МЕТОДЫ ПОЛНОСТЬЮ ГОМОМОРФНОГО ШИФРОВАНИЯ НА ОСНОВЕ МАТРИЧНЫХ ПОЛИНОМОВ

***Бабенко Людмила Клементьевна**, доктор технических наук, профессор, г. Таганрог*
***Буртыка Филипп Борисович**, г. Таганрог*
***Макаревич Олег Борисович**, доктор технических наук, профессор, г. Таганрог*
***Трепачева Алина Викторовна**, г. Таганрог*

Полностью гомоморфное шифрование позволяет по зашифрованным данным $Enc(m_1),...,Enc(m_t)$ и произвольной функции f вычислить шифртекст $Enc(f(m_1,...,m_t))$, не зная ключа расшифрования и исходных данных $m_1,...,m_t$. До опубликования новаторской работы Крейга Джентри в 2009 году были известны лишь частично гомоморфные схемы шифрования, позволяющие вычислять некоторые функции (но не все возможные) над зашифрованными данными. Однако на данный момент предложено уже достаточно большое количество полностью гомоморфных конструкций. В данной работе наиболее подробно освещается полностью гомоморфная криптосистема, основанная на матричных полиномах.

***Ключевые слова**: облачные вычисления, гомоморфное шифрование, криптографические вычисления, проверяемые вычисления, функциональное шифрование.*

FULLY HOMOMORPHIC ENCRYPTION TECHNIQUES USING MATRIX POLYNOMIALS

***Ludmila Babenko**, Doctor of Technical Sciences, Professor, Taganrog*
***Philipp Burtyka,** Taganrog*
***Oleg Makarevich**, Doctor of Technical Sciences, Professor, Taganrog*
***Alina Trepacheva,** Taganrog*

A fully homomorphic encryption scheme enables computation $Enc(f(m_1,...,m_t))$ of arbitrary functions f on encrypted data $Enc(m_1),...,Enc(m_t)$ without knowing decryption key and plaintext messages $m_1,...,m_t$. Before publishing of groundbreaking Gentry's paper in 2009 where known only partial homomorphic encryption schemes, allowing to evaluate some (but not all possible) functions on encrypted data. However, at the moment a large number of fully homomorphic constructions is already known. In this paper, the most careful attention is given to fully homomorphic cryptosystem based on matrix polynomials.

***Keywords**: cloud computations, homomorphic encryption, functional encryption, secure computations, verifiable computations.*

I. ВВЕДЕНИЕ

Данная работа, по замыслу авторов, должна способствовать появлению России на научной карте мира в области современной теоретической криптографии. Современная криптография – это нечто большее, чем просто наука о секретной передаче информации от одного корреспондента к другому. Это целый ряд вопросов относительно возможностей обработки секретной информации и разграничения её использования. Начало современной криптографии – шифрование с открытым ключом, предложенное в новаторской работе Диффи и Хеллмана [1] и впервые построенное Ривестом, Шамиром и Эдлманом [2] – предоставляет возможность для отправителя шифровать сообщение с помощью открытого ключа получателя, а для получателя – расшифровать шифртекст, чтобы получить исходное сообщение, используя свой секретный ключ. Однако с этой точки зрения криптосхемы позволяют осуществить доступ к зашифрованным данным по принципу все или ничего – наличие секретного ключа расшифрования позволяет узнать сообщение целиком, а без ключа расшифрования шифртекст совершенно бесполезен.

Такое положение дел вызывает интригующий вопрос, впервые поставленный Ривестом, Адлеманом и Дертузо в 1978 году: *Можно ли делать произвольные вычисления над данными, в то время как они остаются зашифрованными, никогда не расшифровывая их?* Это требует, казалось бы, фантастической способности выполнять вычисления над зашифрованными данными, не будучи в состоянии «видеть» их.

Такая способность также приводит к ряду полезных приложений, включая возможность конфиденциального делегирования произвольных вычислений в «облако» и способности хранить все данные в зашифрованном виде и выполнять вычисления на зашифрованных данных, расшифровывая только тогда, когда необходимо узнать их.

Полностью гомоморфное шифрование – особый тип криптосистемы, который позволяет проводить произвольно сложные вычисления с зашифрованными данными. Длительное время полностью гомоморфное шифрование рассматривалось как «святой Грааль криптографии», и лишь в 2009 году в новаторской работе Джентри была впервые показана его возможность. Приглашаем читателя в путешествие по увлекательным математическим методам, лежащим в основе этих разработок, которые, в свою очередь, порождают множество новых интересных вопросов в криптографии.

Организация данной статьи. Начав с краткой истории, мы перейдем затем к формальным определениям гомоморфного шифрования и его различным полезным свойствам. Затем мы опишем последние работы в этой области, которые значительно отличаются от исходных криптосистем и приводящие к более простому устройству и большей эффективности. В заключение обсудим приложения полностью гомоморфного шифрования и (очень неполный) перечень научных направлений. Наша цель в этом краткой статье – передать читателю дух основных идей и разработок в этой области, ссылаясь на оригинальные работы для более подробного ознакомления.

II. КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ И ВОПРОСЫ, СВЯЗАННЫЕ С НИМИ

Понятие схем шифрования, которые позволяют нетривиальные вычисления над зашифрованными данными, впервые было предложено Ривестом, Адлеманом и Дертузо [3] в 1978 году, в удивительно прозорливой (провидческой) статье под названием «О банках данных и гомоморфизмах, сохраняющих конфиденциальность». Ривест и др. [3] предложили функцию возведения в степень и функцию RSA в качестве аддитивного и мультипликативного конфиденциальных гомоморфизмов, соответственно. Заметим, однако, что ни одна из этих функций сама по себе не обеспечивает криптостойкости даже против атаки по выбранному открытому тексту.

Первая семантически криптостойкая гомоморфная схема шифрования была предложена в работе Гольдвассер и Микали [4], в которой впервые введено удобное определение криптостойкости для шифрования. В GM схема шифрования поддерживает сложение зашифрованных битов по модулю 2 (то есть, функцию «исключающее или»). Ряд систем шифрования, которые либо аддитивно либо мультипликативно гомоморфны, последовали его примеру. Это включает в себя криптосистему Эль Гамаля [5], криптосистему Пэйе [6] и ее обобщение Дамгаардом (Damgård) и Юриком (Jurik) [7], множество криптосхем на основе теории решеток, начиная с работ Айтая и Дворк [8], [9], [10], и многие другие [11], [12], [13]. Все эти схемы поддерживают либо гомоморфное сложение, либо умножение открытых текстов, но не то и другое одновременно! Построение схемы шифрования, которая была бы одновременно аддитивно и мультипликативно гомоморфной, оставалось открытым каверзным вопросом. Очевидно, что поскольку сложение и умножение (скажем, над $\mathbf{Z}_2$) образуют полный набор операций, такая криптосхема позволит выполнять любые вычисления на зашифрованных данных за полиномиальное время!

Аддитивно гомоморфные схемы шифрования уже весьма полезны в ряде приложений. Не будем пытаться привести исчерпывающий список здесь, но упомянем три таких приложения. Коэн и Фишер [11] предложили аддитивно гомоморфную криптосистему на основе вычетов высокого порядка и показали, как использовать её для проведения безопасного электронного голосования. Это предложение и его продолжения прошли свой путь до современных веб-систем голосования, таких как *Гелиос* [14]. Совсем недавно, Пейкерт и Вотерс [15] построили с потерями, и все, кроме одного, односторонние функции с лазейками из аддитивно гомоморфных криптосхем (с некоторыми дополнительными свойствами), которые они, в свою очередь, использовали для создания шифрования с открытым ключом, криптостойкого против атаки по выбранному шифртексту (CCA-криптостойкой). Третье приложение

– это протоколы конфиденциального получения информации (КПИ), рассказ о которых отложим до конца этого раздела.

Потребовалось много времени, чтобы построить криптосхемы, которые выходят за рамки простого аддитивного (или мультипликативного) гомоморфизма. Боне, Го и Нисим [16] представили криптосхему на основе билинейных спариваний на эллиптических кривых, которые могли бы выполнять сколь угодно много сложений, а также одно умножение открытых текстов (Джентри, Галеви и Вэйкунтанасан [17] позже показали, как добиться такой же функциональности, используя решетки).

