ОСОБЕННОСТИ РЕАЛИЗАЦИИ СИСТЕМ КРИПТОАНАЛИЗА ГОМОМОРФНЫХ ШИФРОВ, ОСНОВАННЫХ НА ЗАДАЧЕ ФАКТОРИЗАЦИИ ЧИСЕЛ, НА ПРИМЕРЕ КРИПТОСИСТЕМЫ MORE

Бабенко Л. К.[1], Стародубцев В. С.[2]

DOI: 10.21681/2311-3456-2024-3-141-145

Цель работы: *определение общих техник, тактик и процедур для различных методов криптоанализа гомоморфных шифров, основанных на задаче факторизации чисел, и разработка независимой от применяемого метода криптоанализа архитектуры системы для упрощения этого процесса путём предоставления удобного окружения и инструментов.*

Методы исследования: *анализ возможных реализаций архитектурных особенностей при создании систем криптоанализа гомоморфных шифров, основанных на задаче факторизации чисел.*

Объект исследования: *гомоморфные шифры, основанные на задаче факторизации чисел, криптосистема MORE (Matrix Operation for Randomization or Encryption), криптоанализ гомоморфных шифров, основанных на задаче факторизации чисел, особенности архитектуры систем для проведения криптоанализа гомоморфных шифров, основанных на задаче факторизации чисел при различных типах атак.*

Результаты исследования: *разработана архитектура системы криптоанализа для оценки криптостойкости рассматриваемых шифров, основанных на задаче факторизации чисел путём проведения всестороннего анализа уязвимостей для различных атак. На примере атаки с известным открытым текстом на криптосистему MORE, основанную на задаче факторизации чисел, определены общие особенности архитектуры и особенности, свойственные конкретным шифрам, основанным на задаче факторизации чисел, и конкретным типам атак.*

Практическая значимость: *реализация системы криптоанализа на основе предложенной архитектуры позволит исследователям и криптоаналитикам более подробно изучить потенциальные уязвимости в гомоморфных криптосистемах, основанных на задаче факторизации чисел, что позволит разработать более эффективные меры по укреплению стойкости таких шифров.*

Ключевые слова: *Информационная безопасность; конфиденциальная информация; гомоморфное шифрование; криптосистема MORE; криптоанализ; архитектура системы криптоанализа.*

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

Babenko L. K.[3], Starodubcev V. S.[4]

Purpose of the work: *definition of common techniques, tactics and procedures for various methods of cryptanalysis of homomorphic ciphers based on the problem of factorization of numbers, and development of a system architecture independent of the applied cryptanalysis method to simplify this process by providing a convenient environment and tools.*

1 Бабенко Людмила Климентьевна, доктор технических наук, профессор, Южный Федеральный Университет «ЮФУ», Институт компьютерных технологий и информационной безопасности, г. Таганрог, Россия. E-mail: lkbabenko@sfedu.ru

2 Стародубцев Виталий Сергеевич, студент, Южный Федеральный Университет «ЮФУ», Институт компьютерных технологий и информационной безопасности, г. Таганрог, Россия. E-mail: vstarodubcev@sfedu.ru

3 Liudmila Babenko, Dr.Sc., Professor, Southern Federal University «SFedU», Institute of Computer Technologies and Information Security, Taganrog, Russia. E-mail: lkbabenko@sfedu.ru

4 Vitalij Starodubcev, student, Southern Federal University «SFedU», Institute of Computer Technologies and Information Security, Taganrog, Russia. E-mail: vstarodubcev@sfedu.ru

Research methods: *analysis of possible implementations of architectural features in the creation of cryptanalysis systems for homomorphic ciphers based on the problem of number factorization.*

The object of research: *homomorphic ciphers based on the problem of number factorization, cryptosystem MORE (Matrix Operation for Randomization or Encryption), cryptanalysis of homomorphic ciphers based on the problem of number factorization, features of the architecture of systems for cryptanalysis of homomorphic ciphers based on the problem of number factorization in various types of attacks.*

