

Сорокин Михаил Максимович – Южный федеральный университет; e-mail: sorokin@sfedu.ru; г. Таганрог, Россия; кафедра систем автоматизированного проектирования им. Виктора Михайловича Курейчика; аспирант.

Гладков Леонид Анатольевич – Южный федеральный университет; e-mail: lagladkov@sfedu.ru; г. Таганрог, Россия; кафедра систем автоматизированного проектирования им. Виктора Михайловича Курейчика; профессор.

Гладкова Надежда Викторовна – Южный федеральный университет; e-mail: nvgladkova@sfedu.ru; г. Таганрог, Россия; кафедра систем автоматизированного проектирования им. Виктора Михайловича Курейчика; старший преподаватель.

Sorokin Mikhail Maximovich – Southern Federal University; e-mail: sorokin@sfedu.ru; Taganrog, Russia; the Department of Computer Aided Design named after V.M. Kureichik; postgraduate student.

Gladkov Leonid Anatol'evich – Southern Federal University; e-mail: lagladkov@sfedu.ru; Taganrog, Russia; the Department of Computer Aided Design named after V.M. Kureichik; professor.

Gladkova Nadezhda Viktorovna – Southern Federal University; e-mail: nvgladkova@sfedu.ru; Taganrog, Russia; the Department of Computer Aided Design named after V.M. Kureichik; senior teacher.

УДК 004.056.55

DOI 10.18522/2311-3103-2026-4-150-159

В.С. Стародубцев, Л.К. Бабенко**АЛГОРИТМЫ СНИЖЕНИЯ ВРЕМЕННЫХ ЗАТРАТ НА ВЫПОЛНЕНИЕ ОПЕРАЦИЙ КРИПТОСИСТЕМЫ ДОМИНГО-ФЕРРЕРА**

Проведён анализ литературы по тематике полностью гомоморфного шифрования. Представлено краткое описание полностью гомоморфной криптографической системы Доминго-Феррера, основанной на задаче факторизации чисел, приведены временные характеристики этапов атаки с известным открытым текстом на данную криптосистему. Проанализированы временные характеристики операций криптосистемы, описаны методы и средства их практической реализации. Предложены новые алгоритмы реализации операций криптосистемы Доминго-Феррера, позволяющие снизить время их выполнения. Обоснование оценок временных затрат операций криптосистемы формируется на основе теоретических расчётов, а также результатов экспериментальных исследований. Целью исследования является снижение времени выполнения операций криптосистемы Доминго-Феррера посредством разработки алгоритмов их модификации, учитывающих особенности практической реализации. Основным результатом настоящей работы является снижение времени выполнения следующих операций криптосистемы Доминго-Феррера: шифрования – на 10-15%, расшифрования – в 2 раза, гомоморфного умножения – в 64 раза для цепочки из 200 умножений при использовании степени полиномов представления шифртекста $d=100$ и незначительном увеличении временных затрат на генерацию ключа. Проведённое исследование представляет собой значимый вклад в развитие полностью гомоморфной криптосистемы Доминго-Феррера, основанной на задаче факторизации целых чисел. Настоящая работа обладает практической значимостью, поскольку позволяет значительно повысить производительность гомоморфных вычислений данной криптосистемы. Полученные результаты могут стать основой для разработки эффективных (с точки зрения вычислительных затрат и обеспечения уровня безопасности) программно-аппаратных комплексов облачных вычислений, использующих полностью гомоморфную криптосистему Доминго-Феррера для обеспечения конфиденциальности обрабатываемой информации.

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

V.S. Starodubcev, L.K. Babenko**ALGORITHMS FOR REDUCING THE TIME REQUIRED TO PERFORM OPERATIONS OF THE DOMINGO-FERRER CRYPTOSYSTEM**

An analysis of the literature on the topic of fully homomorphic encryption is carried out. A brief description of the completely homomorphic Domingo-Ferrer cryptographic system based on the number factorization problem is presented, and the time characteristics of the stages of an attack with a known plaintext on this cryptosystem are given. The time characteristics of cryptosystem operations are analyzed,

methods and means of their practical implementation are described. New algorithms for implementing the operations of the Domingo-Ferrer cryptosystem are proposed to reduce their execution time. The justification of estimates of the time costs of cryptosystem operations is formed on the basis of theoretical calculations, as well as the results of experimental studies. The aim of the study is to reduce the execution time of the Domingo-Ferrer cryptosystem by developing algorithms for their modification, taking into account the specifics of practical implementation. The main result of this work is a reduction in the execution time of the following operations of the Domingo-Ferrer cryptosystem: encryption by 10-15%, decryption by 2 times, homomorphic multiplication by 64 times for a chain of 200 multiplications using the degree of polynomials of the ciphertext representation $d=100$ and a slight increase in the time spent on key generation. The conducted research represents a significant contribution to the development of a fully homomorphic Domingo-Ferrer cryptosystem based on the integer factorization problem. This work has practical significance because it significantly improves the performance of homomorphic calculations of this cryptosystem. The results obtained can become the basis for the development of efficient (in terms of required computing costs and the level of security provided) cloud computing software and hardware systems using a fully homomorphic Domingo-Ferrer cryptosystem to ensure the confidentiality of processed information.

