УДК 004.738.2

ИСПОЛЬЗОВАНИЕ СОВРЕМЕННЫХ МЕТОДОВ ЗАЩИТЫ ИНФОРМАЦИИ ПРИ ОРГАНИЗАЦИИ ОБМЕНА ДАННЫМИ В СЕТИ

Е. О. Скурихин, Е. В. Ткаченко, Н. С. Мороков, В. В. Следков, О. А. Сафарьян
Донской государственный технический университет (г. Ростов-на-Дону, Российская Федерация)

Наиболее важным аспектом передачи данных в сети является их защита. Как следствие, необходимо установить общий для пользователей секретный ключ. В данной статье рассматривается применение синхронизируемых искусственных нейронных сетей для генерации общего криптографического ключа при создании клиент-серверного приложения. Результатом работы является мессенджер, написанный на языке программирования Python, который реализует принципы сквозного шифрования.

***Ключевые слова*:** нейрокриптография, сквозное шифрование, мессенджер, безопасность, алгоритм AES, алгоритм ДМЧ, обмен ключами, Python.

USE OF MODERN METHODS OF INFORMATION PROTECTION IN THE ORGANIZATION OF DATA EXCHANGE IN THE NETWORK

E. O. Skurihin, E. V. Tkachenko, N. S. Morokov, V. V. Sledkov, O. A. Safaryan
Don State Technical University (Rostov-on-Don, Russian Federation)

The most important aspect of data transmission in the network is its protection and, as a result, the need to establish a common secret key between the users. This article discusses the use of synchronized artificial neural networks for generating a shared cryptographic key for creating client-server application. The result is a messenger written in the Python programming language that implements the principles of end-to-end encryption.

Keywords: neural cryptography, end-to-end encryption, messenger, security, AES algorithm, TPM algorithm, key exchange, Python.

Введение. Организация защищенной передачи данных в сети — один из самых важных аспектов в информационном мире [1,2]. Конститутивным фактором служит современная криптография, основанная на теории чисел.

Безопасность большинства криптографических алгоритмов зависит от факторизации и дискретного логарифмирования. Однако рост вычислительной мощности автоматизированных систем и вероятный потенциал будущих квантовых технологий актуализировали задачу поиска и реализации криптографических схем, не опирающихся на теорию чисел. Раздел криптографии, который изучает применение стохастических алгоритмов для шифрования и криптоанализа, называется нейрокриптография. Один из таких алгоритмов базируется на синхронизации двух нейронных сетей и позволяет получить общий секретный ключ. Суть алгоритма — различить однонаправленную и двунаправленную синхронизацию нейронных сетей.

Основная часть. Цель данной работы — реализация десктопного приложения, содержащего элементы сквозного шифрования с использованием принципов нейрокриптографии и симметричного шифрования. Программный продукт реализован на языке Python 3.7.

Структура мессенджера. Безотказная работа клиент-серверного приложения подразумевает использование строгих правил для обмена пакетами данных. Структура пакета, передаваемого между клиентом и сервером, представляет собой словарь с изменяющимся набором

ключей. Чтобы клиент и сервер выполняли необходимые действия, решено использовать в каждом пакете данных целевой ключ type, который принимает целочисленное значение от 0 до 10. Каждое значение ключа отвечает за необходимый алгоритм поведения приложения.

Список значений целевого ключа для сообщений между клиентом и сервером:

0 — ошибка,
1 — уведомление о присоединении нового пользователя,
2 — уведомление об отключении пользователя,
3 — отправка сообщения всем пользователям,
4 — разрыв соединения с пользователем,
5 — отправка текстового сообщения конкретному пользователю,
6 — отправка запроса на подключение к другому пользователю,
7 — ответ на запрос подключения,
8–9 — вспомогательные запросы для формирования общего ключа,
10 — получение списка пользователей онлайн.

Таким образом, использование специального ключа в каждом пакете данных обеспечивает определенную логику для обмена информацией в клиент-серверном приложении.

