Раздел II. Алгоритмы обработки информации

УДК 004.5 DOI 10.18522/2311-3103-2024-3-55-64

Л.К. Бабенко, В.С. Стародубцев

ОСОБЕННОСТИ РЕАЛИЗАЦИИ СИСТЕМЫ КРИПТОАНАЛИЗА ГОМОМОРФНЫХ ШИФРОВ, ОСНОВАННЫХ НА ЗАДАЧЕ ФАКТОРИЗАЦИИ ЧИСЕЛ

Рассматриваются гомоморфные криптосистемы, основанные на задаче факторизации чисел. В сравнении с криптосистемами типа Джентри их реализация менее трудоемка, но при этом требуется тщательная проверка стойкости. В качестве примера гомоморфной криптосистемы, основанной на задаче факторизации чисел рассматривается симметричная криптосистема Доминго-Феррера. Для этой криптосистемы представлены процессы генерации ключа, шифрования, расшифрования и выполнения гомоморфных операций. Приводится описание атаки с известным открытым текстом на криптосистему Доминго-Феррера, а также демонстрационный пример такой атаки с небольшим значением степени полиномов представления шифртекстов. Для разрабатываемой архитектуры системы представляются основные требования и общая схема с кратким описанием области ответственности отдельных модулей и их взаимосвязями. Целью исследования является выявление подходов, техник и тактик, общих для конкретных методов криптоанализа гомоморфных криптосистем, основанных на задаче факторизации чисел, и создание такой архитектуры системы, которая бы позволила упростить криптоанализ путем предоставления криптоаналитику удобного окружения и инструментария для реализации собственных методов криптоанализа. Основным результатом настоящей работы является архитектура системы криптоанализа, позволяющая провести комплексный анализ уязвимостей для различных атак и оценить уровень криптостойкости рассматриваемого шифра, основанного на задаче факторизации чисел, а также обоснование применения такой архитектуры для анализа гомоморфных шифров на примере криптосистемы Доминго-Феррера. Реализация системы криптоанализа по предлагаемой архитектуре поможет исследователям и специалистам по криптографии более детально изучить возможные слабые места в гомоморфных шифрах, основанных на задаче факторизации чисел и разработать соответствующие меры для укрепления их стойкости. Таким образом, проводимое исследование имеет важное значение для развития криптографических систем, основанных на задаче факторизации чисел, и предоставляет новый инструментарий для криптоаналитиков в области анализа гомоморфных криптосистем. Полученные результаты могут быть использованы для повышения уровня стойкости существующих шифров и разработки новых методов криптографии.

Информационная безопасность; конфиденциальная информация; гомоморфное шифрование; криптосистема Доминго-Феррера; криптоанализ; архитектура системы криптоанализа.

L.K. Babenko, V.S. Starodubtsev

FEATURES OF THE IMPLEMENTATION OF THE CRYPTANALYSIS SYSTEM OF HOMOMORPHIC CIPHERS BASED ON THE PROBLEM OF FACTORIZATION OF NUMBERS

This article discusses homomorphic cryptosystems based on the problem of factorization of numbers. In comparison with Gentry-type cryptosystems, their implementation is less laborious, but it requires careful verification of durability. The Domingo-Ferrer symmetric cryptosystem is considered as an example of a homomorphic cryptosystem based on the number factorization problem. For this cryptosystem, the processes of key generation, encryption, decryption, and performing homomorphic operations are presented. A description of an attack with a known plaintext on the Domingo-Ferrer cryptosystem is given, as

well as a demonstration example of such an attack with a small value of the degree of the polynomials of the ciphertext representation. For the system architecture under development, the basic requirements and a general scheme are presented with a brief description of the area of responsibility of individual modules and their interrelationships. The aim of the study is to identify approaches, techniques and tactics common to specific cryptanalysis methods of homomorphic cryptosystems based on the problem of factorization of numbers, and to create a system architecture that would simplify cryptanalysis by providing the cryptanalyst with a convenient environment and tools for implementing his own cryptanalysis methods. The main result of this work is the architecture of the cryptanalysis system, which allows for a comprehensive analysis of vulnerabilities for various attacks and to assess the level of cryptographic strength of the cipher in question, based on the problem of factorization of numbers, as well as the justification for the use of such an architecture for the analysis of homomorphic ciphers using the example of the Domingo-Ferrer cryptosystem. The implementation of a cryptanalysis system based on the proposed architecture will help researchers and cryptography specialists to study in more detail possible weaknesses in homomorphic ciphers based on the problem of factorization of numbers and develop appropriate measures to strengthen their durability. Thus, the ongoing research is important for the development of cryptographic systems based on the problem of factorization of numbers and provides new tools for cryptanalysts in the field of analysis of homomorphic cryptosystems. The results obtained can be used to increase the strength of existing ciphers and develop new cryptographic methods.