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

Введение. В настоящее время гомоморфное шифрование является одним из наиболее перспективных направлений благодаря своей возможности обеспечивать конфиденциальность при обработке информации с помощью облачных вычислений [1, 2]. Постоянный рост объемов обрабатываемой информации вынуждает компании постоянно наращивать свои вычислительные мощности. Однако в большинстве случаев развертывание собственной инфраструктуры связано со значительными денежными затратами, поэтому наиболее часто компании не приобретают, а вместо этого арендуют необходимое оборудование у провайдеров облачных вычислений. Это позволяет значительно сократить как денежные, так и временные затраты на развертывание необходимого окружения, поскольку технология облачных вычислений обеспечивает высокую гибкость и масштабируемость используемых решений [3].

Однако, несмотря на все вышеобозначенные преимущества, область применения облачных вычислений существенно ограничена. Подобная технология обладает существенным недостатком – в большинстве случаев облачная инфраструктура представляет собой среду, в которой не гарантируется конфиденциальность обрабатываемых сведений [4]. Следовательно, компании, обрабатывающие информацию ограниченного доступа, вынуждены отказываться от использования облачных вычислений. Одним из решений данной проблемы является использование гомоморфных операций, которые обрабатывают информацию в зашифрованном виде.

Впервые идея выполнения гомоморфных вычислений была предложена Ривестом и др. в работе [5], когда выяснилось, что числа, зашифрованные с помощью асимметричного шифра RSA [6], возможно перемножать в зашифрованном виде. Результат вычислений над шифртекстами был эквивалентен результату аналогичных операций, выполненных над открытыми текстами. Это термин авторы обозначили «Privacy Homomorphism», а их работа легла в основу концепции гомоморфного шифрования. Вскоре стало ясно, что для формирования полноценной системы гомоморфных вычислений требуется разработать полностью гомоморфную криптосистему, поддерживающую выполнение и операций сложения, и умножения. Впоследствии различными авторами было предложено множество схем, однако большая часть из них оказалась либо небезопасной, либо, подобно RSA, лишь частично гомоморфной [4] (поддерживала выполнение только одной гомоморфной операции – сложения или умножения).

Значительный прорыв в области гомоморфного шифрования совершил Крейг Джендри, когда в 2009 году в своей работе [7] предложил новую криптографическую систему. Его криптосистема оказалась первой схемой полностью гомоморфного шифрования, которая продемонстрировала высокий уровень криптографической стойкости. Однако, к сожалению, время выполнения операций криптосистемы Джендри было очень большим, из-за чего применение данной схемы на практике было неоправданно дорогим. С тех пор учёное сообщество разделилось на две основные части: первая (и наиболее

значительная) часть исследователей стремится ускорить выполнение операций в криптосистемах типа Джентри, а вторая сконцентрировала свои усилия на разработке и повышении стойкости криптографических систем, основанных на других концепциях. На данный момент наиболее распространенными криптосистемами типа Джентри являются: BFV, BGV, CKKS, TFHE и FHEW [8–13]. Для примера рассмотрим реализацию схемы BFV в библиотеке PALISADE с модулем открытого текста $p = 786433$ и степенью полиномов $N = 32768$. Так, при использовании процессора Intel(R) Core™ i7-10700 время выполнения одного гомоморфного сложения составило в среднем 7 мс., а умножения – в среднем 428 мс. [13]. Если сравнить данный результат с временем выполнения обычных операций умножения над целыми числами в языке программирования C#, которое для данного процессора в среднем составляет 10 нс., заметно, что гомоморфные операции выполняются крайне медленно.

Наиболее известной альтернативой схемам типа Джентри является более производительная криптосистема Доминго-Феррера, основанная на задаче факторизации чисел [14]. Главным недостатком криптосистемы Доминго-Феррера является её низкая стойкость к атаке с известным открытым текстом, представленной в работе [15]. В работах [16, 17] была рассмотрена трудоёмкость этой атаки на криптосистему. Для оценки влияния естественным является рассмотрение набора параметров криптосистемы Доминго-Феррера, при котором атака будет проходить крайне медленно, а гомоморфные вычисления выполняться за приемлемое для использования на практике время.

Постановка задачи. На основании анализа работ по тематике полностью гомоморфного шифрования установлено, что влияние атаки с известным открытым текстом на безопасность криптосистемы Доминго-Феррера остается недостаточно исследованным. В предшествующих наших работах [16–18] была оценена вычислительная сложность операций рассматриваемой криптосистемы и время реализации атаки с известным открытым текстом на эту криптосистему. Исходя из результатов, полученных в данных работах, можно предположить, что для обеспечения безопасности криптосистемы Доминго-Феррера необходимо выбрать такие параметры, при которых существенно возрастёт время реализации данной атаки. Однако, при увеличении параметров криптосистемы растёт и время её операций, что делает критически важным использование методов и алгоритмов, обладающих меньшей вычислительной сложностью. Целью данной работы является снижение времени выполнения операций криптосистемы Доминго-Феррера. Соответственно, научная задача заключается в разработке алгоритмов повышения производительности операций полностью гомоморфной криптосистемы Доминго-Феррера.

