БЕЗОПАСНОСТЬ ЦИФРОВЫХ ТЕХНОЛОГИЙ. – 2025. – № 4 (119). – 23–42

МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

УДК 004 DOI: 10.17212/2782-2230-2025-4-23-42

СРАВНИТЕЛЬНЫЙ АНАЛИЗ КРИПТОГРАФИЧЕСКИХ АЛГОРИТМОВ AES, DES, RSA И ECC: МАТЕМАТИЧЕСКИЕ ОСНОВЫ, КРИПТОАНАЛИЗ И УСТОЙЧИВОСТЬ К КВАНТОВЫМ АТАКАМ*

В.В. РЕТИВЫХ[1], А.А. МАРИНОВ[2], А.В. РЕТИВЫХ[3], Е.А. АВЕРКИНА[4]

[1] *РФ, 664074, г. Иркутск, ул. Лермонтова, 83, Иркутский национальный исследовательский технический университет, старший преподаватель Центра компетенций по кибербезопасности. E-mail: vladimir.retivykh@gmail.com*
[2] *РФ, 664074, г. Иркутск, ул. Лермонтова, 83, Иркутский национальный исследовательский технический университет, доцент Центра компетенций по кибербезопасности. E-mail: i@am-irk.ru*
[3] *РФ, 664074, г. Иркутск, ул. Лермонтова, 83, Иркутский национальный исследовательский технический университет, старший преподаватель Центра компетенций по кибербезопасности. E-mail: alret1991@yandex.ru*
[4] *РФ, 125047, г. Москва, ул. 2-я Тверская-Ямская, 18, помещ. 7/2, ООО «НЬЮТОНЛЭБ», генеральный директор, научный консультант промышленной реализации проекта в области гомоморфного шифрования данных. E-mail: averkina6797@gmail.com*

В работе выполнен комплексный сравнительный анализ четырех фундаментальных криптографических алгоритмов, формирующих основу безопасности современных информационных систем: симметричных блочных шифров AES и DES, а также асимметричных систем RSA и ECC. Исследование включает детальное описание математических моделей и структурных особенностей каждого алгоритма, подкрепленное соответствующими математическими выкладками. Проведен всесторонний анализ эволюции криптоаналитических атак на данные схемы – от классических методов (дифференциальный и линейный криптоанализ) до перспективных квантовых алгоритмов (Шора и Гровера) с оценкой их сложности и условий практической реализуемости. Систематизированы современные и перспективные механизмы защиты, включая переход на квантово-устойчивые стандарты. На основе анализа сформулирован вывод о том, что единственным известным в настоящее время методом, обеспечивающим полную конфиденциальность данных в условиях развития квантовых вычислений на всех этапах их жизненного цикла (хранение, передача и обработка), является полное гомоморфное шифрование (Fully Homomorphic Encryption, FHE).

* Статья получена 13 ноября 2025 г.

Ключевые слова: криптография, AES, DES, RSA, ECC, симметричное шифрование, асимметричное шифрование, криптоанализ, алгоритм Шора, алгоритм Гровера, квантовые вычисления, постквантовая криптография, полное гомоморфное шифрование

ВВЕДЕНИЕ

Современная цифровая экономика и инфраструктура критически зависят от обеспечения конфиденциальности, целостности и аутентичности информации. Криптографические алгоритмы, являющиеся ядром систем защиты, прошли длительную эволюцию от относительно простых конструкций середины XX века до сложных математических схем, стойкость которых основана на вычислительной сложности решения определенных теоретико-числовых задач [1]. В настоящее время практическая криптография базируется на двух основных классах алгоритмов: симметричных (AES, DES) и асимметричных (RSA, ECC). Несмотря на их повсеместное использование, сравнительный анализ с точки зрения математических основ, стойкости к классическому и квантовому криптоанализу, а также эффективности остается актуальной исследовательской задачей [2].

Развитие криптографии в XX веке представляет собой непрерывное противоборство между создателями шифров и криптоаналитиками.

- *DES* (*Data Encryption Standard*). Разработан в начале 1970-х годов в IBM на основе алгоритма Lucifer. В 1977 году был утвержден Национальным институтом стандартов и технологий (NIST) США в качестве федерального стандарта шифрования для несекретных данных [6].
- *RSA*. Алгоритм был впервые представлен в 1977 году Роном Ривестом, Ади Шамиром и Леонардом Адлеманом [2]. Это была первая практическая реализация криптосистемы с открытым ключом, основанная на сложности факторизации больших целых чисел.
- *AES* (*Advanced Encryption Standard*). В 1997 году NIST инициировал открытый конкурс на новый стандарт шифрования для замены DES [8].
- *ECC* (*Elliptic Curve Cryptography*). Теоретической основой послужили работы Нила Коблица и Виктора Миллера середины 1980-х годов, которые независимо предложили использовать группу точек эллиптической кривой над конечным полем для построения криптосистем [9].

Появление квантовых вычислений кардинально меняет ландшафт криптографической безопасности. Алгоритм Шора [3] ставит под угрозу все широко используемые асимметричные системы, основанные на задачах факторизации и дискретного логарифмирования, в то время как алгоритм Гровера [4] суще-

ственно снижает стойкость симметричных шифров. Это обусловливает необходимость не только перехода на новые квантово-устойчивые алгоритмы, но и фундаментального пересмотра парадигмы защиты данных, в частности активного развития полного гомоморфного шифрования.

Цель работы – провести всесторонний сравнительный анализ криптографических схем AES, DES, RSA и ECC.

