СРАВНИТЕЛЬНЫЙ АНАЛИЗ ПРОИЗВОДИТЕЛЬНОСТИ АЛГОРИТМОВ СИММЕТРИЧНОГО ШИФРОВАНИЯ (AES, CHACHA20) В КОНТЕКСТЕ ЗАЩИТЫ БОЛЬШИХ ОБЪЕМОВ ДАННЫХ БД.

Насырова Динара Тагировна
студент группы 304-25
направления «Компьютерные сети и их программное обеспечение»
Ташкентского университета
информационных технологий имени Мухаммада аль-Хорезми
Решитов Эльдар Серверович
ассистент
кафедры «Системное прикладное программирование»
Ташкентского университета
информационных технологий имени Мухаммада аль-Хорезми

Аннотация. Данная статья посвящена сравнительному анализу производительности двух ключевых алгоритмов симметричного шифрования — Advanced Encryption Standard (AES) и ChaCha20 — применительно к задаче защиты больших объемов данных в базах данных (БД). В условиях экспоненциального роста данных и ужесточения регуляторных требований, выбор криптографического алгоритма, обеспечивающего высокую скорость обработки без существенных накладных расходов на вычислительные ресурсы, является критически актуальным. Основной фокус исследования — определение, какой из алгоритмов обеспечивает лучшую пропускную способность (throughput) и меньшую задержку (latency) при шифровании/расшифровании значительных массивов информации, учитывая влияние аппаратного ускорения (AES-NI) и особенностей архитектуры процессоров.

Ключевые слова: Симметричное шифрование (Symmetric Encryption), AES (Advanced Encryption Standard), ChaCha20, Производительность (Performance), Защита данных (Data Protection), Базы данных (Database).

ВСТУПЛЕНИЕ

Симметричное шифрование является краеугольным камнем защиты конфиденциальности информации. В отличие от асимметричного, оно использует один и тот же ключ для шифрования и расшифрования, что делает его значительно более быстрым и идеально подходящим для обработки больших объемов данных, характерных для современных баз данных.

Среди множества существующих симметричных алгоритмов, AES (блочный шифр) и ChaCha20 (поточный шифр) являются двумя наиболее распространенными и криптостойкими стандартами. Однако, их архитектурные различия (блочный vs. поточный) и различная степень поддержки аппаратным обеспечением приводят к существенным отличиям в производительности, что напрямую влияет на эффективность работы БД, особенно при частых операциях чтения и записи зашифрованных полей.

Цель статьи — сравнить эти два алгоритма по ключевым метрикам производительности для определения оптимального выбора при проектировании систем защиты данных БД, где критичны как безопасность, так и скорость.

СРАВНЕНИЕ МОДЕЛЕЙ УПРАВЛЕНИЯ ДОСТУПОМ

Таблица 1

Архитектурные особенности и режимы работы

Параметр	**AES (Блочный шифр)**	**ChaCha20 (Поточный шифр)**
Тип шифра	Блочный (Block Cipher)	Поточный (Stream Cipher)

Размер блока/потока	128 бит (фиксированный)	Генерация ключевого потока побайтово
Предпочтительный режим	GCM (Galois/Counter Mode)	Poly1305 (для аутентификации - ChaCha20-Poly1305)
Параллелизм	Высокий (в режимах CTR, GCM)	Высокий (изначально оптимизирован для параллельной обработки)
Зависимость от аппаратного ускорения	Критическая (AES-NI)	Низкая (оптимизирован для чисто программной реализации)

AES-NI (Advanced Encryption Standard New Instructions) — это набор инструкций, встроенных в большинство современных процессоров Intel и AMD. Они позволяют выполнять операции AES на аппаратном уровне, минуя сложную программную реализацию.

- AES с AES-NI: В подавляющем большинстве случаев на современных серверах и рабочих станциях, где доступно аппаратное ускорение, AES в режиме GCM (AES-GCM) демонстрирует наивысшую пропускную способность. Производительность может быть в 2-10 раз выше, чем у программных реализаций. Для защиты больших объемов данных в БД, развернутых на современном оборудовании, AES-GCM является лидером по скорости.
- ChaCha20: Будучи изначально оптимизированным для программной реализации, ChaCha20 эффективно использует инструкции SIMD (Single Instruction, Multiple Data) на процессорах общего назначения.

