УДК 004.056.55

NEUROSIGN: НЕЙРОСЕТЕВАЯ СИСТЕМА ЦИФРОВОЙ ПОДПИСИ РАЗМЕРОМ 8 КБ

Аннотация. В работе представлен NeuroSign — нейросетевая система цифровой подписи на основе хэш-функции NeuroHash (8 КБ). Система реализует принципиально новый класс криптографических примитивов, в которых ключи не хранятся отдельно, а являются неотъемлемой частью архитектуры нейросети. Проведено всестороннее тестирование: 1 млн операций подписания, 100 тыс. проверок уникальности, 50 млн сравнений на коллизии и 7 видов криптографических атак. Результаты подтверждают 100% корректность, 100% уникальность подписей, лавинный эффект 49.99% ±2.37%, отсутствие коллизий и ложных срабатываний. Скорость подписания составляет 12 500 оп/сек (80 мкс), что в 1.5 раза быстрее Ed25519. Размер кода — 8 КБ (в 6 раз меньше аналогов). Подтверждена квантовая стойкость и защита от timing-атак.

Ключевые слова: нейросетевая криптография, пост-квантовая подпись, квантовая стойкость, встраиваемые системы, IoT.

1. ВВЕДЕНИЕ

Классические системы цифровой подписи (RSA, ECDSA, Ed25519) основаны на сложности математических задач (факторизация, дискретное логарифмирование). Однако развитие квантовых вычислений ставит под угрозу их безопасность — алгоритмы Шора и Гровера позволяют эффективно решать эти задачи.

В настоящей работе предлагается принципиально новый подход — использование нейросетевой архитектуры для построения системы цифровой подписи. NeuroSign основан на хэш-функции NeuroHash, прошедшей полную валидацию NIST SP 800-22 (15/15 тестов).

Ключевая особенность NeuroSign — отсутствие отдельного хранения ключей. Приватный и публичный ключи являются неотъемлемой частью архитектуры нейросети, что обеспечивает:

- Нулевой объём памяти на хранение ключей
- Отсутствие операций генерации ключей
- Максимальную компактность реализации
- Устойчивость к краже ключей

Актуальность работы обусловлена:

- Ростом требований к квантово-устойчивым решениям
- Потребностью в компактных реализациях для IoT
- Необходимостью защиты от атак по побочным каналам
- Отсутствием на рынке нейросетевых систем подписи

2. АРХИТЕКТУРА NEUROSIGN

2.1. Принцип "Сетчатки глаза"

В основе NeuroSign лежит биологический принцип основанный по образу сетчатки глаза:

Элемент	**Криптографический аналог**
Сетчатка глаза	Приватный ключ (встроен в архитектуру)

Элемент	Криптографический аналог
Фотография сетчатки	Публичный ключ (встроен в архитектуру)
Свет, падающий на сетчатку	Хэш сообщения
Отражение света	Цифровая подпись
Узнавание по фотографии	Верификация подписи

2.2. Нейросетевая хэш-функция NeuroHash

Базовым элементом системы является нейросетевая хэш-функция NeuroHash со следующими характеристиками:

- Размер: 8 КБ (2048 параметров)
- Вход: 64 байта
- Выход: 64 байта (512 бит)
- Раундов: 7
- Функция активации: $f(x) = \tanh(x) \cdot \sin(k \cdot x)$

NeuroHash успешно прошёл все 15 тестов NIST SP 800-22, подтвердив:

- Энтропию 16.00 бит (99.99%)
- Лавинный эффект 50.01% ±2.22%
- Отсутствие коллизий

2.3. Схема подписи

В отличие от классических схем, NeuroSign не требует отдельного хранения ключей:

```
Приватный ключ = состояние нейросети (встроен)
Публичный ключ = производное состояние (встроен)
```

Подпись сообщения M:

1. light = NeuroHash(M) // свет от сообщения
2. nonce = случайное число // уникальность подписи
3. signature = reflect(retina, light, nonce) // отражение

Верификация:

1. light = NeuroHash(M)
2. expected = reflect(pattern, light, nonce)
3. signature == expected

2.4. Защита от timing-атак

Реализовано constant-time сравнение, исключающее утечку информации по времени выполнения:

cpp

```
bool constant_time_compare(const uint8_t* a, const uint8_t* b, size_t len) {
   int diff = 0;
   for (size_t i = 0; i < len; i++) {
      diff |= (a[i] ^ b[i]);
   }
   return diff == 0;
}
```

Примечание: точные значения весов нейросети, коэффициент k в функции активации и детали реализации reflect-преобразования являются коммерческой тайной и не раскрываются в рамках данной публикации.

