r_i = x\}$. Then by a Chernoff bound,

$$\begin{aligned} &\Pr\left[\textsc{Ratio}_{x\to y}(r, \mathsf{ChB}(r)) - p_B(y|x) \geq n^{-\frac{1}{3}}\right] \\ &= \Pr\left[\sum_{i\in S_x} V_i - N_x(r)\cdot p_B(y|x) \geq N_x(r)\cdot n^{-\frac{1}{3}}\right] \\ &\leq \exp\left(\frac{-N_x(r)\cdot n^{-2/3}}{3\cdot p_B(y|x)}\right). \end{aligned}$$

Since $p_B(y|x) \leq 1$ and $r \in \textsc{Good}$ implies $N_x(r) = \Theta(n)$,

$$\Pr\left[\sum_{i\in S_x} V_i - N_x(r)\cdot p_B(y|x) \geq N_x(r)\cdot n^{-\frac{1}{3}}\right] \leq e^{-\Omega(n^{1/3})} = \mathsf{negl}(n).$$

Thus, by a union bound, for all $r \in \textsc{Good}$

$$\Pr\left[\exists x \in \mathcal{X}, y \in \mathcal{Y},\ \textsc{Ratio}_{x\to y}(r, \mathsf{ChB}(r)) > p_B(y|x) + n^{-\frac{1}{3}}\right] \leq |\mathcal{X}|\cdot|\mathcal{Y}|\cdot\mathsf{negl}(n) = \mathsf{negl}(\lambda)$$

and the proof follows. □

5.3 Security

5.3.1 Overview

In our security game, the adversary receives $R_E = \mathsf{ChE}(R)$ and oracle access to $f_{b,R,\mathsf{ChB},n}$ for a random $b \in \{0,1\}$ and tries to guess b. Intuitively, since R is independent of b, if for all $b \in \{0,1\}$, an adversary is unable to generate an input $\widehat{r}_B$ such that $f_{b,r,p_B,n}(\widehat{r}_B) \neq \perp$, then the adversary should be unable to learn anything about b. Thus, we will first attempt to show this.

To simplify our proof, we define the following function $h_{r,\mathsf{ChB},n}$ which on input r_B outputs 1 if all of the ratios $\textsc{Ratio}_{x\to y}(r, r_B)$ are sufficiently close to the channel probabilities $p_B(y \mid x)$ and 0 otherwise.

Definition 5.9. *Let $r \in \mathcal{X}^n$ and $r_B \in \mathcal{Y}^n$. Define $h_{r,\mathsf{ChB},n} : \mathcal{Y}^n \to \{0,1\}$ as*

$h_{r,\mathsf{ChB},n}(r_B)$*:*

> *If for all $x \in \mathcal{X}$ and $y \in \mathcal{Y}$, $|\textsc{Ratio}_{x\to y}(r, r_B) - p_B(y \mid x)| \leq |\mathcal{Y}|\cdot n^{-\frac{1}{3}}$, output 1.*
>
> *Else, output 0.*

We will first show that for any arbitrary strategy g that an adversary applies to R_E,

$$\Pr[h_{R,\mathsf{ChB},n}(g(R_E)) = 1] \leq \mathsf{negl}(\lambda).$$

We will then prove that this implies that for any arbitrary strategy g that an adversary applies to R_E,

$$\Pr[f_{m,R,\mathsf{ChB},n}(g(R_E)) \neq \perp] \leq \mathsf{negl}(\lambda).$$

Then we will prove that this implies security.

To prove the first step, we will need to rely on the fact that ChB is not a degradation of ChE. This means that for all channels ChS, then

$$\mathsf{ChB} \neq \mathsf{ChS} \circ \mathsf{ChE}$$

Thus, if Eve's strategy g was to apply a DMC channel ChS to each symbol of R_E, then the distribution of $g(R_E) = \mathsf{ChS}(\mathsf{ChE}(R))$ should differ from the distribution of $\mathsf{ChB}(R)$, and therefore result in $h_{R,\mathsf{ChB},n}(g(R_E)) = 0$ with high probability.

However, Eve may instead choose any arbitrary strategy g. Thus, to prove our result, we will show through a series of hybrids $g, \text{Eve}_0, \text{Eve}_1, \text{Eve}_2, \text{Eve}_3$ that strategy g is only polynomially better that strategy Eve_3, where Eve_3's strategy is to apply a DMC independently to each symbol of R_E. Then, we can use the not-degraded condition to show that Eve_3's probability of success is negligible. We refer further intuition to the Technical Overview.

We will first assume that Eve's arbitrary strategy g is optimal, defined below:

Definition 5.10. *We say that a strategy $g^* : \mathcal{Z}^n \to \mathcal{Y}^n$ for guessing $\widehat{r}_B$ is optimal if*

$$g^* = \arg\max_g \left(\Pr_{R,\mathsf{ChE}}[h_{R,\mathsf{ChB},n}(g(R_E)) = 1] \right).$$

Remark 5.11. By definition, for any optimal strategy g^*,

$$g^*(r_E) = \max_{\widehat{r}_B} \left(\Pr_{R,\mathsf{ChE}}[h_{R,\mathsf{ChB},n}(\widehat{r}_B) = 1 \mid R_E = r_E] \right)$$

Observe that there may be multiple possible optimal strategies g^* which achieve the same maximal probability of success. Furthermore, since g^* may arbitrarily break ties for the maximum, then there always exists an optimal strategy which is deterministic.

We also define a notion of weight.

Definition 5.12. *For $r_E \in \mathcal{Z}^n$, we define the weight of r_E as*

$$\mathsf{wt}(r_E) = (N_{z_1}(r_E), \ldots, N_{z_{|\mathcal{Z}|}}(r_E))$$

where $\mathcal{Z} = \{z_1, \ldots, z_{|\mathcal{Z}|}\}$. We define an equivalence relation EQWT *on $\mathcal{Z}^n \times \mathcal{Z}^n$ by*

$$\begin{aligned} \text{EQWT} &= \{(r_E, {r_E}') \in \mathcal{Z}^n \times \mathcal{Z}^n \mid \mathsf{wt}(r_E) = \mathsf{wt}({r_E}')\} \\ &= \{(r_E, {r_E}') \in \mathcal{Z}^n \times \mathcal{Z}^n \mid \exists \pi \in S_n,\ r_E = \pi({r_E}')\}. \end{aligned}$$

We define the lexicographically first element in the equivalence class to be the canonical representative of the class.

Definition 5.13. *Let $r_{E_{w,0}}$ denote the lexicographically first vector in the equivalence class $\{r_E \in \mathcal{Z}^n \mid \mathsf{wt}(r_E) = w\}$.*

5.3.2 Applying Symmetry

Let g^* be any optimal deterministic strategy. We will first construct a new optimal strategy EVE_0 that has the property that for all $r_E \in \mathcal{Z}^n$ and all permutations π, $\text{EVE}_0(\pi(r_E)) = \pi(\text{EVE}_0(r_E))$.

First, we prove a fact about the symmetry of r and r_E.

Claim 5.14. *For all $r \in \mathcal{X}^n$, $r_E \in \mathcal{Z}^n$, $\pi \in S_n$,*

$$\Pr[R = r \mid R_E = r_E] = \Pr[R = \pi(r) \mid R_E = \pi(r_E)]$$

Proof. The proof follows by symmetry. We defer the proof to Appendix B. □

Then we concretize the observation that $h_{r,\mathsf{ChB},n}$ depends only on the global probabilities of input-output pairs in $\mathcal{X} \times \mathcal{Y}$.

Claim 5.15. *For a fixed $r \in \mathcal{X}^n, r_B \in \mathcal{Y}^n$, and any $\pi \in S_n$, $h_{r,\mathsf{ChB},n}(r_B) = 1$ if and only if $h_{\pi(r),\mathsf{ChB},n}(\pi(r_B)) = 1$.*

Proof. Again, the proof follows by symmetry. We defer the proof to Appendix B. □

Claim 5.14 and Claim 5.15 give the following corollary which states that a guess $\widehat{r}_B$ given received string r_E should succeed with the same probability as a guess $\pi(\widehat{r}_B)$ given received string $\pi(r_E)$. More concretely,

Corollary 5.16. *For all $\widehat{r}_B \in \mathcal{Y}^n, r_E \in \mathcal{Z}^n, \pi \in S_n$,*

$$\Pr_{R,\mathsf{ChE}}[h_{R,\mathsf{ChB},n}(\widehat{r}_B) = 1 \mid R_E = r_E] = \Pr_{R,\mathsf{ChE}}[h_{R,\mathsf{ChB},n}(\pi(\widehat{r}_B)) = 1 \mid R_E = \pi(r_E)]$$

Proof. This follows immediately from Claim 5.14 and Claim 5.15. We defer the proof to Appendix B. □

Now, we can prove that any optimal deterministic strategy $g^* : \mathcal{X}^n \to \mathcal{Y}^n$ does equally well on all permutations of received string r_E.

Lemma 5.17. *For all $r_E \in \mathcal{Z}^n, \pi \in S_n$, and for any optimal deterministic strategy $g^* : \mathcal{X}^n \to \mathcal{Y}^n$,*

$$\Pr_{R,\mathsf{ChE}}[h_{R,\mathsf{ChB},n}(g^*(R_E)) \mid R_E = r_E] = \Pr_{R,\mathsf{ChE}}[h_{R,\mathsf{ChB},n}(g^*(R_E)) \mid R_E = \pi(r_E)]$$

Proof. Using the definition of an optimal strategy and Corollary 5.16 we have

$$\begin{aligned}\Pr_{R,\mathsf{ChE}}[h_{R,\mathsf{ChB},n}(g^*(R_E)) \mid R_E = r_E] &= \max_{\widehat{r}_B} \Pr_{R,\mathsf{ChE}}[h_{R,\mathsf{ChB},n}(\widehat{r}_B) = 1 \mid R_E = r_E] \\ &= \max_{\widehat{r}_B} \Pr_{R,\mathsf{ChE}}[h_{R,\mathsf{ChB},n}(\pi(\widehat{r}_B)) = 1 \mid R_E = \pi(r_E)]\end{aligned}$$

Define $r_B{}' = \pi(\widehat{r}_B)$. Then express the above as follows:

$$\begin{aligned}\Pr_{R,\mathsf{ChE}}[h_{R,\mathsf{ChB},n}(g^*(R_E)) \mid R_E = r_E] &= \max_{r_B{}'} \Pr_{R,\mathsf{ChE}}[h_{R,\mathsf{ChB},n}(r_B{}') = 1 \mid R_E = \pi(r_E)] \\ &= \Pr_{R,\mathsf{ChE}}[h_{R,\mathsf{ChB},n}(g^*(R_E)) = 1 \mid R_E = \pi(r_E)]\end{aligned}$$

□

Although g^* has the same probability of success on all permutations of a given string r_E, g^* may still behave rather differently on each permutation. To deal with this, we construct a new optimal strategy $\textsc{Eve}_0$ that acts in a structured manner on each permutation of r_E so that $\textsc{Eve}_0(\pi(r_E)) = \pi(\textsc{Eve}_0(r_E))$ for all $\pi \in S_n$.

We define $\textsc{Eve}_0$ from g^* as follows:

$\textsc{Eve}_0(r_E)$:
Given optimal deterministic strategy g^*.

1. Let $w = \mathsf{wt}(r_E)$. Let $r_{Ew,0}$ be the lexicographically first vector in $\mathcal{Z}^n$ of weight w.
2. Let permutation $\sigma \in S_n$ be such that $\sigma(r_{Ew,0}) = r_E$.
3. Output $\widehat{r}_B = \sigma(g^*(\sigma^{-1}(r_E))) = \sigma(g^*(r_{Ew,0}))$.

Remark 5.18. For any weight w and any permutation $\tau \in S_n$,

$$\textsc{Eve}_0(\tau(r_{Ew,0})) = \tau(g^*(r_{Ew,0}))$$

In particular,

$$\textsc{Eve}_0(r_{Ew,0}) = g^*(r_{Ew,0})$$

Lemma 5.19. *If $g^* : \mathcal{Z}^n \to \mathcal{Y}^n$ is an optimal deterministic strategy, then $\textsc{Eve}_0 : \mathcal{Z}^n \to \mathcal{Y}^n$ is an optimal strategy. Moreover, for any $r_E \in \mathcal{Z}^n$ and $\pi \in S_n$, $\textsc{Eve}_0(\pi(r_E)) = \pi(\textsc{Eve}_0(r_E))$.*

Proof. Fix any $r_E \in \mathcal{Z}^n$. Let $w = \mathsf{wt}(r_E)$, and let $r_{Ew,0}$ be the lexicographically first vector of weight w in $\mathcal{Z}^n$. Let $\sigma \in S_n$ such that $\sigma(r_{Ew,0}) = r_E$.

By Corollary 5.16, we have that

$$\Pr_{R,\mathsf{ChE}}[h_{R,\mathsf{ChB},n}(\sigma(g^*(r_{Ew,0}))) = 1 \mid R_E = \sigma(r_{Ew,0})] = \Pr_{R,\mathsf{ChE}}[h_{R,\mathsf{ChB},n}(g^*(r_{Ew,0})) = 1 \mid R_E = r_{Ew,0}]$$

By Lemma 5.17, we have that

$$\Pr_{R,\mathsf{ChE}}[h_{R,\mathsf{ChB},n}(g^*(r_{Ew,0})) = 1 \mid R_E = r_{Ew,0}] = \Pr_{R,\mathsf{ChE}}[h_{R,\mathsf{ChB},n}(g^*(r_E)) = 1 \mid R_E = r_E]$$

Therefore, by definition of $\textsc{Eve}_0$ and σ and applying the above corollary and lemma,

$$\begin{aligned}
\Pr_{R,\mathsf{ChE}}[h_{R,\mathsf{ChB},n}(\textsc{Eve}_0(R_E)) = 1 \mid R_E = r_E] &= \Pr_{R,\mathsf{ChE}}[h_{R,\mathsf{ChB},n}(\sigma(g^*(r_{Ew,0}))) = 1 \mid R_E = \sigma(r_{Ew,0})] \\
&= \Pr_{R,\mathsf{ChE}}[h_{R,\mathsf{ChB},n}(g^*(r_{Ew,0})) = 1 \mid R_E = r_{Ew,0}] \\
&= \Pr_{R,\mathsf{ChE}}[h_{R,\mathsf{ChB},n}(g^*(r_E)) = 1 \mid R_E = r_E]
\end{aligned}$$

Thus, $\textsc{Eve}_0$ has the same probability of success as g^*, so $\textsc{Eve}_0$ is also an optimal strategy.

Finally, for any $r_E \in \mathcal{Z}^n$ and any $\pi \in S_n$, to show that $\textsc{Eve}_0(\pi(r_E)) = \pi(\textsc{Eve}_0(r_E))$, by Remark 5.18 we have that

$$\begin{aligned}
\textsc{Eve}_0(\pi(r_E)) &= \textsc{Eve}_0(\pi(\sigma(r_{Ew,0}))) \\
&= \pi(\sigma(g^*(r_{Ew,0})) \\
&= \pi(\textsc{Eve}_0(\sigma(r_{Ew,0}))) \\
&= \pi(\textsc{Eve}_0(r_E))
\end{aligned}$$

□

5.3.3 Randomized Locations

Consider a probabilistic EVE_1 that on input $r_E \in \mathcal{Z}^n$ deviates slightly from the deterministic EVE_0. For any $z \in \mathcal{Z}$, $y \in \mathcal{Y}$, and input $r_E \in \mathcal{Z}^n$, EVE_0 maps some deterministically chosen subset of size k_{zy} of the y's in r_E to be a z in $\widehat{r}_B$. Instead, EVE_1, will map a random subset of size k_{zy} of the y's in r_E to be a z in $\widehat{r}_B$.

More formally, we define EVE_1 as follows.

$\text{EVE}_1(r_E)$:

1. For each $y \in \mathcal{Y}$ and $z \in \mathcal{Z}$, compute $k_{z,y} = N_z(r_E) \cdot \text{RATIO}_{z \to y}(r_E, \text{EVE}_0(r_E))$.
2. Start with $S = [n]$.
   For each $y \in \mathcal{Y}$ and $z \in \mathcal{Z}$
   (a) Pick a random set $S_{z,y} \subset S \cap \{i \in [n] \mid r_{E,i} = z\}$ such that $|S_{z,y}| = k_{z,y}$.
   (b) Set $\widehat{r}_{B,i} = y$ for all $i \in S_{z,y}$.
   (c) Set $S = S \backslash S_{z,y}$.
3. Output $\widehat{r}_B$.

Remark 5.20. Observe that for any fixed randomness e of EVE_1 and any $r_E \in \mathcal{Z}^n$, then there exists a permutation $\pi_e \in S_n$ such that $\text{EVE}_1(r_E; e) = \pi_e(\text{EVE}_0(r_E))$ where $\pi_e(r_E) = r_E$.

We show that such a probabilistic EVE_1 has the same success probability as EVE_0.

Lemma 5.21.

$$\Pr_{R,\mathsf{ChE},\text{EVE}_1}[h_{R,\mathsf{ChB},n}(\text{EVE}_1(R_E)) = 1] = \Pr_{R,\mathsf{ChE}}[h_{R,\mathsf{ChB},n}(\text{EVE}_0(R_E)) = 1]$$

Proof. It suffices to prove that for all $r_E \in \mathcal{Z}^n$ and randomness e for EVE_1,

$$\Pr_{R,\mathsf{ChE}}[h_{R,\mathsf{ChB},n}(\text{EVE}_1(R_E; e)) = 1 \mid R_E = r_E] = \Pr_{R,\mathsf{ChE}}[h_{R,\mathsf{ChB},n}(\text{EVE}_0(R_E)) = 1 \mid R_E = r_E]$$

Fix some choice of randomness e for EVE_1 and some $r_E \in \mathcal{Z}^n$. By Remark 5.20, there exists a permutation $\pi_e \in S_n$ such that $\text{EVE}_1(r_E; e) = \pi_e(\text{EVE}_0(r_E))$. By our construction of EVE_0 as stated in Lemma 5.19, $\pi_e(\text{EVE}_0(R_E)) = \text{EVE}_0(\pi_e(R_E))$. Therefore,

$$\begin{aligned}
\Pr_{R,\mathsf{ChE}}[h_{R,\mathsf{ChB},n}(\text{EVE}_1(R_E; e)) = 1 \mid R_E = r_E] &= \Pr_{R,\mathsf{ChE}}[h_{R,\mathsf{ChB},n}(\pi_e(\text{EVE}_0(R_E))) = 1 \mid R_E = r_E] \\
&= \Pr_{R,\mathsf{ChE}}[h_{R,\mathsf{ChB},n}(\text{EVE}_0(\pi_e(R_E))) = 1 \mid R_E = r_E] \\
&= \Pr_{R,\mathsf{ChE}}[h_{R,\mathsf{ChB},n}(\text{EVE}_0(R_E)) = 1 \mid R_E = r_E]
\end{aligned}$$

where the last equality follows since $\pi_e(r_E) = r_E$. □

5.3.4 Stochastic Matrix Strategy

Consider a probabilistic EVE_2 that on input $r_E \in \mathcal{Z}^n$ defines a new channel Ch_{r_E} from $\mathcal{Z}$ to $\mathcal{Y}$ such that $p_{r_E}(z \mid y) = \text{RATIO}_{z \to y}(r_E, \text{EVE}_0(r_E))$ and applies this channel to each symbol of r_E to get $\widehat{r}_B$.

$\textsc{Eve}_2(r_E)$:

1. Define a channel Ch_{r_E} from $\mathcal{Z}$ to $\mathcal{Y}$ by stochastic matrix
$$P_{r_E} = [p_{r_E}(y \mid z)]_{z\in\mathcal{Z},y\in\mathcal{Y}} = [\textsc{Ratio}_{z\to y}(r_E, \textsc{Eve}_0(r_E))]_{z\in\mathcal{Z},y\in\mathcal{Y}}$$
2. For $i \in [n]$, set $\widehat{r}_{Bi} = \mathsf{Ch}_{r_E}(r_{Ei})$.
3. Output $\widehat{r}_B$.

We will now prove that $\textsc{Eve}_2$ cannot perform much worse than $\textsc{Eve}_1$. In particular, we will prove that for an overwhelming fraction of $r_E \in \mathcal{Z}^n$, then with probability at least $\frac{1}{\mathsf{poly}(n)}$, $\textsc{Eve}_2(r_E)$ will produce an output that is distributed identically to the distribution of $\textsc{Eve}_1(r_E)$.

First, we prove a fact about multinomial distributions and about R_E.

