cryptis

Разработка прозрачного прототипа криптографической NoSQL базы данных

Вахрушев Павел Андреевич
webartifex@gmail.com
http://cryptis.ru

cryptis

Цель проекта

Разработать прозрачный для прикладных программ криптографический посредник облачной нереляционной базы данных

cryptis

Проблемная область

Хранение **ценной** информации:

- персональные данные
- коммерческая документация
- другие конфиденциальные данные

Неэффективно из-за:

- оборудование
- персонал
- помещения
- риски безопасности

cryptis

Риски

- **0,98 млрд** рублей - выявленные потери индустрии за 2013 год [1]
- **45 млн** - средний ущерб от инцидента [2]
- **78%** крупных организаций атакованы в 2012 году [2]
- В **40%** используются целевые хакерские атаки с использованием уязвимостей БД [3]

1. Symantec. Отчет «2013 Cost of Data Breach Study: Global»
2. InfoSecurity. Отчет «2012 Information Security Breaches Survey»
3. Application Security Inc. Отчет «Безопасность баз данных»

cryptis

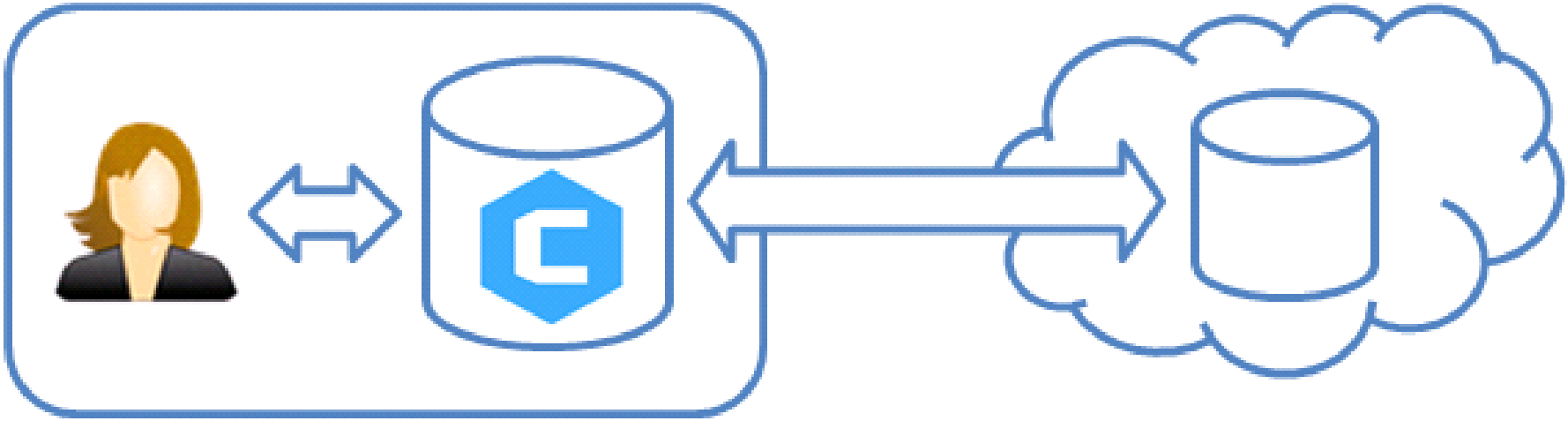
Актуальность

- **0,9 млн** рублей - стоимость аппаратного модуля только для шифрования [1]
- **6,95 млрд** – объем рынка облачных услуг РФ в 2012 году [2]
- **26,6 млрд** – рынок облачных услуг в мире [3]
- **45%** - средняя экономия средств при внедрении облачных технологий [4]

