Романенко Кирилл Сергеевич – Южный федеральный университет; e-mail: kirromanenko@sfedu.ru; г. Таганрог, Россия; тел.: +79885190125; кафедра безопасности информационных технологий им. Макаревича О.Б.; ассистент.

Ищукова Евгения Александровна – Южный федеральный университет; e-mail: uaishukova@sfedu.ru; г. Таганрог, Россия; тел.: +79281435898; кафедра безопасности информационных технологий им. Макаревича О.Б.; к.т.н.; доцент.

Ельчанинова Наталья Борисовна – Южный федеральный университет; e-mail: inf_2012@mail.ru; г. Таганрог, Россия; тел.: +79185000495; кафедра безопасности информационных технологий им. Макаревича О.Б.; к.т.н.; доцент.

Romanenko Kirill Sergeevich – Southern Federal University; e-mail: kirromanenko@sfedu.ru; phone: +79885190125; Taganrog, Russia; the Department of Information Technology Security named after Makarevich O.B.; assistant.

Ishchukova Evgeniya Aleksandrovna – Southern Federal University; e-mail: uaishukova@sfedu.ru; phone: +79281435898; Taganrog, Russia; the Department of Information Technology Security named after Makarevich O.B.; cand. of eng. sc.; associate professor.

Elchaninova Nataliya Borisovna – Southern Federal University; e-mail: inf_2012@mail.ru; phone: +79185000495; Taganrog, Russia; the Department of Information Technology Security named after Makarevich O.B.; cand. of eng. sc.; associate professor.

УДК 004.056.55 DOI 10.18522/2311-3103-2025-3-110-118

В.С. Стародубцев, Л.К. Бабенко, Н.Б. Ельчанинова

ОЦЕНКА ВРЕМЕНИ ВЫПОЛНЕНИЯ ПОИСКА СОСТАВЛЯЮЩИХ КЛЮЧА В АТАКЕ С ИЗВЕСТНЫМ ОТКРЫТЫМ ТЕКСТОМ НА КРИПТОСИСТЕМУ ДОМИНГО-ФЕРРЕРА

Представлено краткое описание полностью гомоморфной криптографической системы Доминго-Феррера, приводится характеристика этапов атаки с известным открытым текстом на данную криптосистему. Анализируется этап поиска составляющих ключа рассматриваемой атаки, для которого описываются существующие методы реализации, среди которых определяется метод, обладающий минимальной вычислительной сложностью. Обоснование вычислительной сложности и временных затрат рассматриваемого метода реализации этапа поиска составляющих ключа формируется на основе теоретических расчётов, а также экспериментальных исследований. Целью исследования является оценка сложности реализации этапа поиска составляющих ключа в атаке с известным открытым текстом на полностью гомоморфную криптографическую систему Доминго-Феррера с помощью метода Гаусса, разработанного для решения систем линейных алгебраических уравнений по модулю простого числа. Основным результатом настоящей работы является оценка вычислительной сложности этапа поиска составляющих ключа в атаке с известным открытым текстом на криптографическую систему Доминго-Феррера, реализованного с использованием метода Гаусса. Оценка сложности выражена в количестве базовых математических операций и подтверждена рядом экспериментальных исследований, что позволяет сделать обоснованные выводы о вычислительной сложности рассматриваемого метода. Проведенное исследование представляет собой значимый вклад в развитие полностью гомоморфной криптосистемы Доминго-Феррера, основанной на задаче факторизации целых чисел. Оно обладает практической значимостью, так как позволяет оценить критичность атаки с известным открытым текстом на данную криптосистему. Полученные результаты могут служить основой для исследователей и криптографов при разработке рекомендаций по выбору параметров криптосистемы Доминго-Феррера для обеспечения необходимого уровня безопасности в различных приложениях.

Информационная безопасность; гомоморфное шифрование; гомоморфная схема шифрования; полностью гомоморфное шифрование; криптосистема Доминго-Феррера; криптоанализ.