Элементы сквозного шифрования в мессенджере. Основная задача мессенджера — поддержка мгновенного обмена зашифрованными сообщениями. Сквозное шифрование — это способ передачи данных, при котором только определенные пользователи имеют доступ к сообщениям. В качестве основы для реализации принципов сквозного шифрования выбран симметричный алгоритм блочного шифрования AES в режиме CBC. Основные достоинства такой модификации:

— постоянная скорость обработки блоков;
— возможность распараллеливания дешифрования;
— отсутствие статистических особенностей, характерных для некоторых режимов работы.

Для реализации алгоритма AES выбран автономный пакет низкоуровневых примитивов PyCryptodome.

Наличие симметричного алгоритма шифрования подразумевает использование некоторого протокола для формирования общего секретного ключа способом, основанным на синхронизации весовых коэффициентов двух искусственных нейронных сетей (ИНС). Такие сети принято называть древовидными машинами четности (ДМЧ). Они соединены открытым каналом связи, а синхронизация достигается благодаря общим случайным воздействиям.

Алгоритм обмена ключами на ДМЧ. ДМЧ — это вид многоуровневой нейронной сети прямого распространения (перцептрона). Такая сеть находится на стороне каждого пользователя и состоит из $K \times N$ входных нейронов, K скрытых нейронов и одного выходного нейрона. Входные нейроны принимают случайные двоичные значения, которые передаются сервером: $x_{ij} \in \{-1, +1\}$. Весовые коэффициенты между входными и скрытыми нейронами изначально инициализируются случайно и принимают значения: $w_{ij} \in \{-L, \dots, 0, \dots, +L\}$. Значение каждого скрытого нейрона рассчитывается как сумма произведений входного значения и весового коэффициента:

$$\sigma_i = sgn(\sum_{j=1}^{N} w_{ij} x_{ij}).$$

Здесь w_{ij} — весовые коэффициенты; x_{ij} — случайные двоичные значения; N — параметр сети; sgn(x) вычисляется по формуле:

$$sgn(x) = \begin{cases} -1, x \le 0 \\ 1, x > 0 \end{cases}.$$

Значение выходного нейрона является произведением всех скрытых нейронов:

$$\tau = \prod_{i=1}^{K} \sigma_i,$$

где σ_i — значение i-го скрытого нейрона; K — параметр сети.

Процесс синхронизации состоит из конечного числа тактов. Цикл синхронизации описан ниже.

1. Сервер генерирует случайный входной вектор.
2. Пользователи вычисляют значения скрытых нейронов и выходного нейрона.
3. Пользователи сравнивают значения выходов. Если они разные, начинается новый цикл синхронизации. Если одинаковые, применяется одно из нескольких правил для преобразования весовых коэффициентов.

Для обновления весовых коэффициентов есть несколько правил [3].

1. Правило Хебба:

$$w_i = w_i + \sigma_i x_i \theta(\sigma_i \tau)\theta(\tau^A \tau^B).$$

2. Антиправило Хебба:

$$w_i = w_i - \sigma_i x_i \theta(\sigma_i \tau)\theta(\tau^A \tau^B).$$

3. Случайное блуждание:

$$w_i = w_i + x_i \theta(\sigma_i \tau)\theta(\tau^A \tau^B).$$

Здесь τ^A, τ^B — значения выходов двух ДМЧ; x_i — случайные двоичные значения на входе; w_i — весовые коэффициенты; $\theta(\sigma_i \tau)$ и $\theta(\tau^A \tau^B)$ — сигмоидальные функции.

Выбор оптимальных параметров ДМЧ. Параметры сетей N, K, L коррелируют со временем синхронизации. Поэтому основные задачи внедрения протокола ДМЧ в схему сквозного шифрования — поиск оптимальной конфигурации ИНС и выбор числа тактов, необходимого для синхронизации. Проведено статистическое исследование, в рамках которого ДМЧ злоумышленника, прослушивая канал связи, пыталась синхронизироваться с двумя ДМЧ пользователей. Устойчивость к такой атаке обеспечивается при $L = 4$, $N \times K = 84$ [4].