Для достижения поставленной цели были сформулированы следующие задачи:

– рассмотреть математические основы криптоанализа, включая квантовые;

– определить дальнейшее развитие и применение криптографических средств защиты информации.

1. СИММЕТРИЧНЫЕ СХЕМЫ ШИФРОВАНИЯ

Симметричные криптосистемы используют один и тот же секретный ключ для операций шифрования и дешифрования. Их основное преимущество – высокая скорость работы; недостаток – сложность безопасного распределения ключей между сторонами.

Общая модель симметричного блочного шифра может быть представлена как функция

$$C = E(K, P), \tag{1}$$

где P – блок открытого текста, C – блок шифротекста, K – секретный ключ, E – детерминированный алгоритм шифрования.

Дешифрование:

$$P = D(K, C), \tag{1}$$

где D – алгоритм дешифрования.

Большинство современных блочных шифров, включая DES и AES, построены по итерационной структуре (сети Фейстеля или SP-сети), где исходный текст подвергается многократному преобразованию с использованием раундовых ключей, полученных из основного ключа. Это обеспечивает лавинный эффект, когда незначительное изменение открытого текста или ключа приводит к значительному изменению шифротекста.

1.1. СХЕМА AES

1.1.1. МАТЕМАТИЧЕСКИЕ ОСНОВЫ

AES оперирует с блоками данных размером 128 бит. Ключ может иметь длину 128, 192 или 256 бит (AES-128, AES-192, AES-256 соответственно). Основные математические операции выполняются в конечном поле $GF(2^8)$, порожденном неприводимым многочленом $m(x) = x^8 + x^4 + x^3 + 1$ [8, с. 8].

Каждый байт данных $a(x) = a_7 x^7 + a_6 x^6 + \ldots + a_0$ интерпретируется как элемент поля $GF(2^8)$. Операции в поле:

– *сложение* (побитовый XOR);
– *умножение* (умножение полиномов по модулю $m(x)$).

1.1.2. СТРУКТУРА РАУНДА

Алгоритм состоит из N_r раундов: 10 для AES-128, 12 для AES-192, 14 для AES-256. Каждый раунд (кроме последнего) состоит из четырех преобразований [8, с. 11–12].

1. *SubBytes*. Нелинейная замена каждого байта состояния с использованием *S*-блока. Преобразование основано на взятии мультипликативного обратного в поле $GF(2^8)$ с последующим аффинным преобразованием

$$S(a) = Aa^{\{-1\}} + b, \tag{3}$$

где A – матрица, b – вектор.

2. *ShiftRows*. Циклический сдвиг строк состояния. Строка i сдвигается на i байт влево ($i = 0, 1, 2, 3$).

3. *MixColumns*. Преобразование столбцов состояния. Каждый столбец рассматривается как полином степени 3 над $GF(2^8)$ и умножается на фиксированный полином

$$c(x) = (\{03\} \cdot x^3 + \{01\} \cdot x^2 + \{01\} \cdot x + \{02\}) mod\ (x^4 + 1). \tag{4}$$

4. *AddRoundKey*. Побитовое сложение (XOR) состояния с раундовым ключом.

На рис. 1 приведена блок-схема реализации шифрования AES-128.

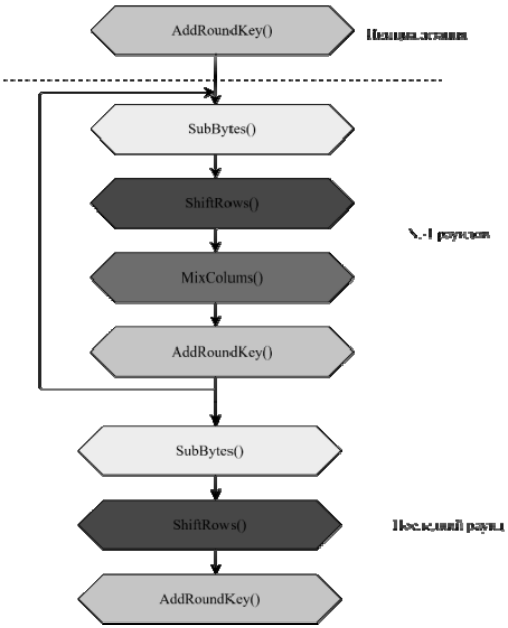

Рис. 1. Блок-схема реализации шифрования AES-128

1.1.3. ГЕНЕРАЦИЯ КЛЮЧЕЙ

Процесс расширения ключа генерирует массив из $4(N_r+1)$ слов. Ключевое расписание использует функцию SubWord (применение *S*-блока к каждому байту слова), RotWord (циклический сдвиг слова) и константы раунда $R_{con}[i]$, которые являются степенями $x(x^{\{i-1\}})$ в поле $GF(2^8)$ [8].

1.2. СХЕМА DES

1.2.1. МАТЕМАТИЧЕСКИЕ ОСНОВЫ И СТРУКТУРА

DES – это 16-раундовый блочный шифр с длиной блока 64 бита и ключом 56 бит (с избыточными восемью битами для проверки четности). Алгоритм построен на основе сети Фейстеля [6, с. 1].

Сеть Фейстеля делит входной блок на две половины (L_0 и R_0). На каждом раунде i

$$L_0 = R_{\{i-1\}},$$

$$R_i = L_{\{i-1\}} \oplus F(L_{\{i-1\}}, K_i),$$

где F – раундовая функция, K_i – раундовый ключ.