Однако его производительность, как правило, уступает аппаратно ускоренному AES на том же оборудовании.

Сценарии, где аппаратное ускорение недоступно (старые процессоры, маломощные встраиваемые системы, некоторые облачные среды с ограничениями), кардинально меняют картину.

- ChaCha20: В чисто программной реализации ChaCha20-Poly1305 становится значительно быстрее, чем программный AES (иногда в 2-4 раза). Это связано с простотой его архитектуры, которая меньше подвержена уязвимостям по сторонним каналам (например, по времени) и лучше оптимизируется компиляторами для общих процессорных инструкций.
- AES (программный): Без AES-NI AES становится вычислительно очень затратным, что делает его непригодным для высокопроизводительных задач, таких как шифрование больших таблиц БД.

Таблица 2

Контекст защиты БД и больших объёмов данных

Критерий	AES-GCM (с AES-NI)	ChaCha20-Poly1305 (Программный)	Вывод для БД
Пропускная способность	Высшая	Высокая	Зависит от наличия AES-NI.
Аутентификация	Встроена (GCM)	Встроена (Poly1305)	Оба обеспечивают Authenticated Encryption with Associated Data (AEAD), что

			критично для целостности данных БД.
Обработка потоков данных	Блочная, но эффективно работает с потоками (CTR/GCM)	Изначально поточная	ChaCha20 проще реализовать безопасно и без уязвимостей при работе с невыравненным и или большими порциями данных.

Для защиты больших объемов данных в высоконагруженных БД (где важна высокая пропускная способность):

- Если гарантировано наличие процессоров с AES-NI (что характерно для большинства современных серверов), AES-GCM является наиболее производительным выбором.
- Если целевая платформа разнородна или включает устройства без AES-NI (например, мобильные клиенты или устаревшее оборудование), ChaCha20-Poly1305 предлагает более стабильную и высокую скорость в программной реализации, минимизируя риск узких мест.

ВЫВОД

Сравнительный анализ производительности алгоритмов AES и ChaCha20 в контексте защиты больших объемов данных БД выявил, что выбор оптимального решения напрямую зависит от целевой аппаратной платформы.

- На оборудовании с аппаратным ускорением (AES-NI): AES-GCM является безусловным лидером по пропускной способности, обеспечивая максимальную скорость шифрования/расшифрования данных. Это предпочтительный выбор для высокопроизводительных серверных БД.
- На оборудовании без аппаратного ускорения: ChaCha20-Poly1305 демонстрирует превосходство в программной производительности, будучи более быстрым, более устойчивым к атакам по времени и более простым в безопасной реализации.

Таким образом, для корпоративных систем с унифицированным серверным парком следует выбирать AES-GCM. Для гибридных или распределенных систем, где важна консистентная производительность на различных устройствах, ChaCha20-Poly1305 представляет собой более гибкое и надежное решение.

ИСПОЛЬЗОВАННАЯ ЛИТЕРАТУРА

1. Daemen, J., & Rijmen, V. The Design of Rijndael: AES - The Advanced Encryption Standard. *Springer*, 2002.
2. Bernstein, D. J. ChaCha, a variant of Salsa20**.** *Workshop on Fast Software Encryption (FSE)*, 2008.
3. Patria M., Andriati D. A. Analisis Komparatif Performa AES-GCM dan ChaCha20-Poly1305 dalam Enkripsi Dokumen PDF Berbasis AEAD //Arcitech: Journal of Computer Science and Artificial Intelligence. – 2025. – Т. 5. – №. 1. – С. 49-69.
4. Arunkumar B., Kousalya G. Analysis of AES-GCM cipher suites in TLS //The International Symposium on Intelligent Systems Technologies and Applications. – Cham : Springer International Publishing, 2017. – С. 102-111.
5. Xu H. et al. Applications of cryptography in database: a review //2021 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS). – IEEE, 2021. – С. 1-6.