A Negative Result for Fuzzy Extractors

Luke Demarest
University of Connecticut
luke.h.demarest@gmail.com

Benjamin Fuller
University of Connecticut
benjamin.fuller@uconn.edu

Alexander Russell
University of Connecticut
acr@uconn.edu

March 30, 2022

Abstract

We show a negative result for efficient fuzzy extractors for all distributions with fuzzy min entropy even when given a (quasi) polynomial advice string from an unbounded collaborator.

1 Introduction

We show a negative result for efficient fuzzy extractors for all distributions with fuzzy min entropy even when given a (quasi) polynomial advice string from an unbounded collaborator.

We will compare to other works like [1].

2 Preliminaries

In this section we will introduce existing results to help clarify our place in the literature, provide necessary existing definitions to show what we are borrowing and what we build on, and we will provide new definitions in support of our novel results.

2.1 Previous Results

It has been shown that universal fuzzy extractors are impossible in the information theoretic setting.

2.2 Existing Definitions

Fuzzy extractors and more

2.3 New Definitions

Fuzzy extractors with quasipolynomial advice.

3 Negative Results for Secure Sketches

In this section we provide results for secure sketches.

References

[1] Benjamin Fuller, Leonid Reyzin, and Adam Smith. When are fuzzy extractors possible? *IEEE Transactions on Information Theory*, 66(8):5282–5298, 2020.