конференция
РусКрипто' 2016

САНКТ-ПЕТЕРБУРГСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ ПЕТРА ВЕЛИКОГО

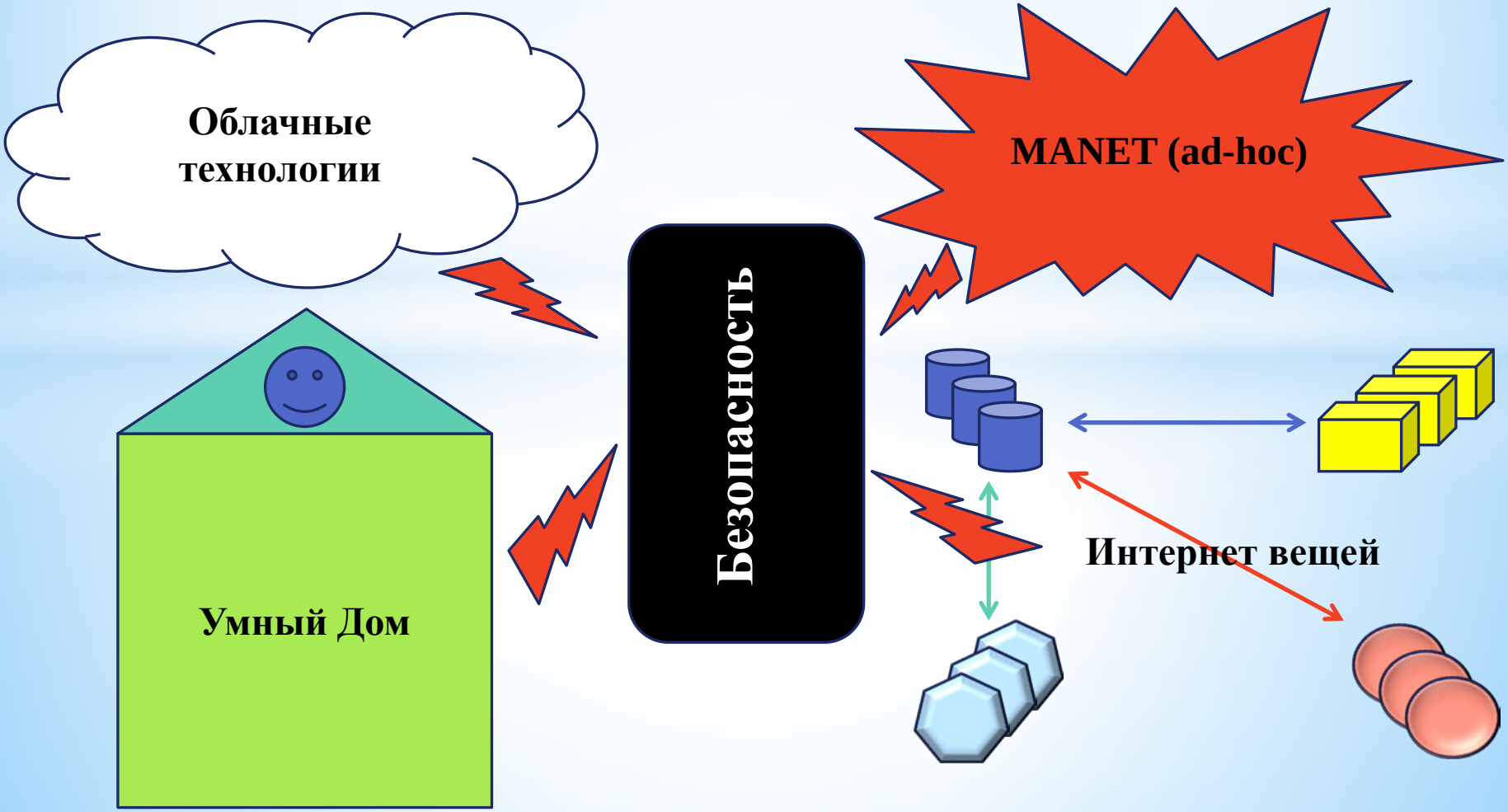
СПбГПУ - ИБКС - 1997
OPE ET CONSILIO OPERA ET STUDIO

Обеспечение безопасности гетерогенных систем с применением гомоморфной модулярной криптографии

Шенец Николай Николаевич
кандидат физ.-мат. наук

Санкт-Петербургский Политехнический университет Петра Великого
кафедра «Информационная безопасность компьютерных систем»

Гетерогенные информационные системы



Гомоморфная криптография: задачи

Задача 1: Необходимо производить вычисления над зашифрованными данными так, чтобы результат после расшифрования соответствовал результату тех же вычислений над открытыми данными. Сформулирована в 1978 году Ривестом, Адлеманом и Дертузосом. Является основной для систем полностью гомоморфного шифрования (**FHE**).