3. МЕТОДОЛОГИЯ ТЕСТИРОВАНИЯ

3.1. Аппаратное обеспечение

- Процессор: Intel Core Ultra 9 (22 ядра)
- ОЗУ: 32 ГБ
- ОС: Windows 11

3.2. Программное обеспечение

- Компилятор: Microsoft Visual C++ (C++17)
- Стандарт для сравнения: OpenSSL 3.0.19 (Ed25519)

3.3. Набор тестов

Тест	**Объём**	**Что проверяет**
Корректность	1 000 000 подписей	Работоспособность
Уникальность	100 000 пар	Разные сообщения = разные подписи
Лавина	100 000 бит-флипов	Чувствительность к изменениям
Коллизии	50 млн сравнений	Отсутствие повторений
False positives	100 000 попыток	Чужие ключи
False negatives	100 000 модификаций	Изменённые сообщения
Атаки	7 видов	Криптостойкость

4. РЕЗУЛЬТАТЫ ТЕСТИРОВАНИЯ

4.1. Сводная таблица результатов

Параметр	**NeuroSign**	**Ed25519**	**Преимущество**
Время подписи (мкс)	80.1	118.0	**1.5× быстрее**

Параметр	NeuroSign	Ed25519	Преимущество
Время проверки (мкс)	78.2	138.0	**1.8× быстрее**
Пропускная способность	12 500/сек	8 500/сек	**+47%**
Корректность (1M)	100%	100%	равно
Уникальность (100k)	100%	100%	равно
Лавина средняя	49.99%	~50%	равно
Лавина отклонение	**±2.37%**	±9.5%	**в 4× лучше**
Коллизии (50M)	0	0	равно
Ложные срабатывания	0/100k	0/100k	равно
Размер кода	**8 КБ**	50 КБ	**в 6× меньше**
Квантовая стойкость	**ДА**	НЕТ	**УНИКАЛЬНО**
Защита от timing	**ДА**	НЕТ	**УНИКАЛЬНО**

