ISSN 2225-9309 (Print)
2024. № 2 (31). С. 10–15
Молодежный Вестник УГАТУ
http://journal.ugatu.su

УДК 004.056.55

ГОМОМОРФНОЕ ШИФРОВАНИЕ В ЗАЩИТЕ ИНФОРМАЦИИ

Т.Б. БАЛГАЗИН

[1] Tagir.balgazin@yandex.ru

ФГБОУ ВО «Уфимский университет науки и технологий» (УУНиТ)

Аннотация. В данной работе рассмотрены способы и алгоритмы гомоморфного шифрования. Было создано прикладное программное обеспечение, реализующее криптосистему Пайе, обладающую гомоморфными свойствами, была произведена проверка гомоморфных свойств данной системы.

Ключевые слова: гомоморфизм, криптосистема, алгоритм, шифрование, ключ.

ВВЕДЕНИЕ

Данная статья посвящена исследованию гомоморфного шифрования, а также его возможных приложений в сфере информационной безопасности. Обладающие свойством гомоморфизма алгоритмы шифрования подразумевают возможность произведения определенных видов математических операций над зашифрованными данными с сохранением корректности результата данных операций. Представленное в статье исследование является актуальным, поскольку данный метод шифрования позволяет проводить обработку данных без предварительной расшифровки, что существенно повышает безопасность информационной системы (поскольку нет необходимости передавать не только закрытый, но даже открытый ключ), что открывает широкие возможности, к примеру возможность работы с конфиденциальной информацией, используя сторонние вычислительные ресурсы, возможность использования зашифрованных данных в качестве обучающей выборки для алгоритмов машинного обучения и так далее.

В процессе анализа данной научной области в открытых источниках не было найдено ни одной реализации криптосистемы Пайе в виде прикладного ПО, что позволяет сделать выводы об отсутствии аналогов предложенному в статье прикладному программному обеспечению (ПО). Разработанное прикладное ПО дает возможность быстро и удобно использовать криптосистему Пайе через оконный интерфейс, что позволяет использовать её непрофильным специалистам, также существует возможность адаптации разработанной программы для её использования в качестве серверного ПО для работы с большими объемами информации.

Под гомоморфным шифрованием (ГШ) понимается технология, позволяющая производить вычисления над зашифрованными данными без необходимости их предварительного расшифровывания. Гомоморфизм – это соответствие между алгебраическими системами, сохраняющее все основные отношения и операции, при котором каждому элементу первой системы соответствует ровно один элемент второй системы.

ОСНОВНЫЕ ТИПЫ ГОМОМОРФНОГО ШИФРОВАНИЯ

Методы гомоморфного шифрования можно разделить на следующие типы:

1) Полностью гомоморфное шифрование (Fully Homomorphic Encryption, FHE). Данный тип шифрования подразумевает возможность выполнять широкий спектр математических операций над зашифрованными данными неограниченное количество раз, что обеспечивает высочайший уровень безопасности и конфиденциальности, поскольку данные могут оставаться зашифрованными на протяжении всего процесса вычислений, однако алгоритмы полностью гомоморфного шифрования обладают высокой вычислительной сложностью, что

существенно понижает производительность информационных систем, использующих данный тип шифрования.

2) Гомоморфное шифрование с ограниченной полнотой (Somewhat Homomorphic Encryption, SHE). Данный тип шифрования позволяет выполнять ограниченное количество математических операций (обычно сложение и умножение) над зашифрованными данными до накопления определенного уровня шума.

3) Частичное гомоморфное шифрование (Partial Homomorphic Encryption). Данный тип шифрования подразумевает возможность выполнять только один тип операции над зашифрованными данными, например, сложение или умножение. Шифрование такого типа осуществляют такие распространенные алгоритмы, как RSA, Криптосистема Голдвассера-Микали, Криптосистема Эль-Гамаля, криптосистема Пайе.

На практике наиболее распространенными являются частично гомоморфные шифры, допускающие либо сложение, либо умножение, поскольку они обладают более низкой вычислительной сложностью, а также более просты в реализации.