Information security; confidential information; homomorphic encryption; Domingo-Ferrer cryptosystem; cryptanalysis; architecture of the cryptanalysis system.

Введение. Гомоморфное шифрование является одной из важных техник в области криптографии, которая предоставляет возможность выполнять операции с зашифрованными данными без необходимости расшифровывать их [1]. Это особенно полезно в контексте облачных вычислений и обработки данных, где часто возникает необходимость в анализе и использовании конфиденциальной информации [2].

Гомоморфное шифрование активно развивается, поскольку существующие схемы обладают определенными ограничениями, сокращающими область их применения, и авторы либо пытаются усовершенствовать существующие схемы, либо предлагают новые. При этом не существует единой методологии для обоснования стойкости большинства гомоморфных шифров, и их криптоанализ представляет собой сложную задачу [3]. Для упрощения процедуры криптоанализа конкретных шифров можно некоторые особенности его проведения учесть при построении архитектуры системы криптоанализа, предоставляя криптоаналитику удобное окружение и инструментарий.

Постановка задачи. Впервые понятие гомоморфного шифрования было введено Рональдом Ривестом, Леонардом Адлеманом и Майклом Дертузосом в 1978 году, когда они предложили использовать созданный годом ранее алгоритм RSA для выполнения операции умножения над зашифрованными текстами без их расшифрования [4]. Однако, поскольку алгоритм RSA, а также ряд других алгоритмов, появившихся в то время, являлись частично гомоморфными (свойства гомоморфизма проявлялись относительно только одной операции – сложения или умножения), их применение в данной области было сильно ограничено [5].

В 2009 году произошел значительный прорыв в области развития полностью гомоморфного шифрования. Это связано с предложением Крейгом Джентри варианта полностью гомоморфной криптосистемы, основанной на криптографии на решетках [6]. На данный момент было разработано несколько десятков схем полностью гомоморфного шифрования, основанных на этой концепции. При шифровании криптосистемой типа Джентри в значение шифртекста внедряется небольшое случайное значение – шум, размер которого постоянно увеличивается при выполнении гомоморфных операций. Пример механизма добавления шума в криптосистемах BGV, BFV описан в [7] и [8] соответственно и приведен на рис. 1.

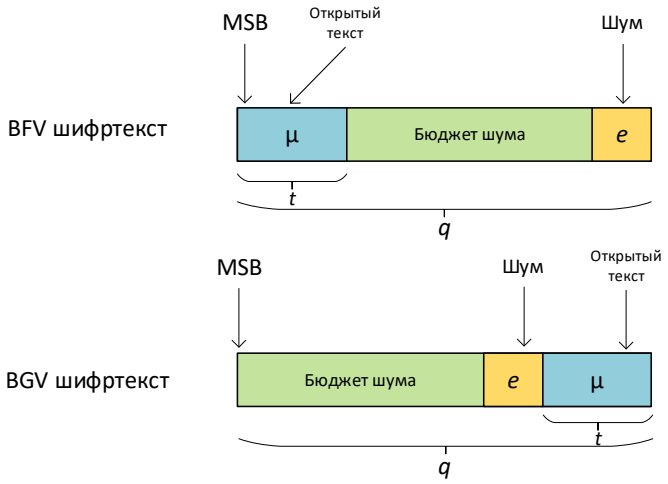

Рис. 1. Размещение шума в шифртекстах схем BFV, BGV

При выполнении сложения шум нарастает аддитивно, и не вызывает больших проблем, однако при умножении шум нарастает очень быстро и приводит к тому, что шифртекст больше не может быть расшифрован корректно [9] (бюджет шума был превышен и шумовые коэффициенты наложились на шифртекст).

Для решения данной проблемы был предложен специальный алгоритм самокоррекции [10], однако его применение существенно замедляет выполнение математических операций.

В качестве альтернативы различными авторами были предложены криптосистемы, являющиеся полностью гомоморфными, но при этом не использующими механизм добавления шума в шифртексты [11]. В этом случае процедуры гомоморфного умножения и сложения не приводят к существенному замедлению вычислений. Как правило, для обоснования стойкости таких систем криптоаналитику требуется применять разнообразные методы криптоанализа, что требует значительных временных затрат [12]. В этом случае разработка инструментария для проведения автоматического криптоанализа является актуальной задачей.

Описание криптосистемы Доминго-Феррера. Данная криптосистема была разработана в 1996 году и поддерживает выполнение гомоморфного сложения, вычитания и умножения. Система является симметричной (для шифрования и расшифрования используется один и тот же ключ) [13]. Количество последовательных выполнений гомоморфных операций в данной криптосистеме не ограничено, однако размеры результирующих шифртекстов увеличиваются (при умножении размер шифртекста растёт экспоненциально).

Для реализации криптосистемы Доминго-Феррера используется следующий набор значений [11]:

1) p и q – большие простые числа;

2) $n = p * q$ – труднофакторизуемое число;

3) d – степень полиномов представления шифртекстов.

