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

Yuval Ishai[1], Alexis Korb[2], Paul Lou[3], and Amit Sahai[4]

[1] Technion, Haifa, Israel, yuvali@cs.technion.ac.il
[2] UCLA, Los Angeles, USA, alexiskorb@cs.ucla.edu
[3] UCLA, Los Angeles, USA, pslou@cs.ucla.edu
[4] UCLA, Los Angeles, USA, sahai@cs.ucla.edu

[5] The full version of this paper can be found at
https://eprint.iacr.org/2022/343.pdf

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.

1 Introduction

The wiretap channel, first introduced by Wyner [26], 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 [26] 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., [24] for a survey.

The classic work of Csiszár and Korner [10] 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 (see Definition 8), 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 [23] that Eve's channel is not less noisy than Bob's channel if and only if $\epsilon > 0.36 = 4p(1-p)$, and thus by [10], 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 [6,27] to the feasibility of secure multi-party computation with a dishonest majority [14]. However, despite the popularity of Wyner's work, no improvement over [10] 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 she receives a uniform value in $\{0, 1\}$, 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 [9]. 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 [10,23] 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.[6]

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 (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 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. [1], 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).

[6] 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 for more details).

In our second step, we show how to bootstrap from Theorem 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* [3], 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 across Eve's channel (see Section 7 for details). Using this kind of obfuscation, we obtain the following result in the plain model:

Theorem 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 [18] 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. [4,15]). 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 simple auxiliary information about the obfuscated function.

- Furthermore, in fact, the work of [2] 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" [17], 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 $(\mathrm{Enc}, \mathrm{Dec})$ 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. [1], 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 [1] 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 [1] and our work.

Another closely related line of work studies the notion of fuzzy extractors, introduced by Dodis et al. [11]. 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. [7] and Fuller et al. [12]. 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 [21] 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 [22] 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 [23] studied information-theoretic relationships between BSC and BEC channels.

Bellare et al. [5] 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.

Finally, the wiretap problem we study is also related to other fuzzy cryptographic primitives, including fuzzy vaults [19] and fuzzy commitments [20]. However, our work is technically incomparable because they use different definitions of noise and study security in different regimes. In both cases, the achieved parameters are not optimal (certainly not in a computational setting), whereas our construction achieves the best possible parameters.

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 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 [10,23] 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 (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 thus learn as much information as 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 3. *Let $\mathcal{X}$ and $\mathcal{Y}$ be any two discrete finite sets and let $n \in \mathbb{N}$. 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.[7]

```
$h_{m,r,\mathsf{ChB},n}(r_B)$:
    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 that considers only one-sided bounds.

[7] 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.