1. КриптоПРО HSM
2. http://digit.ru/business/20130924/405894294.html
3. http://www.business365.ru/node/102
4. EMC Consulting, http://russia.emc.com/collateral/emc-perspective/h6870-consulting-cloud-ep.pdf

cryptis

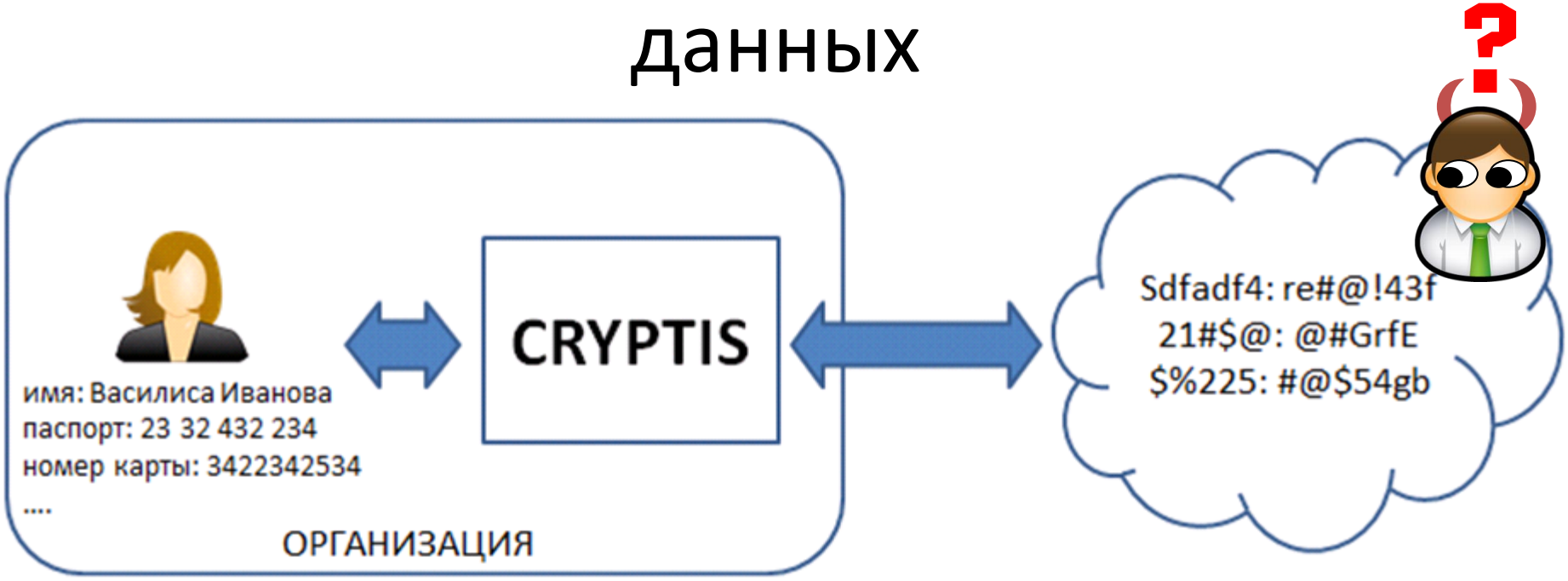
Хранение в облаке зашифрованных данных



- Прозрачный посредник, эмулирует базу данных
- Занимается шифрованием, кешированием, пересылкой данных и эмуляцией запросов

