УДК 004.056.55

Карый Михаил Александрович, студент,
Донской государственный технический университет
Kary Mikhail Alexandrovich, student,
Don State Technical University

Бурунин Алексей Сергеевич, студент,
Донской государственный технический университет
Burunin Alexey Sergeevich, student,
Don State Technical University

Шевчук Петр Сергеевич,
доктор технических наук, профессор,
профессор кафедры «Информационная безопасность
в вычислительных системах и сетях»,
Донской государственный технический университет
Shevchuk Petr Sergeevich,
Doctor of Technical Sciences, Professor,
Professor, Department of Information Security
in Computing Systems and Networks,
Don State Technical University

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ПРОИЗВОДИТЕЛЬНОСТИ АЛГОРИТМОВ СИММЕТРИЧНОГО ШИФРОВАНИЯ В КАНАЛАХ С ОГРАНИЧЕННОЙ ПРОПУСКНОЙ СПОСОБНОСТЬЮ
COMPARATIVE PERFORMANCE ANALYSIS OF SYMMETRIC ENCRYPTION ALGORITHMS IN BANDWIDTH-LIMITED CHANNELS

Аннотация. В работе выполнен сравнительный анализ производительности алгоритмов симметричного шифрования AES, «Кузнечик» (ГОСТ Р 34.12-2015) и ChaCha20 применительно к каналам связи с ограниченной пропускной способностью. Предложена модель оценки эффективной пропускной способности канала с учётом структурных накладных расходов шифрования. Показано, что при программной реализации без аппаратного ускорения наибольшую скорость обеспечивает ChaCha20, а при наличии набора команд AES-NI преимущество переходит к AES. Сформулированы рекомендации по выбору алгоритма в зависимости от характеристик канала и вычислительной платформы.

Abstract.: the paper presents a comparative performance analysis of the symmetric encryption algorithms AES, Kuznyechik (GOST R 34.12-2015) and ChaCha20 for bandwidth-limited communication channels. A model for estimating the effective channel throughput that accounts for the structural overhead of encryption is proposed. It is shown that in a software implementation without hardware acceleration ChaCha20 provides the highest speed, whereas with the AES-NI instruction set the advantage shifts to AES. Recommendations for algorithm selection depending on the channel characteristics and the computing platform are formulated.

Ключевые слова: Симметричное шифрование, AES, «Кузнечик», ChaCha20, пропускная способность, накладные расходы.

Keywords: Symmetric encryption, AES, Kuznyechik, ChaCha20, throughput, overhead.

Введение.

Защита данных, передаваемых по открытым каналам связи, остаётся одной из ключевых задач информационной безопасности телекоммуникационных систем.

Симметричное шифрование обеспечивает конфиденциальность информации при относительно низких вычислительных затратах, поэтому именно оно применяется для потоковой защиты трафика. Вместе с тем в ряде практически значимых случаев канал связи обладает ограниченной пропускной способностью: это беспроводные сенсорные сети, каналы интернета вещей, спутниковые и радиорелейные линии, промышленные шины передачи данных. В таких условиях к алгоритму шифрования предъявляются повышенные требования не только по стойкости, но и по производительности, а также по объёму служебных данных, добавляемых к полезной нагрузке.

Цель работы – сравнить три распространённых алгоритма симметричного шифрования (AES, отечественный шифр «Кузнечик» и потоковый шифр ChaCha20) по совокупности показателей производительности и оценить их влияние на эффективную пропускную способность канала с ограниченной полосой.

Характеристика исследуемых алгоритмов.

AES (Advanced Encryption Standard, FIPS PUB 197) – блочный шифр с размером блока 128 бит и длиной ключа 128, 192 или 256 бит, построенный по схеме подстановочно-перестановочной сети [3]. Широкое распространение AES и наличие в современных процессорах набора команд AES-NI позволяют достигать высокой скорости аппаратно ускоренного шифрования.

«Кузнечик» – блочный шифр, установленный национальным стандартом ГОСТ Р 34.12-2015, с размером блока 128 бит и длиной ключа 256 бит [1]. Алгоритм реализует подстановочно-перестановочную сеть с нелинейным преобразованием и линейным преобразованием над конечным полем. Применение «Кузнечика» обязательно в ряде информационных систем Российской Федерации, однако его программная реализация без специальной оптимизации уступает по скорости зарубежным аналогам.

ChaCha20 – потоковый шифр семейства ARX (сложение, циклический сдвиг, побитовое исключающее ИЛИ) с длиной ключа 256 бит, стандартизованный для протоколов IETF [4]. Он не требует аппаратной поддержки и демонстрирует высокую скорость при чисто программной реализации, что делает его привлекательным для мобильных и встраиваемых платформ. На практике ChaCha20 применяется совместно с кодом аутентификации Poly1305, образуя схему аутентифицированного шифрования ChaCha20-Poly1305.

