Пакетное симметричное полностью гомоморфное шифрование на основе матричных полиномов[1]

Ф.Б. Буртыка <bbfilipp@ya.ru>
Южный федеральный университет,
344006, Россия, г. Ростов-на-Дону, ул. Большая Садовая, д. 105/42

Аннотация. Методы полностью гомоморфного шифрования (ПГШ) – общепризнанный способ организации криптографической защиты облачных вычислений. Однако существующие криптосхемы ПГШ по своим характеристикам не достаточны для применения на практике – одни криптосхемы имеют слишком малую криптостойкость, другие требуют слишком больших вычислительных ресурсов. Для развития последних исследователями из IBM был предложен метод «упаковывания шифртекстов», который был применен ими к криптосхеме с открытым ключом, стойкость которой основана на сложности задач теории решеток. В данной работе метод «упаковки шифртекстов» применен к симметричной криптосхеме на основе матричных полиномов: приводится описание возможных способов организации такой упаковки, представлено описание одного из вариантов таких криптосистем с оценкой сложности алгоритма умножения шифртекстов. В заключение приведено сравнение эффективности полученной криптосхемы с криптосхемами исследователей из IBM.

Ключевые слова: защита информации; облачные вычисления; полностью гомоморфное шифрование; «упаковка шифртекстов»; матричные полиномы; вычисления над зашифрованными данными.

1. Введение

В связи с необходимостью борьбы с угрозами безопасности для облачных вычислений актуальна задача построения эффективных и криптостойких методов полностью гомоморфного шифрования (ПГШ) [1-5]. Такое шифрование позволяет производить любые операции с зашифрованными данными и получать зашифрованный результат, который соответствует результату операций, выполняемых с открытыми данными. Задача построения ПГШ впервые была поставлена в работе [1], но принципиально решена лишь в работе Крейга Джентри [2], где было описано построение алгоритмов ПГШ,

[1] Работа выполнена при поддержке гранта РФФИ №15-07-00597 А «Разработка и исследование алгоритмов полностью гомоморфного шифрования»

сложность которых была полиномиальна от размеров входных данных, а задача взлома сводилась к сложным задачам теории решеток. Эта конструкция, однако, имела лишь теоретическое значение из-за низкой *практической* эффективности алгоритмов ПГШ. Вскоре после [2] последовала серия работ, направленных на улучшение исходных алгоритмов ПГШ Джентри [6-13]. Однако ни в одной из этих работ не было предложено решения пригодного для практического использования. Среди альтернатив криптосхемам Джентри можно упомянуть криптосистему с открытым ключом Polly Cracker [18,19] Нила Коблица и симметричные криптосистемы Доминго-Феррера [16], Ростовцева [21], Кренделева [5,14], Пуульпановой и Хойсика [15]. Однако все эти криптосхемы либо еще менее эффективны, чем схема Джентри, либо имеют невысокую криптостойкость [22, 23]. В [24] и [25] были предложены криптосхемы ПГШ на основе матричных полиномов, которые отличаются высокой эффективностью при предположительно значительной криптостойкости.

В данной работе предлагается повысить эффективность ПГШ на основе матричных полиномов [24,25] с помощью метода упаковки в один шифртекст нескольких открытых текстов с последующей «пакетной» обработкой зашифрованных данных. Данный метод впервые был введен в работах Джентри для ускорения работы его конструкций. И несмотря на то, что даже с использованием этого метода криптосистемы типа Джентри не стали пригодными для практики, их эффективность за счет него на порядок увеличилась. Метод «упаковки шифртекстов» является очень перспективным. Поскольку пакетная обработка подразумевает, что при одной операции над двумя шифртекстами происходит одновременное выполнение операций по-координатно над всеми содержащимися в этих шифртекстах открытыми текстами (SIMD организация обработки).

Статья организована следующим образом. В разделе 2 приведены необходимые обозначения, теоретические сведения и определение гомоморфного шифрования. В разделе 3 более подробно описывается метод «упаковки шифртекстов» В разделе 4 показаны различные способы модификации ПГШ на основе матричных полиномов в ПГШ с возможностью «упаковки шифртекстов». В разделе 5 приведены экспериментальные данные по реализации описанных криптосхем на матричных полиномах, а также сравнение по производительности с криптосхемами Джентри, Бракерски и Вэйкунтанасана из работ [8,26].

2. Основные определения и обозначения

Далее в статье множество натуральных чисел будем обозначать как $\mathbf{N}$, кольцо классов вычетов по модулю p будем обозначать как $\mathbf{Z}_p$ (в статье будем использовать только кольца по простому модулю для облегчения доказательств). Прописными греческими буквами (например,) будут обозначаться различные параметры, при этом λ будет всегда обозначать параметр уровня криптостойкости. Матрицы будут обозначаться заглавными латинскими буквами полужирным шрифтом (например, $\mathbf{A}, \mathbf{B}$), при этом единичную матрицу будем обозначать как $\mathbf{I}$. Векторы будут обозначаться прописными латинскими буквами со стрелкой над ними, например . Обозначим через $\mathbf{Z}_p^{N\times N}$ кольцо $N \times N$ матриц с элементами из кольца $\mathbf{Z}_p$. Напомним, что *спектром* матрицы $\mathbf{A}$ (обозначение $Sp(\mathbf{A})$) называется множество собственных векторов матрицы $\mathbf{A}$, т.е. таких векторов $\vec{v}$ для которых $\mathbf{A}\cdot\vec{v} = a\cdot\vec{v}$ при некотором $a \in \mathbf{Z}_p$. Множество матриц коммутирующих с матрицей $\mathbf{A}$ будем называть коммутантом матрицы и обозначать $Comm(\mathbf{A})$. При описании алгоритмов будем использовать запись $x \xleftarrow{\$} X$ для обозначения того, что *x* выбрано случайно по равномерному распределению из конечного множества *X*. Также в статье будет использовано понятие схемы из функциональных элементов (СФЭ), для которой нам будет достаточно знать что это вектор-функция над векторами фиксированной размерности с элементами из $\mathbf{Z}_p$.