```
$f_{m,r,\mathsf{ChB},n}(r_B)$:
    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 $r_B \in \mathcal{Y}^n$ 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.

```
$\mathrm{Enc}_{\mathsf{ChB}}(1^\lambda, m)$:
  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 $f_{b,r,\mathsf{ChB},n}(\widehat{r}_B) = f_{b,r,\mathsf{ChB},n}(g(r_E)) = b$. 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 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 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 $N_{z_i}(r_E) = |i \in [n] \mid r_{E_i} = z_i|$. We define an equivalence relation $\textsc{EqWt}$ 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 $k_{z,y}$ 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 $\mathsf{Ch}_{r_E}$ 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 $\mathsf{Ch}_w$ from $\mathcal{Z}$ to $\mathcal{Y}$ by stochastic matrix

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

  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 6 (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*

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

Remark 1. 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.

Definition 7 (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

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

Whenever we discuss channels in the context of efficient algorithms, we assume all channels have finite description size with constant alphabet size and rational probabilities.

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.

Less Noisy and Channel Degradation

Definition 8 (Less Noisy, [10]). *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 9 (Channel Degradation, [9]). *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 10 (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.

Remark 2 (Notions of Degradation). The notion of degradation defined above is sometimes referred to as *stochastic* degradation. There is also a notion of *physical* degradation. (See [25] for further discussion.) However, the difference between these notions is irrelevant in the current context.

Provided in the full version, we obtain the following Lemma:

Lemma 1. *If channel* ChB *is not a degradation of channel* ChE, *then there exists a constant* $d > 0$ *such that for all stochastic matrices* $P_S = [p_S(y \mid z)]_{z \in \mathcal{Z}, y \in \mathcal{Y}}$,

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

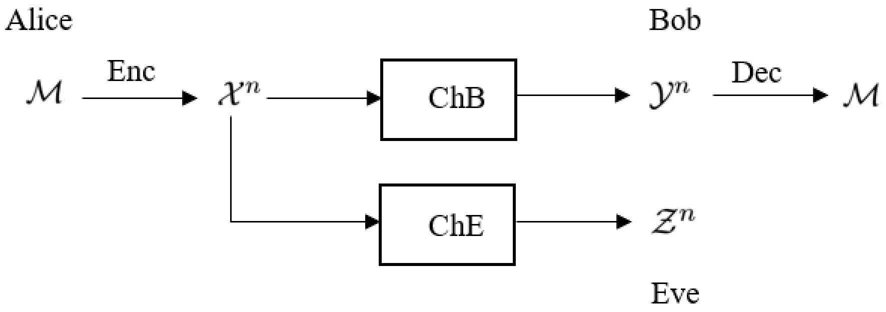
where $P_B = [p_B(y \mid x)]_{x \in \mathcal{X}, y \in \mathcal{Y}}$ *is the stochastic matrix of* ChB *and* $P_E = [p_E(z \mid x)]_{x \in \mathcal{X}, z \in \mathcal{Z}}$ *is the stochastic matrix of* ChE.

Proof. We defer the proof to the full version.

4 Wiretap Channels

A wiretap channel [26,10] 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 11 (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 [5][8], we use the standard notion of semantic security [16]. 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 the full version.)

Definition 12 (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.*

[8] Our security definition corresponds to requiring the distinguishing advantage Adv^{ds} of [5] to be negligible. [5] define a separate notion for semantic security, but prove that the two definitions are equivalent.

Definition 13 (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 $(\mathsf{ChB}, \mathsf{ChE})$.

4.1 Ideal Obfuscation Model

Similarly to the recent use of obfuscation in [1], 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 3 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 14 (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 15 (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 $\{0,1\}$.

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

Theorem 3. ChE *is not less noisy than* ChB *if and only if there exists a statistically secure wiretap coding scheme for* $(\mathsf{ChB}, \mathsf{ChE})$.[9]

Proof. We defer the proof to the full version.

Remark 3 (Computationally bounded adversaries). Definition 15 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 13.

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

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 to be a uniform random variable over $\mathcal{X}^n$, $R_B \coloneqq \mathsf{ChB}(R)$, and $R_E \coloneqq \mathsf{ChE}(R)$. 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 16. *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*

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

[9] This is also true with respect to statistically secure wiretap coding schemes over larger message spaces (see the full version).

Definition 17. *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 4. *If $(\mathsf{ChB}, \mathsf{ChE})$ is a wiretap channel where ChB is not a degradation of ChE, then $(\mathrm{Enc}_{\mathsf{ChB}}, \mathrm{Dec}^{(\cdot)}_{\mathsf{ChB}})$ 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 a simple Chernoff bound which we defer to the full version. Security follows by Theorem 7 which are proven below.

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

Corollary 1. *If* $(\mathsf{ChB}, \mathsf{ChE})$ *is a wiretap channel where* ChB *is not a degradation of* ChE*, then* $(\mathrm{Enc}_{\mathsf{ChB}}, \mathrm{Dec}_{\mathsf{ChB}}^{(\cdot)})$ *is a bounded query secure wiretap coding scheme in the ideal obfuscation model.*

Remark 4. Theorem 4 and Corollary 1 hold even if we modify $f_{m,r,\mathsf{ChB},n}$ to have binary output domain by outputting 0 in place of $\bot$. Correctness still holds since the probability that the decoder using the original function outputs $\bot$ is negligible, so changing $\bot$ to 0 results in at most a negligible change in correctness. For security, observe that by outputting 0 instead of $\bot$, 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.

5.1 Security

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 $f_{b,r,\mathsf{ChB},n}(\widehat{r}_B) \neq \bot$, 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 18. *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,

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

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 $g, \textsc{Eve}_0, \textsc{Eve}_1, \textsc{Eve}_2, \textsc{Eve}_3$ that strategy g is only polynomially better that 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 not-degraded condition to show that $\textsc{Eve}_3$'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 19. *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. 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 20. *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 $\textsc{EqWt}$ *on $\mathcal{Z}^n \times \mathcal{Z}^n$ by*

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

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

Definition 21. *Let $r_{E\,w,0}$ denote the lexicographically first vector in the equivalence class $\{r_E \in \mathcal{Z}^n \mid \mathsf{wt}(r_E) = w\}$.*

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

First, we prove a fact about symmetry.

Lemma 2. *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. We defer the proof to the full version.

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 3. *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. We defer the proof to the full version.

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 6. 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 4. *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. We defer the proof to the full version.

Randomized Locations 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 $r_E \in \mathcal{Z}^n$, $\textsc{Eve}_0$ maps 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, $\textsc{Eve}_1$, will map a random subset of size $k_{z,y}$ of the y's in r_E to be a z in $\widehat{r}_B$.

More formally, we define $\textsc{Eve}_1$ as follows.

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

1. $\forall y \in \mathcal{Y}, z \in \mathcal{Z}$, 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 $\widehat{r}_B$.
```

