Облачная криптографическая NoSQL СУБД

Научный руководитель:
к.т.н., доцент
Черников Арсений Викторович

Выполнил:
студент 6 курса КМБ-1,2-2009
Вахрушев Павел Андреевич

Проблемная область

Хранение **ценной** информации:

- персональные данные
- коммерческая документация
- другие конфиденциальные данные

Затратно из-за расходов на:

- оборудование
- персонал
- помещения
- риски безопасности

Риски хранения информации

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

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

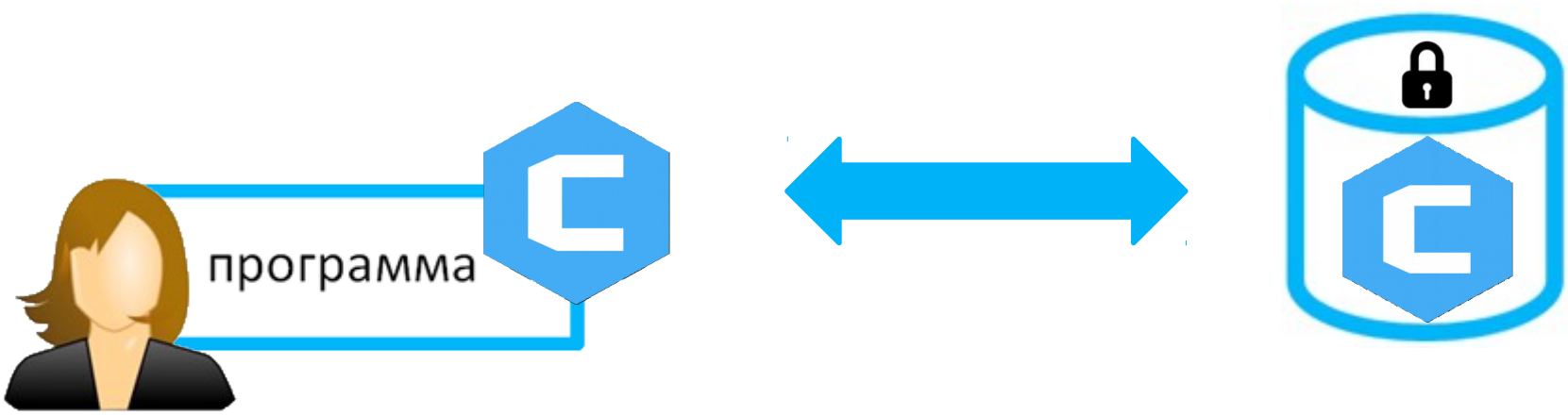
Актуальность

- **0,9 млн ₽** – стоимость аппаратного модуля только для шифрования [1]
- **6,95 млрд ₽** – объем рынка облачных услуг РФ в 2013 году [2]
- **26,6 млрд ₽** – рынок облачных услуг в мире [3]
- **45%** – средняя экономия средств при внедрении облачных технологий [4]

1. КриптоПРО HSM
2. РИА Новости. Исследование «Рынок облачных услуг в РФ»
3. Unicloud. Исследование «Big Data как технология обработки данных»
4. EMC Consulting. Отчет «Преимущества облака для бизнеса»