2.1 Матричные полиномы

Рассмотрим множество последовательностей матриц из $\mathbf{Z}_p^{N\times N}$:

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

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 $F, G \in \mathbf{Z}_p^{N\times N}[X]$, $G = \{\mathbf{B}_0, \mathbf{B}_1, \mathbf{B}_2, \ldots\}, \mathbf{B}_i \in \mathbf{Z}_p^{N\times N}$, то определим

$$\begin{aligned} &F + G = \{\mathbf{A}_0 + \mathbf{B}_0, \mathbf{A}_1 + \mathbf{B}_1, \mathbf{A}_2 + \mathbf{B}_2, \ldots\}, \\ &F \cdot G = \{\mathbf{A}_0 \cdot \mathbf{B}_0, \mathbf{A}_0 \cdot \mathbf{B}_1 + \mathbf{A}_1 \cdot \mathbf{B}_0, \mathbf{A}_0 \cdot \mathbf{B}_2 + \mathbf{A}_1 \cdot \mathbf{B}_1 + \mathbf{A}_2 \cdot \mathbf{B}_0, \ldots\} = \{\mathbf{C}_k\}, \\ &\quad \text{где } \mathbf{C}_k = \sum\nolimits_{i+j=k} \mathbf{A}_i \cdot \mathbf{B}_j, k = 0, 1, 2, \ldots. \end{aligned} \tag{1}$$

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.*

Лемма 1. *Матричные полиномы образуют (ассоциативное) кольцо.*
Доказательство. Выполняется непосредственной проверкой аксиом кольца.

Приведенный матричный полином – это такой полином, у которого коэффициент при старшей степени равен единичной матрице. Также для дальнейшего важным элементом является *деление матричных полиномов*.

Теорема 1 (О делении матричных полиномов, [29,30]) Пусть $M(X) = X^m + \mathbf{A}_{m-1} \cdot X^{m-1} + \ldots + \mathbf{A}_0$ и $W(X) = X^p + \mathbf{B}_{p-1} \cdot X^{p-1} + \ldots + \mathbf{B}_0$, при $m \geq p$. Тогда существуют единственный приведенный матричный полином *F(X)* степени *m–p* и единственный матричный полином *L(X)* степени *p–1* такие что

$$M(X) = F(X) \cdot X + \mathbf{B}_p \cdot F(X) \cdot X^p + \ldots + \mathbf{B}_1 \cdot F(X) + L(X). \quad (2)$$

Доказательство. Пусть $F(X) = X^{m-p} + \mathbf{F}_{m-p-1} \cdot X^{m-p-1} + \ldots + \mathbf{F}_0$, и $L(X) = X^p + \mathbf{L}_{p-1} \cdot X^{p-1} + \ldots + \mathbf{L}_0$. Приравнивая коэффициенты в равенстве (2), $\mathbf{F}_0, \mathbf{F}_1, \ldots, \mathbf{F}_{m-p-1}$ и $\mathbf{L}_0, \mathbf{L}_1, \ldots, \mathbf{L}_{p-1}$ могут быть определены из полученной системы m матричных уравнений.

Следствие: каждый приведенный матричный полином порождает (левосторонний) идеал в кольце матричных полиномов.

Каждому матричному полиному $\mathbf{P}(X)$ можно естественным образом сопоставить матричное уравнение $\mathbf{P}(X) = \mathbf{0}$. Интересно, что такое матричное уравнение может иметь корней больше, чем его степень [29,30], а может и не иметь корней совсем. В случае если такое уравнение не имеет корней, соответствующий матричный полином будем называть *неприводимым*. Множество корней матричного полинома $\mathbf{P}(X)$ будем обозначать через $roots(\mathbf{P}(X))$. Матричный полином, являющийся одновременно неприводимым и приведенным будем называть *примитивным*.

2.2 Определения гомоморфного шифрования

Общая организация системы защищенных вычислений с помощью симметричного гомоморфного шифрования будет идентична описанной в [25]. Для удобства дальнейшего изложения введем некоторые формальные определения, связанные с такой системой шифрования: гомоморфная криптосхема ε представляет собой четвёрку алгоритмов $(\mathrm{KeyGen}_\varepsilon, \mathrm{Encrypt}_\varepsilon, \mathrm{Decrypt}_\varepsilon, \mathrm{Evaluate}_\varepsilon)$. Вероятностный алгоритм $\mathrm{KeyGen}_\varepsilon$ принимает на вход параметр уровня криптостойкости λ и выдает в качестве результата пару ключей **(sk, rk)**, где **sk** – секретный ключ, который хранится у клиента, а **rk** – ключ перешифрования, передаваемый серверу (он позволяет серверу сокращать размер шифртекстов в процессе вычислений, но не позволяет зашифровывать или расшифровывать). Алгоритмы $\mathrm{Encrypt}_{\varepsilon}$ и $\mathrm{Decrypt}_{\varepsilon}$ принимают на вход, соответственно, шифртекст или открытый текст вместе с секретным ключом **sk**. Алгоритм $\mathrm{Evaluate}_{\varepsilon}$ принимает на вход СФЭ F, набор шифртекстов $\langle m_1, ..., m_t \rangle$, ключ перешифрования **rk**, и выдает в качестве результата шифртекст *c*. Вычислительная сложность всех этих алгоритмов должна быть полиномиальна от параметра уровня криптостойкости λ и (в случае алгоритма $\mathrm{Evaluate}_{\varepsilon}$) количества схемных элементов F, а также они должны удовлетворять приведенным ниже требованиям корректности.