КРИПТОСИСТЕМА ПАЙЕ (PAILLIER'S CRYPTOSYSTEM)

Криптосистема Пайе (Paillier's cryptosystem) — это асимметричная криптосистема с открытым ключом, разработанная Паскалем Пайе в 1999 году. Она основана на вычислительной сложности задачи факторизации составного числа, являющегося произведением двух простых чисел. Одной из отличительных черт данной системы является возможность выполнения гомоморфных операций сложения над зашифрованными данными.

Процесс шифрования и дешифрования в данной криптосистеме выглядит следующим образом:

1) генерация ключей:
   а) выбираем два простых числа p и q;
   б) вычисляем произведение этих числе n = p * q;
   в) вычисляем $\lambda = \mathrm{lcm}(p-1, q-1)$, где lcm – наименьшее общее кратное;
   г) выбираем случайное число g, такое, что $g \in z_{n^2}^*$;
   д) вычисляем μ:

$$\mu = \left(L\left(g^{\lambda} \bmod n^2\right)\right)^{-1} \bmod n,$$

где: $L(u) = div\left(\frac{u-1}{n}\right)$, div – целочисленное деление;

   е) открытым ключом является пара (n, g), закрытым – (λ, μ);

2) шифрование:
   а) пусть m будет шифруемым сообщением, где $m \in z_n$;
   б) выбор случайного числа r, $r \in z_n^*$;
   в) вычисление шифротекста c:

$$c = g^n * r^n \bmod n^2;$$

3) расшифровка:
   а) Принимаем зашифрованное сообщение $c \in z_{n^2}^*$, открытый (n, g) и закрытый (λ, μ) ключи;
   б) Вычисляем исходное сообщение по формуле:

$$m = \left(L\left(c^{\lambda} \bmod n^2\right) * \mu\right) \bmod n$$

Данный способ шифрования обладает гомоморфизмом по сложению: произведение двух зашифрованных чисел по модулю n^2, где n – первая часть открытого ключа будет равно зашифрованной с теми же ключами сумме изначальных чисел:

$$(c_1 * c_2) \bmod (n^2) = c_3,$$

где c_1 – зашифрованное число m_1, c_2 – зашифрованное число m_2, а c_3 – зашифрованное число $m_3 = m_1 + m_2$.

Для того, чтобы проверить данное свойство криптосистемы был реализован предложенный алгоритм при помощи языка программирования Python и библиотеки Tkinter (для работы с окном) в виде оконного прикладного программного обеспечения. Проверка данного свойства является актуальной, поскольку наличие свойства гомоморфности криптосистемы открывает широкие возможности в области работы с зашифрованными данными, в частности для их использования в качестве обучающей выборки для алгоритмов машинного обучения, проведения определенных вычислений над ними.

ПРАКТИЧЕСКАЯ ЧАСТЬ

В данной работе было разработано прикладное программное обеспечение, реализующего криптосистему Пайе.