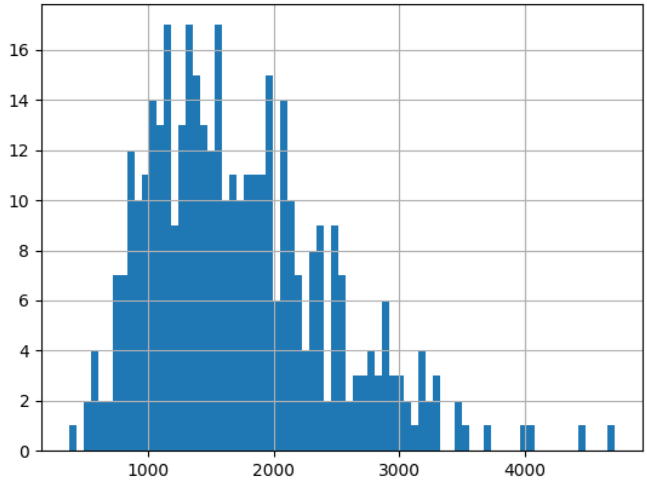
Для количества тактов синхронизации и времени синхронизации двух машин в табл. 1 сведены статистические характеристики: размер выборки, математическое ожидание (МО), среднеквадратическое отклонение (СКО), минимальное значение (мин), 25-й процентиль (25 %), 50-й процентиль (50 %), 75-й процентиль (75 %), максимальное значение (макс).

Таблица 1

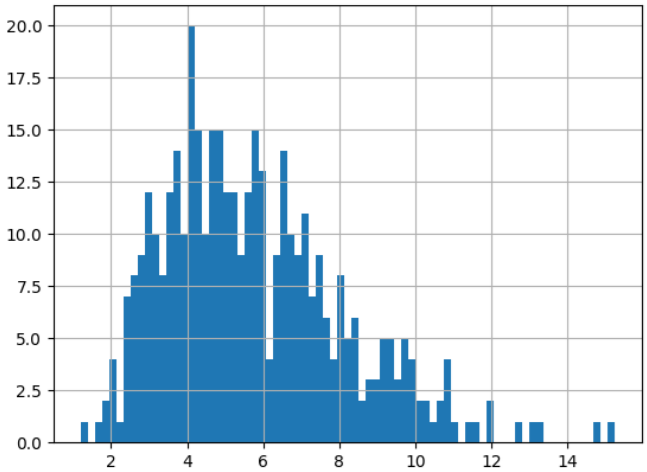
Статистические характеристики

	Размер	**МО**	**СКО**	**Мин**	**25 %**	**50 %**	**75 %**	**Макс**
Такты	400	1723,95	713,31	366,00	1160,50	1611,00	2117,00	4724,00
Время	400	5,74862	2,38588	1,19380	4,03246	5,34745	7,12276	15,2566

На рис. 1 изображены гистограммы для выборки количества тактов синхронизации и для выборки времени синхронизации двух машин.



а)



б)

Рис. 1. Гистограммы числа тактов (*а*) и времени (*б*):

вертикальная шкала — количество успешных синхронизаций

Полученные характеристики позволяют выявить некоторые особенности параметров, влияющие на процесс синхронизации двух ДМЧ. Гистограммы выборок имеют вид смещенного нормального распределения с редкими выбросами. Как показывают значения процентилей, для синхронизации 75 % выборки достаточно 2117 тактов, что соответствует 7,1 секунды. Если для данных параметров *N*, *K*, *L* среднеквадратическое отклонение меньше, чем половина математического ожидания, значит, разброс элементов выборки достаточно мал.