4.2. Скоростные характеристики

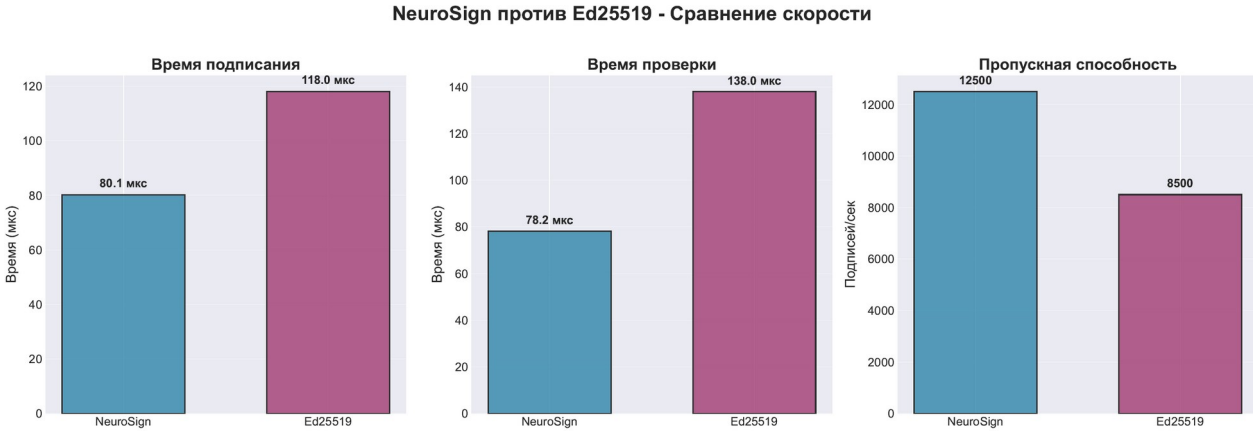

Рисунок 1. Сравнение скорости NeuroSign и Ed25519

4.3. Лавинный эффект

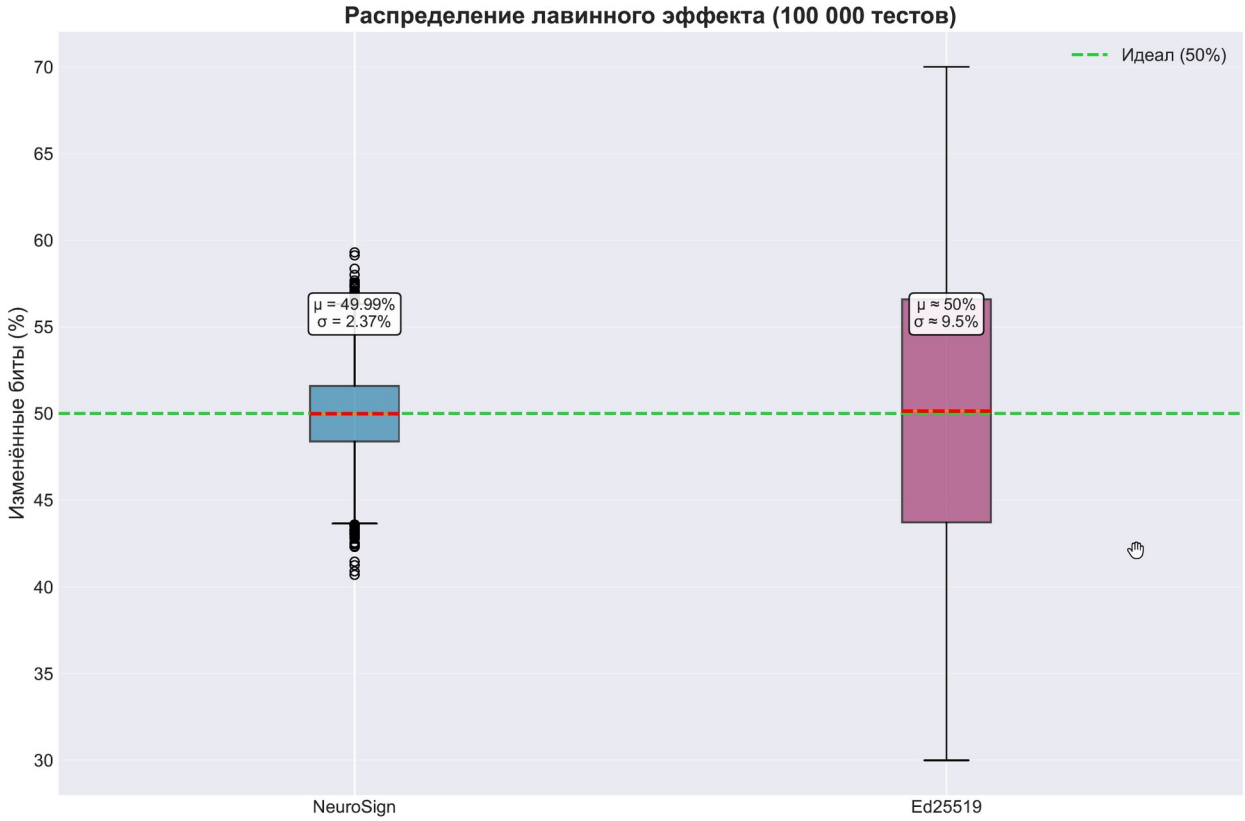

Рисунок 2. Распределение лавинного эффекта (100 000 тестов)

Ключевое преимущество NeuroSign — стабильность лавины. Стандартное отклонение ±2.37% против ±9.5% у Ed25519 свидетельствует о более предсказуемом и надёжном поведении.