В работе Сэндера, Янга и Юнга [18] была построена криптосистема, которая может вычислять NC^1 схемы (шифртексты в их кнриптосистеме растут в геометрической прогрессии с нарастанием глубины схемы и влекут ограничение на NC^1), а криптосистема Агилара-Мелькора, Гэйборита и Герранца [19] гомоморфно вычисляет (многомерные) полиномы (причем шифртекст растет экспоненциально от степени полинома). Кандидат на полностью гомоморфное шифрование, предложенный Феллоузом и Коблицем [20] на основе сложности проблемы принадлежности идеалу (ППИ) в кольце полиномов от нескольких переменных $\mathsf{F}_q[x_1,\ldots,x_n]$, был взломан при многих вариантах выбора параметров, хотя криптостойкость их схемы в общем еще кажется открытым вопросом.

Важное применение гомоморфного шифрования следует из работы Кашилевица и Островского [21], в которой показано, как построить (на одном сервере) протокол конфиденциального получения информации (КПИ) с сублинейной коммуникационной сложностью из любой аддитивно гомоморфной криптосистемы. Конфиденциальное получение информации, введённое Чором, Кашилевицем, Голдричем и Суданом [22], – это задача, в которой пользователь пытается получить i-й элемент в базе данных размером N, не раскрывая никакой информации об индексе i владельцу базы данных (основной вариант задачи как таковой не касается дополнительной проблемы защиты конфиденциальности владельца базы данных). Конечно, так как это может быть тривиально достигнуто за счет отправки владельцем базы данных всей база данных пользователю, нетривиальный вопрос: можем ли мы поступить лучше с точки зрения коммуникационной сложности? Для базы данных размером N протокол Кашелевица-Островского требует пересылки только N^{ε} бит для сколь угодно малой постоянной $\varepsilon > 0$.

Конфиденциальное получение информация тесно связано с полностью гомоморфным шифрованием. В самом деле, можно легко увидеть, как построить *неэффективную* полностью гомоморфную криптосхему из какой-либо схемы КПИ. Построение осуществляется с помощью простого выписывания таблиц истинности функций (например, n-битных входов и один выходной бит) в качестве базы данных. Шифртекст сообщения $m \in \{0,1\}^n$ вычисляется как запуск пользователем протокола КПИ для извлечения m-го элемента (записи) из таблицы – а именно - $f(m)$. Так как запрос пользователя КПИ скрывает m, шифрование семантически криптостойкое. Кроме того, длина шифртекста после гомоморфного вычисления в точности равна коммуникационной сложности протокола КПИ, которая сублинейна, или даже логарифмична [23], [24], [25], [26]. Загвоздка в том, что для функции с n аргументами, гомоморфное вычисление требует $2^{O(n)}$ шагов. Более интересно, Ишай и Пэскин [27] показали, как использовать специфичные, очень эффективные *аддитивно* гомоморфные криптосистемы для построения криптосистемы, способной вычислять *ветвящиеся программы* гомоморфно. Мы считаем, что эти связи между КПИ и криптосхемами ПГШ далеко не случайны, и более углубленное исследование этой связи непременно обнаружит бесценные сокровища.

Подводя итог состоянию дел до 2009, были известны криптосистемы, которые могли бы выполнять сложения и одиночное умножение [16], [17], а также криптосистемы, которые могли бы вычислять ветвящиеся программы [27], полиномы [19] и NC^1 схемы при увеличении размера шифртекста [18].

Большой прорыв пришел с работой Джентри [25] в 2009 году, который показал первое правдоподобное построение полностью гомоморфной криптосхемы, которая позволяет вычислять произвольные функции над зашифрованными данными, производя при этом компактные шифртексты.

После выхода основополагающей работы Джентри активность исследователей значительно возросла. Стали выходить работы с модификациями исходной криптосистемы Джентри, которые улучшали её производительность.

Параллельно с этим другие криптографы пытались найти альтернативные принципы построения ПГШ. Одним из таких направлений является попытка построить симметричное гомоморфное шифрование как более эффективное, чем с открытым ключом [28].

В работе [29] сделана попытка построить симметричную гомоморфную криптосхему с использованием полиномов от многих переменных. Отечественные исследователи предлагали построить гомоморфное шифрование на основе полиномов от одной переменной [30-32].

Другой цикл работ связан с матричными полиномами [33,34].

III. ОПРЕДЕЛЕНИЯ И СВОЙСТВА ГОМОМОРФНОГО ШИФРОВАНИЯ

Прежде чем описывать построение и последующие работы о полностью гомоморфном шифровании на основе матричных полиномов, мы сперва формализуем понятие гомоморфного шифрования, опишем его различные свойства и введем обозначения для последующего обсуждения.

3.1. Гомоморфное шифрование - определения

В этом разделе (и в этой статье) мы используем λ для обозначения параметра уровня криптостойкости. Кроме того, все криптосхемы в этой статье шифруют побитно, и следовательно, наши определения относятся только к этому случаю. Обобщение для произвольного пространства сообщений следует немедленно.

Гомоморфная (с открытым ключом) криптосистема $\varepsilon = (\mathrm{KeyGen}_\varepsilon, \mathrm{Enc}_\varepsilon, \mathrm{Dec}_\varepsilon, \mathrm{Eval}_\varepsilon)$ – это четверка вероятностных полиномиальных по количеству шагов (ВПКШ) алгоритмов, выраженная следующим образом.

• Генерация ключа.

Алгоритм $(evk, sk) \leftarrow \mathrm{KeyGen}_\varepsilon(1^\lambda)$ принимает на вход параметр криптостойкости λ и выдает открытый ключ для вычисления evk и секретный ключ sk для зашифрования и расшифрования.

• Зашифрование.

Алгоритм $c \leftarrow \mathrm{Enc}_\varepsilon(sk, m)$ принимает на вход секретный ключ sk и однобитное сообщение открытого текста $m \in \{0,1\}$ и выдает шифртекст c.

• Расшифрование.

Алгоритм $m^* \leftarrow \mathrm{Dec}_\varepsilon(sk, c)$ принимает на вход секретный ключ sk и шифртекст c и выдает сообщение открытого текста $m^* \in \{0,1\}$.

• Гомоморфное вычисление.

Алгоритм $c_f \leftarrow \mathrm{Eval}_\varepsilon(f, c_1, ..., c_l)$ получает на вход ключ для вычисления evk, функцию $f : \{0,1\}^l \to \{0,1\}$ и набор из l шифртекстов $c_1, ..., c_l$ и выдает шифртекст c_f.

Представление функции f – важный вопрос. Так как представление может варьироваться в зависимости от СФЭ, мы оставляем этот вопрос за пределами этого синтаксического определения. Заметим, однако, что в данном исследовании мы будем представлять f с помощью арифметической схемы из функциональных элементов над $\mathbf{F}_2$ (эквивалентно булевой схеме из функциональных элементов AND и XOR).

Отметим, что в то время как можно рассматривать ключ для вычисления как часть открытого ключа, как это было сделано в некоторых работах по полностью гомоморфному шифрованию, на наш взгляд, стоит рассматривать его как отдельный объект и различать открытые элементы, которые используются для шифрования (а именно, открытый ключ зашифрования) и те, которые используются только для гомоморфного вычисления (а именно, ключ вычисления evk).

Единственное понятие криптостойкости, которое мы рассмотрим в этой работе — это семантическая криптостойкость, а именно криптостойкость в отношении (со ссылкой на) пассивных нарушителей. Мы используем его широко известную формулировку, как IND-CPA криптостойкость, определяемую следующим образом.

Определение 3.1 (CPA криптостойкость). Схема ε обладает IND-CPA криптостойкостью, если для любого полиномиального по числу шагов алгоритма нарушителя A выполняется, что

$$\mathrm{Adv}_{\mathrm{CPA}}[\mathsf{A}] = \left|\Pr[\mathsf{A}(evk, \mathrm{Enc}_\varepsilon(sk, 0)) = 1] - \Pr[\mathsf{A}(evk, \mathrm{Enc}_\varepsilon(sk, 1)) = 1]\right| = negl(\lambda),$$

где $(evk, sk) \leftarrow \mathrm{KeyGen}_\varepsilon(1^\lambda)$.