Claim 5.22. *Let $n \in \mathbb{N}$, let ℓ be a nonnegative constant, and let $p_1 = p_1(n), \ldots, p_\ell = p_\ell(n)$ be such that $\sum_{i=1}^{\ell} p_i = 1$ and $\forall i \in [\ell], p_i \in [0,1]$ and $n \cdot p_i \in \mathbb{N} \cup \{0\}$. Let $X = (X_1, \ldots, X_\ell) \sim \mathsf{Multinomial}(n;\ p_1, p_2, \ldots, p_\ell)$ where X_i is a random variable denoting the number of occurrences of outcome i in n independent trials where $\Pr[\text{outcome } i \text{ occurs in a trial}] = p_i$. Then the probability that each X_i hits its expected value is*

$$\Pr_X\left[\bigwedge_{i=1}^{\ell}(X_i = n \cdot p_i)\right] = \Omega\left(\frac{1}{n^{\ell/2}}\right)$$

Proof. We defer the proof to Appendix B. □

Definition 5.23. *Let $\textsc{Good}_E = \{r_E \in \mathcal{Z}^n \mid \forall z \in \mathcal{Z}, N_z(r_E) \geq \frac{n}{2|\mathcal{X}|} \cdot \max_{x\in\mathcal{X}}(p_E(z|x))\} \subset \mathcal{Z}^n$. Observe that for all $r_E \in \textsc{Good}_E$ and $z \in \mathcal{Z}$, then $N_z(r_E) = \Theta(n)$.*

Lemma 5.24. $\Pr_{R,\mathsf{ChE}}[r_E \in \textsc{Good}_E] \geq 1 - \mathsf{negl}(\lambda)$

Proof. We defer the proof to Appendix B. □

Lemma 5.25. *For all $r_E \in \textsc{Good}_E$, there exists a polynomial $p(n) = O\left(n^{|\mathcal{Z}||\mathcal{Y}|/2}\right)$ such that*

$$\Pr_{R,\mathsf{ChE},\textsc{Eve}_2}[h_{R,\mathsf{ChB},n}(\textsc{Eve}_2(R_E)) = 1 \mid R_E = r_E] \geq \frac{1}{p(n)} \cdot \Pr_{R,\mathsf{ChE},\textsc{Eve}_1}[h_{R,\mathsf{ChB},n}(\textsc{Eve}_1(R_E)) = 1 \mid R_E = r_E]$$

Proof. Fix any $r_E \in \textsc{Good}_E$. We first want to show that with probability at least $\frac{1}{\mathsf{poly}(\lambda)}$, we have that

$$\forall z \in \mathcal{Z}, y \in \mathcal{Y}, \textsc{Ratio}_{z\to y}(r_E, \textsc{Eve}_2(r_E)) = \textsc{Ratio}_{z\to y}(r_E, \textsc{Eve}_0(r_E)).$$

Fix any $z \in \mathcal{Z}$. Let $\mathcal{Y} = (y_1, \ldots, y_{|\mathcal{Y}|})$ and let $V_z = (V_{z,1}, \ldots, V_{z,|\mathcal{Y}|})$ be a random variable over the randomness of $\textsc{Eve}_2$ defined by

$$V_{z,i} = N_z(r_E) \cdot \textsc{Ratio}_{z\to y_i}(r_E, \textsc{Eve}_2(r_E)).$$

For $i \in [|\mathcal{Y}|]$, let $p_i = \textsc{Ratio}_{z\to y_i}(r_E, \textsc{Eve}_0(r_E))$. Now, by definition of $\textsc{Eve}_2$,

$$V_z = (V_{z,1}, \ldots, V_{z,\ell_z}) \sim \mathsf{Multinomial}(N_z(r_E);\ p_1, \ldots, p_{|\mathcal{Y}|}).$$

Then by Claim 5.22 and since $r_E \in \textsc{Good}_E$ implies $N_z(r_E) = \Theta(n)$, then

$$\Pr_V\left[\bigwedge_{i=1}^{\ell_z}(V_{z,i} = N_z(r_E)\cdot p_i)\right] = \Omega\left(\frac{1}{n^{|\mathcal{Y}|/2}}\right).$$

Observe that since $\textsc{Eve}_2$'s choice of $\widehat{r}_{Bi}$ is conditionally independent of $\widehat{r}_{Bj}$ given r_E for $i \neq j$, then for all $z \neq z'$, V_z is independent of $V_{z'}$ given r_E. Therefore,

$$\Pr_V\left[\bigwedge_{z\in\mathcal{Z}}\bigwedge_{i=1}^{\ell_z}(V_{z,i} = N_z(r_E)\cdot p_i)\right] = \Omega\left(\frac{1}{n^{|\mathcal{Z}||\mathcal{Y}|/2}}\right).$$

Now, for a fixed $r_E \in \textsc{Good}_E$, observe that $\bigwedge_{z\in\mathcal{Z}}\bigwedge_{i=1}^{\ell_z}(V_{z,i} = N_z(r_E)\cdot p_i)$ is equivalent to the statement that $\forall z \in \mathcal{Z}, y \in \mathcal{Y}$, $\textsc{Ratio}_{z\to y}(r_E, \textsc{Eve}_2(r_E)) = \textsc{Ratio}_{z\to y}(r_E, \textsc{Eve}_1(r_E))$. Thus, the distribution of $\textsc{Eve}_2(r_E)$ conditioned on this event is uniformly distributed over all $\widehat{r}_B \in \mathcal{Y}^n$ with the property that $\forall z \in \mathcal{Z}, y \in \mathcal{Y}$, $\textsc{Ratio}_{z\to y}(r_E, \widehat{r}_B) = \textsc{Ratio}_{z\to y}(r_E, \textsc{Eve}_0(r_E))$. But this means that conditioned on this event, the distribution of $\textsc{Eve}_2(r_E)$ is identical to the distribution of $\textsc{Eve}_1(r_E)$ and so $\textsc{Eve}_2$ succeeds with equal probability as $\textsc{Eve}_1$. Therefore there exists a polynomial $p(n) = O\left(n^{|\mathcal{Z}||\mathcal{Y}|/2}\right)$ such that

$$\Pr_{R,\mathsf{ChE},\textsc{Eve}_2}[h_{R,\mathsf{ChB},n}(\textsc{Eve}_2(R_E)) = 1 \mid R_E = r_E] \geq \frac{1}{p(n)}\cdot\Pr_{R,\mathsf{ChE},\textsc{Eve}_1}[h_{R,\mathsf{ChB},n}(\textsc{Eve}_1(R_E)) = 1 \mid R_E = r_E].$$

□

Corollary 5.26. *There exists a polynomial $p(n) = O\left(n^{|\mathcal{Z}||\mathcal{Y}|/2}\right)$ such that*

$$p(n)\cdot\Pr_{R,\mathsf{ChE},\textsc{Eve}_2}[h_{R,\mathsf{ChB},n}(\textsc{Eve}_2(R_E)) = 1] + \mathsf{negl}(\lambda) \geq \Pr_{R,\mathsf{ChE},\textsc{Eve}_1}[h_{R,\mathsf{ChB},n}(\textsc{Eve}_1(R_E)) = 1]$$

Proof. For $r_E \in \textsc{Good}_E$, let $p_{r_E}(n)$ be the polynomial for r_E described in Lemma 5.25. Let $p(n) = \max_{r_E\in\textsc{Good}_E}(p_{r_E}(n)) = O\left(n^{|\mathcal{Z}||\mathcal{Y}|/2}\right)$. Then, by Lemma 5.25,

$$\begin{aligned}
&p(n)\cdot\Pr_{R,\mathsf{ChE},\textsc{Eve}_2}[h_{R,\mathsf{ChB},n}(\textsc{Eve}_2(R_E)) = 1] + \Pr[R_E \notin \textsc{Good}_E]\\
&\geq \sum_{r_E\in\textsc{Good}_E}\left(p(n)\cdot\Pr_{R,\mathsf{ChE},\textsc{Eve}_2}[h_{R,\mathsf{ChB},n}(\textsc{Eve}_2(R_E)) = 1 \mid R_E = r_E]\cdot\Pr[R_E = r_E]\right) + \Pr[R_E \notin \textsc{Good}_E]\\
&\geq \sum_{r_E\in\textsc{Good}_E}\left(\frac{p(n)}{p_{r_E}(n)}\cdot\Pr_{R,\mathsf{ChE},\textsc{Eve}_2}[h_{R,\mathsf{ChB},n}(\textsc{Eve}_2(R_E)) = 1 \mid R_E = r_E]\cdot\Pr[R_E = r_E]\right) + \Pr[R_E \notin \textsc{Good}_E]\\
&\geq \Pr_{R,\mathsf{ChE},\textsc{Eve}_2}[h_{R,\mathsf{ChB},n}(\textsc{Eve}_2(R_E)) = 1 \mid R_E \in \textsc{Good}_E] + \Pr[R_E \notin \textsc{Good}_E]\\
&\geq \Pr_{R,\mathsf{ChE},\textsc{Eve}_2}[h_{R,\mathsf{ChB},n}(\textsc{Eve}_2(R_E)) = 1]
\end{aligned}$$

The corollary then follows since $\Pr[R_E \notin \textsc{Good}_E] = \mathsf{negl}(\lambda)$ by Lemma 5.24. □

5.3.5 Input-Independent Strategy

Now, although $\textsc{Eve}_2$'s strategy is to apply a channel Ch_{r_E} to each symbol of her input r_E, the choice of channel she applies is dependent on which r_E she received. To remove this dependence, we construct an $\textsc{Eve}_3$ who in addition to getting input r_E also gets an independent random input w that defines which channel Ch_w that $\textsc{Eve}_3$ should apply to r_E. More formally,

$\textsc{Eve}_3(w, r_E)$:

1. Let $r_{Ew,0} \in \mathcal{Z}^n$ be the lexicographically first vector of weight w.
2. Define a channel Ch_w from $\mathcal{Z}$ to $\mathcal{Y}$ by stochastic matrix
$$P_w = [p_{Y|Z}(y \mid z)]_{z\in\mathcal{Z},y\in\mathcal{Y}} = [\textsc{Ratio}_{z\to y}(r_{Ew,0}, \textsc{Eve}_0(r_{Ew,0}))]_{z\in\mathcal{Z},y\in\mathcal{Y}}$$
3. For $i \in [n]$, set $\widehat{r}_{Bi} = \mathsf{Ch}_w(r_{Ei})$.
4. Output $\widehat{r}_B$.

Notation

- Let $\mathcal{W}_n = \{w = (w_1, \ldots, w_{|\mathcal{Z}|}) \mid \sum_{i=1}^{|\mathcal{Z}|}(w_i) = n\} = \{w \in \mathbb{N}^n \mid w = \mathsf{wt}(r_E) \text{ for some } r_E \in \mathcal{Z}^n\}$ be the set of all weight vectors of $\mathcal{Z}^n$.
- Note that $|\mathcal{W}_n| = \binom{n+|\mathcal{Z}|-1}{|\mathcal{Z}|-1} = \mathsf{poly}(n)$.
- Let W be a random variable uniformly distributed over $\mathcal{W}_n$.

Now, we will show that $\textsc{Eve}_3(\mathsf{wt}(r_E), r_E)$ has the same behavior as $\textsc{Eve}_2(r_E)$.

Lemma 5.27. *For all weights $w \in \mathcal{W}_n$ and all $r_E \in \mathcal{Z}^n$ such that $\mathsf{wt}(r_E) = w$, then*
$$\mathsf{Ch}_w = \mathsf{Ch}_{r_E}$$
where Ch_w is defined as in $\textsc{Eve}_3$ *and Ch_{r_E} is defined as in* $\textsc{Eve}_2$.

Proof. Since for all $r_E \in \mathcal{Z}^n$ and $\pi \in S_n$, $\textsc{Eve}_0(\pi(r_E)) = \pi(\textsc{Eve}_0(r_E))$, then
$$\begin{aligned}[\textsc{Ratio}_{z\to y}(r_E, \textsc{Eve}_0(r_E))]_{z\in\mathcal{Z},y\in\mathcal{Y}} &= [\textsc{Ratio}_{z\to y}(\pi(r_E), \pi(\textsc{Eve}_0(r_E)))]_{z\in\mathcal{Z},y\in\mathcal{Y}} \\ &= [\textsc{Ratio}_{z\to y}(\pi(r_E), \textsc{Eve}_0(\pi(r_E)))]_{z\in\mathcal{Z},y\in\mathcal{Y}}\end{aligned}$$
Therefore, for all $(r_E, r_E') \in \textsc{Eqwt}$, $\mathsf{Ch}_{r_E} = \mathsf{Ch}_{r_E'}$. Thus, $\mathsf{Ch}_w = \mathsf{Ch}_{r_{Ew,0}} = \mathsf{Ch}_{r_E}$. □

Corollary 5.28. *For any $r_E \in \mathcal{Z}^n$, the distribution of* $\textsc{Eve}_3(\mathsf{wt}(r_E), r_E)$ *is the same as the distribution of* $\textsc{Eve}_2(r_E)$.

Proof. This follows directly from Lemma 5.27 by definition of $\textsc{Eve}_2$ and $\textsc{Eve}_3$. □

We claim that given a uniformly randomly chosen weight vector w, $\textsc{Eve}_3$'s probability of success is not much worse than $\textsc{Eve}_2$'s probability of success. This follows since there are only polynomially many possible weight vectors, so with some inverse polynomially probability, the randomly chosen weight w for $\textsc{Eve}_3$ will be equal to $\mathsf{wt}(r_E)$ and thus $\textsc{Eve}_3$ will act identically to $\textsc{Eve}_2$.

Lemma 5.29.
$$\Pr_{R,\mathsf{ChE},\textsc{Eve}_3,W}[h_{R,\mathsf{ChB},n}(\textsc{Eve}_3(W, R_E)) = 1] \geq \frac{1}{q(n)} \cdot \Pr_{R,\mathsf{ChE},\textsc{Eve}_2}[h_{R,\mathsf{ChB},n}(\textsc{Eve}_2(R_E)) = 1]$$
where $q(n) = \binom{n+|\mathcal{Z}|-1}{|\mathcal{Z}|-1} = |\mathcal{W}_n| = \mathsf{poly}(n)$.

Proof.

$$\begin{aligned}
&\Pr_{R,\mathsf{ChE},\textsc{Eve}_3,W}[h_{R,\mathsf{ChB},n}(\textsc{Eve}_3(W,R_E))=1]\\
&=\Pr_{R,\mathsf{ChE},\textsc{Eve}_3,W}[W=\mathsf{wt}(R_E)]\cdot\Pr_{R,\mathsf{ChE},\textsc{Eve}_3,W}[h_{R,\mathsf{ChB},n}(\textsc{Eve}_3(W,R_E))=1\mid W=\mathsf{wt}(R_E)]\\
&=\frac{1}{|\mathcal{W}_n|}\Pr_{R,\mathsf{ChE},\textsc{Eve}_3,W}[h_{R,\mathsf{ChB},n}(\textsc{Eve}_3(W,R_E))=1\mid W=\mathsf{wt}(R_E)]\\
&=\frac{1}{|\mathcal{W}_n|}\Pr_{R,\mathsf{ChE},\textsc{Eve}_2}[h_{R,\mathsf{ChB},n}(\textsc{Eve}_2(R_E))=1]
\end{aligned}$$

where the last equality follows by Corollary 5.28. □

Finally, we prove that $\textsc{Eve}_3$ only succeeds with negligible probability. This step crucially requires that the main channel ChB is not a degradation of Eve's channel ChE. Recall that $\textsc{Good} = \{r \in \mathcal{X}^n \mid \forall x \in \mathcal{X}, N_x(r) \geq \frac{n}{2|\mathcal{X}|}\} \subset \mathcal{X}^n$ and that for all $r \in \textsc{Good}$ and $x \in \mathcal{X}$, then $N_x(r) = \Theta(n)$.

Lemma 5.30.

$$\Pr_{R,\mathsf{ChE},\textsc{Eve}_3,W}[h_{R,\mathsf{ChB},n}(\textsc{Eve}_3(W,R_E))=1]\leq\mathsf{negl}(\lambda)$$

Proof. First,

$$\begin{aligned}
&\Pr_{R,\mathsf{ChE},\textsc{Eve}_3,W}[h_{R,\mathsf{ChB},n}(\textsc{Eve}_3(W,R_E))=1]\\
&\leq\Pr_{R,\mathsf{ChE},\textsc{Eve}_3,W}[h_{R,\mathsf{ChB},n}(\textsc{Eve}_3(W,R_E))=1\mid R\in\textsc{Good}]+\Pr_R[R\notin\textsc{Good}]\\
&\leq\max_{w\in W,r\in\textsc{Good}}\left(\Pr_{R,\mathsf{ChE},\textsc{Eve}_3,W}[h_{R,\mathsf{ChB},n}(\textsc{Eve}_3(W,R_E))=1\mid W=w,R=r]\right)+\Pr_R[R\notin\textsc{Good}]\\
&=\max_{w\in W,r\in\textsc{Good}}\left(\Pr_{\mathsf{ChE},\textsc{Eve}_3}[h_{r,\mathsf{ChB},n}(\textsc{Eve}_3(w,\mathsf{ChE}(r))=1]\right)+\Pr_R[R\notin\textsc{Good}]
\end{aligned}$$

By Lemma 5.7, $\Pr_R[R \notin \textsc{Good}] \leq \mathsf{negl}(\lambda)$, so it suffices to prove that $\forall w \in \mathcal{W}_n$ and $\forall r \in \textsc{Good}$,

$$\Pr_{\mathsf{ChE},\textsc{Eve}_3}[h_{r,\mathsf{ChB},n}(\textsc{Eve}_3(w,\mathsf{ChE}(r))=1]=\mathsf{negl}(\lambda)$$

Fix any $w \in \mathcal{W}_n$ and any $r \in \textsc{Good}$. Let Ch_w be defined by stochastic matrix

$$P_w=[p_w(y\mid z)]_{z\in\mathcal{Z},y\in\mathcal{Y}}=[\textsc{Ratio}_{z\to y}(r_{Ew,0},\textsc{Eve}_0(r_{Ew,0}))]_{z\in\mathcal{Z},y\in\mathcal{Y}}$$

Let $\widehat{R}_{B|r,w}$ be a random variable representing the output of $\textsc{Eve}_3(w, \mathsf{ChE}(r))$. Now, by definition of $\textsc{Eve}_3$, the distribution of each $(\widehat{R}_{B|r,w})_i = \mathsf{Ch}_w(\mathsf{ChE}(r_i))$. In other words, $\widehat{R}_{B|r,w}$ is produced by sending r symbol by symbol through a channel formed by concatenating ChE with Ch_w. Intuitively, since ChB is not a degradation of ChE then this concatenated channel should not emulate ChB well, and therefore we expect some ratio $\textsc{Ratio}_{x\to y}(r, \widehat{R}_{B|r,w})$ to be far from the ratio $p_B(y|x)$ expected by $f_{m,r,\mathsf{ChB},n}$.

Indeed, since ChB is not a degradation of ChE, then by Lemma 3.13 there exists a constant $d > 0$ and $x^* \in \mathcal{X}, y^* \in \mathcal{Y}$ such that

$$|[P_B - P_E \cdot P_w]_{x^*,y^*}| \geq d.$$

Or equivalently, for $p_{E\cdot w}(y^*|x^*) = [P_E \cdot P_w]_{x^*,y^*} = \Pr[\mathsf{Ch}_w(\mathsf{ChE}(x^*)) = y^*]$,

$$|p_B(y^*|x^*) - p_{E\cdot w}(y^*|x^*)| \geq d$$

Therefore, since d is constant,

$$\begin{aligned}
&\Pr_{\mathsf{ChE},\text{EVE}_3}[h_{r,\mathsf{ChB},n}(\text{EVE}_3(w, \mathsf{ChE}(r))) = 1] \\
&\leq \Pr_{\mathsf{ChE},\text{EVE}_3}\left[|\text{RATIO}_{x^*\to y^*}(r, \widehat{R}_{B|r,w}) - p_B(y^*|x^*)| \leq |\mathcal{Y}| \cdot n^{-\frac{1}{3}}\right] \\
&\leq \Pr_{\mathsf{ChE},\text{EVE}_3}\left[|\text{RATIO}_{x^*\to y^*}(r, \widehat{R}_{B|r,w}) - p_{E\cdot w}(y^*|x^*)| \geq |\mathcal{Y}| \cdot n^{-\frac{1}{3}}\right]
\end{aligned}$$

For all $i \in [n]$, define

$$V_i = \begin{cases} 1 \text{ if } r_i = x^* \text{ and } (\widehat{R}_{B|r,w})_i = y^* \\ 0 \text{ else} \end{cases}$$

Let $S_{x^*} = \{i \in [n] \mid r_i = x^*\}$. Then,

$$\begin{aligned}
\forall i \in S_{x^*}, \Pr[V_i = 1] &= p_{E\cdot w}(y^*|x^*) \\
\mathbb{E}\left[\sum_{i\in S_{x^*}} V_i\right] &= N_{x^*}(r) \cdot p_{E\cdot w}(y^*|x^*) \\
\sum_{i\in S_{x^*}} V_i &= N_{x^*}(r) \cdot \text{RATIO}_{x^*\to y^*}(r, \widehat{R}_{B|r,w})
\end{aligned}$$

By a Chernoff bound,

$$\begin{aligned}
&\Pr_{\mathsf{ChE},\text{EVE}_3}\left[|\text{RATIO}_{x^*\to y^*}(r, \widehat{R}_{B|r,w}) - p_{E\cdot w}(y^*|x^*)| \geq |\mathcal{Y}| \cdot n^{-\frac{1}{3}}\right] \\
&= \Pr\left[\left|\sum_{i\in S_{x^*}} V_i - N_{x^*}(r) \cdot p_{E\cdot w}(y^*|x^*)\right| \geq N_{x^*}(r) \cdot |\mathcal{Y}| \cdot n^{-\frac{1}{3}}\right] \\
&\leq 2 \cdot \exp\left(\frac{-N_{x^*}(r) \cdot |\mathcal{Y}|^2 \cdot n^{-2/3}}{3 \cdot p_{E\cdot w}(y^*|x^*)}\right).
\end{aligned}$$

Since $p_{E\cdot w}(y^*|x^*) \leq 1$ and $r \in \text{GOOD}$ implies $N_{x^*}(r) = \Theta(n)$,

$$\Pr\left[\left|\sum_{i\in S_{x^*}} V_i - N_{x^*}(r) \cdot p_{E\cdot w}(y^*|x^*)\right| \geq N_{x^*}(r) \cdot |\mathcal{Y}| \cdot n^{-\frac{1}{3}}\right] \leq 2 \cdot e^{-\Omega(n^{1/3})} = \mathsf{negl}(\lambda).$$

Thus, our lemma holds since for any $w \in \mathcal{W}_n$ and any $r \in \text{GOOD}$,

$$\Pr_{\mathsf{ChE},\text{EVE}_3}[h_{r,\mathsf{ChB},n}(\text{EVE}_3(w, \mathsf{ChE}(r))) = 1] \leq \mathsf{negl}(\lambda)$$

□

5.3.6 Putting it Together

Theorem 5.31. *For all randomized functions $g : \mathcal{Z}^n \to \mathcal{Y}^n$,*

$$\Pr_{R,\mathsf{ChE},g}[h_{R,\mathsf{ChB},n}(g(R_E)) = 1] \leq \mathsf{negl}(\lambda)$$