Определение 1. (Корректность расшифрования после гомоморфного вычисления). Криптосхема $\varepsilon = (\mathrm{KeyGen}, \mathrm{Encrypt}, \mathrm{Decrypt}, \mathrm{Evaluate})$ корректна для СФЭ F, имеющей t входов, если для любой пары ключей **(sk, rk)**, выданной алгоритмом $\mathrm{KeyGen}(\lambda)$, любых t открытых текстов m_i и соответствующих им шифртекстов $c_i \leftarrow \mathrm{Encrypt}(\mathbf{sk}, m_i)$ выполняется:

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

Определение 2. Криптосхема $\varepsilon = (\mathrm{KeyGen}, \mathrm{Encrypt}, \mathrm{Decrypt}, \mathrm{Evaluate})$ полностью гомоморфна для класса СФЭ, если она корректна для всех СФЭ из этого класса.

Определение 3. Гомоморфная криптосхема называется *компактной*, если размер шифртекстов, получающихся в результате гомоморфного вычисления произвольной функции f над шифртекстами, не зависит от размера схемы из функциональных элементов, представляющей f, и ограничен полиномом $\beta(\lambda)$.

Замечание: вышеприведенному определению компактности не удовлетворяет, например, криптосистема из [15] или криптосистема с булевыми полиномами [5] поскольку размер шифртекстов в них хотя в общем и ограничен, но это ограничение экпоненциально (не полиномиально).

Системы определений альтернативные вышеприведенной можно найти в [15] и [14], где оно было введено через понятия *открытого и секретного идеалов в кольце*.

3. Гомоморфное шифрование и метод упаковки шифртекстов

Впервые идея проведения векторных (SIMD) операций над зашифрованными данными была высказана в работе Смарта и Веркотерена [6]. В [6] было замечено, что с применением китайской теоремы об остатках, пространство открытых текстов некоторых известных к тому времени криптосхем ПГШ может быть расширено за счет введения векторов, компоненты которых – «ячейки» для отдельных открытых текстов (plaintext slots). При этом одно гомоморфное сложение (Add) или умножение (Mult) пары шифртекстов неявно складывает или умножает (по-компонентно) векторы открытых текстов целиком.

Каждая ячейка для открытого текста предназначается для хранения элемента из какого-то конечного поля $\mathbf{K}_n = \mathrm{F}_{p^n}$, и, абстрактно, если есть два шифртекста, которые хранят (зашифрованные) сообщения $m_0,...,m_{l-1} \in \mathbf{K}_n^l$ и $m'_0,...,m'_{l-1} \in \mathbf{K}_n^l$ соответственно в ячейках $0,...,l-1$ открытого текста, в результате применения l-арного сложения к двум шифртекстам получается новый шифртекст, хранящий $m_0 + m'_0,...,m_{l-1} + m'_{l-1} \in \mathbf{K}_n^l$, а применение l-арного умножения двух шифртекстов дает новый шифртекст, хранящий $m_0 \cdot m'_0,...,m_{l-1} \cdot m'_{l-1} \in \mathbf{K}_n^l$. Смарт и Веркотерен использовали это наблюдение для создания пакетной (или SIMD [12]) системы гомоморфного шифрования.

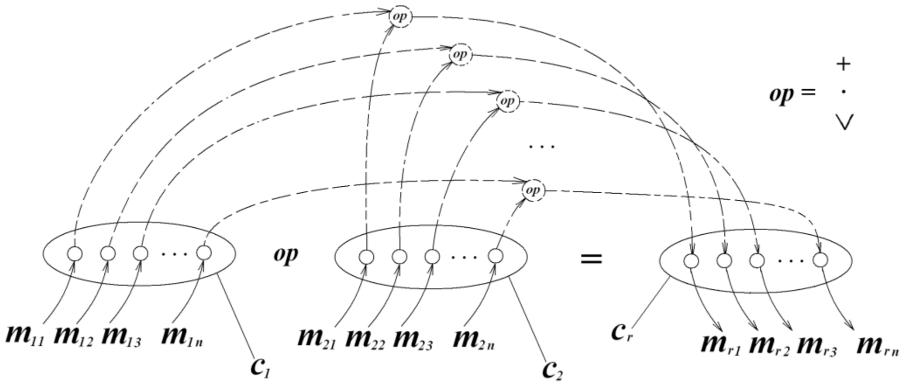

Рис. 1. Выполнение SIMD операций с пакетными шифртекстами.

Говоря о пакетном шифровании и SIMD криптосистемах удобно говорить о составном (Aggregate) пространстве открытых текстов и ключей. Дело в том, что, поскольку над всеми содержащимися в шифртексте открытыми данными производятся параллельно одни и те же операции, можно рассматривать такие наборы открытых данных как единые элементы пространства наборов открытых данных.

Идея пакетного шифрования получила развитие и использование в работах [6-13] благодаря возможности переставлять открытые тексты внутри одного шифртекста без расшифрования. Это открывает большие перспективы гомоморфной обработки данных, в частности делает возможным проведение над зашифрованными числами в битовом представлении стандартных машинных операций таких как Add, Mult, Xor (т.е. сложение, умножение, деление в битовом представлении, побитовое исключающее или и сравнение).

Конкретно, перестановка битов данных между ячейками (слотами, slots) одного шифртекста может быть реализована по-разному, например в [12] для этой цели используется т.н. автоморфизм Фробениуса, а работе [27] описывается использование для этих целей сетей Бенеша.