Remark 7. Observe that for any fixed randomness e of $\textsc{Eve}_1$ and any $r_E \in \mathcal{Z}^n$, then there exists a permutation $\pi_e \in S_n$ such that $\textsc{Eve}_1(r_E; e) = \pi_e(\textsc{Eve}_0(r_E))$ where $\pi_e(r_E) = r_E$.

We show that such a probabilistic $\textsc{Eve}_1$ has the same success probability as $\textsc{Eve}_0$.

Lemma 5.

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

Proof. We defer the proof to the full version.

Stochastic Matrix Strategy Consider a probabilistic $\textsc{Eve}_2$ that on input $r_E \in \mathcal{Z}^n$ defines a new channel Ch_{r_E} from $\mathcal{Z}$ to $\mathcal{Y}$ such that $p_{r_E}(z \mid y) = \textsc{Ratio}_{z \to y}(r_E, \textsc{Eve}_0(r_E))$ and applies this channel to each symbol of r_E to get $\widehat{r}_B$.

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

1. Define a channel $\mathsf{Ch}_{r_E}$ 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 $\textsc{Eve}_1(r_E)$.

Definition 22.
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 6. $\Pr_{R,\mathsf{ChE}}[r_E \in \textsc{Good}_E] \geq 1 - \mathsf{negl}(\lambda)$

Proof. We defer the proof to the full version.

Lemma 7. *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*

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

Proof. We defer the proof to the full version.

Corollary 2. *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. We defer the proof to the full version.

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 $r_{E w,0} \in \mathcal{Z}^n$ be the lexicographically first vector of weight $w$.
  2. Define a channel $\mathsf{Ch}_w$ from $\mathcal{Z}$ to $\mathcal{Y}$ by stochastic matrix
       $P_w = [p_w(y \mid z)]_{z \in \mathcal{Z}, y \in \mathcal{Y}} = [\textsc{Ratio}_{z \to y}(r_{E w,0}, \textsc{Eve}_0(r_{E w,0}))]_{z \in \mathcal{Z}, y \in \mathcal{Y}}$
  3. For $i \in [n]$, set $\widehat{r}_{B i} = \mathsf{Ch}_w(r_{E i})$.
  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 8. *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. We defer the proof to the full version.

Corollary 3. *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 8 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 9.

$$\Pr_{R,\mathsf{ChE},\textsc{Eve}_3,W}[h_{R,\mathsf{ChB},n}(\textsc{Eve}_3(W, R_E)) = 1] \geq \frac{1}{q(n)} \cdot \Pr_{R,\mathsf{ChE},\textsc{Eve}_2}[h_{R,\mathsf{ChB},n}(\textsc{Eve}_2(R_E)) = 1]$$

where $q(n) = \binom{n+|\mathcal{Z}|-1}{|\mathcal{Z}|-1} = |\mathcal{W}_n| = \mathsf{poly}(n)$.

Proof. We defer the proof to the full version.

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.

Lemma 10.

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

Proof. We defer the proof to the full version.

Putting it Together

Theorem 5. *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 4, $\textsc{Eve}_0$ is an optimal strategy so

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

Then, by Lemma 5, Corollary 2, Lemma 9, and Lemma 10 for some polynomials $p(n), q(n) = \mathsf{poly}(n)$,

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

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

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

implies

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

Proof. We defer the proof to the full version.