Proof. By Lemma 5.19, EVE_0 is an optimal strategy so

$$\Pr_{R,\mathsf{ChE},g}[h_{R,\mathsf{ChB},n}(g(R_E)) = 1] \leq \Pr_{R,\mathsf{ChE}}[h_{R,\mathsf{ChB},n}(\text{EVE}_0(R_E)) = 1]$$

Then, by Lemma 5.21, Corollary 5.26, Lemma 5.29, and Lemma 5.30 for some polynomials $p(n), q(n) = \mathsf{poly}(n)$,

$$\begin{aligned}
\Pr_{R,\mathsf{ChE}}[h_{R,\mathsf{ChB},n}(\text{EVE}_0(R_E)) = 1] &= \Pr_{R,\mathsf{ChE},\text{EVE}_1}[h_{R,\mathsf{ChB},n}(\text{EVE}_1(R_E)) = 1] \\
&\leq p(n) \cdot \Pr_{R,\mathsf{ChE},\text{EVE}_2}[h_{R,\mathsf{ChB},n}(\text{EVE}_2(R_E)) = 1] + \mathsf{negl}(\lambda) \\
&\leq p(n) \cdot q(n) \cdot \Pr_{R,\mathsf{ChE},\text{EVE}_3,W}[h_{R,\mathsf{ChB},n}(\text{EVE}_3(W, R_E)) = 1] + \mathsf{negl}(\lambda) \\
&\leq p(n) \cdot q(n) \cdot \mathsf{negl}(\lambda) + \mathsf{negl}(\lambda) \\
&\leq \mathsf{negl}(\lambda)
\end{aligned}$$

□

We now show that this implies that any strategy g can only cause $f_{m,R,\mathsf{ChB},n}$ to output m with negligible probability. This follows from the lemma below:

Lemma 5.32. *For any $r \in \mathcal{X}^n$ and $\widehat{r}_B \in \mathcal{Y}^n$,*

$$\forall x \in \mathcal{X}, y \in \mathcal{Y},\ \text{RATIO}_{x\to y}(r, \widehat{r}_B) \leq p_B(y|x) + n^{-\frac{1}{3}}$$

implies

$$\forall x \in \mathcal{X}, y \in \mathcal{Y},\ |\text{RATIO}_{x\to y}(r, \widehat{r}_B) - p_B(y|x)| \leq |\mathcal{Y}| \cdot n^{-\frac{1}{3}}$$

Proof. Fix any $r \in \mathcal{X}^n$ and $\widehat{r}_B \in \mathcal{Y}^n$. Suppose that $\forall x \in \mathcal{X}, y \in \mathcal{Y},\ \text{RATIO}_{x\to y}(r, g(R_E)) \leq p_B(y|x) + n^{-\frac{1}{3}}$. Then, clearly

$$\forall x \in \mathcal{X}, y \in \mathcal{Y}, \text{RATIO}_{x\to y}(r, \widehat{r}_B) \leq p_B(y|x) + |\mathcal{Y}| \cdot n^{-\frac{1}{3}}$$

Now fix any $x^* \in \mathcal{X}$ and $y^* \in \mathcal{Y}$. Then, by definition of the ratio function,

$$\begin{aligned}
N_{x^*}(r) &= \sum_{y\in\mathcal{Y}} N_{x^*}(r) \cdot \text{RATIO}_{x^*\to y}(r, \widehat{r}_B) \\
1 &= \sum_{y\in\mathcal{Y}} \text{RATIO}_{x^*\to y}(r, \widehat{r}_B)
\end{aligned}$$

This implies

$$\begin{aligned}
\text{RATIO}_{x^*\to y^*}(r, \widehat{r}_B) &= 1 - \sum_{y\neq y^*\in\mathcal{Y}} \text{RATIO}_{x^*\to y}(r, \widehat{r}_B) \\
&\geq 1 - \sum_{y\neq y^*\in\mathcal{Y}} \left(p_B(y|x^*) + n^{-\frac{1}{3}}\right) \\
&= \left(1 - \sum_{y\neq y^*\in\mathcal{Y}} p_B(y|x^*)\right) - \sum_{y\neq y^*\in\mathcal{Y}} n^{-\frac{1}{3}} \\
&= p_B(y^* \mid x^*) - (|\mathcal{Y}| - 1)n^{-\frac{1}{3}}
\end{aligned}$$

Thus,

$$\forall x \in \mathcal{X}, y \in \mathcal{Y}, \textsc{Ratio}_{x\to y}(r, \widehat{r}_B) \geq p_B(y|x) - |\mathcal{Y}| \cdot n^{-\frac{1}{3}}$$

so the claim follows. □

Therefore, we obtain

Theorem 5.33. *For all randomized functions $g : \mathcal{Z}^n \to \mathcal{Y}^n$ and any message $m \in \{0,1\}$,*

$$\Pr_{R,\mathsf{ChE},g}[f_{m,R,\mathsf{ChB},n}(g(R_E)) \neq \perp] \leq \mathsf{negl}(\lambda)$$

Proof. By Theorem 5.31 and Lemma 5.32

$$\begin{aligned}
&\Pr_{R,\mathsf{ChE},g}[f_{m,R,\mathsf{ChB},n}(g(R_E)) \neq \perp] \\
&= \Pr_{R,\mathsf{ChE},g}[\forall x \in \mathcal{X}, y \in \mathcal{Y},\ \textsc{Ratio}_{x\to y}(R, g(R_E)) \leq p_B(y|x) + n^{-\frac{1}{3}}] \\
&\leq \Pr_{R,\mathsf{ChE},g}[\forall x \in \mathcal{X}, y \in \mathcal{Y},\ |\textsc{Ratio}_{x\to y}(R, g(R_E)) - p_B(y|x)| \leq n^{-\frac{1}{3}}] \\
&= \Pr_{R,\mathsf{ChE},g}[h_{R,\mathsf{ChB},n}(g(R_E)) = 1] \leq \mathsf{negl}(\lambda)
\end{aligned}$$

□

We now prove full security.

Theorem 5.34. *For every polynomial query bound $q(\lambda)$ and (computationally unbounded) adversary $\mathcal{A}^{(\cdot)}$ that makes at most $q(\lambda)$ queries to its oracle,*

$$\Pr[\mathcal{A}^{f_{b,r,\mathsf{ChB},n}}(1^\lambda, \mathsf{ChE}(r)) = b \mid (f_{b,r,\mathsf{ChB},n}, r) \leftarrow \mathrm{Enc}_{\mathsf{ChB}}(1^\lambda, b)] \leq \frac{1}{2} + \mathsf{negl}(\lambda)$$

where b is uniformly distributed over $\{0,1\}$.

Proof. Consider any unbounded adversary $\mathcal{A}^{(\cdot)}$ which will make at most a polynomial number $q(n)$ of queries to its oracle. For $i \in \{0,1,2,\ldots,q(n)\}$, define $\mathsf{View}_b^{(i)}$ to be the distribution of views (transcripts) of $\mathcal{A}$ interacting with the oracle $f_{b,r,\mathsf{ChB},n}$ i-times when the challenge bit is b. Let $V_b^{(i)}$ be a random variable over $\mathsf{View}_b^{(i)}$ and define for convenience an indicator $\mathcal{Q} : \mathsf{View}_b^{(i)} \to \{\top, \perp\}$ such that $\mathcal{Q}(v) = \perp$ if and only if $f_{b,r,\mathsf{ChB},n}$ output $\perp$ for all queries in v. For example, the starting view is (r_E) and after a single query $\widehat{r}_{B1}$ to the oracle that returned $\perp$ the view is $(r_E, \widehat{r}_{B1}, \perp)$. Observe that if $\mathcal{A}$ submits no queries to the oracle, then $\mathcal{A}$ is completely unable to distinguish between the $b = 0$ and $b = 1$ case as $v = (r_E)$ is a random string chosen independently from b, so

$$\Pr_{\mathsf{View}_0^{(0)}}\left[V_0^{(0)} = v\right] = \Pr_{\mathsf{View}_1^{(0)}}\left[V_1^{(0)} = v\right]$$

Then the first query $\widehat{r}_{B1}$ is equally like to be chosen regardless of b since the views were identically distributed when $i = 0$. Therefore as long as the oracle does not reveal the message–doing so reveals the challenge bit–the distribution of views is identical.

$$\Pr_{\mathsf{View}_0^{(1)}}\left[V_0^{(1)} = v \mid \mathcal{Q}(v) = \perp\right] = \Pr_{\mathsf{View}_1^{(1)}}\left[V_1^{(1)} = v \mid \mathcal{Q}(v) = \perp\right]$$

Then by induction the ith query is equally likely to be chosen assuming all previous queries do not reveal the message.

$$\Pr_{\mathsf{View}_0^{(q(n))}}\left[V_0^{(q(n))} = v \mid \mathcal{Q}(v) = \perp\right] = \Pr_{\mathsf{View}_1^{(q(n))}}\left[V_1^{(p(n))} = v \mid \mathcal{Q}(v) = \perp\right]$$

Now it remains to show that the probability that $\mathcal{Q}(v) = \perp$ over $v \in \mathsf{View}_b^{(q(n))}$ is negligible. We proceed by a standard union bound strategy. Suppose g_1 is the first randomized strategy that $\mathcal{A}$ uses to produce a query to the oracle. By Theorem 5.33 the probability that any randomized strategy g_1 produces a guess that reveals the message b is negligible:

$$\Pr_{R,\mathsf{ChE},g_1}[f_{b,R,\mathsf{ChB},n}(g_1(r_E)) \neq \perp] \leq \mathsf{negl}(\lambda)$$

Now consider any randomness $(r_1^*, \ldots, r_{i-1}^*)$ needed for generating the first $i-1$ queries of $\mathcal{A}$. Let g_i be the randomized strategy that $\mathcal{A}$ would use to produce the ith query assuming that all of the first $i-1$ queries to the oracle (that would have been generated by $(R_E, r_1^*, \ldots, r_{i-1}^*)$) all returned $\perp$. Again by Theorem 5.33 the probability that any randomized strategy g_i produces a guess that reveals the message b is negligible.

$$\Pr_{R,\mathsf{ChE},g_i}[f_{b,r,\mathsf{ChB},n}(g_i(R_E)) \neq \perp] \leq \mathsf{negl}(\lambda)$$

By a union bound, the probability that $\mathcal{A}$ learns b from any polynomial $q(n)$ number of queries is $q(n) \cdot \mathsf{negl}(\lambda)$. Thus, with probability $1 - q(n) \cdot \mathsf{negl}(\lambda) = 1 - \mathsf{negl}(\lambda)$, $\mathcal{A}$ will not learn b from any oracle query, so

$$\Pr_{\mathsf{View}_b^{(q(n))}}\left[\mathcal{Q}\left(V_b^{(q(n))}\right) = \perp\right] = 1 - \mathsf{negl}(\lambda).$$

In other words, $\mathcal{A}$ can only distinguish between $b = 0$ and $b = 1$ when $\mathcal{Q}(V_b^{(q(n))}) = \top$, but this occurs with $\mathsf{negl}(\lambda)$ probability. □

6 Universal Coding Schemes

A universal coding scheme for a main channel ChB is a wiretap coding scheme that allows decoding for Bob but is secure against any eavesdropping channel ChE from some set $\mathcal{E}$.

Definition 6.1 (Secure $(\mathsf{ChB}, \mathcal{E})$-universal coding scheme)**.** *A statistically secure (resp. computationally secure, resp. bounded query secure in the ideal obfuscation model)* $(\mathsf{ChB}, \mathcal{E})$*-universal coding scheme for channel* ChB*, a class of eavesdropping channels* $\mathcal{E}$*, and message space* $\mathcal{M}$ *is a wiretap coding scheme* $(\mathrm{Enc}, \mathrm{Dec})$ *that is a statistically secure (resp. computationally secure, resp. bounded query secure in the ideal obfuscation model) wiretap coding scheme for all wiretap channels in the set* $\{(\mathsf{ChB}, \mathsf{ChE}) \mid \mathsf{ChE} \in \mathcal{E}\}$ *and for message space* $\mathcal{M}$*.*

6.1 Our Construction is a Universal Coding Scheme in the Ideal Oracle Model

We observe that for any channel ChB, our wiretap coding scheme $(\mathrm{Enc}_{\mathsf{ChB}}, \mathrm{Dec}_{\mathsf{ChB}})$ in the ideal oracle model gives us a universal coding scheme against all eavesdropping channels for which secure wiretap coding schemes are possible. Recall, that if ChB is a degradation of ChE, then no secure wiretap coding scheme is possible since the adversary can simulate anything that ChB produces.

Theorem 6.2. *Let* ChB *be any channel and let*

$$\mathsf{Not\text{-}Degraded}(\mathsf{ChB}) = \{\mathsf{ChE} \mid \mathsf{ChB} \textit{ is not a degradation of } \mathsf{ChE}\}.$$

Then, $(\mathrm{Enc}_{\mathsf{ChB}}, \mathrm{Dec}^{(\cdot)}_{\mathsf{ChB}})$ *is a bounded query secure* $(\mathsf{ChB}, \mathsf{Not\text{-}Degraded}(\mathsf{ChB}))$ *wiretap coding scheme in the ideal oracle model.*

Proof. The proof follows by Corollary 5.4 and the observation that $(\mathrm{Enc}_{\mathsf{ChB}}, \mathrm{Dec}^{(\cdot)}_{\mathsf{ChB}})$ only depend on ChB. □

6.2 Universal Coding Schemes in the Information Theoretic Setting

In contrast, in the information theoretic setting, there exist channels ChB for which there is no positive rate universal coding schemes against all channels ChE that are not less noisy than ChB. Recall that there exist positive rate statistically secure wiretap codings for general message spaces for wiretap channel $(\mathsf{ChB}, \mathsf{ChE})$ if and only if ChE is not less noisy than ChB (Theorem 4.17).

Remark 6.3. As we are considering positive rate wiretap codings, we consider universality with respect to the definition of statistically secure wiretap codings for general message spaces (see Section 4.4).

We consider a simple example where both ChB and ChE are BSC channels. Note that if $\mathsf{ChB} = \mathsf{BSC}_p$ and $\mathsf{ChE} = \mathsf{BSC}_{p'}$ with $p' > p$, then ChE is a degradation of ChB and therefore not less noisy than ChB.

Theorem 6.4. *There is no positive rate statistically secure* $(\mathsf{ChB}, \mathcal{E})$*-universal coding scheme, where* $\mathsf{ChB} = \mathsf{BSC}_p$ *and* $\mathcal{E} = \{\mathsf{BSC}'_p : p' > p\}$.

Proof. Suppose for sake of contradiction that $(\mathrm{Enc}, \mathrm{Dec})$ is a statistically secure $(\mathsf{ChB}, \mathcal{E})$-universal coding scheme with rate $R > 0$ for some message space $\mathcal{M}$. Now, the secrecy capacity of a $(\mathsf{ChB} = \mathsf{BSC}_p, \mathsf{ChE} = \mathsf{BSC}_{p'})$ wiretap channel is the difference of their capacities, namely $C_s(\mathsf{BSC}_p, \mathsf{BSC}_{p'}) = h_2(p') - h_2(p)$ [Mau93]. Thus, for any $\varepsilon > 0$, there exists a parameter $p_\varepsilon > 0.1$ such that $C_s(\mathsf{BSC}_{0.1}, \mathsf{BSC}_{p_\varepsilon}) = \varepsilon$. Choose any positive $\varepsilon' < R$. Then, $\mathsf{BSC}_{p_{\varepsilon'}} \in \mathcal{E}$ and $C_s(\mathsf{BSC}_p, \mathsf{BSC}_{p_{\varepsilon'}}) < R$. But by definition of secrecy capacity, this means that a wiretap coding scheme with rate $R > C_s$ cannot satisfy both CK correctness and security. But since CK correctness and security are weaker than requiring overwhelming correctness and semantic security, then this means that $(\mathrm{Enc}, \mathrm{Dec})$ cannot be a statistically secure wiretap coding scheme for $(\mathsf{BSC}_p, \mathsf{BSC}_{p_{\varepsilon'}})$, which is a contradiction. □

Theorem 6.4 shows that in general, there are no positive rate statistically secure universal coding schemes for every channel ChB against all channels that are not less noisy than ChB. We conjecture that outside this case there are many settings in which there are no positive rate statistically secure universal coding schemes. To prove this conjecture, it suffices to show that for any main channel ChB and any $\varepsilon > 0$, there exists a channel ChE_ε whose secrecy capacity with ChB is equal to ε.

7 Instantiating the Oracle via Obfuscation

7.1 Obfuscation Definitions

We now give obfuscation definitions that suffice for building computationally secure wiretap coding schemes. Crucially, we will use the fact that the function classes we are obfuscating are *statistically*

evasive – that is, even given the information that Eve receives over her channel, it is infeasible for (even a computationally unbounded) Eve to find even one input that causes the function to output anything but 0. We formalize this notion now.

Definition 7.1 (Statistically Evasive Circuit Collection with Auxiliary Input)**.** *A statistically evasive circuit collection with auxiliary input $(\mathscr{F}, \mathscr{G})$ is defined by*

- *a collection $\mathscr{F} = \{\mathcal{C}_\lambda\}_{\lambda \in \mathbb{N}}$ of circuits such that each $C \in \mathcal{C}_\lambda$ maps λ input bits to a single output bit and has size $\mathsf{poly}(\lambda)$*
- *a collection $\mathscr{G}$ of pairs (D, Aux) where D is a PPT sampler that takes as input the security parameter 1^λ and output circuits from $\mathcal{C}_\lambda$, and Aux is a PPT auxiliary input generator that takes as input the security parameter 1^λ and a circuit in $\mathcal{C}_\lambda$ and outputs an auxiliary input*

such that for every computationally unbounded oracle machine $\mathcal{A}^{(\cdot)}$ that is limited to polynomially many queries to the oracle, and for every $(D, \mathsf{Aux}) \in \mathscr{G}$, there exists a negligible function μ such that for every $\lambda \in \mathbb{N}$,

$$\Pr_{C \leftarrow D(1^\lambda)} \left[C\left(\mathcal{A}^C\left(1^\lambda, \mathsf{Aux}(1^\lambda, C)\right)\right) = 1 \right] \leq \mu(\lambda).$$

Obfuscation for evasive functions has been studied in several works, most relevantly for us in [BBC+14, BMSZ16]. We stress that while there are impossibility results for several definitions of obfuscation, there are no impossibility results known for obfuscation of statistically evasive circuits with auxiliary input. Indeed, this is for good reason: all known impossibilities for obfuscating circuits involve either: *(i)* providing (computationally hiding) obfuscations as auxiliary input [GK05], which is ruled out in the statistically evasive case; or *(ii)* "feeding an obfuscated circuit to itself" [BGI+01] which requires a non-evasive circuit family. Beyond merely avoiding impossibilities, both the circuit families that we are obfuscating and the auxiliary inputs we are considering are quite natural, and there are multiple natural avenues for instantiating our obfuscation using previous work.

In particular, we consider essentially Definition 2.3 from [BMSZ16], which is itself a generalization of the standard average-case VBB definition of obfuscation [BGI+01], but extended to consider auxiliary input. The work of [BMSZ16] gives a construction achieving this definition for evasive functions based on multilinear map candidates [GGH13, CLT13], that remain secure even in light of all known attacks on multilinear map candidates (when instantiated with sufficiently large security parameters). Below, we also comment that the recent construction of indistinguishability obfuscation from well-studied assumptions [JLS21] also gives a plausible candidate for obfuscating our oracle.

Here, our definition slightly extends the average-case VBB definition given in [BMSZ16] only in that we consider security with respect to a class of possibly randomized auxiliary input generators as opposed to a single deterministic auxiliary input generator. The proof of security in [BMSZ16] is oblivious to this change. We also restrict our notion of obfuscation to statistically evasive circuits collections with auxiliary input.

Definition 7.2 (Average-Case Virtual Black Box Obfuscation for Statistically Evasive Circuit Collections with Auxiliary Input)**.** *Consider a statistically evasive circuit collection with auxiliary input, $(\mathscr{F}, \mathscr{G})$ where $\mathscr{F} = \{\mathcal{C}_\lambda\}_{\lambda \in \mathbb{N}}$ and $\mathscr{G}$ are defined as in Definition 7.1. A uniform PPT algorithm Obf is an average-case virtual black box obfuscator for $(\mathscr{F}, \mathscr{G})$ if there exist negligible functions ϵ and μ such that*

- ***Correctness**: For all $\lambda \in \mathbb{N}$, every circuit $C \in \mathcal{C}_\lambda$, and every input y to C,*

$$\Pr\left[\mathsf{Obf}(1^\lambda, C)(y) \neq C(y)\right] \leq \epsilon(\lambda)$$

- ***$\mathscr{G}$-VBB Security**: For all non-uniform polynomial time adversaries $\mathcal{A}$, there exists a non-uniform polynomial time oracle algorithm $\mathsf{Sim}^{(\cdot)}$ such that for all $\lambda \in \mathbb{N}$ and for every $(D, \mathsf{Aux}) \in \mathscr{G}$,*

$$\Big| \Pr_{C \leftarrow D(1^\lambda)}[\mathcal{A}(1^\lambda, \mathsf{Obf}(1^\lambda, C), \mathsf{Aux}(1^\lambda, C)) = 1] - \Pr_{C \leftarrow D(1^\lambda)}[\mathsf{Sim}^C(1^\lambda, 1^{|C|}, \mathsf{Aux}(1^\lambda, C)) = 1] \Big| \leq \mu(\lambda)$$

7.2 Fuzzy Point Function Obfuscation for the BSC-BEC Case

As a warm-up we consider fuzzy point function obfuscation which suffices when the main channel is a BSC_p channel and Eve's channel is a BEC_ϵ channel such that $\epsilon > 2p$. Notably this fuzzy point function solution uses only Hamming distance. Therefore this solution is based on a standard definition of fuzzy point functions.

Notation Define $\Delta_H(x, y)$ for two binary strings x, y to be the Hamming distance between x and y.