Для решения актуальной научной задачи и достижения поставленной цели в рамках настоящей работы необходимо решить следующие задачи:

- ♦ проанализировать шаги выполнения операций криптосистемы Доминго-Феррера;
- ♦ оценить вычислительную сложность и время выполнения данных шагов с помощью известных методов реализации;
- ♦ разработать алгоритмы и средства реализации операций криптосистемы Доминго-Феррера, отличающиеся от существующих меньшей трудоёмкостью;
- ♦ подтвердить полученные результаты экспериментальными оценками временных затрат, полученными для существующих и предлагаемых в работе методов реализации операций.

Описание криптосистемы Доминго-Феррера. Данная полностью гомоморфная криптосистема основана на задаче факторизации чисел [14]. В качестве параметров криптографической системы используются следующие значения:

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

Исходя из того, что подробное описание криптосистемы Доминго-Феррера приводилось авторами в предшествующих работах [16–18], в настоящей статье представлено краткое описание всех операций, а их промежуточные шаги опущены. Криптосистема Доминго-Феррера является вероятностной: один и тот же открытый текст при каждом шифровании будет преобразован в разные шифртексты. Кратко охарактеризуем опера-

ции криптосистемы: на этапе шифрования открытый текст m кодируется в полином $a(x)$, затем преобразуется в 2 полинома шифртекста $\pi(x)$ и $\rho(x)$ путём умножения $a(x)$ на значения ключа (r_p, r_q) в соответствующих степенях. При расшифровании сначала «снимаются» значения ключей путём умножения полиномов шифртекста на их мультипликативные обратные, затем из сумм всех коэффициентов полученных полиномов с помощью Китайской теоремы об остатках [19] восстанавливается значение открытого текста m . Для выполнения гомоморфных операций достаточно покоординатно умножить (сложить) полиномы шифртекстов. Все шаги генерации ключа, шифрования и расшифрования в криптосистеме Доминго-Феррера приведены на рис. 1.

Генерация ключа:		$r_p \xleftarrow{\$} Z_p^*, r_q \xleftarrow{\$} Z_q^*$
Шифрование:		Расшифрование:
$a_i \xleftarrow{\$} Z_n; a_d \xleftarrow{\$} Z_n \setminus \{0\}$		$A_p(x) = (b_d \cdot (r_p^{-1})^d x^d + \dots + b_1 \cdot (r_p^{-1}) x) \bmod p$
$a_1 = m - \left(\sum_{i=2}^d a_i \right) \bmod n$		$A_q(x) = (b_d \cdot (r_q^{-1})^d x^d + \dots + b_1 \cdot (r_q^{-1}) x) \bmod q$
$a(x) = a_d x^d + \dots + a_1 x$		$M_p = \sum_{i=1}^d b_i \bmod p$
$C = \begin{cases} \pi(x) = (a_d \cdot r_p^d x^d + \dots + a_1 \cdot r_p x) \bmod p \\ \rho(x) = (a_d \cdot r_q^d x^d + \dots + a_1 \cdot r_q x) \bmod q \end{cases}$		$M_q = \sum_{i=1}^d b_i \bmod q$
		$m = CRT(\{M_p, M_q\}, \{p, q\})$
Выполнение гомоморфных операций:		
$C_3 = C_1 \circ C_2 = (\pi(x)_1 \circ \pi(x)_2, \rho(x)_1 \circ \rho(x)_2)$		

Рис. 1. Описание алгоритмов операций шифра Доминго-Феррера

Атака с известным открытым текстом на криптосистему Доминго-Феррера. В работе [15] 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 путём вычисления результата, на втором – выполняется поиск составных частей ключа (r_p, r_q) с помощью решения системы линейных алгебраических уравнений. Согласно результатам [17] время выполнения атаки на процессоре AMD Ryzen 5 3500U (2.1 ГГц) составляет несущественное время 424,86 с. при использовании высокой степени полинома шифртекста $d = 2000$ для практических целей.

Оценка времени кодирования открытого текста. Как уже было упомянуто выше, операция шифрования в криптосистеме Доминго-Феррера начинается с кодирования значения открытого текста в полином $a(x)$. Для этого требуется сгенерировать $d - 1$ случайных чисел, не превышающих n . Безусловно, вычислительная сложность данного этапа шифрования напрямую зависит от используемого генератора псевдослучайных чисел, а чтобы оценить время выполнения, необходимо провести экспериментальные исследования. Для экспериментов использовалась реализация криптосистемы Доминго-Феррера на языке C#, развёрнутая в рамках системы для анализа полностью гомоморфных криптосистем, описанной в работе [20]. В качестве генератора псевдослучайных чисел использован RandomNumberGenerator из пространства имён System.Security.Cryptography.

