ЧАСТОТНЫЙ КРИПТОАНАЛИЗ АСИММЕТРИЧНОЙ КРИПТОГРАФИЧЕСКОЙ СИСТЕМЫ, ОСНОВАННОЙ НА ИСКУССТВЕННЫХ НЕЙРОННЫХ СЕТЯХ И ПОМЕХОУСТОЙЧИВОМ КОДИРОВАНИИ ИНФОРМАЦИИ

Козачок А. В.[1], Тарасенко С. С.[2], Козачок А. В.[3]

DOI: 10.21681/2311-3456-2025-2-64-70

Целью написания *данной статьи является описание статистической атаки на асимметричную криптосистему, основанную на искусственных нейронных сетях и помехоустойчивом кодировании информации, а также оценка практической применимости данной системы в современных условиях с учетом возможности проведения подобного вида атак. В тексте работы приводится пошаговая реализация атаки и рассчитывается стойкость системы к данному виду криптоанализа.*

Методология *проводимого исследования заключается в математическом моделировании источника битов с заданными параметрами вероятности, а также анализе статистических характеристик генерируемых им значений.*

Результат: *на основе проведенного анализа выходных значений смоделированного источника авторы исследования выводят формулу для расчета стойкости рассматриваемой асимметричной криптосистемы к описанной атаке. Также они приходят к выводу о том, что рассматриваемая криптосистема в том виде, в котором она существует на данный момент, в современных условиях является крайне неэффективной, не имеет практического применения и представляет исключительно академический интерес. Однако в заключении авторы отмечают, что при возможности ограничения получения нарушителем неограниченного количества пар «открытый текст»/«шифртекст», рассмотренный в данной работе частотный способ криптоанализа будет неприменим. Это даст возможность вновь рассматривать криптосистему как применимую на практике, как минимум, с точки зрения описанного в данной работе частотного криптоанализа.*

Ключевые слова: *частотный криптоанализ, криптографическая стойкость, асимметричная криптография, статистические характеристики, биномиальное распределение, нормальное распределение.*

Введение

На текущий момент научным сообществом активно разрабатываются и исследуются различные постквантовые криптографические схемы и алгоритмы, которые могут быть устойчивы к криптоанализу с использованием квантовых вычислений [1–4].

В частности, к классу потенциально устойчивых к квантовому криптоанализу криптосистем относятся системы, основанные на применении искусственных нейронных сетей (ИНС) [5–8].

Объектом исследования в данной работе является асимметричная криптосистема, основанная на искусственных нейронных сетях и помехоустойчивом кодировании информации, описанная и исследованная в работах [9, 10]. Суть данной системы заключается в имплементировании в нейронной сети одновременного решения двух задач: генерации помехоустойчивых последовательностей и внесения в них некоторого количества битовых ошибок в пределах доступной исправляющей способности. Данная сеть стремится реализовать задачу, схожую с задачей, на сложности которой основана другая постквантовая криптографическая система $McEliece$[4], описание, вариации и сравнение с существующими системами которой приводится в работах [11–13]: декодирование произвольного кода, которая, в свою очередь, является NP-полной задачей[5]. Таким образом, функционирование нейронной сети можно описать следующим выражением:

$$0 \longrightarrow ИНС \longrightarrow c_0 + e_i,$$
$$1 \longrightarrow ИНС \longrightarrow c_1 + e_j,$$

где c_0 и c_1 — базовые помехоустойчивые кодовые бинарные последовательности с исправляющей

1 Козачок Александр Васильевич, доктор технических наук, доцент, профессор кафедры КБ-4 инсти-тута кибербезопасности и цифровых технологий РТУ МИРЭА. Москва, Россия. E-mail: kozachok_a@mirea.ru

2 Тарасенко Сергей Сергеевич, кандидат технических наук, Академия ФСО России. Орёл, Россия. E-mail: dor7la96@mail.ru

3 Козачок Андрей Васильевич, кандидат технических наук, доцент кафедры КБ-4 института кибер-безопасности и цифровых технологий РТУ МИРЭА. Москва, Россия. E-mail: kozachok@mirea.ru

4 McEliece, Robert J. (1978). «A Public-Key Cryptosystem Based on Algebraic Coding Theory». DSN Progress Report. 44: 114–116. Bibcode:1978DSNPR.44.114M.