Цель дипломной работы

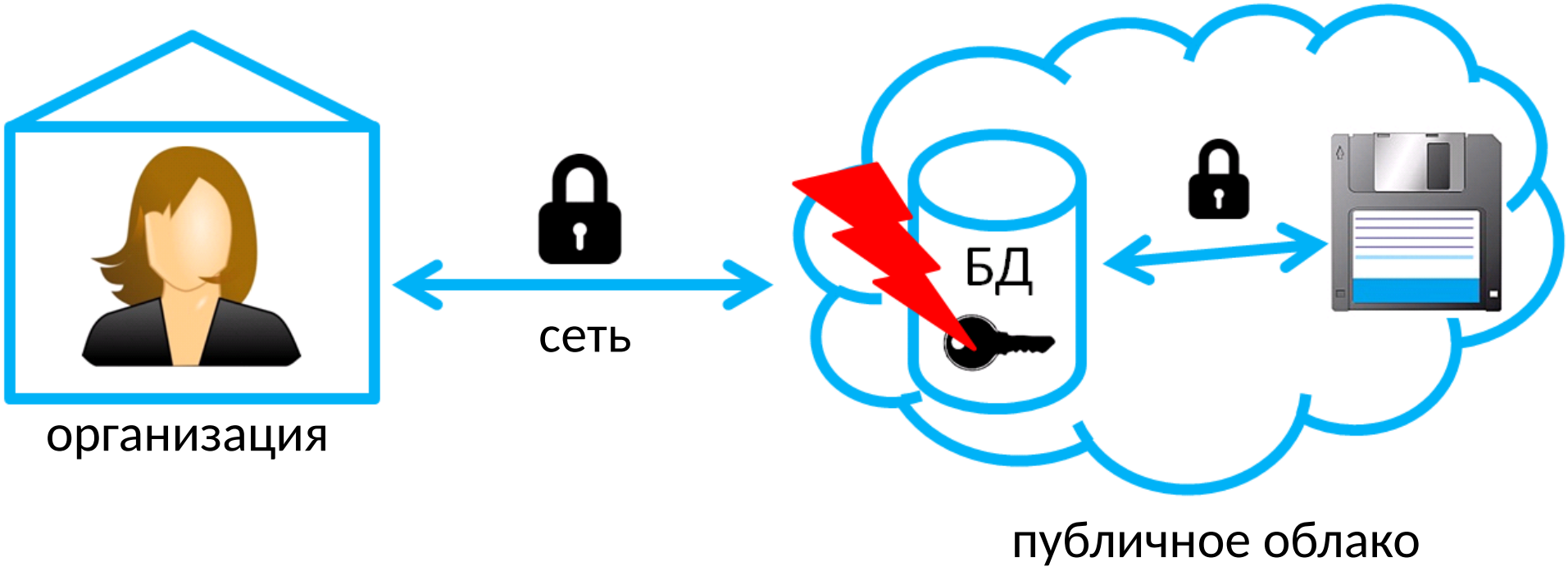
Разработка прототипа криптографически защищенной NoSQL базы данных, способного работать в облаке