Во всех рассматриваемых случаях для обеспечения не только конфиденциальности, но и целостности применяются режимы аутентифицированного шифрования (AEAD): для AES – режим GCM [2], для «Кузнечика» – режим MGM [5], для ChaCha20 – конструкция с Poly1305. Такие режимы добавляют к сообщению имитовставку и требуют передачи значения синхропосылки (nonce).

Модель влияния шифрования на пропускную способность канала.

Обобщённая модель защищённой передачи данных по каналу с ограниченной пропускной способностью приведена на рисунке 1. Полезная нагрузка объёмом Lп перед передачей преобразуется шифратором, после чего к ней добавляются служебные данные Lн, необходимые для корректного расшифрования и проверки целостности.

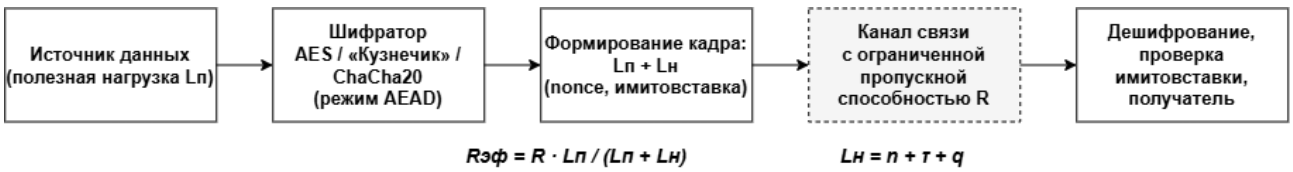

Рисунок 1. Обобщённая модель защищённой передачи данных по каналу с ограниченной пропускной способностью

Структурные накладные расходы на один кадр складываются из длины синхропосылки n, длины имитовставки τ и длины дополнения q (для блочных шифров при выравнивании до целого числа блоков):

$$L_н = n + \tau + q \quad (1)$$

Эффективная пропускная способность канала Lэф, то есть скорость передачи именно полезных данных, при физической пропускной способности R определяется долей полезной нагрузки в общем объёме кадра:

$$R_{эф} = R \cdot \frac{L_п}{L_п + L_н} \quad (2)$$

Из выражения (2) следует, что при малом размере полезной нагрузки Lп, сопоставимом с Lн, потери эффективной пропускной способности становятся значительными. Так, при передаче коротких кадров длиной 32 байта добавление 12-байтовой синхропосылки и 16-байтовой имитовставки снижает эффективную пропускную способность более чем на 45 %. Это означает, что для узких каналов структурный размер служебных данных нередко важнее «сырой» скорости шифрования.

Время обработки блока данных объёмом L шифратором зависит от скорости шифрования V, обеспечиваемой конкретной реализацией алгоритма на заданной платформе:

$$t_{обр} = \frac{L}{V} \quad (3)$$

Совокупная задержка доставки складывается из времени шифрования на передающей стороне, времени распространения по каналу и времени расшифрования на приёмной стороне. При ограниченной пропускной способности вклад времени шифрования, как правило, невелик по сравнению с временем передачи, однако на маломощных вычислительных платформах именно скорость V может стать «узким местом».

Результаты сравнения.

Сравнение алгоритмов по основным показателям приведено в таблице 1. Приведённые значения скорости характерны для однопоточной обработки на процессоре общего назначения и носят иллюстративный характер; при выполнении экспериментального исследования их следует уточнять непосредственными измерениями на целевой платформе.

Таблица 1

Сравнительная характеристика алгоритмов симметричного шифрования

Показатель	**AES-256**	**«Кузнечик»**	**ChaCha20**
Тип шифра	блочный	блочный	потоковый
Размер блока / состояния	128 бит	128 бит	512 бит (состояние)
Длина ключа	256 бит	256 бит	256 бит
Синхропосылка (nonce/IV)	12 байт (GCM)	16 байт (MGM)	12 байт
Имитовставка (AEAD)	16 байт	16 байт	16 байт
Скорость, программная реализация	≈180 МБ/с	≈50 МБ/с	≈500 МБ/с
Скорость с аппаратным ускорением	≈2600 МБ/с (AES-NI)	зависит от реализации	ускорение не требуется
Аппаратное ускорение в CPU общего назначения	есть (AES-NI)	как правило, нет	не требуется

Для наглядности относительная производительность алгоритмов при программной реализации представлена на рисунке 2. В отсутствие аппаратного ускорения наибольшую скорость обеспечивает ChaCha20, тогда как «Кузнечик» в базовой реализации существенно

уступает. При наличии команд AES-NI картина меняется: аппаратно ускоренный AES опережает конкурентов приблизительно на порядок.