5 Dinh H., Moore C., Russell A. McEliece and Niederreiter Cryptosystems That Resist Quantum Fourier Sampling At-tacks (англ.) // Advances in Cryptology — CRYPTO 2011: 31st Annual Cryptology Conference, Santa Barbara, CA, USA, August 14–18, 2011, Proceedings / P. Rogaway – Springer-Verlag, 2011. – P. 761–779. – 782 p. – ISBN 978-3-642-22791-2 – doi:10.1007/978-3-642-22792-9_43.

способностью t: Минимальное расстояние Хемминга между ними $d_{\min} \geq 2 \cdot t + 1$ (рис. 1); e_i и e_j — векторы ошибок, которые при каждом запуске ИНС формируются случайным образом вследствие добавления равномерного шума при вычислении значения функции активации некоторых нейронов ИНС. Последовательности c_0 и c_1 являются приватным ключом, компрометация которого приводит к полной компрометации всей системы.

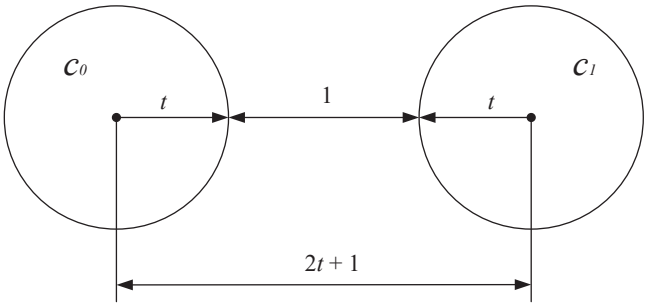

Рис. 1. Минимальное расстояние Хемминга между помехоустойчивыми последовательностями с исправляющей способностью t

Одним из ключевых отличий рассматриваемой системы от криптосистемы *McEliece* является то, что для данной системы количество возможных открытых текстов (это могут быть только бит «0» или бит «1») значительно меньше, чем количество открытых текстов в криптосистеме *McEliece*, число которых определяется с помощью параметра k из набора (n, k, t) используемого помехоустойчивого кода[6]. Так как в рассматриваемой асимметричной криптографической системе нарушитель не ограничен в количестве попыток шифрования информации, то задача собрать большое количество пар «открытый текст»/ /«шифртекст» не является для него сложной. Это, в свою очередь, даёт возможность проведения для рассматриваемой криптосистемы криптоанализа, основанного на подсчёте частоты появления определенных бит в каждом из разрядов помехоустойчивой последовательности с ошибками, сгенерированной ИНС, для каждого из возможных открытых текстов (бита «0» или бита «1»). Данный способ анализа является отличным от типовых способов реализации частотного криптоанализа [14–16], ввиду чего не был изначально представлен и проанализирован в качестве вектора атаки в работе, посвященной исследованию стойкости рассматриваемой криптосистемы [10].

6 Daniel Augot; et al. (7 September 2015). «Initial recommendations of long-term secure post-quantum systems». PQCRYPTO: Post-Quantum Cryptography for Long-Term Security. URL: https://pqcrypto.eu.org/docs/initial-recommendations.pdf.

Методика исследования

Описание частотной атаки

1. Нарушитель генерирует множество шифртекстов $N\_ciphertexts\_0$ для открытого текста «0».

2. Нарушитель генерирует множество шифртекстов $N\_ciphertexts\_1$ для открытого текста «1».

3. Так как количество вносимых ИНС ошибок в помехоустойчивую последовательность всегда меньше половины длины данной последовательности, то в любой момент времени в каждом сгенерированном ИНС шифртексте присутствует $n/2 + 1$ верный бит. Следовательно, *верных бит всегда больше, чем неверных*. Таким образом, накопив большое количество шифртекстов $N\_ciphertexts\_0$ и $N\_ciphertexts\_1$, криптоаналитик может с определенной вероятностью быть уверен, что выбор значения бита в определенном разряде, *согласно мажоритарному правилу,* на основе накопленных статистических данных даст верное значение бита в данном разряде.