Ключ в криптосистеме Доминго-Феррера представляется двумя числами – r_p и r_q, которые случайно выбираются из мультипликативных групп с соответствующим модулем: формулы (1) и (2) соответственно.

$$r_p \xleftarrow{Rand()} Z_p^*, \tag{1}$$

где Z_p^* – мультипликативная группа по модулю p.

$$r_q \xleftarrow{Rand()} Z_q^*, \tag{2}$$

где Z_q^* – мультипликативная группа по модулю q.

Для выполнения шифрования в криптосистеме Доминго-Феррера необходимо убедиться, что шифруемое сообщение $m \in Z_n$. После этого формируется набор случайных чисел $a_1, \dots, a_d$.Числа $a_2, \dots, a_{d-1}$ заполняются по формуле (3).

$$a_i \xleftarrow{Rand()} Z_n, \tag{3}$$

где i – индекс в диапазоне [2; d-1], Z_n – кольцо по модулю n.

Число a_d получает случайное ненулевое значение из Z_n по формуле (4).

$$a_d \xleftarrow{Rand()} Z_n \setminus \{0\}. \tag{4}$$

Числу a_1 присваивается значение в соответствии с формулой (5).

$$a_1 = m - \left(\sum_{i=2}^{d} a_i\right) mod\ n, \tag{5}$$

где m – шифруемое сообщение, n – модуль, определенный в параметрах схемы шифрования.

В результате представленных выше действий из набора чисел a формируется полином по формуле (6).

$$a(x) = a_d x^d + \cdots + a_1 x. \tag{6}$$

Если суммировать все коэффициенты полученного полинома, результат должен быть равен m, как показано в формуле (7).

$$\sum_{i=1}^{d} a_i\ mod\ n = m. \tag{7}$$

После того, как сформирован полином открытого текста, его необходимо зашифровать на ключе (r_p, r_q). Шифрование на первой части ключа r_p выполняется по формуле (8).

$$\pi(x) = \left(a_d \cdot r_p^d\ x^d + \cdots + a_1 \cdot r_p\ x\right) mod\ p. \tag{8}$$

Таким образом формируется многочлен, каждый коэффициент которого представлен умножением коэффициента полинома $a(x)$ на первую часть ключа r_p, возведенную в ту степень, перед которой этот коэффициент установлен.

Шифрование на второй части ключа r_q выполняется аналогично шифрованию на первой части ключа и вычисляется по формуле (9).

$$\rho(x) = \left(a_d \cdot r_q^d\ x^d + \cdots + a_1 \cdot r_q\ x\right) mod\ q. \tag{9}$$

Сформированная пара $(\pi(x), \rho(x))$ – зашифрованное сообщение m.

Для выполнения операции (сложение, вычитание, умножение) над двумя шифртекстами в криптосистеме Доминго-Феррера нужно применить эту операцию к полиномам шифртекстов, как показано в формуле (10).

$$C_3 = \{(\pi(x)_1 \circ \pi(x)_2), (\rho(x)_1 \circ \rho(x)_2)\}, \tag{10}$$

где C_3 – результирующий шифртекст, $(\pi(x), \rho(x))_1$ – первый шифртекст, $(\pi(x), \rho(x))_2$ – второй шифртекст.

Важно отметить, что в данном случае операция покоординатная, то есть умножаются (складываются) только те коэффициенты полиномов, у которых степени совпадают.

Для расшифрования в криптосистеме Доминго-Феррера предварительно необходимо для значений ключа (r_p, r_q) найти мультипликативные обратные (r_p^{-1}, r_q^{-1}). Для расшифрования шифртекста $(\pi(x), \rho(x))$ нужно вычислить значения $A_p(x)$ и $A_q(x)$ по формулам (11) и (12) соответственно.

$$A_p(x) = \left(b_d \cdot (r_p^{-1})^d\ x^d + \cdots + b_1 \cdot (r_p^{-1})\ x\right) mod\ p, \tag{11}$$

где b – коэффициенты полинома $\pi(x)$ шифртекста.

$$A_q(x) = \left(b_d \cdot (r_q^{-1})^d\ x^d + \cdots + b_1 \cdot (r_q^{-1})\ x\right) mod\ q, \tag{12}$$

где b – коэффициенты полинома $\rho(x)$ шифртекста.

Далее для $A_p(x)$ вычисляется сумма всех коэффициентов по формуле (13).

$$M_p = \sum_{i=1}^{d} a_i \ mod\ p, \tag{13}$$

где a_i – коэффициенты полинома $A_p(x)$.

Аналогично сумме M_p вычисляется сумма M_q по формуле (14).

$$M_q = \sum_{i=1}^{d} b_i \ mod\ q, \tag{14}$$

где b_i – коэффициенты полинома $A_q(x)$.

