Производительность ГОСТ-шифрования на x86- и GPU-процессорах

В статье представлены результаты тестирования оптимизированных алгоритмов шифрования ГОСТ, полученные в сентябре и марте 2014 г. компанией "Код Безопасности", на новых серверных процессорах Intel, а также на графических процессорах различных производителей.

Кролевецкий Алексей – ведущий программист отдела перспективных разработок ООО «Код Безопасности».

Введение: ускорение шифрования ГОСТ 28147-89

С развитием ИТ-технологий резко возросли объемы данных, передаваемых по глобальной сети Интернет, находящихся в сетевых хранилищах и обрабатываемых в «облаках». Часть этих данных конфиденциальна, поэтому необходимо обеспечить их защиту от несанкционированного доступа. Для защиты конфиденциальных данных традиционно используется шифрование, а при шифровании больших объемов – алгоритмы симметричного шифрования, такие, как широко известный блочный алгоритм – AES. Для соответствия российскому законодательству при шифровании таких сведений, как персональные данные, необходимо использовать отечественный алгоритм симметричного блочного шифрования – ГОСТ 28147–89. Операция шифрования данных достаточно затратна и требует дополнительного времени на обработку данных, вследствие чего снижается производительность и увеличиваются задержки. Для снижения этого негативного эффекта при защите данных необходимо увеличивать скорость шифрования. В основном алгоритмы шифрования реализуются программно, но для достижения больших скоростей применяют аппаратные способы. К сожалению, в современных процессорах архитектуры x86 аппаратное ускорение шифрования реализовано только для стандарта AES (набор инструкций AES-NI). Этот стандарт основывается на особой алгебраической структуре, и ускорить другие стандарты шифрования с помощью инструкций AES-NI можно, только если их структура совпадает с AES (например, Camellia).

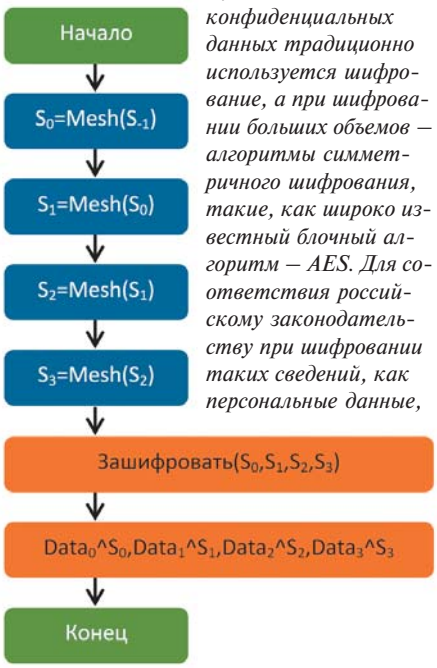

Рис. 1. Основной цикл обработки данных в режиме гаммирования при параллельной обработке четырех блоков шифрования.

При реализации ГОСТ 28147–89 нельзя задействовать инструкции AES-NI, но можно применить другие подходы в ускорении шифрования. Например, мультиблочное шифрование – один программный поток шифрования параллельно обрабатывает несколько блоков. Но распараллелить обработку единого массива данных (рис. 1) можно только в тех режимах шифрования ГОСТ 28147–89, где нет обратной связи между обрабатываемыми блоками (гаммирование, ECB). Для режимов, имеющих обратную связь между блоками (CFB, MAC), можно использовать параллельную обработку нескольких блоков от разных потоков шифрования (рис. 2). При таком подходе скорость шифрования ГОСТ 28147–89 можно измерять в режиме ECB без потери общности. При этом стоит отметить размер буфера для каждого такого потока шифрования – он не должен превышать 4КБ (размер сектора на HDD). В приведенных ниже результатах мы ограничились размером в 512 байт, а каждый поток шифровался на своем ключе.

