A.V. Epishkina, A.N. Gerasimov
National Research Nuclear University MEPhI,31, Kashirskoe sh., Moscow, 114509, Russian Federation
e-mail: AVEpishkina@mephi.ru, ORCID iD is 0000-0001-7681-0382;e-mail: Gerasimov625@gmail.com, ORCID iD is 0000-0002-6642-2391

Systematization and analysis of partially and fully homomorphic cryptosystem

Keywords: cryptography, homomorphic encryption, cloud computing
In this article provides an overview of the known partially and fully homomorphic cryptosystem, such as: RSA, ElGamal, Paillier, Gentry and Halevi. Justified the homomorphic properties of the considered cryptosystems. The comparative analysis of the homomorphic encryption algorithms has been committed

А.В. Епишкина, А.Н. Герасимов
Национальный исследовательский ядерный университет «МИФИ», Каширское шоссе,31,г. Москва, 115409, Россия,
e-mail: AVEpishkina@mephi.ru, ORCID iD is 0000-0001-7681-0382;e-mail: Gerasimov625@gmail.com, ORCID iD is 0000-0002-6642-2391

СИСТЕМАТИЗАЦИЯ И АНАЛИЗ ЧАСТИЧНО И ПОЛНОСТЬЮ ГОМОМОРФНЫХ КРИПТОСИСТЕМ

Ключевые слова: криптография, гомоморфное шифрование, облачные вычисления
В статье представлен обзор известных частично и полностью гомоморфных криптосистем, таких как: RSA, Пэйе Эль-Гамаля, Джентри и Галеви. Обоснованы гомоморфные свойства рассмотренных криптосистем. Проведен сопоставительный анализ особенностей применения алгоритмов гомоморфного шифрования.

Введение

В настоящее время облачные вычисления являются одной из самых востребованных на текущий период технологий на рынке информационных услуг. Основной причиной такого развития является возможность для компаний и частных лиц снижения расходов на поддержание собственной ИТ-инфраструктуры за счет передачи этой работы провайдеру облачного сервиса. Однако в такой ситуации становятся небезопасными хранение и обработка конфиденциальных данных в облачной инфраструктуре.

Решением этой проблемы может служить шифрование всех конфиденциальных данных с помощью гомоморфной схемы шифрования, позволяющей проводить вычисления над зашифрованными данными без их расшифрования. Таким образом, поставщик облачных услуг выполняет требуемые операции при сохранении конфиденциальности данных клиента.

Впервые такая задача была поставлена в работе «Банки данных и секретные гомоморфизмы» [1] Ривестом (Rivest), Шамиром (Shamir) и Адлеманом (Adleman) — создателями криптосистемы RSA. Уже сама криптосистема RSA обеспечивала мультипликативный гомоморфизм. Особый же интерес представляют алгоритмы полностью гомоморфного шифрования, то есть шифрования, позволяющего проводить над шифртекстами любые необходимые вычисления. Принципиальную возможность такого шифрования доказал исследователь из IBM Крейг Джентри (Craig Gentry) в своей диссертации в 2009 году [2].

Помимо облачных вычислений, гомоморфное шифрование также находит применение в поисковых системах, в системах электронного голосования, в частности, при применении подписи вслепую.

Несмотря на множество исследований в данной области, многие основные проблемы остаются нерешёнными. В связи с этим становится актуальна задача построения

эффективных и криптографически стойких алгоритмов полностью гомоморфного шифрования, требующих меньших вычислительных ресурсов.

Систематизация известных схем гомоморфных криптосистем

Полностью гомоморфные схемы шифрование позволяют выполнять арифметические операции над зашифрованными данными без их предварительного расшифровывания. Частично гомоморфные криптосистемы обладают свойством гомоморфности относительно только одной операции, например, сложения или умножения.

Криптосистема RSA

Криптосистема RSA обладает мультипликативным гомоморфизмом. Для любых открытых текстов $m_1, m_2 \in Z_n$ и открытого ключа (e,n) выполняется равенство:

$$\begin{aligned} E_{(e,n)}(m_1)\cdot E_{(e,n)}(m_2) &= m_1^e \bmod n \cdot m_2^e \bmod n = \\ &= (m_1 \cdot m_2)^e \bmod n = E_{(e,n)}(m_1 \cdot m_2). \end{aligned} \quad (1)$$