После вычисления сумм M_p и M_q открытый текст исходного сообщения рассчитывается с помощью Китайской теоремы об остатках по формуле (15).

$$m = CRT(\{M_p, M_q\}, \{p, q\}), \tag{15}$$

где $CRT()$ – функция, использующая Китайскую теорему об остатках для поиска значения открытого текста m.

Атака с известным открытым текстом на криптосистему Доминго-Феррера. Условием успешности атаки является наличие d + 1 пар (открытый текст – шифртекст), сформированных на одном ключе [15].

Данная атака осуществляется в 2 этапа: на первом происходит раскрытие факторизации числа n, на втором – непосредственно поиск ключа.

Для раскрытия факторизации числа n необходимо сформировать матрицу по формуле (16).

$$A = \begin{pmatrix} m_1 & y_{11} & y_{12} & \cdots & y_{1d} \\ m_2 & y_{21} & y_{22} & \cdots & y_{2d} \\ & & & \vdots & \\ m_{d+1} & y_{(d+1)1} & y_{(d+1)2} & \cdots & y_{(d+1)d} \end{pmatrix}, \tag{16}$$

где m – открытый текст, y – коэффициент многочлена соответствующей степени первой части шифртекста $\pi(x)$.

Затем вычисляется факторизация числа n по формуле (17).

$$p = \text{НОД}(|A| \ mod\ n, n);\ q = \frac{n}{p}. \tag{17}$$

Для поиска первой части ключа r_p необходимо сформировать матрицу B, представляющую СЛАУ по формуле (18).

$$B \equiv \begin{pmatrix} -m_1 & y_{11} & y_{12} & \cdots & y_{1d} \\ -m_2 & y_{21} & y_{22} & \cdots & y_{2d} \\ & & & \vdots & \\ -m_{d+1} & y_{(d+1)1} & y_{(d+1)2} & \cdots & y_{(d+1)d} \end{pmatrix} \equiv \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} mod\ p, \tag{18}$$

где m – открытый текст, y – коэффициент многочлена соответствующей степени первой части шифртекста $\pi(x)$.

Затем необходимо найти решение t СЛАУ и вычислить значение первой части ключа r_p по формуле (19).

$$r_p = t^{-1} mod\ p. \tag{19}$$

Чтобы вычислить вторую часть (r_q) ключа, нужно построить аналогичную СЛАУ с единственным отличием – y выбирается, как коэффициент многочлена соответствующей степени второй части шифртекста $\rho(x)$.

Выявленные характерные черты криптосистемы Доминго-Феррера. Для реализации криптосистемы Доминго-Феррера необходимо и достаточно определить её параметры (p, q, d) и произвести следующий набор действий:

1. Генерация ключа.
2. Шифрование.
3. Расшифрование.
4. Гомоморфные операции.

Для реализации других криптосистем, основанных на задаче факторизации чисел необходимо определить аналогичный набор действий и параметров, применительно к реализуемой криптосистеме.

Архитектура системы криптоанализа гомоморфных шифров, основанных на задаче факторизации чисел. При разработке архитектуры системы криптоанализа гомоморфных шифров, основанных на задаче факторизации чисел, учитывались следующие требования:

1. Универсальность – система должна позволять проводить анализ существующих гомоморфных шифров, основанных на задаче факторизации чисел.
2. Модульность и переносимость – система должна состоять из отдельных составных частей (модулей) с высокой связанностью и низким зацеплением.
3. Масштабируемость – система должна позволять добавлять реализации новых атак на гомоморфные шифры, основанные на задаче факторизации чисел.

Исходя из представленных требований, была сформирована архитектура системы, приведенная на рис. 2.