Чтобы обеспечить меньшую вычислительную сложность, заранее определялась битовая длина псевдослучайной последовательности (ПСП), которая затем генерировалась за одно обращение к генератору ПСП, а затем сегментировалась на отдельные числа. В рамках эксперимента были выбраны модули длиной 20 бит, а степень полинома шиф-

ртекста d варьировалась в диапазоне от 10000 до 2000000 с шагом 10000. Для каждой степени полинома шифртекста d выполнялось 100 запусков, после чего вычислялось среднее значение времени. Текущий и все последующие эксперименты, изложенные в настоящей работе, выполнялись на стенде с процессором AMD Ryzen 5 3500U (2.1 ГГц) и 16 Гб оперативной памяти. Для обоснования выбора подхода к генерации псевдослучайных чисел за одно обращение к генератору ПСП был проведен аналогичный эксперимент, где генерация осуществлялась за $d - 1$ обращений к генератору ПСП. Результаты экспериментов представлены на графике, приведенном на рис. 2.

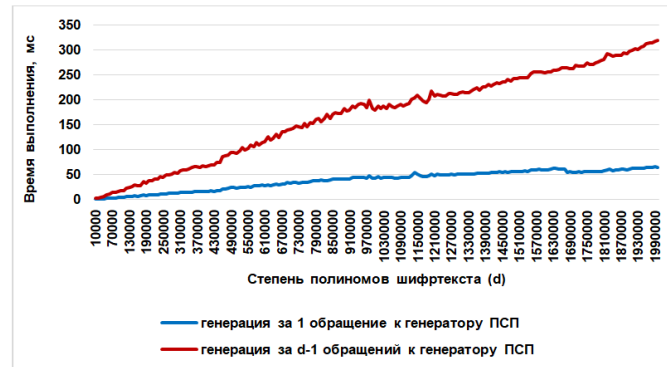


Рис. 2. Зависимость времени кодирования открытого текста от степени полинома шифртекста d

По результатам эксперимента можно заметить, что генерация за $d - 1$ обращений к генератору ПСП имеет линейную вычислительную сложность, а генерация псевдослучайных чисел за одно обращение к генератору ПСП характеризуется асимптотикой порядка $O(\log d)$. Кроме того, очевидно, что операция генерации псевдослучайных чисел не является трудоемкой и выполняется крайне быстро. Так, например, выполнение этапа кодирования открытого текста m в полином со степенью $d = 10000$ составило 350 мкс.

Описание модифицированной операции генерации ключа. На втором этапе шифрования производится умножение коэффициентов полиномов на значения ключей (r_p, r_q) , возведённых в соответствующую степень. При использовании классического алгоритма для шифрования каждого нового открытого текста требуется каждый раз возводить значения ключей (r_p, r_q) в степени от 2 до d , что требует $d - 1$ умножений. Кроме того, такое же количество умножений требуется и при расшифровании. Очевидно, что задача возведения значений ключа (r_p, r_q) в степень не зависит от шифруемых (или расшифровываемых) данных, поэтому она может быть выполнена ещё на этапе генерации ключа. Таким образом можно избежать дополнительных операций умножения в операциях шифрования и расшифрования. Следовательно, ключ можно хранить в виде полиномов $(R_p, R_q, R_p^{-1}, R_q^{-1})$, приведенных в (1).

$$\begin{aligned}
 R_p &= (r_p, r_p^2, \dots, r_p^d), \\
 R_q &= (r_q, r_q^2, \dots, r_q^d), \\
 R_p^{-1} &= (r_p^{-1}, (r_p^{-1})^2, \dots, (r_p^{-1})^d), \\
 R_q^{-1} &= (r_q^{-1}, (r_q^{-1})^2, \dots, (r_q^{-1})^d).
 \end{aligned} \tag{1}$$

Результаты проведенных экспериментов показали, что подобная модификация позволяет сократить время шифрования на 10-15% при незначительном повышении временных затрат на генерацию ключа. Так, например, для получения шифртекста со степенью полиномов $d = 10000$ классический алгоритм затратил 10 мс., а модифицированная версия – 8,56 мс. при увеличении времени генерации ключа на 2 мс.

На первый взгляд может показаться, что данная модификация позволяет лишь незначительно повысить производительность операций криптосистемы Доминго-Феррера, однако, если рассмотреть её вклад в общее время выполнения расшифрования становится ясно, что подобная изменение необходимо. Как было показано на рис. 1, операция расшифрования не требует генерации псевдослучайных чисел, из-за чего выполняется крайне быстро. В частности, эксперименты показали, что при степени полиномов шифртекстов $d = 10000$ время расшифрования шифртекста составляет 1,41 мс. и в данном случае предложенная модификация позволила сократить время данной операции в 2 раза.

Алгоритм снижения времени выполнения гомоморфного умножения. Для выбора методов практической реализации необходимо сначала рассмотреть вычислительную сложность гомоморфных операций криптосистемы с использованием тривиальных методов реализации. Гомоморфное сложение требует выполнить сложение соответствующих полиномов в шифртекстах. Операция сложения полиномов является вычислительно простой (линейная сложность). Суммарно для выполнения сложения шифртекстов требуется выполнить $2d$ операций сложения по модулю.