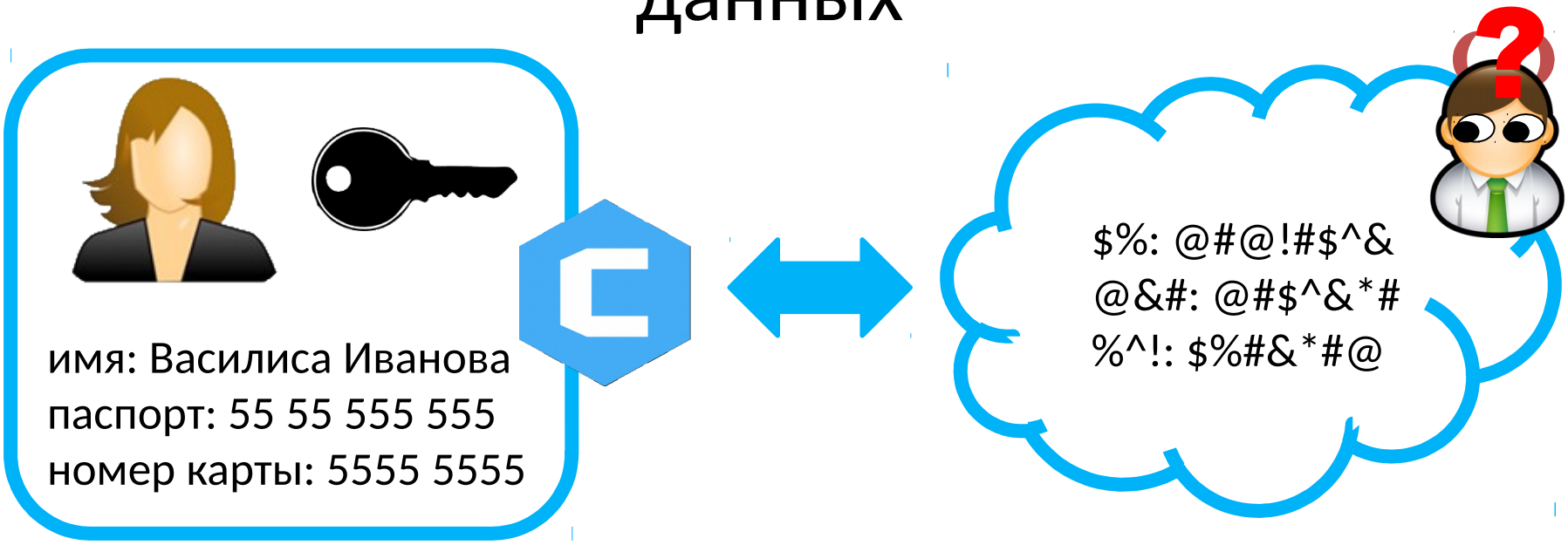
Задачи дипломной работы

1) Изучение существующих технологий и обзор готовых решений
2) Изучение особенностей работы NoSQL БД и их размещения в облачных сервисах
3) Выбор и обоснование архитектуры и родительской NoSQL базы данных для реализации
4) Выбор и обоснование криптографических примитивов для шифрования
5) Выбор и обоснование методов и средств реализации прототипа
6) Реализация прототипа системы управления базами данных
7) Тестирование и испытание системы, замер производительности и безопасности

