МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н.Г. ЧЕРНЫШЕВСКОГО»

Кафедра компьютерной алгебры и теории чисел

Гомоморфное шифрование и облачные вычисления

АВТОРЕФЕРАТ МАГИСТЕРСКОЙ РАБОТЫ

студента 2 курса 227 группы

направления 02.04.01 –Математика и компьютерные науки
код и наименование направления

профиль подготовки: Математические основы компьютерных наук

механико-математического факультета
наименование факультета, института, колледжа

КУЗНЕЦОВА СЕРГЕЯ АЛЕКСАНДРОВИЧА
фамилия, имя, отчество

Научный руководитель
зав.каф., к.ф.-м.н., доцент _____ А.М. Водолазов
должность, уч. степень, уч. звание | подпись, дата | инициалы, фамилия

Зав. кафедрой
зав.каф., к.ф.-м.н., доцент _____ А.М. Водолазов
должность, уч. степень, уч. звание | подпись, дата | инициалы, фамилия

Саратов 2020

ВВЕДЕНИЕ

Актуальность работы. Проблема безопасного хранения и обработки конфиденциальных данных пользователей в удаленных базах данных продолжает оставаться актуальной и в настоящее время. При этом, наука о защите информации - криптография добилась значительного прогресса за последние несколько десятилетий. Данный прогресс обусловлен следующими факторами:

1) С ростом и развитием вычислительной техники, а также её повсеместным использованием в большинстве случаев целью криптографии стала защита компьютерной информации.

2) Современные методы криптографической защиты стали доступны для использования обычными пользователями или организациями для защиты собственных данных, тогда как раньше криптография применялась только в государственных структурах, зачастую являясь засекреченной информацией.

Цель работы.

1) Изучить математическую постановку процесса гомоморфного шифрования с помощью теории p-адических чисел.

2) Привести описание алгоритмов частично и полностью гомоморфного шифрования.

3) Изучить технологию облачных вычислений и рассмотреть вопрос применения гомоморфного шифрования для обеспечения безопасности облачных технологий.

Описание структуры работы.

Магистерская работа состоит из введения, семи разделов, заключения, списка использованных источников, содержащего 24 наименования и приложения. Работа содержит 67 страниц и 1 иллюстрацию.

Краткая характеристика материалов работы. Работа основана на источниках, указанных в списке литературы. В работе произведена реализация гомоморфного шифрования сообщения методами RSA, Эль-Гамаля, а также схемой полностью гомоморфного шифрования Джентри на языке Python версии 3.7.5.

Научная новизна и значимость работы. Научная значимость работы состоит в систематизации сведений об использовании p-адических чисел для описания процесса гомоморфного шифрования.

Положения, выносимые на защиту. На защиту выносятся следующие результаты:

1. Подробные доказательства ряда теорем, необходимых для математической постановки процесса гомоморфного шифрования в случае p-адических чисел.

2. Описание алгоритмов частично и полностью гомомофного шифрования. Приведение примеров основных криптпосистем гомоморфного шифрования.

3. Реализация гомоморфного шифрования сообщений методами RSA, Эль-Гамаля, а также схемой полностью гомоморфного шифрования Дженри.

Основное содержание работы Во введении кратко представлены основные факторы развития науки о защите информации - криптографии. А также, кратко описывается содержание представленной работы.

Раздел 1: Основные понятия p -адического анализа

В данном разделе были представлены основные понятия, связанные с p-адическим анализом, такие как: ряды Ван дер Пута, функции Липшица класса 1, мера Хаара, а также p-адические динамические системы. Данный раздел состоит из пяти параграфов.

В первом введены понятия метрики, метрического пространства и нормы. Примером нормы поля рациональных чисел $\mathbb{Q}$ является абсолютная величина $|x|$, метрика которой представлена в виде $d(x,y) = \parallel x-y \parallel$. Далее определяем на множестве рациональных чисел $\mathbb{Q}$ отображение $|\cdot|_p$ в виде

$$|x|_p = \begin{cases} \frac{1}{p^{ord_p(x)},} & \text{если} \quad x \neq 0 \\ 0, & \text{если} \quad x = 0 \end{cases}$$

где $ord_p(x)$ - p-адический порядок рационального числа $x \in \mathbb{Q}$. Определим поле $\mathbb{Q}_p$ p-адических чисел как пополнение поля $\mathbb{Q}$ по p-адической норме $|\cdot|_p$. Представленное пространство удовлетворяет сильному неравенству тре-

угольника ($|x+y|_p \leq max(|x|_p, |y|_p)$). Элементами $\mathbb{Q}_p$ являются классы эквивалентности последовательностей Коши $\mathbb{Q}$ по p-адической норме. Множество $\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x|_p \leq 1\}$ называется кольцом p-адических целых чисел [1].