Ускорение ГОСТ 28147-89 на центральном процессоре (ЦП) с помощью SIMD-технологий

Современные процессоры архитектуры x86 (а также ARM, PowerPC и др.) содержат блок векторных вычислений для параллельной обработки нескольких потоков данных с помощью технологии SIMD (single instruction, multiple data). Этот блок ЦП можно эффективно задействовать для мультиблочного шифрования ГОСТ 28147–89. Наибольший эффект при этом достигается за счет аппаратных инструкций перемешивания данных (первым предложил А.В. Луценко), которые позволяют существенно ускорить нелинейное преобразование (далее S-box) в алгоритме. В сочетании с расширениями команд AVX (или AVX2) и возможностью процессоров архитектуры x86 выполнять несколько команд параллельно (out-of-order execution) мультиблочное шифрование дает высокую скорость даже для одного ядра процессора.

Реализация алгоритма ГОСТ 28147–89 с помощью инструкций AVX (процессор Intel-архитектуры Sandy Bridge/Ivy Bridge) позволяет обрабатывать данные со скоростью 8,5 тактов/байт для одного ядра процессора (такая же скорость для алгоритма AES-256 без использования инструкций AES-NI). Для архитектуры Intel Haswell с поддержкой AVX2 производительность возрастает до 6,7 тактов/байт. Если целевая шифрующая система использует только ЦП, то ее производительность будет линейно расти от суммарного количества ядер ЦП (рис. 3) в системе и их частоты. На платформе Intel Xeon 2 x E5-2697 v3 при обработке 16 потоков шифрования ГОСТ 28147–89 на одном ядре ЦП (AVX, рис. 3) максимальная скорость составила 9425 Мбайт/с (10,5 Мбайт/с на 1 поток). При использовании инструкций AVX2 (32 потока шифрования) на тестовой платформе скорость составила 13133 Мбайт/с (7,3 Мбайт/с на 1 поток) или более 100 Гбит/с.

Низкую скорость шифрования одного потока необходимо пояснить. Например,

Рис. 2. Параллельная обработка четырех потоков шифрования на одном ядре ЦП.

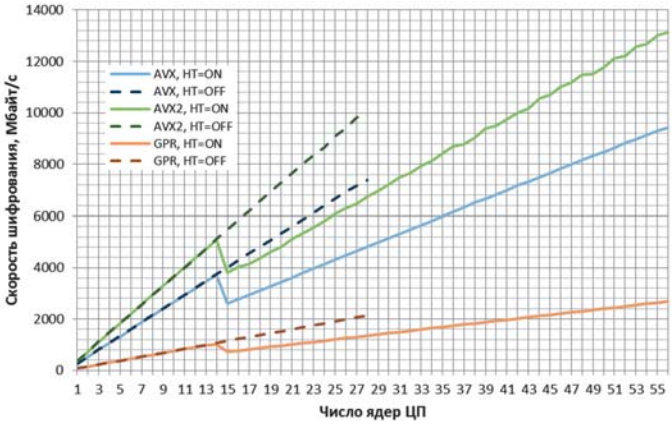

Рис. 3. Шифрование ГОСТ 28147–89 ECB на CPU при параллельной обработке буфера 8 Мбайт с помощью различных технологий на платформе 2 x Intel Xeon E5-2697 v3 @ 2.6 ГГц.

нам необходимо зашифровать 128 секторов на жестком диске (размер сектора 512 байт). Так как сектора можно шифровать параллельно, то скорость шифрования на 1 ядре ЦП в этом случае составит 10,5 Мбайт/с x 16 потоков = 168 Мбайт/с и 7,3 Мбайт/с x 32 потока = 233,3 Мбайт/с для AVX и AVX2, соответственно. Стоит отметить, что технология Intel Hyper-threading позволяет увеличить суммарную скорость платформы на 30% при 50%-ном снижении скорости на один поток (рис. 3).