Definition 7.3 (Fuzzy Point Function (FPF))**.** *A fuzzy point function $\mathsf{fuzzy}_{b,x,\delta,n} : \{0,1\}^n \to \{0,1\}$ contains a hardcoded bit $b \in \{0,1\}$ and $x \in \{0,1\}^n$, and takes as input $y \in \{0,1\}^n$. If the Hamming distance $\Delta_H(x, y)$ is less than $n\delta$, then $\mathsf{fuzzy}_{b,x,\delta,n}$ outputs b. Otherwise, $\mathsf{fuzzy}_{b,x,\delta,n}$ outputs 0.*

Consider again the wiretap channel $(\mathsf{ChB}, \mathsf{ChE}) = (\mathsf{BSC}_p, \mathsf{BEC}_\epsilon)$. Recall that in our ideal obfuscation model construction from Section 5, our wiretap coding scheme uses an encoder $\mathrm{Enc}_{\mathsf{BSC}_p}$ that outputs a description of a circuit computing $f_{m,r,\mathsf{BSC}_p,n}$ where $n = \lambda$, $m \in \{0,1\}$, and $r \leftarrow \{0,1\}^n$. This function checks if its input r_B is in the set

$$S_{r,p,n} \triangleq \{r' \in \{0,1\}^n : \forall i, j \in \{0,1\}, \textsc{Ratio}_{i \to j}(r, r') \leq \delta_{ij} p + (1 - \delta_{ij})(1 - p) + n^{-\frac{1}{3}}\}.$$

where δ_{ij} is the Kronecker-delta and outputs m if $r_B \in S_{r,p,n}$ and 0 otherwise.[5] This function is not a fuzzy point function; however, we show below that there exists a fuzzy point function that suffices for constructing a secure wiretap coding scheme. This arises from the observation that every string in $S_{r,p,n}$ has no more than $pn + n^{2/3}$ bit flips.

An Alternate Fuzzy Point Function Solution

Definition 7.4. *Let $g_{m,r,p,n} : \{0,1\}^n \to \{0,1\}$ be the fuzzy point function which outputs $m \in \{0,1\}$ if the input is contained in the set*

$$A_{r,p,n} \triangleq \{r' \in \mathcal{Y}^n : \Delta_H(r', r) \leq pn + n^{2/3}\}$$

and 0 otherwise. Note that $g_{m,r,p,n} = \mathsf{fuzzy}_{m,r,p+n^{-1/3},n}$

[5] Here we use Remark 5.5 to assume $f_{m,r,\mathsf{BSC}_p,n}$ has binary output.

Remark 7.5 ($S_{r,p,n} \subsetneq A_{r,p,n}$)**.** Observe that $S_{r,p,n} \subsetneq A_{r,p,n}$. Let $N_0(r)$ be the number of 0's in r. If $r' \in S_{r,p,n}$, then the number of additional flips over the expected number pn of flips is

$$N_0(r) \cdot \left|\textsc{Ratio}_{0\to1}(r,r') - p\right| + (n - N_0(r)) \cdot \left|\textsc{Ratio}_{1\to0}(r,r') - p\right| \leq n^{2/3}.$$

Thus, the total number of flips is less than $pn + n^{2/3}$. The reverse inclusion does not hold: There exist strings in $A_{r,p,n}$ that are not in $S_{r,p,n}$: for example $r = 0^n$ is in $A_{0^n,p,n}$, but not in $S_{0^n,p,n}$.

Definition 7.6 (FPF Function Class and Sampler)**.** *For $p \in [0, \frac{1}{2})$, define a class of FPFs $\mathscr{P}_p = \{\mathscr{P}_{p,n}\}_{n\in\mathbb{N}}$ by*

$$\mathscr{P}_{p,n} = \{g_{m,r,p,n}\}_{r\in\{0,1\}^n, m\in\{0,1\}}$$

For $m \in \{0,1\}$, we define $D_{m,p}$ to be a PPT circuit sampler for $\mathscr{P}$ such that

$$D_{m,p}(1^n) \text{ outputs a uniformly random circuit from } \{g_{m,r,p,n}\}_{r\in\{0,1\}^n}.$$

Definition 7.7 (FPF Wiretap Auxiliary Input Generator)**.** *For $p \in [0, \frac{1}{2})$, we define a class of auxiliary input generators for $\mathscr{P}_p$ by*

$$\mathscr{A}_{\mathsf{BSC}_{\epsilon>2p}} \triangleq \{\mathsf{Aux}_{\mathsf{BEC}_\epsilon} \mid \epsilon > 2p\}$$

where

$$\mathsf{Aux}_{\mathsf{BEC}_\epsilon}(1^n, g_{m,r,p,n}) \text{ outputs } \mathsf{BEC}_\epsilon(r)$$

Lemma 7.8 (Wiretap Fuzzy Point Functions are Statistically Evasive with Auxiliary Input)**.** *For every $p \in [0, \frac{1}{2})$, $(\mathscr{P}_p, \mathscr{G}_p)$ where $\mathscr{G}_p = \{D_{0,p}, D_{1,p}\} \times \mathscr{A}_{\mathsf{BSC}_{\epsilon>2p}}$ is a statistically evasive circuit collection with auxiliary input.*

Proof. Let $p \in [0, \frac{1}{2})$. Using the definition of statistically evasive circuit collections and the definitions of $(\mathscr{P}_p, \mathscr{G}_p)$, it suffices to show that for all $n \in \mathbb{N}$, $m \in \{0,1\}$, $\epsilon > 2p$, and for every computationally unbounded oracle machine $\mathcal{A}^{(\cdot)}$ that is limited to polynomially many queries to the oracle,

$$\Pr[g_{m,R,p,n}(\mathcal{A}^{g_{m,R,p,n}}(1^n, \mathsf{BEC}_\epsilon(R))) = 1] \leq \mathsf{negl}(n)$$

where R is a uniform random variable over $\{0,1\}^n$. First, we show that no adversary given a single query to $g_{m,R,p,n}$ can cause $g_{m,R,p,n}$ to output 1 with more than negligible probability.

Claim 7.9. *Let $n \in \mathbb{N}$, $p \in [0, \frac{1}{2})$, and $\epsilon > 2p$. Let R be a uniform random variable over $\{0,1\}^n$. For any randomized function $\mathcal{A}$,*

$$\Pr_{R,\mathsf{BEC}_\epsilon,\mathcal{A}}\left[\Delta_H(R, \mathcal{A}(\mathsf{BEC}_\epsilon(R))) \leq n^{2/3} + pn\right] \leq \mathsf{negl}(n)$$

Proof. Choose $\eta', \eta'' > 0$ to be some small enough constants such that $(1-\eta')\left(\frac{\epsilon}{2}\right) > (1+\eta'') \cdot p$. Such constants exist since $\epsilon > 2p$. Let η be a constant such that $0 < \eta < \eta'$. By a Chernoff bound $\mathsf{BEC}_\epsilon(R)$ contains with overwhelming probability at least $(1-\eta)(\epsilon \cdot n)$ erasures. $\mathcal{A}$'s best strategy is to guess randomly on the erasures, resulting with overwhelming probability (by Chernoff) an output string with Hamming distance from R at least $(1-\eta')\left(\frac{\epsilon\cdot n}{2}\right)$. Then,

$$\Pr_{R,\mathsf{BEC}_\epsilon,\mathcal{A}}\left[\Delta_H(R, \mathcal{A}(\mathsf{BEC}_\epsilon(R))) > (1-\eta')\left(\frac{\epsilon \cdot n}{2}\right)\right] \geq 1 - \mathsf{negl}(n).$$

But since $(1-\eta')\left(\frac{\epsilon\cdot n}{2}\right) > (1+\eta'')(pn) > pn + n^{2/3}$ for sufficiently large n,

$$\Pr_{R,\mathsf{BEC}_\epsilon,\mathcal{A}}\left[\Delta_H(R, \mathcal{A}(\mathsf{BEC}_\epsilon(R))) \leq n^{2/3} + pn\right] \leq \mathsf{negl}(n).$$

□

Then, by using the above claim and a similar proof as in Theorem 5.34, we obtain security against an adversary that is given polynomially many queries to $g_{m,R,p,n}$. □

Theorem 7.10. *Let $p \in [0, \frac{1}{2})$. If there exists an average-case virtual black box with auxiliary input obfuscator Obf_p for $(\mathscr{P}_p, \mathscr{G}_p)$ where $\mathscr{G}_p = \{D_{0,p}, D_{1,p}\} \times \mathscr{A}_{\mathsf{BSC}_{\epsilon > 2p}}$, then there exists a computationally secure wiretap coding scheme for every $(\mathsf{BSC}_p, \mathsf{BEC}_\epsilon)$-wiretap channel where $\epsilon > 2p$.*

Proof. Let $(\mathsf{BSC}_p, \mathsf{BEC}_\epsilon)$ be a wiretap channel where $p \in [0, \frac{1}{2})$ and $\epsilon > 2p$. Let Obf_p be an average-case virtual black box with auxiliary input obfuscator for $(\mathscr{P}_p, \mathscr{G}_p)$. Let $\mathsf{ECC} = (\mathsf{ECC}.\mathrm{Enc}, \mathsf{ECC}.\mathrm{Dec})$ be a sufficiently strong error correcting code for BSC_p such that for all $x \in \{0,1\}^*$,

$$\Pr[\mathsf{ECC}.\mathrm{Dec}(1^\lambda, \mathsf{BSC}_p(\mathsf{ECC}.\mathrm{Enc}(1^\lambda, x))) = x] \geq 1 - \mathsf{negl}(\lambda)$$

We define the following wiretap coding scheme $(\mathrm{Enc}_p, \mathrm{Dec}_p)$. Recall that Alice sends a message $m \in \{0,1\}$ to Bob by sending $\mathrm{Enc}_p(1^\lambda, m)$ over BSC_p and BEC_ϵ to Bob and Eve respectively. Bob decodes his channel's output using Dec_p.

- Enc_p takes as input a security parameter 1^λ and a message $m \in \{0,1\}$, and sets $n = \lambda$. The encoder outputs a uniformly random chosen $r \in \{0,1\}^n$, and an error-correcting encoding $\mathcal{E} = \mathsf{ECC}.\mathrm{Enc}(1^n, \mathsf{Obf}_p(1^n, g_{m,r,p,n}))$ of the obfuscation of the circuit description of $g_{m,r,p,n}$ from Definition 7.4.
- Dec_p takes as input a security parameter 1^λ, the noisy encoding $\widehat{\mathcal{E}} = \mathsf{ChB}(\mathcal{E})$, and a string $r_B = \mathsf{ChB}(r)$. The decoder first uses the error-correcting code to decode $\widehat{\mathcal{E}}$ to $\mathsf{Obf}_p(1^n, g_{m,r,p,n})$ and then outputs $(\mathsf{Obf}_p(1^n, g_{m,r,p,n}))(r_B)$.

Observe that $\Pi_p = (\mathrm{Enc}_p, \mathrm{Dec}_p)$ above is essentially the same as the ideal oracle model construction $\Pi_{\mathsf{BSC}_p} = (\mathrm{Enc}_{\mathsf{BSC}_p}, \mathrm{Dec}_{\mathsf{BSC}_p})$ from Section 5 except that we have replaced the oracle for $f_{m,r,\mathsf{BSC}_p,n}$ with an error correcting encoding of the obfuscation of $g_{m,r,p,n}$.

For correctness, first observe that by correctness of the error correcting code and the obfuscation, the decoder outputs a value equal to $g_{m,r,p,n}(r_B) = g_{m,r,p,n}(\mathsf{ChB}(r))$ except with negligible probability. By Remark 7.5, for any r and m, the set of strings $S_{r,p,n}$ on which the original function $f_{m,r,\mathsf{ChB},n}$ from the ideal obfuscation model construction outputs bit m is a subset of the set of strings $A_{r,p,n}$ on which $g_{m,r,p,n}$ outputs the bit m. Therefore,

$$\Pr_{R,\mathsf{ChB}}[f_{m,R,\mathsf{BSC}_p,n}(\mathsf{ChB}(R)) = m] \leq \Pr_{R,\mathsf{ChB}}[g_{m,R,p,n}(\mathsf{ChB}(R)) = m]$$

Then we note by Theorem 5.8 that

$$\Pr_{R,\mathsf{ChB}}[f_{m,R,\mathsf{BSC}_p,n}(\mathsf{ChB}(R)) = m] \geq 1 - \mathsf{negl}(\lambda)$$

Therefore, for all $m \in \{0,1\}$,

$$\Pr[\mathrm{Dec}_p(1^\lambda, \mathsf{ChB}(\mathrm{Enc}_p(1^\lambda, m))) = m] \geq 1 - \mathsf{negl}(\lambda)$$

For semantic security, the proof is nearly identical to the proof we will later show for generalized fuzzy point functions in Theorem 7.17, so we omit it here. □

7.3 Generalized Fuzzy Point Function Obfuscation

In general wiretap settings, a fuzzy point function obfuscation does not suffice to produce secure wiretap coding schemes. Thus, we define a generalization of fuzzy point functions that do suffice.

Definition 7.11 (Generalized Fuzzy Point Function (GFPF))**.** *Let $\mathcal{X}$ and $\mathcal{Y}$ be finite alphabets. For a value $n \in \mathbb{N}$, a message $m \in \{0,1\}$, a string $r \in \mathcal{X}^n$, a parameter $\delta \in [0,1]$, and a stochastic matrix $P = [p(y \mid x)]_{x,y \in \mathcal{X} \times \mathcal{Y}}$, the generalized fuzzy point function $f_{m,r,P,n,\delta} : \mathcal{Y}^n \to \{0,1\}$ is defined as*

$f_{m,r,P,n,\delta}(r_B)$*:*

1. *If for all alphabet pairs $(x,y) \in \mathcal{X} \times \mathcal{Y}$ such that $\textsc{Ratio}_{x \to y}(r, r_B) \leq p(y \mid x) + \delta$, then output m.*
2. *Otherwise output 0.*

As we will only be concerned with the case where $\delta = n^{-1/3}$ and P is some stochastic matrix for a channel ChB, we define the following:

Definition 7.12. *Let ChB be a channel with stochastic matrix P_B. We define*

$$f_{m,r,\mathsf{ChB},n} = f_{m,r,P_B,n,n^{-1/3}}.$$

Remark 7.13. The definition above is identical to the definition for the function with the same notation used in Section 5.[6]

Definition 7.14 (GFPF Function Class and Sampler)**.** *For a channel ChB, we define a class of GFPFs $\mathscr{F}_{\mathsf{ChB}} = \{\mathscr{F}_{\mathsf{ChB},n}\}_{n \in \mathbb{N}}$ by*

$$\mathscr{F}_{\mathsf{ChB},n} = \{f_{m,r,\mathsf{ChB},n}\}_{r \in \mathcal{X}^n, m \in \{0,1\}}.$$

For $m \in \{0,1\}$, we define $D_{m,\mathsf{ChB}}$ to be a PPT circuit sampler such that

$$D_{m,\mathsf{ChB}}(1^n) \text{ outputs a uniformly random circuit from } \{f_{m,r,\mathsf{ChB},n}\}_{r \in \mathcal{X}^n}.$$

Definition 7.15 (GFPF Wiretap Auxiliary Input Generator)**.** *For a channel $\mathsf{ChB} : \mathcal{X} \to \mathcal{Y}$, we define a class of auxiliary input generators*

$$\mathscr{A}_{\mathsf{ChB}} = \{\mathsf{Aux}_{\mathsf{ChE}} \mid \text{channel } \mathsf{ChE} : \mathcal{X} \to \mathcal{Z} \text{ such that } \mathsf{ChB} \text{ is not a degradation of } \mathsf{ChE}\}$$

where

$$\mathsf{Aux}_{\mathsf{ChE}}(1^n, f_{m,r,\mathsf{ChE},n}) \text{ outputs } \mathsf{ChE}(r)$$

Lemma 7.16 (Wiretap Generalized Fuzzy Point Functions are Statistically Evasive with Auxiliary Input)**.** *For every channel ChB, $(\mathscr{F}_{\mathsf{ChB}}, \mathscr{G}_{\mathsf{ChB}})$ where $\mathscr{G}_{\mathsf{ChB}} = \{D_{0,\mathsf{ChB}}, D_{1,\mathsf{ChB}}\} \times \mathscr{A}_{\mathsf{ChB}}$ is a statistically evasive circuit collection with auxiliary input.*

Proof. Let ChB be any channel, and let $\mathcal{X}$ be the input domain of ChB. Using the definition of statistically evasive circuit collections and the definitions of $(\mathscr{F}_{\mathsf{ChB}}, \mathscr{G}_{\mathsf{ChB}})$, it suffices to show that for all $n \in \mathbb{N}$, $m \in \{0,1\}$, channels ChE such that ChB is not a degradation of ChE, and for every

[6] Here we use Remark 5.5 to assume $f_{m,r,\mathsf{ChB},n}$ has binary output.

computationally unbounded oracle machine $\mathcal{A}^{(\cdot)}$ that is limited to polynomially many queries to the oracle,

$$\Pr[f_{m,R,p,n}(\mathcal{A}^{f_{m,R,p,n}}(1^n, \mathsf{ChE}(R))) = 1] \leq \mathsf{negl}(n)$$

where R is a uniform random variable over $\mathcal{X}^n$. The proof then follows directly from Theorem 5.34. □

Theorem 7.17. *Let* ChB *be a channel. If there exists an average-case virtual black box with auxiliary input obfuscator* $\mathsf{Obf}_{\mathsf{ChB}}$ *for* $(\mathscr{F}_{\mathsf{ChB}}, \mathscr{G}_{\mathsf{ChB}})$ *where* $\mathscr{G}_{\mathsf{ChB}} = \{D_{0,\mathsf{ChB}}, D_{1,\mathsf{ChB}}\} \times \mathscr{A}_{\mathsf{ChB}}$*, then there exists a computationally secure wiretap coding scheme for every* $(\mathsf{ChB}, \mathsf{ChE})$*-wiretap channel where* ChE *is not a degradation of* ChB*.*

Proof. Let $(\mathsf{ChB}, \mathsf{ChE})$ be a wiretap channel where ChE is not a degradation of ChB. Let $\mathsf{Obf}_{\mathsf{ChB}}$ be an average-case virtual black box with auxiliary input obfuscator for $(\mathscr{F}_{\mathsf{ChB}}, \mathscr{G}_{\mathsf{ChB}})$. Let $\mathsf{ECC} = (\mathsf{ECC.Enc}, \mathsf{ECC.Dec})$ be a sufficiently strong error correcting code for ChB such that for all $x \in \{0,1\}^*$,

$$\Pr[\mathsf{ECC.Dec}(1^\lambda, \mathsf{ChB}(\mathsf{ECC.Enc}(1^\lambda, x))) = x] \geq 1 - \mathsf{negl}(\lambda)$$

We define the following wiretap coding scheme dependent only on ChB. Recall that Alice sends a message $m \in \{0,1\}$ to Bob by sending $\mathrm{Enc}(1^\lambda, m)$ over ChB and ChE to Bob and Eve respectively. Bob decodes his channel's output using Dec.

- Enc takes as input a security parameter 1^λ and a message $m \in \{0,1\}$, and sets $n = \lambda$. The encoder outputs a uniformly random $r \in \mathcal{X}^n$, and an error-correcting encoding $\mathcal{E} = \mathsf{ECC.Enc}(1^n, \mathsf{Obf}_{\mathsf{ChB}}(1^n, f_{m,r,\mathsf{ChB},n}))$ of the obfuscation of the circuit description of $f_{m,r,\mathsf{ChB},n}$ from Definition 7.12.
- Dec takes as input a security parameter 1^λ, the noisy encoding $\widehat{\mathcal{E}} = \mathsf{ChB}(\mathcal{E})$, and a string $r_B = \mathsf{ChB}(r)$. The decoder first uses the error-correcting code to decode $\widehat{\mathcal{E}}$ to $\mathsf{Obf}_{\mathsf{ChB}}(1^n, f_{m,r,\mathsf{ChB},n})$ and then outputs $(\mathsf{Obf}_{\mathsf{ChB}}(1^n, f_{m,r,\mathsf{ChB},n}))(r_B)$.

Observe that $\Pi = (\mathrm{Enc}, \mathrm{Dec})$ above is essentially the same as the ideal oracle model construction $\Pi_{\mathsf{ChB}} = (\mathrm{Enc}_{\mathsf{ChB}}, \mathrm{Dec}_{\mathsf{ChB}})$ from Section 5 except that we have replaced the oracle for $f_{m,r,\mathsf{ChB},n}$ with an error correcting encoding of the obfuscation of $f_{m,r,\mathsf{ChB},n}$.

For correctness, first observe that by correctness of the error correcting code and the obfuscation, the decoder outputs a value equal to $f_{m,r,\mathsf{ChB},n}(r_B) = f_{m,r,\mathsf{ChB},n}(\mathsf{ChB}(r))$ except with negligible probability. Thus, with high probability, Dec outputs the same value as $\mathrm{Dec}_{\mathsf{ChB}}$, so correctness follows by Theorem 5.8.