Другими словами вероятность того, что алгоритм криптоаналитика A правильно отличит шифртекст нуля от шифртекста единицы – функция, бесконечно малая от λ.

Мы переходим к определению корректности гомоморфного вычисления. Обратите внимание, что мы не определяем «корректность» расшифрования как такового[1], а скорее, некоторая форма корректности будет следовать из корректности гомоморфного вычисления.

Начнем с определения криптосистемы, гомоморфной по отношению к какой-то конкретной функции. Это понятие также иногда называют «ограниченный гомоморфизм».

1 Классически [35] корректная криптосистема определяется через справедливость соотношения $\mathrm{Dec}(sk, \mathrm{Enc}(sk, m)) = m$, т.е. после расшифрования шифртекста должен получиться исходный открытый текст.

Определение 3.2 (корректность расшифрования после гомоморфного вычисления). Криптосхема $\varepsilon = (\mathrm{KeyGen}, \mathrm{Enc}, \mathrm{Dec}, \mathrm{Eval})$ корректна для булевой СФЭ F, имеющей t входов, если для любой пары ключей (sk, evk), выданной алгоритмом $\mathrm{KeyGen}(\lambda)$, любых t открытых текстов m_i и соответствующих им шифртекстов $c_i \leftarrow \mathrm{Enc}(\mathbf{sk}, m_i)$ выполняется:

$$\mathrm{Dec}\left(\mathbf{sk}, \mathrm{Eval}(\mathbf{rk}, F, c)\right) = F(m_1, ..., m_t).$$

Обратите внимание, что вышеприведенное синтаксическое определению само по себе разрешает довольно неинтересные гомоморфные криптосхемы. В частности, рассмотрим алгоритм гомоморфного вычисления, который действует как тождественная функция и выдает шифртексты $c_1, ..., c_l$, а также описание функции f. Расшифрование восстанавливает сообщения $m_1, ..., m_l$ и выдает $f(m_1, ..., m_l)$.

Ключевым свойством криптосхемы гомоморфного шифрования, предотвращающим такие неинтересные (и бесполезные!) конструкции, является понятие компактности, определенное ниже.

Определение 3.3 (компактность). Гомоморфная криптосхема ε компактна если существует полином $s = s(\lambda)$ такой, что длина результата $\mathrm{Eval}_\varepsilon(f, c_1, ..., c_l)$ не превышает s битов (независимо от f или количества входов).

Другими словами, требуется, чтобы компактность размеров шифртекста после гомоморфного вычисления не зависела бы ни от числа входов l, ни от сложности функции f, но только от размера выхода f. Обратите внимание, что гомоморфная криптосхема (из определения выше) не обязательно компактна.

Мы даем минимальное определение полностью гомоморфного шифрования, которого достаточно для большинства приложений.

Определение 3.4 (полностью гомоморфное шифрование). Криптосхема ε полностью гомоморфна если она является как компактной, так и гомоморфной для всех булевых СФЭ.

3.2 Два полезных свойства

Опишем два полезных свойства гомоморфных криптосхем, а именно схемная конфиденциальность (circuit privacy) и многоразовый гомоморфизм (multyhop homomorphism).

В сценарии делегирования вычислений (описанного в разделе 1) использование гомоморфного шифрования защищает конфиденциальность клиента, *но не конфиденциальность сервера*. Схемная конфиденциальность – это свойство гомоморфного шифрования, которое гарантирует, что входные данные сервера - а именно, функция f - остаются в секрете от клиента.

В частности, схемная конфиденциальность подразумевает, что результат работы алгоритма $\mathrm{Eval}_\varepsilon(f, c_1, ..., c_l)$ не раскрывает какой-либо информации об f клиенту, кроме $f(m_1, ..., m_l)$. Следует отметить, что клиент знает секретный ключ sk, а также вероятностное распределение, используемое для генерации шифртекстов c_i. Это формализовано в определении на основе моделирования, которое требует, чтобы результат работы алгоритма $\mathrm{Eval}_\varepsilon(f, c_1, ..., c_l)$ можно было смоделировать используя только $f(m_1, ..., m_l)$ (но не какую-либо другую информацию об f). Был изучен ряд вариантов схемной конфиденциальности для борьбы с нарушителями или получестными клиентами и с ослаблением требования, что клиенту разрешается узнавать некоторую ограниченную информацию о f, например, размер вычислительной схемы f, но ничего больше. Для детального обсуждения схемной конфиденциальности мы отсылаем читателя к [27], [36].

В некоторых случаях полезно, потребовать, чтобы результаты работы алгоритма $\mathrm{Eval}_\varepsilon$ могли бы быть использованы в качестве входных данных для другого гомоморфного вычисления. Гомоморфная криптосхема с этим свойством называется «многоразово гомоморфная» схема шифрования – понятие, введенное в работе Джентри, Галеви и Вэйкунтанасана [36]. Для детального обсуждения многоразового (итерационный, повторяемый) гомоморфизма и его приложений мы отсылаем читателя к [36].

Криптосхемы, которые мы представляем в этой работе, являются схемно конфиденциальными (или могут быть легко преобразованы в таковые), а также «многоразово гомоморфны», но мы не освещаем подробно эти свойства далее в этой работе.

IV. КРИПТОСХЕМА НА ОСНОВЕ МАТРИЧНЫХ ПОЛИНОМОВ

Шифры Кренделева предполагали простоту и производительность, однако на деле не оказались ни компактными, ни криптостойкими [37, 38]. Криптосистемы А.Г. Ростовцева показали компактность, но не криптостойкость против атаки на основе известного открытого текста [39].

Все эти криптосистемы построены на основе скалярных полиномов. Что такое полиномы?

Одно из современных формальных определений [40] состоит в том, чтобы определить полиномы как последовательности, состоящие из конечного числа ненулевых элементов. Полиномы можно складывать и умножать, и эти операции для полиномов определены естественно в случае, если их коэффициенты образуют такую алгебраическую структуру как кольцо [40] (причем коммутативность коэффициентов не имеет значения [41]).

Итак, пусть $\mathbf{Z}_p^{N\times N}$ – кольцо $N\times N$ матриц с элементами из кольца $\mathbf{Z}_p$ целых чисел по модулю числа p. Рассмотрим множество последовательностей матриц из $\mathbf{Z}_p^{N\times N}$

$$F=\{\mathbf{A}_0,\mathbf{A}_1,\mathbf{A}_2,...\},\mathbf{A}_i\in\mathbf{Z}_p^{N\times N},$$

таких, что все $\mathbf{A}_i$, кроме конечного их числа, равны нулевой матрице. Пусть $\mathbf{Z}_p^{N\times N}[X]$ обозначает множество всех таких последовательностей. Если $F,G\in\mathbf{Z}_p^{N\times N}[X]$, $G=\{\mathbf{B}_0,\mathbf{B}_1,\mathbf{B}_2,...\},\mathbf{B}_i\in\mathbf{Z}_p^{N\times N}$, то определим

$$F+G=\{\mathbf{A}_0+\mathbf{B}_0,\mathbf{A}_1+\mathbf{B}_1,\mathbf{A}_2+\mathbf{B}_2,...\},$$
$$F\cdot G=\{\mathbf{A}_0\cdot\mathbf{B}_0,\mathbf{A}_0\mathbf{B}_1+\mathbf{A}_1\mathbf{B}_0,\mathbf{A}_0\mathbf{B}_2+\mathbf{A}_1\mathbf{B}_1+\mathbf{A}_2\mathbf{B}_0,...\}=\{\mathbf{C}_k\},$$

где $\mathbf{C}_k=\sum_{i+j=k}\mathbf{A}_i\cdot\mathbf{B}_j,k=0,1,2,...$.

Можно показать, что при таких определениях сложения и умножения множество $\mathbf{Z}_p^{N\times N}[X]$ становится кольцом. Элементы этого кольца будем называть *матричными полиномами*.