Во втором параграфе дано определение левой и правы меры Хаара на топологической группе G, которая является локально-компактной группой. Так как $\mathbb{Q}_p$ является локально-компактной коммутативной группой относительно операции сложения, то на данном поле можно определить меру Хаара.

В третьем параграфе были описаны функции Липшица класса 1. Под данным термином подразумевается выполнение условия $|f(x)-f(y)|_p \leq |x-y|_p$, для всех x, $y \in \mathbb{Z}_p$. Данное условие эквивалентно следующему: Из тождественного равенства $x \equiv y\,(mod\, p^k)$ следует $f(x) \equiv f(y)\,(mod\, p^k)$ для всех $k \geq 1$. Далее была выражена формула координатного представление 1-липшицевых функций. Для вывода данного представления применялось разложение p-адического целого числа (как элемент кольца $\mathbb{Z}_p$) в ряд вида:

$$x = x_0 + px_1 + \ldots + p^k x_k + \ldots, x_j \in \{0, 1, \ldots, p-1\}$$

с последующими обозначениями

$$(x)_k = x_0 + x_1 p + \ldots + x_{k-1} p^{k-1},\ k \geq 1,$$

$$[x]_k = (x_0, x_1, \ldots, x_{k-1}),\ k \geq 1. \tag{1}$$

Далее, была введена функция $\delta_k(x) : \mathbb{Z}_p \to \{0, 1, \ldots, p-1\}$, такая, что $\delta_k(x) = x_k$, где $x \in \mathbb{Z}_p$, $k = 0, 1, 2, \ldots$. Учитывая обозначения, представленные в формуле (1) при $k \geq 0$, были введены следующие функции p-значной логики

$$\varphi_k : \underbrace{\{0, \ldots, p-1\} \times \ldots \times \{0, \ldots, -1\}}_{k+1} \to \{0, \ldots, p-1\},$$

и $\varphi_k : [x]_{k+1} \to \delta_k(f(x))$. В результате преобразований, было получено следующее соотношение

$$f(x) = \sum_{k=0}^{\infty} p^k \varphi_k(x_0, \ldots, x_k) = \varphi_0 + \sum_{k=1}^{\infty} p^k \sum_{a=0}^{p^k-1} I_{[a]_k}([x]_{k-1}) \varphi_{k,[a]_k}(x_k), \qquad (2)$$

где $I_{[a]_k}$ является характеристической функцией, то есть

$$I_{[a]_k}(x_0, \ldots, x_{k-1}) \;=\; \begin{cases} 1, & \text{если } (x_0, \ldots, x_{k-1}) = [a]_k \\ 0, & \text{в противоположном случае} \end{cases}$$

Данное соотношение является координатным представлением 1-липшицевых функций f [2].

В четвертом параграфе были рассмотрены ряды Ван дер Пута, которые определяется следующим образом. Пусть $f : \mathbb{Z}_p \to \mathbb{Z}_p$ - непрерывная функция. Тогда существует единственная последовательность p-адических коэффициентов $B_0, B_1, B_2, \ldots$, такая, что

$$f(x) = \sum_{m=0}^{\infty} B_m \chi(m, x)$$

для всех $x \in \mathbb{Z}_p$. Характеристическая функция $\chi(m, x)$ задается в виде

$$\chi(m, x) \;=\; \begin{cases} 1, & \text{если } |x - m|_p \le p^{-n} \\ 0, & \text{в противоположном случае} \end{cases}$$

где n однозначно определяется неравенством $p^{n-1} \le m \le p^n - 1$.