Криптосистема Пэйе [3] обладает следующим гомоморфным свойством: для любых открытых текстов m_1 и m_2, открытого ключа (n,g) выполняется:

$$\begin{aligned} E_{(n,g)}(m_1)\cdot E_{(n,g)}(m_2) &= \left(\left(g^{m_1}\cdot r_1^n\right)\cdot\left(g^{m_2}\cdot r_2^n\right)\right)\bmod n^2 = \\ &= \left(g^{m_1+m_2}\cdot(r_1\cdot r_2)^n\right)\bmod n^2 = E_{(n,g)}(m_1+m_2). \end{aligned} \quad (2)$$

Криптосистема Эль-Гамаля [4] обладает мультипликативным гомоморфизмом. Для любых открытых текстов m_1, m_2 и открытого ключа (p,g,y) выполняется:

$$\begin{aligned} E_{(p,g,y)}(m_1)\cdot E_{(p,g,y)}(m_2) &= \left(\left(g^{k_1}\cdot g^{k_2} \bmod p\right),\left(m_1\cdot y^{k_1}\cdot m_2\cdot y^{k_2} \bmod p\right)\right) = \\ &= \left(\left(g^{k_1+k_2} \bmod p\right),\left(m_1\cdot m_2\cdot y^{k_1+k_2} \bmod p\right)\right) = E_{(p,g,y)}(m_1\cdot m_2). \end{aligned} \quad (3)$$

Симметричная гомоморфная криптосистема над целыми числами [5] обладает аддитивным и мультипликативным гомоморфизмом. Шифрование одного бита определяется формулой 4.

$$E(m) = m' + pq = c. \quad (4)$$

Расшифровывание определяется формулой 5:

$$D(c) = (c \bmod p) \bmod 2 = m. \quad (5)$$

Для любых $m_1, m_2 \in \{0,1\}$, ключа p выполнено:

$$\begin{aligned} &E(m_1)+E(m_2) = c_1 + c_2 = \\ &= (m'_1 + m'_2) + p(q_1+q_2) = 2(r_1+r_2) + (m_1+m_2) + p(q_1+q_2) = E(m_1 + .m_2) \end{aligned} \quad (6)$$

$$\begin{aligned} Encryption(m_1)\cdot Encryption(m_2) = c_1\cdot c_2 = (m'_1+pq_1)\cdot(m'_2+pq_2) = \\ = m'_1\,m'_2+m'_1\,pq_2+m'_2\,pq_1+p^2q_1q_2 = \\ = (2r_1+m_1)(2r_2+m_2)+m'_1\,pq_2+m'_2\,pq_1+p^2q_1q_2 = \\ = m_1m_2+2(m_1r_2+m_2r_1+2r_1r_2)+p(m'_1\,q_2+m'_2\,q_1+pq_1q_2) = E(m_1\cdot m_2). \end{aligned} \quad (7)$$

Шифрование для чисел из Z_2

В основе данной схемы [6] лежит гомоморфизм колец полиномов от нескольких переменных над Z_2 . Схема обладает аддитивным и мультипликативным гомоморфизмом

Рассмотрим числа $a_0, b_0 \in Z_2$, построим полином $a(x_1,\ldots,x_n)$ и $b(x_1,\ldots,x_n)$ от n переменных, в которых a_0 и b_0 соответственно являются свободными членами. При умножении полиномов $a(x_1,\ldots,x_n)$ и $b(x_1,\ldots,x_n)$ свободный член равен a_0b_0 при сложении полиномов $a(x_1,\ldots,x_n)$ и $b(x_1,\ldots,x_n)$ свободный член равен a_0+b_0 .

Для построения гомоморфизма используется взаимно – однозначная замена переменных:

$$\begin{cases} y_1 = f_1(x_1,\ldots,x_n), \\ y_2 = f_2(x_1,\ldots,x_n), \\ \quad\ldots \\ y_n = f_n(x_1,\ldots,x_n). \end{cases} \quad (8)$$

Для построения таких замен переменных используется интерполяционный многочлен Лагранжа. Взаимная однозначность замены переменных обеспечивает возможность построения обратной замены и корректного расшифрования данных.

В таблице 1 приведено сравнение рассмотренных гомоморфных схем шифрования.

Таблица 1 — Сравнение гомоморфных схем шифрования

Криптосистема	Стойкость и преимущества криптосистемы	Недостатки криптосистемы
RSA	Стойкость основана на задаче факторизации больших чисел. Алгоритм может использоваться совместно с алгоритмом OAEP. Криптосистема обладает мультипликативным гомоморфизмом.	Для обеспечения криптостойкости необходимо использовать размер ключа больше, чем 1024 бит. Существует множество атак на алгоритм – атака на основе выбранного шифртекста, цифровая подпись уязвима к мультипликативной атаке.
Пэйе	Стойкость основана на задаче факторизации больших чисел. Гомоморфные свойства криптосистемы используются в системах электронного голосования.	Размер шифртекста примерно в два раза больше размера открытого текста. Осуществима атака на основе адаптивно подобранного открытого текста.