Для удобства дальнейшего изложения введем следующие обозначения: 1) $s\xleftarrow{\$}R$ означает, что s из R выбирается по равномерному распределению; 2) ω,δ,ψ – некоторые заранее установленные константы. Алгоритмы криптосхемы действуют следующим образом.

• Генерация секретного ключа.

1) Генерируется приведенный (т.е. его старший коэффициент – единичная матрица) полином $\mathbf{K}(X)\in\mathbf{Z}_p^{N\times N}[X]$, такой что $\deg(\mathbf{K}(X))\le\omega\cdot\lambda$, а его коэффициенты $\mathbf{K}_i\xleftarrow{\$}\mathbf{Z}_p^{N\times N},i=0,...,\deg(\mathbf{K}(X))-1$.
2) Генерируется вектор $\vec{k}\in\mathbf{Z}_p^N$, $k_i\xleftarrow{\$}\mathbf{Z}_p$, такой что хотя бы одна координата вектора должна быть обратимой в $\mathbf{Z}_p$. Итого, на выходе алгоритма секретный ключ $sk\leftarrow\{\mathbf{K}(X),\vec{k}\}$.

• Генерация ключа вычисления.

1) Генерируется матричный полином $\mathbf{R}'(X)\in\mathbf{Z}_p^{N\times N}[X]$ такой, что $\deg(\mathbf{R}'(X))\le\delta\cdot\lambda$, $\mathbf{R}'_i\xleftarrow{\$}\mathbf{Z}_p^{N\times N},i=0,...,\deg(\mathbf{R}'(X))-1$. Тогда ключ вычисления – это $evk=\{\mathbf{R}'(X)\cdot\mathbf{K}(X)\}$.

• Зашифрование.

1) Открытому тексту $m\in\mathbf{Z}_p$ сопоставляется случайная матрица $\mathbf{M}\in\mathbf{Z}_p^{N\times N}$ такая, что $\mathbf{M}\cdot\vec{k}=m\cdot\vec{k}$ и $\mathbf{M}\cdot\mathbf{K}(X)=\mathbf{K}(X)\cdot\mathbf{M}$, т.е. она имеет собственный вектор $\vec{k}$ при собственном значении m и коммутирует с матричным полиномом $\mathbf{K}(X)$.
2) Генерируется $\mathbf{R}(X)\in\mathbf{Z}_p^{N\times N}[X]$, где $\deg\mathbf{R}(X)\le\psi\cdot\lambda$ выбирается, так что $\deg(\mathbf{R}(X))<\deg(\mathbf{R}'(X))-\deg(\mathbf{K}(X))$, $\mathbf{R}_i\xleftarrow{\$}\mathbf{Z}_p^{N\times N},i=0,...,\deg(\mathbf{R}(X))$.
3) Вычисляется шифртекст $\mathbf{C}(X)=\mathbf{R}(X)\cdot\mathbf{K}(X)+\mathbf{M}$.

• Расшифрование.

1) Вычисляется $\mathbf{M}=\mathbf{C}(X)\bmod\mathbf{K}(X)$.
2) Для обратимой координаты k_i вычисляется $m=k_i^{-1}\left(\mathbf{M}\cdot\vec{k}\right)$.

• Гомоморфное вычисление.

Сопоставление полиному $f(x_1,...,x_t)$ над $m_1,...,m_t\in\mathbf{Z}_p$ полинома $f^{\perp}(\mathrm{X}_1,...,\mathrm{X}_t)$ над соответствующими шифртекстами $\mathrm{C}_1,...,\mathrm{C}_t$ осуществляется простой заменой операций над $\mathbf{Z}_p$ на сложение и умножение полиномов в $\mathbf{Z}_p^{N\times N}[X]$. Для предотвращения роста степени матричных полиномов после их умножения осуществляется приведение по модулю **rk**.

Для выданных алгоритмом Enc_ε шифртекстов $c\leftarrow\mathbf{R}(X)\cdot\mathbf{K}(X)+\mathbf{M}$ алгоритм расшифрования выдает $m=k_i^{-1}\left((\mathbf{C}(X)\bmod\mathbf{K}(X))\cdot\vec{k}\right)$. При сложении $c_1+c_2=\left(\mathbf{R}_1(X)+\mathbf{R}_2(X)\right)\cdot\mathbf{K}(X)+\mathbf{M}_1+\mathbf{M}_2$ что является правильным шифртекстом суммы $(m_1+m_2)\bmod 2$, поскольку $\left(\mathbf{M}_1+\mathbf{M}_2\right)\cdot\vec{k}=(m_1+m_2)\cdot\vec{k}$. Гомоморфное умножение дает

$$c_1\cdot c_2=\mathbf{R}_1(X)\cdot\mathbf{K}(X)\cdot\mathbf{R}_2(X)\cdot\mathbf{K}(X)+$$
$$+\mathbf{R}_1(X)\cdot\mathbf{K}(X)\cdot\mathbf{M}_2+\mathbf{M}_1\cdot\mathbf{R}_2(X)\cdot\mathbf{K}(X)+\mathbf{M}_1\cdot\mathbf{M}_2=$$
$$=(\mathbf{R}_1(X)\cdot\mathbf{K}(X)\cdot\mathbf{R}_2(X)+\mathbf{R}_1(X)\cdot\mathbf{M}_2+\mathbf{R}_2(X)\cdot\mathbf{M}_1)\cdot\mathbf{K}(X)+$$
$$+\mathbf{M}_1\cdot\mathbf{M}_2,$$

что также является корректным шифртекстом и после расшифрования даёт $(m_1\cdot m_2)\bmod p$, поскольку $(\mathbf{M}_1\cdot\mathbf{M}_2)\cdot\vec{k}=\mathbf{M}_1\cdot(\mathbf{M}_2\cdot\vec{k})=$
$=\mathbf{M}_1\cdot(m_2\cdot\vec{k})=m_2\cdot(\mathbf{M}_1\cdot\vec{k})=m_1\cdot m_2\cdot\vec{k}$.

Рассмотрим теперь вопрос о криптостойкости описанной криптосхемы. В статьях [33] и [34] вводятся два новых сложностных предположения относительно матричных полиномов, а именно.

Определение 4.1. (задача нахождения корней матричных полиномов).

Экземпляр (N,d,n) - задачи нахождения корней матричного полинома состоит в том, чтобы по заданному матричному полиному $\mathbf{F}(X)$ степени d с коэффициентами из матричного кольца $\mathbf{Z}_n^{N\times N}$ ответить на вопрос, есть ли корни у матричного полинома? (распознавательный вариант), и найти эти корни (вычислительный вариант).

Определение 4.2. (задача факторизации матричных полиномов).

Экземпляр (N,d,n,r) -задачи факторизации матричных полиномов состоит в том, чтобы по заданному матричному полиному $\mathbf{F}(X)$ степени d с коэффициентами из матричного кольца $\mathbf{Z}_n^{N\times N}$ ответить на вопрос, возможно ли разложение $\mathbf{F}(X)=\mathbf{F}_{left}(X)\cdot\mathbf{F}_{right}(X)$ такое, что $\deg\left(\mathbf{F}_{right}(X)\right)=r$, и если ответ положительный, то найти все такие $\mathbf{F}_{right}(X)$.

Гипотеза 1. Предполагая сложность задач факторизации матричных полиномов, а также нахождения корней матричных полиномов, вышеприведенная криптосхема является семантически криптостойкой (CPA-криптостойкой).

Вопрос о справедливости этой гипотезы будет освещен в отдельной статье. В случае если эта гипотеза справедлива, взлом криптосхемы равносилен факторизации матричных полиномов или нахождению их корней, а обе задачи выглядят довольно сложными [34].

V. ПРИЛОЖЕНИЯ

Протокол КПИ позволяет клиенту получить интересующую его конфиденциальную информацию из БД, хранящейся на сервере. Предполагается, что клиенту известен индекс нужной ему записи, однако сервер не может распознать, какая именно часть информации стала известна клиенту.