Операция гомоморфного умножения, напротив, при использовании тривиального метода реализации (далее – «наивное» умножение) требует $2d^2$ операций умножения по модулю. Но даже это не является главной проблемой – после каждого умножения шифртекстов степень полиномов результирующего шифртекста будет равна сумме степеней полиномов-сомножителей. Из этого следует, что каждая следующая за умножением операция будет вычислительно «дороже» предыдущих.

Однако, помимо «наивного» умножения полиномов существует ряд других алгоритмов [21–24], обладающих меньшей вычислительной сложностью. Одним из наиболее распространенных является метод, использующий быстрое преобразование Фурье (БПФ) для умножения полиномов [21]. Данный метод обладает оценкой вычислительной сложности $O(d \log_2 d)$ [23], что делает предпочтительным его применение в рамках выполнения гомоморфных операций умножения. Метод гомоморфного умножения с использованием БПФ состоит из следующих шагов:

- ◆ прямое преобразование Фурье;
- ◆ поточечное умножение;
- ◆ обратное преобразование Фурье;
- ◆ получение остатка от деления коэффициентов на n .

Для оценки времени выполнения операций гомоморфного умножения данный метод был реализован на языке C# с использованием библиотеки BigFloatLibrary. В качестве исходных параметров криптосистемы были выбраны модули p и q размером 30 бит, а степень $d = 100$. В процессе эксперимента формировалась цепочка умножений и фиксировалось время выполнения операции с помощью «наивной» реализации и с помощью БПФ. Результаты экспериментальных исследований изложены на графике, приведенном на рис. 3.

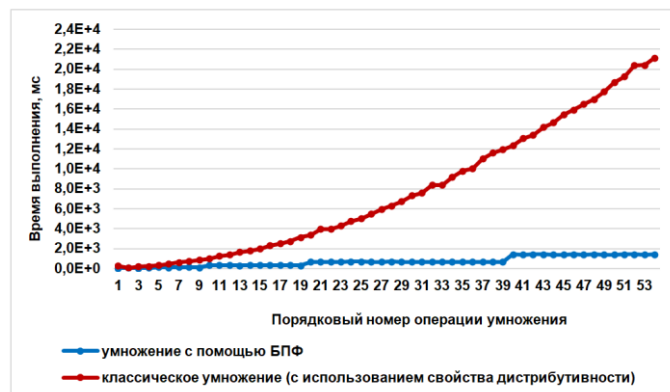


Рис. 3. Время выполнения гомоморфной операции умножения в зависимости от порядкового номера операции

Проанализировав сложность прямого и обратного преобразований Фурье и сравнив её со временем умножения значений в точках, можно заметить, что наибольшее время при выполнении гомоморфного умножения занимает именно преобразование шифртекстов из полиномиального вида в точечное. Также можно обратить внимание, что при выполнении гомоморфных операций данное преобразование необходимо лишь для того, чтобы привести коэффициенты результирующего полинома по модулю n . В свою очередь, данная операция необходима для контроля размера коэффициентов полиномов. В связи с этим возникло предположение о возможности снижения времени выполнения гомоморфных операций умножения за счёт сокращения количества трудоёмких прямых и обратных преобразований БПФ в процессе гомоморфных операций ценой увеличения объема потребляемой оперативной памяти. Дополнительный объем памяти потребовался для того, чтобы можно было приводить коэффициенты полиномов по модулю n не после каждой операции умножения, а по завершении выполнения последовательности из нескольких операций. С целью проверки упомянутого выше предположения проведен ряд экспериментальных исследований. В качестве параметров криптосистемы использовались значения, идентичные предыдущему эксперименту (для проведения в дальнейшем сравнительного анализа). Объем памяти, отводимый для хранения значений в точках, был увеличен, а операции БПФ выполнялись через каждые 4 умножения точек (значения были определены эмпирическим путём). В рамках экспериментов оценивался объем потребляемой памяти, а также время выполнения гомоморфного умножения с помощью предложенного алгоритма с сокращенным числом преобразований Фурье. Результаты экспериментальных исследований показаны на графиках, приведенных на рис. 4 и 5 соответственно.

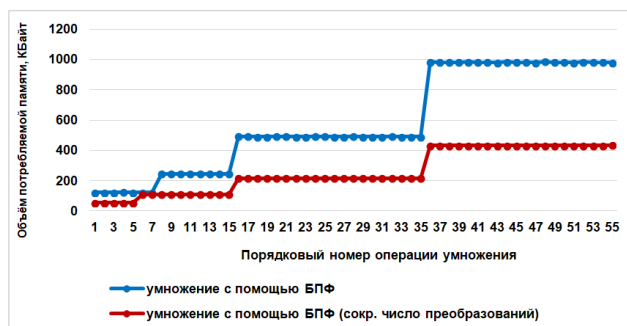


Рис. 4. Объем потребляемой оперативной памяти при выполнении гомоморфной операции умножения в зависимости от порядкового номера операции