Эль-Гамаля	Стойкость основана на трудоемкости вычисления дискретных логарифмов. Алгоритм является вероятностным. Криптосистема обладает мультипликативным гомоморфизмом.	Существует множество атак на алгоритм – атака на основе выбранного шифртекста, возможна атака «человек посередине».
Джентри и Галеви	Меняя параметр λ, можно управлять соотношением между производительностью и криптостойкостью. Возможен метод самокоррекции шифртекстов, сжатия открытого ключа, модульного переключения. Базовая схема, на которой построены многие полностью гомоморфные схемы шифрования. Криптосистема обладает аддитивным и мультипликативным гомоморфизмом	Высокая вычислительная сложность алгоритмов шифрования и расшифрования. Присутствует «шум» в шифртексте. При применении операции сложения или умножения размер шифртекста увеличивается. Размер шифртекста увеличивается при использовании метода самокоррекции.
Схема шифрования для чисел из множества Z_2	Неограниченное количество применений операций сложения и умножения. Отсутствие «шума». Криптосистема обладает аддитивным и мультипликативным гомоморфизмом	Высокая вычислительная сложность алгоритмов шифрования и расшифрования.

Заключение

В процессе выполнения работы были получены следующие основные результаты:

- анализ гомоморфных свойств известных криптосистем, таких как RSA, Гольдвассер-Микали, Бенало, Пэйе, Эль-Гамаля, включающий выявление особенностей генерации ключей, функции шифрования и расшифрования;
- систематизация схем полностью гомоморфного шифрования
- обоснование гомоморфных свойств рассмотренных криптосистем;
- сопоставительный анализ особенностей применения алгоритмов гомоморфного шифрования.

Результаты работы являются значимыми как в практическом, так и в научном плане, поскольку могут быть использованы для дальнейшего исследования полностью гомоморфных криптосистем с целью усовершенствования алгоритмов гомоморфного шифрования.

СПИСОК ЛИТЕРАТУРЫ:

1. R. L. Rivest, L. Adleman, M. L. Dertouzos. On data banks and privacy homomorphism // Foundations of secure computation. — 1978. — 169-180 p.
2. C. Gentry. Fully homomorphic encryption using ideal lattices // Annual ACM Symposium on Theory of Computing. — 2009. — 182-194 p.
3. Pascal Paillier. Public-key cryptosystems based on composite degree residuosityclasses. // EUROCRYPT 1999. — 1999. — 223-238 p
4. T. ElGamal. A public-key cryptosystem and a signature scheme based on discrete logarithms // CRYPTO 1984. — 1984. — 10-18 p.
5. M. van Dijk, C. Gentry, S. Halevi and V. Vaikuntanathan. Fully homomorphic encryption over the integers // EUROCRYPT 2012. — 2012. — 502-519 p.
6. А.О.Жиров, О.В.Жирова, С.Ф. Кренделев, Безопасные облачные вычисления с помощью гомоморфной криптографии // журнал БИТ: безопасность информационных технологий. — 2013. — 6-12 с

REFERENCES:

1. R. L. Rivest, L. Adleman, M. L. Dertouzos. On data banks and privacy homomorphism // Foundations of secure computation. — 1978. — 169-180 p.
2. C. Gentry. Fully homomorphic encryption using ideal lattices // Annual ACM Symposium on Theory of Computing. — 2009. — 182-194 p.
3. Pascal Paillier. Public-key cryptosystems based on composite degree residuosityclasses. // EUROCRYPT 1999. — 1999. — 223-238 p
4. T. ElGamal. A public-key cryptosystem and a signature scheme based on discrete logarithms // CRYPTO 1984. — 1984. — 10-18 p.
5. M. van Dijk, C. Gentry, S. Halevi and V. Vaikuntanathan. Fully homomorphic encryption over the integers // EUROCRYPT 2012. — 2012. — 502-519 p.
6. A.O.ZHirov, O.V.ZHirova, S.F. Krendelev, Bezopasnye oblachnye vychisleniya s pomoshchyu gomomorfnoj kriptografii // zhurnal BIT: bezopasnost informacionnyh tekhnologij. — 2013. — 6-12p