Уязвимость традиционных решений

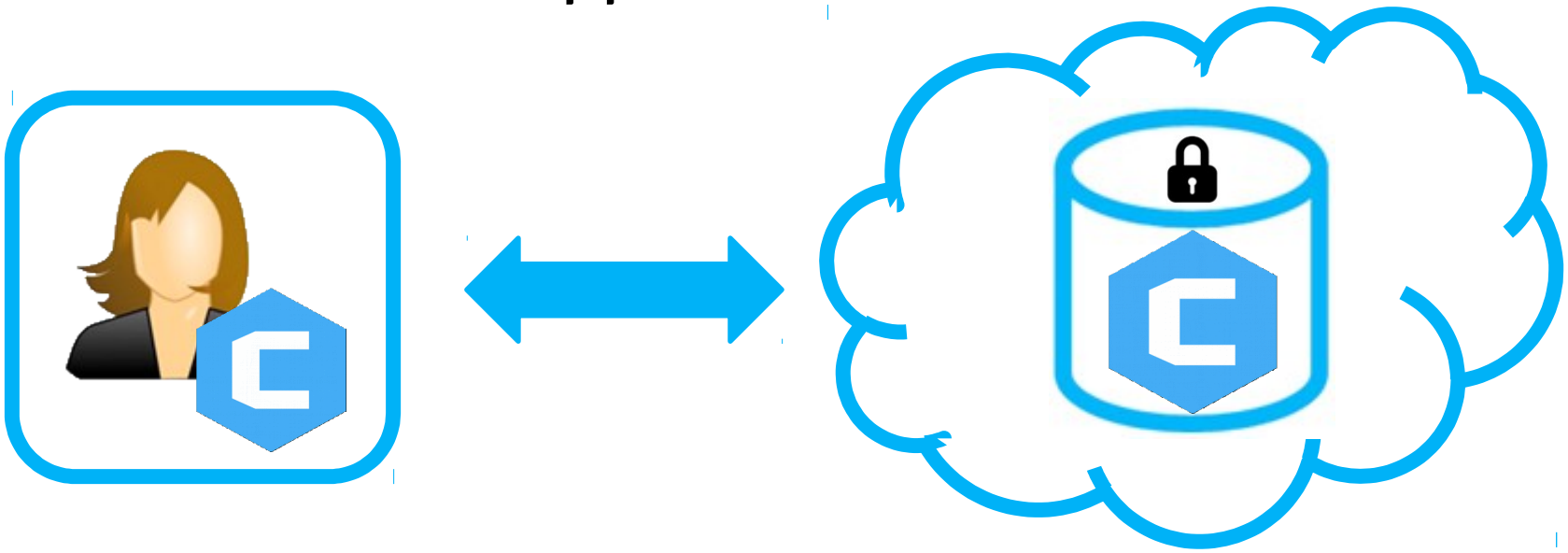


Хранение в облаке зашифрованных данных



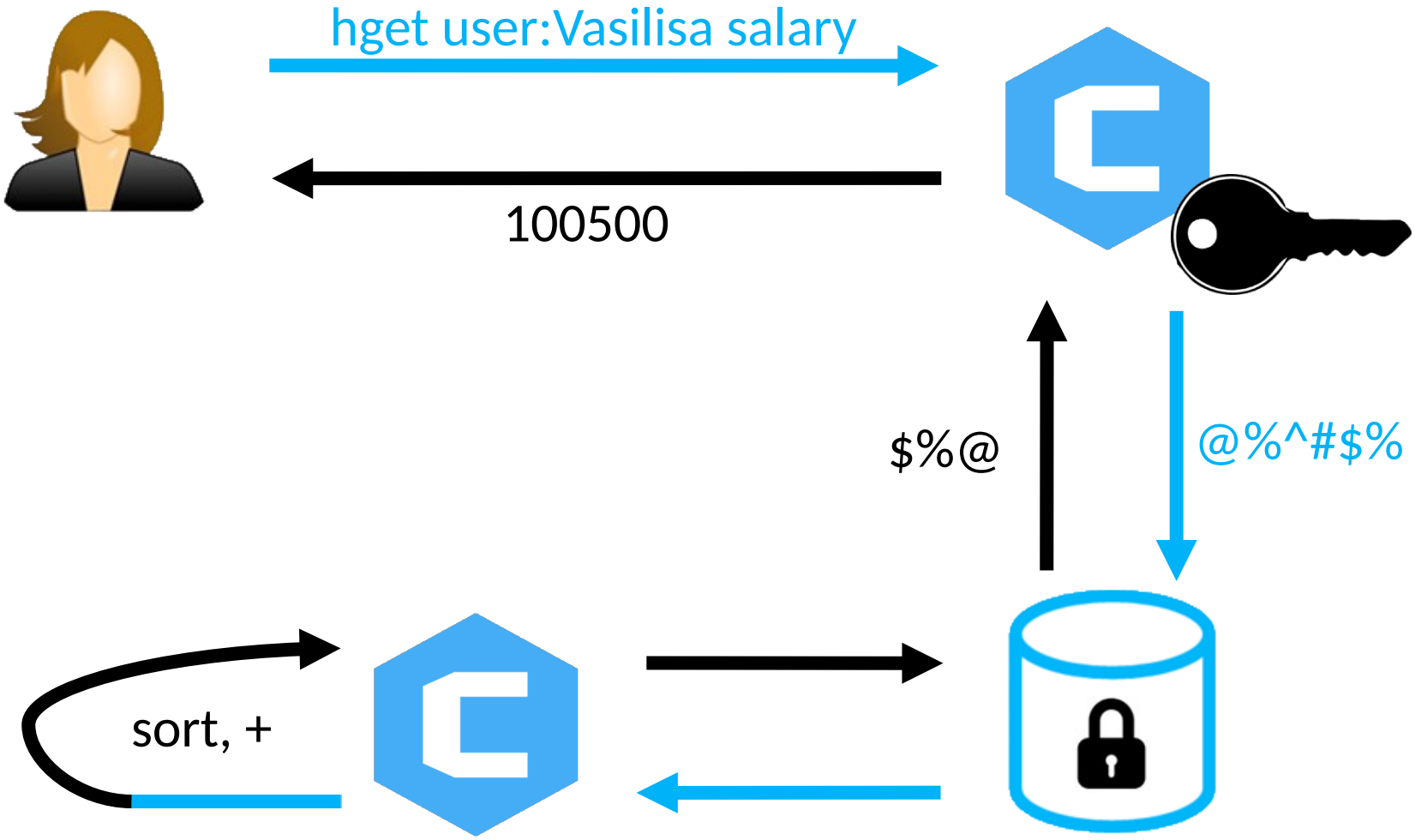
- Данные в облаке не расшифровываются
- Нереляционность повышает производительность
- Выполнение операций в облаке без расшифровки

