# Private Information Retrieval

SS2013

Maximilian Schneider

Bob has a database $x \in \{0,1\}^n$

Alice wants to know $x_i$

Bob should not know $i \in [n]$

**PIR does not provide**

anonymity
deniability
encryption

**trivial** approach $O(n)$

**optimal** approach $O(n)$

(for a single database)

## 1995 Chor, Kushilevitz, Goldreich, Sudan

# Private Information Retrieval

multiple replications stored
on non-co-operating servers

for 2 servers best known
protocol until today with
total communication: $12\sqrt[3]{n}$

## 1997 Ambainis

# Upper Bound on the Communication Complexety of Private Information..

builds upon Chor et alii

for k servers: $O\left(\sqrt[2k-1]{n}\right)$

**2002 Beimel, Ishai, Kushilevitz, Raymond**

# Breaking the $O\left(\sqrt[2k-1]{n}\right)$ Barrier for Information-Theoretic Private..

first improvement in 5 years
improves Locally Decodable Codes

for k servers: $n^{O\left(\frac{\log\log k}{k\log k}\right)}$

# Locally Decodable Codes

"A $q$ query LDC encodes a $n$-bit message $x$ as a $N$-bit codeword $C(x)$ such that any bit $x_i$ of the message can be probabilistically recovered by querying only $q$ bits of the codeword $C(x)$, even if some constant fraction of the codeword has been corrupted."

Source: http://en.wikipedia.org/wiki/Locally_decodable_code

## 2006 Yekhanin

# New Locally Decodable Codes and Private Information Retrieval Schemes

improves Locally Decodable Codes
3 Server PIR

for largest known MP: $O\left(\sqrt[32582658]{n}\right)$

assuming infinite MPs: $\sqrt[O(\log\log n)]{n}$

1997 Chor, Gilboa

# Computationally Private Information Retrieval

Main assumption:
Server is computationally bounded

for $\varepsilon \in (0;1) : O(n^{\varepsilon})$

## 1997 Kushilevitz, Ostrovsky

# Replication is not needed: Single Database, Computationally-Private..

Single Server CPIR

Based on Quadratic Residues

# CPIR as a cryptographic primitive

1:n Oblivious Transfer aka.
"Symmetric Private Information Retrieval"

Collision Resistant Hashing

## 2005 Lipmaa

# An Oblivious Transfer Protocol with log-squared Communication

Based on Damgård-Jurik

$$O\left(\log^2 n\right)$$