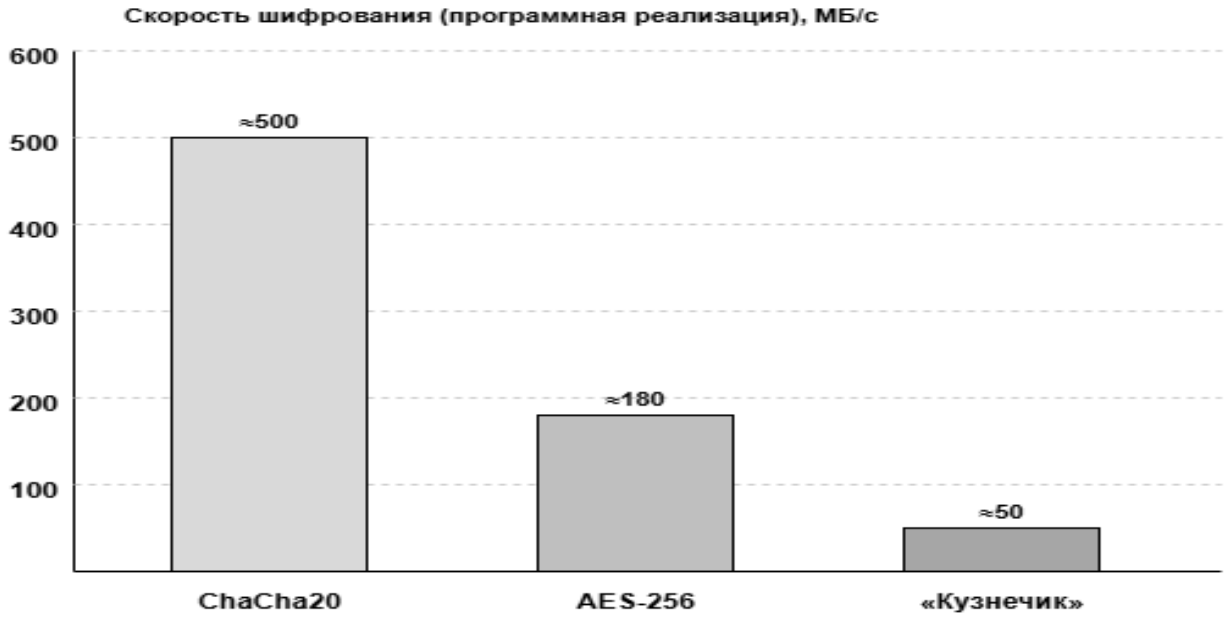

Рисунок 2. Скорость шифрования при программной реализации (представительные значения)

Рекомендации по выбору алгоритма.

На основании проведённого сравнения можно сформулировать следующие рекомендации. На платформах с аппаратной поддержкой AES-NI (серверы, современные рабочие станции) предпочтителен режим AES-GCM, обеспечивающий максимальную скорость при минимальных накладных расходах. На маломощных и мобильных платформах без аппаратного ускорения (устройства интернета вещей, встраиваемые системы) целесообразно применение ChaCha20-Poly1305, сочетающего высокую программную скорость и умеренный объём служебных данных. В информационных системах, для которых нормативно обязательно применение отечественных криптографических алгоритмов, следует использовать «Кузнечик» в режиме MGM, предусматривая при этом оптимизированную или аппаратную реализацию для компенсации сравнительно низкой программной скорости. Независимо от выбранного алгоритма для каналов с ограниченной пропускной способностью критически важно минимизировать структурные накладные расходы, в том числе за счёт укрупнения кадров и выбора компактной синхропосылки.

Заключение.

В работе рассмотрены три алгоритма симметричного шифрования и предложена модель оценки их влияния на эффективную пропускную способность канала связи. Установлено, что для каналов с ограниченной полосой определяющее значение имеют не только скорость шифрования, но и структурные накладные расходы, вносимые режимом аутентифицированного шифрования. Показано, что выбор алгоритма должен учитывать характеристики вычислительной платформы: при наличии аппаратного ускорения предпочтителен AES, при его отсутствии – ChaCha20, а в регулируемых сферах – «Кузнечик» с оптимизированной реализацией. Полученные результаты могут быть использованы при проектировании подсистем криптографической защиты телекоммуникационных систем, функционирующих в условиях ограниченной пропускной способности.

Список литературы:

1. ГОСТ Р 34.12-2015. Информационная технология. Криптографическая защита информации. Блочные шифры. – М.: Стандартинформ, 2016. – 25 с.
2. ГОСТ Р 34.13-2015. Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров. – М.: Стандартинформ, 2016. – 38 с.
3. FIPS PUB 197. Advanced Encryption Standard (AES). – Gaithersburg: National Institute of Standards and Technology, 2001. – 51 p.
4. Nir Y., Langley A. ChaCha20 and Poly1305 for IETF Protocols. RFC 8439. – IETF, 2018. – 46 p.
5. Р 1323565.1.026-2019. Информационная технология. Криптографическая защита информации. Режим работы блочных шифров, реализующий аутентифицированное шифрование. – М.: Стандартинформ, 2019.
6. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы и исходный код на С. – М.: Диалектика, 2018. – 1040 с.
7. Шевчук П. С. Криптографическая защита информации: учебник. – Москва: РИОР: ИНФРА-М, 2018. – 321 с.