Research results: *the architecture of a cryptanalysis system has been developed to assess the cryptographic strength of the ciphers in question, based on the task of factorizing numbers by conducting a comprehensive vulnerability analysis for various attacks. Using the example of an attack with a known plaintext on the MORE cryptosystem based on the number factorization problem, general architectural features and features peculiar to specific ciphers based on the number factorization problem and specific types of attacks are determined.*

Practical significance: *the implementation of a cryptanalysis system based on the proposed architecture will allow researchers and cryptanalysts to study in more detail potential vulnerabilities in homomorphic cryptosystems based on the problem of number factorization, which will allow developing more effective measures to strengthen the durability of such ciphers.*

Keywords: *Information security; confidential information; homomorphic encryption; cryptosystem MORE; cryptanalysis; architecture of the cryptanalysis system.*

Введение

Гомоморфное шифрование представляет собой метод защиты данных, позволяющий выполнять операции над зашифрованными данными и получать корректный результат, соответствующий операциям, выполненным над открытым текстом [1–3]. В данной статье рассматриваются гомоморфные криптосистемы, основанные на задаче факторизации чисел (Доминго-Феррера[5], Жирова А. О., Жировой О. В., Кренделева С. Ф.[6], MORE[7]), упоминаемые в [4–6]. Особенностью гомоморфных шифров, основанных на задаче факторизации чисел является то, что при их использовании для отражения различных типов атак необходимо иметь информацию о стойкости рассматриваемых шифров, то есть проводить трудоемкий криптоанализ. Разработка разнообразных средств, позволяющих облегчить проведение криптоанализа, является важной задачей. В данной работе рассматриваются актуальная задача разработки системных средств и определение архитектурных особенностей, повышающих эффективность и создающих удобства при оценке стойкости шифров для разных типов атак. Изложение основывается на рассмотрении одной из гомоморфных криптосистем, основанных на задаче факторизации чисел – криптосистеме MORE.

Рассматриваются архитектурные особенности системы криптоанализа, которая обладает универсальностью, предоставляет исследователям необходимое окружение и удобные инструменты и, как следствие, позволит сконцентрироваться на реализации собственных методов криптоанализа, а не тратить время на создание среды для проведения необходимых операций и оценки полученных результатов.

5 Domingo-Ferrer J. A provably secure additive and multiplicative privacy homomorphism //International Conference on Information Security. – Berlin, Heidelberg : Springer Berlin Heidelberg, 2002. – С. 471–483.

6 Жиров А. О., Жирова О. В., Кренделев С. Ф. Безопасные облачные вычисления с помощью гомоморфной криптографии //Безопасность информационных технологий. – 2013. – Т. 20. – №. 1. – С. 6–12.

7 Kipnis A., Hibshoosh E. Efficient methods for practical fully homomorphic symmetric-key encrypton, randomization and verification //Cryptology ePrint Archive. – 2012.

Описание криптосистемы MORE

Данная криптосистема использует шифрование открытых текстов путем их сочетания со случайной обратимой матрицей по модулю RSA в качестве ключа шифрования [7]. Благодаря применению случайного элемента при шифровании, один и тот же открытый текст может иметь разные шифртексты при использовании того же ключа [8].

Для реализации криптосистемы MORE определяются значения p и q, из которых затем формируется труднофакторизуемое число $n = p \cdot q$.

Для формирования секретного ключа необходимо создать обратимую матрицу K размером 2x2 со случайными элементами $k \in Z_n$ по формуле (1).

$$K = \begin{pmatrix} k_{11} & k_{12} \\ k_{21} & k_{22} \end{pmatrix}. \quad (1)$$

Для шифрования открытого текста m необходимо сформировать случайное большое число $s \in Z_n$ по формуле (2).

$$s \xleftarrow{\$} Z_n, \quad (2)$$

где $\xleftarrow{\$}$ является операцией выбора случайного элемента.