Хранение в облаке зашифрованных данных



- Прозрачный для исходных кодов клиент СУБД
  - Занимается шифрованием, кешированием, пересылкой данных и эмуляцией запросов
- Модифицированная для поддержки шифрований СУБД

Принцип работы

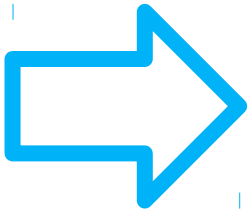


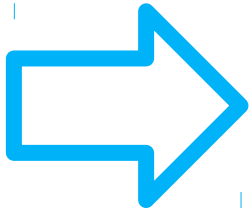
Специальные шифрования

1) Гомоморфное шифрование - **Пейе**
   - выполнять математические операции с зашифрованным текстом и получать зашифрованный результат
2) Сохраняющее порядок шифрование - **OPES**
   - сохранить порядок чисел после шифрования
3) Блочное шифрование - **AES**
   - надежное хранение

Гомоморфизм криптосистемы Пейе

$$E(m_1) * E(m_2) \bmod n^2 \equiv E(m_1 + m_2 \bmod n)$$





INCR X 5

MULT @$ 98

@$←@$*98

X ← X + 5

Сохраняющее порядок шифрование

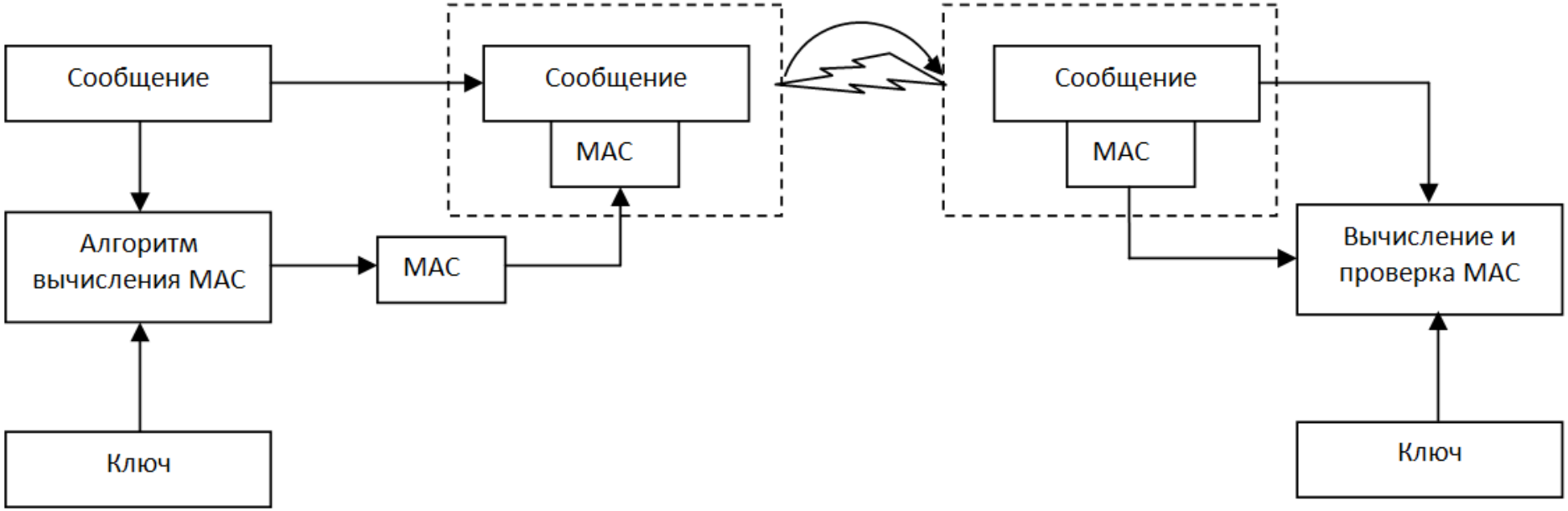
- Сохранить порядок после шифрования

```
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)
```