Now we analyze the semantic security of the encoding scheme. Recall semantic security requires:

$$\Pr[\mathcal{A}(1^\lambda, \mathsf{ChE}(\mathrm{Enc}(1^\lambda, b))) = b] \leq \frac{1}{2} + \mathsf{negl}(\lambda).$$

Note that this is equivalent to requiring

$$\left|\Pr[\mathcal{A}(1^\lambda, \mathsf{ChE}(\mathrm{Enc}(1^\lambda, 0))) = 1] - \Pr[\mathcal{A}(1^\lambda, \mathsf{ChE}(\mathrm{Enc}(1^\lambda, 1))) = 1]\right| \leq \mathsf{negl}(\lambda).$$

By construction of the encoder above, the above statement is equivalent to

$$\Big| \Pr_{r \leftarrow R}[\mathcal{A}(1^n, \mathsf{ChE}(\mathsf{ECC.Enc}(1^n, \mathsf{Obf}_{\mathsf{ChB}}(1^n, f_{0,r,\mathsf{ChB},n}))), \mathsf{ChE}(r)) = 1] - \Pr_{r \leftarrow R}[\mathcal{A}(1^n, \mathsf{ChE}(\mathsf{ECC.Enc}(1^n, \mathsf{Obf}_{\mathsf{ChB}}(1^n, f_{1,r,\mathsf{ChB},n}))), \mathsf{ChE}(r)) = 1]\Big| \leq \mathsf{negl}(n)$$

where R is the uniform distribution on $\mathcal{X}^n$. A strengthening of $\mathcal{A}$ is to assume $\mathcal{A}$ correctly decodes the encoded obfuscated circuit description. Therefore, rewriting the above using the notation from Definition 7.14 and Definition 7.15, it suffices to prove

$$\Big| \Pr_{C_0 \leftarrow D_{0,\mathsf{ChB}}(1^n)}[\mathcal{A}(1^n, \mathsf{Obf}_{\mathsf{ChB}}(1^n, C_0), \mathsf{Aux}_{\mathsf{ChE}}(1^n, C_0)) = 1] - \Pr_{C_1 \leftarrow D_{1,\mathsf{ChB}}(1^n)}[\mathcal{A}(1^n, \mathsf{Obf}_{\mathsf{ChB}}(1^n, C_1), \mathsf{Aux}_{\mathsf{ChE}}(1^n, C_1)) = 1] \Big| \leq \mathsf{negl}(n). \quad (\star)$$

Now we aim to show $(\star)$ through a series of inequalities.

First, the security definition of average-case virtual black box with auxiliary input obfuscation in Definition 7.2 yields a simulator non-uniform polynomial time oracle machine Sim such that,

$$\Big| \Pr_{C_0 \leftarrow D_{0,\mathsf{ChB}}(1^n)}[\mathcal{A}(1^n, \mathsf{Obf}_{\mathsf{ChB}}(1^n, C_0), \mathsf{Aux}_{\mathsf{ChE}}(1^n, C_0)) = 1] - \Pr_{C_0 \leftarrow D_{0,\mathsf{ChB}}(1^n)}[\mathsf{Sim}^{C_0}(1^n, 1^{|C_0|}, \mathsf{Aux}(1^n, C_0)) = 1] \Big| \leq \mathsf{negl}(n) \quad (1)$$

$$\Big| \Pr_{C_1 \leftarrow D_{1,\mathsf{ChB}}(1^n)}[\mathcal{A}(1^n, \mathsf{Obf}_{\mathsf{ChB}}(1^n, C_1), \mathsf{Aux}_{\mathsf{ChE}}(1^n, C_1)) = 1] - \Pr_{C \leftarrow D_{1,\mathsf{ChB}}(1^n)}[\mathsf{Sim}^{C_1}(1^n, 1^{|C_1|}, \mathsf{Aux}(1^n, C_1)) = 1] \Big| \leq \mathsf{negl}(n) \quad (2)$$

Next, we note by Lemma 7.16, that $(\mathscr{F}_{\mathsf{ChB}}, \mathscr{G}_{\mathsf{ChB}})$ is statistically evasive. Therefore, with high probability, since $\mathsf{Sim}^{(\cdot)}$ is polynomial time, $\mathsf{Sim}^{C_0}(1^n, 1^{|C_0|}, \mathsf{Aux}(1^n, C_0))$ and $\mathsf{Sim}^{C_1}(1^n, 1^{|C_0|}, \mathsf{Aux}(1^n, C_0))$ both only ever receive 0's from their oracles, so

$$\Big| \Pr_{C_0 \leftarrow D_{0,\mathsf{ChB}}(1^n)}[\mathsf{Sim}^{C_0}(1^n, 1^{|C_0|}, \mathsf{Aux}(1^n, C_0)) = 1] - \Pr_{C_0 \leftarrow D_{0,\mathsf{ChB}}(1^n), C_1 \leftarrow D_{1,\mathsf{ChB}}(1^n)}[\mathsf{Sim}^{C_1}(1^n, 1^{|C_0|}, \mathsf{Aux}(1^n, C_0))) = 1] \Big| \leq \mathsf{negl}(n). \quad (3)$$

Then, observe that since the auxiliary input generator is only dependent on r, and $D_{0,\mathsf{ChB}}$ and $D_{1,\mathsf{ChB}}$ output circuits of the same size, then the resulting distribution of

$$(1^n, 1^{|C_0|}, \mathsf{Aux}(1^n, C_0))$$

when $C_0 \leftarrow D_{0,\mathsf{ChB}}$ is identical to that of

$$(1^n, 1^{|C_1|}, \mathsf{Aux}(1^n, C_1))$$

when $C_1 \leftarrow D_{1,\mathsf{ChB}}$. Therefore,

$$\Big| \Pr_{C_0 \leftarrow D_{0,\mathsf{ChB}}(1^n), C_1 \leftarrow D_{1,\mathsf{ChB}}(1^n)}[\mathsf{Sim}^{C_1}(1^n, 1^{|C_0|}, \mathsf{Aux}(1^n, C_0))) = 1] - \Pr_{C_1' \leftarrow D_{1,\mathsf{ChB}}(1^n), C_1 \leftarrow D_{1,\mathsf{ChB}}(1^n)}[\mathsf{Sim}^{C_1}(1^n, 1^{|C_1'|}, \mathsf{Aux}(1^n, C_1'))) = 1] \Big| \leq \mathsf{negl}(n). \quad (4)$$

Then, again since $(\mathscr{F}_{\mathsf{ChB}}, \mathscr{G}_{\mathsf{ChB}})$ is evasive,

$$\Big| \Pr_{C_1' \leftarrow D_{1,\mathsf{ChB}}(1^n), C_1 \leftarrow D_{1,\mathsf{ChB}}(1^n)}[\mathsf{Sim}^{C_1}(1^n, 1^{|C_1'|}, \mathsf{Aux}(1^n, C_1'))) = 1] - \Pr_{C_1 \leftarrow D_{1,\mathsf{ChB}}(1^n)}[\mathsf{Sim}^{C_1}(1^n, 1^{|C_1|}, \mathsf{Aux}(1^n, C_1))) = 1] \Big| \leq \mathsf{negl}(n). \quad (5)$$

Applying the triangle inequality on (1), (2), (3), (4), (5) yields $(\star)$. As mentioned earlier, $(\star)$ suffices to show semantic security of the scheme. □

7.4 Construction from $i\mathcal{O}$

Finally, we remark that if there exists a uniformly bounded average case virtual black box with auxiliary input obfuscator, then $i\mathcal{O}$ (indistinguishability obfuscation) also implies secure wiretap coding schemes for $(\mathsf{ChB}, \mathsf{ChE})$ wiretap channels where ChB is not a degradation of ChE.

Definition 7.18. *A uniform PPT algorithm* Obf *for a collection* $\{\mathscr{F}_\lambda\}_{\lambda\in\mathbb{N}}$ *of circuits is said to be be uniformly bounded if it satisfies the following property:*

- ***Polynomially Bounded Obfuscation Circuit Size****: There exists a polynomial* $p(\lambda)$ *such that for all* $\lambda \in \mathbb{N}$ *and for all* $C \in \mathscr{F}_\lambda$*, we have* $\left|\mathsf{Obf}(1^\lambda, C)\right| = p(|C|)$ *where* $|C|$ *is the circuit size of* C*.*

Definition 7.19 (Indistinguishability Obfuscation ($i\mathcal{O}$) for Circuits, Imported from [JLS21])**.** *A uniform PPT algorithm* $i\mathcal{O}$ *is called a* (T, γ)*-secure indistinguishability obfuscator for polynomial-sized circuits if the following holds:*

- ***Completeness:*** *For every* $\lambda \in \mathbb{N}$*, every circuit* C *with input length* n*, every input* $x \in \{0,1\}^n$ *we have that*
$$\Pr\left[C'(x) = C(x) : C' \leftarrow i\mathcal{O}(1^\lambda, C)\right] = 1$$
- (T, γ)***-Indistinguishability:*** *For every two ensembles* $\{C_{0,\lambda}\}, \{C_{1,\lambda}\}$ *of polynomial-sized circuits that have the same size, input length, and output length, and are functionally equivalent, that is,* $\forall\lambda$*,* $C_{0,\lambda}(x) = C_{1,\lambda}(x)$ *for every input* x*, the following distributions are* (T, γ)*-indistinguishable.*
$$\{i\mathcal{O}(1^\lambda, C_{0,\lambda})\} \qquad \{i\mathcal{O}(1^\lambda, C_{1,\lambda})\}$$
meaning that for all adversaries running in time $T \cdot \mathsf{poly}(\lambda)$ *we have that for all sufficiently large* λ*,*
$$\left|\Pr\left[\mathcal{A}(1^\lambda, i\mathcal{O}(1^\lambda, C_{0,\lambda})) = 1\right] - \Pr\left[\mathcal{A}(1^\lambda, i\mathcal{O}(1^\lambda, C_{1,\lambda})) = 1\right]\right| \leq \gamma(\lambda).$$

Following the discussion on $i\mathcal{O}$ in [AIK+21], we note that $i\mathcal{O}$ is a "best-possible" obfuscation [GR07]. More specifically, if there exists some instantiation of the ideal obfuscation that gives a secure computational wiretap coding scheme, then replacing that instantiation with $i\mathcal{O}$ should preserve the security properties. However, in our setting, the adversary is given additional auxiliary information that may depend on the obfuscated circuit. Despite this auxiliary information, we formally show below that $i\mathcal{O}$ still behaves as a best possible obfuscation.

Lemma 7.20. *Let* ChB *be a channel and* λ *be a security parameter. If there exists a uniformly bounded average-case virtual black box with auxiliary input obfuscator* $\mathsf{Obf}_{\mathsf{ChB}}$ *with perfect correctness for* $(\mathscr{F}_{\mathsf{ChB}}, \mathscr{G}_{\mathsf{ChB}})$ *where* $\mathscr{G}_{\mathsf{ChB}} = \{D_{0,\mathsf{ChB}}, D_{1,\mathsf{ChB}}\} \times \mathscr{A}_{\mathsf{ChB}}$*, then* (λ, μ)*-secure* $i\mathcal{O}$ *for a negligible* μ *implies a computationally secure wiretap coding scheme for any* $(\mathsf{ChB}, \mathsf{ChE})$*-wiretap channel where* ChB *is not a degraded version of* ChE*.*

Proof. Let $(\mathsf{ChB}, \mathsf{ChE})$ be a wiretap channel where ChB is not a degration of ChE. Let $\mathsf{Obf}_{\mathsf{ChB}}$ be a uniformly bounded average-case virtual black box with auxiliary input obfuscator with perfect correctness for $(\mathscr{F}_{\mathsf{ChB}}, \mathscr{G}_{\mathsf{ChB}})$. Let p be the polynomial which bounds the obfuscation circuit size (i.e. $|\mathsf{Obf}(1^\lambda, C)| = p(|C|)$). Let Pad_p be a function that pads a circuit $C \in \mathscr{F}_{\mathsf{ChB}}$ to a functionally identical circuit of size $p(|C|)$.

Our computationally secure wiretap coding scheme construction is identical to the construction in Theorem 7.17 except we replace $\mathsf{Obf}(1^n, f_{m,r,\mathsf{ChB},n})$ with $i\mathcal{O}(1^n, \mathsf{Pad}_p(f_{m,r,\mathsf{ChB},n}))$. Correctness follows in the same way as in Theorem 7.17 by correctness of $i\mathcal{O}$.

Analogously to the proof of Theorem 7.17, to show semantic security, it suffices to show for all non-uniform polynomial time adversaries $\mathcal{A}$ that

$$\Big|\Pr_{C_0\leftarrow D_{0,\mathsf{ChB}}(1^\lambda)}\Big[\mathcal{A}(1^\lambda, i\mathcal{O}(1^\lambda, \mathsf{Pad}_p(C_0)), \mathsf{Aux}_{\mathsf{ChE}}(1^\lambda, C_0)) = 1\Big] - \Pr_{C_1\leftarrow D_{1,\mathsf{ChB}}(1^\lambda)}\Big[\mathcal{A}(1^\lambda, i\mathcal{O}(1^\lambda, \mathsf{Pad}_p(C_1)), \mathsf{Aux}_{\mathsf{ChE}}(1^\lambda, C_1)) = 1\Big]\Big| \leq \mathsf{negl}(\lambda). \quad (\star)$$

First we show the following claim:

Claim 7.21.

$$\Big|\Pr_{C_0\leftarrow D_{0,\mathsf{ChB}}(1^\lambda)}\Big[\mathcal{A}(1^\lambda, i\mathcal{O}(1^\lambda, \mathsf{Pad}_p(C_0)), \mathsf{Aux}_{\mathsf{ChE}}(1^\lambda, C_0)) = 1\Big] - \Pr_{C_0\leftarrow D_{0,\mathsf{ChB}}(1^\lambda)}\Big[\mathcal{A}(1^\lambda, i\mathcal{O}(1^\lambda, \mathsf{Obf}_{\mathsf{ChB}}(1^\lambda, C_0)), \mathsf{Aux}_{\mathsf{ChE}}(1^\lambda, C_0)) = 1\Big]\Big| \leq \mu(\lambda). \quad (1)$$

Proof. For the sake of contradiction, suppose not. Then there exists an adversary $\mathcal{A}^*$ such that

$$\Big|\Pr_{C_0\leftarrow D_{0,\mathsf{ChB}}(1^\lambda)}\Big[\mathcal{A}^*(1^\lambda, i\mathcal{O}(1^\lambda, \mathsf{Pad}_p(C_0)), \mathsf{Aux}_{\mathsf{ChE}}(1^\lambda, C_0)) = 1\Big] - \Pr_{C_0\leftarrow D_{0,\mathsf{ChB}}(1^\lambda)}\Big[\mathcal{A}^*(1^\lambda, i\mathcal{O}(1^\lambda, \mathsf{Obf}_{\mathsf{ChB}}(1^\lambda, C_0)), \mathsf{Aux}_{\mathsf{ChE}}(1^\lambda, C_0)) = 1\Big]\Big| > \mu(\lambda).$$

Let (C^*, r^*) be the circuit C^* from $D_{0,\mathsf{ChB}}$ and the randomness r^* for the auxiliary input generator that maximizes $\mathcal{A}^*$'s distinguishing advantage. Now, we construct a distinguisher $\mathcal{A}'$ that breaks the (λ, μ)-indistinguishability of $i\mathcal{O}$ on circuits $\mathsf{Pad}_p(C^*)$ and $\mathsf{Obf}_{\mathsf{ChB}}(C^*)$. $\mathcal{A}'$ takes as input Q which is either $i\mathcal{O}(1^\lambda, \mathsf{Pad}_p(C^*))$ or $i\mathcal{O}(1^\lambda, \mathsf{Obf}_{\mathsf{ChB}}(C^*))$ as well as non-uniform advice r^* and circuit descriptions of $\mathcal{A}^*$ and C^*, and outputs either 0 or 1.

$\mathcal{A}'(1^\lambda, Q, \langle\mathcal{A}^*\rangle, \langle C^*\rangle, r^*)$:

- Output $\mathcal{A}^*(1^\lambda, Q, \mathsf{Aux}_{\mathsf{ChE}}(1^\lambda, C^*; r^*))$

Then, $\mathcal{A}'$ on input $i\mathcal{O}(1^\lambda, \mathsf{Pad}_p(C^*))$ outputs $\mathcal{A}^*(1^\lambda, i\mathcal{O}(1^\lambda, \mathsf{Pad}_p(C^*)), \mathsf{Aux}_{\mathsf{ChE}}(1^\lambda, C^*; r^*))$ and on input $i\mathcal{O}(1^\lambda, \mathsf{Obf}_{\mathsf{ChB}}(C^*))$ outputs $\mathcal{A}^*(1^\lambda, i\mathcal{O}(1^\lambda, \mathsf{Obf}_{\mathsf{ChB}}(1^\lambda, C^*)), \mathsf{Aux}_{\mathsf{ChE}}(1^\lambda, C^*; r^*))$. But then since $\mathcal{A}^*$ has greater than $\mu(\lambda)$ advantage in distinguishing the two, then $\mathcal{A}'$ has greater than $\mu(\lambda)$ advantage in distinguishing the obfuscations, contradicting (λ, μ)-indistinguishability. □

The same exact argument gives

$$\Big|\Pr_{C_1\leftarrow D_{1,\mathsf{ChB}}(1^\lambda)}\Big[\mathcal{A}(1^\lambda, i\mathcal{O}(1^\lambda, \mathsf{Pad}_p(C_1)), \mathsf{Aux}_{\mathsf{ChE}}(1^\lambda, C_1)) = 1\Big] - \Pr_{C_1\leftarrow D_{1,\mathsf{ChB}}(1^\lambda)}\Big[\mathcal{A}(1^\lambda, i\mathcal{O}(1^\lambda, \mathsf{Obf}_{\mathsf{ChB}}(1^\lambda, C_1)), \mathsf{Aux}_{\mathsf{ChE}}(1^\lambda, C_1)) = 1\Big]\Big| \leq \mu(\lambda). \quad (2)$$

Then, as shown in $(\star)$ of the proof of Theorem 7.17, by security of $\mathsf{Obf}_{\mathsf{ChB}}$ and since $(\mathscr{F}_{\mathsf{ChB}}, \mathscr{G}_{\mathsf{ChB}})$ is statistically evasive,

$$\Big|\Pr_{C_0\leftarrow D_{0,\mathsf{ChB}}(1^\lambda)}[\mathcal{A}(1^\lambda, \mathsf{Obf}_{\mathsf{ChB}}(1^\lambda, C_0), \mathsf{Aux}_{\mathsf{ChE}}(1^\lambda, C_0)) = 1] - \Pr_{C_1\leftarrow D_{1,\mathsf{ChB}}(1^\lambda)}[\mathcal{A}(1^\lambda, \mathsf{Obf}_{\mathsf{ChB}}(1^\lambda, C_1), \mathsf{Aux}_{\mathsf{ChE}}(1^\lambda, C_1)) = 1]\Big| \leq \mathsf{negl}(n).$$

which implies

$$\Big| \Pr_{C_0 \leftarrow D_{0,\mathsf{ChB}}(1^\lambda)} \Big[\mathcal{A}(1^\lambda, i\mathcal{O}(1^\lambda, \mathsf{Obf}_{\mathsf{ChB}}(1^\lambda, C_0)), \mathsf{Aux}_{\mathsf{ChE}}(1^\lambda, C_0)) = 1\Big] - \Pr_{C_1 \leftarrow D_{1,\mathsf{ChB}}(1^\lambda)} \Big[\mathcal{A}(1^\lambda, i\mathcal{O}(1^\lambda, \mathsf{Obf}_{\mathsf{ChB}}(1^\lambda, C_1)), \mathsf{Aux}_{\mathsf{ChE}}(1^\lambda, C_1)) = 1\Big] \Big| \leq \mu(\lambda). \tag{3}$$

Applying the triangle inequality on (1), (2), (3) gives ($\star$). □

8 Acknowledgments

Y. Ishai was supported in part by ERC Project NTSC (742754), BSF grant 2018393, and ISF grant 2774/20. This research was supported in part from a Simons Investigator Award, DARPA SIEVE award, NTT Research, NSF Frontier Award 1413955, BSF grant 2012378, a Xerox Faculty Research Award, a Google Faculty Research Award, and an Okawa Foundation Research Grant. This material is based upon work supported by the Defense Advanced Research Projects Agency through Award HR00112020024.

9 References

[AIK+21] Shweta Agrawal, Yuval Ishai, Eyal Kushilevitz, Varun Narayanan, Manoj Prabhakaran, Vinod Prabhakaran, and Alon Rosen. Secure computation from one-way noisy communication, or: Anti-correlation via anti-concentration. In *CRYPTO*, 2021.

[BBC+14] Boaz Barak, Nir Bitansky, Ran Canetti, Yael Tauman Kalai, Omer Paneth, and Amit Sahai. Obfuscation for evasive functions. In *Theory of Cryptography Conference*, pages 26–51. Springer, 2014.

[BGI+01] Boaz Barak, Oded Goldreich, Russell Impagliazzo, Steven Rudich, Amit Sahai, Salil P. Vadhan, and Ke Yang. On the (im)possibility of obfuscating programs. In Joe Kilian, editor, *Advances in Cryptology – CRYPTO 2001*, volume 2139 of *Lecture Notes in Computer Science*, pages 1–18, Santa Barbara, CA, USA, August 19–23, 2001. Springer, Heidelberg, Germany.

[BM84] Manuel Blum and Silvio Micali. How to generate cryptographically strong sequences of pseudorandom bits. *SIAM journal on Computing*, 13(4):850–864, 1984.

[BMSZ16] Saikrishna Badrinarayanan, Eric Miles, Amit Sahai, and Mark Zhandry. Post-zeroizing obfuscation: New mathematical tools, and the case of evasive circuits. In Marc Fischlin and Jean-Sébastien Coron, editors, *Advances in Cryptology – EUROCRYPT 2016, Part II*, volume 9666 of *Lecture Notes in Computer Science*, pages 764–791, Vienna, Austria, May 8–12, 2016. Springer, Heidelberg, Germany.

[BTV12] Mihir Bellare, Stefano Tessaro, and Alexander Vardy. A cryptographic treatment of the wiretap channel. *IACR Cryptology ePrint Archive*, 2012:015, 2012.

[CFP+21] Ran Canetti, Benjamin Fuller, Omer Paneth, Leonid Reyzin, and Adam D. Smith. Reusable fuzzy extractors for low-entropy distributions. *J. Cryptol.*, 34(1):2, 2021. Earlier version in Eurcrypt 2016.

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

[CLT13] Jean-Sébastien Coron, Tancrède Lepoint, and Mehdi Tibouchi. Practical multilinear maps over the integers. In Ran Canetti and Juan A. Garay, editors, *Advances in Cryptology – CRYPTO 2013, Part I*, volume 8042 of *Lecture Notes in Computer Science*, pages 476–493, Santa Barbara, CA, USA, August 18–22, 2013. Springer, Heidelberg, Germany.