Затем открытый текст m и сформированное случайное число s размещаются на главной диагонали матрицы A по формуле (3).

$$A = \begin{pmatrix} s & 0 \\ 0 & m \end{pmatrix}. \quad (3)$$

Шифртекст вычисляется путём умножения матрицы секретного ключа K на закодированный открытый

текст A с последующим умножением полученного результата на обратную матрицу ключа K^{-1} по формуле (4).

$$C = (K \cdot A) \cdot K^{-1}. \quad (4)$$

Важно отметить, что операция умножения матриц в общем случае некоммутативна, поэтому в формуле (4) крайне важно соблюдение порядка действий [9].

Криптосистема MORE определяет следующий перечень гомоморфных операций [6]:

1. Сложение;
2. Умножение;
3. Деление.

Для выполнения сложения достаточно сложить матрицы соответствующих шифртекстов по формуле (5).

$$C_3 = C_1 + C_2, \quad (5)$$

где C_3 – результирующий шифртекст, C_1 – первый шифртекст, C_2 – второй шифртекст.

Для выполнения умножения необходимо умножить матрицы соответствующих шифртекстов по формуле (6).

$$C_3 = C_1 \cdot C_2, \quad (6)$$

где C_3 – результирующий шифртекст, C_1 – первый шифртекст, C_2 – второй шифртекст.

Для выполнения деления необходимо умножить матрицу шифртекста C_1 на обратную матрицу шифртекста C_2 по формуле (7). Деление выполняется только при условии, что определитель матрицы C_2 не равен 0.

$$C_3 = C_1 \cdot C_2^{-1}, \quad (7)$$

где C_3 – результирующий шифртекст, C_1 – первый шифртекст, C_2 – второй шифртекст.

Для расшифрования шифртекста C необходимо умножить обратную матрицу ключа K^{-1} на матрицу шифртекста C, с последующим умножением полученного результата на матрицу секретного ключа K по формуле (8).

$$M = (K^{-1} \cdot C) \cdot K. \quad (8)$$

Поскольку полученный после умножений результат – матрица M размерами 2x2, для получения открытого текста её необходимо раскодировать – извлечь элемент m_{22} по формуле (9).

$$M = \begin{pmatrix} m_{11} & m_{12} \\ m_{21} & m_{22} \end{pmatrix}. \quad (9)$$

Атака с известным открытым текстом на криптосистему MORE

Атака данного типа подразумевает, что криптоаналитик обладает некоторым набором пар (открытый текст, шифртекст), изготовленных на одном ключе [10].

Обозначим K матрицу ключа. Зная, как происходит генерация ключа, можно определить, что элементы главной диагонали ненулевые [11], поэтому справедливо выражение, приведенное в формуле (10).

$$K = D \cdot \begin{pmatrix} 1 & b \\ c & 1 \end{pmatrix}, \quad (10)$$

где D – диагонально обратная матрица.

Поскольку операция умножения для диагональных матриц обладает свойством коммутативности [12], можно составить уравнение, показанное в формуле (11).

$$E_K(m) = K^{-1} \cdot \begin{pmatrix} s & 0 \\ 0 & m \end{pmatrix} \cdot K = \begin{pmatrix} 1 & b \\ c & 1 \end{pmatrix}^{-1} \cdot D^{-1} \cdot \begin{pmatrix} s & 0 \\ 0 & m \end{pmatrix} \cdot \mathrm{D} \cdot = \\ = \begin{pmatrix} 1 & b \\ c & 1 \end{pmatrix}^{-1} \cdot \begin{pmatrix} s & 0 \\ 0 & m \end{pmatrix} \cdot \begin{pmatrix} 1 & b \\ c & 1 \end{pmatrix}, \quad (11)$$

где $E_K(m)$ – операция шифрования открытого текста m на ключе K, s – случайное большое число $s \in Z_n$, сформированное на этапе шифрования.