Пакетное гомоморфное шифрование имеет настолько важное практическое значение, что процедуры для его реализации были включены в недавно вышедшую программную библиотеку HELib компании IBM [28].

4. Построение симметричных гомоморфных SIMD шифров на основе матричных полиномов

Вкратце напомним устройство полностью гомоморфной криптосхемы из [24], основанной на использовании булевых матричных полиномов. Открытыми текстами являются элементы кольца классов вычетов $\mathbf{Z}_p$ по модулю простого числа p, секретный ключ состоит из матрицы $\mathbf{K} \in \mathbf{Z}_p^{N\times N}$ и вектора $\vec{k} \in \mathbf{Z}_p^N$. Открытый текст $m \in \mathbf{Z}_p$ сначала кодируется в матрицу $\mathbf{M} \in \mathbf{Z}_p^{N\times N}$, такую что $\mathbf{M}\cdot\vec{k} = m\cdot\vec{k}$ и $\mathbf{M} \in Comm(\mathbf{K})$, а затем в матричный полином $\mathbf{C}(X) = \mathbf{R}(X)\cdot(X-\mathbf{K})+\mathbf{M}$, где $\mathbf{R}(X)$ – случайный матричный полином. После умножения двух таких шифртекстов результат приводится по модулю матричного полинома вида $\hat{\mathbf{R}}(X)\cdot(X-\mathbf{K})$, называемого ключом перешифрования. Семантическая криптостойкость такого шифра связана с задачей нахождения корней булевых матричных полиномов [29].

Определение 4. (Задача нахождения корней булевого матричного полинома) Экземпляр (N,d,n)-задачи нахождения корней булевого 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 задачи) и найти эти корни (вычислительный вариант задачи).

Применительно к матричным полиномам концепция SIMD может быть реализована как минимум тремя способами:

1) с использованием китайской теоремы об остатках;
2) путем записи в одной матрице нескольких различных собственных значений при различных собственных векторах;
3) с помощью интерполяции матричных полиномов.

Рассмотрим эти концепции по порядку. Использование китайской теоремы об остатках в духе [9] – наиболее перспективный путь, однако он требует построения обширной алгебраической теории. Использование нескольких собственных чисел матрицы – простой, но не очень эффективный путь. Рассмотрим далее реализацию пакетного шифрования с помощью интерполяции матричных полиномов.

Теорема 2 (Об интерполяции матричных полиномов) Для заданных m пар матриц $(\mathbf{X}_i, \mathbf{Y}_i), i=1,\ldots,m$ существует матричный полином

$\mathbf{A}(X) = \mathbf{A}_m \cdot X^m + \mathbf{A}_{m-1} \cdot X^{m-1} + \ldots + \mathbf{A}_1 \cdot X + \mathbf{A}_0$ такой, что

$\mathbf{A}(\mathbf{X}_i) = \mathbf{Y}_i, i=1,\ldots,m$ в случае если блочно-матричная система линейных уравнений

$$\left(\mathbf{A}_1, \mathbf{A}_2, \ldots, \mathbf{A}_m\right) \cdot \begin{pmatrix} \mathbf{I} & \mathbf{I} & \ldots & \mathbf{I} \\ X_1 & X_2 & \ldots & X_m \\ \ldots & \ldots & \ldots & \ldots \\ X_1^{m-1} & X_2^{m-1} & \ldots & \end{pmatrix} = \left(\mathbf{Y}_1, \mathbf{Y}_2, \ldots, \mathbf{Y}_m\right) \tag{3}$$

имеет решение.

В нижеописанной криптосхеме (составным) пространством открытых текстов является $\mathbf{Z}_p^l$ (пространство l-мерных векторов с элементами из $\mathbf{Z}_p$), пространством шифртекстов – $\mathbf{Z}_p^{N\times N}[X]$ (кольцо матричных полиномов), (составным) пространством ключей – вектор пар «матрица из $\mathbf{Z}_p^{N\times N}$, вектор из $\mathbf{Z}_p^N$» вместе с некоторой обратимой матрицей из $\mathbf{Z}_p^{N\times N}$. Опишем далее алгоритмы криптосхемы.

Алгоритм 1. Генерация ключа (KeyGen)

Входные данные: параметр уровня криптостойкости λ, модуль пространства открытых текстов p, количество ячеек l.

Результат: секретный ключ **sk**, ключ перешифрования **rk**.

1. Установить $N \leftarrow \lambda, d \leftarrow \omega(\lambda)$.
2. Выбрать произвольную обратимую матрицу $\mathbf{K}_0 \in GL(N, \mathbf{Z}_p)$.
3. Выбрать l матриц $\mathbf{K}_i, i = 1,\dots,l$, таких, что $\mathbf{K}_i \neq \mathbf{K}_i^2 \neq \dots \neq \mathbf{K}_i^{p-1}$, $\mathbf{I} \in Sp(\mathbf{K}_i)$.
4. Для каждой матрицы $\mathbf{K}_i$ выбрать случайный собственный вектор $\vec{k}_i$.
5. $\mathbf{sk} \leftarrow \{(\mathbf{K}_i, k_i), i = 1,\dots,l\}, \mathbf{K}_0$
6. Сгенерировать случайный приведенный матричный полином $\hat{\mathbf{R}}(X), \deg\left(\hat{\mathbf{R}}(X)\right) \leq d$.
7. Сгенерировать приведенный матричный полином, $\mathbf{S}(X), \deg\left(\mathbf{S}(X)\right) = l+1$ такой что $\mathbf{S}(\mathbf{K}_i) = \mathbf{0}, i = 1,\dots,l$ (т.е. все $\mathbf{K}_i$ – его корни).
8. $\mathbf{R}(X) \leftarrow \hat{\mathbf{R}}(X) \cdot \mathbf{S}(X)$
9. $\mathbf{rk} \leftarrow \mathbf{R}(X - \mathbf{K}_0)$