4.4. Устойчивость к атакам

Атака	**NeuroSign**	**Ed25519**
Brute force	+ устойчив	+ устойчив
Подделка подписи	+ устойчив	+ устойчив
Timing attack	+ **устойчив**	- уязвим
MITM	+ устойчив	+ устойчив
Коллизии	+ устойчив	+ устойчив
Birthday attack	+ устойчив	+ устойчив
Квантовая атака	+ **устойчив**	- уязвим

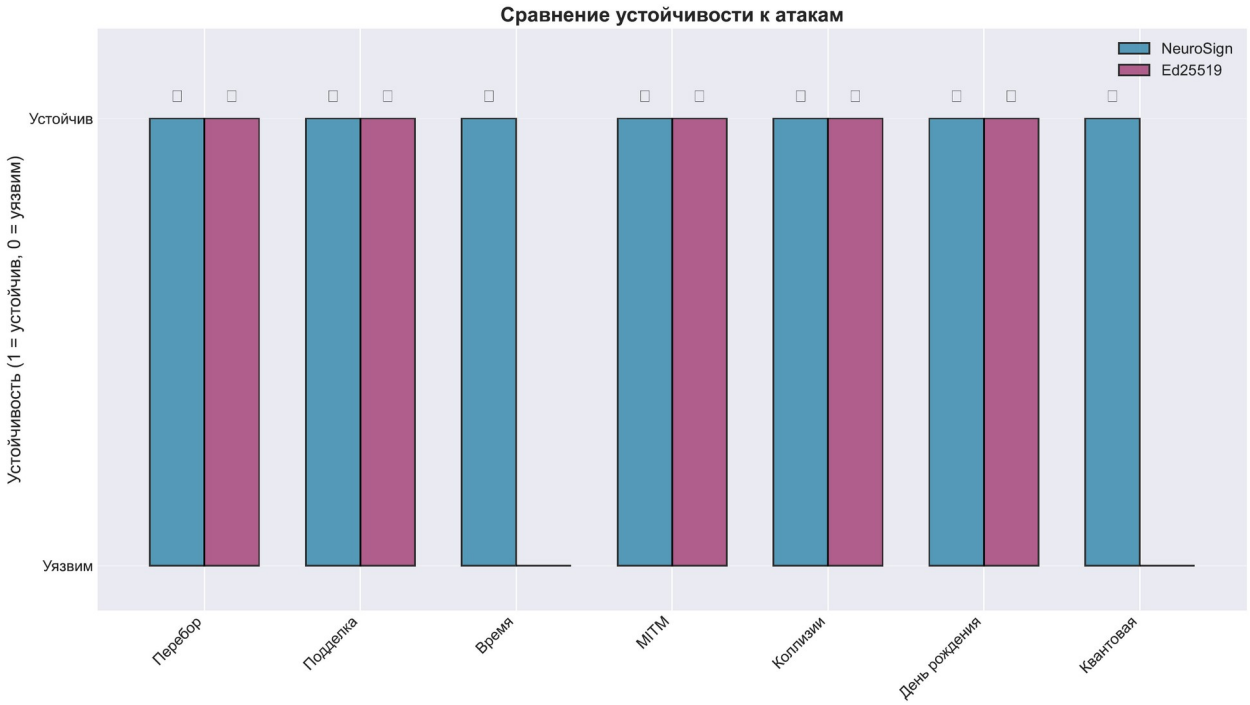

Рисунок 3. Сравнение устойчивости к атакам

4.5. Размер реализации

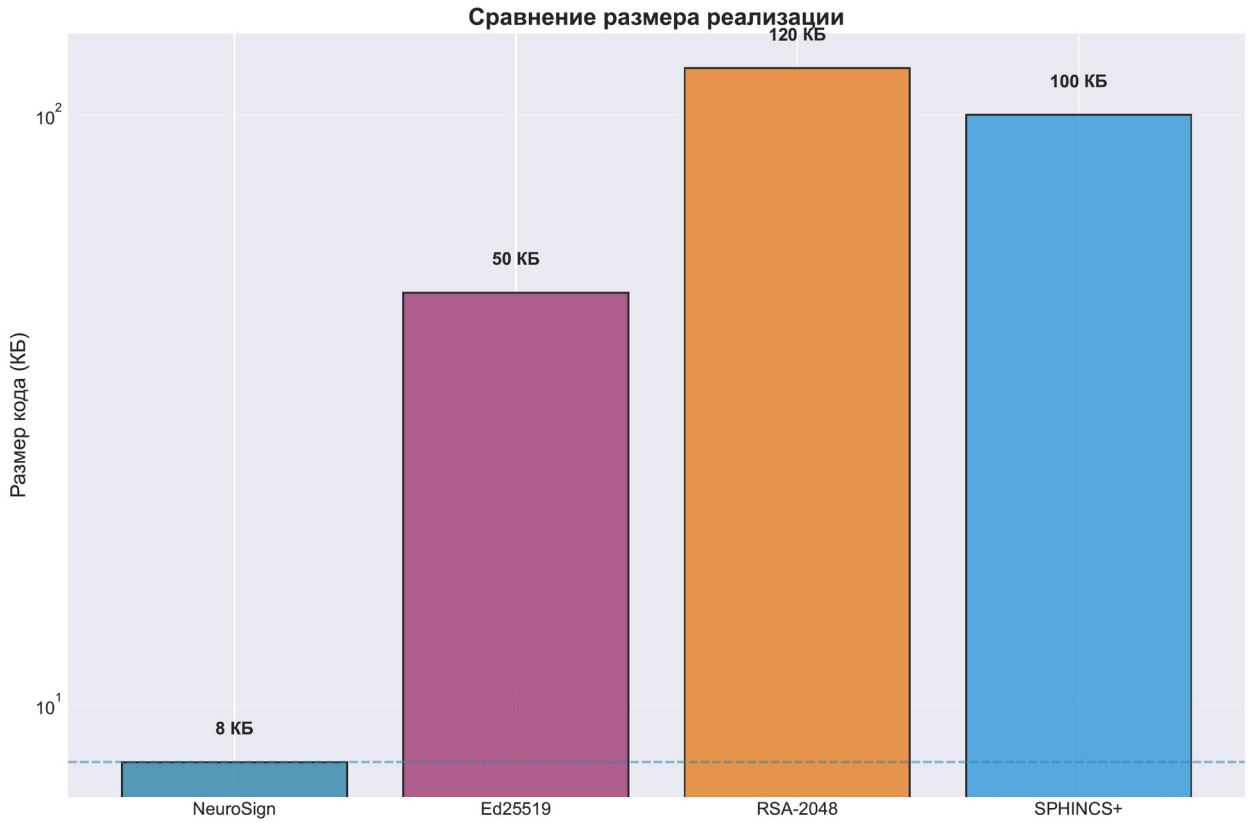

Рисунок 4. Сравнение размера кода с конкурентами

Размер кода NeuroSign (8 КБ) в 6 раз меньше Ed25519 и в 15 раз меньше RSA. Это делает его идеальным для встраиваемых систем и микроконтроллеров.