4. После нахождения базовых последовательностей c_0 и c_1 криптоаналитик, перехватывая шифртексты, отправляемые от легитимного «отправителя» «получателю», рассчитывает расстояние Хемминга d между перехваченным шифртекстом $ciphertext$ и c_0:

$$d(ciphertext,\ c_0),$$

а также между шифртекстом $ciphertext$ и c_1:

$$d(ciphertext,\ c_0).$$

5. Находит минимальное из этих двух значений:

$$dH_{\min} = \min(d(ciphertext,\ c_0),\ d(ciphertext,\ c_0)).$$

6. Если $dH_{\min} = \min(d(ciphertext,\ c_0)$, то передаваемым открытым текстом является бит «0», если $dH_{\min} = \min(d(ciphertext,\ c_1)$, то передаваемым открытым текстом является бит «1».

Выполнив пункты 1–3 единожды и выполняя пункты 4–6 для каждого перехваченного шифртекста, криптоаналитик способен расшифровывать все предназначающиеся легитимному «получателю» сообщения.

Оценка стойкости криптосистемы с учетом возможности проведения частотной атаки

Для определения возможности применения на практике рассматриваемой системы с учетом возможности реализации описанной атаки необходимо осуществить оценку необходимого количества шифртекстов N, требуемых для определения с заданной вероятностью p_{edge} каждого бита базовых помехоустойчивых последовательностей c_0 и c_1 при их длине, равной n, а количестве возможных ошибок t.

Количество возможных открытых текстов (а, следовательно, и соответствующих им помехоустойчивых

кодовых последовательностей) выразим следующим образом:

$$2^k,$$

где k — длина открытого текста в битах. Для рассматриваемой системы значение k равно 1, так как длина открытого текста равна одному биту.

Строго говоря, события внесения битовых ошибок в различные разряды в рассматриваемой криптосистеме не являются независимыми, так как количество ошибок в n разрядах ограничено количеством t. Подобные процессы описываются с использованием *гипергеометрического распределения*[7], использующегося в тех случаях, когда выбор объектов осуществляется без возвращения.

Однако при больших значениях n можно принять, что в рамках одного независимо взятого разряда серию наблюдений его значений приближенно можно описывать с использованием *биномиального распределения*[8].

В таком случае вероятность того, что ошибка затронет определенный разряд, вычисляется следующим образом:

$$p_{false\_bit} = \frac{t}{n}.$$

При многократном наблюдении за шифртекстами (N сообщений) частота каждого бита в определенном разряде стремится к следующему распределению:

- если *базовый* бит в разряде – «0»:
  - «0» встречается с вероятностью $1 - \frac{t}{n}$,
  - «1» встречается с вероятностью $\frac{t}{n}$;
- если базовый бит в разряде – «1»:
  - «1» встречается с вероятностью $1 - \frac{t}{n}$
  - «0» встречается с вероятностью $\frac{t}{n}$.

Формализуем постановку задачи для определения количества испытаний N, после которых вероятность $p_{decrypt\_bit}$ того, что количество верных бит $true\_bits$ (соответствующих базовому биту базовой последовательности) будет больше, чем количество ложных бит $false\_bits$, будет не менее заданной величины p_{edge}:

$$p_{decrypt\_bit}\,(count(true\_bits) > count(false\_bits)) \geq p_{edge}.$$

Вероятность появления правильного бита p_{true_bit}:

$$p_{true\_bit} = 1 - \frac{t}{n}.$$

Обозначим случайную величину X как *количество появлений верных бит* в определенном разряде среди N испытаний. Она распределена по *биномиальному закону*:

$$X \sim Bin(N, p_{true\_bit}).$$

Таким образом, вероятность получить ровно m правильных бит среди N опытов равна:

$$P(X = m) = \binom{N}{m} p_{true\_bit}^{m}\,(1 - p_{true\_bit})^{N-m}.$$

Необходимо найти минимальное N, при котором выполняется следующее условие:

$$P(X > \frac{n}{2}) \geq p_{edge}.$$

Данная вероятность может быть представлена в виде суммы вероятностей:

$$P(X > \frac{n}{2}) = \sum_{m > N/2}^{N} \binom{N}{m} p_{true\_bit}^{m}\,(1 - p_{true\_bit})^{N-m}.$$

Так как X в нашем случае – это сумма N независимых испытаний Бернулли[9] (выпал «правильный бит» или «ложный бит» и вероятность p_{true_bit} не меняется), то мы имеем право воспользоваться *центральной предельной теоремой*[10], говорящей о том, что при сложении большого количества N независимых случайных величин их сумма приближается к *нормальному распределению*.