[DORS08] Yevgeniy Dodis, Rafail Ostrovsky, Leonid Reyzin, and Adam D. Smith. Fuzzy extractors: How to generate strong keys from biometrics and other noisy data. *SIAM J. Comput.*, 38(1):97–139, 2008.

[FMR20] Benjamin Fuller, Xianrui Meng, and Leonid Reyzin. Computational fuzzy extractors. *Inf. Comput.*, 275:104602, 2020. Earlier version in Asiacrypt 2013.

[GGH13] Sanjam Garg, Craig Gentry, and Shai Halevi. Candidate multilinear maps from ideal lattices. In Thomas Johansson and Phong Q. Nguyen, editors, *Advances in Cryptology – EUROCRYPT 2013*, volume 7881 of *Lecture Notes in Computer Science*, pages 1–17, Athens, Greece, May 26–30, 2013. Springer, Heidelberg, Germany.

[GK05] Shafi Goldwasser and Yael Tauman Kalai. On the impossibility of obfuscation with auxiliary input. In *46th Annual Symposium on Foundations of Computer Science*, pages 553–562, Pittsburgh, PA, USA, October 23–25, 2005. IEEE Computer Society Press.

[GM84] Shafi Goldwasser and Silvio Micali. Probabilistic encryption. *Journal of computer and system sciences*, 28(2):270–299, 1984.

[GMW87] Oded Goldreich, Silvio Micali, and Avi Wigderson. How to play any mental game or A completeness theorem for protocols with honest majority. In Alfred Aho, editor, *19th Annual ACM Symposium on Theory of Computing*, pages 218–229, New York City, NY, USA, May 25–27, 1987. ACM Press.

[GR07] Shafi Goldwasser and Guy N. Rothblum. On best-possible obfuscation. In Salil P. Vadhan, editor, *TCC 2007: 4th Theory of Cryptography Conference*, volume 4392 of *Lecture Notes in Computer Science*, pages 194–213, Amsterdam, The Netherlands, February 21–24, 2007. Springer, Heidelberg, Germany.

[JLS21] Aayush Jain, Huijia Lin, and Amit Sahai. Indistinguishability obfuscation from well-founded assumptions. In *Proceedings of the 53rd Annual ACM SIGACT Symposium on Theory of Computing*, pages 60–73, 2021.

[LKP09] Yingbin Liang, Gerhard Kramer, and H Vincent Poor. Compound wiretap channels. *EURASIP Journal on Wireless Communications and Networking*, 2009:1–12, 2009.

[Mau93] U.M. Maurer. Secret key agreement by public discussion from common information. *IEEE Transactions on Information Theory*, 39(3):733–742, 1993.

[Mau94] Ueli M Maurer. The strong secret key rate of discrete random triples. In *Communications and Cryptography*, pages 271–285. Springer, 1994.

[MW00] Ueli M. Maurer and Stefan Wolf. Information-theoretic key agreement: From weak to strong secrecy for free. In Bart Preneel, editor, *Advances in Cryptology – EUROCRYPT 2000*, volume 1807 of *Lecture Notes in Computer Science*, pages 351–368, Bruges, Belgium, May 14–18, 2000. Springer, Heidelberg, Germany.

[Nai10] Chandra Nair. Capacity regions of two new classes of two-receiver broadcast channels. *IEEE Transactions on Information Theory*, 56(9):4207–4214, 2010.

[PS17] H. Vincent Poor and Rafael F. Schaefer. Wireless physical layer security. *Proceedings of the National Academy of Sciences*, 114(1):19–26, 2017.

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

[Yao82] Andrew C Yao. Theory and application of trapdoor functions. In *23rd Annual Symposium on Foundations of Computer Science (SFCS 1982)*, pages 80–91. IEEE, 1982.

A [CK78] and [MW00] Definitions

In this section, we connect the definitions of wiretap channels and secrecy capacity used in [CK78] and [MW00] to the definitions used in our preliminaries.

A.1 [CK78] Definitions

First, we state the definitions from [CK78].

Definition A.1 (Achievable Rate Pairs, Imported from [CK78])**.** *A rate pair (R, R_e) of non-negative numbers is an achievable rate pair for a $(\mathsf{ChB}, \mathsf{ChE})$-wiretap channel if there exists a family of messages $\{\mathcal{M}_n\}_{n\in\mathbb{N}}$ and encoder-decoder pairs $\{(\mathrm{Enc}_n, \mathrm{Dec}_n)\}_{n\in\mathbb{N}}$ where Enc_n outputs an encoding of length n and such that*

- ***Message Rate** R:*
$$\lim_{n\to\infty} \frac{1}{n} \log |\mathcal{M}_n| = R$$
- ***Correctness**: For all $m \in \mathcal{M}_n$,*
$$\Pr[\mathrm{Dec}_n(\mathsf{ChB}(\mathrm{Enc}_n(m))) = m] \geq 1 - \epsilon_n$$
where
$$\lim_{n\to\infty} \epsilon_n = 0$$
- ***Equivocation Rate (Secrecy)** R_e:*
$$\lim_{n\to\infty} \frac{1}{n} H(M_n \mid \mathsf{ChE}(\mathrm{Enc}_n(M_n))) \geq R_e$$
where M_n is uniform over $\mathcal{M}_n$.

We denote the set of all achievable rate pairs as $\mathcal{R}$.

The equivocation rate R_e captures a notion of statistical secrecy for a uniform random message. As the equivocation rate increases, the information that Eve has about the message decreases:

$$\lim_{n\to\infty} \frac{1}{n} I(M_n; \mathsf{ChE}(\mathrm{Enc}_n(M_n))) = \lim_{n\to\infty} \frac{1}{n} \left[H(M_n) - H(M_n \mid \mathsf{ChE}(\mathrm{Enc}_n(M_n)))\right] \leq R - R_e$$

In particular, when $R = R_e$, then $\lim_{n\to\infty} \frac{1}{n} I(M_n; \mathsf{ChE}(\mathrm{Enc}_n(M_n))) = 0$.

This motivates the definition of secrecy capacity.

Definition A.2 (Secrecy Capacity, Imported from [CK78])**.** *The secrecy capacity of a wiretap channel is defined to be*
$$C_s = \max_{(R,R)\in\mathcal{R}} R.$$

The definition of CK Rate-R Wiretap Encoding Family (Definition 4.9) then follows by requiring $R = R_e$, and the alternate definition of secrecy capacity (Definition 4.10) is immediate.

A.2 [MW00] Definitions

The definitions of secrecy capacity and strong secrecy capacity used in [MW00] are essentially the same as the definitions used in [CK78] and our preliminaries except that

- The message space is binary:
$\mathcal{M}_n = \{0,1\}^k$ where $k := \lfloor (R - \epsilon_n)n \rfloor$

- We only require correctness with respect to a random message:

$$\Pr[\mathrm{Dec}_n(\mathsf{ChB}(\mathrm{Enc}_n(M_n))) = M_n] \geq 1 - \epsilon_n$$

  where M_n is uniformly distributed over $\mathcal{M}_n = \{0,1\}^k$.

Note that if we have a wiretap coding that satisfies the [CK78] definition, then it also satisfies the [MW00] definition as we can simply map each $m \in \mathcal{M}_n$ to a binary string in $\{0,1\}^k$.

Now, suppose we have a wiretap coding scheme that satisfies the [MW00] definition. Observe that by an averaging argument, if

$$\Pr[\mathrm{Dec}_n(\mathsf{ChB}(\mathrm{Enc}_n(M_n))) = M_n] \geq 1 - \epsilon_n$$

where M_n is uniformly distributed over $\{0,1\}^k$, then for at least a $\sqrt{1-\epsilon_n}$ fraction of the messages $m \in \{0,1\}^k$,

$$\Pr[\mathrm{Dec}_n(\mathsf{ChB}(\mathrm{Enc}_n(m))) = m] \geq \sqrt{1-\epsilon_n}$$

Thus, we can define a new message space

$$\mathcal{M}'_n = \{m \mid \Pr[\mathrm{Dec}_n(\mathsf{ChB}(\mathrm{Enc}_n(m))) = m] \geq \sqrt{1-\epsilon_n}\}$$

Then, the encoding scheme satisfying the [MW00] definition satisfies the [CK78] definition with respect to $\mathcal{M}'_n$ and $\epsilon'_n = 1 - \sqrt{1-\epsilon_n}$. Note that since we only removed a $1 - \sqrt{1-\epsilon_n}$ fraction of messages from $\mathcal{M}_n$ and $\epsilon_n \to 0$, then the rate and secrecy requirement of [CK78] also hold in the limit since $\epsilon'_n \to 0$. In particular, this means that Theorem 4.14 holds with respect to the definitions we use in the preliminaries.

B Main Theorem Additional Proofs

In this section, we prove some theorems deferred from Section 5.

Definition 5.6. Let $\textsc{Good} = \{r \in \mathcal{X}^n \mid \forall x \in \mathcal{X}, N_x(r) \geq \frac{n}{2|\mathcal{X}|}\} \subset \mathcal{X}^n$.

Lemma 5.7. $\Pr[R \in \textsc{Good}] \geq 1 - \mathsf{negl}(\lambda)$

Proof. For any $x \in \mathcal{X}$ and $i \in [n]$, define

$$V_{x,i} = \begin{cases} 1 \text{ if } R_i = x \\ 0 \text{ else} \end{cases}$$

Since R is uniformly random over $\mathcal{X}^n$, then $\mathbb{E}[V_{x,i}] = \frac{1}{|\mathcal{X}|}$. Let $N_x(R) = \sum_{i\in[n]} V_{x,i}$. Then, $\mathbb{E}[N_x(R)] = \frac{n}{|\mathcal{X}|}$. Therefore, by a Chernoff bound, for any $x \in \mathcal{X}$, we have

$$\Pr\left[N_x(R) \leq \frac{1}{2} \cdot \frac{n}{|\mathcal{X}|}\right] < e^{-\frac{n}{8|\mathcal{X}|}} = \mathsf{negl}(n)$$

Thus,

$$\begin{aligned} \Pr[\forall x \in \mathcal{X}, N_x(R) \geq \frac{n}{2|X|}] &= 1 - \Pr[\exists x \in \mathcal{X}, N_x(R) < \frac{n}{2|X|}] \\ &\geq 1 - \sum_{x\in\mathcal{X}} \Pr[N_x(R) < \frac{n}{2|X|}] \\ &= 1 - |\mathcal{X}| \cdot \mathsf{negl}(n) = 1 - \mathsf{negl}(\lambda) \end{aligned}$$

□

Claim 5.14. For all $r \in \mathcal{X}^n$, $r_E \in \mathcal{Z}^n$, $\pi \in S_n$,

$$\Pr[R = r \mid R_E = r_E] = \Pr[R = \pi(r) \mid R_E = \pi(r_E)]$$

Proof. Let $r = (r_1, \ldots, r_n)$ and $r_E = (r_{E1}, \ldots, r_{En})$. Since each bit of r is chosen identically and independently and ChE acts independently on each input symbol, then

$$\begin{aligned}
\Pr[R = r \mid R_E = r_E] &= \frac{\Pr[R_E = r_E \mid R = r] \cdot \Pr[R = r]}{\Pr[R_E = r_E]} \\
&= \prod_{i \in [n]} \frac{\Pr[R_{Ei} = r_{Ei} \mid R_i = r_i] \cdot \Pr[R_i = r_i]}{\Pr[R_{Ei} = r_{Ei}]} \\
&= \prod_{j \in \pi([n])} \frac{\Pr[R_{Ej} = r_{Ej} \mid R_j = r_j] \cdot \Pr[R_j = r_j]}{\Pr[R_{Ej} = r_{Ej}]} \\
&= \frac{\Pr[R_E = \pi(r_E) \mid R = \pi(r)] \cdot \Pr[R = \pi(r)]}{\Pr[R_E = \pi(r_E)]} \\
&= \Pr[R = \pi(r) \mid R_E = \pi(r_E)]
\end{aligned}$$

□

Claim 5.15. For a fixed $r \in \mathcal{X}^n, r_B \in \mathcal{Y}^n$, and any $\pi \in S_n$, $h_{r,\mathsf{ChB},n}(r_B) = 1$ if and only if $h_{\pi(r),\mathsf{ChB},n}(\pi(r_B)) = 1$.

Proof. Consider the multiset of input-output pairs $\{(r_i, r_{Bi})\}_{i \in [n]}$ of r and r_B. This is equal to the multiset of input-output pairs $\{(\pi(r)_i, \pi(r_B)_i)\}_{i \in [n]}$ of $\pi(r)$ and $\pi(r_B)$. Therefore for all $x \in \mathcal{X}$ and $y \in \mathcal{Y}$, we have

$$\begin{aligned}
\textsc{Ratio}_{x \to y}(r, r_B) &= \frac{|i \in [n] : r_i = x, r_{Bi} = y|}{N_x(r)} \\
&= \frac{|i \in [n] : \pi(r)_i = x, \pi(r_B)_i = y|}{N_x(\pi(r))} \\
&= \textsc{Ratio}_{x \to y}(\pi(r), \pi(r_B))
\end{aligned}$$

Thus, $h_{r,\mathsf{ChB},n}(r_B) = h_{\pi(r),\mathsf{ChB},n}(\pi(r_B))$. □

Corollary 5.16. For all $\widehat{r}_B \in \mathcal{Y}^n, r_E \in \mathcal{Z}^n, \pi \in S_n$,

$$\Pr_{R,\mathsf{ChE}}[h_{R,\mathsf{ChB},n}(\widehat{r}_B) = 1 \mid R_E = r_E] = \Pr_{R,\mathsf{ChE}}[h_{R,\mathsf{ChB},n}(\pi(\widehat{r}_B)) = 1 \mid R_E = \pi(r_E)]$$

Proof. This follows immediately from Claim 5.14 and Claim 5.15:

$$\begin{aligned}
\Pr_{R,\mathsf{ChE}}[h_{R,\mathsf{ChB},n}(\widehat{r}_B) = 1 \mid R_E = r_E] &= \sum_r h_{r,\mathsf{ChB},n}(\widehat{r}_B) \cdot \Pr[R = r \mid R_E = r_E] \\
&= \sum_r h_{\pi(r),\mathsf{ChB},n}(\pi(\widehat{r}_B)) \cdot \Pr[R = \pi(r) \mid R_E = \pi(r_E)] \\
&= \sum_{\pi(r)} h_{\pi(r),\mathsf{ChB},n}(\pi(\widehat{r}_B)) \cdot \Pr[R = \pi(r) \mid R_E = \pi(r_E)] \\
&= \sum_{r'} h_{r',\mathsf{ChB},n}(\pi(\widehat{r}_B)) \cdot \Pr[R = r' \mid R_E = \pi(r_E)] \\
&= \Pr_{R,\mathsf{ChE}}[h_{R,\mathsf{ChB},n}(\pi(\widehat{r}_B)) = 1 \mid R_E = \pi(r_E)]
\end{aligned}$$

□

Claim 5.22. Let $n \in \mathbb{N}$, let ℓ be a nonnegative constant, and let $p_1 = p_1(n), \ldots, p_\ell = p_\ell(n)$ be such that $\sum_{i=1}^{\ell} p_i = 1$ and $\forall i \in [\ell], p_i \in [0,1]$ and $n \cdot p_i \in \mathbb{N} \cup \{0\}$. Let $X = (X_1, \ldots, X_\ell) \sim \mathsf{Multinomial}(n;\ p_1, p_2, \ldots, p_\ell)$ where X_i is a random variable denoting the number of occurrences of outcome i in n independent trials where $\Pr[\text{outcome } i \text{ occurs in a trial}] = p_i$. Then the probability that each X_i hits its expected value is

$$\Pr_X\left[\bigwedge_{i=1}^{\ell}(X_i = n \cdot p_i)\right] = \Omega\left(\frac{1}{n^{\ell/2}}\right)$$

Proof. First consider the case where each $p_i > 0$. Then, the Multinomial distribution's probability mass function gives

$$\Pr_X\left[\bigwedge_{i=1}^{\ell} X_i = n \cdot p_i\right] = \frac{n!}{\prod_{i=1}^{\ell}(n \cdot p_i)!} \cdot \prod_{i=1}^{\ell} p_i^{n \cdot p_i}.$$

Apply Stirling's Approximation[7] to obtain

$$\frac{n!}{\prod_{i=1}^{\ell}(n \cdot p_i)!} = \Theta\left(\frac{1}{(\sqrt{2\pi n})^{\ell-1}\prod_{i=1}^{\ell} p_i^{n \cdot p_i + 1/2}}\right)$$

Therefore, we get

$$\Pr_X\left[\bigwedge_{i=1}^{\ell} X_i = n \cdot p_i\right] = \Theta\left(\frac{1}{(\sqrt{2\pi n})^{\ell-1}\prod_{i=1}^{\ell} \sqrt{p_i}}\right)$$

Since each $p_i \leq 1$,

$$\Pr_X\left[\bigwedge_{i=1}^{\ell} X_i = n \cdot p_i\right] = \Omega\left(\frac{1}{n^{(\ell-1)/2}}\right)$$

Now, consider the case where $p_i = 0$ for some $i \in [l]$. Let $S = \{i \in [l] \mid p_i \neq 0\}$. Then, for $i \notin S$, we always have $X_i = np_i = 0$, and for $j \in S$, then the distribution of X_j is not affected by events of probability 0. Therefore,

$$\Pr_X\left[\bigwedge_{i=1}^{\ell} X_i = n \cdot p_i\right] = \Pr_X\left[\bigwedge_{i \in S} X_i = n \cdot p_i\right] = \Omega\left(\frac{1}{n^{(|S|-1)/2}}\right) = \Omega\left(\frac{1}{n^{\ell/2}}\right).$$

□

Definition 5.23. Let $\textsc{Good}_E = \{r_E \in \mathcal{Z}^n \mid \forall z \in \mathcal{Z}, N_z(r_E) \geq \frac{n}{2|\mathcal{X}|} \cdot \max_{x \in \mathcal{X}}(p_E(z|x))\} \subset \mathcal{Z}^n$. Observe that for all $r_E \in \textsc{Good}_E$ and $z \in \mathcal{Z}$, then $N_z(r_E) = \Theta(n)$.

Lemma 5.24. $\Pr_{R,\mathsf{ChE}}[r_E \in \textsc{Good}_E] \geq 1 - \mathsf{negl}(\lambda)$

Proof. For any $z \in \mathcal{Z}$ and $i \in [n]$, define

$$V_{z,i} = \begin{cases} 1 \text{ if } R_{Ei} = z \\ 0 \text{ else} \end{cases}$$

[7]Note that since we have assumed $n, p_i > 0$ and $np_i \in \mathbb{N} \cup \{0\}$, then $np_i = \Omega(1)$. If np_i is a constant, then Stirling's approximation still holds up to a constant since in this case $(np_i)! = \Theta(\sqrt{2\pi np_i}\left(\frac{np_i}{e}\right)^{np_i}) = \Theta(1)$

Then,

$$\begin{aligned}\mathbb{E}[V_{z,i}] &= \sum_{x\in\mathcal{X}} p_E(z|x)\Pr[R_i = x] \\ &= \sum_{x\in\mathcal{X}} p_E(z|x)\frac{1}{|\mathcal{X}|} \\ &\geq \frac{1}{|\mathcal{X}|}\cdot\max_{x\in\mathcal{X}}(p_E(z|x))\end{aligned}$$

Therefore, by the Chernoff bound, for any $z \in \mathcal{Z}$, we have $N_z(R_E) = \sum_{i\in[n]} V_{z,i}$, and

$$\begin{aligned}&\Pr\left[N_z(R_E) \leq \frac{1}{2}\frac{n}{|\mathcal{X}|}\cdot\max_{x\in\mathcal{X}}(p_E(z|x))\right] \\ &\leq \Pr\left[N_z(R_E) \leq \frac{1}{2}\cdot\mathbb{E}[N_z(R_E)]\right] \\ &< \exp\left(-\frac{\mathbb{E}[N_z(R_E)]}{8}\right) \\ &\leq \exp\left(-\frac{n}{8|\mathcal{X}|}\cdot\max_{x\in\mathcal{X}}(p_E(z|x))\right) = \mathsf{negl}(n)\end{aligned}$$

Thus,

$$\begin{aligned}\Pr\left[\forall z\in\mathcal{Z}, N_z(R_E) \geq \frac{n}{2|\mathcal{X}|}\cdot\max_{x\in\mathcal{X}}(p_E(z|x))\right] &= 1 - \Pr\left[\exists z\in\mathcal{Z}, N_z(R_E) < \frac{n}{2|\mathcal{X}|}\cdot\max_{x\in\mathcal{X}}(p_E(z|x))\right] \\ &\geq 1 - \sum_{z\in\mathcal{Z}}\Pr\left[N_z(R_E) < \frac{n}{2|\mathcal{X}|}\cdot\max_{x\in\mathcal{X}}(p_E(z|x))\right] \\ &= 1 - |\mathcal{Z}|\cdot\mathsf{negl}(n) \\ &= 1 - \mathsf{negl}(\lambda)\end{aligned}$$

□

C Proof of Theorem 4.17

In this section, we prove Theorem 4.17.

Theorem 4.17. The following are equivalent:

1. ChE is not less noisy than ChB. (Definition 3.7)
2. $C_s > 0$ (Definition 4.10)
   i.e. There exists a CK Rate-R wiretap coding family for $(\mathsf{ChB}, \mathsf{ChE})$ with positive rate R. (Definition 4.9)
3. $\overline{C_s} > 0$ (Definition 4.13)
   i.e. There exists a CK Rate-R wiretap coding family with strong secrecy for $(\mathsf{ChB}, \mathsf{ChE})$ with positive rate R. (Definition 4.12)
4. There exists a 0.99-statistically secure wiretap coding scheme for $(\mathsf{ChB}, \mathsf{ChE})$. (Definition 4.4)

5. There exists a statistically secure wiretap coding scheme for $(\mathsf{ChB}, \mathsf{ChE})$. (Definition 4.2)

6. There exists a statistically secure wiretap coding scheme for general message spaces for $(\mathsf{ChB}, \mathsf{ChE})$ with a positive constant rate. (Definition 4.19. See Section 4.4 below for the definition.)