По условию атаки с известным открытым текстом [13] криптоаналитику известно значение матрицы шифртекста, как показано в формуле (12).

$$E_K(m) = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}. \quad (12)$$

Тогда формула (12) может быть представлена в виде, приведенном в формуле (13).

$$\begin{pmatrix} 1 & b \\ c & 1 \end{pmatrix} \cdot \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = \begin{pmatrix} s & 0 \\ 0 & m \end{pmatrix} \cdot \begin{pmatrix} 1 & b \\ c & 1 \end{pmatrix}; \\ \begin{pmatrix} \alpha+b\gamma & \beta+b\delta \\ c\alpha+\gamma & c\beta+\delta \end{pmatrix} = \begin{pmatrix} s & sb \\ mc & m \end{pmatrix}. \quad (13)$$

Из показанного в формуле (13) уравнения можно выразить значение открытого текста m по формуле (14).

$$m = c\beta + \delta. \quad (14)$$

В формуле (14) для криптоаналитика является неизвестным только значение c, зависящее от ключа шифрования K, которое можно вычислить по формуле (15).

$$c = \frac{m - \delta}{\beta}. \quad (15)$$

Таким образом, для взлома шифра MORE при помощи атаки с известным открытым текстом, криптоаналитику достаточно обладать одной парой (открытый текст – шифртекст).

Описание особенностей архитектуры системы криптоанализа гомоморфных шифров, основанных на задаче факторизации чисел

Исходя из приведенных в формулах (10)–(15) этапов атаки с известным открытым текстом на криптосистему MORE, а также сравнения с другими атаками на шифры, основанные на задаче факторизации чисел, видно, что этапы атаки являются специфичными для конкретной криптосистемы и не могут быть объединены в единый программный модуль. Поэтому система криптоанализа предоставляет лишь интерфейсы, в рамках которых прикладной программист реализует методы криптоанализа.

Однако криптоанализ не ограничивается реализацией конкретных методов. Важными задачами

является выбор, подготовка и хранение исходных данных, отслеживание промежуточных этапов атаки, регистрация временных характеристик, отображение и сохранение результатов. Задачи подобного рода актуальны для различных атак и могут быть автоматизированы путём создания общих программных модулей, объединенных в разработанную систему криптоанализа.

Реализация системы криптоанализа гомоморфных шифров, основанных на задаче факторизации чисел выполнена на языке программирования C#10 (.NET 6.0), поскольку данный язык широко распространен, обеспечивает высокую производительность и эффективное управление ресурсами, интегрируется с другими технологиями Microsoft, такими как ASP.NET, WPF, Xamarin и т. д., что обеспечивает возможность разработки приложений для различных платформ [14].

Архитектура системы криптоанализа состоит из ядра с подключаемыми модулями. Имеется графический пользовательский интерфейс.

Ядро системы – не имеет зависимостей ни от платформы, ни от остальных модулей системы. Определяет программные модули и интерфейсы, общие для различных атак и графического пользовательского интерфейса.

Подключаемые модули реализаций конкретных атак – зависят только от ядра системы. Определяют методы реализации конкретных атак на криптосистемы, основанные на задаче факторизации чисел. Данные модули собираются в файлы DLL (Dynamic Link Library), которые затем подключаются к ядру приложения динамически с помощью контроллера атак [15].

Графический пользовательский интерфейс – зависит от платформы и ядра системы. Отвечает за отображение данных и удобное взаимодействие пользователя с ними.

Ядро системы криптоанализа определяет следующие модули:

1. Контроллер атак – определяет механизм подключения реализаций конкретных атак, собранных в файлы DLL.
2. Контроллер пакетов запусков – управляет созданием, открытием, сохранением, связыванием с реализациями атак и закрытием пакетов запусков. Пакетом запусков именуется набор запусков, связанных с подключенной атакой. Запуск атаки – это исходные данные, с которыми была проведена атака, а также результаты этой атаки (если атака выполнялась).
3. Система регистрации и учёта действий пользователя – контролирует изменения текущего пакета запусков. Любое действие с пакетом представляется объектом типа «команда», определяющим два действия: выполнить и отменить (operation-oriented механизм Undo / Redo) [16]. Первое действие выполняет изменения пакета, запрошенное пользователем, второе – откатывает пакет к предыдущему состоянию. Таким образом, любые изменения пакета являются обратимыми.
4. Логгер – записывает историю всех действий пользователя, а также событий системы в текстовый файл лога с разделением по уровням [17]. Позволяет упростить поддержку системы путем подробной записи информации о возникших исключениях, сообщениях об ошибках с трассировкой стека и предысторией действий пользователя, которая затем может быть использована для определения причины ошибки и её повторного воспроизведения [18].