Таким образом, если N большое, то справедливо записать следующее:

$$X \approx N(\mu, \sigma^2),$$

где $\mu = N \cdot p_{true\_bit}$ – математическое ожидание (среднее количество появления «верных бит»), $\sigma^2 = N \cdot p_{true\_bit} \cdot (1 - p_{true\_bit})$ – дисперсия биномиального распределения.

Стандартное отклонение σ в таком случае будет равно:

$$\sigma = \sqrt{N \cdot p_{true\_bit} \cdot (1 - p_{true\_bit})}.$$

Далее для простоты расчетов необходимо перейти к *стандартному нормальному распределению*.

Воспользуемся техникой стандартизации случайной величины X и определим переменную Z:

$$Z = \frac{X - \mu}{\sigma}.$$

Так как X приближенно распределена нормально, то после стандартизации Z будет следовать стандартному нормальному распределению:

$$Z \sim N(0, 1),$$

для которого известны табличные значения.

Так как Z является лишь *приведённой к стандартному виду* нормальной случайной величиной X, то справедливо следующее выражение:

$$P(X > \frac{N}{2}) = P(Z > Z_\alpha) = P(\frac{X - \mu}{\sigma} > \frac{\frac{N}{2} - \mu}{\sigma}),$$

7 Rice, John A. (2007). Mathematical Statistics and Data Analysis (Third ed.). Duxbury Press. p. 42.

8 Johnson, N. L., Kotz, S.; Kemp, A. W.: Univariate discrete distributions. Second Edition — John Wiley & Sons 1992, 565 pp.

9 Гмурман В. Е. Теория вероятностей и математическая статистика: учебное пособие для бакалавров. — 12-е изд. Юрайт, 2013. — 478 с. — ISBN 9785991626477, 5991626472.

10 Montgomery, Douglas C.; Runger, George C. (2014). Applied Statistics and Probability for Engineers (6-th ed.). Wiley. p. 241.

где Z_α – критическое значение стандартного нормального распределения, при котором:

$$P(Z > Z_\alpha) = p_{edge}.$$

Тогда:

$$Z_\alpha = \frac{\frac{N}{2} - \mu}{\sigma} = \frac{\frac{N}{2} - \mathrm{N} \cdot p_{true\_bit}}{\sqrt{N \cdot p_{true\_bit} \cdot (1 - p_{true\_bit})}}.$$

Выразим N в явном виде:

$$Z_\alpha \cdot \sqrt{N \cdot p_{true\_bit} \cdot (1 - p_{true\_bit})} = N \cdot (\frac{1}{2} - p_{true\_bit});$$

$$Z_\alpha^{\,2} \cdot \mathrm{N} \cdot p_{true\_bit} \cdot (1 - p_{true\_bit}) = N^2 \cdot (\frac{1}{2} - p_{true\_bit})^2;$$

$$N = \frac{Z_\alpha^{\,2} \cdot p_{true\_bit} \cdot (1 - p_{true\_bit})}{(\frac{1}{2} - p_{true\_bit})^2}.$$

Таким образом, конечная общая формула, показывающая не менее какого количества испытаний N необходимо произвести криптоаналитику для восстановления с использованием мажоритарного правила «верного бита» (при вероятности выпадения «верного бита», равной p_{true_bit}) в определенном разряде, принимает следующий вид:

$$N = \frac{Z_\alpha^{\,2} \cdot p_{true\_bit} \cdot (1 - p_{true\_bit})}{(\frac{1}{2} - p_{true\_bit})^2}. \quad (1)$$