Механизм получения записей из БД может быть представлен так [42]: пусть $d_0,d_1,...,d_n$, $d_i\in\{0,1\}$ – управляющие сигналы, на которые подается номер записи, который нужно извлечь, а $x_0,x_1,...,x_{2^n}$ – информационные сигналы (т.е. в нашем случае все записи БД). Тогда для того, чтобы выбрать один из x_i, подав i в битовом представлении на входы $d_0,d_1,...,d_n$, нужно вычислить следующую функцию:

$$y=f(d_0,...,d_n,x_0,...,x_{2^n})=$$
$$=x_0\cdot((d_0\oplus 1)\,\&\,(d_1\oplus 1)\,\&\,...\,\&\,(d_n\oplus 1))+$$
$$+x_1\cdot(d_0\,\&\,(d_1\oplus 1)\,\&\,...\,\&\,(d_n\oplus 1))+$$
$$+x_2\cdot((d_0\oplus 1)\,\&\,d_1\,\&\,...\,\&\,(d_s\oplus 1))+...$$
$$...+x_{2^n}\cdot(d_0\,\&\,d_1\,\&\,...\,\&\,d_s)\,.$$

Отметим, что здесь x_i не обязательно являются битами. Они могут, например, являться элементами некоторого конечного поля F_q. Поэтому операции $\{+,\cdot\}$ в формуле – это сложение и умножение по модулю q.

Если все x_i зашифрованы с помощью гомоморфной криптосистемы, то $f(d_0,...,d_n,x_0,...,x_{2^n})$ можно вычислить гомоморфно над шифртекстами. Для этого клиенту достаточно зашифровать индексы $d_0,d_1,...,d_n$ нужной ему записи и отправить эти шифровки на сервер. Результат гомоморфного вычисления f над шифровками будет шифровкой запрашиваемого клиентом x_i. Ясно, что для того, чтоб все работало корректно, используемая криптосистема должна поддерживать как гомоморфное сложение, так и умножение.

В [42] также можно найти и другие прикладные протоколы запросов к БД, направленные не только на конфиденциальное получение элемента БД по индексу, но также и конфиденциальное получение самих индексов записей, удовлетворяющих некоторым условиям описываемым, например с помощью стандартных SQL-запросов.

Помимо множества сценариев, в которых выгодно хранить все данные в зашифрованном виде и выполнять вычисления на зашифрованных данных, полностью гомоморфное шифрование используется для решения ряда других проблем в области криптографии. Два таких примера – это проблема проверки делегированных вычислений [43], [44], [45], [46] и проблема построения короткого неинтерактивного доказательства с нулевым разглашением [47]. Некоторые приложения ПГШ не требуют его полную мощность - для КПИ достаточно иметь частично гомоморфные криптосхемы, способные вычислять простые функции индексации базы данных.

VI. ДАЛЬНЕЙШИЕ НАПРАВЛЕНИЯ ИССЛЕДОВАНИЯ

Изучение полностью гомоморфного шифрования привело как к множеству новых и интересных концепций и вопросов, так и мощному инструментарию для их решения. Мы завершаем это ис-

следование, описывая ряд научных направлений, связанных с ПГШ, и в более общем плане, проблему вычислений на зашифрованных данных.

6.1. Открытые вопросы по производительности

В то время как оригинальная конструкция Джентри рассматривалась как непрактичная, последние конструкции и усилия по осуществлению резко улучшили эффективность полностью гомоморфного шифрования. Начальные попытки реализации оригинальной криптосхемы Джентри и её модификаций [48], [49], [50], [51], казалось бы, ясно показывали неотъемлемые «узкие места» эффективности. Однако последующие реализации использовали последние алгоритмические достижения [26], [52], что привело к асимптотически лучшим системам ПГШ, а также новым алгебраическим методам повышения фактической эффективности этих схем [53], [54], [50].

Распространенной практикой для повышения эффективности в последнее время стало так называемое пакетное шифрование [55].

6.2. Открытые вопросы о криптостойкости

Большое значение имеет корректное и полное теоретическое обоснование криптостойкости гомоморфного шифрования на основе матричных полиномов. Стоит отметить, однако, что несмотря на отсутствие такого обоснования для криптосистемы RSA, на протяжении уже почти сорока лет она активно используется.

Для гомоморфных криптосистем имеют большое значение и другие свойства, влияющие на криптостойкость, такие как т.н. нетолерантность (non-malleability). Гомоморфизм и нетолерантность – противоречащие друг другу свойства криптосхемы. Гомоморфные криптосхемы позволяют всем преобразовывать шифртексты сообщения m в шифртекст $f(m)$ для нетривиальной функции f. Нетолерантное шифрование, с другой стороны, предотвращает именно такого рода вещи – оно требует, чтобы криптоаналитик не мог превратить шифртекст m в шифртекст любого «зависимого» сообщения.

На самом деле, то, что нам нужно, это комбинация обоих свойств, которые избирательно позволяют гомоморфные вычисления. А именно, вычислитель должен иметь возможность гомоморфно вычислить любую функцию из некоторого предопределенного класса F_{HOM}, но она не должна быть в состоянии превратить шифртекст m в шифртекст $f(m)$ для любого $f \notin \mathsf{F}_{HOM}$. Таким образом, вопрос: можем ли мы контролировать то, что в настоящее время (гомоморфно) вычисляется?

Формализация этого понятия оказывается сложнее. Боне, Сэджев и Вотерс [56] предлагают понятие целевой толерантности - кандидат формализация такого требования, - а также устройство такой криптосхемы. Их схема шифрования на основе сильного сложностного предположения «Знания типа показателя», и позволяет итерационно вычислять не более t функций, где t – предварительно задаваемая константа. Улучшение их построения, а также лежащие в основе сложностные предположения – важная открытая проблема.

Кроме того, это интересно – распространить определение нетолерантности для атак по выбранному шифртексту. Рассмотрим, например, реализацию зашифрованной системы адресной рекламы, которая генерирует объявления в зависимости от содержания электронной почты пользователя. Поскольку электронная почта хранится в зашифрованном (с помощью ключа пользователя) виде, сервер электронной почты выполняет гомоморфное оценку и вычисляет зашифрованное объявление для отправки обратно пользователю. Пользователь расшифровывает его и выполняет действие в зависимости от того, что он видит.

А именно, если объявление является актуальным, он мог бы нажать нужную кнопку на нем, а в противном случае он будет игнорировать его. Теперь, если сервер электронной почты причастен к этой информации, речь идет о том, нажал пользователь на объявление или нет, появляется возможность использовать это в качестве ограниченного «оракула расшифрования», чтобы взломать криптосхему пользователя и, возможно, даже восстановить его секретный ключ. Такие атаки появляются всякий раз, когда мы вычисляем на зашифрованных данных, так что CCA криптостойкость кажется невозможной. Тем не менее, легко видеть, что криптостойкая против атаки по произвольному шифртексту (CCA2-криптостойкой) гомоморфная криптосхема не может существовать.

Таким образом, нам необходимо соответствующее определение криптостойкости и построения, которые удовлетворяют определению.

Другой важный открытый вопрос относится к криптографическим предположениям, лежащим в основе криптосхем ПГШ. Большинство известных криптосхем ПГШ строятся на основе сложностных предположений теории решеток. Насколько сложны криптографические предположения, связанные с матричными полиномами? Можем ли мы

построить ПГШ на других, возможно, теоретико-числовых предположениях – как насчет сложности факторизации или дискретных логарифмов?

6.3. Связь с функциональным шифрованием

Гомоморфные криптосхемы позволяют всем вычислять функции на зашифрованных данных, но вычисляющий не видит никакой информации о результате. Возможно ли построить схему шифрования, при которой пользователь может вычислить $f(m)$ в открытом виде по шифртексту сообщения m, но не должен узнать никакой другой информации об m (в том числе промежуточные результаты при вычислении f)? Таким образом, вопрос состоит в следующем: «можно ли управлять тем, что вычисляющий может узнать?» Такая криптосхема под названием «функциональная схема шифрования» была впервые введена Сахаем и Вотерсом [57] и изучена в ряде работ ([58], [59], [60], [2] и многих других). Хотя эти построения работают на нескольких интересных семействах функций (таких как монотонные формулы и скалярное произведение) построение универсальной криптосхемы функционального шифрования – открытый вопрос.