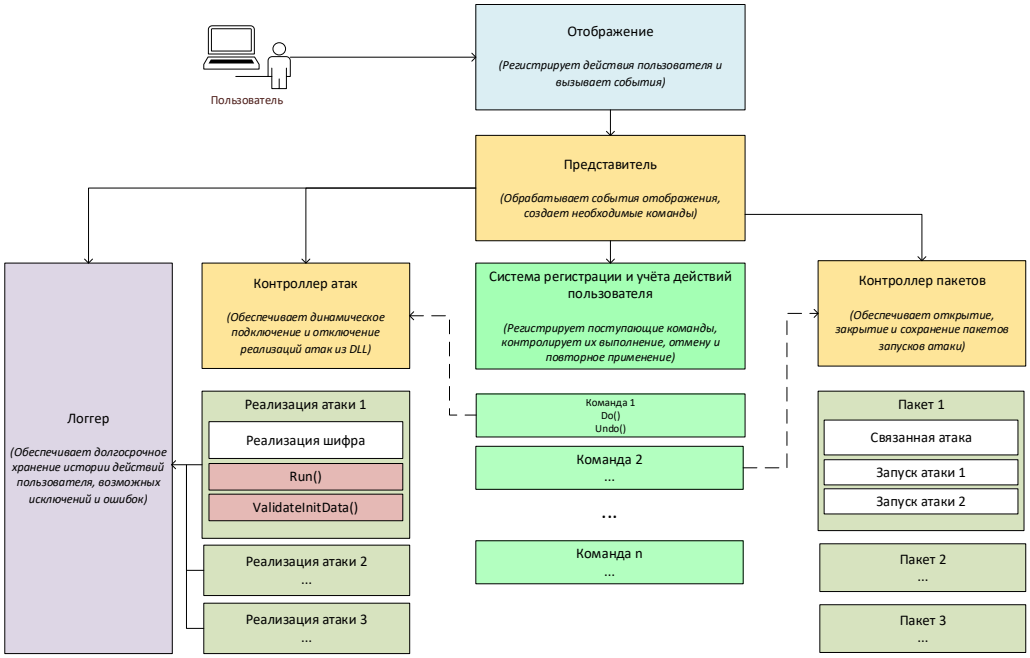

Рис. 2. Архитектура системы криптоанализа

Экземпляр системы криптоанализа, построенный по архитектуре, приведенной на рис. 2 представляет собой ПО, состоящее из:

1. Контроллера атак.
2. Контроллера пакетов запусков.
3. Системы регистрации и учёта действий пользователя.
4. Графического пользовательского интерфейса, построенного по шаблону MVP (Model-View-Presenter) [16].

Покажем на примере атаки с известным открытым текстом на криптосистему Доминго-Феррера как выглядит реализация криптоанализа с применением предложенных средств.

Выбраны следующие параметры:

1) $p = 17$; $q = 13$;
2) $n = p * q = 17 * 13 = 221$;
3) $d = 2$.

В качестве ключа шифрования был выбран ключ $(r_p, r_q) = (5, 4)$ и сформированы 3 пары (открытый текст – шифртекст), приведенные в табл. 1.

Таблица 1

Пары (открытый текст – шифртекст) для проведения атаки с известным открытым текстом на криптосистему Доминго-Феррера

Открытый текст	Шифртекст	
	$\pi(x)$	$\rho(x)$
218	$12x^2 + 3x$	$11x^2 + 8x$
104	$10x^2 + 8x$	$x^2 + 3x$
199	$3x^2 + 5x$	$7x^2 + 11x$

Для поиска первой части ключа r_p сформирована матрица A, приведенная в формуле (20).

$$A = \begin{pmatrix} 218 & 3 & 12 \\ 104 & 8 & 10 \\ 199 & 5 & 3 \end{pmatrix}. \quad (20)$$

Факторизация числа n раскрыта по формулам (21) и (22).

$$p = \text{НОД}(-13498, 221) = 17. \quad (21)$$

$$q = \frac{n}{p} = \frac{221}{17} = 13. \quad (22)$$

Для поиска первой части ключа r_p сформирована матрица Bp, представляющая СЛАУ по формуле (23).

$$Bp \equiv \begin{pmatrix} -14 & 3 & 12 \\ -2 & 8 & 10 \\ -12 & 5 & 3 \end{pmatrix} \equiv \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} mod\ 17. \quad (23)$$

Методом Гаусса найдено решение t СЛАУ Bp по формулам (24) и (25).

$$Bp \equiv \begin{pmatrix} -14 & 3 & 12 \\ -2 & 8 & 10 \\ -12 & 5 & 3 \end{pmatrix} \equiv \begin{pmatrix} -14 & 3 & 12 \\ -13 & 14 & 0 \\ -12 & 5 & 3 \end{pmatrix} mod\ 17. \quad (24)$$

$$14t \equiv 13\ mod\ 17; t \equiv 13 \cdot 14^{-1} mod\ 17 \equiv 13 \cdot 11 \equiv 7\ mod\ 17. \quad (25)$$

Значение первой части ключа r_p вычислено по формуле (26).

$$r_p \equiv t^{-1} mod\ p \equiv 7^{-1}\ mod\ 17\ \equiv 5. \quad (26)$$

Для поиска второй части ключа r_q сформирована матрица Bq, представляющая СЛАУ по формуле (27).

$$Bq \equiv \begin{pmatrix} -14 & 8 & 11 \\ -2 & 3 & 1 \\ -12 & 11 & 7 \end{pmatrix} \equiv \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} mod\ 13. \quad (27)$$

Методом Гаусса найдено решение t СЛАУ Bq по формулам (28) и (29).

$$Bq \equiv \begin{pmatrix} -14 & 8 & 11 \\ -2 & 3 & 1 \\ -12 & 11 & 7 \end{pmatrix} \equiv \begin{pmatrix} -14 & 8 & 11 \\ -5 & 7 & 0 \\ -12 & 11 & 7 \end{pmatrix} mod\ 13. \quad (28)$$

$$7t \equiv 5\ mod\ 13; t \equiv 5 \cdot 7^{-1} mod\ 13 \equiv 5 \cdot 2 \equiv 10\ mod\ 13. \quad (29)$$

Значение второй части ключа r_q вычислено по формуле (30).

$$r_q \equiv t^{-1} mod\ q \equiv 10^{-1}\ mod\ 13\ \equiv 4. \quad (30)$$

Найденный в результате атаки ключ $(r_p, r_q) = (5, 4)$ идентичен ключу, использованному при формировании пар (открытый текст – шифртекст), что доказывает успешность проведенной атаки.