V.S. Starodubcev, L.K. Babenko, N.B. Yelchaninova

ESTIMATION OF THE SEARCH TIME FOR KEY COMPONENTS IN A KNOWN PLAINTEXT ATTACK ON THE DOMINGO-FERRER CRYPTOSYSTEM

This paper provides a brief description of the fully homomorphic Domingo-Ferrer cryptographic system and describes the stages of an attack with a known plaintext on this cryptosystem. The stage of searching for the key components of the attack in question is analyzed, for which existing implementation methods are described, among which the method with minimal computational complexity is determined. The rationale for the computational complexity and time costs of the considered method for implementing the key component search stage is based on theoretical calculations, as well as experimental studies. The aim of the study is to evaluate the complexity of implementing the stage of searching for key components in an attack with a known plaintext on a fully homomorphic Domingo-Ferrer cryptographic system using the Gauss method, developed for solving systems of linear algebraic equations modulo a prime number. The main result of this work is an assessment of the computational complexity of the key component search stage in a known plaintext attack on the Domingo-Ferrer cryptographic system, implemented using the Gauss method. The complexity estimate is expressed in the number of basic mathematical operations and is confirmed by a number of experimental studies, which allows us to draw reasonable conclusions about the computational complexity of the method under consideration. The conducted research represents a significant contribution to the development of a fully homomorphic Domingo-Ferrer cryptosystem based on the integer factorization problem. It has practical significance, as it allows us to assess the criticality of an attack with a known plaintext on a given cryptosystem. The results obtained can serve as a basis for researchers and cryptographers to develop recommendations for choosing the parameters of the Domingo-Ferrer cryptosystem to ensure the necessary level of security in various applications.

Information security; homomorphic encryption; homomorphic encryption scheme; fully homomorphic encryption; Domingo-Ferrer cryptosystem; cryptanalysis.

Введение. В настоящее время облачные вычисления получили широкое распространение, что обусловлено их преимуществами в области обработки и хранения данных [1]. Однако, несмотря на указанные достоинства, существует критический недостаток данной технологии: данные, подлежащие обработке, должны быть представлены в открытом виде. Это создает серьезные проблемы в тех областях, где конфиденциальность информации имеет первостепенное значение и где публикация данных в недоверенной среде является неприемлемой.

Традиционным решением данной проблемы является использование гомоморфного шифрования, которое позволяет выполнять операции над зашифрованными данными без необходимости их предварительной расшифровки [2]. Первая стойкая полностью гомоморфная криптографическая система была представлена в 2009 году Крейгом Джентри [3]. Эта система основана на идеальных решетках и использует добавление небольшого значения шума в шифртексты [4].

В дальнейшем было предложено множество гомоморфных криптосистем, основанных на концепциях, выдвинутых Джентри, которые получили название «криптосистемы типа Джентри» [5]. Эти схемы имеют доказанную высокую криптографическую стойкость, но обладают высокой вычислительной сложностью выполнения гомоморфных операций [6], что значительно ограничивает их практическое применение.

В качестве альтернативы криптосистемам типа Джентри были разработаны различные схемы, обладающие значительно меньшей вычислительной сложностью [7–10]. Однако, эти криптосистемы не получили широкого распространения, их криптографическая стойкость и вычислительная сложность операций недостаточно оценены. В данной работе рассматривается основанная на задаче факторизации чисел криптосистема Доминго-Феррера [8]. Задача факторизации чисел всегда считалась эталоном вычислительной сложности в криптографических задачах [11, 12], что позволяет предполагать, что исследование стойкости криптосистемы Доминго-Феррера может быть перспективным для оценки возможностей её практического применения.

В статье [13] приводится описание атаки с известным открытым текстом на криптосистему Доминго-Феррера, требующей наличия пар (открытый текст – шифртекст) на 1 больше, чем степень полиномов представления шифртекста (d). В работе [14] предложе-

на модификация атаки с известным открытым текстом (known-plaintext attack), позволяющая сократить количество необходимых пар (открытый текст – шифртекст) до 2. Поскольку для криптосистемы Доминго-Феррера актуальна атака с известным открытым текстом, необходимо рассмотреть вычислительную сложность практической реализации данной атаки.

Описание криптосистемы Доминго-Феррера. Данная криптосистема поддерживает гомоморфные операции, включая сложение, вычитание и умножение [8]. Шифр Доминго-Феррера относится к классу симметричных криптосистем, поскольку для процессов шифрования и расшифрования используется один и тот же ключ [15]. Важно отметить, что данная криптосистема не имеет ограничений на количество последовательных гомоморфных операций, что, несомненно, является её значительным преимуществом перед криптосистемами типа Джентри. Но необходимо учитывать, что размер итоговых шифртекстов при выполнении этих операций увеличивается: в частности, при проведении операций умножения наблюдается экспоненциальный рост объёма шифртекстов. Для инициализации криптосистемы Доминго-Феррера используется следующий набор параметров:

- p и q – большие простые числа;
- $n = p \times q$ – труднофакторизуемое число;
- d – степень полиномов представления шифртекстов.

Алгоритмы, выполняющие генерацию ключа, а также процессы шифрования и расшифрования в криптосистеме Доминго-Феррера, представлены на рис. 1.