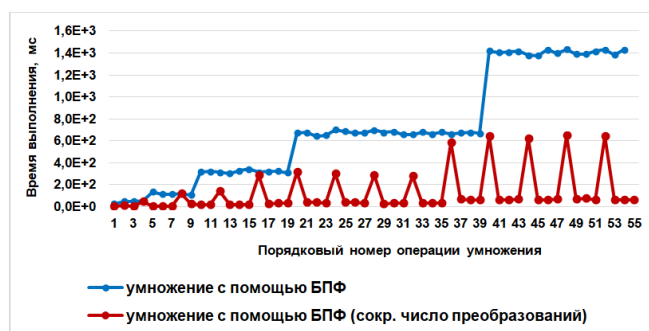


Рис. 5. Время выполнения гомоморфной операции умножения в зависимости от порядкового номера операции

Результаты экспериментов показали, что при сокращении числа операций БПФ время выполнения рассматриваемой цепочки гомоморфных умножений уменьшилось в 6 раз, а объем потребляемой памяти увеличился в 2,3 раза и составил 960 КБ, что подтвер-

дило корректность выдвинутого ранее предположения. Таким образом, для выполнения гомоморфных операций умножения в криптосистеме Доминго-Феррера необходимо использовать БПФ по описанной выше схеме. При этом в криптосистеме необходимо модифицировать операцию расшифрования: на начальном её этапе необходимо добавить обратное преобразование Фурье для получения полиномов шифртекста из набора точек.

Заключение. В настоящей работе проведён анализ вычислительной сложности операций полностью гомоморфной криптосистемы Доминго-Феррера с точки зрения методов и алгоритмов их практической реализации. Для операций криптосистемы предложен ряд алгоритмов модификации, отличающийся от известных меньшей вычислительной сложностью. Целесообразность применения предложенных изменений подтверждена рядом экспериментальных исследований на стенде с процессором AMD Ryzen 5 3500U (2.1 ГГц) и 16 Гб оперативной памяти.

В частности, при использовании модулей длиной 20 бит и степени полиномов шифртекста $d = 10000$ получены следующие временные оценки:

- ♦ время генерации ключа составило 2 мс.;
- ♦ время шифрования – 8,5 мс.;
- ♦ время расшифрования – 1,41 мс.

Операции гомоморфного умножения значительно более трудоемкие и даже при учёте использования предложенной модификации с применением БПФ, время выполнения цепочки из 54 умножений составило 6,5 с. Относительно «наивной» схемы умножения полиномов удалось достичь снижения времени работы в 64 раза при использовании модулей длиной 30 бит и степени полиномов шифртекста $d = 100$.

Однако, несмотря на значимость полученных в данной работе результатов, выполнение гомоморфных операций по-прежнему занимает значительное время, что препятствует применению криптосистемы Доминго-Феррера в реальных сценариях защищённых вычислений. Экспериментально подтверждено, что атака с известным открытым текстом на криптосистему с идентичными описанным выше параметрам может быть реализована всего за 150 мс., что не позволит безопасно выполнять гомоморфные вычисления [16, 17]. Анализ вычислительной сложности гомоморфных операций показывает существенный компромисс между безопасностью и временем выполнения гомоморфных операций: при использовании малых степеней полиномов шифртекста система подвержена атакам, тогда как повышение степени полиномов d до значений, обеспечивающих её безопасность, делает гомоморфные операции неоправданно трудоёмкими. Таким образом, можно прийти к выводу, что, к сожалению, область применения криптографической системы Доминго-Феррера по-прежнему ограничена и приоритетным направлением дальнейшей работы является разработка мер по повышению её безопасности. Авторы имеют предложения по решению этой проблемы, которые будут изложены в последующих работах.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Munjal K., Bhatia R. A systematic review of homomorphic encryption and its contributions in healthcare industry // *Complex & Intelligent Systems*. – 2023. – Vol. 9, No. 4. – P. 3759-3786. – DOI: 10.1007/s40747-022-00756-z.
2. Yang W. et al. A review of homomorphic encryption for privacy-preserving biometrics // *Sensors*. – 2023. – Vol. 23, No. 7. – P. 3566. – DOI: 10.3390/s23073566.
3. Sadeeq M.M. et al. IoT and Cloud computing issues, challenges and opportunities: A review // *Qubahan Academic Journal*. – 2021. – Vol. 1, No. 2. – P. 1-7. – DOI: 10.48161/qaj.v1n2a36.
4. Marcolla C. et al. Survey on fully homomorphic encryption, theory, and applications // *Proceedings of the IEEE*. – 2022. – Vol. 110, No. 10. – P. 1572-1609. – DOI: 10.36227/techrxiv.19315202.v5.
5. Rivest R.L. et al. On data banks and privacy homomorphisms // *Foundations of secure computation*. – 1978. – Vol. 4, No. 11. – P. 169-180.
6. Rivest R.L., Shamir A., Adleman L. A method for obtaining digital signatures and public-key cryptosystems // *Communications of the ACM*. – 1978. – Vol. 21, No. 2. – P. 120-126.
7. Gentry C. A fully homomorphic encryption scheme. – Stanford university, 2009.
8. Al Badawi A. et al. Openfhe: Open-source fully homomorphic encryption library // *Proceedings of the 10th workshop on encrypted computing & applied homomorphic cryptography*. – 2022. – P. 53-63. – DOI: 10.1145/3560827.3563379.