Замечание 1: Матрицы, удовлетворяющие условию $\mathbf{K}_i \neq \mathbf{K}_i^2 \neq \dots \neq \mathbf{K}_i^{p-1}$ нужны для эффективной генерации матриц из $Comm\left(\mathbf{K}_i\right)$, поскольку известно что линейные комбинации степеней матрицы гарантированно лежат в её коммутанте. В наиболее важном случае $p = 2$ это условие сводится к $\mathbf{K}_i \neq \mathbf{K}_i^2$, такие матрицы называются *неидемпотентными*.

Замечание 2: Наличие единицы в спектре матрицы вместе с предыдущим условием является гарантией возможности выбора из $Comm\left(\mathbf{K}_i\right)$ нетривиальных матриц с произвольными собственными числами.

Замечание 3: Запись $\omega(\lambda)$ обозначает некоторую функцию, линейную от λ (т.е. $\omega(\lambda) = \mathrm{O}(\lambda)$), её конкретизация существенна для анализа криптостойкости, но несущественна для анализа асимптотической сложности вычислений над шифртекстами.

Алгоритм 2. Зашифрование данных (Encrypt)

Входные данные: вектор-сообщение открытых текстов $m_i, i = 1,\ldots,l$, секретный ключ **sk**.

Результат: матричный полином шифртекста.

1. Для каждого $m_i, i = 1,\ldots,l$ выбрать случайную матрицу $\mathbf{M}_i$ такую что m_i будет являться её собственным числом при собственном векторе $\vec{k}_i$.
2. С помощью алгоритма интерполяции матричных многочленов вычислить $\hat{\mathbf{C}}(X)$ такой, что $\deg\left(\hat{\mathbf{C}}(X)\right) \le N + \omega(\lambda)$, $\hat{\mathbf{C}}(\mathbf{K}_i) = \mathbf{M}_i$.
3. Вычислить $\mathbf{C}(X) = \hat{\mathbf{C}}(X - \mathbf{K}_0)$.
4. Вернуть в качестве результата $\mathbf{C}(X)$.

Умножение матричных полиномов в Алгоритме 2 может быть выполнено как по определению (формулам (1)), так и с использованием более эффективных алгоритмов, что будет рассмотрено далее.

Алгоритм 3. Расшифрование (Decrypt)

Входные данные: Матричный полином шифртекста $\mathbf{C}(X)$, секретный ключ **sk**.

Результат: сообщение открытого текста $m \in \mathbf{Z}_p$.

1. $\hat{\mathbf{C}}(X) \leftarrow \mathbf{C}(X - \mathbf{K}_0^{-1})$
2. Для каждого $i = 1,\ldots,l$ выполнить $\mathbf{M}_i \leftarrow \hat{\mathbf{C}}(\mathbf{K}_i)$, для ненулевой координаты $(k_j^{-1})_i$ вектора k_i вычислить $m_i = (k_j^{-1})_i \left(\mathbf{M}_i \cdot \vec{k}_i\right)$**.**
3. Вернуть в качестве результата $\left(m_1,\ldots,m_l\right)$.

Криптосхема поддерживает как аддитивный, так и мультипликативный гомоморфизмы. После умножения двух шифртекстов для понижения степени результат нужно приводить по модулю ключа перешифрования – матричного полинома. Деление можно выполнять, например с помощью алгоритма, указанного в [25].

Корректность расшифрования основывается на обобщенной теореме Безу (для матричных полиномов).

Теорема 2 (Обобщенная теорема Безу) Если S – корень матричного полинома $\mathbf{M}(X)$, то справедливо

$$M(\lambda) = Q(\lambda) \cdot (I\lambda - S),$$

где $Q(\lambda)$ – матричный полином степени $m-1$.

Доказательство теоремы приведено в [30,31] для матричных полиномов над комплексными числами, однако оно справедливо и для матричных полиномов над конечными полями (требование алгебраической замкнутости поля в доказательстве не используется)

Лемма 2 (корректность расшифрования) *Расшифрование вышеописанной криптосхемы корректно и является гомоморфизмом для всех арифметических схем, состоящих из сложений и умножений по модулю* p **.**

Для обоснования корректности расшифрования достаточно заметить, что подстановка полинома указанного вида – изоморфизм колец.

Лемма 3. *Вышеописанная криптосхема компактна.*

Для обоснования этого утверждения достаточно заметить что в процессе вычислений над шифртекстами степень матричных полиномов результата не превысит заданной.

Анализ сложности умножения шифртекстов. Самой значимой характеристикой эффективности ПГШ является анализ сложности алгоритма произведения двух шифртекстов. По соображениям, сходным с описанными в [24] и [25], асимптотическая сложность этой операции составит $\approx O(\lambda^{3.76})$ **.**

Важный вопрос о криптостойкости будет освещен в расширенном варианте статьи, однако стоит отметить, что при выполнении криптоанализа подобного выполненному в работах [24] и [25] видно что вышеописанная криптосхема может иметь достаточно высокую криптостойкость.