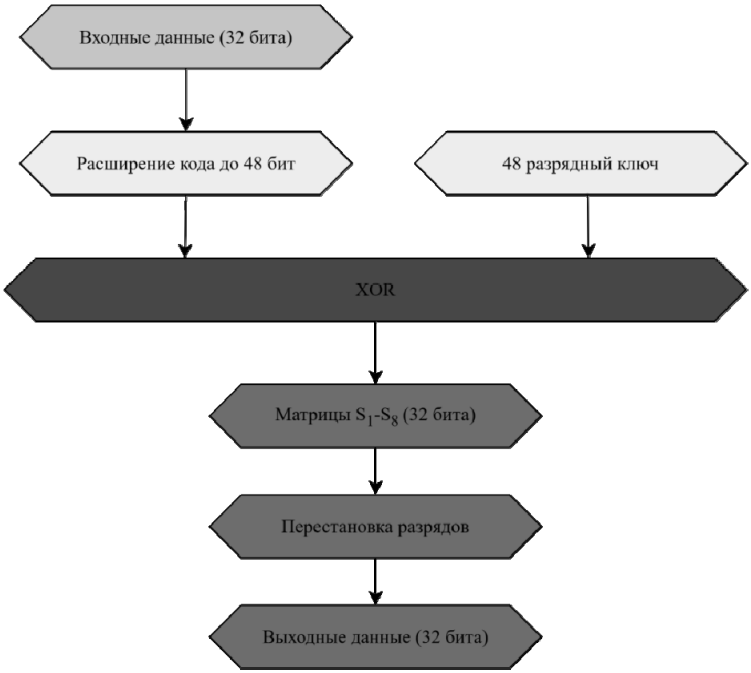

Рис. 2. Блок-схема алгоритма DES-64

1.2.2. ФУНКЦИЯ *F*

Раундовая функция F является ядром алгоритма [6].

1. *Расширение* (E): 32-битная половина $R_{\{i-1\}}$ расширяется до 48 бит с помощью фиксированной перестановки с повторением некоторых бит.

2. *Сложение с ключом*: результат складывается по XOR с 48-битным раундовым ключом K_i.

3. *S*-блоки (подстановка): полученные 48 бит разбиваются на 8 групп по 6 бит. Каждая группа поступает на вход своего *S*-блока $S_1 \ldots S_8$. Каждый *S*-блок представляет собой таблицу 4×16; 6-битный вход определяет строку (первые и последний биты) и столбец (средние 4 бита); 4-битное значение из таблицы является выходом *S*-блока.

4. *Перестановка* (*P*): выходы всех *S*-блоков (32 бита) подвергаются фиксированной перестановке.

1.2.3. ГЕНЕРАЦИЯ КЛЮЧЕЙ

56-битный ключ подвергается перестановке с выбором (PC-1). Результат делится на две 28-битные половины (C_0 и D_0). На каждом раунде обе половины циклически сдвигаются влево на один или два бита (в зависимости от раунда). Затем из объединенных C_i и D_i выбирают 48 бит с помощью перестановки PC-2, формируя раундовый ключ K_i [6].

2. АСИММЕТРИЧНЫЕ СХЕМЫ ШИФРОВАНИЯ

В асимметричных криптосистемах (или криптосистемах с открытым ключом) используют два различных, но математически связанных ключа: открытый ключ K_{pub} для шифрования и секретный ключ K_{priv} для дешифрования. Их стойкость основана на вычислительной сложности задач, обратных к легковычислимым функциям с секретной информацией [2].

Общая модель:

– генерация ключей: $(K_{pub}, K_{priv}) \leftarrow KeyGen(l^{\lambda})$;

– шифрование: $C = E(K_{pub}, M)$;

– дешифрование: $M = D(K_{priv}, C)$.

Основные преимущества: решается проблема распределения ключей, обеспечивается цифровая подпись. Недостатки: низкая скорость работы по сравнению с симметричными схемами.

2.1. СХЕМА RSA

2.1.1. МАТЕМАТИЧЕСКИЕ ОСНОВЫ

Стойкость RSA основана на сложности задачи факторизации больших целых чисел – нахождения простых делителей p и q произведения $n = pq$ [2, с. 120].

2.1.2. ГЕНЕРАЦИЯ КЛЮЧЕЙ

1. Выбираются два больших простых числа (p и q) одинаковой длины.
2. Вычисляется модуль $n = pq$ и функция Эйлера $\varphi(n) = (p-1)(q-1)$.
3. Выбирается открытая экспонента e такая, что $1 < e < \varphi(n)$ и $\text{НОД}(e, \varphi(n)) = 1$. Часто используют $e = 2^{16} + 1 = 65\,537$.
4. Вычисляется секретная экспонента d такая, что $de \equiv 1 (mod\, \varphi(n))$. Это мультипликативное обратное к e по модулю $\varphi(n)$.
5. *Открытый ключ* (n, e).
6. *Закрытый ключ* (d, p, q) или (d, n) [2, с. 123].

2.1.3. ШИФРОВАНИЕ И ДЕШИФРОВАНИЕ

- *Шифрование*: для сообщения M (представленного как число $(0 \le M < n)$ шифротекст вычисляется как $C = M^e \, mod \, n$.
- *Дешифрование*: $M = C^d \, mod \, n$ [2, с. 126].