Рис. 1. Описание алгоритмов операций шифра Доминго-Феррера

Атака с известным открытым текстом на криптосистему Доминго-Феррера. В работе [14] представлена атака с известным открытым текстом на криптографическую систему Доминго-Феррера. Для успешной реализации данной атаки противнику необходимо обладать по крайней мере d парами (открытый текст – шифртекст), созданными на одном ключе, где d – степень полинома представления шифртекста.

Атака с известным открытым текстом является двухэтапной. На первом этапе происходит факторизация числа n, на втором – выполняется поиск составных частей ключа (r_p, r_q).

Раскрытие факторизации числа n осуществляется путём вычисления наибольшего общего делителя (НОД) этого числа и результанта A двух полиномов, составленных из значений открытых текстов (m_1, m_2) и первой части шифртекстов $(\pi(x)_1, \pi(x)_2)$, как показано в формуле (1).

$$A = Res(\pi(x)_1 - m_1, \pi(x)_2 - m_2), \quad (1)$$

где Res – функция поиска результанта полиномов.

Число n известно, поэтому первая его составляющая (p) вычисляется по формуле (2), а значение q определяется, как частное от деления n на p.

$$p = \text{НОД}(A, n). \tag{2}$$

На втором этапе атаки происходит поиск частей ключа (r_p, r_q) путём решения двух систем линейных алгебраических уравнений (СЛАУ) по соответствующим модулям (p, q). Из значений открытых текстов $m_1 \ldots m_d$ и первой части шифртекстов $\pi(x)_1 \ldots \pi(x)_d$ формируется матрица B по формуле (3).

$$B \equiv \begin{pmatrix} -m_1 & y_{11} & y_{12} & \cdots & y_{1d} \\ -m_2 & y_{21} & y_{22} & \cdots & y_{2d} \\ & & & \vdots & \\ -m_d & y_{d1} & y_{d2} & \cdots & y_{dd} \end{pmatrix} \equiv \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} mod\ p, \tag{3}$$

где $m_1 \ldots m_d$ – открытые тексты, y – коэффициент многочлена соответствующей степени первой части шифртекстов $\pi(x)_1 \ldots \pi(x)_d$.

Важно отметить, что полученная матрица B является СЛАУ по модулю p. Переменные, входящие в матрицы не являются независимыми друг от друга, представляют собой мультипликативные обратные значения первой части ключа ${r_p}^{-1}$ по модулю p, возведённые в степени, соответствующие их позициям в уравнениях. Рассмотрим решение СЛАУ методом Гаусса.

Значение первой части ключа r_p вычисляется по формуле (4), как мультипликативное обратное по модулю p решения системы линейных уравнений t, представленных матрицей B.

$$r_p = t^{-1} mod\ p. \tag{4}$$

Значение второй части ключа r_q вычисляется аналогичным образом по формулам (3) и (4), за исключением того, что значения коэффициентов y в матрице B выбираются, как коэффициенты соответствующей степени второй части шифртекста $\rho(x)$.

Решение СЛАУ по модулю простого числа. При реализации атаки с известным открытым текстом возникает необходимость поиска решения СЛАУ по модулю. Итерационные методы [16] неприменимы для поиска решения подобных СЛАУ, по причине отсутствия у таких СЛАУ свойства диагонального преобладания [17], поэтому при выполнении атаки с известным открытым текстом для поиска решения рассматриваемой СЛАУ необходимо применять прямые (численные) методы. Одним из простых прямых методов поиска решения СЛАУ, обладающим низкой вычислительной сложностью, является метод Гаусса [18].

При поиске решения СЛАУ по модулю классический метод Гаусса имеет следующие особенности. В силу свойств СЛАУ, составляющие её переменные не являются независимыми друг от друга, а по сути являются одной переменной, возведенной по модулю в степень, соответствующую её позиции в уравнении. Иными словами, СЛАУ состоит из набора уравнений от одной переменной. Следовательно, единственным решением подобной СЛАУ является значение только одной переменной со степенью 1. Тогда в процессе решения СЛАУ методом Гаусса достаточно получить только одну строку с ненулевым коэффициентом переменной со степенью 1. Это означает, что на этапе обратного хода метода Гаусса нужно выполнить всего 1 шаг, что существенно сокращает время выполнения алгоритма.