cryptis

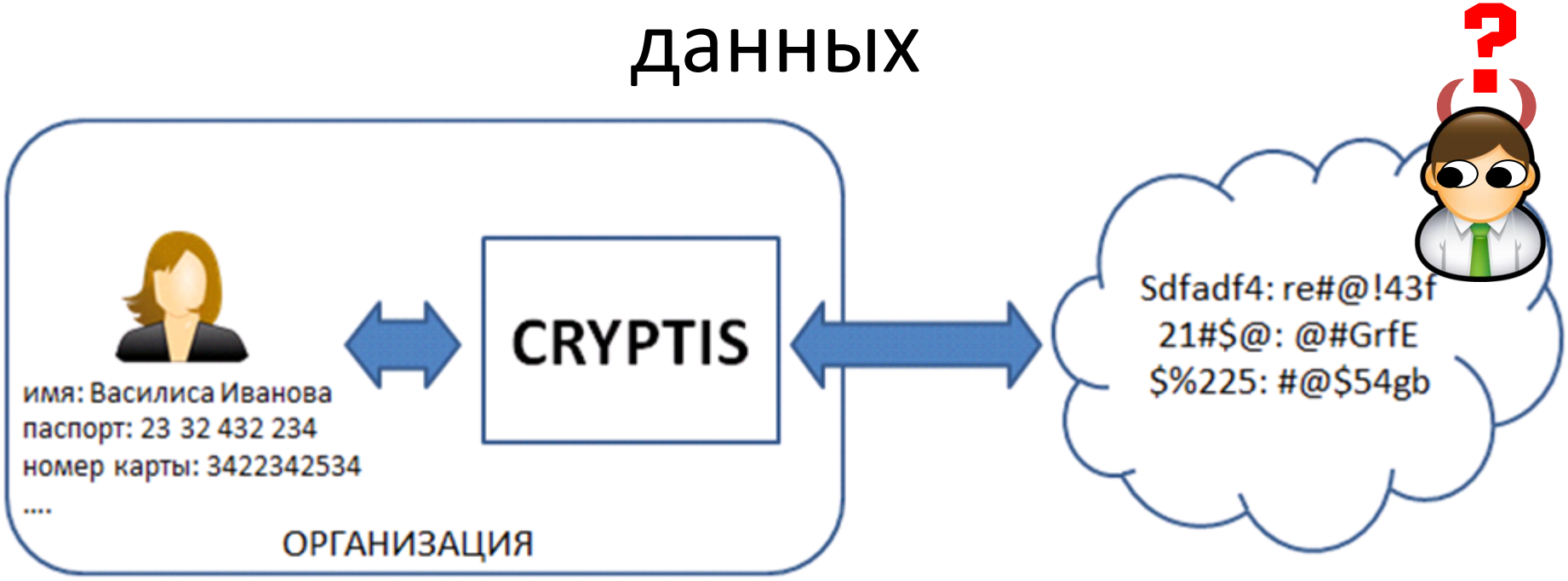
Хранение в облаке зашифрованных данных



- Данные в облаке не расшифровываются
- Нереляционность повышает производительность
- Выполнение операций в облаке без расшифровки

cryptis

Хранение в облаке зашифрованных данных



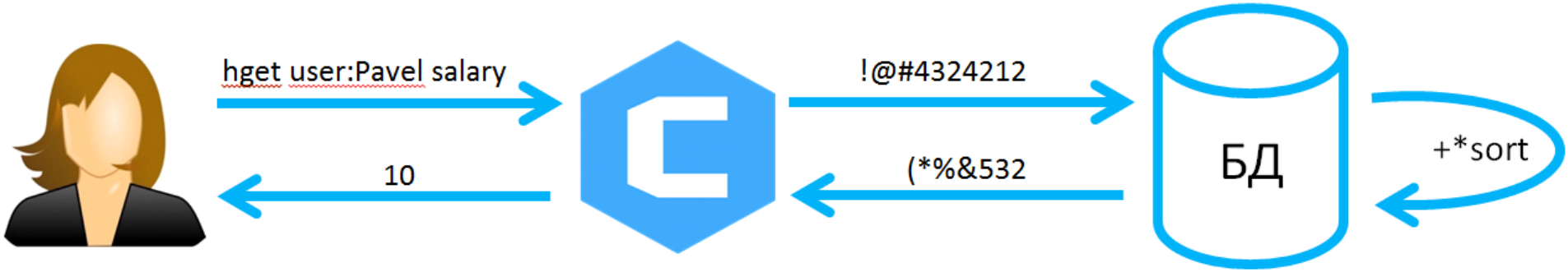
+ контроль конфиденциальности и целостности