Корректность следует из теоремы Эйлера: если M и n взаимно простые, то $M^{\{\varphi(n)\}} \equiv 1 mod\, n$. Следовательно, $C^d \equiv (M^e)^d \equiv M^{ed} \equiv M^{\{k \cdot \varphi(n)+1\}} \equiv$ $\equiv M^{\{\varphi(n)\}k} M \equiv M \, mod \, n$.

2.2. СХЕМА ECC

2.2.1. МАТЕМАТИЧЕСКИЕ ОСНОВЫ

Стойкость ECC основана на сложности задачи дискретного логарифмирования в группе точек эллиптической кривой (ECDLP – Elliptic Curve Discrete Logarithm Problem) [9, с. 206; 10, с. 421].

Эллиптическая кривая над простым полем $GF(p)$, где $p > 3$, задается уравнением Вейерштрасса: $y^2 \equiv x^3 + ax = b(mod\ p)$, где $4a^3 + 27b^3 + 27b^2 \neq \neq 0 mod p$.

Множество точек на кривой $E(GF(p))$ вместе со специальной точкой O (точка в бесконечности) образует абелеву группу. Операция сложения точек имеет геометрическую интерпретацию: прямая, проходящая через две точки P и Q, пересекает кривую в третьей точке R', и тогда $P + Q = -R'$ [9, с. 203–206].

2.2.2. ГЕНЕРАЦИЯ КЛЮЧЕЙ И ПРОТОКОЛЫ

Генерация ключей

1. Выбираются параметры домена: p, a, b, G, n, h, где G – базовая точка (генератор) порядка n; h – кофактор [12, с. 36–38].

2. Выбирается случайное целое число d из интервала $[1 \ldots n - 1]$. Это *закрытый ключ*.

3. Вычисляется открытый ключ $Q = dG$ [12, с. 37–39].

Шифрование (*ECIES, гибридная схема*). Чаще всего ECC используется для согласования ключа по протоколу Диффи – Хеллмана [11, с. 644–649], а затем данные шифруются симметричным алгоритмом (например, AES) на этом ключе.

Цифровая подпись (*ECDSA*) вычисляется по алгоритму.

1. Вычисляется хеш сообщения: $e = H(m)$.
2. Выбирается случайное k из $[1 \ldots n - 1]$.
3. Вычисляется точка $(x_1, y_1) = kG$.
4. Вычисляется $r = x_1 \ mod\ n$. Если $r = 0$, выбрать другое k.
5. Вычисляется $s = k^{\{-1\}}(e + d \cdot r) mod\ n$. Если $s = 0$, выбрать другое k.
6. *Подпись*: (r, s) [12, с. 38].

3. ПОДРОБНОЕ СРАВНЕНИЕ СХЕМ AES, DES, RSA, ECC

Для наглядности ключевые сравнительные параметры алгоритмов представлены в таблице.

Сравнительная характеристика криптографических алгоритмов

Параметр	AES	DES	RSA	ECC
Тип	Симметричный, блочный	Симметричный, блочный	Асимметричный	Асимметричный
Размер блока/модуля	128 бит	64 бита	1024…4096 бит (модуль n)	160…521 бит
Размер ключа	128, 192, 256 бит	56 бит (номинально 64)	1024, 2048, 3072, 4096 бит	160, 224, 256, 384, 521 бит
Стойкость (NIST)	128 бит	43 бита	2048 бит	256 бит
Основа стойкости	Восстановление ключа перебором	Восстановление ключа перебором	Факторизация $n = pq$	ECDLP в $E(GF(p))$
Скорость шифрования	Очень высокая (Гбит/с)	Низкая (Мбит/с)	Низкая (кбит/с)	Средняя (согласование ключа)
Скорость дешифрования	Очень высокая (Гбит/с)	Низкая (Мбит/с)	Очень низкая	Средняя (согласование ключа)
Применение	Шифрование данных	Устаревшие системы (3DES)	Шифрование ключей, цифровая подпись	Цифровая подпись, согласование ключей
Размер шифротекста	128 бит	64 бита	1024 бита	Зависит от схемы

Ключевые выводы из сравнения

1. *Симметричные схемы против асимметричных*. AES и DES быстрее RSA и ECC. Они используются для шифрования больших объемов данных.

2. *AES против DES*. AES безопаснее и значительно быстрее DES; DES следует считать полностью устаревшим и небезопасным.

3. *RSA против ECC*. Для сопоставимой криптостойкости ECC требует значительно меньших размеров ключей. Это приводит к экономии памяти, пропускной способности вычислительных ресурсов; ECC быстрее при генерации ключей и создании подписей; RSA быстрее при проверке подписей.

4. *Гибридные схемы*. На практике системы используют симметричное шифрование (AES) для данных и асимметричное (RSA или ECC) для шифрования симметричного ключа сессии. Это объединяет преимущества обоих подходов [12].

4. ОПИСАНИЕ АТАК НА РАЗЛИЧНЫЕ СХЕМЫ ШИФРОВАНИЯ

4.1. КЛАССИЧЕСКИЕ АТАКИ НА СИММЕТРИЧНЫЕ СХЕМЫ

- *Дифференциальный криптоанализ* (*1993*, *Бихам и Шамир*). Атака на DES, использующая анализ разностей между парами открытых текстов и соответствующих им шифротекстов. Сложность атаки оценивается как 2^{47} операций, что значительно меньше полного перебора 2^{56} [14].
- *Линейный криптоанализ* (*1993*, *Мацуи*). Атака на DES, основанная на поиске линейных приближений для нетривиальных соотношений между битами открытого текста, шифротекста и ключа. Наилучшее известное линейное приближение для DES имеет вероятность $0{,}5 + 2^{\{-19\}}$, что позволяет провести атаку со сложностью 2^{43} операций [15, с. 391–396].
- *Атаки на AES*. Наиболее успешными являются атаки, связанные с использованием related-key или атак на уменьшенное число раундов. Для AES-128 наиболее эффективная атака (Biclique cryptanalysis, 2011) снижает сложность перебора до $2^{\{126,1\}}$, что не представляет практической угрозы для полновесного алгоритма [16].