Однако, наряду с описанным упрощением обратного хода метода Гаусса, вытекающим из свойств решаемых им СЛАУ, также требуются и некоторые изменения, увеличивающие количество выполняемых операций. Исходя из того, что поиск решения СЛАУ выполняется по модулю, после всех математических операций требуется дополнительная операция получения остатка от деления. Кроме того, на этапе прямого хода метода Гаусса необходимо выполнить обнуление некоторых элементов для приведения матрицы к верхнему треугольному виду. В классическом виде обнуление элемента матрицы a_{ij} происходит путём вычитания элементов строки матрицы a_k из элементов строки a_i, ум-

ноженных на коэффициент, вычисляемый как частное от деления a_{ij} на a_{kj}, где i – номер строки, j – номер столбца, k – номер выбранной строки, используемой для обнуления элемента a_{ij}. В случае, когда все операции выполняются в кольце по модулю p, операция деления (a_{ij}/a_{kj}) заменяется умножением $a_{ij} \times (a_{kj})^{-1} mod\ p$, где $(a_{kj})^{-1}$ – мультипликативное обратное a_{kj} по модулю p. Следовательно, для каждого обнуляемого элемента матрицы a_{ij} требуется одна операция поиска мультипликативного обратного с помощью расширенного алгоритма Евклида [19].

Оценка временной сложности метода Гаусса для поиска решения СЛАУ по модулю. На этапе прямого хода матрица приводится к верхнему треугольному виду, при этом первая строка матрицы остается без изменений, во второй обнуляется первый элемент, и в каждой последующей обнуляется на один элемент больше, чем в предыдущей. Следовательно, число шагов $StepCount$ прямого хода метода Гаусса определяется формулой (5).

$$StepCount = \sum_{i=1}^{d-1} i = \frac{d^2-d}{2}, \quad (5)$$

где d – размер системы линейных алгебраических уравнений.

Далее рассматривается сложность одного шага прямого хода метода Гаусса для поиска для решения СЛАУ по модулю. В первую очередь определяется подходящая строка a_k для обнуления элемента a_{ij}. После того, как подходящая строка a_k для обнуления элемента a_{ij} определена, необходимо найти коэффициент M, на который её элементы будут умножены, чтобы после вычитания строк получить $a_{ij} = 0$. Коэффициент M определяется по формуле (6).

$$M = a_{ij} \times (a_{kj})^{-1} mod\ p, \quad (6)$$

где i – номер строки, j – номер столбца, k – номер найденной строки для обнуления элемента a_{ij}, p – значение первой составляющей модуля, определенное в параметрах криптосистемы.

Из формулы (6) видно, что при поиске коэффициента M выполняется 1 операция умножения, 1 операция получения остатка от деления и 1 получение мультипликативного обратного с помощью расширенного алгоритма Евклида.

Количество шагов расширенного алгоритма Евклида зависит от чисел, которые поступают на вход. В контексте выполняемой задачи данные числа – случайные, поэтому заранее точно определить требуемое число шагов расширенного алгоритма Евклида невозможно. Однако, зная значение модуля p, согласно теореме Ламе, формулируемую как «число делений с остатком в процессе применения алгоритма Евклида не превосходит упятеренного количества цифр меньшего числа, записанного в десятичной системе» [20], возможно вычислить число шагов $MaxEuclidSteps$ для наихудшего случая расширенного алгоритма Евклида по формуле (7).

$$MaxExEuclidSteps = \log_{10}(p-1) \times 5, \quad (7)$$

где p – значение первой составляющей модуля, определенное в параметрах криптосистемы.

В работе [21] приводится оценка количества элементарных операций, выполняемых на каждом шаге расширенного алгоритма Евклида, следовательно в наихудшем случае для поиска мультипликативного обратного необходимо выполнить $MaxExEuclidSteps$ делений, $MaxExEuclidSteps \times 3$ вычитаний и $MaxExEuclidSteps \times 3$ умножения.

Завершающей операцией по обнулению коэффициента a_{ij} является вычитание строки a_k из строки a_i по формуле (8).

$$a_i = a_i - M \times a_k\ mod\ p, \quad (8)$$

где i – номер строки, M – коэффициент, найденный по формуле (6), k – номер найденной строки для обнуления элемента a_{ij}, p – значение первой составляющей модуля, определенное в параметрах криптосистемы.

Из формулы (8) следует, что для вычисления нового элемента строки a_i нужно умножить соответствующий ему элемент из строки a_k на коэффициент M, вычесть найденное значение из текущего элемента строки a_i, а затем получить остаток от деления на p. Так как в методе Гаусса используется расширенная матрица, то количество операций умножения, сложения и получения остатка от деления на p при вычитании строки a_k из строки a_i на 1 больше числа переменных.

После завершения прямого хода формируется матрица верхнего треугольного вида, из которой необходимо найти значение переменной со степенью 1 с помощью обратного хода метода Гаусса. Из особенностей рассматриваемых СЛАУ, решаемых методом Гаусса, следует, что обратный ход такого метода всегда выполняется в один шаг и состоит из одной операции поиска мультипликативного обратного элемента по модулю, одного умножения и одной операции получения остатка от деления.