C.1 Background Information

To prove the theorem, we will use universal hash functions and average case extractors. We include some useful definitions and lemmas below.

Definition C.1 (Universal Hash Function)**.** *A family of functions $\mathcal{H} = \{H_k : \{0,1\}^n \to \{0,1\}^\ell\}_{k \in \mathcal{K}}$ is universal if $\forall x \neq x' \in \{0,1\}^n$,*

$$\Pr_{k \leftarrow \mathcal{K}}[H_k(x) = H_k(x')] = 2^{-\ell}$$

Lemma C.2 (Generalized Leftover Hash Lemma, imported from [DORS08])**.** *Assume $\mathcal{H} = \{H_k : \{0,1\}^n \to \{0,1\}^\ell\}_{k \in \mathcal{K}}$ is a family of universal hash functions. Then, for any random variables X and Aux,*

$$\Delta((H_K(X), K, \mathsf{Aux}), (U_\ell, K, \mathsf{Aux})) \leq \frac{1}{2}\sqrt{2^{-\tilde{H}_\infty(X|\mathsf{Aux})2^\ell}}$$

where K is uniform on $\mathcal{K}$ and U_ℓ is uniform over $\{0,1\}^\ell$.

Definition C.3 (Average Conditional Min-Entropy)**.** *The average conditional min-entropy of a random variable A given a random variable B is defined as*

$$\tilde{H}_\infty(A \mid B) \triangleq -\log\left(\mathbb{E}_{b \leftarrow B}[\max_a \Pr[A = a \mid B = b]\right)$$

Definition C.4 (Average Case Extractor)**.** *Let $\mathrm{Ext} : \{0,1\}^n \times \{0,1\}^r \to \{0,1\}^\ell$ be a polynomial time probabilistic function which uses r bits of randomness. We say that Ext is an efficient average-case (n, m, ℓ, ϵ)-strong extractor if for all pairs of random variables (X, Aux) such that X is an n-bit string satisfying $\tilde{H}_\infty(X \mid \mathsf{Aux}) \geq m$,*

$$\Delta((\mathrm{Ext}(X; R), R, \mathsf{Aux}), (U_\ell, R, \mathsf{Aux})) \leq \epsilon$$

where R is uniform on $\{0,1\}^r$ and U_ℓ is uniform on $\{0,1\}^\ell$.

Corollary C.5 (Imported from [DORS08])**.** *Universal hash functions are average-case (n, m, ℓ, ϵ)-strong extractors whenever $\ell \leq m - 2\log(1/\epsilon) + 2$.*

Lemma C.6. *If $(A_1, \ldots, A_n)$ and $(B_1, \ldots, B_n)$ are random variables such that for all $i \in [n]$, (A_i, B_i) is independent of $\{(A_j, B_j)\}_{j \in [n] \setminus i}$, then*

$$\tilde{H}_\infty((A_1, \ldots, A_n) \mid (B_1, \ldots, B_n)) = \sum_{i=1}^{n} \tilde{H}_\infty(A_i \mid B_i)$$

Proof.

$$
\begin{aligned}
&\tilde{H}_\infty((A_1,\dots,A_n) \mid (B_1,\dots,B_n)) \\
&= -\log\left(\sum_{b_1,\dots,b_n} \Pr[B_1=b_1,\dots,B_n=b_n] \max_{a_1,\dots a_n} \Pr\left[A_1=a_1,\dots A_n=a_n \mid B_1=b_1,\dots B_n=b_n\right]\right) \\
&= -\log\left(\sum_{b_1,\dots,b_n} \prod_{i=1}^{n} \Pr[B_i=b_i] \max_{a_1,\dots a_n} \prod_{i=1}^{n} \Pr\left[A_i=a_i \mid B_i=b_i\right]\right) \\
&= -\log\left(\sum_{b_1,\dots,b_n} \prod_{i=1}^{n} \Pr[B_i=b_i] \max_{a_i} \Pr\left[A_i=a_i \mid B_i=b_i\right]\right) \\
&= -\log\left(\prod_{i=1}^{n}\left(\sum_{b_i} \Pr[B_i=b_i] \max_{a_i} \Pr\left[A_i=a_i \mid B_i=b_i\right]\right)\right) \\
&= \sum_{i=1}^{n}\left(-\log\left(\sum_{b_i} \Pr[B_i=b_i] \max_{a_i} \Pr\left[A_i=a_i \mid B_i=b_i\right]\right)\right) \\
&= \sum_{i=1}^{n} \tilde{H}_\infty(A_i \mid B_i)
\end{aligned}
$$

□

Lemma C.7. *Let $\{X_n\}_{n\in\mathbb{N}}$ be a sequence of discrete random variables where each X_n is over a set $\mathcal{X}_n$. Let $\{f_n\}_{n\in\mathbb{N}}$ be a sequence of functions and let $Z_n = f_n(X_n)$. If*

$$\lim_{n\to\infty} I(X_n; Z_n) = 0$$

then for all $\epsilon > 0$, there exists N_ϵ such that for all $n > N_\epsilon$,

$$\tilde{H}_\infty(X_n \mid Z_n) \geq \log\log(|\mathcal{X}_n|) - \log(\log(|\mathcal{X}_n|) - H(X_n) + 1 + \epsilon)$$

Proof. Define g_n by $g_n(z) = \arg\max_{x\in\mathcal{X}_n} \Pr[X_n = x \mid Z_n = z]$. Then, define p_n such that

$$1 - p_n := \Pr[g_n(Z_n) = X_n] = \sum_z \Pr[Z_n = z]\left(\max_{x\in\mathcal{X}_n} \Pr[X_n = x \mid Z_n = z]\right)$$

By Fano's inequality,

$$H(X_n \mid Z_n) \leq H_2(p_n) + p_n \log(|\mathcal{X}_n|) \leq 1 + p_n \log(|\mathcal{X}_n|)$$

which implies that

$$p_n \geq \frac{H(X_n \mid Z_n) - 1}{\log(|\mathcal{X}_n|)}$$

Then, since $\lim_{n\to\infty} I(X_n; Z_n) = 0$, for all $\epsilon > 0$, there exists N_ϵ such that for all $n > N_\epsilon$,

$$H(X_n \mid Z_n) = H(X_n) - I(X_n; Z_n) \geq H(X_n) - \epsilon$$

Thus, for all $n > N_\epsilon$,

$$1 - p_n \leq 1 - \frac{(H(X_n) - \epsilon - 1)}{\log(|\mathcal{X}_n|)} = \frac{\log|\mathcal{X}_n| - H(X_n) + 1 + \epsilon}{\log|\mathcal{X}_n|}$$

Now, by definition of average conditional min-entropy.

$$\tilde{H}_\infty(X_n \mid Z_n) := -\log\left(\sum_z \Pr[Z_n = z]\left(\max_{x \in \mathcal{X}_n} \Pr[X_n = x \mid Z_n = z]\right)\right) = -\log(1 - p_n)$$

Thus, for all $n > N_\epsilon$,

$$\begin{aligned}\tilde{H}_\infty(X_n \mid Z_n) &\geq -\log\left(\frac{\log|\mathcal{X}_n| - H(X_n) + 1 + \epsilon}{\log|\mathcal{X}_n|}\right) \\ &= \log\log(|\mathcal{X}_n|) - \log(\log(|\mathcal{X}_n|) - H(X_n) + 1 + \epsilon)\end{aligned}$$

□

Lemma C.8 (Imported from [DORS08])**.** *If the support of B has size at most 2^λ, then*

$$\tilde{H}_\infty(A \mid (B, C)) \geq \tilde{H}_\infty(A \mid C) - \lambda$$

Lemma C.9 (Maximal Guessing Probability)**.** *Let X be a random variable over $\{0,1\}$, let Y be a random variable over $\mathcal{Y}$, and let U be a uniform distribution over $\{0,1\}$ that is independent of (X, Y). Then, over all function $f : \mathcal{Y} \to \{0,1\}$,*

$$\max_f \Pr[f(Y) = X] = \Delta((X,Y),(U,Y)) + \frac{1}{2}$$

Furthermore,

$$\tilde{H}_\infty(X \mid Y) = -\log(\max_f \Pr[f(Y) = X])$$

Proof.

$$\begin{aligned}\max_f \Pr[f(Y) = X] &= \sum_{y \in \mathcal{Y}}\left(\Pr[Y = y] \max_{x \in \{0,1\}} \Pr[X = x \mid Y = y]\right) \\ &= \sum_{y \in \mathcal{Y}}\left(\Pr[Y = y]\left(\max_{x \in \{0,1\}} \Pr[X = x \mid Y = y] - \frac{1}{2}\right)\right) + \frac{1}{2} \\ &= \frac{1}{2}\sum_{y \in \mathcal{Y}}\left(\Pr[Y = y] \cdot 2 \max_{x \in \{0,1\}}\left|\Pr[X = x \mid Y = y] - \frac{1}{2}\right|\right) + \frac{1}{2} \\ &= \frac{1}{2}\sum_{y \in \mathcal{Y}}\left(\Pr[Y = y] \cdot \sum_{x \in \{0,1\}}\left|\Pr[X = x \mid Y = y] - \frac{1}{2}\right|\right) + \frac{1}{2} \\ &= \frac{1}{2}\sum_{x \in \{0,1\}, y \in \mathcal{Y}}\left(\left|\Pr[X = x \mid Y = y]\Pr[Y = y] - \frac{1}{2}\Pr[Y = y]\right|\right) + \frac{1}{2} \\ &= \frac{1}{2}\sum_{x \in \{0,1\}, y \in \mathcal{Y}}(|\Pr[X = x, Y = y] - \Pr[U = x, Y = y]|) + \frac{1}{2} \\ &= \Delta((X,Y),(U,Y)) + \frac{1}{2}\end{aligned}$$

This proves the first statement. The second follows by definition:

$$\tilde{H}_\infty(X \mid Y) = -\log\left(\sum_{y\in\mathcal{Y}}\left(\Pr[Y=y]\max_{x\in\{0,1\}}\Pr[X=x \mid Y=y]\right)\right) = -\log(\max_f \Pr[f(Y)=X])$$

□

Lemma C.10. *If A and B are discrete random variables with support in $\mathcal{X}$ and $f : \mathcal{X} \to \mathcal{Y}$ is any (possibly randomized) function, then*

$$\Delta(f(A), f(B)) \leq \Delta(A, B)$$

Furthermore, if f is a bijection,

$$\Delta(f(A), f(B)) = \Delta(A, B)$$

Proof.

$$\begin{aligned}
\Delta(f(A), f(B)) &= \frac{1}{2}\sum_{y\in\mathcal{Y}} |\Pr[f(A)=y] - \Pr[f(B)=y]| \\
&= \frac{1}{2}\sum_{y\in\mathcal{Y}} \left|\sum_{x\in\mathcal{X}} (\Pr[f(A)=y \mid A=x]\Pr[A=x] - \Pr[f(B)=y \mid B=x]\Pr[B=x])\right| \\
&= \frac{1}{2}\sum_{y\in\mathcal{Y}} \left|\sum_{x\in\mathcal{X}} \Pr[f(x)=y](\Pr[A=x] - \Pr[B=x])\right| \\
&\leq \frac{1}{2}\sum_{y\in\mathcal{Y}}\sum_{x\in\mathcal{X}} \Pr[f(x)=y]\,|(\Pr[A=x] - \Pr[B=x])| \\
&= \frac{1}{2}\sum_{x\in\mathcal{X}} |(\Pr[A=x] - \Pr[B=x])| \\
&= \Delta(A, B)
\end{aligned}$$

If f is a bijection, the statistical distances are equal since $(A, B) = (f^{-1}(f(A)), f^{-1}(f(B)))$ additionally implies that $\Delta(f(A), f(B)) \geq \Delta(A, B)$. □

Notation If f is a function with a binary domain $\{0,1\}$, then for $x = (x_1, \ldots, x_t) \in \{0,1\}^t$, we use $f(x)$ to denote $f(x_1)||\ldots||f(x_t)$.

C.2 Proof

We now prove Theorem 4.17.

Proof.
The theorem follows from the relations below.

- 1 $\iff$ 2. This follows from Theorem 4.11.
- 2 $\iff$ 3. This follows from Theorem 4.14.

- $6 \Rightarrow 5$. A statistically secure wiretap coding scheme for general message spaces can be easily transformed into one for a binary message spaces by ignoring all but the first bit of the message from the general message space.

- $5 \Rightarrow 2$ Although, the correctness and security requirements of a statistically secure wiretap coding scheme are strictly stronger than those of a CK rate-R wiretap coding family, (2) requires the rate R to be positive[8] whereas (5) has no requirement on rate and can be satisfied with rate 0. Thus, our proof though simple is not immediate.

  Assume for contradiction that there is a statistically secure wiretap coding scheme for $(\mathsf{ChB}, \mathsf{ChE})$, but there does not exist a CK Rate-R wiretap coding family for $(\mathsf{ChB}, \mathsf{ChE})$ with positive rate. Let M be a uniform random variable over $\{0,1\}$. By correctness there exists some negligible function $\epsilon(\lambda)$ such that

  $$\Pr[\mathrm{Dec}(1^\lambda, \mathsf{ChB}(\mathrm{Enc}(1^\lambda, M))) = M] \geq 1 - \epsilon(\lambda).$$

  Observe also that

  $$I(M; \mathsf{ChB}(\mathrm{Enc}(1^\lambda, M))) = 1 - H(M \mid \mathsf{ChB}(\mathrm{Enc}(1^\lambda, M)))$$

  Then by Fano's inequality and for sufficiently large λ, we have $H(M \mid \mathsf{ChB}(\mathrm{Enc}(1^\lambda, M))) \leq H(\epsilon(\lambda))$ so that

  $$I(M; \mathsf{ChB}(\mathrm{Enc}(1^\lambda, M))) \geq 1 - H(\epsilon(\lambda)) = 1 - \mathsf{negl}(\lambda)$$

  Moreover, by Theorem 4.16, for Eve, we have that

  $$I(M; \mathsf{ChE}(\mathrm{Enc}(1^\lambda, M))) = \mathsf{negl}(\lambda).$$

  By the above, there exists some $n_0 \in \mathbb{N}$ such that $I(M; \mathsf{ChB}(\mathrm{Enc}(1^{n_0}, M))) \geq 2/3$ and $I(M; \mathsf{ChE}(\mathrm{Enc}(1^{n_0}, M))) \leq 1/3$. Let $\mathrm{Enc}_{n_0} \triangleq \mathrm{Enc}(1^{n_0}, \cdot)$. We now define a new wiretap channel $(\mathsf{ChB}', \mathsf{ChE}')$ where

  $$\mathsf{ChB}' \triangleq \mathsf{ChB} \circ \mathrm{Enc}_{n_0}$$
  $$\mathsf{ChE}' \triangleq \mathsf{ChE} \circ \mathrm{Enc}_{n_0}$$

  are two channels that first apply the encoder with block size n_0 and then apply the original channel ChB (resp. ChE). Then observe that

  $$I(M; \mathsf{ChB}(\mathrm{Enc}_{n_0}(M))) - I(M; \mathsf{ChE}(\mathrm{Enc}_{n_0}(M))) \geq 1/3$$

  so ChE' is not less noisy than ChB'. Then Theorem 4.11 implies there exists a positive rate $R > 0$ CK rate-R code for the $(\mathsf{ChB}', \mathsf{ChE}')$-wiretap channel with encoder-decoder family $\{(\mathrm{Enc}'_n, \mathrm{Dec}'_n)\}$ and message family $\{\mathcal{M}'_n\}$. This CK rate-R wiretap coding family for the $(\mathsf{ChB}', \mathsf{ChE}')$-wiretap channel can be converted into a CK rate-R/n_0 code for the $(\mathsf{ChB}, \mathsf{ChE})$-wiretap channel by constructing the encoder-decoder family

  $$\{(\mathrm{Enc}_{n_0} \circ \mathrm{Enc}'_n, \mathrm{Dec}_{n_0} \circ \mathrm{Dec}'_n)\}_n$$

  with message space $\{\mathcal{M}'_n\}$. Since n_0 is a fixed positive constant, R/n_0 is a positive constant. This contradicts our assumption that there are no positive rate CK coding families for this $(\mathsf{ChB}, \mathsf{ChE})$-wiretap channel.

[8] A CK rate-0 wiretap coding family is ill-posed for security: A zero rate encoding satisfies $\lim_{n\to\infty} \frac{\log|\mathcal{M}_n|}{n} = 0$ so even if Eve learns all information, meaning $I(M_n; Y) = H(M_n) = \log|\mathcal{M}_n|$, Eve would satisfy the security definition as $\lim_{n\to\infty} \frac{1}{n} I(M_n; Y) = 0$.

- $3 \Rightarrow 4$ Suppose that $(\mathrm{Enc}_n, \mathrm{Dec}_n)_{n\in\mathbb{N}}$ satisfies 3 for $(\mathsf{ChB}, \mathsf{ChE})$. Recall the definition of 3:

  Definition C.11 (CK Rate-R Wiretap Coding Family with Strong Secrecy [CK78, MW00])**.** *A family of wiretap encoder-decoder pairs $\{(\mathrm{Enc}_n, \mathrm{Dec}_n)\}_{n\in\mathbb{N}}$ is a rate-R information theoretic wiretap coding family for a wiretap channel $(\mathsf{ChB}, \mathsf{ChE})$ and message family $\{\mathcal{M}_n\}_{n\in\mathbb{N}}$ if each Enc_n outputs an encoding of length n such that*

  - ***Message Rate** R:*
  $$\lim_{n\to\infty} \frac{1}{n} \log |\mathcal{M}_n| = R$$
  - ***Correctness**: For all $m \in \mathcal{M}_n$,*
  $$\Pr[\mathrm{Dec}_n(\mathsf{ChB}(\mathrm{Enc}_n(m))) = m] \geq 1 - \epsilon_n$$
  where
  $$\lim_{n\to\infty} \epsilon_n = 0$$
  - ***Strong Security**:*
  $$\lim_{n\to\infty} I(M_n; \mathsf{ChE}(\mathrm{Enc}_n(M_n))) = 0$$
  where M_n is uniform over $\mathcal{M}_n$.

  We denote the set of all achievable rate pairs as $\mathcal{R}$.

  To construct a 0.99-statistically secure wiretap encoding family for $(\mathsf{ChB}, \mathsf{ChE})$, we first need to move to a binary message space. To do so, we will use an extractor to extract a secure bit from a random message m over the larger message space $\mathcal{M}_n$ which we will then use to pad our binary message b. The 0.99 correctness of the new scheme will follow from the correctness of $(\mathrm{Enc}_n, \mathrm{Dec}_n)$. Then, using the security of the extractor, we can show that Eve's probability of decoding the message is at most $\frac{1}{2} + 0.01$.

  Let $\ell(n) = \lceil \log(|\mathcal{M}_n|) \rceil$. For the remainder of this proof, we will assume that there is some canonical mapping between $\mathcal{M}_n$ and $\{0,1\}^{\ell(n)}$ and will allow for implicit conversions between the two representations.

  - Let $\mathsf{ECC} = (\mathsf{ECC}.\mathrm{Enc}, \mathsf{ECC}.\mathrm{Dec})$ be an error correcting code for ChB for single bit messages such that for $b \in \{0,1\}$,
  $$\Pr[\mathsf{ECC}.\mathrm{Dec}(1^n, \mathsf{ChB}(\mathsf{ECC}.\mathrm{Enc}(1^n, b)))] \geq 1 - \mathsf{negl}(n)$$
  and
  $$|\mathsf{ECC}.\mathrm{Enc}(1^n, b)| = dn$$
  for some constant d.
  - Let $\mathrm{Ext}_n : \{0,1\}^{\ell(n)} \to \{0,1\}$ be a $(\ell(n), \log(nR) - 2, 1, (nR)^{-1/4})$ average case strong extractor that takes r_n bits of randomness. Such an extractor exists for large enough n (i.e. $n > 4/R$) by Corollary C.5 since
  $$1 \leq \log(nR) - 2 - 2\log((nR)^{1/4}) + 2 = \log(nR) - \frac{1}{2}\log(nR) = \frac{1}{2}\log(nR)$$
  Furthermore, for large n, since $\lim_{n\to\infty} \frac{1}{n}\log(|\mathcal{M}_n|) = R$, then $\ell(n) = O(n)$, so $r_n = O(n)$.

  Define $(\mathrm{Enc}'_n, \mathrm{Dec}'_n)_{n\in\mathbb{N}}$ by

$\mathrm{Enc}'_n(b)$:

1. On input a message $b \in \{0,1\}$
2. Sample extractor randomness $v \leftarrow \{0,1\}^{r_n}$.
3. Sample uniform random $x \leftarrow \mathcal{M}_n$.
4. Let $c_1 = \mathsf{ECC}.\mathrm{Enc}(1^n, v, p = (\mathrm{Ext}_n(x; v) \oplus b))$.[a]
5. Let $c_2 = \mathrm{Enc}_n(x)$.
6. Output (c_1, c_2).

$\mathrm{Dec}'_n(c)$:

1. Parse c as $(\mathsf{ChB}(c_1), \mathsf{ChB}(c_2))$.
2. Use $\mathsf{ECC}.\mathrm{Dec}(1^n, \mathsf{ChB}(c_1))$ to recover (v, p).
3. Let $\hat{x} = \mathrm{Dec}_n(\mathsf{ChB}(c_2)) = \mathrm{Dec}_n(\mathsf{ChB}(\mathrm{Enc}_n(x)))$.
4. Output $\mathrm{Ext}_n(\hat{x}; v) \oplus p$.

[a] We use this notation to mean running the error-correcting code on each bit of the input to $\mathsf{ECC}.\mathrm{Enc}$ and similarly for $\mathsf{ECC}.\mathrm{Dec}$.