5. Результаты экспериментов и сравнение с аналогами

Для оценки производительности полученных криптосистем автором была сделана тестовая реализация вышеописанных алгоритмов с помощью библиотеки NTL в среде программирования Qt Creator 1.3.1. Для тестирования использовался ноутбук с процессором AMD Phenon 1.8 Quad Core 2 с оперативной памятью 4 Гб. При реализации были использованы следующие параметры: открытые тексты выбираются из $\mathbf{Z}_2$, количество открытых текстов на один шифртекст – 11 , степень матричного полинома – 12. Таким образом, на каждый бит открытого текста приходится приблизительно 157 битов шифртекста при 144-битной криптостойкости. Время, необходимое для умножения двух шифртекстов – 50 мсек.

В статье [26] исследователи из IBM Крейг Джентри, Дэн Боне и соавт. представили реализацию криптосхемы из [8] со следующими параметрами: уровень криптостойкости – 128 бит, количество открытых текстов на один шифртекст – 7866, модуль пространства открытых текстов $p = 1000021573$, $\log_2 q = 238$. На каждый бит открытого текста в таком случае приходится приблизительно 218 битов шифртекста. В [32] приводятся следующие данные по производительности: на Intel Core i7-2600 с 3.4 ГГц и более 200 Гб ОЗУ умножение двух шифртекстов при 128 битной криптостойкости выполняется за 148 мсек.

6. Заключение

Были описаны и проанализированы возможные подходы к построению пакетного ПГШ на основе матричных полиномов, а также представлен набор алгоритмов, реализующий один из этих подходов – криптосхему ПГШ с интерполяцией матричных полиномов. Было показано, что по эффективности построенная криптосхема превосходит аналоги, разработанные исследователями из IBM. Более полное описание криптосхем с обоснованием криптостойкости будет приведено в отдельной статье.

Список литературы

[1]. *R. L. Rivest, L. Adleman, M. L. Dertouzos*. On data banks and privacy homomorphisms. *Foundations of secure computation*. 1978, T. 4. №. 11. pp. 169-180.

[2]. *C. Gentry*. Fully homomorphic encryption using ideal lattices. *Proceedings of the 41st annual ACM symposium on Symposium on theory of computing-STOC'09*. Vol. 9 – ACM Press, 2009. pp. 169-169. doi:10.1145/1536414.1536440

[3]. *A. Silverberg*. Fully homomorphic encryption for mathematicians. *Women in Numbers 2: Research Directions in Number Theory*. – 2013. – T. 606. – pp. 111.

[4]. *Н. П. Варновский, А. В. Шокуров*. Гомоморфное шифрование. *Труды ИСП РАН*, том 12, 2007 г. стр. 27-36.

[5]. *А. О. Жиров, О. В. Жирова, С. Ф. Кренделев*. Безопасные облачные вычисления с помощью гомоморфной криптографии. *Журнал БИТ (безопасность информационных технологий)*, том 1, 2013. стр. 6–12.

[6]. *Nigel P. Smart, F. Vercauteren*. Fully Homomorphic Encryption with Relatively Small Key and Ciphertext Sizes. *Public Key Cryptography-PKC 2010: 13th International Conference on Practice and Theory in Public Key Cryptography, Paris, France, May 26-28, 2010, Proceedings*. – Springer, 2010. p. 420.

[7]. *M. Naehrig, K. Lauter, V. Vaikuntanathan*. Can homomorphic encryption be practical? *Proceedings of the 3rd ACM workshop on Cloud computing security workshop. – ACM*, 2011. pp. 113-124. doi: 10.1145/2046660.2046682

[8]. *C. Gentry, S. Halevi, N. P. Smart*. Fully homomorphic encryption with polylog overhead. *Advances in Cryptology–EUROCRYPT 2012. – Springer Berlin Heidelberg*, 2012. pp. 465-482. doi: 10.1007/978-3-642-29011-4_28

[9]. *J. H. Cheon, J. S. Coron, J. Kim, M. S. Lee, T. Lepoint, M. Tibouchi, A. Yun.* Batch Fully Homomorphic Encryption over the Integers. Advances in Cryptology–EUROCRYPT 2013. – T. 7881. – 2013. pp. 315-335. doi: 10.1007/978-3-642-38348-9_20

[10]. *Z. Brakerski, C. Gentry, S. Halevi*. Packed ciphertexts in LWE-based homomorphic encryption. *Public-Key Cryptography–PKC 2013. – Springer Berlin Heidelberg*, 2013. – pp. 1-13. doi: 10.1007/978-3-642-36362-7_1

[11]. *M. Yasuda, T. Shimoyama, J. Kogure, K. Yokoyama, T. Koshiba*. Packed homomorphic encryption based on ideal lattices and its application to biometrics. *Security Engineering and Intelligence Informatics. – Springer Berlin Heidelberg, 2013*. pp. 55-74.

[12]. *Nigel P. Smart, F. Vercauteren*. Fully homomorphic SIMD operations. *Designs, codes and cryptography*, 2014. – Т. 71. – №. 1. – pp. 57-81. doi: 10.1007/s10623-012-9720-4

[13]. *M. Yasuda, T. Shimoyama, J. Kogure, K. Yokoyama, T. Koshiba*. Practical packing method in somewhat homomorphic encryption. *Data Privacy Management and Autonomous Spontaneous Security. – Springer Berlin Heidelberg*, 2014. pp. 34-50.

[14]. *A. Zhirov, O. Zhirova, S. F. Krendelev*. Practical fully homomorphic encryption over polynomial quotient rings. *Internet Security (WorldCIS), 2013 World Congress on. – IEEE*, 2013. pp. 70-75. doi: 10.1109/WorldCIS.2013.6751020

[15]. *M. Hojsík, V. Půlpánová*. A fully homomorphic cryptosystem with approximate perfect secrecy. *Proceedings of the 13th international conference on Topics in Cryptology. – Springer-Verlag*, 2013. pp. 375-388. doi: 10.1007/978-3-642-36095-4_24

[16]. *J. Domingo-Ferrer*. A Provably Secure Additive and Multiplicative Privacy Homomorphism*. *Information Security. – Springer Berlin Heidelberg*, 2002. pp. 471-483.