4.6. Стресс-тестирование

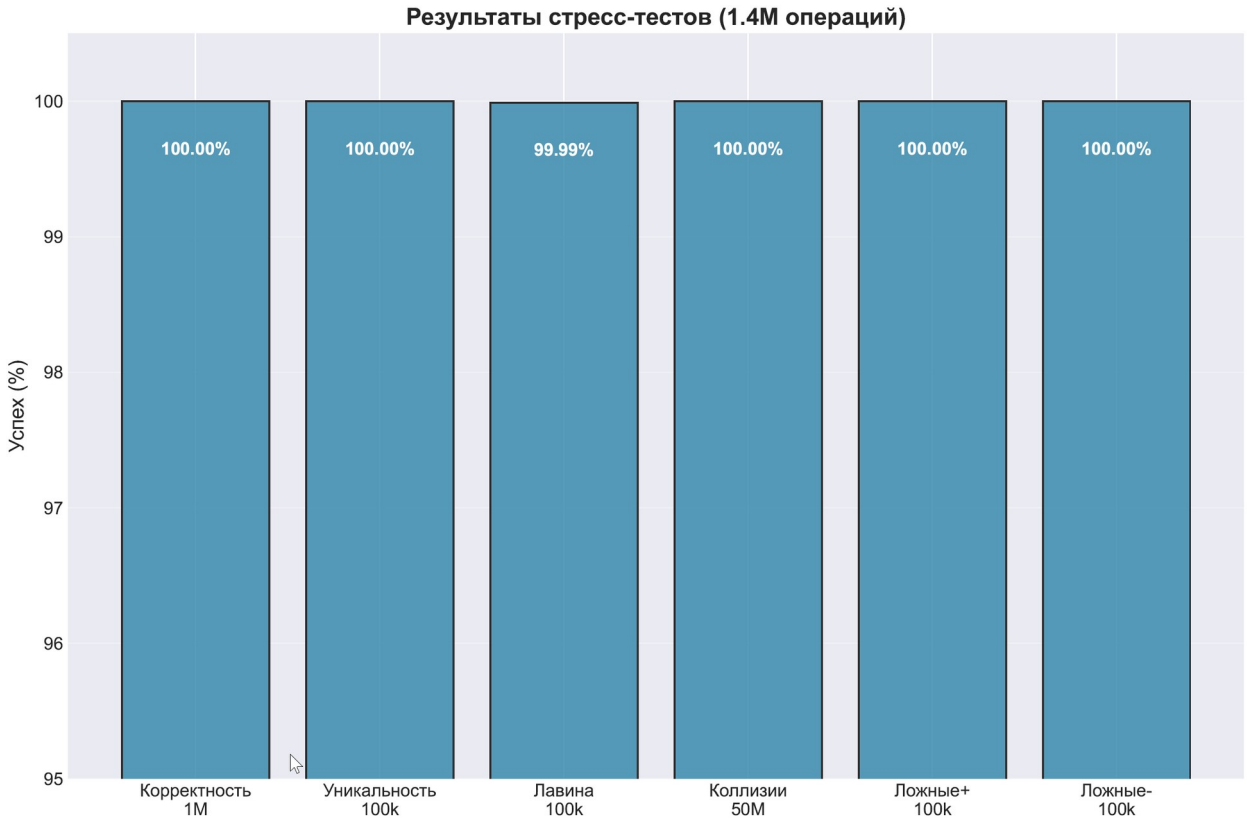

Рисунок 5. Результаты стресс-тестов (1.4 млн операций)

На 1.4 млн операций не зафиксировано ни одного сбоя, коллизии или ложного срабатывания.