Атаки на гомоморфные шифры, основанные на задаче факторизации чисел могут иметь различные типы и отличаться по сценарию, вследствие чего их невозможно объединить в единый программный модуль. Поэтому система криптоанализа предоставляет

интерфейсы и модули, в рамках которых прикладной программист реализует этапы атаки, представленные в формулах (20)–(30). Система обеспечивает удобные и универсальные механизмы для хранения, отображения и редактирования исходных данных и результатов атак путем создания пакета запусков, связанного с реализацией конкретной атаки. Таким образом, система предоставляет необходимые инструменты для реализации и оценки эффективности методов криптоанализа через программные интерфейсы и модули, что позволяет прикладному программисту сосредоточиться на реализации самой атаки, а не затрачивать время на создание окружения.

Реализация системы криптоанализа гомоморфных шифров, основанных на задаче факторизации чисел, была выполнена на языке программирования C#10 (.NET 6.0) [17, 18].

Основные программные модули, общие для анализа гомоморфных шифров, основанных на задаче факторизации чисел, определяются в ядре приложения, которое не имеет зависимостей от других модулей системы, а также от целевой платформы.

Разработанные прикладным программистом атаки собираются в файлы DLL (Dynamic Link Library), которые затем подключаются к ядру приложения динамически с помощью контроллера атак [19].

Для удобства пользователей взаимодействие с пакетом запусков осуществляется с помощью системы регистрации и учёта действий пользователя (operation-oriented механизм Undo / Redo) [20].

Графический интерфейс системы реализован с помощью шаблона графического пользовательского интерфейса MVP (Model-View-Presenter) [16]. Модель (model) и представитель (presenter) реализованы в ядре, отображение (view) – в отдельном проекте Windows Forms. Поскольку архитектура системы модульная, для переноса системы на другую платформу достаточно создать только отображение для новой платформы без необходимости внесения изменений в другие модули.

Заключение. В данной работе была подробно рассмотрена симметричная криптосистема Доминго-Феррера, проанализирована и проведена атака с известным открытым текстом на эту криптосистему. На примере криптосистемы Доминго-Феррера обоснован набор параметров и функций, общих для гомоморфных шифров, основанных на задаче факторизации чисел с целью определения архитектурных особенностей системы автоматизации выполнения криптоанализа. Сформирована архитектура системы, обеспечивающая удобные и универсальные инструменты для хранения, отображения и редактирования исходных данных и результатов атак.

В качестве шаблона проектирования пользовательского интерфейса был выбран MVP (Model-View-Presenter), разработанный для разделения ответственности в презентационной логике, в результате чего было достигнута простота переноса программного решения на другие платформы.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Короткова Д.А.* Полностью гомоморфное шифрование // Аллея науки. – 2018. – Т. 5, № 5. – С. 1144-1146.
2. *Micciancio D.* A first glimpse of cryptography's Holy Grail // Communications of the ACM. – 2010. – Vol. 53, No. 3. – P. 96-96.
3. *Бабенко Л.К., Буртыка Ф.Б., Макаревич О.Б., Трепачева А.В.* Полностью гомоморфное шифрование (обзор) // Вопросы защиты информации. – 2015. – № 3. – С. 3-26.
4. *Potey M.M., Dhote C.A., Sharma D.H.* Homomorphic Encryption for Security of Cloud Data // Procedia Computer Science. – 2016. – Vol. 100, No. 79. – P. 175-181.
5. *Петренко А.С.* О реализации частично гомоморфной криптосистемы RSA // The 2019 Symposium on Cybersecurity of the Digital Economy-CDE'19. – 2019. – С. 266-268.
6. *Parmar P.V. et al.* Survey of various homomorphic encryption algorithms and schemes // International Journal of Computer Applications. – 2014. – Vol. 91, No. 8.
7. *Brakerski Z., Gentry C., Vaikuntanathan V.* (Leveled) fully homomorphic encryption without bootstrapping // ACM Transactions on Computation Theory (TOCT). – 2014. – Vol. 6, No. 3. – P. 1-36.
8. *Fan J., Vercauteren F.* Somewhat practical fully homomorphic encryption // Cryptology ePrint Archive. – 2012.

