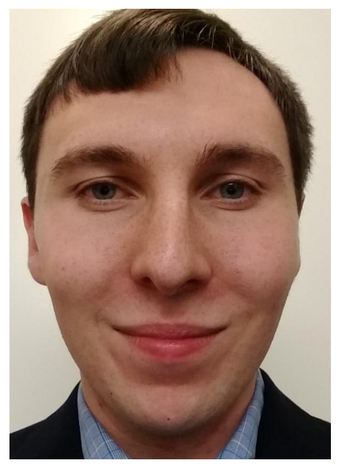
Capacity-achieving Schemes for Private Information Retrieval with Multi-user Collusion

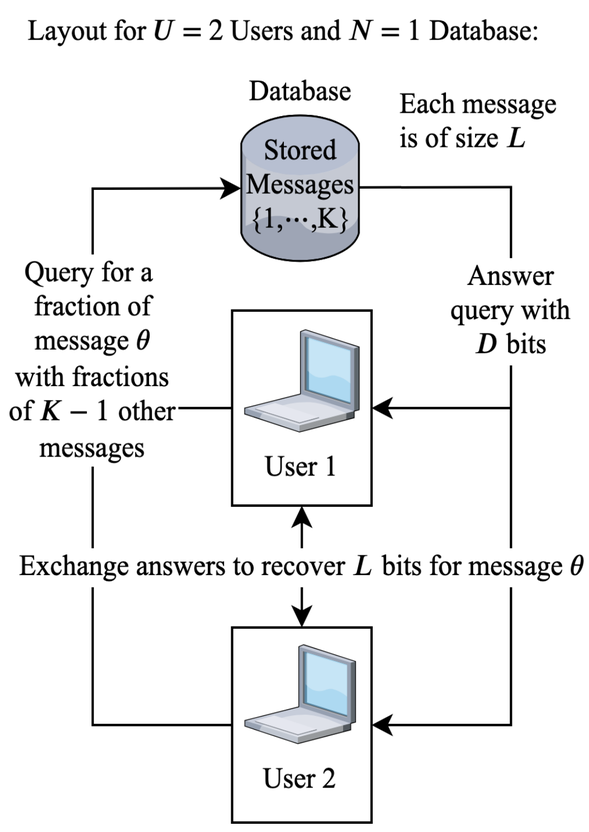
William Barnhart, PI: Zhi Tian, George Mason University

SaTC: CORE: Medium: Collaborative: Privacy Attacks and Defense Mechanisms in Online Social Networks



The objective of Private Information Retrieval (PIR) to obtain message θ from a database while preventing the database from determining what message was sought.

- Novel approach: Introduce multiple users (U) to retrieve a message from a database
- Each database out of N databases has K replicated messages of length L, and may assume all users are colluding
- Rate (R) is the ratio of desired message bits to the total number of downloaded bits (L/D)
  - Maximum achievable rate is capacity (C)
- For a single database $(N = 1)$ and a single user $(U = 1)$, $C = 1/K$
  - Previous work applied PIR to multiple databases to improve efficiency
  - $C = 1/K$ found in settings with all databases colluding against a user



Important considerations for our approach:

- What if all databases assume all users are colluding to retrieve information?
  - Users must change their query schemes
- Can we approach PIR with multiple databases the same way for a single database with user collusion?
  - If all queries from each user are identical in structure, we can utilize the same approach

Our work has the most scientific impact in relevant research topics such as

- Cryptography
- Information Theory
- Privacy in Social Networks
- Network Management
- Information Management

Key findings for our research:

1. When all databases assume users are colluding, all messages must be obtainable by users
2. When all databases assume users are not colluding, only one message needs to be obtainable
3. Multi-user PIR with a database unaware of collusion is identical to PIR with a user accessing multiple non-colluding databases

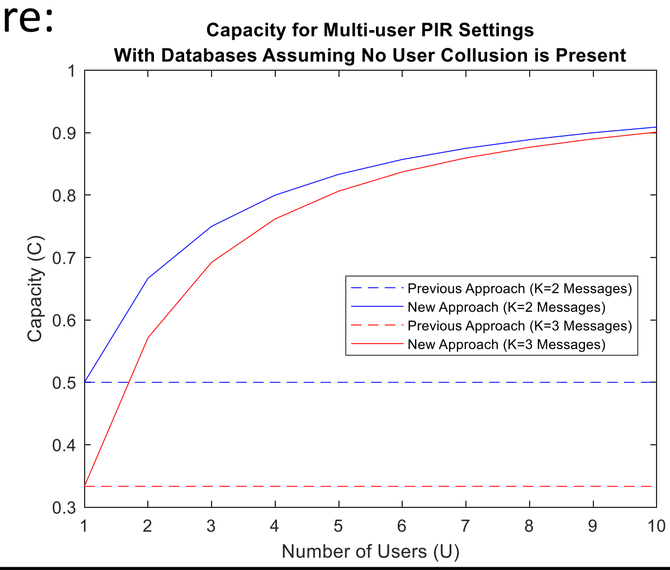
We find that the capacities for multi-user PIR are:

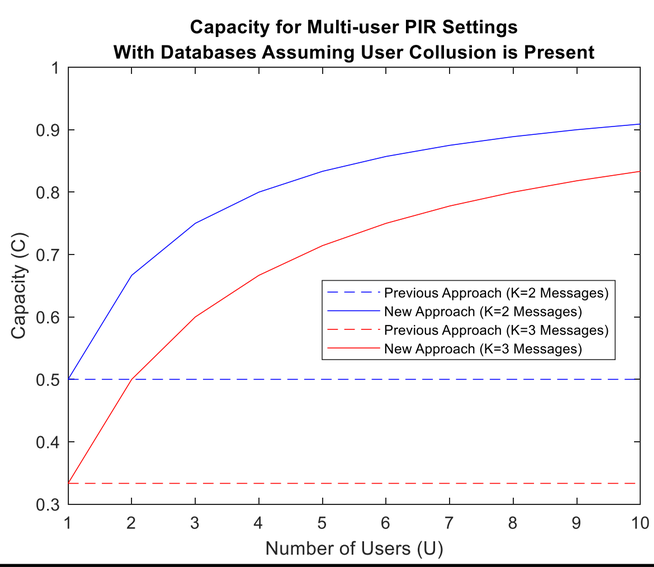
- Databases with no knowledge of user collusion

$$C = \left(1 + \frac{1}{U} + \cdots + \frac{1}{U^{K-1}}\right)^{-1}$$

- For databases with knowledge of user collusion

$$C = \frac{U}{K + U - 1}$$





Scientific broader impact – Useful applications for:

- Medical professionals
- Social workers
- Politicians
- Diplomats
- Individuals in countries with extreme surveillance

Scientific broader impact – Education and outreach:

- GMU VSE Undergraduate Research Celebration, April 16, 2019
  - Presented to VSE undergraduates and faculty
- GMU Honors College Multidisciplinary Research Seminar, Spring 2019
  - Periodically presented to undergraduates from diverse academic backgrounds

Scientific broader impact – Quantification:

- Retrieval rate increases by at least 33% from the addition of another user to a setting with one user
- C is independent of N databases if all databases are identical when there are $U > 1$ users