Аутентификация EMV MAC



Особенности работы

- 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
- Использование смарт-карт EMV для аутентификации

Заключение

- Все поставленные задачи решены
- В среднем на 85% производительнее существующих решений
- Проверена аутентификация EMV

http://cryptis.ru

Спасибо за внимание

Дипломная работа

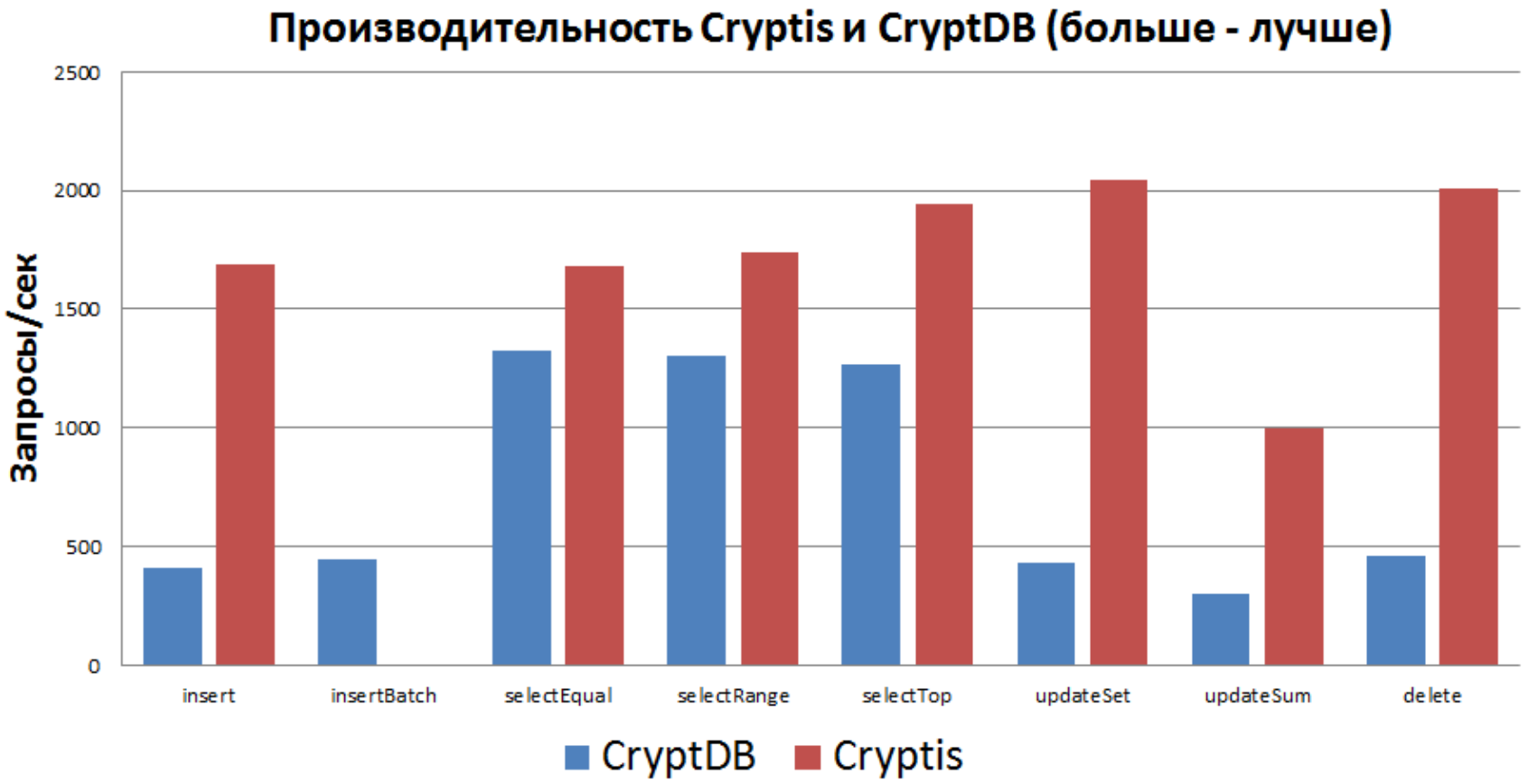
1) Уход от прокси-архитектуры и переход к модификации непосредственно сервера Redis
2) Двухфакторная аутентификация EMV в сервере Redis
3) Реализация гомоморфного шифрования - криптосистемы Пэйе в сервере Redis
4) Тестирование в облачной инфраструктуре DigitalOcean