9. *Gentry C., Halevi S., Smart N.P.* Better bootstrapping in fully homomorphic encryption // International Workshop on Public Key Cryptography. – Berlin, Heidelberg: Springer Berlin Heidelberg, 2012. – P. 1-16.
10. *Zvika Brakerski.* Fully homomorphic encryption without modulus switching from classical gapsvp // Annual Cryptology Conference. – Springer, 2012. – P. 868-886.
11. *Трепачева А.В.* Улучшенная атака по известным открытым текстам на гомоморфную криптосистему Доминго-Феррера // Тр. Института системного программирования РАН. – 2014. – Т. 26, № 5. – С. 83-98.
12. *Трепачева А.В.* Криптоанализ симметричных полностью гомоморфных линейных криптосистем на основе задачи факторизации чисел // Известия ЮФУ. Технические науки. – 2015. – № 5 (166). – С. 89-102.
13. *Alabdulatif A., Kaosar M.* Privacy preserving cloud computation using Domingo-Ferrer scheme // Journal of King Saud University-Computer and Information Sciences. – 2016. – Vol. 28, No. 1. – P. 27-36.
14. *Cheon J.H., Kim W.H., Nam H.S.* Known-plaintext cryptanalysis of the Domingo-Ferrer algebraic privacy homomorphism scheme // Information Processing Letters. – 2006. – Vol. 97, No. 3. – P. 118-123.
15. *Cheon J.H., Nam H.S.* A cryptanalysis of the original domingo-ferrer's algebraic privacy homomophism // Cryptology EPrint Archive. – 2003.
16. *Kalelkar M., Churi P., Kalelkar D.* Implementation of model-view-controller architecture pattern for business intelligence architecture // International Journal of Computer Applications. – 2014. – Vol. 102, No. 12.
17. *Hejlsberg A. et al.* The C# programming language. – Pearson Education, 2008.
18. *Bahar A.Y. et al.* Survey on Features and Comparisons of Programming Languages (PYTHON, JAVA, AND C#) // 2022 ASU International Conference in Emerging Technologies for Sustainability and Intelligent Systems (ICETSIS). – IEEE, 2022. – P. 154-163.
19. *Нагибин В.А.* Проектирование и реализация системы подключаемых модулей в приложениях на языке C // Путь в науку: прикладная математика, информатика и информационные технологии. – 2023. – С. 27-29.
20. *Мартынов А.* Back/Forward и Undo/Redo в .NET-приложениях // RSDN Magazine. – 2003. – No. 2.

REFERENCES

1. *Korotkova D.A.* Polnost'yu gomomorfnoe shifrovanie [Fully homomorphic encryption], *Alleya nauki* [Science Alley], 2018, Vol. 5, No. 5, pp. 1144-1146.
2. *Micciancio D.* A first glimpse of cryptography's Holy Grail, *Communications of the ACM,* 2010, Vol. 53, No. 3, pp. 96-96.
3. *Babenko L.K., Burtyka F.B., Makarevich O.B., Trepacheva A.V.* Polnost'yu gomomorfnoe shifrovanie (obzor) [Fully homomorphic encryption (review), *Voprosy zashchity informatsii* [Information security issues], 2015, No. 3, pp. 3-26.
4. *Potey M.M., Dhote C.A., Sharma D.H.* Homomorphic Encryption for Security of Cloud Data, *Procedia Computer Science,* 2016, Vol. 100, No. 79, pp. 175-181.
5. *Petrenko A.S.* O realizatsii chastichno gomomorfnoy kriptosistemy RSA [On the implementation of the partially homomorphic RSA cryptosystem], *The 2019 Symposium on Cybersecurity of the Digital Economy-CDE'19,* 2019, pp. 266-268.
6. *Parmar P.V. et al.* Survey of various homomorphic encryption algorithms and schemes, *International Journal of Computer Applications,* 2014, Vol. 91, No. 8.
7. *Brakerski Z., Gentry C., Vaikuntanathan V.* (Leveled) fully homomorphic encryption without bootstrapping, *ACM Transactions on Computation Theory (TOCT),* 2014, Vol. 6, No. 3, pp. 1-36.
8. *Fan J., Vercauteren F.* Somewhat practical fully homomorphic encryption // Cryptology ePrint Archive. – 2012.
9. *Gentry C., Halevi S., Smart N.P.* Better bootstrapping in fully homomorphic encryption, *International Workshop on Public Key Cryptography*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2012, pp. 1-16.
10. *Zvika Brakerski.* Fully homomorphic encryption without modulus switching from classical gapsvp, *Annual Cryptology Conference*. Springer, 2012, pp. 868-886.
11. *Trepacheva A.V.* Uluchshennaya ataka po izvestnym otkrytym tekstam na gomomorfnuyu kriptosistemu Domingo-Ferrera [Improved Known Plaintext Attack on the Domingo-Ferrer Homomorphic Cryptosystem], *Tr. Instituta sistemnogo programmirovaniya RAN* [Proceedings of the Institute of System Programming of the Russian Academy of Sciences], 2014, Vol. 26, No. 5, pp. 83-98.
12. *Trepacheva A.V.* Kriptoanaliz simmetrichnykh polnost'yu gomomorfnykh lineynykh kriptosistem na osnove zadachi faktorizatsii chisel [Cryptanalysis of symmetric fully homomorphic linear cryptosystems based on the problem of factorization of numbers], *Izvestiya YuFU. Tekhnicheskie nauki* [Izvestiya SFedU. Engineering Sciences], 2015, No. 5 (166), pp. 89-102.