Предположим, что исправляющая способность t последовательностей c_0 и c_1 – максимальная (что является наихудшим сценарием для криптоаналитика), а длина базовых последовательностей равна n. Тогда:

$$t = \frac{n}{2} - 1.$$

С учетом этого формула для расчета N преобразуется следующим образом:

$$p_{true\_bit} = \frac{\frac{n}{2} + 1}{n},\ 1 - p_{true\_bit} = p_{false\_bit} = \frac{\frac{n}{2} - 1}{n};$$

$$N \geq \frac{Z_\alpha^2 \cdot \left(\frac{\frac{n}{2} + 1}{n}\right) \cdot \left(\frac{\frac{n}{2} - 1}{n}\right)}{\left(\frac{\frac{n}{2} + 1}{n} - \frac{1}{2}\right)^2} = \frac{Z_\alpha^2 \cdot \left(\frac{\frac{n}{4} - 1}{n^2}\right)}{Z_\alpha^2};$$

$$N \geq Z_\alpha^2 \cdot (\frac{n^2}{2} - 1). \quad (2)$$

Из данной формулы также можно выразить минимальное значение n, чтобы обеспечить требуемую вероятность:

$$n = \frac{2 \cdot \sqrt{(N + Z_\alpha^2)}}{|Z_\alpha|}. \quad (3)$$

Расширение на случай n бит и 2^k помехоустойчивых последовательностей.

Вероятность P_{edge_n} того, что за N наблюдений анализ, согласно мажоритарному правилу, покажет во всех n разрядах одной помехоустойчивой последовательности правильные биты, можно рассчитать следующим образом:

$$P_{edge\_n} = p_{edge}^{\,n}.$$

Вероятность P_{edge_all} того, что за N наблюдений анализ, согласно мажоритарному правилу, покажет во всех n разрядах всех 2^k последовательностях правильные биты, можно рассчитать следующим образом:

$$P_{edge\_all} = ((p_{edge})^n)^{2^k} = p_{edge}^{\,2^k \cdot n}.$$

Следовательно, чтобы выяснить требуемую для этого вероятность p_{edge}, можно воспользоваться следующей формулой:

$$p_{edge} = \sqrt[2^k \cdot n]{P_{edge\_all}}. \quad (4)$$

Обсуждение результатов исследования

Предположим, что $P_{edge\_all} = 0{,}99$. Тогда:

$$p_{edge} = \sqrt[2 \cdot 1500]{0{,}99} = 0{,}99999665.$$

В таком случае переменная Z_α вычисляется либо по соответствующей таблице для стандартного нормального распределения, либо с использованием *квантильной функции* $\Phi^{-1}(p)$, которая является обратной функцией к функции стандартного нормального распределения и вычисляет *аргумент функции распределения*, которому соответствует заданная вероятность p. Для приведенного выше значения p_{edge} переменная $Z_\alpha \approx 4{,}503$ и формула для расчета n принимает следующий вид:

$$n = 2\,\frac{\sqrt{N + 20{,}277}}{4{,}503}.$$

При фиксированной вероятности p_{edge}, а, следовательно, и значении Z_α, а также больших N, наблюдается следующая взаимосвязь переменных n и N:

$$n \sim \sqrt{N}. \quad (5)$$

Значение N в контексте проводимого частотного криптоанализа можно рассматривать как стойкость криптосистемы, *выраженную в количестве переборных операций*, которые необходимо совершить криптоаналитику для выявления «верного бита» в определенном разряде базовой помехоустойчивой последовательности с заданной вероятностью p_{edge}.

В таком случае для поддержания такой стойкости (чтобы при меньшем значении N вероятность правильно определить бит была менее p_{edge}) длина одной базовой кодовой последовательности должна быть не менее n.

В итоге для обеспечения стойкости системы $\sim 10^{77}$ ($\sim 2^{256}$) длина базовой кодовой последовательности n должна быть $\sim 10^{38}$ бит, что не реализуемо на практике. Если же, например, принять стойкость $\sim 10^{19}$ ($\sim 2^{64}$), то n должна быть $\sim 10^9$ бит, что примерно равняется 125 Мб. Данный сценарий уже

реализуем на практике, однако, помимо обеспечения относительно низкой по современным требованиям стойкости, является крайне неэффективным по сравнению с применением существующих современных асимметричных криптосистем[11].

Заключение

Подводя итоги проведенного в работе анализа, можно констатировать, что рассматриваемая асимметричная криптографическая система, основанная на искусственных нейронных сетях и помехоустойчивом кодировании информации, в том виде, в котором она представлена в работах [9, 10] подвержена статистической атаке, основанной на подсчете количества появлений «верных бит» в определенном разряде кодовой последовательности с ошибками, сгенерированной ИНС. Как показывают расчеты, возможность применения такого вида криптоанализа к данной криптосистеме делает ее непригодной для обеспечения требуемой криптографической стойкости в современных условиях. Таким образом, в текущем виде рассмотренная криптосистема не имеет практического применения и представляет исключительно академический интерес.