+ уменьшение затрат

– снижение производительности (в среднем 11%)

cryptis

Принцип работы



cryptis

Специальные шифрования

- Гомоморфное шифрование
  - выполнять математические операции с зашифрованным текстом и получать зашифрованный результат
- Шифрование, сохраняющее порядок
  - сохранить порядок чисел после шифрования
- Блочное шифрование
  - надежное хранение

cryptis

Пример операции +

Encrypt(2) = @xf4

Encrypt(3) = *sdk

Encrypt(5) = &#kc

2 + 3 = 5

@xf4 + *sdk = &#kc

cryptis

Сохраняющее порядок

- Сохранить порядок после шифрования

  c1=Encrypt(p1)
  c2=Encrypt(p2)
  If (p1 < p2) then (c1 < c2)

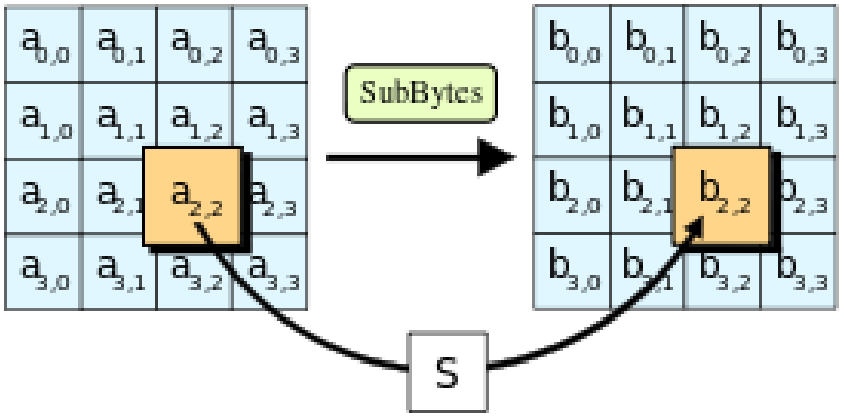
- Простейшее – на массиве

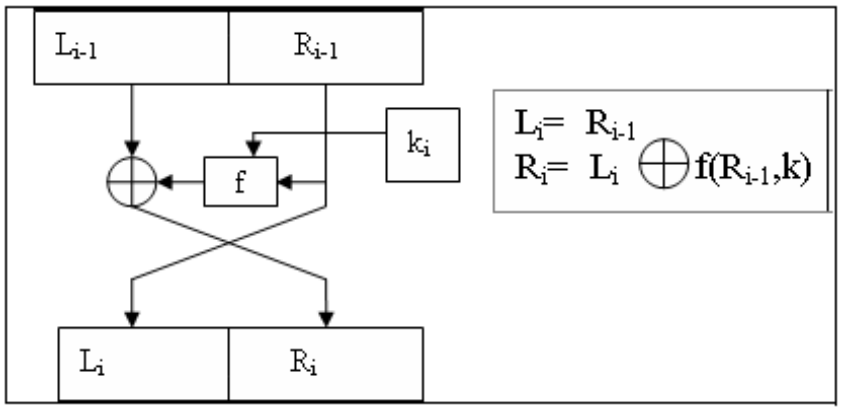
  INIT:
  T = array [n] (random())
  sort T
  ENC: c = T[p]
  DEC: p = binarySearch(c, T)