Примеры атак на схемы AES

1. *Кеширующие/тайминг-атаки* (*cache timing, Flush+Reload и пр.*). Исследования показали практические техники извлечения AES-ключей из программных реализаций (OpenSSL, GnuPG и др.), если реализация использует таблицы (T-tables) или иные формируемые/поделенные блоки в кеше. Ключевые работы: FLUSH+RELOAD (Yarom & Falkner, 2014), улучшения атак на AES-реализации (Gülmezoglu et al., 2015), CacheBleed (2016) и др. Как проводили атаки: измеряли время доступа к разделяемым кеш-линиям, восстанавливали статистику обращений к таблицам S-box/T-tables → восстанавливали ключ.

2. *Power / EM side-channel*. Атаки на аппаратные устройства (смарт-карты, встраиваемые устройства) – извлечение ключей AES через измерения потребления энергии или электромагнитного излучения.

3. *Спекулятивное выполнение* (*Spectre / Meltdown и производные*). Эти аппаратные уязвимости позволяли извлекать секретные данные (включая AES-ключи) через побочные эффекты кеша и спекулятивное выполнение. Анализ спектра работ по Spectre показывает, что при определенных условиях AES-ключи в памяти/кеше могут быть извлечены.

4. *Конкретные исследования XTS-AES / диск-шифрования*. Исследователи показали побочные каналы на распространенных режимах и конструкциях (XTS-AES, реализации в HDD/SSD/контроллерах).

4.2. КЛАССИЧЕСКИЕ АТАКИ НА АСИММЕТРИЧНЫЕ СХЕМЫ

- *Факторизация RSA*. Наилучшим классическим алгоритмом является общее решето числового поля (GNFS). Для RSA-2048 это составляет примерно 2^{110} операций [17, с. 1475–1477].
- *Решение ECDLP*. Наилучшие классические алгоритмы (rho-метод Полларда) имеют экспоненциальную сложность $O(\sqrt{n})$, где n – порядок группы. Для кривой P-256 это 2^{128} операций.

Примеры атак на схемы RSA

1. *FREAK – downgrade* TLS. Заставлял клиентов/серверы перейти на export-grade RSA-ключи (40…512 бит), которые можно было факторизовать и дешифровать. Практический эффект – перехват HTTPS-сессий через использование слабых ключей.

2. *DROWN* – кросс-протокольная атака на TLS через уязвимый SSLv2. Даже если основной сервер не поддерживает SSLv2, наличие любой системы, где тот же RSA-сертификат использовался с SSLv2, позволяло расшифровать TLS-сессии. Как проводили атаки: использовали сервер SSLv2 в роли oracle, который выдавал информацию, помогающую расшифровать TLS.

3. *ROCA* – уязвимость генерации RSA-ключей в ПО/чипах Infineon (CVE-2017-15361). Исследования показали, что ряд ключей, сгенерированных на уязвимой библиотеке, можно факторизовать практически. Как проводили атаки: ошибка в алгоритме генерации простых чисел привела к структуре, облегчающей факторизацию.

4. *ROBOT* – вариации адаптивного padding-oracle для RSA PKCS#1 v1.5 в TLS.

5. *Группа уязвимостей и эксплойтов в TLS/сертификатах* – серия инцидентов по эксплуатации слабых режимов реализации.

Примеры атак на схемы ECC

1. *PS3 ECDSA nonce reuse* – классический инцидент. Компания Sony при электронной подписи использовала неправильные параметры в ECDSA. Это позволило полностью восстановить приватный ключ и скомпрометировать систему.

2. *Android Bitcoin wallets* / *SecureRandom bug*. Из-за плохой генерации случайных чисел некоторые Android-кошельки с ECDSA подписывали транзакции с предсказуемым/повторяющимся параметром, что позволяло выводить средства.

3. *Side-channel и microarchitectural атаки на ECC.* Атаки, выстроенные на основе эллиптических кривых.

4. *Полезные практические исследования*. Например, обнаружение и применение атак на реальные блокчейны/кошельки. Ошибки в использовании ECDSA/ECDSA-параметров в реальном мире часто приводят к утечкам ключей безопасности.

4.3. КВАНТОВЫЕ АТАКИ

- *Алгоритм Шора* позволяет решить задачу факторизации и задачу дискретного логарифма за полиномиальное время [3, с. 1484].

  o *Для RSA* факторизация числа n требует $O((\log n)^3)$ квантовых операций.

  o *Для ECC* решение ECDLP в группе порядка n требует $O((\log n)^3)$ квантовых операций.

  o *Математическая основа*: алгоритм использует квантовое преобразование Фурье для нахождения периода функции $f(x) = a^x \bmod n$.

- *Алгоритм Гровера* ускоряет перебор неструктурированных данных, уменьшая сложность с $O(N)$ до $O(\sqrt{N})$ [4, с. 212].

  o *Для симметричных шифров* эффективная сложность взлома AES-128 снижается до 2^{64}, AES-256 – до 2^{128} [5, с. 190; 18, с.75].