В целом, то, что нам нужно, это новый, более широкий взгляд на криптосистемы, которые предоставляют нам точный контроль над тем, что можно узнать о данных, и тем, что можно вычислить над данными.

Научные результаты получены при поддержке Российским фондом фундаментальных исследований инициативного научного проекта 15-07-00597 А «Разработка и исследование алгоритмов полностью гомоморфного шифрования».

Литература

1. W. Diffie and M. Hellman, «New directions in cryptography,» IEEE Transactions on Information Theory, vol. IT-22, pp. 644–654, 1976.
2. R. L. Rivest, A. Shamir, and L. M. Adleman, «A method for obtaining digital signatures and public-key cryptosystems (reprint),» Commun. ACM, vol. 26, no. 1, pp. 96–99, 1983.
3. R. Rivest, L. Adleman, and M. Dertouzos, «On data banks and privacy homomorphisms,» in Foundations of Secure Computation. Academic Press, 1978, pp. 169–177.
4. S. Goldwasser and S. Micali, «Probabilistic encryption,» Journal of Computer and System Sciences, vol. 28, no. 2, pp. 270–299, 1984.
5. T. El-Gamal, «A public key cryptosystem and a signature scheme based on discrete logarithms,» in CRYPTO, 1984, pp. 10–18.
6. P. Paillier, «Public-key cryptosystems based on composite degree residuosity classes,» in EUROCRYPT, 1999, pp. 223–238.
7. I. Damgård and M. Jurik, «A generalisation, a simplification and some applications of Paillier's probabilistic public-key system,» in Public Key Cryptography, 2001, pp. 119–136.
8. M. Ajtai and C. Dwork, «A public-key cryptosystem with worst-case/average-case equivalence,» in STOC, 1997, pp. 284–293.
9. O. Regev, «New lattice-based cryptographic constructions,» J. ACM, vol. 51, no. 6, pp. 899–942, 2004.
10. O. Regev, «On lattices, learning with errors, random linear codes, and cryptography,» in STOC, 2005, pp. 84–93.
11. J. D. Cohen and M. J. Fischer, «A robust and verifiable cryptographically secure election scheme (extended abstract),» in FOCS. IEEE, 1985, pp. 372–382.
12. D. Naccache and J. Stern, «A new public key cryptosystem based on higher residues,» in ACM Conference on Computer and Communications Security, 1998, pp. 59–66.
13. T. Okamoto and S. Uchiyama, «A new public-key cryptosystem as secure as factoring,» in EUROCRYPT, 1998, pp. 308–318.
14. B. Adida, «Helios: Web-based open-audit voting,» in USENIX Security Symposium, 2008, pp. 335–348.
15. C. Peikert and B. Waters, «Lossy trapdoor functions and their applications,» in STOC, 2008, pp. 187–196.
16. D. Boneh, E.-J. Goh, and K. Nissim, «Evaluating 2-DNF formulas on ciphertexts,» in Theory of Cryptography - TCC'05, ser. Lecture Notes in Computer Science, vol. 3378. Springer, 2005, pp. 325–341.
17. C. Gentry, S. Halevi, V. Vaikuntanathan, «A simple BGN-type cryptosystem from LWE,» in EUROCRYPT, 2010, pp. 506–522.
18. T. Sander, A. Young, and M. Yung, «Non-interactive cryptocomputing for NC1,» in FOCS, 1999, pp. 554–567.
19. C. A. Melchor, P. Gaborit, and J. Herranz, «Additively homomorphic encryption with d-operand multiplications,» in CRYPTO, 2010, pp. 138–154.
20. M. Fellows and N. Koblitz, «Combinatorial cryptosystems galore!» Finite Fields: Theory, Applications and Algorithms, pp. 51–61, 1993.
21. E. Kushilevitz and R. Ostrovsky, «Replication is not needed: Single database, computationally-private information retrieval,» in FOCS, 1997, pp. 364–373.
22. B. Chor, E. Kushilevitz, O. Goldreich, and M. Sudan,»Private information retrieval,» J. ACM, vol. 45, no. 6, pp. 965–981, 1998.
23. C. Cachin, S. Micali, and M. Stadler, «Computationally private information retrieval with polylogarithmic communication,» in EUROCRYPT, 1999, pp. 402–414.

24. C. Gentry and Z. Ramzan, «Single-database private information retrieval with constant communication rate,» in ICALP, ser. Lecture Notes in Computer Science, L. Caires, G. F. Italiano, L. Monteiro, C. Palamidessi, and M. Yung, Eds., vol. 3580. Springer, 2005, pp. 803–815.
25. Gentry, «Fully homomorphic encryption using ideal lattices,» in STOC, 2009, pp. 169–178.
26. Brakerski Vaikuntanathan, «Efficient fully homomorphic encryption from (standard) LWE,» in FOCS, 2011, appears in this proceedings. Also available at Cryptology ePrint Archive, Report 2011/344.
27. Y. Ishai and A. Paskin, «Evaluating branching programs on encrypted data,» in TCC, ser. Lecture Notes in Computer Science, S. P. Vadhan, Ed., vol. 4392. Springer, 2007, pp. 575–594.
28. Бабенко, Л. К., Буртыка, Ф. Б., Макаревич, О. Б., Трепачева, А. В. Защищенные вычисления и гомоморфное шифрование. // III Национальный суперкомпьютерный форум (25-27 ноября 2014, г.Переславль-Залесский). ИПС имени А.К. Айламазяна РАН, 2014. URL: http://2014.nscf.ru/TesisAll/4_Systemnoe_i_promezhytochnoe_PO/01_141_ByrtikaFB.pdf
29. Hojsík M., Půlpánová V. A fully homomorphic cryptosystem with approximate perfect secrecy // Topics in Cryptology–CT-RSA 2013. – Springer Berlin Heidelberg, 2013. – С. 375-388.
30. Жиров А. О., Жирова А. О., Кренделев С. Ф. Безопасные облачные вычисления с помощью гомоморфной криптографии // Безопасность информационных технологий. 2013. №. 1. С. 6-12
31. Zhirov A., Zhirova O., Krendelev S. F. Practical fully homomorphic encryption over polynomial quotient rings //Internet Security (WorldCIS), 2013 World Congress on. – IEEE, 2013. – С. 70-75.
32. Ростовцев А., Богданов А., Михайлов М. Метод безопасного вычисления полинома в недоверенной среде с помощью гомоморфизмов колец // Проблемы информационной безопасности. Компьютерные системы. – 2011. – №. 2. – С. 76-85.
33. Burtyka P., Makarevich O. Symmetric Fully Homomorphic Encryption Using Decidable Matrix Equations //Proceedings of the 7th International Conference on Security of Information and Networks. – ACM, 2014. – С. 186.
34. Буртыка Ф.Б. Симметричное полностью гомоморфное шифрование с использованием неприводимых матричных полиномов // Известия Южного федерального университета. Технические науки. – 2014. – Т. 158. – №. 9. – С. 107-122.
35. Пилиди В. С. Криптография. Вводные главы. Ростов-на-Дону: ЮФУ. – 2009.
36. C. Gentry, S. Halevi, and V. Vaikuntanathan, «i-hop homomorphic encryption and rerandomizable yao circuits,» in CRYPTO, ser. Lecture Notes in Computer Science, T. Rabin, Ed., vol. 6223. Springer, 2010, pp. 155–172.
37. Trepacheva A., Babenko L. Known plaintexts attack on polynomial based homomorphic encryption //Proceedings of the 7th International Conference on Security of Information and Networks. – ACM, 2014. – С. 157.
38. Trepacheva A. Cryptanalysis of Polynomial based Homomorphic Encryption // Proceedings of the 7th International Conference on Security of Information and Networks. – ACM, 2014. – С. 205.
39. Трепачева А.В. Криптоанализ гомоморфных криптосистем на основе полиномиальных гомоморфизмов // Известия Южного федерального университета. Технические науки. – 2014. – Т. 158. – №. 9. – С. 31-49.
40. Зарисский О., Самюэль П. Коммутативная алгебра. Т.1. /М.: ИИЛ. 1963. 379 с.
41. Вавилов Н. Конкретная теория колец. Основные понятия. URL: http://www.math.spbu.ru/user/valgebra/col121.html
42. Макаревич О. Б., Буртыка Ф. Б. Защищенная облачная база данных с применением гомоморфной криптографии. – Тез. докл. 6-й Росс. мультиконференции «Информационные технологии в управлении»(ИТУ–2014). СПб, 2014. – С. 567-572.
43. S. Goldwasser, Y. T. Kalai, and G. N. Rothblum, «Delegating computation: interactive proofs for muggles,» in STOC, 2008, pp. 113–122
44. R. Gennaro, C. Gentry, and B. Parno, «Non-interactiveverifiable computing: Outsourcing computation to untrusted workers,» in CRYPTO, 2010, pp. 465–482..
45. K.-M. Chung, Y. T. Kalai, and S. P. Vadhan, «Improved delegation of computation using fully homomorphic encryption,» in CRYPTO, 2010, pp. 483–501.
46. B. Applebaum, Y. Ishai, and E. Kushilevitz, «From secrecy to soundness: Efficient verification via secure computation,» in ICALP (1), 2010, pp. 152–163.
47. Gentry C. A fully homomorphic encryption scheme. PhD. – 2009.
48. N. P. Smart and F. Vercauteren, «Fully homomorphic encryption with relatively small key and ciphertext sizes,» in Public Key Cryptography, ser. Lecture Notes in Computer Science, P. Q. Nguyen and D. Pointcheval, Eds., vol. 6056. Springer, 2010, pp. 420–443.
49. C. Gentry and S. Halevi, «Implementing gentry's fully-homomorphic encryption scheme,» in EUROCRYPT, ser. Lecture Notes in Computer Science, K. G. Paterson, Ed., vol. 6632. Springer, 2011, pp. 129–148.
50. N. Smart and F. Vercauteren, «Fully homomorphic SIMD operations,» Cryptology ePrint Archive, Report 2011/133, 2011, http://eprint.iacr.org/2011/133.
51. J.-S. Coron, A. Mandal, D. Naccache, and M. Tibouchi, «Fully homomorphic encryption over the integers with shorter public keys,» in CRYPTO, 2011, pp. 487–504.
52. Z. Brakerski and V. Vaikuntanathan, « Fully homomorphic encryption from ring-LWE and security for key dependent messages,» in CRYPTO, vol. 6841, 2011, p. 501.
53. K. Lauter, M. Naehrig, and V. Vaikuntanathan, «Can homomorphic encryption be practical?» pre-print available at http://eprint.iacr.org/2011/405.
54. C. Gentry, S. Halevi, and N. Smart, «Personal communication,» 2011.
55. Cheon J. H. et al. Batch Fully Homomorphic Encryption over the Integers //EUROCRYPT. – 2013. – Т. 7881. – С. 315-335.
56. D. Boneh, G. Segev, and B. Waters, «Targeted malleability: Homomorphic encryption for restricted computations,» Cryptology ePrint Archive, Report 2011/311, 2011, http://eprint.iacr.org/2011/311.
57. A. Sahai and B. Waters, «Fuzzy identity-based encryption,» in EUROCRYPT, 2005, pp. 457–473.
58. J. Katz, A. Sahai, and B. Waters, «Predicate encryption supporting disjunctions, polynomial equations, and inner products,» in EUROCRYPT, 2008, pp. 146–162.

