- ≈ 100 статей, 5 диссертаций, 1 книга, ≈2 продукта начиная с 1996г
- активно публикуется по настоящее время
- развивается несколькими научными сообществами одновременно
- уже является частью учебных программ по базам данных, криптографии, компьютерной безопасности, экономике ведущих университетов мира

Обработка Закрытых Запросов

Дмитрий Асонов

Московская секция ACM SIGMOD, МГУ
26.04.07.
ИСП РАН
20.03.07

Содержание

	слайдов
1. Одна БД	[10]
– Постановка задачи	2
– Приложения	1
– Решения	7
– Открытые проблемы	1
2. Две БД	[5]

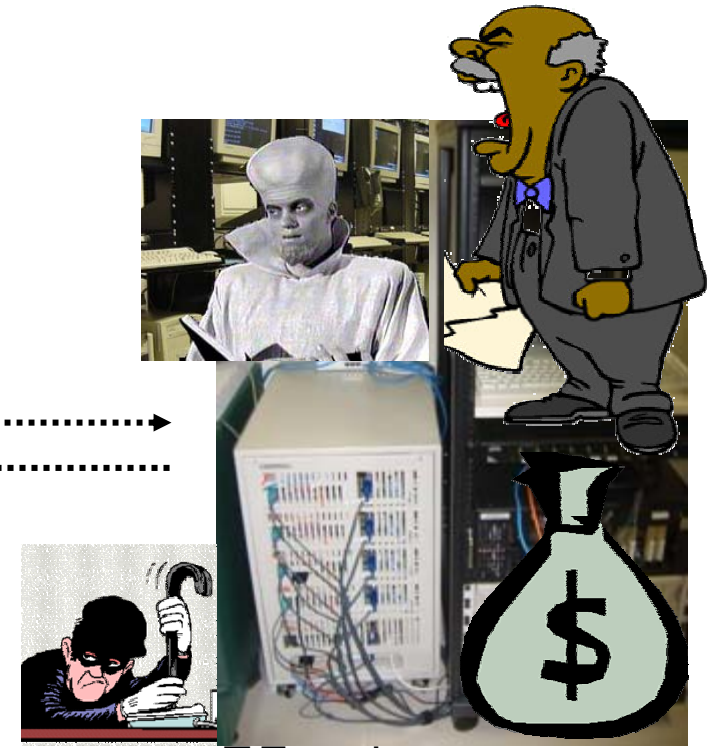
Неформальная постановка задачи

- Хранение БД локально неэкономично
- Шифрование не помогает

клиент

запрос

результат

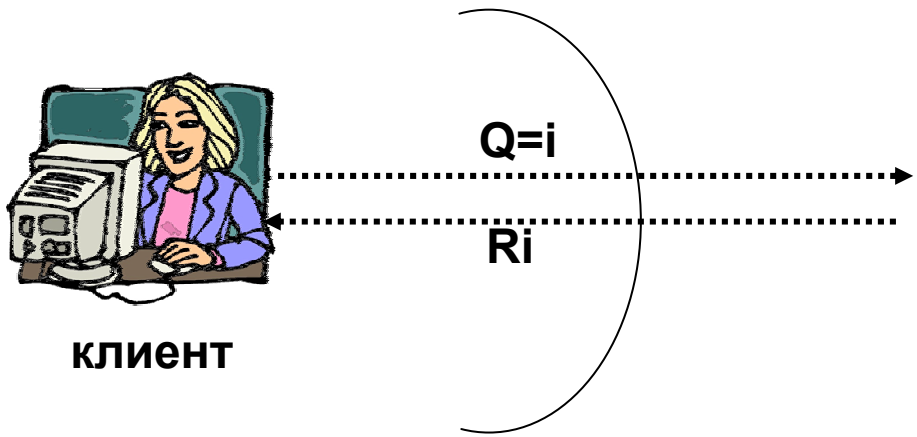


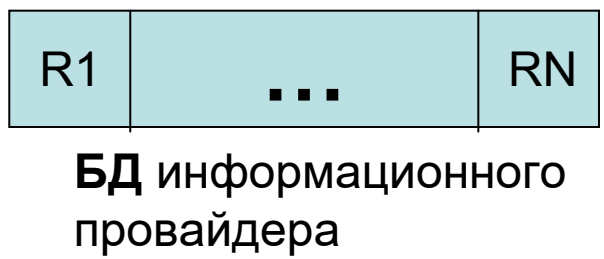
БД информационного провайдера

O1: Никто кроме клиента не должен узнать о содержании запроса и результата.

