Linus Sun Capstone Title + Abstract

Course: CSCI1515 - Applied Cryptography

Title: PIR Compression Optimization

Abstract: In cryptography, Private Information Retrieval details a protocol which allows a user to retrieve an item from a server's database without revealing to the server what item the user has retrieved. Rather than the naive and computationally expensive solution where the server sends the entire database to the user, we want to minimize the amount of communication costs between the user and server. Such protocols need to optimize for the balance between user-server and server-user communication and local computation- my capstone project implements a few different communication optimizations by compressing the data being transferred between client-server and server-client.