Таким образом, с учётом количества шагов $StepCount$ прямого хода метода Гаусса, определяемого по формуле (5) и количества всех операций, выполняемых на каждом шаге прямого хода, а также, принимая во внимание те операции, которые необходимо выполнить на этапе обратного хода, можно определить общее количество операций метода Гаусса для поиска решения двух СЛАУ размера d, которое составляет:

- $2(\sum_{i=1}^{d-1} i + 1) = d^2 - d + 2$ операций поиска мультипликативного обратного элемента по модулю;
- $2(\sum_{i=1}^{d-1} i \times (d+1)) = d^3 - d$ операций вычитания;
- $2(\sum_{i=1}^{d-1} i \times (d+2) + 1) = d^3 + d^2 - 2d + 2$ операций умножения;
- $2(\sum_{i=1}^{d-1} i \times (d+2) + 1) = d^3 + d^2 - 2d + 2$ операций получения остатка от деления.

Практическая оценка вычислительной сложности метода Гаусса для поиска решения СЛАУ по модулю. Выше сложность расширенного алгоритма Евклида была оценена теоретически как наихудший случай. Однако в контексте оценки критичности реализации атаки важно понимать не только наихудший случай, но и средний, поэтому рассматриваемая атака была реализована на языке C# в рамках описанной в работах [22, 23] системы для анализа гомоморфных шифров. Исходными данными для запуска атаки выбраны значения модулей $p = 193$, $q = 197$, а степень полинома представления шифртекста d варьировалась от 1000 до 2000 включительно с шагом 100.

Зависимость количества шагов расширенного алгоритма Евклида от степени полинома представления шифртекста d приводится на рис. 2.

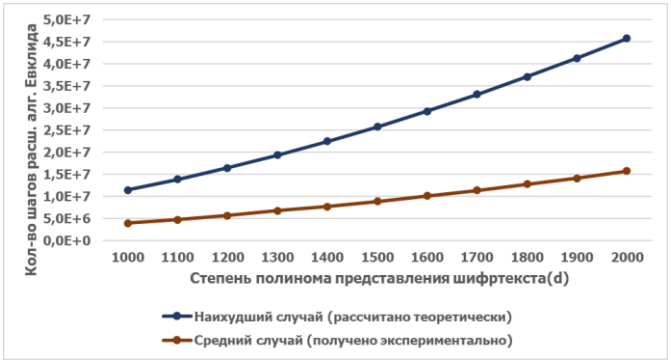

Рис. 2. Количество шагов расширенного алгоритма Евклида, выполняемых при атаке с известным открытым текстом в зависимости от степени полинома представления шифртекста (d)

Заключение. В данной работе рассмотрена атака с известным открытым текстом на криптографическую систему Доминго-Феррера. В данной атаке на этапе поиска составных частей ключа (r_p, r_q) требуется решение систем линейных алгебраических уравнений по модулю, что влечет за собой значительные вычислительные затраты. Для поиска ре-

шения подобных СЛАУ применен метод Гаусса. Данный метод обладает кубической вычислительной сложностью $O(d^3)$ и реализован в однопоточном режиме. Полученные оценки вычислительной сложности подтверждены экспериментальными исследованиями соответствующей реализации на языке программирования C#. В качестве исходных данных криптосистемы выбраны параметры модулей $p = 193$, $q = 197$ и степень полинома представления шифртекста $d = 2000$. Время реализации в рассмотренной атаке этапа поиска составляющих ключа на процессоре AMD Ryzen 5 3500U (2.1 ГГц) в однопоточном режиме составило 290,25 с.