Формальная постановка задачи

- DB[1,…,N]
- Q=i, 1≤i≤N
- O1: Никто кроме пользователя, даже СУБД, не должна узнать ничего о i.





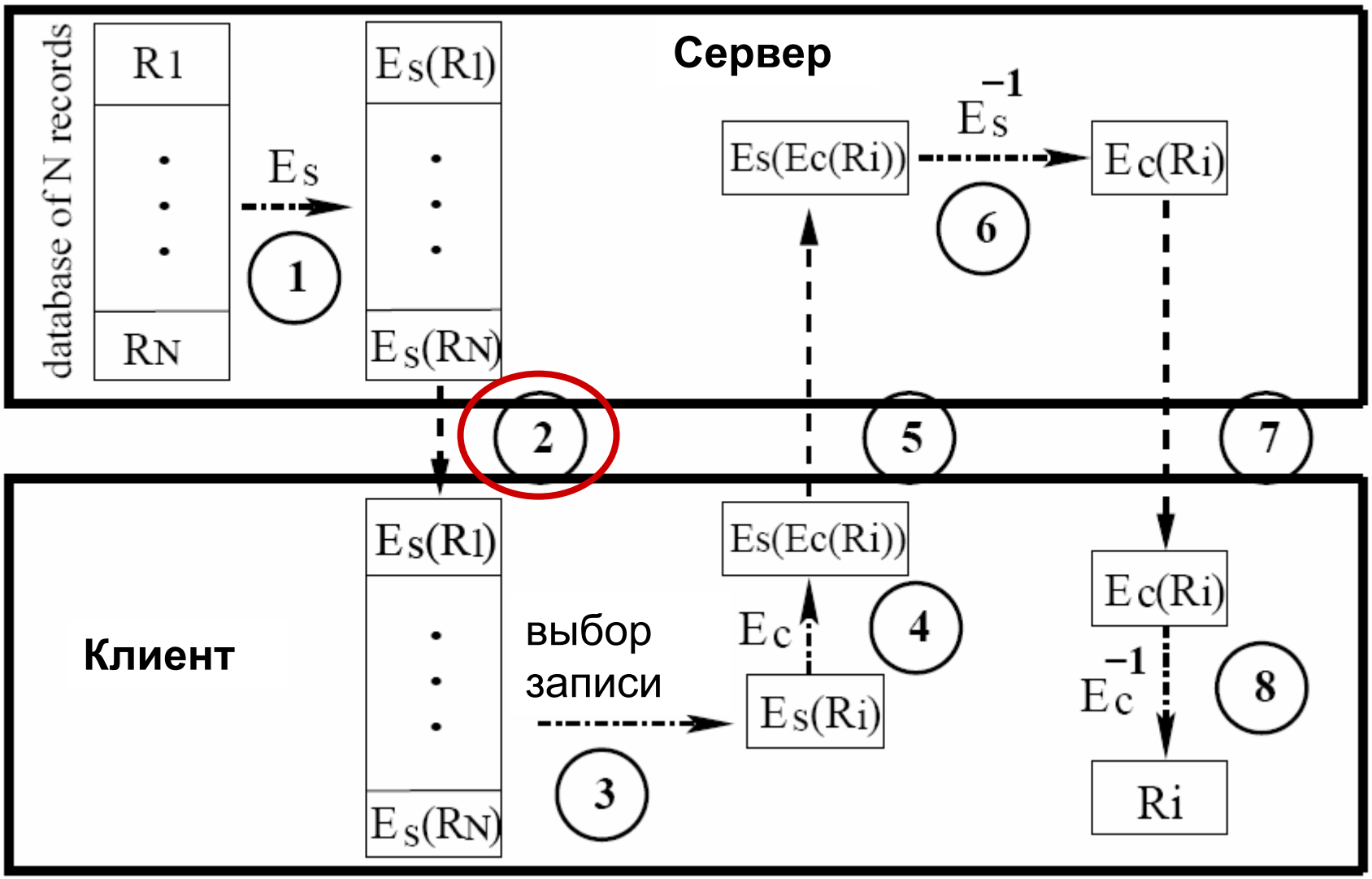
Области применения

- Магазины цифровых товаров
  - эл. книги, музыка, видео, патенты
- Медицина
  - фармацевтические БД
- Биржевые торги
- Оборонные
- ….