Задача 2: Имеется 2 или более стороны. Необходимо вычислить произвольную функцию, аргументы которой являются секретными данными этих сторон, таким образом, чтобы ни одна из сторон не узнала вход другой стороны, а результат вычисления функции был корректен. Сформулирована Яо в 1982 году. Является основной задачей протоколов секретных распределенных вычислений (**SMC**).

Гомоморфная криптография: возможности применения

И FHE, и SMC обеспечивают конфиденциальность данных конечных пользователей (устройств), позволяя получать результат вычисления произвольной функции над секретными данными.

Системы FHE ориентированы на архитектуру «клиент-сервер», при этом сервер сам производит все вычисления над шифртекстами. Наиболее обосновано их применение при обработке баз данных, хранимых в облаке. В MANET можно организовать скрытую маршрутизацию устройств с помощью FHE.

Системы SMC, наоборот, требуют наличия двух и более сторон для вычисления функции. Они уже активно применяются в системах электронного голосования, аукционов и торгов. SMC уместно применять для получения результата обработки данных различных устройств (MANET, ИВ, УД) без раскрытия самих данных.

Системы FHE: формальная задача

Пусть имеется два множества элементов $\mathbf{U}$ и $\mathbf{V}$, на которых задано n бинарных операций: $\left\{\odot_i^{\mathbf{U}}\right\}, \left\{\otimes_i^{\mathbf{V}}\right\}, i=\overline{1,n}.$

Требуется найти такое отображение $\varphi: \mathbf{U} \to \mathbf{V}$, чтобы выполнялось ***обобщенное свойство гомоморфности***:

$$\varphi(x \odot_i^{\mathbf{U}} y) = \varphi(x) \otimes_i^{\mathbf{V}} \varphi(y),\ \forall x, y \in \mathbf{U},\ \forall i = \overline{1,n}.$$

Криптографическое свойство отображения φ – оно должно быть ***односторонним***, т.е. вычислительно трудно найти прообразы отображения. Однако легальный пользователь должен уметь это делать эффективно. Иными словами, φ должно иметь вид ***функции с лазейкой***.

В отношении FHE используется понятие «семантическая криптостойкость»: пассивный нарушитель не может отличить шифртекст «0» от шифртекста «1».

Системы FHE: имеющиеся разработки (методы)

1. Крейг Джентри (2009 г., на основе идеальных решеток)
2. М. ван Дейк, К. Джентри, Ш. Халеви, В. Вайкунтанатан (2010 г., в $\mathbb{Z}$)
3. З. Бракерски, В. Вайкунтанатан (2011 г., на основе задачи LWE в решетках)
4. З. Бракерски, К. Джентри, В. Вайкунтанатан (2011 г., BGV)
5. К. Джентри, С. Хелави, Н. Смарт (2011 г., GHS - модификация BGV)
6. А. Ростовцев, А. Богданов (2011 г., полиномиальные схемы)
7. К. Джентри, А. Сахоу, Б. Вотерс (2013 г., матричные схемы на основе LWE)
8. С. Кренделев, А. Жиров (2013 г., полиномиальные схемы в классах вычетов)
9. Ф. Буртыка, О. Макаревич (2014 г., матричные полиномы)
10. Л. Дукас, Д. Миччиансио (2014 г., решетки)

Известные продукты:
Библиотека Helib (IBM) – реализует схему GHS.
Библиотека FHEW – реализует схему Л. Дукаса и Д. Миччиансио.
Надстройка к базам данным: CryptoDB (MIT) – использует различные схемы FHE.