Графический интерфейс системы реализован с помощью шаблона графического пользовательского интерфейса MVP (Model-View-Presenter) [19]. Модель (model) и представитель (presenter) реализованы в ядре, отображение (view) – в отдельном проекте Windows Forms [20]. Такой подход позволяет перенести систему на другую платформу изменением только одного модуля отображения (view) без необходимости внесения изменений в других модулях.

Пример использования системы для реализации атаки с известным открытым текстом на криптосистему MORE

Продемонстрируем на примере атаки с известным открытым текстом на криптосистему MORE как выглядит реализация криптоанализа с применением предложенных средств.

Пользователь запускает графический интерфейс системы криптоанализа, создает новый пакет запусков. Созданный пакет связывает с реализацией атаки на криптосистему MORE. Далее создает новый запуск и заполняет исходные данные атаки. В качестве примера использовались следующие исходные данные: $p = 13$ и $q = 17$, количество пар (открытый текст – шифртекст) – 1. Введенные пользователем данные проходят валидацию с помощью метода, предусмотренного реализацией атаки. Если данные корректны, пользователь запускает процесс атаки на криптосистему. В системе регистрации и учёта действий пользователя записывается предыдущее состояние, формируется и передается на выполнение соответствующая команда. Графический интерфейс становится неактивным для действий пользователя за исключением компонента, отображающего промежуточные данные в ходе атаки.

В качестве ключа шифрования выбран ключ

$$K = \begin{pmatrix} 49 & 27 \\ 204 & 141 \end{pmatrix}$$

и сформирована одна пара (открытый текст – шифртекст):

$$\left(146, \begin{pmatrix} -391{,}5310 & 102{,}9315 \\ -2237{,}8844 & 574{,}5310 \end{pmatrix}\right).$$

Значение c, зависящее от ключа шифрования K вычислено по формуле (16).

$$c = \frac{m - \delta}{\beta} = \frac{146 - 574{,}5310}{102{,}9315} = -4{,}1633. \qquad (16)$$

Для проверки корректности найденного значения с сформирована другая пара (открытый текст – шифртекст) на том же ключе:

$$\left(121, \begin{pmatrix} -41{,}7388 & 31{,}1627 \\ -677{,}5246 & 250{,}7388 \end{pmatrix}\right).$$

Шифртекст из созданной пары расшифрован с помощью значения с по формуле (17).

$$m' = c\beta + \delta = (-4{,}1633) \cdot 31{,}1627 + 250{,}7388 = 121. \quad (17)$$

Найденное в результате атаки значение c позволяет получить соответствующий открытый текст $m' = m = 121$ (формула (17)), что доказывает успешность проведенной атаки.

По завершении процесса атаки в графическом пользовательском интерфейсе отображаются результаты атаки: временные характеристики проведенной атаки, количество итераций и атомарных операций, а также полная история всех шагов. Кроме того, полученные результаты автоматически сохраняются в пакет запусков для обеспечения возможности просмотра без необходимости повторного запуска атаки.

Выводы

В данной работе проведен анализ симметричной гомоморфной криптосистемы MORE, а также атаки с известным открытым текстом на этот шифр. На основе проведенного исследования на примере криптосистемы MORE определено, какие действия являются специфичными для конкретной криптосистемы, а какие могут быть автоматизированы путём создания общих программных модулей, объединенных в систему криптоанализа гомоморфных шифров, основанных на факторизации чисел.

Представлено описание основных модулей архитектуры системы криптоанализа гомоморфных шифров: ядро, графический пользовательский интерфейс и интерфейс подключаемых модулей. Для каждого модуля системы приводится описание подхода к реализации, а также преимущества применения данного подхода.