Для метода Гаусса существуют способы параллельной реализации, применимые и для рассмотренной задачи. Следовательно, одним из направлений дальнейшей работы является оценка времени выполнения атаки с известным открытым текстом на криптографическую систему Доминго-Феррера с использованием параллельной реализации метода Гаусса.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Прудникова А.А., Садовникова Т.М.* Анализ облачных сервисов с точки зрения информационной безопасности // T-Comm-Телекоммуникации и Транспорт. – 2012. – № 7. – С. 153-156.
2. *Бабенко Л.К., Русаловский И.Д.* Метод реализации гомоморфного деления // Известия ЮФУ. Технические науки. – 2020. – № 4 (214). – С. 212-221. – DOI: 10.18522/2311-3103-2020-4-212-221.
3. *Gentry C.* A fully homomorphic encryption scheme. – Stanford university, 2009.
4. *Lyubashevsky V., Peikert C., Regev O.* On ideal lattices and learning with errors over rings // Advances in Cryptology–EUROCRYPT 2010: 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques, French Riviera, May 30–June 3, 2010. Proceedings 29. – Springer Berlin Heidelberg, 2010. – P. 1-23.
5. *Бабенко Л.К. и др.* Полностью гомоморфное шифрование (обзор) // Вопросы защиты информации. – 2015. – № 3. – С. 3-26.
6. *Acar A. et al.* A survey on homomorphic encryption schemes: Theory and implementation // ACM Computing Surveys (Csur). – 2018. – Vol. 51, No. 4. – P. 1-35.
7. *Armknecht F. et al.* On constructing homomorphic encryption schemes from coding theory // IMA International Conference on Cryptography and Coding. – Berlin, Heidelberg: Springer Berlin Heidelberg, 2011. – P. 23-40.
8. *Domingo-Ferrer J.* A provably secure additive and multiplicative privacy homomorphism // International Conference on Information Security. – Berlin, Heidelberg : Springer Berlin Heidelberg, 2002. – P. 471-483.
9. *Zhirov A., Zhirova O., Krendelev S.F.* Practical fully homomorphic encryption over polynomial quotient rings // World Congress on Internet Security (WorldCIS-2013). – IEEE, 2013. – P. 70-75.
10. *Kipnis A., Hibshoosh E.* Efficient methods for practical fully homomorphic symmetric-key encrypton, randomization and verification // Cryptology ePrint Archive. – 2012.
11. *Merkel W. et al.* Factorization of numbers with physical systems // Fortschritte der Physik: Progress of Physics. – 2006. – Vol. 54, No. 8-10. – P. 856-865.
12. *Lenstra A. K. et al.* The factorization of the ninth Fermat number // Mathematics of Computation. – 1993. – Vol. 61, No. 203. – P. 319-349.
13. *Cheon J.H., Nam H.S.* A cryptanalysis of the original domingo-ferrer's algebraic privacy homomophism // Cryptology EPrint Archive. – 2003.
14. *Trepacheva A. V.* Improved known plaintexts attack on Domingo-Ferrer homomorphic cryptosystem // Proceedings of the Institute for System Programming of the RAS (Proceedings of ISP RAS). – 2014. – Vol. 26, No. 5. – P. 83-98.
15. *Чернявский А.Ф., Козлова Е.И., Чернявский Ю.А.* Особенности структурно-аппаратного обеспечения преобразования информации в криптосистемах // Доклады Белорусского государственного университета информатики и радиоэлектроники. – 2024. – Т. 22, № 5. – С. 80-88. – DOI: 10.35596/1729-7648-2024-22-5-80-88.
16. *Соколова Е.В.* Обобщение прямых и итерационных методов решения систем линейных алгебраических уравнений // Математика и ИТ - вместе в цифровое будущее: Сб. трудов Молодежной школы, Нижний Новгород, 25–29 апреля 2022 года. – Нижний Новгород: Национальный исследовательский Нижегородский государственный университет им. Н.И. Лобачевского, 2022. – С. 111-120.

17. *Ефанов В.В., Закота А.А., Гунькина А.С.* Методика оценки точности определения параметров движения воздушной цели в условиях скрытного наблюдения за ней на основе применения метода итерации // Тр. МАИ. – 2021. – № 117. – DOI: 10.34759/trd-2021-117-18.
18. *Сеченов П.А.* Сравнение быстродействия численных методов Гаусса и LUP-разложения в задаче нахождения равновесного химического состава // Вестник Воронежского государственного технического университета. – 2023. – Т. 19, №. 2. – С. 79-85. – DOI: 10.36622/VSTU.2023.19.2.012.
19. *Iliev A., Kyurkchiev N.* The faster extended Euclidean algorithm // Collection of scientific works from conference. – 2018. – P. 21-26.
20. *Абрамов С.А.* Математические построения и программирование. – 1978.
21. *Бабенко Л.К., Стародубцев В.С.* Оценка времени выполнения операций шифрования, расшифрования, гомоморфных вычислений с использованием криптосистемы Доминго-Феррера // Известия ЮФУ. Технические науки. – 2024. – № 5 (241). – С. 6-15. – DOI: 10.18522/2311-3103-2024-5-6-15.
22. *Бабенко Л.К., Стародубцев В.С.* Особенности реализации системы криптоанализа гомоморфных шифров, основанных на задаче факторизации чисел // Известия ЮФУ. Технические науки. – 2024. – № 3 (239). – С. 55-64. – DOI: 10.18522/2311-3103-2024-3-55-64.
23. *Бабенко Л.К., Стародубцев В.С.* Особенности реализации систем криптоанализа гомоморфных шифров, основанных на задаче факторизации чисел, на примере криптосистемы MORE // Вопросы кибербезопасности. – 2024. – № 3 (61). – С. 141-145. – DOI: 10.21681/2311-3456-2024-3-141-145.

