Private Information Retrieval
Michael Kouremetis and Craig West

Background & Scope

• **Private Information Retrieval (PIR)** – retrieving information from an entity (database) without the entity knowing the information retrieved.
• Allows the user not to be tracked
• Prevents database administrators from associating information with queries
• Implemented with cryptographic protocols

Method

• Research and discover protocols
• Design our system, choose protocols
• Implement proof of concept with
• The chosen protocol and system design
• Analyze system/protocol performance and gain insight into further required advancements for PIR to become more conducive to real world implementations.

Problem Description

• Many PIR protocols and schemes are not applicable to actual implementations
• Computationally difficult and only apply to simple models
• Heavy computation and communication costs

Future Work

• Implement protocol on existing database systems
• Incorporate privacy and anonymity
• Research less computational solutions

Fig. 1.1. The problem of querying databases privately.