13. *Alabdulatif A., Kaosar M.* Privacy preserving cloud computation using Domingo-Ferrer scheme, *Journal of King Saud University-Computer and Information Sciences,* 2016, Vol. 28, No. 1, pp. 27-36.
14. *Cheon J.H., Kim W.H., Nam H.S.* Known-plaintext cryptanalysis of the Domingo-Ferrer algebraic privacy homomorphism scheme, *Information Processing Letters,* 2006, Vol. 97, No. 3, pp. 118-123.
15. *Cheon J.H., Nam H.S.* A cryptanalysis of the original domingo-ferrer's algebraic privacy homomophism, *Cryptology EPrint Archive,* 2003.
16. *Kalelkar M., Churi P., Kalelkar D.* Implementation of model-view-controller architecture pattern for business intelligence architecture, *International Journal of Computer Applications,* 2014, Vol. 102, No. 12.
17. *Hejlsberg A. et al.* The C# programming language. Pearson Education, 2008.
18. *Bahar A.Y. et al.* Survey on Features and Comparisons of Programming Languages (PYTHON, JAVA, AND C#), *2022 ASU International Conference in Emerging Technologies for Sustainability and Intelligent Systems (ICETSIS).* IEEE, 2022, pp. 154-163.
19. *Nagibin V.A.* Proektirovanie i realizatsiya sistemy podklyuchaemykh moduley v prilozheniyakh na yazyke C [Design and implementation of a system of plug-in modules in applications in the C language], *Put' v nauku: prikladnaya matematika, informatika i informatsionnye tekhnologii* [Path to science: applied mathematics, computer science and information technology], 2023, pp. 27-29.
20. *Martynov A.* Back/Forward i Undo/Redo v .NET-prilozheniyakh [Back/Forward and Undo/Redo in .NET applications], *RSDN Magazine* [RSDN Magazine], 2003, No. 2.

Статью рекомендовала к опубликованию д.ф.-м.н. Ф.Б. Тебуева.

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 – e-mail: vstarodubcev@sfedu.ru; тел.: +79996928150; кафедра безопасности информационных технологий им. Макаревича О.Б.; студент.

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 – e-mail: vstarodubcev@sfedu.ru; phone: +79996928150; the Department of Information Technology Security named after Makarevich O.B.; student.

УДК 004.383.3 DOI 10.18522/2311-3103-2024-3-64-70

Д.И. Бакшун, И.И. Турулин

МЕТОДИКА ПОСТРОЕНИЯ СТРУКТУРЫ РЕКУРСИВНОГО ФИЛЬТРА С КОНЕЧНОЙ ИМПУЛЬСНОЙ ХАРАКТЕРИСТИКОЙ В ВИДЕ ФУНКЦИИ, АППРОКСИМИРУЮЩЕЙ ОКНО ХАННА

Фильтры с импульсной характеристикой (ИХ) в виде весовой (сглаживающей) функцией находят применение в абсолютно разных областях цифровой обработки сигналов, таких как спектральный анализ – с целью уменьшения эффекта Гиббса, в формировании амплитудного распределения – для уменьшения уровня боковых лепестков, в том числе для радиотехнических систем с синтезированной апертурой и других. В статье рассмотрена структура рекурсивного КИХ-фильтра (РКИХ-фильтра) с ИХ в виде аппроксимированного окна Ханна при ограниченном фиксированном количестве операций перемножения и суммирования для любой длительности окна. Такая структура имеет существенно меньшую вычислительную сложность по сравнению с классической структурой КИХ-фильтра, и применять её можно во встраиваемых системах с ограниченными вычислительными ресурсами. Функция, аппроксимирующая окно Ханна, представляет собой полином третьей степени, коэффициенты которого рассчитаны с использованием дискретного интегрирования квазисинусной функции. Получена аналитическая формула для коэффициентов нерекурсивной части фильтра путём вычисления обратной конечной разности четвертой степени от аппроксимирующей функции окна Ханна. Коэффициентами нерекурсивной части являются целые числа, значения которых зависят от числа отсчетов (длины) полупериода квазисинусной функции, что упрощает реализацию подобного РКИХ-фильтра на базе программируемой логической интегральной схемы (ПЛИС). Вычислена средняя абсолютная ошибка аппрок-