Связь рядов Ван дер Пута и функций Липшица класса 1 представлена в следующем утверждении. Функция f, представленная через ряд Ван-дер-Пута, является 1-липшицевой тогда и только тогда, когда $|B_m|_p \le p^{-[log_p m]}$ для всех $m \ge 0$. Предполагая, что $B_m = p^{[log_p m]} b_m$, можно определить, что функция f 1-липшицева тогда и только тогда, когда ее можно представить в виде

$$f(x) = \sum_{m=0}^{\infty} B_m \chi(m, x) = p^{[log_p m]}\, b_m \chi(m, x), \qquad (3)$$

где $b_m \in \mathbb{Z}_p$, $m \geq 0$. В результате была получена формула, связывающая функции Липшица класса 1 и ряды Ван дер Пута [2].

В пятом параграфе были описаны критерии сохранения меры для функций Липшица класса 1, которые представлены в следующих теоремах:

Теорема 1. Пусть $f : \mathbb{Z}_p \to \mathbb{Z}_p$ - функция Липшица класса 1, представленная рядом Ван дер Пута (3) сохраняет меру тогда и только тогда, когда

1. $\{b_0, b_1, \ldots, b_{p-1}\}$ устанавливает полный набор вычетов по модулю p, то есть функция $f(x)$ биективна по модулю p,

2. $\{b_{m+p^k}, b_{m+2p^k}, \ldots, b_{m+(p-1)p^k}\}$ для любого $m = 0, \ldots, p^k - 1$ - все ненулевые вычеты по модулю p^k для $k = 2, 3, \ldots$ [2].

Теорема 2. Пусть $f : \mathbb{Z}_p \to \mathbb{Z}_p$ - функция Липшица класса 1 в координатном представлении. Функция f сохраняет меру тогда и только тогда, когда функции φ_0, $\varphi_{k,[a]_k}$, где $a \in \{0, 1, \ldots, p^k - 1\}, k \geq 1$ биективны на множестве $\{0, 1, \ldots, p^k - 1\}$ [2].

Теорема 3. Функция Липшица класса 1 $f : \mathbb{Z}_p \to \mathbb{Z}_p$ сохраняет меру тогда и только тогда, когда $f_k = f \pmod{p^k}$ биективна (по модулю p^k) на $\mathbb{Z}/p^k\mathbb{Z}$ для любого $k = 1, 2, \ldots$ [2].

Раздел 2: Модель шифрования

Второй раздел посвящен p-адической модели шифрования. В данном разделе была рассмотрена автоматная модель шифрования, представленная в виде автомата $\mathfrak{A} = \langle \mathfrak{T}, \mathfrak{S}, \mathfrak{L}, S, L \rangle$, где $\mathfrak{T}$ - конечный набор входных символов (входной алфавит), $\mathfrak{L}$ - конечный набор выходных символов (выходной алфавит), $\mathfrak{S}$ - множество состояний (это множество не обязательно конечно), $S : \mathfrak{T} \times \mathfrak{S} \to \mathfrak{S}$ - функция перехода состояний, $L : \mathfrak{T} \times \mathfrak{S} \to \mathfrak{L}$ - выходная функция. Автомат $\mathfrak{A}$ преобразует входные слова из алфавита $\mathfrak{T}$ в выходные слова из алфавита $\mathfrak{L}$. В данном разделе была доказана следующая теорема, связывающая функцию Липшица класса 1 и функции автоматов [3].

Теорема 4. Функции автоматов являются 1-липшицевыми функциями и наоборот

Функция $f_{\mathfrak{A}(s_0)} : \mathbb{Z}_p \to \mathbb{Z}_p$ автомата $\mathfrak{A}(s_0) = \langle \mathbb{F}_p, \mathfrak{S}, \mathbb{F}_p, S, O, s_0 \rangle$ является 1-липшицевой.

С другой стороны, для любой функции Липшица класса 1 $f : \mathbb{Z}_p \to \mathbb{Z}_p$ существует автомат $\mathfrak{A}(s_0) = \langle \mathbb{F}_p, \mathfrak{S}, \mathbb{F}_p, S, O, s_0 \rangle$ такой, что $f = f_{\mathfrak{A}(s_0)}$.

Раздел 3: Гомоморфные шифры

В третьем разделе был описан процесс гомоморфного шифрования относительно арифметических операций «+», «·» и логических операций «XOR» и «AND» на $\mathbb{Z}_p$. Данный раздел состоит из двух параграфов. В первом параграфе была представлена общая идея гомоморфного (и полностью гомоморфного) шифрования. Во втором параграфе было приведено полное описание 1-липшицевых функций, сохраняющих меру. Рассмотренные функции определяют гомоморфизмы для конкретных операций на $\mathbb{Z}_p$. Данное описание представлено в виде следующих теорем [2].