Решения

- Теоретические ОЗЗ [CGKS96,…]
  - несколько копий БД, сервера не объединяются
  - Вариации: *t*, *M*
- Криптографические ОЗЗ [CG97,…]
  - коммутативные схемы
- ОЗЗ на защищенном ВУ [SS00,…]
  - например, IBM 4758, IBM 4764
- T1: Минимальное время ответа O(N)

Криптографическая ОЗЗ [BDF00, SJ00]

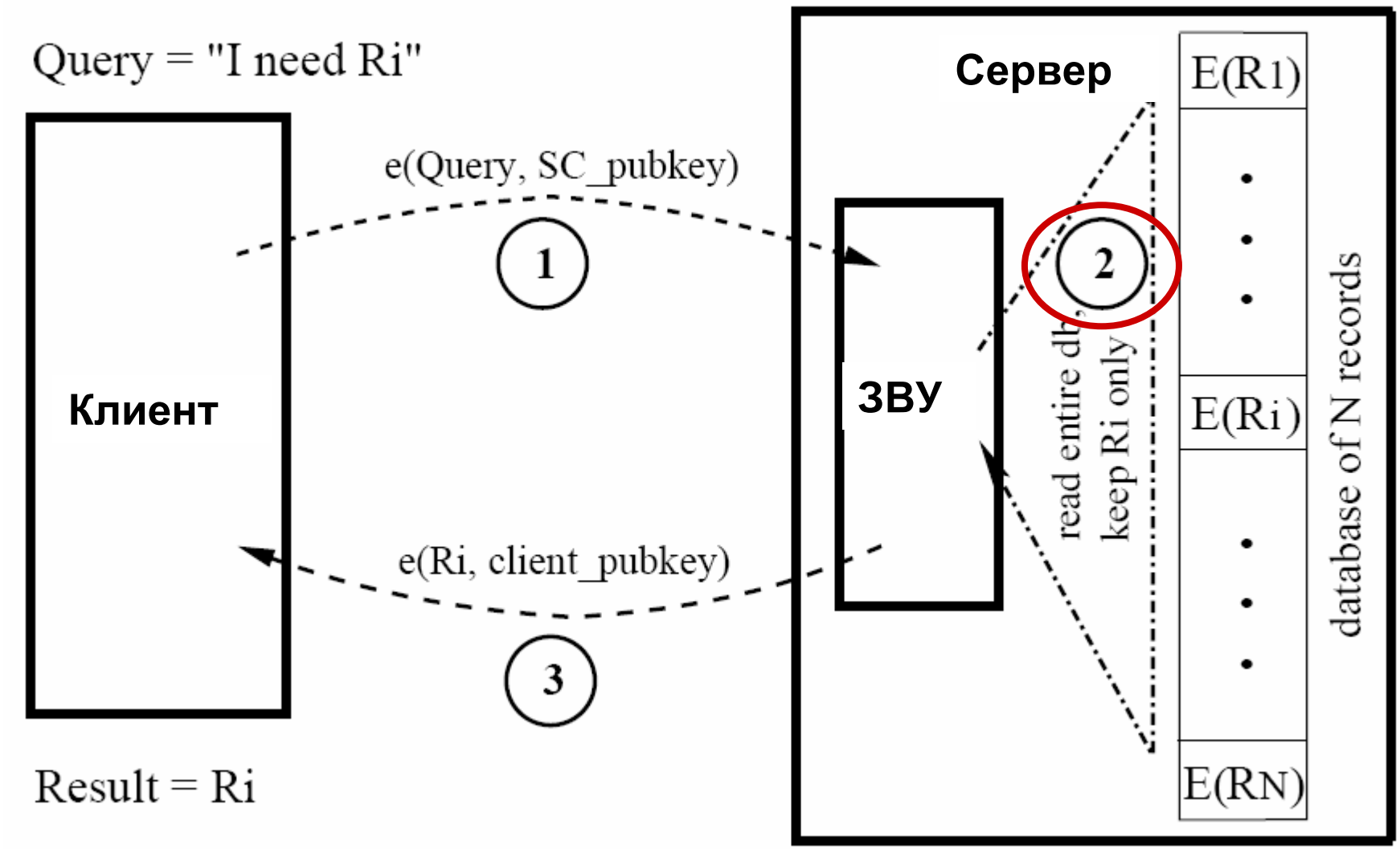


Защищенное ВУ

- PCI интерфейс
- Активная защита от физических и логических атак
- FIPS 140-1-4
- Intel 486, 4MB RAM, 4MB PROM, CP/Q++
- От 1000$
- Стандартное применение - банки