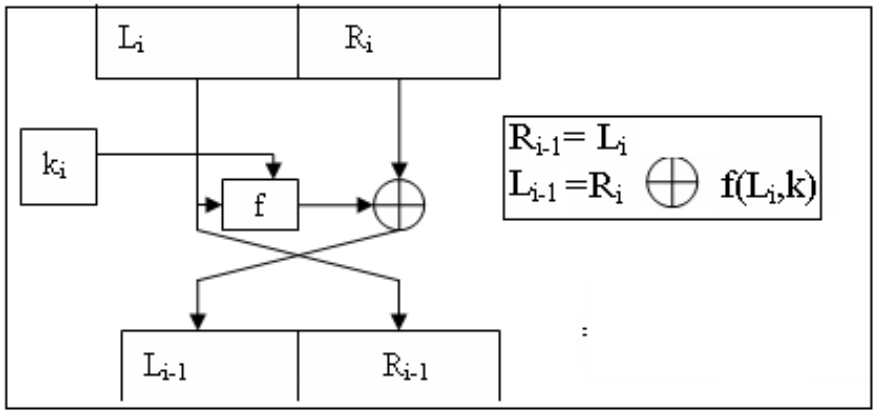
cryptis

Блочное шифрование

- AES
- DES
- ГОСТ 28147-89





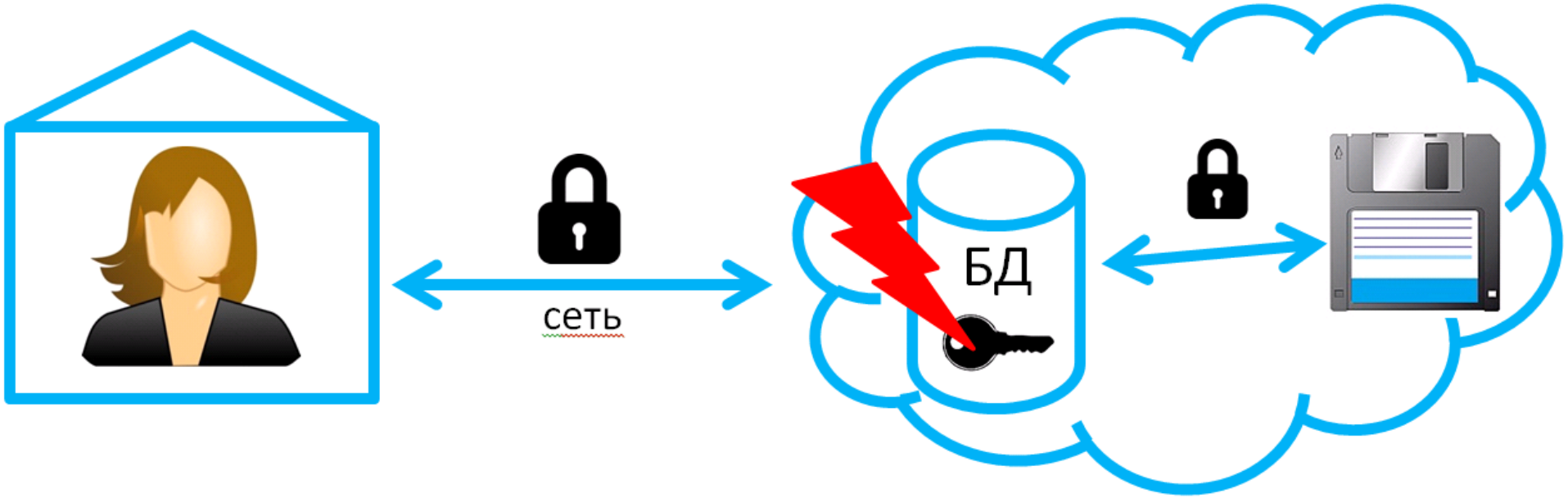


cryptis

Ограничение языка запросов

cryptis

Недостатки существующих решений



cryptis

Научная новизна

- Нереляционная структура криптографической базы данных
- Использование специальных видов шифрований
- Хранение ключей шифрования внутри организации
- Полное шифрование всех данных, без расшифровки в облаке
- Эмуляция выполнения запросов

cryptis

Существующие решения

Имя	Скорость	Прозрачность для ПО	Ключ внутри организации	Полное шифрование	Трафик	Стоимость
Intel Hadoop Security	+	+	–	–	+	±
Cloudera security	+	+	–	–	+	±
File encryption	–	+	+	+	–	±
Transparent Data Encryption (Oracle)	+	+	–	±	+	–
CryptDB	±	–	+	+	+	+
cryptis	+	+	+	+	+	+