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	+	+	+	+	+	+

Аналоги: CryptDB

В среднем Cryptis быстрее SQL конкурента на 85%



Оценки проекта

- Победитель «Лучший свободный диплом» в России
- Победитель «У.М.Н.И.К.»
- Победитель конкурса СКБ.Контур
- Публикация в сборнике «Современные проблемы математики и ее прикладные аспекты»
- Участник ВолгаIT
- Участник Web-ready (Сколково)


СЕРТИФИКАТ

выдан

Вахрушеву Павлу Андреевичу

за участие в научно-практической конференции «Современные проблемы математики и её прикладные аспекты – 2013»

г. Пермь, 29–31 октября 2013 г.

Яковлев Вадим Иванович, декан механико-математического факультета

В рамках программы "От студента к президенту"


Сборник материалов всероссийской научно-практической конференции молодых учёных

СОВРЕМЕННЫЕ ПРОБЛЕМЫ МАТЕМАТИКИ И ЕЁ ПРИКЛАДНЫЕ АСПЕКТЫ

2013


webready

МЕЖДУНАРОДНЫЙ КОНКУРС И ИНВЕСТИЦИОННЫЙ ФОРУМ ДЛЯ ПРОЕКТОВ INTERNET&MOBILE

ДИПЛОМ

УЧАСТНИКА ФИНАЛА WEB READY 2013

ОРГКОМИТЕТ WEB READY:


iВолга

Молодёжный форум ПФО 2013

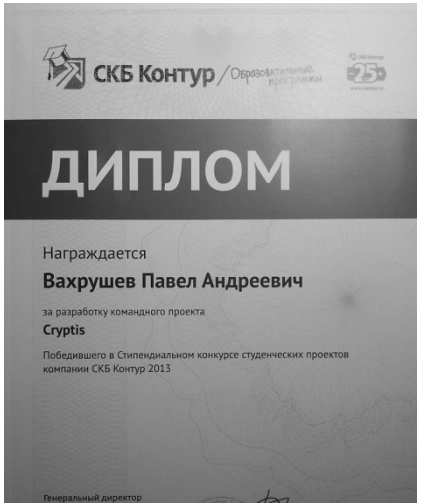
СВИДЕТЕЛЬСТВО

Настоящее свидетельство выдано Вахрушев Павел Андреевич

в том, что он(а) с 18 июня 2013 года по 28 июня 2013 года обучался(-лась) по программе Инновации и техническое творчество

Молодёжного форума Приволжского федерального округа «iВолга – 2013».