Однако, если в ходе дальнейший исследований удастся внести в механизм построения и функционирования криптосистемы модификации, которые обеспечат ограничение по количеству генерируемых шифртекстов для «отправителя», то в таком случае это даст возможность вновь рассматривать криптосистему как применимую на практике. Как минимум, с точки зрения описанного в этой работе способа криптоанализа, ввиду того, что в таком случае он уже будет не применим к данной криптосистеме.

Литература

1. Singh, P., & Chaturvedi, A. (2024). Post-Quantum Cryptography. ArXiv, abs/2402.10576. https://doi.org/10.48550/arXiv.2402.10576.
2. Richter, M., Bertram, M., Seidensticker, J., & Tschache, A. (2022). A Mathematical Perspective on Post-Quantum Cryptography. Mathematics. Vol. 10. Issue 15. P. 2579. https://doi.org/10.3390/math10152579.
3. Bagirovs, E., Provodin, G., Sipola, T., & Hautamäki, J. (2024). Applications of Post-quantum Cryptography. In: Proceedings of the 23rd European Conference on Cyber Warfare and Security. 2024. Vol. 23. No.1. DOI: 10.34190/eccws.23.1.2247.
4. Liu, Y., & Moody, D. (2024). Post-quantum cryptography and the quantum future of cybersecurity. Physical review applied, Vol.21. Issue 4. P. 040501.. https://doi.org/10.1103/physrevapplied.21.040501.
5. Кудакова, В.Ю. Исследование вопросов криптостойкости и методов криптоанализа нейросетевого алгоритма симметричного шифрования / В.Ю. Кудакова // Международная научно-практическая конференция по компьютерной и информационной безопасности (INFSEC 2023): сборник статей, Екатеринбург, 30 июня 2023 года / ООО «Институт цифровой экономики и права». – Екатеринбург: Общество с ограниченной ответственностью «Институт Цифровой Экономики и Права», 2023. – С. 143–146.
6. Liang, Y. (2023). A research on applications of neural network-based cryptography. Applied and Computational Engineering. Vol.7. Issue 3. P. 39. https://doi.org/10.54254/2755-2721/14/20230798.
7. Meraouche, I., Dutta, S., Tan, H., & Sakurai, K. (2021). Neural Networks-Based Cryptography: A Survey. IEEE Access, Vol. 9, P. 124727-124740. https://doi.org/10.1109/ACCESS.2021.3109635.
8. Pal, S., Datta, B., & Karmakar, A. (2022). An Artificial Neural Network Technique of Modern Cryptography. Journal of Scientific Research. https://doi.org/10.3329/jsr.v14i2.55669.
9. Тарасенко С.С. Применение искусственной нейронной сети в качестве односторонней функции с секретом / С.С. Тарасенко. – Текст: непосредственный. // Современная наука: актуальные проблемы теории и практики. Серия «Естественные и технические науки», – г. Москва, 2022. Выпуск № 9. С. 158–166.
10. Тарасенко С.С. Исследование криптостойкости асимметричной криптографической системы, основанной на искусственных нейронных сетях с применением помехоустойчивого кодирования // Телекоммуникации. – 2023. – № 3. – С. 17-31. – DOI 10.31044/1684-2588-2023-0-3-17-31.
11. Wang, R., Wang, Y., & Xie, H. (2021). New McEliece Cryptosystem Based on Polar-LDPC Con-catenated Codes as a Post-quantum Cryptography. 2021 IEEE 21st International Conference on Communication Technology (ICCT), P. 111–116. https://doi.org/10.1109/ICCT52962.2021.9657958.
12. Pratama, P., & Adhitya, G. (2022). Post Quantum Cryptography: Comparison between RSA and McEliece. 2022 International Conference on ICT for Smart Society (ICISS), P. 01–05. https://doi.org/10.1109/ICISS55894.2022.9915232.
13. Makoui, F., Gulliver, T., & Dakhilalian, M. (2024). A McEliece-type Cryptosystem using a Random Inverse Matrix and an Error Vector with Large Hamming Weight. 2024 14th International Confer-ence on Advanced Computer Information Technologies (ACIT), 490–495. https://doi.org/10.1109/ACIT62333.2024.10712631.
14. Лим, В.Г. Исследование частотного криптоанализа шифра Виженера / В.Г. Лим, В.Ю. Чернов // Информационные технологии в моделировании и управлении: подходы, методы, решения: Сборник материалов VII Всероссийской научной конференции с международным участием, Тольятти, 16–18 апреля 2024 года. – Тольятти: Тольяттинский государственный университет, 2024. – С. 284–291.
15. Котов, Ю.А. Средства анализа текстов на основе криптоанализа простой замены / Ю.А. Котов, Д.И. Макарская // Сборник научных трудов Новосибирского государственного технического университета. – 2020. – № 1–2(97). – С. 99–112. – DOI 10.17212/2307-6879-2020-1-2-99-112.
16. L. Tarangga, Arief G. (2020). Letter Frequency In Indonesian Language Using Proportion Estimation. Khazanah (2020): Jurnal Mahasiswa. https://doi.org/10.20885/khazanah.vol12.iss2.art62.