Системы FHE: пример (схема Ростовцева)

$n=pq$, $p \neq q$ – простые числа

Генерация гомоморфизма

$\mathbb{Z}/n\mathbb{Z} \to (\mathbb{Z}/n\mathbb{Z})[z]/(f(z)) \;:\; x \to X(z)$

Вход: n, $x \in \mathbb{Z}/n\mathbb{Z}$

Выход: $f(z), X(z) \in (\mathbb{Z}/n\mathbb{Z})[z]/(f(z))$

Шаги:

1. $t \xleftarrow{R} \mathbb{Z}/n\mathbb{Z}$, $D = t^2 \bmod n.$
2. $f(z) = z^2 - D.$
3. $X(z) = z - t + x.$

Число t – личный ключ, определяющий секретный гомоморфизм для клиента.

Протокол вычисления y=F(z)

Участники: клиент и сервер

Клиент: секрет x

Общий вход: n и F

Выход: $y=F(x)$

Шаги:

К: генерирует пару $f(z)$, $X(z)$ и посылает ее серверу.

С: $Y(z) = F(X(z))$ в кольце $(\mathbb{Z}/n\mathbb{Z})[z]/(f(z))$ и посылает значение клиенту.

К: $y \equiv Y(t) \bmod n.$

Стойкость основана на сложности факторизации многочленов, свободных от квадратов, и нахождении их корней в указанном кольце. Однако система не стойка к атакам на основе известных открытых текстов.

Системы SMC: формальная задача

Пусть имеется $n \geq 2$ сторон и функция f от n переменных. Требуется вычислить $f(x_1,\ldots,x_n)$, не раскрывая значений x_i каждой из сторон другим сторонам. Классический случай SMC.

Модификация задачи: имеется n сторон и функция от m переменных. Значение каждой переменной x_i разделено между сторонами с помощью аддитивно гомоморфной схемы разделения секрета (СРС): $x_i \xrightarrow{CPC} \{s_i^1,\ldots,s_i^n\}$. Требуется получить результат вычисления функции f в разделенном виде, т.е.

$\mathrm{Rec}(f_1,\ldots,f_n) = f(x_1,\ldots,x_m), \quad f_i - \textit{вычисляются на основе } f \textit{ и значений } s_l^j.$

В ходе вычислений требуется, чтобы ни одна из сторон не узнала частичные секреты другой стороны. Рассматриваются как пассивная, так и активная модели нарушителя, но на практике применимы лишь протоколы, безопасные по отношению к пассивному нарушителю.

Системы SMC: имеющиеся разработки (методы)

Общие конструкции	На основе СРС	На основе (×,+)-HE
1. Garbared Circuits (А. Яо, 1986, исп. прот. **OT**) 2. Branching Programs (Х. Липма, 2007, исп. **HE** и прот. **PIR**) 3. Private Boolean Circuits (Дж. Нилсен, 2012, 2 стороны, исп. прот. **OT**)	1. Умножение (Д. Бивер, 1989, СРС Шамира) 2. Симм. булевы функции и битовые операции (И. Дамгард и др. 2006) 3. Деление чисел (2002, В. Шоуп и Т.Тофт (2006) 4. Сравнение, массивы (Т. Тофт 2006)	1. XOR-HE прот. (1996, М. Франклин, С Хабер, пассивный нарушитель) 2. Прот. Крамера (2001, Р. Крамер, И. Дамгард, активный нарушитель) 3. «Mix&Match» (2000 г, М. Якобсон и др.) 4. «Conditional gate»(2004, Б. Шонмэйкерс, П. Тайлс)

HE – homomorphic encryption
OT – oblivious transfer protocol
PIR – private information retrieval

Для обеспечения стойкости к активному нарушителю дополнительно требуются протоколы доказательств с нулевым разглашением, схемы согласия, и/или проверяемые СРС, что делает протоколы существенно более трудоемкими.