cryptis

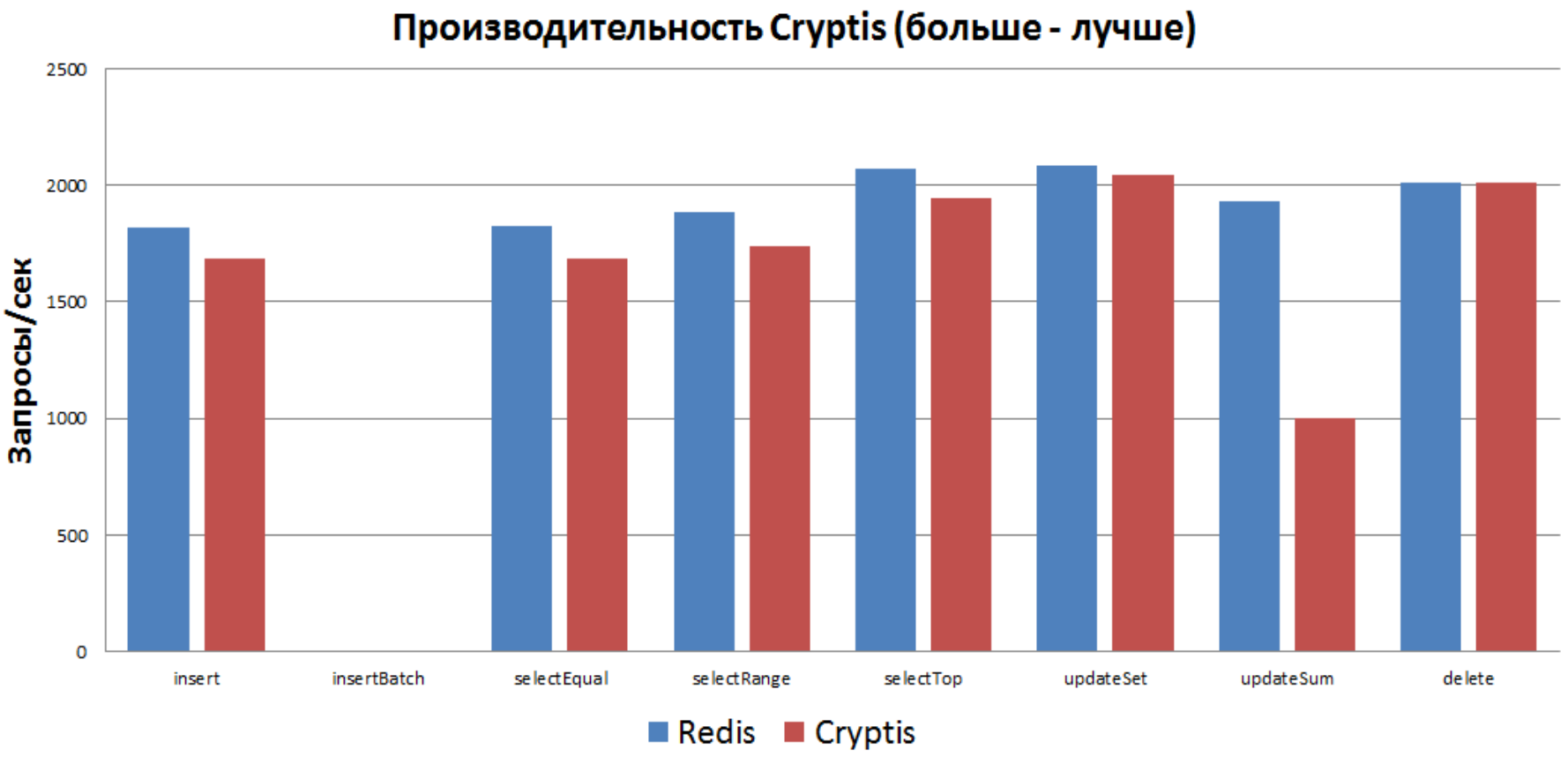
Реализация: сегодня

- Реализован прототип на базе СУБД Redis для проверки идеи
- Поддерживается часть операций: вставки, выборки, сортировки
- Прототип быстрее SQL конкурента на 85%
- Для доведения прототипа до продукта требуется:
  - Реализация прозрачности
  - Реализация еще одного вида шифрования
  - Интеграция с облаком