9. Xie Q. et al. Efficiency optimization techniques in privacy-preserving federated learning with homomorphic encryption: A brief survey // *IEEE Internet of Things Journal*. – 2024. – Vol. 11, No. 14. – P. 24569-24580. – DOI: 10.1109/JIOT.2024.3382875.
10. Cheon J.H. et al. Homomorphic encryption for arithmetic of approximate numbers // *International conference on the theory and application of cryptology and information security*. – Cham: Springer International Publishing, 2017. – P. 409-437. – DOI: 10.1007/978-3-319-70694-8_15.
11. Chillotti I., Gama N., Georgieva M., and Izabachène M. TFHE: Fast fully homomorphic encryption over the torus // *J. Cryptol.* – 2019. – Vol. 33, No. 1. – P. 1-58. – DOI: 10.1007/s00145-019-09319-x.
12. El Mestari S.Z., Lenzini G., Demirci H. Preserving data privacy in machine learning systems // *Computers & Security*. – 2024. – Vol. 137. – P. 103605. – DOI: 10.1016/j.cose.2023.103605.
13. Doan T.V.T. et al. A survey on implementations of homomorphic encryption schemes: DT Van Thao et al. // *The Journal of Supercomputing*. – 2023. – Vol. 79, No. 13. – P. 15098-15139. – DOI: 10.1007/s11227-023-05233-z.
14. 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. – DOI: 10.1007/3-540-45811-5_37.
15. Wagner D. Cryptanalysis of an algebraic privacy homomorphism // *Information Security: 6th International Conference, ISC 2003, Bristol, UK, October 1-3, 2003. Proceedings 6*. – Springer Berlin Heidelberg, 2003. – P. 234-239. – DOI: 10.1007/10958513_18.
16. Бабенко Л.К., Стародубцев В.С., Ельчанинова Н.Б. Оценка времени выполнения поиска составляющих ключа в атаке с известным открытым текстом на криптосистему Доминго-Феррера // *Известия ЮФУ. Технические науки*. – 2025. – № 3 (245). – С. 110-118. – DOI: 10.18522/2311-3103-2025-3-110-118.
17. Бабенко Л.К., Стародубцев В.С. Оценка времени выполнения атаки с известным открытым текстом на криптосистему Доминго-Феррера // *Вопросы кибербезопасности*. – 2026. – № 1 (71). – С. 139-147. – DOI: 10.21681/2311-3456-2026-1-139-147.
18. 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.
19. Alhassan E.A. et al. On some algebraic properties of the Chinese remainder theorem with applications to real life // *Journal of Applied Mathematics and Computation*. – 2021. – Vol. 5, No. 3. – DOI: 10.26855/jamc.2021.09.008.
20. 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.
21. Rajaby E., Sayedi S.M. A structured review of sparse fast Fourier transform algorithms // *Digital Signal Processing*. – 2022. – Vol. 123. – P. 103403. – DOI: 10.1016/j.dsp.2022.103403.
22. Pornin T. Efficient and complete formulas for binary curves // *Cryptology ePrint Archive*. – 2022.
23. Gao X. et al. A fast spectral sum-of-Gaussians method for electrostatic summation in quasi-2D systems // *Numerische Mathematik*. – 2026. – Vol. 158, No. 2. – P. 533-585. – DOI: 10.48550/arXiv.2412.04595.
24. Mateer T. Fast Fourier algorithms with applications: Ph. D. Thesis. – Clemson University, 2008.

REFERENCES

1. Munjal K., Bhatia R. A systematic review of homomorphic encryption and its contributions in healthcare industry, *Complex & Intelligent Systems*, 2023, Vol. 9, No. 4, pp. 3759-3786. DOI: 10.1007/s40747-022-00756-z.
2. Yang W. et al. A review of homomorphic encryption for privacy-preserving biometrics, *Sensors*, 2023, Vol. 23, No. 7, pp. 3566. DOI: 10.3390/s23073566.
3. Sadeeq M.M. et al. IoT and Cloud computing issues, challenges and opportunities: A review, *Qubahan Academic Journal*, 2021, Vol. 1, No. 2, pp. 1-7. DOI: 10.48161/qaj.v1n2a36.
4. Marcolla C. et al. Survey on fully homomorphic encryption, theory, and applications, *Proceedings of the IEEE*, 2022, Vol. 110, No. 10, pp. 1572-1609. DOI: 10.36227/techrxiv.19315202.v5.
5. Rivest R.L. et al. On data banks and privacy homomorphisms, *Foundations of secure computation*, 1978, Vol. 4, No. 11, pp. 169-180.
6. Rivest R.L., Shamir A., Adleman L. A method for obtaining digital signatures and public-key cryptosystems, *Communications of the ACM*, 1978, Vol. 21, No. 2, pp. 120-126.
7. Gentry C. A fully homomorphic encryption scheme. – Stanford university, 2009.
8. Al Badawi A. et al. Openfhe: Open-source fully homomorphic encryption library, *Proceedings of the 10th workshop on encrypted computing & applied homomorphic cryptography*, 2022, pp. 53-63. DOI: 10.1145/3560827.3563379.