Литература

1. *Минаков С. С. Основные криптографические механизмы защиты данных, передаваемых в облачные сервисы и сети хранения данных // Вопросы кибербезопасности. – 2020. – № 3(37). – С. 66–75. DOI: 10.21681/2311-3456-2020-03-66-75*
2. *Гаража А. А., Герасимов И. Ю., Николаев М. В., Чижов И. В. Об использовании библиотек полностью гомоморфного шифрования // International Journal of Open Information Technologies. – 2021. – Т. 9, № 3. – С. 11–22.*
3. *Шачина В. А. Гомоморфная криптография в базах данных // Прикладная математика и информатика: современные исследования в области естественных и технических наук: Материалы V Международной научно-практической конференции (школы-семинара) молодых ученых, Тольятти, 22–24 апреля 2019 года. – 2019. – С. 468–473.*
4. *Hariss K., Noura H., Samhat A. E. An efficient fully homomorphic symmetric encryption algorithm // Multimedia Tools and Applications. – 2020. – Т. 79. – №. 17. – С. 12139-12164. DOI:10.1007/s11042-019-08511-2*
5. *Иванов А. И., Сулавко А. Е. Проект третьего национального стандарта России по быстрому автоматическому обучению больших сетей корреляционных нейронов на малых обучающих выборках биометрических данных // Вопросы кибербезопасности. – 2021. – № 3 (43). – С. 84–93. DOI: 10.21681/2311-3456-2021-3-84-93*
6. *Sana M. U. et al. Enhanced security in cloud computing using neural network and encryption // IEEE Access. – 2021. – Т. 9. – С. 145785–145799. DOI:10.1109/ACCESS.2021.3122938*
7. *Тришин А. Е. Атака Винера и слабые ключи криптосистемы RSA // Дискретная математика. – 2023. – Т. 35. – №. 3. – С. 71–80. DOI: 10.4213/dm1773*
8. *Трепачева А. В. О стойкости гомоморфной криптосистемы Доминго-Феррера против атаки только по шифртекстам // Прикладная дискретная математика. Приложение. – 2023. – № 16. – С. 98–102. DOI: 10.17223/2226308X/16/25*
9. *Гантмахер Ф. Теория матриц. – Litres, 2022. 576 с.*
10. *Горохов Н. Б., Преображенский Ю. П. Об особенностях криптографических систем защиты информации // Молодежь и XXI век-2022. – 2022. – С. 43–46.*
11. *Vaudenay D. V. S. Cryptanalysis of enhanced more //Tatra Mt. Math. Publ. – 2019. – Т. 73. – С. 163-178. DOI: 10.2478/tmmp-2019-0012*
12. *Винберг Э. Курс алгебры. – Litres, 2022. 592 с.*
13. *Yuan Y., Mo Y. L. Security for cyber-physical systems: Secure control against known-plaintext attack // Science China Technological Sciences. – 2020. – Т. 63. – №. 9. – С. 1637–1646. DOI: 10.1007/s11431-020-1621-y*
14. *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. – С. 154-163. DOI: 10.1109/ICETSIS55481.2022.9888839*
15. *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.*
16. *Jeong J., Zeng J., Jung C. Capri: Compiler and architecture support for whole-system persistence // Proceedings of the 31st International Symposium on High-Performance Parallel and Distributed Computing. – 2022. – С. 71-83. DOI: 10.1145/3502181.3531474*
17. *Волушкова В. Л. Многоуровневое логгирование работы процессов и задач // ИТНОУ: информационные технологии в науке, образовании и управлении. – 2021. – №. 1 (17). – С. 60–64. DOI: 10.47501/ITNOU.2021.1.060-064*
18. *Киптенко А. В., Бахарева Н. Ф. Отладка программного обеспечения с помощью лог файлов //Актуальные проблемы информатики, радиотехники и связи. – 2023. – С. 157–158.*
19. *Jánki Z. R., Bilicki V. Rule-Based Architectural Design Pattern Recognition with GPT Models // Electronics. – 2023. – Т. 12. – №. 15. – С. 3364. DOI: 10.3390/electronics12153364*
20. *Pasztaleniec M., Skublewska-Paszkowska M. Comparative analysis of Windows Presentation Foundation and Windows Forms // Journal of Computer Sciences Institute. – 2020. – Т. 14. – С. 26-30. DOI: 10.35784/jcsi.1571*