Вице-губернатор – руководитель Администрации Губернатора Самарской области Д.Е.Овчинников


СКБ Контур / Образовательные программы

ДИПЛОМ

Награждается

Вахрушев Павел Андреевич

за разработку командного проекта

Cryptis

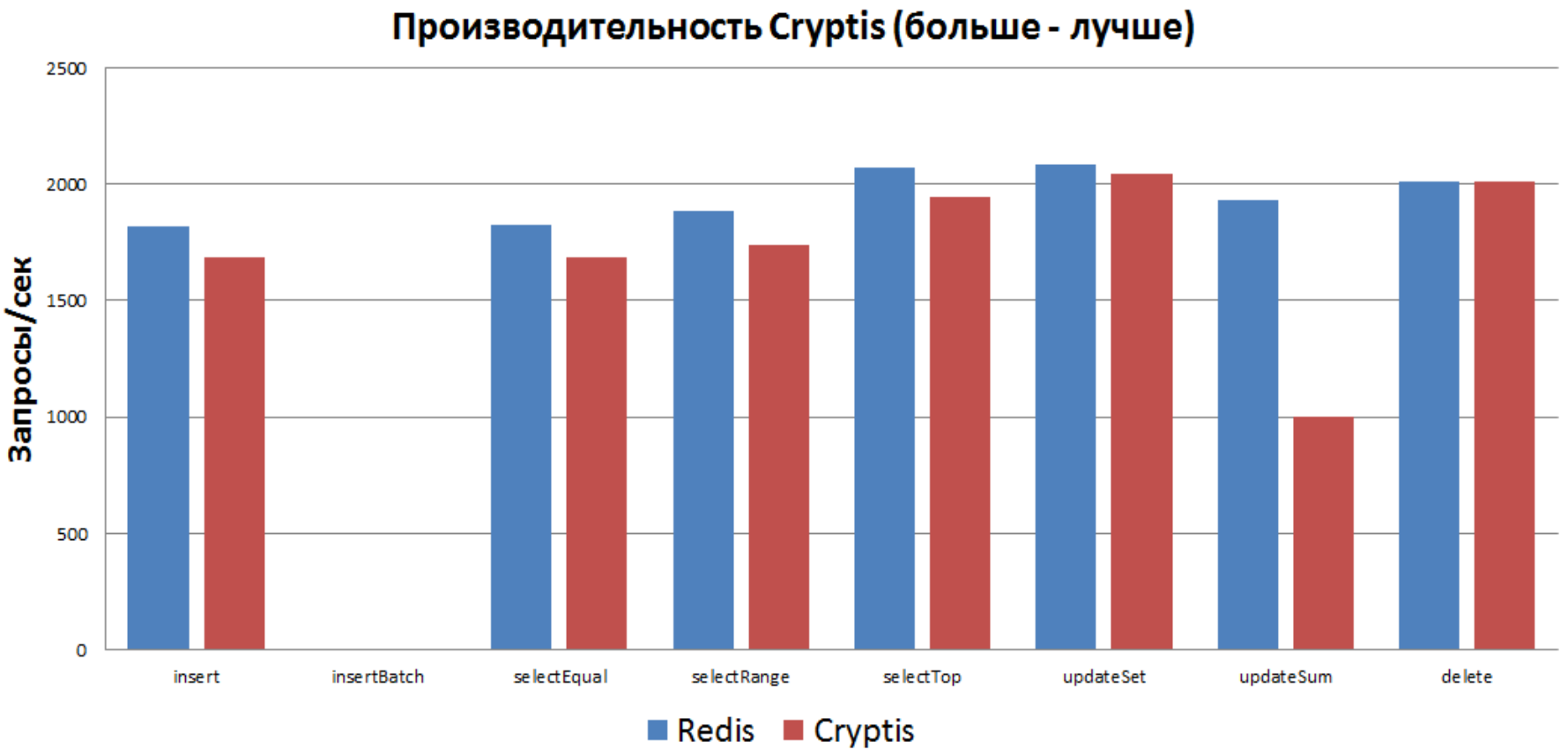
Победившего в Стипендиальном конкурсе студенческих проектов компании СКБ Контур 2013

Генеральный директор

Ограничение языка запросов

Реализация

В среднем падение производительности составляет 11%



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