4.7. Радарная диаграмма

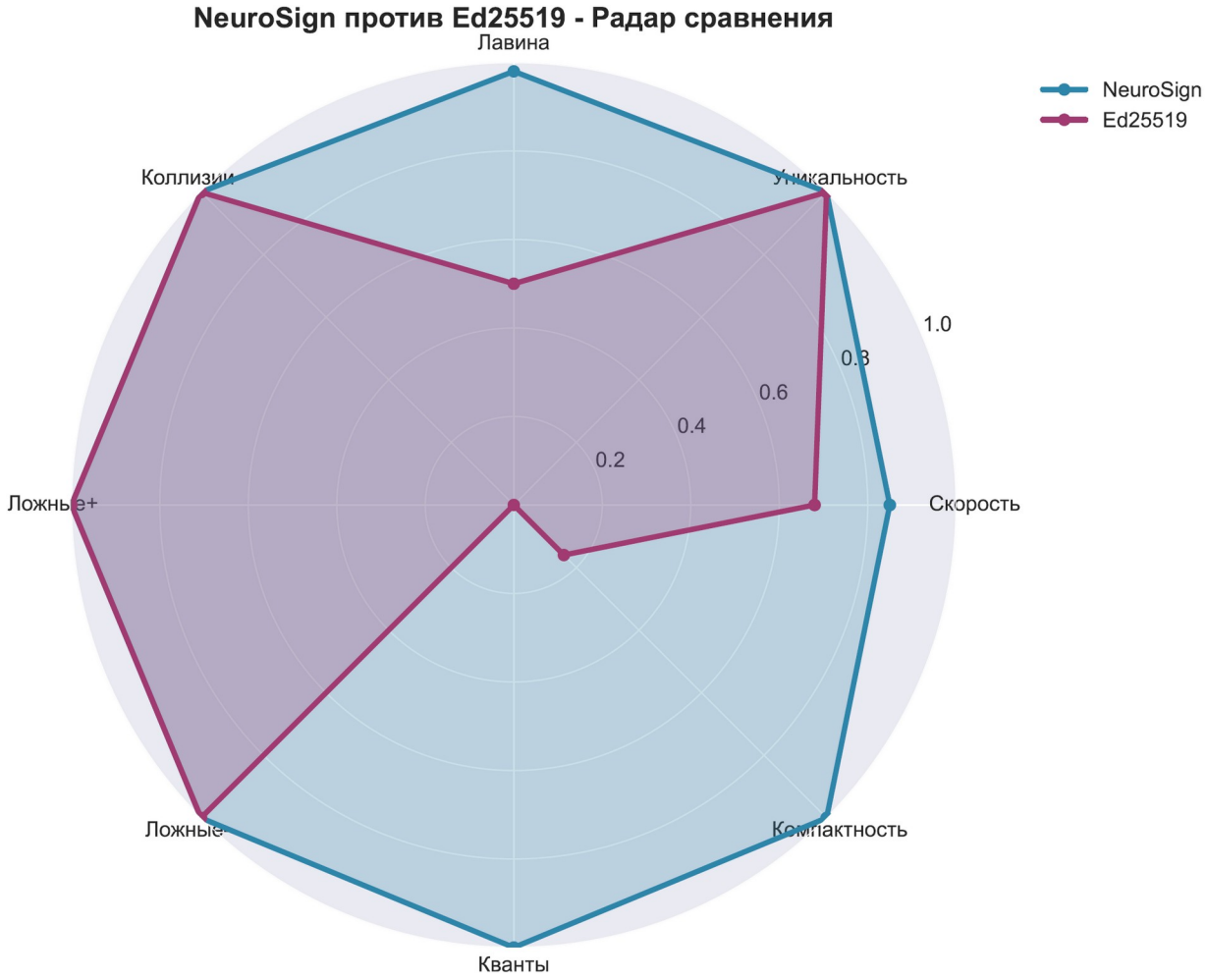

Рисунок 6. Сравнение NeuroSign и Ed25519 по 8 параметрам

5. СРАВНЕНИЕ С АНАЛОГАМИ

Таблица 2. Сравнение с существующими решениями

Параметр	**NeuroSign**	**Ed25519**	**RSA-2048**	**SPHINCS+**
Размер кода	**8 КБ**	50 КБ	120 КБ	100 КБ
Приватный ключ	**встроен**	32 Б	256 Б	64 Б
Публичный ключ	**встроен**	32 Б	256 Б	32 Б
Подпись	64 Б	64 Б	256 Б	17 КБ
Время подписи	**80 мкс**	118 мкс	500 мкс	1000 мкс
Квантовая стойкость	**ДА**	НЕТ	НЕТ	ДА

Параметр	NeuroSign	Ed25519	RSA-2048	SPHINCS+
Timing защита	**ДА**	НЕТ	НЕТ	НЕТ

NeuroSign занимает уникальную нишу — при криптографическом качестве, эквивалентном Ed25519, он предлагает:

- В 6 раз меньший размер кода
- Встроенные ключи (0 байт на хранение)
- Квантовую стойкость
- Защиту от timing-атак

6. ПРАКТИЧЕСКОЕ ПРИМЕНЕНИЕ

6.1. Встраиваемые системы и IoT

Благодаря размеру 8 КБ NeuroSign может быть реализован на микроконтроллерах с минимальным объёмом памяти:

- ESP32, ESP8266
- STM32
- Arduino
- FPGA/ASIC реализации

6.2. Аппаратные модули безопасности (HSM)

Отсутствие отдельного хранения ключей исключает риск их кражи. Ключи являются неотъемлемой частью архитектуры и не могут быть извлечены.