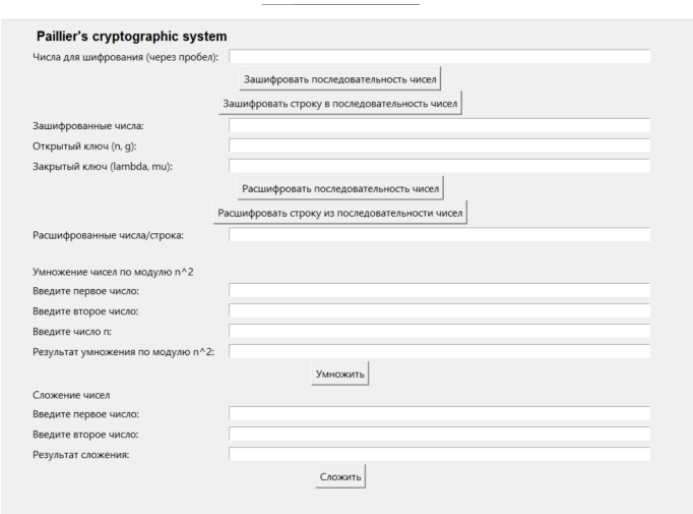

Рис. 1. Оконный интерфейс разработанной программы

Проверим гомоморфные свойства на примере чисел 5 и 55, зашифровав их с открытым ключом (50429, 2512502155) и закрытым ключом (3570, 29309) (в случае, если ключи не были введены или введенные ключи не удовлетворяют требованию n ≥ m, где m – сообщение, n – первая часть открытого ключа, т.к. m ∈ z_n , генерируются новые ключи по выше описанному алгоритму). В результате шифрования получаем числа 1433899025 и 700235992, которые при перемножении по модулю n^2 (где $n = 50429$) дают значение 2083066704, которое в свою очередь после расшифровки с теми же ключами дает значение 60, которое равно сумме изначальных чисел.

Проверим гомоморфные свойства также на примере другой пары чисел – 4 и 14:

Зашифруем их с тем же открытым ключом (50429, 2512502155) и закрытым ключом (3570, 29309) (в случае, если ключи не были введены или введенные ключи не удовлетворяют требованию n >= m, где m – сообщение, n – первая часть открытого ключа, т.к. m ∈ z_n ,генерируются новые ключи по выше описанному алгоритму). В результате шифрования получаем числа 293724083 и 729837275, которые при перемножении по модулю n^2 (где $n = 50429$) дают значение1967494430, которое в свою очередь после расшифровки с теми же ключами дает значение18, которое равно сумме изначальных чисел.

Проверка гомоморфных свойств на примере чисел 4 и 24:

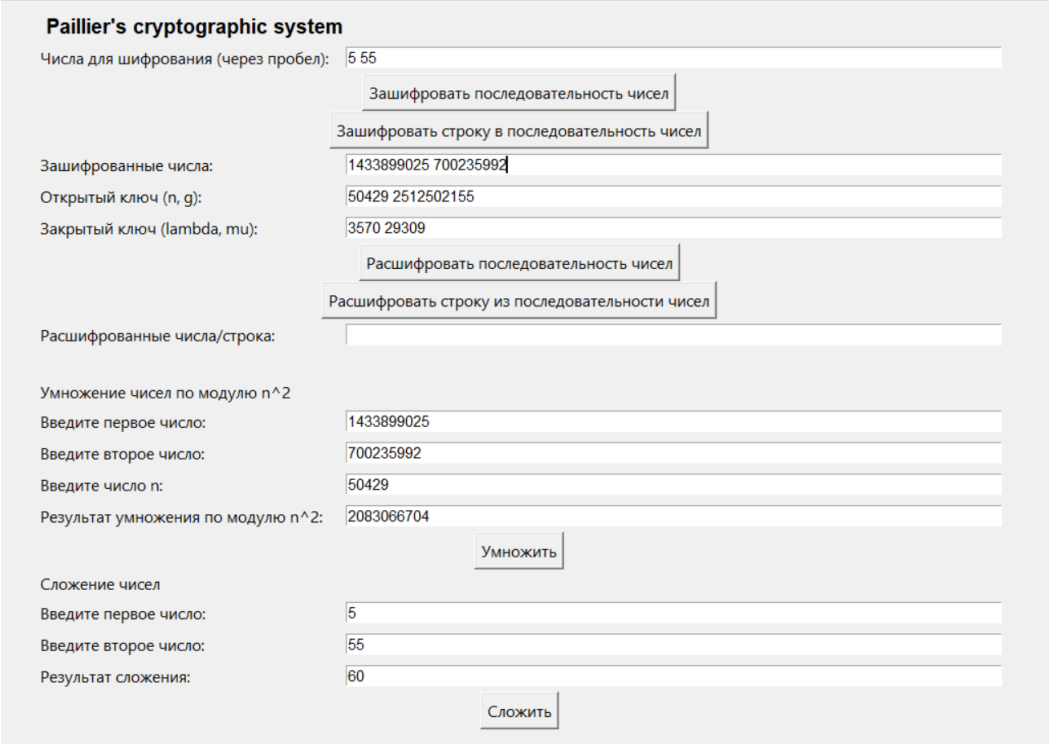

Рис. 2. Иллюстрация работы программы и проверка гомоморфных свойств метода шифрования