9. Xie Q. et al. Efficiency optimization techniques in privacy-preserving federated learning with homomorphic encryption: A brief survey, *IEEE Internet of Things Journal*, 2024, Vol. 11, No. 14, pp. 24569-24580. DOI: 10.1109/JIOT.2024.3382875.
10. Cheon J.H. et al. Homomorphic encryption for arithmetic of approximate numbers, *International conference on the theory and application of cryptology and information security*. Cham: Springer International Publishing, 2017, pp. 409-437. DOI: 10.1007/978-3-319-70694-8_15.
11. Chillotti L., Gama N., Georgieva M., and Izabachène M. TFHE: Fast fully homomorphic encryption over the torus, *J. Cryptol*, 2019, Vol. 33, No. 1, pp. 1-58. DOI: 10.1007/s00145-019-09319-x.
12. El Mestari S.Z., Lenzini G., Demirci H. Preserving data privacy in machine learning systems, *Computers & Security*, 2024, Vol. 137, pp. 103605. DOI: 10.1016/j.cose.2023.103605.
13. Doan T.V.T. et al. A survey on implementations of homomorphic encryption schemes: DT Van Thao et al., *The Journal of Supercomputing*, 2023, Vol. 79, No. 13, pp. 15098-15139. DOI: 10.1007/s11227-023-05233-z.
14. 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. DOI: 10.1007/3-540-45811-5_37.
15. Wagner D. Cryptanalysis of an algebraic privacy homomorphism, *Information Security: 6th International Conference, ISC 2003, Bristol, UK, October 1-3, 2003. Proceedings 6*. Springer Berlin Heidelberg, 2003, pp. 234-239. DOI: 10.1007/10958513_18.
16. Babenko L.K., Starodubtsev V.S., El'chaninova N.B. Otsenka vremeni vypolneniya poiska sostavlyayushchikh klyucha v atake s izvestnym otkrytym tekstem na kriptosistemu Domingo-Ferrera [Estimation of the search time for key components in a known plaintext attack on the Domingo-Ferrer cryptosystem], *Izvestiya YuFU. Tekhnicheskie nauki* [Izvestiya SFedU. Engineering Sciences], 2025, No. 3 (245), pp. 110-118. DOI: 10.18522/2311-3103-2025-3-110-118.
17. Babenko L.K., Starodubtsev V.S. Otsenka vremeni vypolneniya ataki s izvestnym otkrytym tekstem na kriptosistemu Domingo-Ferrera [Estimating the execution time of a known plaintext attack on the Domingo-Ferrer cryptosystem], *Voprosy kiberbezopasnosti* [Cybersecurity Issues], 2026, No. 1 (71), pp. 139-147. DOI: 10.21681/2311-3456-2026-1-139-147.
18. Babenko L.K., Starodubtsev V.S. Otsenka vremeni vypolneniya operatsiy shifrovaniya, rasshifrovaniya, gomomorfnykh vychisleniy s ispol'zovaniem kriptosistemy Domingo-Ferrera [Estimation of the execution time of encryption, decryption, homomorphic calculations 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.
19. Alhassan E.A. et al. On some algebraic properties of the Chinese remainder theorem with applications to real life, *Journal of Applied Mathematics and Computation*, 2021, Vol. 5, No. 3. DOI: 10.26855/jamc.2021.09.008.
20. Babenko L.K., Starodubtsev V.S. Osobennosti realizatsii sistem kriptoolniza gomomorfnykh shifrov, osnovannykh na zadache faktorizatsii chisel, na primere kriptosistemy MORE [Features of the implementation of the cryptanalysis systems of homomorphic ciphers based on the problem of factorization of numbers, using the example of the cryptosystem MORE], *Voprosy kiberbezopasnosti* [Cybersecurity Issues], 2024, No. 3 (61), pp. 141-145. DOI: 10.21681/2311-3456-2024-3-141-145.
21. Rajaby E., Sayedi S.M. A structured review of sparse fast Fourier transform algorithms, *Digital Signal Processing*, 2022, Vol. 123, pp. 103403. DOI: 10.1016/j.dsp.2022.103403.
22. Pornin T. Efficient and complete formulas for binary curves, *Cryptology ePrint Archive*, 2022.
23. Gao X. et al. A fast spectral sum-of-Gaussians method for electrostatic summation in quasi-2D systems, *Numerische Mathematik*, 2026, Vol. 158, No. 2, pp. 533-585. DOI: 10.48550/arXiv.2412.04595.
24. Mateer T. Fast Fourier algorithms with applications: Ph. D. Thesis. Clemson University, 2008.

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

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

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

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