[17]. *G. Gavin*. An efficient FHE based on the hardness of solving systems of non-linear multivariate equations. *IACR Cryptology ePrint Archive*, 2013. №. 262.

[18]. *M. R. Albrecht, P. Farshim, J. C. Faugere, L. Perret*. Polly cracker, revisited. *Advances in Cryptology–ASIACRYPT 2011. – Springer Berlin Heidelberg*, 2011. pp. 179-196.

[19]. *G. Herold*. Polly cracker, revisited, revisited. *Public Key Cryptography–PKC 2012. – Springer Berlin Heidelberg*, 2012. – pp. 17-33.

[20]. *F. Armknecht, D. Augot, L. Perret, A. R. Sadeghi*. On constructing homomorphic encryption schemes from coding theory. *Cryptography and Coding. – Springer Berlin Heidelberg*, 2011. – pp. 23-40.

[21]. *А. Г. Ростовцев, А. Богданов, М. Михайлов*. Метод безопасного вычисления полинома в недоверенной среде с помощью гомоморфизмов колец. *Проблемы информационной безопасности. Компьютерные системы*, том 2, 2011, стр. 76-85.

[22]. *D. Wagner*. Cryptanalysis of an algebraic privacy homomorphism. *Proc. of 6th Information Security Conference (ISC'03)*. – 2003. doi: 10.1.1.5.1420

[23]. *A. Trepacheva, L. Babenko*. Known plaintexts attack on polynomial based homomorphic encryption. *Proceedings of the 7th International Conference on Security of Information and Networks. – ACM*, 2014. – pp. 157. doi: 10.1145/2659651.2659692

[24]. *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. doi: 10.1145/2659651.2659693

[25]. *Ф. Б. Буртыка*. Симметричное полностью гомоморфное шифрование с использованием неприводимых матричных полиномов. *Известия Южного федерального университета. Технические науки*, том 158, №. 9, стр. 107-122, 2014.

[26]. *D. Boneh, C. Gentry, S. Halevi, F. Wang, D. J. Wu*. Private database queries using somewhat homomorphic encryption. *Applied Cryptography and Network Security. – Springer Berlin Heidelberg*, 2013. – pp. 102-118. doi: 10.1007/978-3-642-38980-1_7

[27]. *S. Halevi, V. Shoup*. Algorithms in HElib. *IACR Cryptology ePrint Archive*, 2014. № 106.

[28]. *S. Halevi*. (2012) Performance of HElib. [Online]. Available: http://mpclounge.files.wordpress.com/2013/04/hespeed.pdf (Дата обращения 18.12.2014)

[29]. *Ф. Б. Буртыка*. О сложности нахождения корней булевых матричных полиномов. *Математическое моделирование*, том 27, 2015. – №. 7.

[30]. *Jr J. E. Dennis, J. F. Traub, R. P. Weber*. The algebraic theory of matrix polynomials. *SIAM Journal on Numerical Analysis*, 13(6), 1976. pp. 831-845.

[31]. *Jr J. E. Dennis, J. F. Traub, R. P. Weber*. Algorithms for solvents of matrix polynomials. *SIAM Journal on Numerical Analysis*, 1978. – T. 15. – №. 3. – pp. 523-533.

[32]. *Antoine Guellier*. Can Homomorphic Cryptography ensure Privacy? [Research Report] RR-8568, 2014, pp.111. https://hal.inria.fr/hal-01052509v1

Batch Symmetric Fully Homomorphic Encryption Using Matrix Polynomials

Ph. Burtyka <bbfilipp@ya.ru>
Southern Federal University,
105/42, Bolshaya Sadovaya st., Rostov-on-Don, 344006, Russia

Abstract. Fully homomorphic encryption (FHE) is a recognized tool to obtain the cryptographic protection of cloud computing. However, the characteristics of existing FHE schemes are not sufficient for use in practice – the security of some FHE is unsatisfying, others require too much computational resources. For improvement the efficiency of the last one IBM researchers proposed a method for "ciphertexts batching", which was applied by them to public key FHE scheme whose security is based on the complexity of the lattice theory hardness assumptions. In this paper, we discuss several methods for embedding "ciphertexts batching" into recently proposed symmetric encryption scheme based on matrix polynomials. For one of this method we completely specify how cryptosystem algorithms should work. The results of computer experiments are given.

Keywords: information security, cloud computing, fully homomorphic encryption, batch encryption, matrix polynomials, secret computations.

References

[1]. *R. L. Rivest, L. Adleman, M. L. Dertouzos*. On data banks and privacy homomorphisms. *Foundations of secure computation*. 1978, Vol. 4, №. 11. pp. 169-180
[2]. *C. Gentry*. Fully homomorphic encryption using ideal lattices. *Proceedings of the 41st annual ACM symposium on Symposium on theory of computing-STOC'09. – ACM Press*, 2009. Vol. 9, pp. 169-169. doi:10.1145/1536414.1536440
[3]. *A. Silverberg*. Fully homomorphic encryption for mathematicians. *Women in Numbers 2: Research Directions in Number Theory*, 2013. Vol. 606. p. 111.
[4]. *N.P. Varnovskij, A.V. Shokurov*. Gomomorfnoe shifrovanie. [Homomorphic encryption]. *Trudy ISP RAN [The Proceedings of ISP RAS]*, 2007. Vol. 12, pp. 27-36. (in Russian).
[5]. *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).
[6]. *Nigel P. Smart, F. Vercauteren*. Fully Homomorphic Encryption with Relatively Small Key and Ciphertext Sizes. *Public Key Cryptography-PKC 2010: 13th International Conference on Practice and Theory in Public Key Cryptography, Paris, France, May 26-28, 2010, Proceedings. – Springer*, 2010. p. 420.