cryptis

Реализация: сегодня

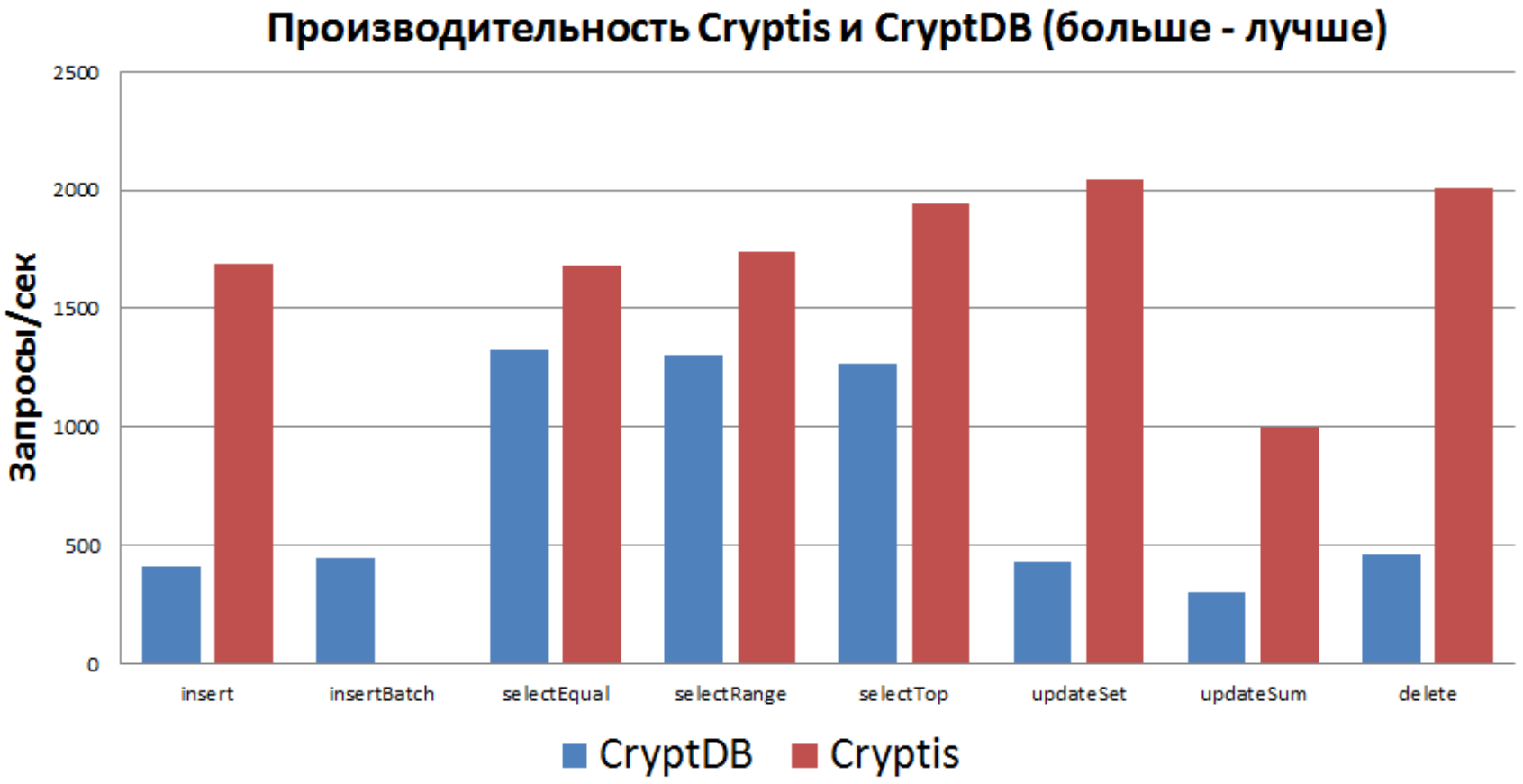
В среднем падение производительности составляет 11%