11 Recommendation for Key Management, Special Publication 800-57 Part 1 Rev. 5, NIST, 05/2020.

FREQUENCY CRYPTANALYSIS OF AN ASYMMETRIC CRYPTOGRAPHIC SYSTEM BASED ON ARTIFICIAL NEURAL NETWORKS AND NOISE-RESISTANT INFORMATION CODING

Kozachok A. V.[12], Tarasenko S. S.[13], Kozachok A. V.[14]

Keywords: *frequency cryptanalysis, cryptographic strength, asymmetric cryptography, statistical characteristics, binomial distribution, normal distribution.*

The purpose *of this article is to describe a statistical attack on an asymmetric cryptosystem based on artificial neural networks and noise-resistant information coding, as well as to assess the practical applicability of this system in modern conditions, taking into account the possibility of carrying out this type of attack. The text of the work provides a step-by-step implementation of the attack and calculates the system's resistance to this type of cryptanalysis.*

The methodology *of the study consists of mathematical modeling of a bit source with given probability parameters, as well as an analysis of the statistical characteristics of the values generated by it.*

Based on the analysis of the output values of the simulated source, the authors of the study derive a formula for calculating the resistance of the considered asymmetric cryptosystem to the described attack. They also come to the conclusion that the considered cryptosystem in the form in which it currently exists is extremely ineffective in modern conditions, has no practical application and is of purely academic interest. However, in conclusion, the authors note that if it is possible to limit the intruder's ability to obtain an unlimited number of " plaintext" / " ciphertext" pairs, the frequency cryptanalysis capability considered in this paper will be inapplicable. This will make it possible to consider the cryptosystem again as applicable in practice, at least from the point of view of the frequency cryptanalysis described in this paper.