Теорема 5. (Арифметические операции). Пусть $f : \mathbb{Z}_p \to \mathbb{Z}_p$ функция Липшица класса 1, отличная от нуля и единичных функций. Тогда

1. f определяет гомоморфизм относительно операции «+», то есть

$$f(x + y) = f(x) + f(y), x, y \in \mathbb{Z}_p$$

тогда и только тогда, когда

$$f(x) = Ax, A \in \mathbb{Z}_p,\ A \neq 0.$$

Данная функция сохраняет меру только тогда, когда $A \not\equiv 0\,(mod\, p)$.

2. f определяет гомоморфизм относительно операции «·», то есть

$$f(x \cdot y) = f(x) \cdot f(y),$$

$x, y \in \mathbb{Z}_p$ тогда и только тогда, когда

$$f(x) \;=\; \begin{cases} p^k A^k (t_0^s\,(mod\, p)) \cdot (1 + pt)^a, & \text{если } x = p^k(t_0 + t_p) \\ 0, & \text{если } x = 0 \end{cases} \tag{4}$$

где $t_0 \not\equiv 0\,(mod\, p), t \in \mathbb{Z}_p$, а $A \in \mathbb{Z}_p, s \in \{1, \ldots, p-1\}, k \geq 0$.

Данная функция сохраняет меру тогда и только тогда, когда

$$A \not\equiv 0\,(mod\,p), \quad \text{НОД}(s, p-1) = 1, \quad a \not\equiv 0\,(mod\,p).$$

Теорема 6. (Логические операции). Пусть $f : \mathbb{Z}_p \to \mathbb{Z}_p$ функция Липшица класса 1, определенная в координатной форме

$$f(x) = f(x_0 + \ldots + p^k x_k + \ldots) = \sum_{k=1}^{\infty} p^k \varphi_k(x_0, \ldots, x_k),$$

где $\varphi_k(x_0, \ldots, x_k)$ - p-значные логические функции. Тогда

1. f определяет гомоморфизм относительно операции XOR тогда и только тогда, когда

$$\varphi_k(x_0, \ldots, x_k) = \alpha_0^{(k)} x_0 + \alpha_1^{(k)} x_1 + \ldots + \alpha_k^{(k)} x_k,$$

где $\alpha_i^{(k)} \in \{0, \ldots, -1\}, 0 \le i \le k, k \ge 0$.

Данные функции сохраняют меру тогда, и только тогда, когда

$$\alpha_k^{(k)} \not\equiv 0\,(mod\,p), k \ge 0.$$

2. f определяет гомоморфизм относительно операции AND тогда и только тогда, когда

$$\varphi_k(x_0, \ldots, x_k) = x_0^{s_0^k} \cdot x_1^{s_1^k} \cdots x_k^{s_k^k},$$

где $s_i^{(k)} \in \{0, \ldots, p-1\}, 0 \le i \le k,\ k \ge 0$.

Такие функции сохраняют меру тогда и только тогда, когда

$$f(x) = f(x_0 + px_1 + \ldots + p^k x_k + \ldots) = \sum_{k=0}^{\infty} p^k (x_k^{s_k^k} (mod\,p),$$

где НОД $(s_k^{(k)}, p-1) = 1,\ k \ge 0$.

Раздел 4: Примеры частично гомоморфных шифров

Четвертый раздел состоит из пяти параграфов, в которых представлены примеры различных методов частично гомоморфного шифрования, такие как: RSA, шифры Эль-Гамаля, Пейе, Бенало и Гольдвассера-Микали.

В первом была рассмотрена криптосистема RSA, гомоморфная относительно операции умножения. Во втором параграфе была рассмотрена криптосистема Эль-Гамаля, гомоморфная относительно операции умножения. В третьем параграфе была рассмотрена криптосистема Гольдвассера-Микали, гомоморфная относительно логической операции сложения. В четвертом была описана криптосистема Бенало, являющаяся гомоморфной относительно операции сложения. В пятом параграфе была представлена криптосистема Пейе, гомоморфная относительно сложения.