REFERENCES

1. *Prudnikova A.A., Sadovnikova T.M.* Analiz oblachnykh servisov s tochki zreniya informatsionnoy bezopasnosti [Analysis of cloud services from the point of view of information security], *T-Comm-Telekommunikatsii i Transport* [T-Comm-Telecommunications and Transport], 2012, No. 7, pp. 153-156.
2. *Babenko L.K., Rusalovskiy I.D.* Metod realizatsii gomomorfnogo deleniya [Method for implementing homomorphic division], *Izvestiya YuFU. Tekhnicheskie nauki* [Izvestiya SFedU. Engineering Sciences], 2020, No. 4 (214), pp. 212-221. DOI: 10.18522/2311-3103-2020-4-212-221.
3. *Gentry C.* A fully homomorphic encryption scheme. Stanford university, 2009.
4. *Lyubashevsky V., Peikert C., Regev O.* On ideal lattices and learning with errors over rings, *Advances in Cryptology–EUROCRYPT 2010: 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques, French Riviera, May 30–June 3, 2010. Proceedings 29*. Springer Berlin Heidelberg, 2010, pp. 1-23.
5. *Babenko L.K. i dr.* Polnost'yu gomomorfnoe shifrovanie (obzor) [Fully homomorphic encryption (review)], *Voprosy zashchity informatsii* [Information Security Issues], 2015, No. 3, pp. 3-26.
6. *Acar A. et al.* A survey on homomorphic encryption schemes: Theory and implementation, *ACM Computing Surveys (Csur),* 2018, Vol. 51, No. 4, pp. 1-35.
7. *Armknecht F. et al.* On constructing homomorphic encryption schemes from coding theory, *IMA International Conference on Cryptography and Coding*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2011, pp. 23-40.
8. *Domingo-Ferrer J.* A provably secure additive and multiplicative privacy homomorphism, *International Conference on Information Security*. Berlin, Heidelberg : Springer Berlin Heidelberg, 2002, pp. 471-483.
9. *Zhirov A., Zhirova O., Krendelev S.F.* Practical fully homomorphic encryption over polynomial quotient rings, *World Congress on Internet Security (WorldCIS-2013)*. IEEE, 2013, pp. 70-75.
10. *Kipnis A., Hibshoosh E.* Efficient methods for practical fully homomorphic symmetric-key encrypton, randomization and verification, *Cryptology ePrint Archive,* 2012.
11. *Merkel W. et al.* Factorization of numbers with physical systems, *Fortschritte der Physik: Progress of Physics,* 2006, Vol. 54, No. 8-10, pp. 856-865.
12. *Lenstra A. K. et al.* The factorization of the ninth Fermat number, *Mathematics of Computation,* 1993, Vol. 61, No. 203, pp. 319-349.
13. *Cheon J.H., Nam H.S.* A cryptanalysis of the original domingo-ferrer's algebraic privacy homomophism, *Cryptology EPrint Archive,* 2003.
14. *Trepacheva A. V.* Improved known plaintexts attack on Domingo-Ferrer homomorphic cryptosystem, *Proceedings of the Institute for System Programming of the RAS (Proceedings of ISP RAS),* 2014, Vol. 26, No. 5, pp. 83-98.
15. *Chernyavskiy A.F., Kozlova E.I., Chernyavskiy Yu.A.* Osobennosti strukturno-apparatnogo obespecheniya preobrazovaniya informatsii v kriptosistemakh [Features of structural and hardware support for information transformation in cryptosystems], *Doklady Belorusskogo gosudarstvennogo universiteta informatiki i radioelektroniki* [Reports of the Belarusian State University of Informatics and Radioelectronics], 2024, Vol. 22, No. 5, pp. 80-88. DOI: 10.35596/1729-7648-2024-22-5-80-88.