- *Гибридные атаки* – сочетание квантового и классического криптоанализа. Например, использование квантового компьютера для ускорения определенных этапов дифференциального или линейного криптоанализа [19, с. 58].

5. КЕЙСЫ ЗАЩИТЫ ОТ АТАК

5.1. ЗАЩИТЫ ДЛЯ СИММЕТРИЧНЫХ СХЕМ

- *Увеличение числа раундов.* В AES число раундов (10, 12, 14) выбрано с запасом безопасности против всех известных атак.
- *Усовершенствованные S-блоки. S*-блоки AES обладают свойствами нелинейности и устойчивости к линейному и дифференциальному криптоанализу.
- *Увеличение длины ключа*. Переход к AES-256 обеспечивает запас безопасности даже против алгоритма Гровера.

5.2. ЗАЩИТЫ ДЛЯ АСИММЕТРИЧНЫХ СХЕМ

- *Увеличение длины ключа*. Для RSA рекомендуется использовать ключи длиной 3072 бита и более, для ECC – 256 бит и более для защиты от классического криптоанализа [13, с. 10–15].
- *Постквантовая криптография.* Стандартизация алгоритмов, устойчивых к квантовым атакам (NIST PQC):
  - *CRYSTALS-Kyber* – алгоритм на основе learning with errors (LWE) [20];
  - *CRYSTALS-Dilithium* – алгоритм цифровой подписи на основе модульных решеток [21].

6. МЕРЫ ЗАЩИТЫ КВАНТОВЫМИ КОМПЬЮТЕРАМИ

В 2025 году квантовые компьютеры с достаточным для взлома RSA-2048 количеством кубитов (10…20 тысяч кубитов) еще не созданы. Однако демонстрационные атаки на упрощенные криптосистемы уже проводятся.

Существующие меры защиты, такие как увеличение длины ключей и переход на постквантовые алгоритмы, решают проблему лишь частично: они обеспечивают безопасность передачи и хранения данных, но не их обработки. В условиях, когда квантовые компьютеры могут быть использованы для взлома шифров непосредственно в процессе вычислений, необходимо принципиально иное решение.

Таким решением, обеспечивающим полную защиту данных на всём протяжении их жизненного цикла (хранение, передача и, что наиболее важно, *обработка*), является *полное гомоморфное шифрование* (*Fully Homotomorphic Encryption, FHE*); FHE позволяет выполнять произвольные вычисления над зашифрованными данными без необходимости их расшифровки. Математическую основу современных FHE-схем (BGV, BFV, CKKS, TFHE) представляет теория решеток (Learning With Errors, Ring-LWE) [5, 24]. Это делает FHE единственным известным в настоящее время криптографическим примитивом, позволяющим обеспечить конфиденциальность данных в эпоху квантовых вычислений на всех этапах работы с ними.

- *Квантово-безопасные алгоритмы.* Переход на стандарты, одобренные NIST (Kyber, Dilithium, Falcon, SPHINCS+).
- *Гибридные схемы*. Использование одновременно классических и квантово-безопасных алгоритмов для обратной совместимости и дополнительной безопасности.

- *Квантовое распределение ключей* (*QKD*). Использование квантовой механики для безопасного обмена ключами. Однако QKD защищает только канал передачи, но не данные на концах канала.

ЗАКЛЮЧЕНИЕ

Проведенный всесторонний анализ демонстрирует, что современные криптографические алгоритмы, такие как AES, RSA и ECC, обеспечивают высокий уровень защиты от классических криптоаналитических атак при корректной реализации и использовании рекомендованных длин ключей. Однако алгоритм DES следует считать полностью устаревшим и небезопасным. Симметричный стандарт AES остается надежным и эффективным решением для шифрования данных, в то время как асимметричные схемы ECC предлагают более эффективную альтернативу RSA для целей управления ключами и цифровой подписи в ресурсоограниченных средах.

Грядущее появление полноценных квантовых компьютеров представляет экзистенциальную угрозу для асимметричных криптосистем RSA и ECC, основанных на факторизации и дискретном логарифмировании. Симметричные алгоритмы, в частности AES, демонстрируют значительно большую устойчивость, требуя лишь удвоения длины ключа для сохранения прежнего уровня стойкости против алгоритма Гровера.

Таким образом, стратегия развития криптографической защиты должна включать следующее:

1) активное использование современных стойких алгоритмов (AES-256, ECC) в гибридных схемах;

2) планирование и начало миграции на стандартизированные NIST постквантовые алгоритмы;

3) инвестирование в исследования и разработку практических реализаций полного гомоморфного шифрования как единственного долгосрочного решения для обеспечения полной конфиденциальности данных в условиях развития квантовых вычислений.

СПИСОК ЛИТЕРАТУРЫ

1. *Menezes A.J., Oorschot P.C. van, Vanstone S.A.* Handbook of applied cryptography. – CRC Press, 1996. – 754 p.

2. *Rivest R.L., Shamir A., Adleman L.* A method for obtaining digital signatures and public-key cryptosystems // Communications of the ACM. – 1978. – Vol. 21 (2). – P. 120–126.

3. *Shor P.W.* Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer // SIAM Journal on Computing. – 1997. – Vol. 26 (5). – P. 1484–1509.

4. *Grover L.K.* A fast quantum mechanical algorithm for database search // Proceedings of the 28th Annual ACM Symposium on Theory of Computing. – ACM Press, 1996. – P. 212–219.