IBM 4758

ОЗЗ на основе защищенного ВУ [SS00, SS01]

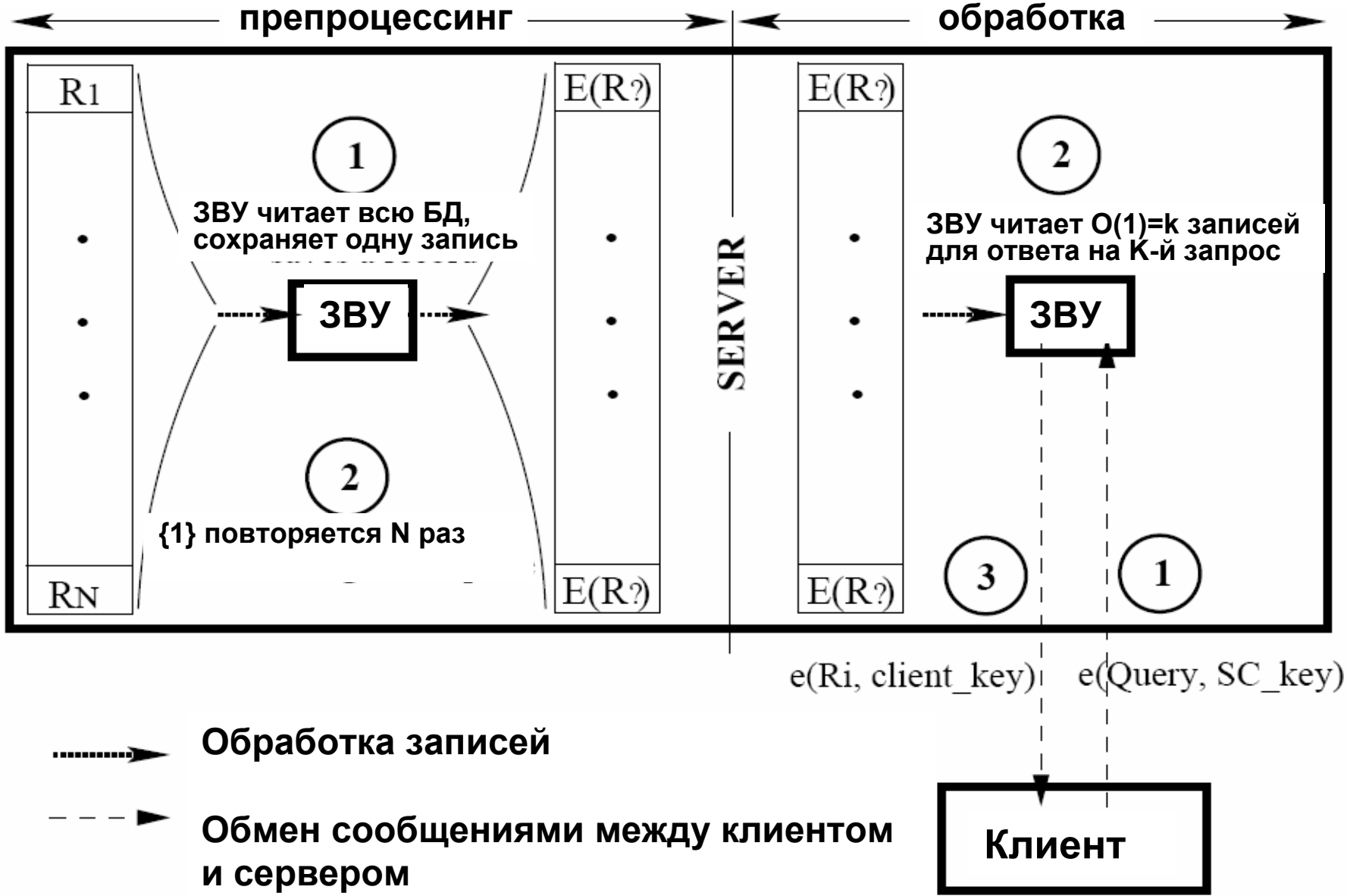


Почти оптимальная ОЗЗ, анализ

[AF02]