Раздел 5: Полностью гомоморфные шифры

Пятый раздел посвящен подробному описанию полностью гомоморфного шифрования относительно каждой пары операций из множества («+», «$\cdot$», «XOR», «AND»). Предложение 7 показывает, что таких полностью гомоморфных шифров не существует. Поэтому была рассмотрена следующая проблема. Предположим, что существует гомоморфный шифр относительно операции «$*$». Рассмотрим операцию «+» на $\mathbb{Z}_p$, доказательство которой было описано в теореме 5. Требуется найти новую операцию «G» такую, что этот шифр определяет гомоморфизм относительно новой операции «G». Все возможные новые операции для гомоморфного шифра относительно «+» описаны в предложении 8.

Пусть $H(*)$ - множество всех ненулевых и нетривиальных 1-липшицевых функций, которые определяют гомоморфизм относительно операции «$*$» на $\mathbb{Z}_p$ и сохраняют меру. Для арифметических и логических координатных операций множества

$$H(+), H(\cdot), H(XOR), H(AND) \tag{5}$$

также сохраняют меру. Доказательства описаны в теоремах 5 и 6. Множество функций, состоящее из одинаковой функции $f(x) = x$, обозначается через I.

Предложение 7. Согласно множествам, представленным в (5) выполняются следующие соотношения:

$$1.H(+) \cap H(\cdot) = I;$$
$$2.H(+) \cap H(XOR) = I;$$
$$3.H(+) \cap H(AND) = I;$$
$$4.H(\cdot) \cap H(XOR) = I;$$
$$5.H(\cdot) \cap H(AND) = I;$$
$$6.H(XOR) \cap H(AND) = I;$$

В предложении 8 представлено описание всех операций «G» (определенных степенными рядами), где линейные функции $f(x) = Ax, A \in \mathbb{Z}_p$ определяют гомоморфизм относительно операции «G». Другими словами, f - гомоморфизм относительно сложения и новой операции «G». Установим «G» (функция $G : \mathbb{Z}_p \times \mathbb{Z}_p \to \mathbb{Z}_p$) как сходящийся степенной ряд в $\mathbb{Z}_p \times \mathbb{Z}_p$ (достаточно потребовать, чтобы общий член ряда сходился к нулю в p-адической метрике) [4].

Функция $G(x, y)$ задается сходящимся степенным рядом

$$G(x, y) = c + ax + by + \sum_{k=1}^{\infty} \sum_{i+j=n_k}^{n_k} c_{i,j} x^i y^j, c_{i,j}, a, b, c \in \mathbb{Z}_p, \tag{6}$$

где для любого $n_k \in \{n_1, n_2, \ldots | n_k \in N, 1 < n_1 < n_2 < \ldots\} = N_G$ существует $0 \leq i, j \leq n_k$ такое, что $c_{i,j} = 0$, и если $n \notin N_G$, то $c_{i,j} \neq 0$ для любого $0 \leq i, j \leq n_k, i + j = n$.

Предложение 8. Пусть $f : \mathbb{Z}_p \to \mathbb{Z}_p, f(x) = Ax, A \in \mathbb{Z}_p, A \neq 0$. Функция f определяет гомоморфизм относительно операции «G», заданный в виде ряда (6) тогда и только тогда, когда для $N_G \neq \emptyset$:

$1.c = 0;$

$2.n_k = dq_k + 1, k \geq 1,$ где $d = \text{НОД}(n_1 - 1, n_2 - 1, \ldots, n_k - 1, \ldots), q_k \in N;$

$3.A^d = 1$

и $G = ax + by$ для любого $A \neq 0$ для $N_G = \emptyset$.

Предположим, что в рамках p-адической модели шифрования компьютерная программа реализует формулу исходных данных. Данная формула записывается с использованием набора операций $g_1 : \mathbb{Z}_p \times \mathbb{Z}_p \to \mathbb{Z}_p$ и $g_2 : \mathbb{Z}_p \times \mathbb{Z}_p \to \mathbb{Z}_p$. По аналогии с формулами булевой алгебры определим формулы относительно операций g_1 и g_2 над $\mathbb{Z}_p$:

1. переменные и операции g_1, g_2 являются формулами;

2. если F_1, F_2 - формулы, то $g_1(F_1, F_2), g_2(F_1, F_2)$ - формулы.

Введём обозначение множества всех формул, определенных относительно операций g_1 и g_2, как $[g_1, g_2]$. Например, $x^3 + y + y^2 \cdot z$- это формула из множества [«+», «·»]. Справедливо следующее утверждение.