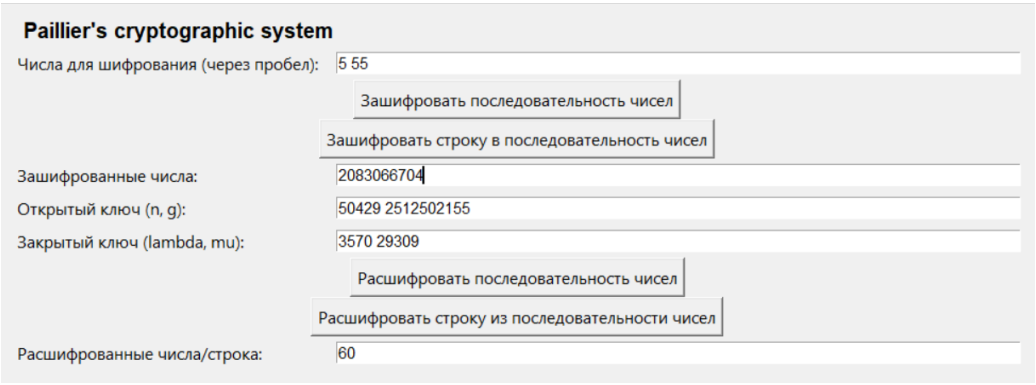

Рис. 3. Иллюстрация работы программы и проверка гомоморфных свойств метода шифрования

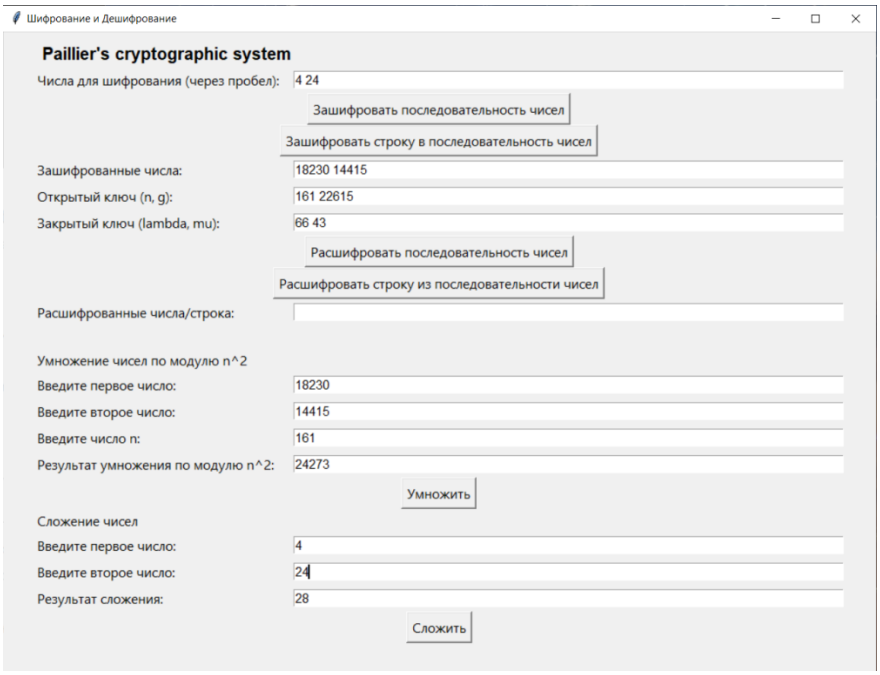

Рис. 4. Иллюстрация работы программы и проверка гомоморфных свойств метода шифрования

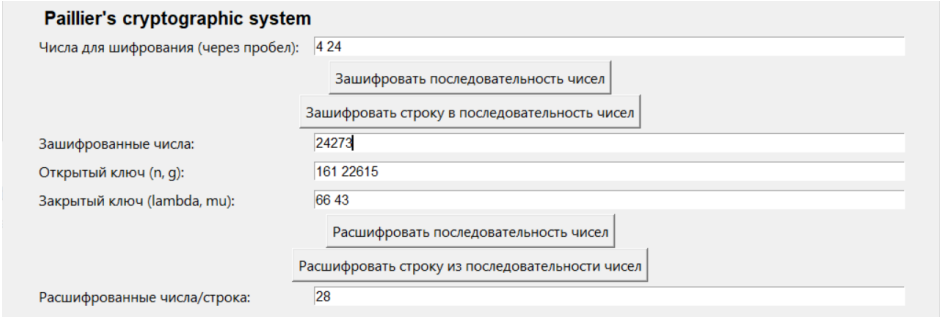

Рис. 5. Иллюстрация работы программы и проверка гомоморфных свойств метода шифрования