59. A. B. Lewko, T. Okamoto, A. Sahai, K. Takashima, and B. Waters, «Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption,» in EUROCRYPT, ser. Lecture Notes in Computer Science, H. Gilbert, Ed., vol. 6110. Springer, 2010, pp. 62–91.
60. S. Agrawal, D. M. Freeman, and V. Vaikuntanathan, «Functional encryption for inner product predicates from learning with errors,» Cryptology ePrint Archive, Report 2011/410, 2011, URL: http://eprint.iacr.org/.

References

1. W. Diffie and M. Hellman, «New directions in cryptography,» IEEE Transactions on Information Theory, vol. IT-22, pp. 644–654, 1976.
2. R. L. Rivest, A. Shamir, and L. M. Adleman, «A method for obtaining digital signatures and public-key cryptosystems (reprint),» Commun. ACM, vol. 26, no. 1, pp. 96–99, 1983.
3. R. Rivest, L. Adleman, and M. Dertouzos, «On data banks and privacy homomorphisms,» in Foundations of Secure Computation. Academic Press, 1978, pp. 169–177.
4. S. Goldwasser and S. Micali, «Probabilistic encryption,» Journal of Computer and System Sciences, vol. 28, no. 2, pp. 270–299, 1984.
5. T. El-Gamal, «A public key cryptosystem and a signature scheme based on discrete logarithms,» in CRYPTO, 1984, pp. 10–18.
6. P. Paillier, «Public-key cryptosystems based on composite degree residuosity classes,» in EUROCRYPT, 1999, pp. 223–238.
7. I. Damgård and M. Jurik, «A generalisation, a simplification and some applications of Paillier's probabilistic public-key system,» in Public Key Cryptography, 2001, pp. 119–136.
8. M. Ajtai and C. Dwork, «A public-key cryptosystem with worst-case/average-case equivalence,» in STOC, 1997, pp. 284–293.
9. O. Regev, «New lattice-based cryptographic constructions,» J. ACM, vol. 51, no. 6, pp. 899–942, 2004.
10. O. Regev, «On lattices, learning with errors, random linear codes, and cryptography,» in STOC, 2005, pp. 84–93.
11. J. D. Cohen and M. J. Fischer, «A robust and verifiable cryptographically secure election scheme (extended abstract),» in FOCS. IEEE, 1985, pp. 372–382.
12. D. Naccache and J. Stern, «A new public key cryptosystem based on higher residues,» in ACM Conference on Computer and Communications Security, 1998, pp. 59–66.
13. T. Okamoto and S. Uchiyama, «A new public-key cryptosystem as secure as factoring,» in EUROCRYPT, 1998, pp. 308–318.
14. B. Adida, «Helios: Web-based open-audit voting,» in USENIX Security Symposium, 2008, pp. 335–348.
15. C. Peikert and B. Waters, «Lossy trapdoor functions and their applications,» in STOC, 2008, pp. 187–196.
16. D. Boneh, E.-J. Goh, and K. Nissim, «Evaluating 2-DNF formulas on ciphertexts,» in Theory of Cryptography - TCC'05, ser. Lecture Notes in Computer Science, vol. 3378. Springer, 2005, pp. 325–341.
17. C. Gentry, S. Halevi, V. Vaikuntanathan, «A simple BGN-type cryptosystem from LWE,» in EUROCRYPT, 2010, pp. 506–522.
18. T. Sander, A. Young, and M. Yung, «Non-interactive cryptocomputing for NC1,» in FOCS, 1999, pp. 554–567.
19. C. A. Melchor, P. Gaborit, and J. Herranz, «Additively homomorphic encryption with d-operand multiplications,» in CRYPTO, 2010, pp. 138–154.
20. M. Fellows and N. Koblitz, «Combinatorial cryptosystems galore!» Finite Fields: Theory, Applications and Algorithms, pp. 51–61, 1993.
21. E. Kushilevitz and R. Ostrovsky, «Replication is not needed: Single database, computationally-private information retrieval,» in FOCS, 1997, pp. 364–373.
22. B. Chor, E. Kushilevitz, O. Goldreich, and M. Sudan, «Private information retrieval,» J. ACM, vol. 45, no. 6, pp. 965–981, 1998.
23. C. Cachin, S. Micali, and M. Stadler, «Computationally private information retrieval with polylogarithmic communication,» in EUROCRYPT, 1999, pp. 402–414.
24. C. Gentry and Z. Ramzan, «Single-database private information retrieval with constant communication rate,» in ICALP, ser. Lecture Notes in Computer Science, L. Caires, G. F. Italiano, L. Monteiro, C. Palamidessi, and M. Yung, Eds., vol. 3580. Springer, 2005, pp. 803–815.
25. Gentry, «Fully homomorphic encryption using ideal lattices,» in STOC, 2009, pp. 169–178.
26. Z. Brakerski, V. Vaikuntanathan, «Efficient fully homomorphic encryption from (standard) LWE», in FOCS, 2011, appears in this proceedings. Also available at Cryptology ePrint Archive, Report 2011/344.
27. Y. Ishai and A. Paskin, «Evaluating branching programs on encrypted data,» in TCC, ser. Lecture Notes in Computer Science, S. P. Vadhan, Ed., vol. 4392. Springer, 2007, pp. 575–594.
28. L. Babenko, Ph. Burtyka, O. Makarevich, A. Trepacheva. Zawiwennye vychislenija i gomomorfnoe shifrovanie [Secure computing and homomorphic encryption]. III National supercomputer forum. November, 25-27 of 2014. (in Russian).
29. Hojsík M., Půlpánová V. A fully homomorphic cryptosystem with approximate perfect secrecy. Proceedings of the 13th international conference on Topics in Cryptology. – Springer-Verlag, 2013. pp. 375-388.
30. O. Zhirov, O. V. Zhirova, and S. F. Krendelev. Bezopasnye oblachnye vychisleniya s pomoshhyu homomorfnoj cryptographii. [Secure cloud computing using homomorphic cryptography]. BIT (bezopasnost' informacionnyx technology) journal [Security of Information Technologies Magazine], 2013, Vol. 1, pp. 6–12. (in Russian).
31. Zhirov A., Zhirova O., Krendelev S. F. Practical fully homomorphic encryption over polynomial quotient rings. Internet Security (WorldCIS), 2013 World Congress on. – IEEE, 2013. pp. 70-75.