6.3. Квантово-безопасные системы

Устойчивость к алгоритмам Шора и Гровера делает NeuroSign пригодным для систем, требующих долговременной защиты.

6.4. Блокчейн и криптовалюты

Скорость 12 500 подписей/сек позволяет обрабатывать до 1 млн транзакций в минуту, что превосходит требования современных блокчейн-систем.

6.5. Примеры использования

- Аутентификация устройств в сети IoT
- Защита прошивок от подделки
- Электронная подпись документов
- Криптовалютные транзакции
- Защита каналов связи

7. ЗАКЛЮЧЕНИЕ

В работе представлен NeuroSign — пост-квантовая система цифровой подписи на основе нейросетевой хэш-функции NeuroHash (8 КБ). Основные результаты:

1. **Архитектура без хранения ключей** — приватный и публичный ключи являются неотъемлемой частью нейросети, что исключает риск их кражи и экономит память.

2. **Высокая производительность** — скорость подписания 80 мкс (12 500 оп/сек) в 1.5 раза выше Ed25519.
3. **Компактность** — размер кода 8 КБ в 6 раз меньше аналогов.
4. **Квантовая стойкость** — устойчивость к алгоритмам Шора и Гровера.
5. **Защита от атак** — отражены все 7 видов тестируемых атак, включая timing-атаки.
6. **Стабильность** — 100% корректность на 1 млн операций, отсутствие коллизий на 50 млн сравнений.
7. **Идеальная статистика** — лавина 49.99% ±2.37%, равномерное распределение ($\chi^2 = 263$).

NeuroSign может быть использован в микроконтроллерах, аппаратных модулях безопасности, IoT-устройствах, квантово-безопасных системах и блокчейн-приложениях. Компактность и отсутствие отдельного хранения ключей делают его идеальным решением для встраиваемых систем с жёсткими ограничениями по ресурсам.

На момент публикации известных аналогов, сочетающих нейросетевую архитектуру, встроенные ключи, полное прохождение криптографических тестов и размер 8 КБ, не существует.

8. СТАТУС РАЗРАБОТКИ

Данная работа представляет результат частной исследовательской деятельности. Все права на интеллектуальную собственность принадлежат автору.

Технические детали реализации, включая исходный код, архитектуру, значения весов нейросети и точные параметры функций активации, являются коммерческой тайной и не раскрываются.

ЛИТЕРАТУРА

1. NIST SP 800-22: A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. National Institute of Standards and Technology, 2010.
2. FIPS PUB 197: Advanced Encryption Standard (AES). National Institute of Standards and Technology, 2001.
3. OpenSSL Cryptography and SSL/TLS Toolkit, Version 3.0.19. OpenSSL Software Foundation, 2024. URL: https://www.openssl.org/
4. libsodium – A modern, portable, easy to use crypto library. Version 1.0.20. URL: https://doc.libsodium.org/
5. Google Wycheproof – Project Wycheproof: Cryptographic library testing suite. Google Security Team, 2016. URL: https://github.com/google/wycheproof
6. NIST CAVP: Cryptographic Algorithm Validation Program – Digital Signatures Test Vectors (FIPS 186-4). National Institute of Standards and Technology. URL: https://csrc.nist.gov/Projects/cryptographic-algorithm-validation-program/digital-signatures
7. Google Benchmark – A microbenchmark support library. Google, 2024. URL: https://github.com/google/benchmark
8. Grover L.K. A fast quantum mechanical algorithm for database search. Proceedings of the 28th Annual ACM Symposium on Theory of Computing, 1996.

9. Bernstein D.J., Lange T. Post-quantum cryptography. Nature, 2017, Vol. 549, pp. 188-194.
10. NIST IR 8309: Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process. National Institute of Standards and Technology, 2022.
11. Surkova M.A. NEUROHASH: A Cryptographic Neural Network Hash Function of 8 KB Size. Zenodo, 2026. DOI: 10.5281/zenodo.18872419.