Предложение 9. Пусть $g_1 : \mathbb{Z}_p \times \mathbb{Z}_p \to \mathbb{Z}_p$ и $g_2 : \mathbb{Z}_p \times \mathbb{Z}_p \to \mathbb{Z}_p$ определяются формулами из [«+», «·»]. Функция Липишица класса 1 $f : \mathbb{Z}_p \to \mathbb{Z}_p$ задает нетривиальный гомоморфизм относительно операций g_1 и g_2.

Тогда $[g_1, g_2] \subset$ [«+», «·»] и $[g_1, g_2] \neq$ [«+», «·»].

В связи с этим предлагается следующий метод с использованием полностью гомоморфного шифрования для обеспечения безопасности удаленных вычислений в рамках обычной модели шифрования.

Пусть $W(d_1, \ldots, d_n)$ - заданная формула (или программа), по которой будут выполняться облачные вычисления. Здесь $d_1, \ldots, d_n \in \mathbb{Z}_p$ обозначает данные. Эта формула может быть дана, например, в основе обычных арифметических операций. Найдем новую пару операций g_1 и g_2, такую что:

1. формула $W \in [g_1, g_1]$;

2. Полностью гомоморфный шифр f_a по операциям g_1 и g_2 существует, где a - ключ, а $[g_1, g_1] \neq$ [«+», «·»].

Тогда $W(f_a(d_1), \ldots, f_a(d_n)) = f_a(W(d_1, \ldots, d_n))$. В результате возможно выполнять облачные вычисления в безопасном режиме для заданной формулы (программы) W [5].

Раздел 6: Схема Джентри полностью гоморфного шифрования

В шестом разделе был рассмотрен предложенный Крейгом Джентри алгоритм на примере шифрования текста на множестве $\mathbb{Z}_2$. В результате было замечено, что существенным недостатком данной схемы является накопление ошибки при выполнении вычислений. После того как накопленное значение

превышает p, расшифровать сообщение становится невозможным. Одним из вариантов решения данной проблемы является перешифровка данных после некоторого количества операций, однако такой вариант снижает производительность вычислений и требует постоянного доступа к секретному ключу [6].

Раздел 7: Общие сведения об облачных вычислениях

В седьмом разделе были описаны общие сведения об облачных вычислениях. В данном разделе представлено определение облачных вычислений, а также указаны некоторые сведения об истории их создания. Раздел состоит из трех параграфов. В первом была приведена классификация моделей облачных вычислений, в которую входят следующие модели: Инфраструктура как сервис (IaaS), Платформа как сервис (PaaS), Программное обеспечение как сервис (SaaS) [7].

Во втором параграфе была представлена классификация моделей развертывания облачных систем. В данную классификацию входят: Общедоступные (публичные) облака (Public cloud), Частные (корпоративные) облака (Private cloud), Облако сообщества (Community cloud), Гибридное облако (Hybrid cloud) [7].

В третьем параграфе была подробно описана актуальность безопасности облачных вычислений. В результате, наиболее надёжным методом для безопасности облачных вычислений является гомоморфное шифрование, особенность которого в том, что оно позволяет производить определённые математические действия с зашифрованным текстом и получать зашифрованный результат, который соответствует результату операций, выполняемых с открытым текстом [8].

ЗАКЛЮЧЕНИЕ

В результате было рассмотрено описание гомоморфных шифров для p-адической модели шифрования относительно арифметических («+» и «·») и логических операций («XOR» и «AND»), а также приведено описание общего вида гомоморфного шифрования. В ходе работы были подробно рассмотрены функции Липшица класса 1, ряды Ван дер Пута, мера Хаара, а также динамические p-адические системы, необходимые для описания заданного набора операций.В качестве примера гомоморфного шифрования были

рассмотрены примеры наиболее распространённых частично гомоморфных шифров: RSA, шифры Эль-Гамаля, Пейе, Бенало и Гольдвассера-Микали, а также алгоритм плоного гомоморфного шифрования Джентри. Также в работе были представлены общие сведения об облачных вычислениях, приведены классификации моделей облаков по различным критериям, а также был рассмотрен вопрос безопасности облачных вычислений. В результате, были сформулированы требования к облачному сервису, которым удовлетворяет гомоморфное шифрование. Но ввиду отсутствия практической реализации алгоритма полностью гомоморфного шифрования Крейга Джентри, данный вопрос по-прежнему остаётся актуальным и в настоящее время.