5. *Bernstein D.J., Lange T.* Post-quantum cryptography // Nature. – 2017. – Vol. 549. – P. 188–194.

6. FIPS 46-3: Data Encryption Standard (DES) / National Institute of Standards and Technology. – NIST, 1999.

7. *Lenstra A.K., Verheul E.R.* Selecting cryptographic key sizes // Journal of Cryptology. – 2001. – Vol. 14 (4). – P. 255–293.

8. FIPS 197: Advanced Encryption Standard (AES) / National Institute of Standards and Technology. – NIST, 2001.

9. *Koblitz N.* Elliptic curve cryptosystems // Mathematics of Computation. – 1987. – Vol. 48 (177). – P. 203–209.

10. *Miller V.S.* Use of elliptic curves in cryptography // Lecture Notes in Computer Science. – 1986. – Vol. 218. – P. 417–426.

11. *Diffie W., Hellman M.E.* New directions in cryptography // IEEE Transactions on Information Theory. – 1976. – Vol. 22 (6). – P. 644–654.

12. *Johnson D., Menezes A., Vanstone S.* The elliptic curve digital signature algorithm (ECDSA) // International Journal of Information Security. – 2001. – Vol. 1 (1). – P. 36–63.

13. *Barker E., Roginsky A.* Transitioning the use of cryptographic algorithms and key lengths. – NIST, 2019. – (NIST Special Publication 800-131A).

14. *Biham E., Shamir A.* Differential cryptanalysis of the data encryption standard. – Springer, 1993. – 188 p.

15. *Matsui M.* Linear cryptanalysis method for DES cipher // Lecture Notes in Computer Science. – 1994. – Vol. 765: Advances in Cryptology – EUROCRYPT '93. – P. 386–397.

16. *Bogdanov A., Khovratovich D., Rechberger C.* Biclique cryptanalysis of the full AES // Lecture Notes in Computer Science. – 2011. – Vol. 7073: Advances in Cryptology – ASIACRYPT 2011. – P. 344–371.

17. *Pomerance C.* A tale of two sieves // Notices of the AMS. – 1996. – Vol. 43 (12). – P. 1473–1485.

18. *Bernstein D.J.* Grover vs. McEliece // Post-Quantum Cryptography. – Springer, 2010. – P. 73–80.

19. *Boneh D., Dagdelen Ö.* The rise of quantum computing: Challenges and opportunities for cryptography // Communications of the ACM. – 2024. – Vol. 67 (2). – P. 56–63.

20. FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism Standard / National Institute of Standards and Technology. – NIST, 2024. – 56 p.

21. FIPS 204: Module-Lattice-Based Digital Signature Standard / National Institute of Standards and Technology. – NIST, 2024. – 65 p.

22. *Brakerski Z., Gentry C., Vaikuntanathan V.* (Leveled) fully homomorphic encryption without bootstrapping // ACM Transactions on Computation Theory (TOCT). – 2014. – Vol. 6 (3). – P. 1–36.

Ретивых Владимир Викторович, старший преподаватель Центра компетенций по кибербезопасности Иркутского национального исследовательского технического университета. Основное направление научных исследований – схемы полного гомоморфного шифрования. E-mail: vladimir.retivykh@gmail.com.

Маринов Александр Андреевич, доцент Центра компетенций по кибербезопасности Иркутского национального исследовательского технического университета. Основное направление научных исследований – безопасность киберфизических систем. E-mail: i@am-irk.ru

Ретивых Алексей Викторович, старший преподаватель Центра компетенций по кибербезопасности Иркутского национального исследовательского технического университета. Основное направление научных исследований – защита информационных систем и объектов информатизации. E-mail: alret1991@yandex.ru.

Аверкина Евгения Андреевна, генеральный директор ООО «НЬЮТОНЛЭБ». Область научных интересов – гомоморфное шифрование данных. E-mail: averkina6797@gmail.com.

DOI: 10.17212/2782-2230-2025-4-23-42

A comparative analysis of the cryptographic algorithms AES, DES, RSA, and ECC: mathematical foundations, cryptanalysis, and resistance to quantum attacks*

V.V. Retivykh[1], A.A. Marinov[2], A.V. Retivykh[3], E.A. Averkina[4]

[1] *Irkutsk National Research Technical University, 83 Lermontov Street, Irkutsk, 664074, Russian Federation, Senior Lecturer of Cybersecurity Competency Center. E-mail: vladimir.retivykh@gmail.com*

[2] *Irkutsk National Research Technical University, 83 Lermontov Street, Irkutsk, 664074, Russian Federation, Associate Professor of Cybersecurity Competence Center. E-mail: i@am-irk.ru*

[3] *Irkutsk National Research Technical University, 83 Lermontov Street, Irkutsk, 664074, Russian Federation, Senior Lecturer of Cybersecurity Competency Center. E-mail: alret1991@yandex.ru*

[4] *Limited liability company NEWTONELAB, 2-ya Tverskaya-Ymskaya Street 18, office 7/2, Moscow, 125047, Russian Federation, General Director, Scientific Consultant for the Industrial Implementation of a Project in the Field of Homomorphic Data Encryption. E-mail:averkina6797@gmail.com*

This work presents a comprehensive comparative analysis of four fundamental cryptographic algorithms that form the basis of security in modern information systems: the symmetric block ciphers AES and DES, as well as the asymmetric systems RSA and ECC. The research includes a detailed description of the mathematical models and structural features of each algorithm, supported by relevant mathematical derivations. A thorough analysis of the evolution of cryptanalytic attacks on these schemes is conducted, ranging from classical methods (differential and linear cryptanalysis) to prospective quantum algorithms (Shor's and Grover's), with an assessment of their complexity and conditions for practical feasibility by 2025. Contemporary and prospective defense mechanisms are systematized, including the transition to quantum-resistant standards. Based on the conducted analysis, it is concluded that the only method known to date that ensures complete data confidentiality in the context of the development of quantum computing at all stages of its life cycle (storage, transmission, and processing) is Fully Homomorphic Encryption (FHE).