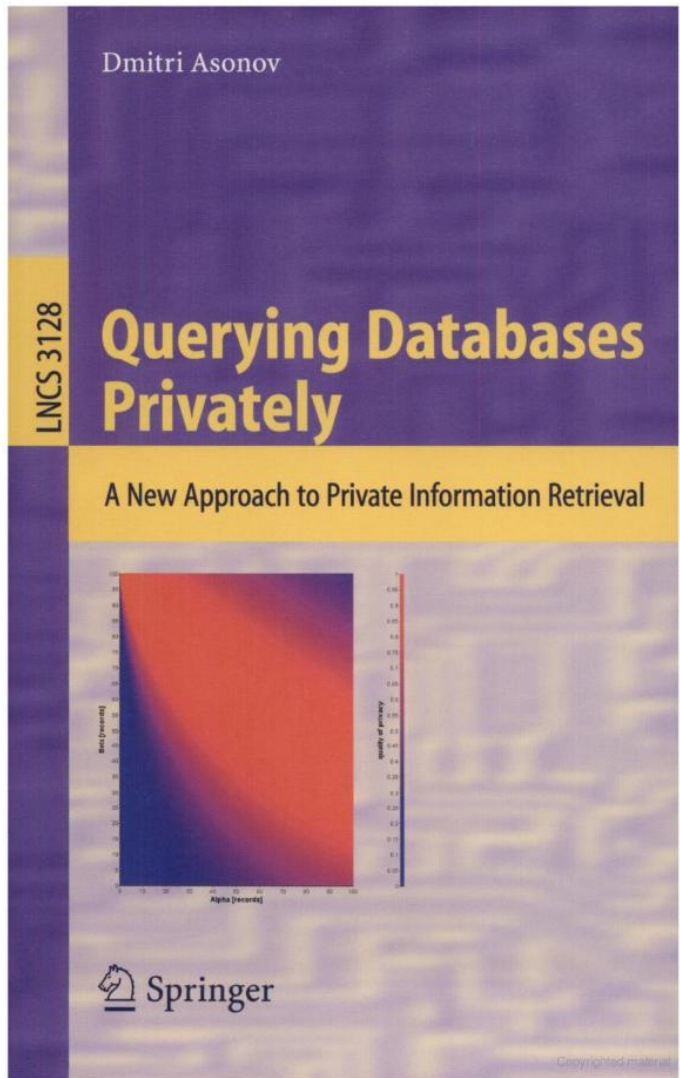
решение / параметры	[BDF00, SJ00]	[SS00, SS01]	?
время ответа	O(1)	O(N)	O(1)
передача данных	O(N)	O(1)	O(1)

Почти оптимальная ОЗЗ



Расширения

- Перестановка O(N) [AF03a]
- Частичная закрытость, степень закрытости [AF03b]
- Защита интеллектуальной собственности [A04]
- Частичные перестановки [B05]
- LDAP X.509 реализация [IS04]
- …



Две БД, постановка задачи

клиент

Q(БД1, БД2)

результат

БД1

БД2

O2: Пользователь не должен узнать ничего о базах данных за исключением результата;
Никто кроме пользователя не должен узнать результат.

Две БД, применения

- Медицина
  - Генетика, фармакология
- Контртеррористические
- Банковские
- Персонифицированная реклама
- Сайты знакомств
- Маркетинговые
- …

Федеральная служба безопасности на транспорте и Авиакомпании

СТОП-лист (>1000000)

Мальчишь-плохишь

Серый волк

….

Пассажиры (100000/день)

Иван Петров

Серый волк

Петр Иванов

…..

Запрос = СТОП-Лист ∩ Пассажиры,

Результат = Серый Волк

Генетическая медицина

- **“When good drugs go bad**
  How can we best reduce the risk of severe adverse reactions to marketed drugs? An international group of scientists argues that a global research network is needed to identify genetically at-risk populations.”
  Nature Volume 446 Number 7139 pp949-1116,
  25 Апреля 2007

Две БД, решения

- Криптографические ОЗЗ
  - ∩, |∩|, join, |join| (операция эквивалентности)
  - SIGMOD2003, SIGMOD2004, Agrawal et. al.
  - First **Computerworld** Horizon Award (2005), **Industry Week's** Notable Innovation of the Year (2005)
- ОЗЗ на защищенном ВУ
  - Любые операции сравнения
  - ICDE2006

Заключение

- ОЗЗ к одной, нескольким БД
- Криптографические примитивы, защищенные ВУ
- Комбинирование КП и ЗВУ?
- Закрытые запросы к ОББД, например Google?
- Нужна ли ОЗЗ??