Системы SMC: разработанные платформы

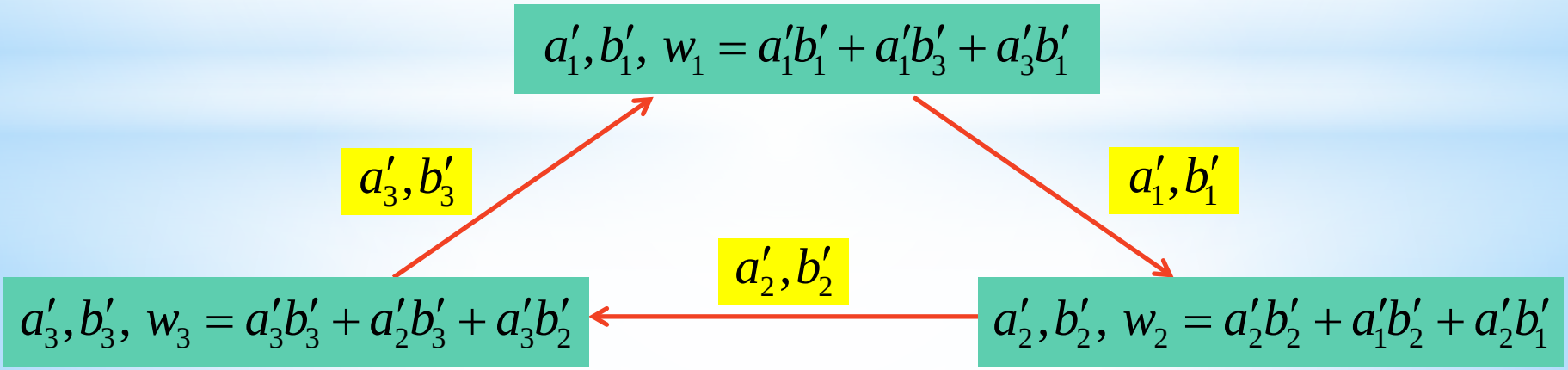
Параметр	FairPlay-MP	Secure-SCM	TASTY	Share-mind	VIFF	SEPIA	VMCrypt
год выхода	2004-2008	2008	2008-2010	2008-2011	2010	2010	2011
Разработ-чики	Израиль	Италия (Милан)	Германия (Бохум)	Эстония (Тарту)	Дания (Архус)	Швейц. Цюрих	США DARPA
Основа	GC	GC	GC+ HE	ЛСРС 3 уч.	СРС Шамира	СРС Шамира	GC (на лету)
Нару-шитель	пасс.	пасс.	пасс/акт	пасс.	пасс.	пасс.	пасс.
Приме-нение	Академ.	Академ.	Академ.	Бизнесс	Академ.	Академ.	Академ.

Системы SMC: пример (умножение в SHAREMIND)

Числа представляются в виде: $a = a_1 + a_2 + a_3 \bmod 2^{32}$, $a = a_1 \oplus a_2 \oplus a_3$.

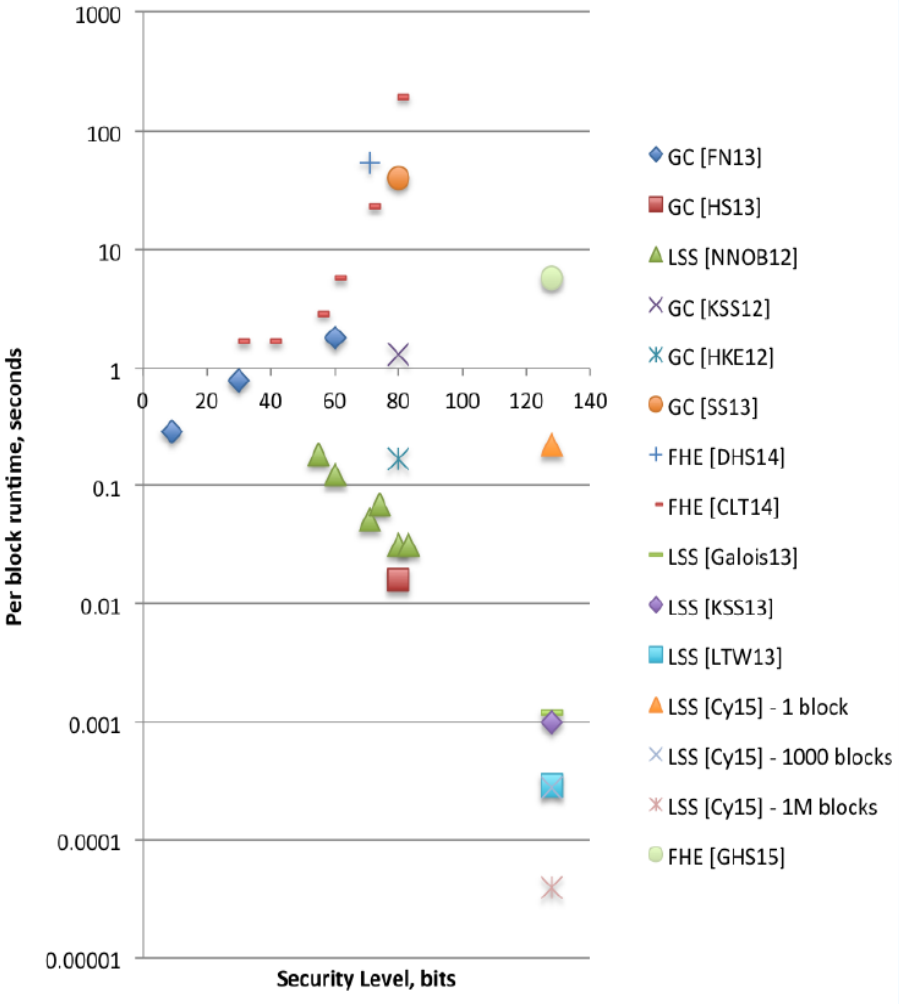
Смена частичных секретов (resharing) проводится до/после операций:

$$a_i' = a_i + r_{ij} - r_{ki}, \quad r_{12}, r_{23,} r_{31} \xleftarrow{R} \mathbb{Z}_{2^n}, \quad P_i \xrightarrow{r_{ij}} P_j.$$



$$w_1 + w_2 + w_3 = a_1'b_1' + a_1'b_3' + a_3'b_1' + a_2'b_2' + a_2'b_1' + a_1'b_2' + a_3'b_3' + a_3'b_2' + a_2'b_3' =$$
$$= (a_1' + a_2' + a_3')(b_1' + b_2' + b_3') = (a_1 + a_2 + a_3)(b_1 + b_2 + b_3)$$

FHE vs SMC:
скорость вычисления блока AES 128 бит



FN13 – Фредериксон, Нильсен (2013, GPU)
HS13 – Хенеска, Шнайдер (2013)
NNOB12 – Нильсен и др. (2012, TinyOT)
KSS12 – Кройтер и др. (2012)
HKE12 – Хуанг и др. (2012)
SS13 – Шелат, Жен (2013)
DHS14 – Дороз и др. (2014, AES на NTRU)
CLT14 – Корон и др. (2014)
GHS15 – Джентри, Хелави, Смарт (2015, AES)
Galois13 – ShareMonad в рамках проекта **PROCCED DARPA** (2013)
KSS13 – Келлер, Шоль, Смарт (2013)
LTW13 – Лоур и др. (2013, Sharemind)
Cy15 – Sharemind в в рамках проекта **PROCCED DARPA** (2015)

США - проект PROCEED от DARPA (2011-2015)
ЕС - проект PRACTICE (2013-2016)

FHE и SMC: общее – модулярность и гомоморфность

Пусть M – некоторый модуль, в котором имеется несколько собственных подмодулей M_1, M_2,…,M_n. Как правило, имеет место разложение:

$$M/M_1 \cdots M_n \cong M/M_1 \oplus \cdots \oplus M/M_n .$$

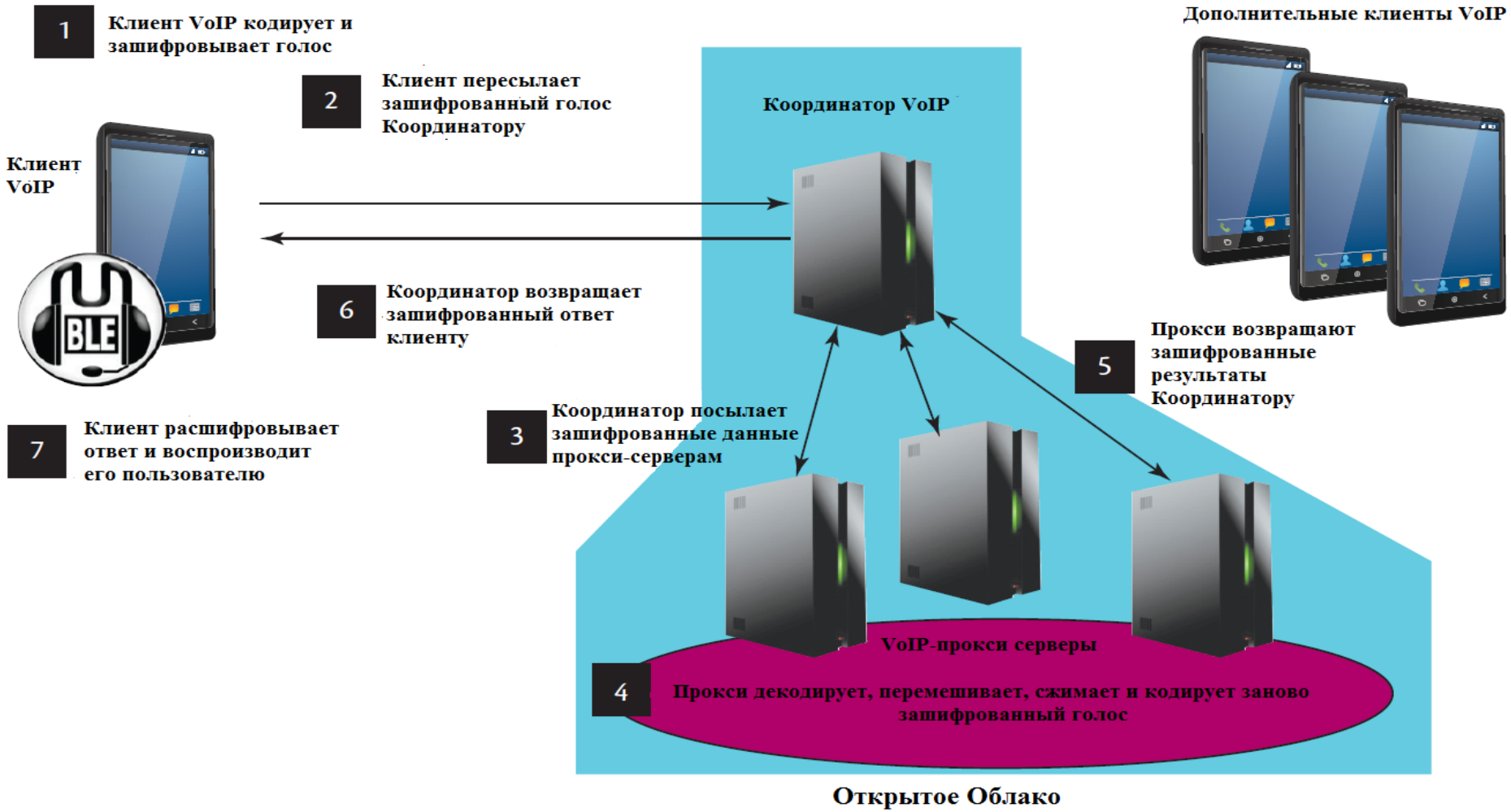
Для реализации FHE необходимо уметь строить и вычислять секретный гомоморфизм модулей. Например, открытые тексты выбираются из M_1, а шифртексты – из M_1M_2, при этом имеется естественное вложение модуля M_1 в M_1M_2. Требуется, чтобы задача факторизации модуля была вычислительно трудной. Однако заметим, что разность шифртекста и открытого текста всегда сравнима с 0 по модулю M_1, что делает большинство хороших колец непригодными с точки зрения стойкости, и реализация FHE, естественно, становится трудной. Подходящие модули – решетки, кольца многочленов от нескольких переменных.

Реализация SMC, наоборот, предполагает, что основные вычисления ведутся в модулях M_i, а результат получается из естественного разложения. При этом факторизация модуля известна, а стойкость основана на совершенности соответствующей модулярной(линейной) СРС.

FHE и SMC: Разработки PROCEED+PRACTICE

GC	1. Маршрутизация 2. Идентификация отпечатков пальцев 3. Поиск «похожих» пациентов (историй болезни), диагностика
FHE	1. VoIP через сервер 2. Почтовый фильтр (только совпадение строк) 3. Распознавание образов (в судебной практике) 4. Генетические алгоритмы
CPC	1. VoIP через облачные сервисы 2. Почтовый фильтр (с использованием регулярных выражений) 3. Байесовский спам-фильтр 4. Статистика (лин. регр. анализ; успеваемость студентов) 5. Поиск коллизий спутниковых систем 6. Аутентификация WEB-сервиса на основе SHA-2 7. Биоинформатика (анализ и генетические алгоритмы) 8. Система поиска мошенников (в налоговой сфере) 9. Линейное программирование (в экономике)

FHE и SMC: пример применения (VoIP через облако)



конференция
РусКрипто' 2016

САНКТ-ПЕТЕРБУРГСКИЙ
ПОЛИТЕХНИЧЕСКИЙ
УНИВЕРСИТЕТ
ПЕТРА ВЕЛИКОГО

Спасибо за внимание!