Максимальное значение выборки — это редкий выброс, что может быть связано с неудачно инициализируемыми весовыми коэффициентами или проблемами работы системы, в которой проводилось тестирование. Показатель синхронизации атакующей машины не превышает 64 %. Таким образом, верхнюю границу можно обозначить значением тактов, равным 4800.

Интерфейс приложения для конечного пользователя. На базе программного средства разработан пользовательский интерфейс для мессенджера. После введения уникального имени пользователя появляется окно, изображенное на рис. 2.

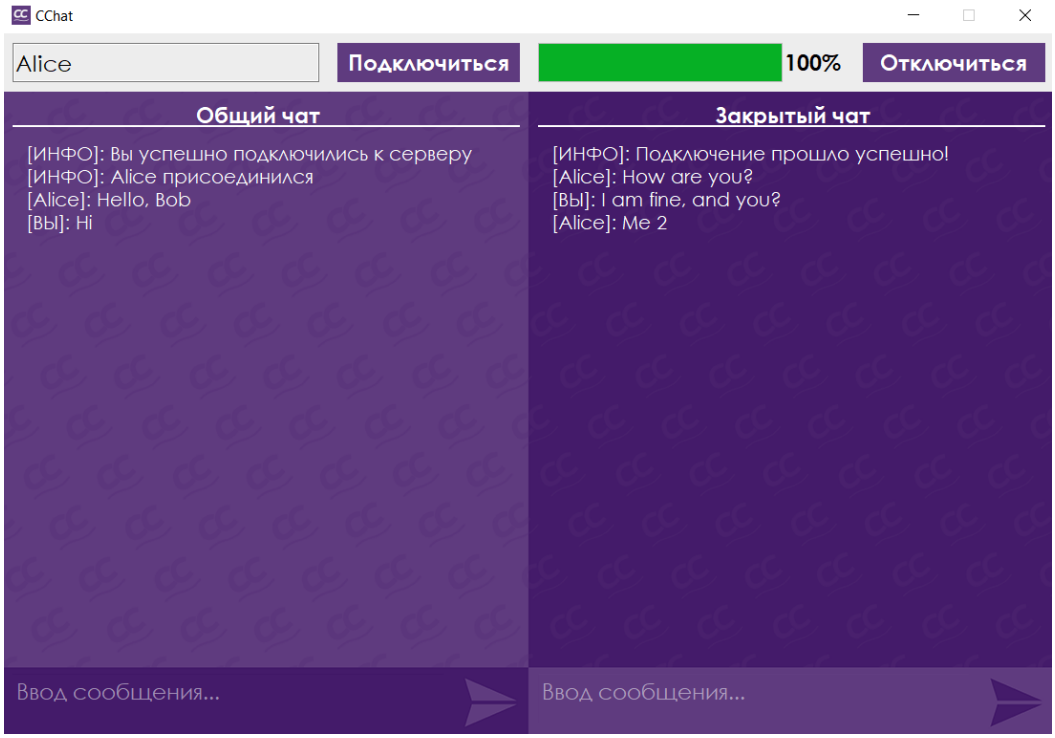


Рис. 2. Пользовательский интерфейс

Слева — окно общего чата и поле для ввода сообщений. В левом верхнем углу — строка для ввода имени пользователя, с которым нужно сформировать общий секретный ключ. После нажатия кнопки «Подключиться» отправляется запрос на синхронизацию ДМЧ для соответствующего пользователя. Если запрос не отклоняется, то начинается процесс синхронизации двух ДМЧ пользователей, о чем свидетельствует индикатор выполнения в правом верхнем углу. После формирования общего секретного ключа появляется возможность писать зашифрованные сообщения. При необходимости прервать общение в закрытом чате пользователь выбирает «Отключиться» в правом верхнем углу. Для выхода из общего чата нужно завершить процесс программы, и остальные пользователи получат уведомление об отключении.