We claim that for a large enough n^*, $(\mathrm{Enc}^*, \mathrm{Dec}^*) = (\mathrm{Enc}'_{n^*}, \mathrm{Dec}'_{n^*})$ satisfies 4.

Correctness: If the decoder correctly recovers (v, p) and $\hat{x} = x$, then the decoder will output

$$\mathrm{Ext}_n(\hat{x}; v) \oplus p = \mathrm{Ext}_n(\hat{x}; v) \oplus \mathrm{Ext}_n(x; v) \oplus b = b$$

By our choice of error correcting code, since $|(v, p)| = O(n)$, the probability of correctly recovering (v, p) is at least $1 - \mathsf{negl}(n)$. By the correctness of $(\mathrm{Enc}_n, \mathrm{Dec}_n)$, the probability of correctly recovering $\hat{x} = x$ is at least $1 - \epsilon_n$ where $\lim_{n\to\infty} \epsilon_n = 0$. Thus, for large enough n, the decoder outputs the message b with probability at least 0.99.

Security: Let X_n, V_n, B, U be uniform random variables on $\mathcal{M}_n$, $\{0,1\}^{r_n}$, $\{0,1\}$, and $\{0,1\}$ respectively. Let $Z_n = \mathsf{ChE}(\mathrm{Enc}_n(X_n))$. Then, by security of $(\mathrm{Enc}_n, \mathrm{Dec}_n)$ and by Lemma C.7, for large enough n,

$$\begin{aligned}\tilde{H}_\infty(X_n \mid Z_n) &\geq \log\log(|\mathcal{M}_n|) - \log(\log(|\mathcal{M}_n|) - H(X_n) + 2) \\ &= \log\log(|\mathcal{M}_n|) - 1\end{aligned}$$

By the rate property of $(\mathrm{Enc}_n, \mathrm{Dec}_n)$, $\lim_{n\to\infty} \frac{1}{n} \log|\mathcal{M}_n| = R$, so for large enough n,

$$\log|\mathcal{M}_n| \geq \frac{nR}{2}$$

Thus, for large enough n,

$$\tilde{H}_\infty(X_n \mid Z_n) \geq \log\left(\frac{nR}{2}\right) - 1 = \log(nR) - 2$$

Then since Ext is an $(\ell(n), \log(nR) - 2, 1, (nR)^{-1/4})$-average case extractor, for large enough n, we have

$$\Delta((V_n, \mathrm{Ext}(X_n; V_n), Z_n), (V_n, U, Z_n)) \leq (nR)^{-1/4}$$

Claim C.12. *For large n,*

$$\max_f \Pr[f(\mathsf{ChE}(\mathrm{Enc}'_n(B))) = B] \leq \frac{1}{2} + (nR)^{-1/4}$$

where f is taken over all functions.

Proof. By Lemma C.9 and the definition of Enc'_n, we have

$$\begin{aligned}
&\max_f \Pr[f(\mathsf{ChE}(\mathrm{Enc}'_n(B))) = B] \\
&= \frac{1}{2} + \Delta((B, \mathsf{ChE}(\mathrm{Enc}'_n(B))), (U, \mathsf{ChE}(\mathrm{Enc}'_n(B)))) \\
&= \frac{1}{2} + \Delta((B, \mathsf{ChE}(\mathsf{ECC}.\mathrm{Enc}(1^n, V_n, \mathrm{Ext}(X_n; V_n) \oplus B)), Z_n), \\
&\qquad\qquad (U, \mathsf{ChE}(\mathsf{ECC}.\mathrm{Enc}(1^n, V_n, \mathrm{Ext}(X_n; V_n) \oplus B)), Z_n))
\end{aligned}$$

Then, by Lemma C.10,

$$\begin{aligned}
&\Delta((B, \mathsf{ChE}(\mathsf{ECC}.\mathrm{Enc}(1^n, V_n, \mathrm{Ext}(X_n; V_n) \oplus B)), Z_n), (U, \mathsf{ChE}(\mathsf{ECC}.\mathrm{Enc}(1^n, V_n, \mathrm{Ext}(X_n; V_n) \oplus B)), Z_n)) \\
&\leq \Delta((B, V_n, \mathrm{Ext}(X_n; V_n) \oplus B, Z_n), (U, V_n, \mathrm{Ext}(X_n; V_n) \oplus B, Z_n)) \\
&= \Delta((B, V_n, \mathrm{Ext}(X_n; V_n), Z_n), (U, V_n, \mathrm{Ext}(X_n; V_n) \oplus B \oplus U, Z_n))
\end{aligned}$$

Furthermore, since (B, U) is independent of $(V_n, \mathrm{Ext}(X_n; V_n), Z_n)$, we have

$$\begin{aligned}
&\Delta((B, V_n, \mathrm{Ext}(X_n; V_n), Z_n), (U, V_n, \mathrm{Ext}(X_n; V_n) \oplus B \oplus U, Z_n)) \\
&= \Delta((B, V_n, \mathrm{Ext}(X_n; V_n), Z_n), (B, V_n, \mathrm{Ext}(X_n; V_n) \oplus U \oplus B, Z_n)) \\
&= \Delta((B, V_n, \mathrm{Ext}(X_n; V_n), Z_n), (B, V_n, U, Z_n)) \\
&= \Delta((V_n, \mathrm{Ext}(X_n; V_n), Z_n), (V_n, U, Z_n)) \\
&\leq (nR)^{-1/4}
\end{aligned}$$

and the claim follows. □

Thus, for large enough n^*, we have that $\max_f \Pr[f(\mathsf{ChE}(\mathrm{Enc}'_{n^*}(B))) = B] \leq \frac{1}{2} + 0.01$.

Rate For any $b \in \{0,1\}$, for some fixed n^*,

$$\mathrm{Enc}^*(b) = \mathrm{Enc}'_{n^*}(b) = (\mathsf{ECC}.\mathrm{Enc}(1^{n^*}, v, \mathrm{Ext}_{n^*}(x; v) \oplus b), \mathrm{Enc}_{n^*}(x))$$

and it is then easy to observe that $|\mathrm{Enc}^*(b)|$ is a constant.

- $4 \Rightarrow 6$ Let $(\mathsf{ChB}, \mathsf{ChE})$ be a wiretap channel. We claim that the following construction is a statistically secure wiretap coding scheme for general messages space for $(\mathsf{ChB}, \mathsf{ChE})$ with positive constant rate.

  Construction 1. We will construct 6 from the following ingredients:

  - A wiretap coding $(\mathrm{Enc}^*, \mathrm{Dec}^*)$ satisfying
    - **Rate**: For all $b \in \{0,1\}, |\mathrm{Enc}^*(b)| = c$ for some constant c.

∗ **Correctness**: For all $b \in \{0,1\}$,

$$\Pr[\mathrm{Dec}^*(\mathsf{ChB}(\mathrm{Enc}^*(b))) = b] \geq 0.95$$

∗ **Security**:

$$\tilde{H}_\infty(B \mid \mathsf{ChE}(\mathrm{Enc}^*(B))) \geq 0.95$$

where B is uniform over $\{0,1\}$.

Note that a wiretap coding $(\mathrm{Enc}^*, \mathrm{Dec}^*)$ satisfying 4 also satisfies this definition as

$$\max_f \Pr[f(\mathsf{ChE}(\mathrm{Enc}^*(B))) = B] \leq \frac{1}{2} + 0.01$$

implies by Lemma C.9 that

$$\tilde{H}_\infty(B \mid \mathsf{ChE}(\mathrm{Enc}^*(B))) = -\log(\max_f \Pr[f(\mathsf{ChE}(\mathrm{Enc}^*(B))) = B]) \geq 0.95$$

– An error-correcting code $\mathsf{ECC} = (\mathsf{ECC}.\mathrm{Enc}, \mathsf{ECC}.\mathrm{Dec})$ for single bit messages for ChB such that for $b \in \{0,1\}$,

$$\Pr[\mathsf{ECC}.\mathrm{Dec}(1^\lambda, \mathsf{ChB}(\mathsf{ECC}.\mathrm{Enc}(1^\lambda, b)] \geq 1 - \mathsf{negl}(\lambda)$$

and

$$|\mathsf{ECC}.\mathrm{Enc}(1^\lambda, b)| = d\lambda$$

for some constant d.

– A universal hash family $\mathcal{H}_\lambda \triangleq \left\{H_k : \{0,1\}^\lambda \to \{0,1\}^{0.6\lambda}\right\}_{k \in \mathcal{K}_\lambda}$ where $\log(|\mathcal{K}_\lambda|) = O(\lambda)$.

– An efficient average-case $(\lambda, 0.35\lambda, 0.1\lambda, 2^{-0.1\lambda})$-strong extractor $\mathrm{Ext}_\lambda : \{0,1\}^\lambda \times \{0,1\}^{r_\lambda} \to \{0,1\}^{0.1\lambda}$ that take $r_\lambda = O(\lambda)$ bits of randomness. Such an extractor exists by Corollary C.5 since

$$0.1\lambda \leq 0.35\lambda - 2\log(2^{0.1\lambda}) + 2 = 0.35\lambda - 0.2\lambda + 2 = 0.15\lambda + 2$$

We now define our wiretap encoding scheme which has message length $\ell(n) = 0.1\lambda$.

$\mathrm{Enc}(1^\lambda, m)$:

1. On input a message $m \in \{0,1\}^{0.1\lambda} = \{0,1\}^{\ell(\lambda)}$
2. Sample a hash key $k \leftarrow \mathcal{K}_\lambda$ and extractor randomness $v \leftarrow \{0,1\}^{r_\lambda}$.
3. Sample a uniform random $x \leftarrow \{0,1\}^\lambda$.
4. Let $c_1 = \mathsf{ECC}.\mathrm{Enc}(1^\lambda, k, v, y = H_k(x), p = (\mathrm{Ext}_\lambda(x; v) \oplus m))$.
5. Let $c_2 = \mathrm{Enc}^*(x)$.
6. Output (c_1, c_2).

$\mathrm{Dec}(1^\lambda, c)$:

1. Parse c as $(\mathsf{ChB}(c_1), \mathsf{ChB}(c_2))$.
2. Use $\mathsf{ECC}.\mathrm{Dec}(1^\lambda, \mathsf{ChB}(c_1))$ to recover (k, v, y, p).
3. Let $\hat{x} = \mathrm{Dec}^*(\mathsf{ChB}(c_2)) = \mathrm{Dec}^*(\mathsf{ChB}(\mathrm{Enc}^*(x)))$.

4. Compute all elements in the set

$$T_{\hat{x}} \triangleq \left\{ x' \in \{0,1\}^\lambda \mid H_k(x') = y \wedge \Delta_H(x', \hat{x}) < 0.1\lambda \right\}$$

where $\Delta_H(x', \hat{x})$ is the hamming distance between x' and $\hat{x}$. If $T_{\hat{x}}$ is a singleton element x^*, return $\mathrm{Ext}_\lambda(x^*; v) \oplus p$. Otherwise return $\perp$.

Correctness: We need to show that for all messages $m \in \{0,1\}^{\ell(\lambda)}$,

$$\Pr[\mathrm{Dec}(1^\lambda, \mathsf{ChB}(\mathrm{Enc}(1^\lambda, m))) = m] \geq 1 - \mathsf{negl}(\lambda)$$

First, we assume that the decoder correctly recovers $(k, v, y = H_k(x), p = (\mathrm{Ext}_\lambda(x; v) \oplus m))$. By our choice of error-correcting code ECC for ChB, this occurs with overwhelming probability. We will also assume $x \in T_{\hat{x}}$. By a Chernoff bound, if $\hat{x} = \mathrm{Dec}^*(\mathsf{ChB}(c_2)) = \mathrm{Dec}^*(\mathsf{ChB}(\mathrm{Enc}^*(x)))$, by the 0.95 correctness of $(\mathrm{Enc}^*, \mathrm{Dec}^*)$, $\Delta_H(\hat{x}, x) < 0.1\lambda$ with overwhelming probability so $x \in T_{\hat{x}}$ with overwhelming probability. We now claim that $T_{\hat{x}}$ is a singleton element $x^* = x$ with all but negligible probability. Observe by definition of $T_{\hat{x}}$ that

$$|T_{\hat{x}}| \leq \binom{\lambda}{0.1\lambda} \leq \left(\frac{e\lambda}{0.1\lambda}\right)^{0.1\lambda} = (10e)^{0.1\lambda} \leq 2^{0.5\lambda}$$

Then, for any fixed x and for any $x' \in \{0,1\}^\lambda$, since $\mathcal{H}$ is a universal hash function, we have

$$\Pr_{k \leftarrow \mathcal{K}_\lambda}[H_k(x) = H_k(x')] \leq 2^{-0.6\lambda}$$

Therefore, by a union bound,

$$\Pr_{k \leftarrow \mathcal{K}_\lambda}[\exists x' \in T_{\hat{x}} \mid x' \neq x \wedge H_k(x') = H_k(x)] \leq 2^{-0.6\lambda} \cdot 2^{0.5\lambda} = 2^{-0.1\lambda} = \mathsf{negl}(\lambda)$$

Thus, with overwhelming probability, $T_{\hat{x}}$ is a singleton element $x^* = x$, which means that the decoder outputs $\mathrm{Ext}_\lambda(x^*; v) \oplus p = \mathrm{Ext}_\lambda(x^*; v) \oplus \mathrm{Ext}_\lambda(x; v) \oplus m = m$ with overwhelming probability.

Security: We need to show that for all adversaries $\mathcal{A}$ and all messages $m_0 \neq m_1 \in \{0,1\}^{\ell(n)}$,

$$\Pr[\mathcal{A}(1^\lambda, m_0, m_1, \mathsf{ChE}(\mathrm{Enc}(1^\lambda, m_B))) = B] \leq \frac{1}{2} + \mathsf{negl}(\lambda)$$

where B is uniformly distributed over $\{0,1\}$. Let (m_0, m_1) be any two messages of length $\ell(n)$, and let $\mathcal{A}$ be any adversary. Let B and U be uniform random variables over $\{0,1\}$. Let $X_\lambda = (X_\lambda^{(1)}, \ldots, X_\lambda^{(\lambda)})$ where each $X_\lambda^{(i)}$ is an independently and identically distributed uniform random variable over $\{0,1\}$, and let $Z_\lambda = (Z_\lambda^{(1)}, \ldots, Z_\lambda^{(\lambda)})$ where $Z_\lambda^{(i)} = \mathsf{ChE}(\mathrm{Enc}^*(X_\lambda^{(i)}))$. Let K_λ, V_λ be uniform random variables over $\mathcal{K}_\lambda$ and $\{0,1\}^{r_\lambda}$ respectively, and let $Y_\lambda = H_{K_\lambda}(X_\lambda)$. First we show the following claim:

Claim C.13.

$$\Delta((K_\lambda, Y_\lambda, V_\lambda, \mathrm{Ext}_\lambda(X_\lambda; V_\lambda), Z_\lambda), (K_\lambda, Y_\lambda, V_\lambda, U_{0.1\lambda}, Z_\lambda)) \leq 2^{-0.1\lambda}$$

where $U_{0.1\lambda}$ is uniform over $\{0,1\}^{0.1\lambda}$.

Proof. Since Ext_λ is a $(\lambda, 0.35\lambda, 0.1\lambda, 2^{-0.1\lambda})$-average case extractor, it suffices to prove that

$$\tilde{H}_\infty(X_\lambda \mid K_\lambda, Y_\lambda, Z_\lambda) \geq 0.35\lambda$$

Now, since $|Y_\lambda| = 0.6\lambda$, by Lemma C.8,

$$\tilde{H}_\infty(X_\lambda \mid K_\lambda, Y_\lambda, Z_\lambda) \geq \tilde{H}_\infty(X_\lambda \mid K_\lambda, Z_\lambda) - 0.6\lambda$$

Then since K_λ is independent of (X_λ, Z_λ), we have

$$\tilde{H}_\infty(X_\lambda \mid K_\lambda, Z_\lambda) = \tilde{H}_\infty(X_\lambda \mid Z_\lambda)$$

Then by Lemma C.6 and by the security property of $(\mathrm{Enc}^*, \mathrm{Dec}^*)$,

$$\tilde{H}_\infty(X_\lambda \mid Z_\lambda) = \sum_{i=1}^{n} \tilde{H}_\infty(X_\lambda^{(i)} \mid Z_\lambda^{(i)}) \geq 0.95\lambda$$

Therefore, we get

$$\tilde{H}_\infty(X_\lambda \mid K_\lambda, Y_\lambda, Z_\lambda) \geq 0.95\lambda - 0.6\lambda = 0.35\lambda$$

□

By Lemma C.9 and Lemma C.10 and since (B, U) is independent of $(X_\lambda, V_\lambda, K_\lambda, Z_\lambda)$, we have

$$\begin{aligned}
&\Pr[\mathcal{A}(1^\lambda, m_0, m_1, \mathsf{ChE}(\mathrm{Enc}(1^\lambda, m_B))) = B] \\
&\leq \max_{\mathcal{A}} \Pr[\mathcal{A}(1^\lambda, m_0, m_1, \mathsf{ChE}(\mathrm{Enc}(1^\lambda, m_B))) = B] \\
&= \max_{\mathcal{A}} \Pr[\mathcal{A}(1^\lambda, m_0, m_1, \mathsf{ChE}(\mathsf{ECC}.\mathrm{Enc}(1^\lambda, K_\lambda, V_\lambda, Y_\lambda, \mathrm{Ext}_\lambda(X_\lambda; V_\lambda) \oplus m_B)), Z_\lambda) = B] \\
&= \frac{1}{2} + \Delta((B, 1^\lambda, m_0, m_1, \mathsf{ChE}(\mathsf{ECC}.\mathrm{Enc}(1^\lambda, K_\lambda, V_\lambda, Y_\lambda, \mathrm{Ext}_\lambda(X_\lambda; V_\lambda) \oplus m_B)), Z_\lambda), \\
&\qquad\qquad (U, 1^\lambda, m_0, m_1, \mathsf{ChE}(\mathsf{ECC}.\mathrm{Enc}(1^\lambda, K_\lambda, V_\lambda, Y_\lambda, \mathrm{Ext}_\lambda(X_\lambda; V_\lambda) \oplus m_B)), Z_\lambda)) \\
&\leq \frac{1}{2} + \Delta((B, K_\lambda, V_\lambda, Y_\lambda, \mathrm{Ext}_\lambda(X_\lambda; V_\lambda) \oplus m_B, Z_\lambda), (U, K_\lambda, V_\lambda, Y_\lambda, \mathrm{Ext}_\lambda(X_\lambda; V_\lambda) \oplus m_B, Z_\lambda)) \\
&= \frac{1}{2} + \Delta((B, K_\lambda, V_\lambda, Y_\lambda, \mathrm{Ext}_\lambda(X_\lambda; V_\lambda), Z_\lambda), (U, K_\lambda, V_\lambda, Y_\lambda, \mathrm{Ext}_\lambda(X_\lambda; V_\lambda) \oplus m_B \oplus m_U, Z_\lambda)) \\
&= \frac{1}{2} + \Delta((B, K_\lambda, V_\lambda, Y_\lambda, \mathrm{Ext}_\lambda(X_\lambda; V_\lambda), Z_\lambda), (B, K_\lambda, V_\lambda, Y_\lambda, \mathrm{Ext}_\lambda(X_\lambda; V_\lambda) \oplus m_U \oplus m_B, Z_\lambda))
\end{aligned}$$

Then, using the claim, Lemma C.10, and the fact that B is independent of $(K_\lambda, Y_\lambda, V_\lambda, Z_\lambda)$, we have that

$$\Delta((B, K_\lambda, Y_\lambda, V_\lambda, \mathrm{Ext}_\lambda(X_\lambda; V_\lambda), Z_\lambda), (B, K_\lambda, Y_\lambda, V_\lambda, U_{0.1\lambda}, Z_\lambda)) \leq 2^{-0.1\lambda}$$

and similarly that

$$\Delta((B, K_\lambda, Y_\lambda, V_\lambda, \mathrm{Ext}_\lambda(X_\lambda; V_\lambda) \oplus m_B \oplus m_U, Z_\lambda), (B, K_\lambda, Y_\lambda, V_\lambda, U_{0.1\lambda}, Z_\lambda)) \leq 2^{-0.1\lambda}$$

Therefore,

$$\Delta((B, K_\lambda, V_\lambda, Y_\lambda, \mathrm{Ext}_\lambda(X_\lambda; V_\lambda), Z_\lambda), (B, K_\lambda, V_\lambda, Y_\lambda, \mathrm{Ext}_\lambda(X_\lambda; V_\lambda) \oplus m_U \oplus m_B, Z_\lambda)) \leq 2 \cdot 2^{-0.1\lambda}$$

and so

$$\Pr[\mathcal{A}(1^\lambda, m_0, m_1, \mathsf{ChE}(\mathrm{Enc}(1^\lambda, m_B))) = B] \leq \frac{1}{2} + 2 \cdot 2^{-0.1\lambda} = \frac{1}{2} + \mathsf{negl}(\lambda)$$

Rate For a message $m \in \{0,1\}^{0.1(\lambda)}$, the encoding of m is $(c_1, c_2) = (\mathsf{ECC}.\mathrm{Enc}(1^\lambda, k, v, y = H_k(x), p = (\mathrm{Ext}_\lambda(x; v) \oplus m)), \mathrm{Enc}^*(x))$. Then, we have

- $|k| = O(\lambda)$
- $|v| = O(\lambda)$
- $|y| = 0.6\lambda$
- $|p| = 0.1\lambda$
- Thus, since ECC is a constant rate error correcting code, we have $|c_1| = O(\lambda)$.
- Since for any bit b, $|\mathrm{Enc}^*(b)|$ is constant and since $|x| = \lambda$, then $|c_2| = |\mathrm{Enc}^*(x)| = O(\lambda)$.

Therefore, $|c_1, c_2| = O(\lambda)$. Thus, the rate is a positive constant.

□