References

1. Singh, P., & Chaturvedi, A. (2024). Post-Quantum Cryptography. ArXiv, abs/2402.10576. https://doi.org/10.48550/arXiv.2402.10576.
2. Richter, M., Bertram, M., Seidensticker, J., & Tschache, A. (2022). A Mathematical Per-spective on Post-Quantum Cryptography. Mathematics. https://doi.org/10.3390/math10152579.
3. Bagirovs, E., Provodin, G., Sipola, T., & Hautamäki, J. (2024). Applications of Post-quantum Cryptography. ArXiv, abs/2406.13258. https://doi.org/10.34190/eccws.23.1.2247.
4. Liu, Y., & Moody, D. (2024). Post-quantum cryptography and the quantum future of cyber-security.. Physical review applied, 21 4. https://doi.org/10.1103/physrevapplied.21.040501.
5. Kudakova, V. Yu. Issledovanie voprosov kriptostojkosti i metodov kriptoanaliza nejrosetevogo algoritma simmetrichnogo shifrovaniya / V. Yu. Kudakova // Mezhdunarodnaya nauchno-prakticheskaya konferenciya po komp'yuternoj i informacionnoj bezopasnosti (INFSEC 2023): sbornik statej, Ekaterinburg, 30 iyunya 2023 goda / OOO «Institut cifrovoj ekonomiki i prava». – Ekaterinburg: Obshchestvo s ogranichennoj otvetstvennost'yu «Institut Cifrovoj Ekonomiki i Prava», 2023. – S. 143–146. – EDN TVCWQM.
6. Liang, Y. (2023). A research on applications of neural network-based cryptography. Applied and Computational Engineering. https://doi.org/10.54254/2755-2721/14/20230798.
7. Meraouche, I., Dutta, S., Tan, H., & Sakurai, K. (2021). Neural Networks-Based Cryptography: A Survey. IEEE Access, 9, 124727–124740. https://doi.org/10.1109/ACCESS.2021.3109635.
8. Pal, S., Datta, B., & Karmakar, A. (2022). An Artificial Neural Network Technique of Modern Cryptography. Journal of Scientific Research. https://doi.org/10.3329/jsr.v14i2.55669.
9. Tarasenko S. S. Primenenie iskusstvennoj nejronnoj seti v kachestve odnostoronnej funkcii s sekretom / S. S. Tarasenko. – Tekst: neposredstvennyj. // Sovremennaya nauka: aktual'nye problemy teorii i praktiki. Seriya «Estestvennye i tekhnicheskie nauki», – g. Moskva, 2022 g. – vypusk № 9. – S. 158–166.
10. Tarasenko S. S. Issledovanie kriptostojkosti asimmetrichnoj kriptograficheskoj sistemy, os-novannoj na iskusstvennyh nejronnyh setyah s primeneniem pomekho-ustojchivogo kodirovaniya / S. S. Tarasenko // Telekommunikacii – Moskva, 2023 g. – vypusk № 03-2023. – S. 17–31.
11. Wang, R., Wang, Y., & Xie, H. (2021). New McEliece Cryptosystem Based on Polar-LDPC Concatenated Codes as a Post-quantum Cryptography. 2021 IEEE 21st International Conference on Communication Technology (ICCT), 111–116. https://doi.org/10.1109/ICCT52962.2021.9657958.
12. Pratama, P., & Adhitya, G. (2022). Post Quantum Cryptography: Comparison between RSA and McEliece. 2022 International Conference on ICT for Smart Society (ICISS), 01-05. https://doi.org/10.1109/ICISS55894.2022.9915232.

12 Aleksandr Vas. Kozachok, Dr. Sc., Associate Professor, Professor of the Department KB-4 of the Institute of Cyberse-curity and Digital Technologies of the RTU MIREA, Moscow, Russia. E-mail: kozachok_a@mirea.ru
13 Sergey S. Tarasenko, Ph. D., Academy of Federal Guard Service, Oryol, Russia. E-mail: Dor7Ia96@mail.ru
14 Andrey Vl. Kozachok, Ph. D., Associate Professor of the Department KB-4 of the Institute of Cybersecurity and Digi-tal Technologies of the RTU MIREA, Moscow. E-mail: kozachok@mirea.ru

13. Makoui, F., Gulliver, T., & Dakhilalian, M. (2024). A McEliece-type Cryptosystem using a Random Inverse Matrix and an Error Vector with Large Hamming Weight. 2024, 14th International Conference on Advanced Computer Information Technologies (ACIT), 490–495. https://doi.org/10.1109/ACIT62333.2024.10712631.
14. Lim, V.G. Issledovanie chastotnogo kriptoanaliza shifra Vizhenera / V.G. Lim, V.Yu. CHernov // Informacionnye tekhnologii v modelirovanii i upravlenii: podhody, metody, resheniya: Sbornik materialov VII Vserossijskoj nauchnoj konferencii s mezhdunarodnym uchastiem, Tol'yatti, 16–18 aprelya 2024 goda. – Tol'yatti: Tol'yattinskij gosudarstvennyj universitet, 2024. – S. 284–291. – EDN GBPDJE.
15. Kotov, Yu.A. Sredstva analiza tekstov na osnove kriptoanaliza prostoj zameny / Yu.A. Kotov, D.I. Makarskaya // Sbornik nauchnyh trudov Novosibirskogo gosudarstven-nogo tekhnicheskogo universiteta. – 2020. – № 1-2(97). – S. 99–112. – DOI 10.17212/2307-6879-2020-1-2-99-112. – EDN CFSRJB.
16. L. Tarangga, Arief G. (2020). Letter Frequency In Indonesian Language Using Proportion Estimation. Khazanah (2020): Jurnal Mahasiswa. https://doi.org/10.20885/khazanah.vol12.iss2.art62.