Заключение. В результате проведенной работы с помощью языка программирования Python создано прикладное программное средство, которое позволяет обмениваться зашифрованными сообщениями в сети. В качестве криптографической основы реализован алгоритм генерации общего секретного ключа, использующий стохастические свойства искусственных нейронных сетей, в стеке с симметричным алгоритмом шифрования AES. Реализованное приложение показывает возможность применения вышеперечисленных алгоритмов при организации работы мессенджера. Данное программное средство полностью работоспособно и может использоваться в операционных системах Windows, Linux и MacOS.

Библиографический список

1. Алгоритмическая оценка сложности системы кодирования и защиты информации, основанной на пороговом разделении секрета, на примере системы электронного голосования / Л. В. Черкесова, О. А. Сафарьян, А. В. Мазуренко, Н. С. Архангельская // Вестник Донского государственного технического университета . 2017. — Т. 17, № 3. — С. 145–155. https://doi.org/10.23947/1992-5980-2017-17-3-145-155

2. Сравнительный анализ систем мгновенного обмена сообщениями / Г. А. Положий, А. Р. Тосунова, О. А. Сафарьян, Л. В. Черкесова // Молодой исследователь Дона : [сайт]. — 2020.

— № 4 (25). — С. 59–63. — URL: https://mid-journal.ru/upload/iblock/be8/11_1143-Polozhiy_59_63.pdf (дата обращения 05.05.2021).

3. Червяков, Н. И. Применение искусственных нейронных сетей и системы остаточных классов в криптографии / Н. И. Червяков, А. И. Галушкин, А. А. Евдокимов. — Москва : Физматлит, 2012. — 280 с.

4. Голиков, В. Ф. Атака на синхронизируемые искусственные нейронные сети, формирующие общий секрет, методом отложенного перебора / В. Ф. Голиков, А. Ю. Ксеневич // Доклады БГУИР. — 2017. — № 8 (110). — С. 48–53.

Об авторах

Скурихин Егор Олегович, студент Донского государственного технического университета (344003, РФ, г. Ростов-на-Дону, пл. Гагарина, 1), egorskurihin@gmail.com.

Ткаченко Евгений Васильевич, студент Донского государственного технического университета (344003, РФ, г. Ростов-на-Дону, пл. Гагарина, 1), zeka.tkach1@gmail.com.

Мороков Никита Сергеевич, студент Донского государственного технического университета (344003, РФ, г. Ростов-на-Дону, пл. Гагарина, 1), vunderkinder99@gmail.com.

Следков Владислав Валерьевич, студент Донского государственного технического университета (344003, РФ, г. Ростов-на-Дону, пл. Гагарина, 1), vladislavsledkov@gmail.com.

Сафарьян Ольга Александровна, доцент кафедры «Кибербезопасность информационных систем» Донского государственного технического университета (344003, РФ, г. Ростов-на-Дону, пл. Гагарина, 1), кандидат технических наук, доцент, safari_2006@mail.ru.

Authors:

Skurikhin, Egor O., Student, Department of Cybersecurity of Information Systems, Don State Technical University (1, Gagarin sq., Rostov-on-Don, RF, 344003), egorskurihin@gmail.com

Tkachenko, Evgeniy V., Student, Department of Cybersecurity of Information Systems, Don State Technical University (1, Gagarin sq., Rostov-on-Don, RF, 344003), zeka.tkach1@gmail.com

Morokov, Nikita S., Student, Department of Cybersecurity of Information Systems, Don State Technical University (1, Gagarin sq., Rostov-on-Don, RF, 344003), vunderkinder99@gmail.com

Sledkov, Vladislav V., Student, Department of Cybersecurity of Information Systems, Don State Technical University (1, Gagarin sq., Rostov-on-Don, RF, 344003), vladislavsledkov@gmail.com

Safaryan, Olga A., Associate professor, Department of Cybersecurity of Information Systems, Don State Technical University (1, Gagarin sq., Rostov-on-Don, RF, 344003), Cand. Sci., Associate professor, safari_2006@mail.ru