Therefore, we obtain

Theorem 6. *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. We defer the proof to the full version.

We now prove full security.

Theorem 7. *For every polynomial query bound $q(\lambda)$ and (computationally unbounded) adversary $\mathcal{A}^{(\cdot)}$ that makes at most $q(\lambda)$ queries to its oracle,*

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

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

Proof. We defer the proof to the full version.

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 23 (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 $\mathcal{M}$.*

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 8. *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 1 and the observation that $(\mathrm{Enc}_{\mathsf{ChB}}, \mathrm{Dec}^{(\cdot)}_{\mathsf{ChB}})$ only depend on ChB.

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.

We defer further discussion on this to the full version.

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 24 (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 [3,2]. 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 [15], which is ruled out in the statistically evasive case; or *(ii)* "feeding an obfuscated circuit to itself" [4] 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 [2], which is itself a generalization of the standard average-case VBB definition of obfuscation [4], but extended to consider auxiliary input. The work of [2] gives a construction achieving this definition for evasive functions based on multilinear map candidates [13,8], 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 [18] also gives a plausible candidate for obfuscating our oracle.

Here, our definition slightly extends the average-case VBB definition given in [2] 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 [2] is oblivious to this change. We also restrict our notion of obfuscation to statistically evasive circuits collections with auxiliary input.

Definition 25 (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 24. 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 $(D, \mathsf{Aux}) \in \mathscr{G}$,*

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

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.

We defer this section to the full version.

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.

We defer this section to the full version.

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. We use the definition of indistinguishability obfuscation ($i\mathcal{O}$) defined in [18].

Following the discussion on $i\mathcal{O}$ in [1], we note that $i\mathcal{O}$ is a "best-possible" obfuscation [17]. 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 show in the full version that $i\mathcal{O}$ still behaves as a best possible obfuscation.

Acknowledgements. 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. We would also like to thank Mark Zhandry for his useful comments.

References

1. Agrawal, S., Ishai, Y., Kushilevitz, E., Narayanan, V., Prabhakaran, M., Prabhakaran, V., Rosen, A.: Secure computation from one-way noisy communication, or: Anti-correlation via anti-concentration. In: CRYPTO (2021)
2. Badrinarayanan, S., Miles, E., Sahai, A., Zhandry, M.: Post-zeroizing obfuscation: New mathematical tools, and the case of evasive circuits. In: Fischlin, M., Coron, J.S. (eds.) Advances in Cryptology – EUROCRYPT 2016, Part II. Lecture Notes in Computer Science, vol. 9666, pp. 764–791. Springer, Heidelberg, Germany, Vienna, Austria (May 8–12, 2016)
3. Barak, B., Bitansky, N., Canetti, R., Kalai, Y.T., Paneth, O., Sahai, A.: Obfuscation for evasive functions. In: Theory of Cryptography Conference. pp. 26–51. Springer (2014)
4. Barak, B., Goldreich, O., Impagliazzo, R., Rudich, S., Sahai, A., Vadhan, S.P., Yang, K.: On the (im)possibility of obfuscating programs. In: Kilian, J. (ed.) Advances in Cryptology – CRYPTO 2001. Lecture Notes in Computer Science, vol. 2139, pp. 1–18. Springer, Heidelberg, Germany, Santa Barbara, CA, USA (Aug 19–23, 2001)
5. Bellare, M., Tessaro, S., Vardy, A.: Semantic security for the wiretap channel. In: Safavi-Naini, R., Canetti, R. (eds.) Advances in Cryptology - CRYPTO 2012 - 32nd Annual Cryptology Conference, Santa Barbara, CA, USA, August 19-23, 2012. Proceedings. Lecture Notes in Computer Science, vol. 7417, pp. 294–311. Springer (2012), https://doi.org/10.1007/978-3-642-32009-5_18
6. Blum, M., Micali, S.: How to generate cryptographically strong sequences of pseudorandom bits. SIAM journal on Computing 13(4), 850–864 (1984)
7. Canetti, R., Fuller, B., Paneth, O., Reyzin, L., Smith, A.D.: Reusable fuzzy extractors for low-entropy distributions. J. Cryptol. 34(1), 2 (2021), earlier version in Eurcrypt 2016
8. Coron, J.S., Lepoint, T., Tibouchi, M.: Practical multilinear maps over the integers. In: Canetti, R., Garay, J.A. (eds.) Advances in Cryptology – CRYPTO 2013, Part I. Lecture Notes in Computer Science, vol. 8042, pp. 476–493. Springer, Heidelberg, Germany, Santa Barbara, CA, USA (Aug 18–22, 2013)
9. Cover, T.: Broadcast channels. IEEE Transactions on Information Theory 18(1), 2–14 (1972)
10. Csiszár, I., Korner, J.: Broadcast channels with confidential messages. IEEE transactions on information theory 24(3), 339–348 (1978)
11. Dodis, Y., Ostrovsky, R., Reyzin, L., Smith, A.D.: Fuzzy extractors: How to generate strong keys from biometrics and other noisy data. SIAM J. Comput. 38(1), 97–139 (2008)