Keywords: cryptography, AES, DES, RSA, ECC, symmetric encryption, asymmetric encryption, cryptanalysis, Shor's algorithm, Grover's algorithm, quantum computing, post-quantum cryptography, fully homomorphic encryption

* *Received 13 November 2025.*

REFERENCES

1. Menezes A.J., Oorschot P.C. van, Vanstone S.A. *Handbook of applied cryptography*. CRC Press, 1996. 754 p.

2. Rivest R.L., Shamir A., Adleman L. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 1978, vol. 21 (2), pp. 120–126.

3. Shor P.W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, 1997, vol. 26 (5), pp. 1484–1509.

4. Grover L.K. A fast quantum mechanical algorithm for database search. *Proceedings of the 28th Annual ACM Symposium on Theory of Computing*. ACM Press, 1996, pp. 212–219.

5. Bernstein D.J., Lange T. Post-quantum cryptography. *Nature*, 2017, vol. 549, pp. 188–194.

6. FIPS 46-3: *Data Encryption Standard (DES)*. National Institute of Standards and Technology. NIST, 1999.

7. Lenstra A.K., Verheul E.R. Selecting cryptographic key sizes. *Journal of Cryptology*, 2001, vol. 14 (4), pp. 255–293.

8. FIPS 197: *Advanced Encryption Standard (AES)*. National Institute of Standards and Technology. NIST, 2001.

9. Koblitz N. Elliptic curve cryptosystems. *Mathematics of Computation*, 1987, vol. 48 (177), pp. 203–209.

10. Miller V.S. Use of elliptic curves in cryptography. *Lecture Notes in Computer Science*, 1986, vol. 218, pp. 417–426.

11. Diffie W., Hellman M.E. New directions in cryptography. *IEEE Transactions on Information Theory*, 1976, vol. 22 (6), pp. 644–654.

12. Johnson D., Menezes A., Vanstone S. The elliptic curve digital signature algorithm (ECDSA). *International Journal of Information Security*, 2001, vol. 1 (1), pp. 36–63.

13. Barker E., Roginsky A. *Transitioning the use of cryptographic algorithms and key lengths*. NIST, 2019. NIST Special Publication 800-131A.

14. Biham E., Shamir A. *Differential cryptanalysis of the data encryption standard*. Springer, 1993. 188 p.

15. Matsui M. Linear cryptanalysis method for DES cipher. *Lecture Notes in Computer Science*, 1994, vol. 765. *Advances in Cryptology – EUROCRYPT '93*, pp. 386–397.

16. Bogdanov A., Khovratovich D., Rechberger C. Biclique cryptanalysis of the full AES. *Lecture Notes in Computer Science*, 2011, vol. 7073. *Advances in Cryptology – ASIACRYPT 2011*, pp. 344–371.

17. Pomerance C. A tale of two sieves. *Notices of the AMS*, 1996, vol. 43 (12), pp. 1473–1485.

18. Bernstein D.J. Grover vs. McEliece. *Post-Quantum Cryptography*. Springer, 2010, pp. 73–80.

19. Boneh D., Dagdelen Ö. The rise of quantum computing: Challenges and opportunities for cryptography. *Communications of the ACM*, 2024, vol. 67 (2), pp. 56–63.

20. FIPS 203: *Module-Lattice-Based Key-Encapsulation Mechanism Standard*. National Institute of Standards and Technology. NIST, 2024. 56 p.

21. FIPS 204: *Module-Lattice-Based Digital Signature Standard*. National Institute of Standards and Technology. NIST, 2024. 65 p.

22. Brakerski Z., Gentry C., Vaikuntanathan V. (Leveled) fully homomorphic encryption without bootstrapping. *ACM Transactions on Computation Theory (TOCT)*, 2014, vol. 6 (3), pp. 1–36.

Для цитирования:

Сравнительный анализ криптографических алгоритмов AES, DES, RSA и ECC: математические основы, криптоанализ и устойчивость к квантовым атакам / В.В. Ретивых, А.А. Маринов, А.В. Ретивых, Е.А. Аверкина // Безопасность цифровых технологий. – 2025. – № 4 (119). – С. 23–42. – DOI: 10.17212/2782-2230-2025-4-23-42.

For citation:

Retivykh V.V., Marinov A.A., Retivykh A.V., Averkina E.A. Sravnitel'nyi analiz kriptograficheskikh algoritmov AES, DES, RSA i ECC: ma-tematicheskie osnovy, kriptoanaliz i ustoichivost' k kvantovym atakam [A comparative analysis of the cryptographic algorithms AES, DES, RSA, and ECC: mathematical foundations, cryptanalysis, and resistance to quantum attacks]. *Bezopasnost' tsifrovykh tekhnologii = Digital Technology Security*, 2025, no. 4 (119), pp. 23–42. DOI: 10.17212/2782-2230-2025-4-23-42.