[7]. *Naehrig M., Lauter K., Vaikuntanathan V*. Can homomorphic encryption be practical? *Proceedings of the 3rd ACM workshop on Cloud computing security workshop. – ACM*, 2011. pp. 113-124. doi: 10.1145/2046660.2046682

[8]. *C. Gentry, S. Halevi, N. P. Smart*. Fully homomorphic encryption with polylog overhead. *Advances in Cryptology–EUROCRYPT 2012. – Springer Berlin Heidelberg*, 2012. pp. 465-482. doi: 10.1007/978-3-642-29011-4_28

[9]. *Cheon, J. H., Coron, J. S., Kim, J., Lee, M. S., Lepoint, T., Tibouchi, M., Yun, A*. Batch Fully Homomorphic Encryption over the Integers. *Advances in Cryptology–EUROCRYPT*. – Vol. 7881. – 2013. pp. 315-335. doi: 10.1007/978-3-642-38348-9_20

[10]. *Z. Brakerski, C. Gentry, S. Halevi*. Packed ciphertexts in LWE-based homomorphic encryption. *Public-Key Cryptography–PKC 2013. – Springer Berlin Heidelberg, 2013*. – pp. 1-13. doi: 10.1007/978-3-642-36362-7_1

[11]. *Yasuda, M., Shimoyama, T., Kogure, J., Yokoyama, K., Koshiba, T*. Packed homomorphic encryption based on ideal lattices and its application to biometrics. *Security Engineering and Intelligence Informatics. – Springer Berlin Heidelberg*, 2013. pp. 55-74.

[12]. *Nigel P. Smart, F. Vercauteren*. Fully homomorphic SIMD operations. *Designs, codes and cryptography*, 2014. Vol. 71, №. 1. – pp. 57-81. doi: 10.1007/s10623-012-9720-4

[13]. *Yasuda, M., Shimoyama, T., Kogure, J., Yokoyama, K., Koshiba, T*. Practical packing method in somewhat homomorphic encryption. *Data Privacy Management and Autonomous Spontaneous Security. – Springer Berlin Heidelberg*, 2014. pp. 34-50.

[14]. *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. doi: 10.1109/WorldCIS.2013.6751020

[15]. *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. doi: 10.1007/978-3-642-36095-4_24

[16]. *J. Domingo-Ferrer*. A Provably Secure Additive and Multiplicative Privacy Homomorphism*. *Information Security. – Springer Berlin Heidelberg*, 2002. pp. 471-483.

[17]. *Gavin G*. An efficient FHE based on the hardness of solving systems of non-linear multivariate equations. *IACR Cryptology ePrint Archive*, 2013. №. 262.

[18]. *Albrecht, M. R., Farshim, P., Faugere, J. C., Perret, L*. Polly cracker, revisited. *Advances in Cryptology–ASIACRYPT 2011. – Springer Berlin Heidelberg*, 2011. pp. 179-196.

[19]. *Herold G*. Polly cracker, revisited, revisited. *Public Key Cryptography–PKC 2012. – Springer Berlin Heidelberg*, 2012. – pp. 17-33.

[20]. *Armknecht, F., Augot, D., Perret, L., Sadeghi, A. R*. On constructing homomorphic encryption schemes from coding theory. *Cryptography and Coding. – Springer Berlin Heidelberg*, 2011. – pp. 23-40.

[21]. *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).

[22]. *Wagner D*. Cryptanalysis of an algebraic privacy homomorphism. *Proc. of 6th Information Security Conference (ISC'03)*. – 2003. doi: 10.1.1.5.1420

[23]. *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. – pp. 157. doi: 10.1145/2659651.2659692

[24]. *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. doi: 10.1145/2659651.2659693

[25]. *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).

[26]. *Boneh, D., Gentry, C., Halevi, S., Wang, F., Wu, D. J.* Private database queries using somewhat homomorphic encryption. *Applied Cryptography and Network Security. – Springer Berlin Heidelberg*, 2013. – pp. 102-118. doi: 10.1007/978-3-642-38980-1_7

[27]. *S. Halevi, V. Shoup*. Algorithms in HElib. *IACR Cryptology ePrint Archive*, 2014. №. 106.

[28]. *S. Halevi*. (2012) Performance of HElib. [Online]. Available: http://mpclounge.files.wordpress.com/2013/04/hespeed.pdf (Visited on 18.12.2014)

[29]. *Burtyka Ph. B.* O slozhnosti naxozhdenija kornej bulevyx matrichnyx polinomov [On the complexity of finding the roots of Boolean matrix polynomials]. *Matematicheskoe modelirovanie [Matematical modelling]*, 2015. Vol. 27, №. 7. (in Russian).

[30]. *Dennis, Jr J. E., Traub J. F., Weber R. P*. The algebraic theory of matrix polynomials. *SIAM Journal on Numerical Analysis*, 13(6), 1976. pp. 831-845.

[31]. *Dennis, Jr J. E., Traub J. F., Weber R. P*. Algorithms for solvents of matrix polynomials. *SIAM Journal on Numerical Analysis,* 1978. Vol. 15. – №. 3. – pp. 523-533.

[32]. *Antoine Guellier*. Can Homomorphic Cryptography ensure Privacy? [Research Report] RR-8568, 2014, pp.111. https://hal.inria.fr/hal-01052509v1