cryptis

Аналоги: CryptDB

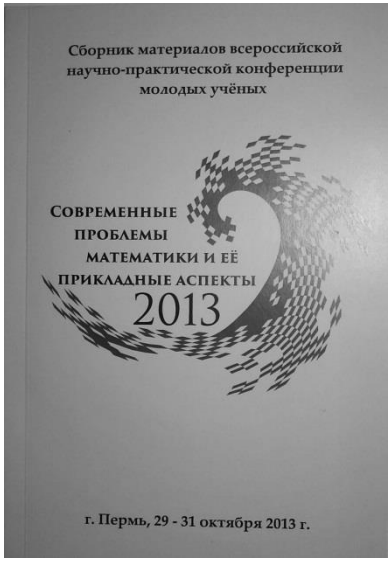
В среднем Cryptis быстрее SQL конкурента на 85%

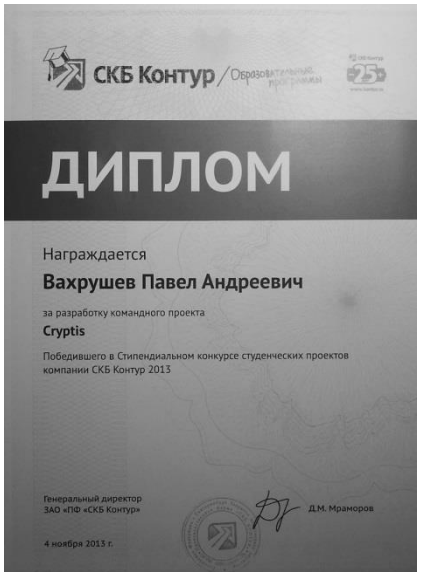


cryptis

Результаты проекта

- Участник ВолгаИТ-2013
- Участник конкурса лучших стартапов рунета Web-ready 2013 (Сколково)
- Публикация в сборнике конференции «Современные проблемы математики и ее прикладные аспекты - 2013» «Криптографическая NoSQL система управления базами данных»
- Победитель конкурса компании СКБ.Контур





cryptis

План реализации проекта

1 год

План	Результат
Выбор СУБД для реализации	Обоснован выбор материнской СУБД
Реализовать прозрачный прокси запросов	Функционирует прозрачный прокси
Встроить в систему шифрование, сохраняющее порядок	Реализованы операции с сортированным множеством
Встроить в систему набор гомоморфных шифрований	В системе работают математические операции
Реализовать механизм выбора шифрований для данных	Механизм выбора шифрований функционирует, написана документация
Обеспечить возможность переноса криптографии на другие СУБД	Выделена криптографическая библиотека

2 год

Создан механизм эмуляции запросов	Проект обеспечивает прозрачность для ПО
Интеграция с облаком Amazon	Проект готов к внедрению

cryptis

Перспективы коммерциализации

- Продукт – облачный сервис с доступом через программу-клиент
- Модель продаж – подписка на услугу
- Основные покупатели:
  - интеграторы в области компьютерной безопасности
  - компании, хранящие большие объемы конфиденциальных данных
- Существует договоренность с Министерством культуры, молодежной политики и массовых коммуникаций об апробации технологии

cryptis

Команда проекта

1. Вахрушев Павел Андреевич - **основатель проекта, разработчик**, опыт работы в высоконагруженной игре tankionline.com, студент специальности компьютерная безопасность

2. Швеин Михаил – разработчик, опыт работы в MACROSCOP, студент специальности компьютерная безопасность
3. Бойцов Иван – экономист-маркетолог
4. Фирсов Антон – научный консультант, старший преподаватель ПГНИУ

cryptis

Спасибо за внимание

Вахрушев Павел Андреевич
webartifex@gmail.com
http://cryptis.ru