Программа также подразумевает шифрование строки в последовательность чисел и дешифрование строки из последовательности чисел:

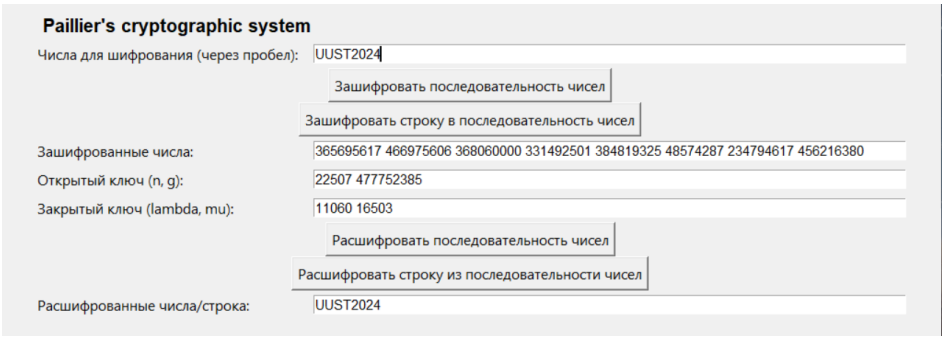

Рис. 6. Шифрование и дешифрование строки про помощи криптосистемы Пайе

ЗАКЛЮЧЕНИЕ

В данной работе представлена анализ алгоритмов гомоморфного шифрования, был разобран один из методов частичного гомоморфного шифрования, а также было создано прикладной программное обеспечение, реализующее данный метод в виде оконного приложения.

Гомоморфные методы шифрования являются перспективным направлением в области криптографии, поскольку открывают новые возможности для безопасной работы с конфиденциальными данными.

Автор выражает благодарность кандидату техн. наук, доценту Н.В. Кучкаровой за высказанные замечания и пожелания по улучшению статьи.

СПИСОК ЛИТЕРАТУРЫ

1. **Щелкунов, А. М., Глухарев, М.Л.** Гомоморфное шифрование в базах данных: статья / А.М. Щелкунов, М. Л. Глухарев. – Санкт-Петербург: Петербургский государственный университет путей сообщения Императора Александра 1, 2018. – 6 с.

2. **Дубенко, К. И.** Будущее криптографии: статья / К.И. Дубенко. – Ростов-на-Дону: Ростовский государственный университет путей сообщения, 2018. – 5 с.

3. **Мартыщенко, Д. О.** Гомоморфизм в криптографии: статья / Д.О. Мартыщенко. – Ростов-на-Дону: Молодой исследователь Дона №3(24) 2020. – 4 с**.**

ОБ АВТОРЕ

БАЛГАЗИН Тагир Ильсурович, ст. 3 курса ИИМРТ по специальности «Программная инженерия» группы ПРО-338Б.

METADATA

Title: Homomorphic encryption in information security

Author: T. I. Balgazin

Affiliation:

[1] Ufa State University of Science and Technology (UUST), Russia.

Email: Tagir.balgazin@yandex.ru,

Language: Russian.

Source: Molodezhnyj Vestnik UGATU (scientific journal of Ufa University of Science and Technology), no. 2 (31), pp. 10-15, 2024. ISSN 2225-9309 (Print).

Abstract: This article discusses methods and algorithms for homomorphic encryption. Application software was created that implements the Paillier's cryptosystem, which has homomorphic properties, and the homomorphic properties of this system were tested.

Key words: homomorphism, cryptosystem, algorithm, encryption, key.

About author:

BALGAZIN Tagir Ilsurovich, third year student of UUST, Institute of Informatics, mathematics and robotics.