32. Rostovtsev A., Bogdanov A., Mikhaylov M. Metod bezopasnogo vychislenija polinoma v nedoverennoj srede s pomowqju gomomorfizmov kolec [Secure evaluation of polynomial using privacy ring homomorphisms]. Problemy informacionnoj bezopasnosti. Kompqjuternye sistemy [Information security issues. Computer systems], 2011. Vol. 2. – pp. 76-85. (in Russian).
33. Ph. Burtyka, O. Makarevich. Symmetric Fully Homomorphic Encryption Using Decidable Matrix Equations. Proceedings of the 7th International Conference on Security of Information and Networks. ACM, 2014, pp. 186–196.
34. F. B. Burtyka. Simmetrichnoe polnost'ju gomomorfnoe shifrovanie s ispol'zovaniem neprivodimyh matrichnyh polinomov [Symmetric fully homomorphic encryption using irreducible matrix polynomials]. Izvestija Juzhnogo federal'nogo universiteta. Tehnicheskie nauki [Proceedings of Southern Federal University. Engineering sciences], 2014, Vol. 158, №. 9, pp. 107-122. (in Russian).
35. V. S. Pilidi. Kriptografija. Vvodnye glavy [Cryptography. Introductory chapters.] Rostov-on-Don: Southern Federal Univesity, 2009. (in Russian).
36. C. Gentry, S. Halevi, and V. Vaikuntanathan, «i-hop homomorphic encryption and rerandomizable Yao circuits,» in CRYPTO, ser. Lecture Notes in Computer Science, T. Rabin, Ed., vol. 6223. Springer, 2010, pp. 155–172.
37. Trepacheva A., Babenko L. Known plaintexts attack on polynomial based homomorphic encryption. Proceedings of the 7th International Conference on Security of Information and Networks. – ACM, 2014. – p. 157.
38. Trepacheva A. Cryptanalysis of Polynomial based Homomorphic Encryption. Proceedings of the 7th International Conference on Security of Information and Networks. – ACM, 2014. – p. 205.
39. Trepacheva A. V. Kriptoanaliz gomomorfnyx kriptosistem na osnove polinomialqnyx gomomorfizmov [Cryptanalisis of cryptosystems based on polynomial rings homomorphisms]. Izvestija Juzhnogo federal'nogo universiteta. Tehnicheskie nauki [Proceedings of Southern Federal University. Engineering sciences], 2014. – Vol. 158. – №. 9. – pp. 31-49. (in Russian).
40. Zariski O., Samuel P., Cohen I. S. Commutative algebra I. – Springer, 1960. – Vol. 1.
41. Vavilov N. Konkretnaja teorija kolec. Osnovnye ponjatija. [Concrete theory of rings. Basic concepts] Preprint [available online at http://www.math.spbu.ru/user/valgebra/col121.html] (in Russian).
42. O. Makarevich, Ph. Burtyka. Zawiwennaja oblachnaja baza dannyx s primeneniem gomomorfnoj kriptografii [Secure cloud database using homomorphic cryptography]. Proceedings of 6th Russian multiconference «Information Technologies in Control» (ITU–2014). SPb, 2014. – pp. 567-572. (in Russian).
43. S. Goldwasser, Y. T. Kalai, and G. N. Rothblum. «Delegating computation: interactive proofs for muggles,» in STOC, 2008, pp. 113–122
44. R. Gennaro, C. Gentry, and B. Parno, «Non-interactiveverifiable computing: Outsourcing computation to untrusted workers,» in CRYPTO, 2010, pp. 465–482.
45. K.-M. Chung, Y. T. Kalai, and S. P. Vadhan, «Improved delegation of computation using fully homomorphic encryption,» in CRYPTO, 2010, pp. 483–501.
46. B. Applebaum, Y. Ishai, and E. Kushilevitz, «From secrecy to soundness: Efficient verification via secure computation,» in ICALP (1), 2010, pp. 152–163.
47. Gentry C. A fully homomorphic encryption scheme. PhD thesis. – 2009.
48. N. P. Smart and F. Vercauteren, «Fully homomorphic encryption with relatively small key and ciphertext sizes,» in Public Key Cryptography, ser. Lecture Notes in Computer Science, P. Q. Nguyen and D. Pointcheval, Eds., vol. 6056. Springer, 2010, pp. 420–443.
49. C. Gentry and S. Halevi, «Implementing gentry's fully-homomorphic encryption scheme,» in EUROCRYPT, ser. Lecture Notes in Computer Science, K. G. Paterson, Ed., vol. 6632. Springer, 2011, pp. 129–148.
50. N. Smart and F. Vercauteren, «Fully homomorphic SIMD operations,» Cryptology ePrint Archive, Report 2011/133, 2011, http://eprint.iacr.org/2011/133.
51. J.-S. Coron, A. Mandal, D. Naccache, and M. Tibouchi, «Fully homomorphic encryption over the integers with shorter public keys,» in CRYPTO, 2011, pp. 487–504.
52. Z. Brakerski and V. Vaikuntanathan, « Fully homomorphic encryption from ring-LWE and security for key dependent messages,» in CRYPTO, vol. 6841, 2011, p. 501.
53. K. Lauter, M. Naehrig, and V. Vaikuntanathan, «Can homomorphic encryption be practical?» [pre-print available at http://eprint.iacr.org/2011/405].
54. C. Gentry, S. Halevi, and N. Smart, «Personal communication,» 2011.
55. Cheon J. H. et al. Batch Fully Homomorphic Encryption over the Integers //EUROCRYPT. – 2013. – T. 7881. – C. 315-335.
56. D. Boneh, G. Segev, and B. Waters, «Targeted malleability: Homomorphic encryption for restricted computations,» Cryptology ePrint Archive, Report 2011/311, 2011, http://eprint.iacr.org/2011/311.
57. A. Sahai and B. Waters, «Fuzzy identity-based encryption,» in EUROCRYPT, 2005, pp. 457–473.
58. J. Katz, A. Sahai, and B. Waters, «Predicate encryption supporting disjunctions, polynomial equations, and inner products,» in EUROCRYPT, 2008, pp. 146–162.
59. A. B. Lewko, T. Okamoto, A. Sahai, K. Takashima, and B. Waters, «Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption,» in EUROCRYPT, ser. Lecture Notes in Computer Science, H. Gilbert, Ed., vol. 6110. Springer, 2010, pp. 62–91.
60. S. Agrawal, D. M. Freeman, and V. Vaikuntanathan, «Functional encryption for inner product predicates from learning with errors,» Cryptology ePrint Archive, Report 2011/410, 2011, http://eprint.iacr.org/.