12. Fuller, B., Meng, X., Reyzin, L.: Computational fuzzy extractors. Inf. Comput. 275, 104602 (2020), earlier version in Asiacrypt 2013
13. Garg, S., Gentry, C., Halevi, S.: Candidate multilinear maps from ideal lattices. In: Johansson, T., Nguyen, P.Q. (eds.) Advances in Cryptology – EUROCRYPT 2013. Lecture Notes in Computer Science, vol. 7881, pp. 1–17. Springer, Heidelberg, Germany, Athens, Greece (May 26–30, 2013)
14. Goldreich, O., Micali, S., Wigderson, A.: How to play any mental game or A completeness theorem for protocols with honest majority. In: Aho, A. (ed.) 19th Annual ACM Symposium on Theory of Computing. pp. 218–229. ACM Press, New York City, NY, USA (May 25–27, 1987)
15. Goldwasser, S., Kalai, Y.T.: On the impossibility of obfuscation with auxiliary input. In: 46th Annual Symposium on Foundations of Computer Science. pp. 553–562. IEEE Computer Society Press, Pittsburgh, PA, USA (Oct 23–25, 2005)
16. Goldwasser, S., Micali, S.: Probabilistic encryption. Journal of computer and system sciences 28(2), 270–299 (1984)
17. Goldwasser, S., Rothblum, G.N.: On best-possible obfuscation. In: Vadhan, S.P. (ed.) TCC 2007: 4th Theory of Cryptography Conference. Lecture Notes in Computer Science, vol. 4392, pp. 194–213. Springer, Heidelberg, Germany, Amsterdam, The Netherlands (Feb 21–24, 2007)
18. Jain, A., Lin, H., Sahai, A.: Indistinguishability obfuscation from well-founded assumptions. In: Proceedings of the 53rd Annual ACM SIGACT Symposium on Theory of Computing. pp. 60–73 (2021)
19. Juels, A., Sudan, M.: A fuzzy vault scheme. Designs, Codes and Cryptography 38(2), 237–257 (2006)
20. Juels, A., Wattenberg, M.: A fuzzy commitment scheme. In: Motiwalla, J., Tsudik, G. (eds.) ACM CCS 99: 6th Conference on Computer and Communications Security. pp. 28–36. ACM Press, Singapore (Nov 1–4, 1999)
21. Liang, Y., Kramer, G., Poor, H.V.: Compound wiretap channels. EURASIP Journal on Wireless Communications and Networking 2009, 1–12 (2009)
22. Maurer, U.: Secret key agreement by public discussion from common information. IEEE Transactions on Information Theory 39(3), 733–742 (1993)
23. Nair, C.: Capacity regions of two new classes of two-receiver broadcast channels. IEEE Transactions on Information Theory 56(9), 4207–4214 (2010)
24. Poor, H.V., Schaefer, R.F.: Wireless physical layer security. Proceedings of the National Academy of Sciences 114(1), 19–26 (2017), https://www.pnas.org/content/114/1/19
25. Thomas, M., Joy, A.T.: Elements of information theory. Wiley-Interscience (2006)
26. Wyner, A.D.: The wire-tap channel. Bell system technical journal 54(8), 1355–1387 (1975)
27. Yao, A.C.: Theory and application of trapdoor functions. In: 23rd Annual Symposium on Foundations of Computer Science (SFCS 1982). pp. 80–91. IEEE (1982)