16. *Sokolova E.V.* Obobshchenie pryamykh i iteratsionnykh metodov resheniya sistem lineynykh algebraicheskikh uravneniy [Generalization of direct and iterative methods for solving systems of linear algebraic equations], *Matematika i IT - vmeste v tsifrovoe budushchee: Sb. trudov Molodezhnoy shkoly, Nizhniy Novgorod, 25–29 aprelya 2022 goda* [Mathematics and IT - together into the digital future: Collection of works of the Youth School, Nizhny Novgorod, April 25-29, 2022]. Nizhniy Novgorod: Natsional'nyy issledovatel'skiy Nizhegorodskiy gosudarstvennyy universitet im. N.I. Lobachevskogo, 2022, pp. 111-120.
17. *Efanov V.V., Zakota A.A., Gun'kina A.S.* Metodika otsenki tochnosti opredeleniya parametrov dvizheniya vozdushnoy tseli v usloviyakh skrytnogo nablyudeniya za ney na osnove primeneniya metoda iteratsii [Methodology for assessing the accuracy of determining the motion parameters of an air target under covert surveillance based on the iteration method], *Tr. MAI* [Proceedings of MAI], 2021, No. 117. DOI: 10.34759/trd-2021-117-18.
18. *Sechenov P.A.* Sravnenie bystrodeystviya chislennykh metodov Gaussa i LUP-razlozheniya v zadache nakhozhdeniya ravnovesnogo khimicheskogo sostava [Comparison of the performance of numerical Gaussian methods and LUP decomposition in the problem of finding the equilibrium chemical composition], *Vestnik Voronezhskogo gosudarstvennogo tekhnicheskogo universiteta* [Bulletin of the Voronezh State Technical University], 2023, Vol. 19, No. 2, pp. 79-85. DOI: 10.36622/VSTU.2023.19.2.012.
19. *Iliev A., Kyurkchiev N.* The faster extended Euclidean algorithm, *Collection of scientific works from conference,* 2018, pp. 21-26.
20. *Abramov S.A.* Matematicheskie postroeniya i programmirovanie [Mathematical constructions and programming], 1978.
21. *Babenko L.K., Starodubtsev V.S.* Otsenka vremeni vypolneniya operatsiy shifrovaniya, rasshifrovaniya, gomomorfnykh vychisleniy s ispol'zovaniem kriptosistemy Domingo-Ferrera [Estimation of execution time of encryption, decryption, homomorphic computations using the Domingo-Ferrer cryptosystem], *Izvestiya YuFU. Tekhnicheskie nauki* [Izvestiya SFedU. Engineering Sciences], 2024, No. 5 (241), pp. 6-15. – DOI: 10.18522/2311-3103-2024-5-6-15.
22. *Babenko L.K., Starodubtsev V.S.* Osobennosti realizatsii sistemy kriptoanaliza gomomorfnykh shifrov, osnovannykh na zadache faktorizatsii chisel [Features of the implementation of the cryptanalysis system of homomorphic ciphers based on the problem of number factorization], *Izvestiya YuFU. Tekhnicheskie nauki* [Izvestiya SFedU. Engineering Sciences], 2024, No. 3 (239), pp. 55-64. DOI: 10.18522/2311-3103-2024-3-55-64.
23. *Babenko L.K., Starodubtsev V.S.* Osobennosti realizatsii sistem kriptoanaliza gomomorfnykh shifrov, osnovannykh na zadache faktorizatsii chisel, na primere kriptosistemy MORE [Features of the implementation of cryptanalysis systems of homomorphic ciphers based on the problem of number factorization, using the example of the MORE cryptosystem], *Voprosy kiberbezopasnosti* [Cybersecurity Issues], 2024, No. 3 (61), pp. 141-145. DOI: 10.21681/2311-3456-2024-3-141-145.

Бабенко Людмила Климентьевна – Южный федеральный университет; e-mail: lkbabenko@sfedu.ru; тел.: +79054530191; г. Таганрог, Россия; кафедра безопасности информационных технологий им. Макаревича О.Б.; д.т.н.; профессор.

Стародубцев Виталий Сергеевич – Южный федеральный университет; e-mail: vstarodubcev@sfedu.ru; тел.: +79996928150; г. Таганрог, Россия; кафедра безопасности информационных технологий им. Макаревича О.Б.; аспирант.

Ельчанинова Наталья Борисовна – Южный федеральный университет; e-mail: nbelchaninova@sfedu.ru; г. Таганрог, Россия; тел.: +79185000495; кафедра безопасности информационных технологий им. Макаревича О.Б.; к.т.н.; доцент.

Babenko Lyudmila Kliment'evna – Southern Federal University; e-mail: lkbabenko@sfedu.ru; phone: +79054530191; Taganrog, Russia; the Department of Information Technology Security named after Makarevich O.B.; dr of eng. sc.; professor.

Starodubcev Vitalij Sergeevich – Southern Federal University; e-mail: vstarodubcev@sfedu.ru; Taganrog, Russia; phone: +79996928150; the Department of Information Technology Security named after Makarevich O.B.; post graduate student.

Yelchaninova Natalia Borisovna – Southern Federal University; e-mail: nbelchaninova@sfedu.ru; Taganrog, Russia; phone: +79185000495; the Department of Information Technology Security named after Makarevich O.B.; cand. of eng. sc.; associate professor.