Ускорение ГОСТ 28147-89 на центральном процессоре (ЦП) на регистрах общего назначения

При реализации ГОСТ 28147–89 на регистрах общего назначения для операции S-box составляется предрасчетная таблица объемом 4 КБ *(первым предложил А. Винокуров)*. Такой подход требует множество операций нелинейного обращения к памяти, и скорость выполнения такой реализации алгоритма шифрования зависит от подсистемы памяти ЦП. Для архитектуры Intel Sandy Bridge/Ivy Bridge производительность шифрования в этом случае составляет 60 тактов/байт. В этой архитектуре присутствуют 2 порта загрузки данных (LD – load data) в каждом ядре ЦП, что позволяет применить мультиблочное шифрование и, в этом случае – шифровать 2 блока параллельно. Тогда скорость шифрования возрастает до 30 тактов/байт. Для тестируемой платформы суммарная скорость шифрования ГОСТ 28147–89 на регистрах общего назначения составила 2682 Мбайт/с (23,9 Мбайт/с на 1 поток) или 21,97 Гбит/с (GPR, рис. 3).

Мультиблочное шифрование с помощью SIMD обеспечивает максимальную производительность при обработке от 4 потоков шифрования. При этом скорость шифрования одного потока на SIMD ниже, чем скорость одного потока на регистрах общего назначения. Коэффициент распараллеливания шифрования на ЦП составил 0,99 без использования технологии Intel Hyper-threading. При использовании этой технологии коэффициент понизился до 0,65.

Ускорение ГОСТ 28147-89 на графическом процессоре (GPU)

Для дальнейшего ускорения шифрования по ГОСТ 28147–89 мы исследовали гетерогенные системы (CPU+GPU). Развитие архитектуры GPU привело к тому, что они по своим возможностям приближаются к ЦП как по методам программирования, так и по аппаратной части. Но использование GPU как ускорителя шифрования сопряжено с рядом технических проблем.

Как правило, графический ускоритель является периферийным устройством, которое подключается к CPU по шине передачи данных PCI Express. Это вносит в реализацию любого алгоритма с помощью технологии общих вычислений на графических ускорителях (GPGPU) дополнительные операции по копированию данных из памяти CPU в память GPU и обратно, но этот эффект можно уменьшить за счет конвейеризации обработки данных (рис. 4).

Рис. 4. Конвейеризация обработки данных на GPU.

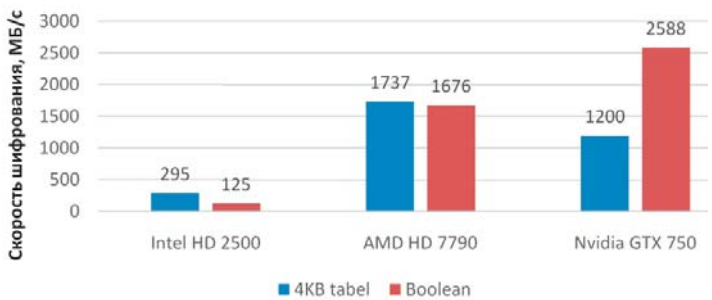

Рис. 5. Шифрование ГОСТ 28147–89 ECB на GPU при параллельной обработке буфера 8 Мбайт, 16 384 потока шифрования по 512 байт.

Ядра в современных GPU по своей структуре похожи на блоки векторных вычислений в ЦП. Архитектурно GPU направлены на выполнение большого числа параллельных потоков программ, которые выполняют множество арифметических операций. Современный графический ускоритель имеет в своем составе большое число арифметически-логических устройств (ALU) и архитектуру памяти, ориентированную на передачу больших блоков данных. В алгоритме ГОСТ 28147–89 операция S-box для процессоров общего назначения требует множество нелинейных операций обращения к памяти, где хранятся таблицы замен. Нелинейные операции чтения из памяти для GPU выполняются с бОльшими задержками, чем для ЦП. Поэтому мы реализовали операцию S-box в алгоритме ГОСТ 28147–89 с помощью булевой функции с целью оптимального использования вычислительных возможностей, предоставляемых GPU. При этом нам удалось получить скорость шифрования на GPU Nvidia GeForce GTX 750 (архитектура Maxwell) 2588 Мбайт/с (161,8 Кбайт/с на 1 поток) или 21,2 Гбит/с (рис. 5). Для GPU AMD HD 7790 (архитектура GCN 1.1) скорость шифрования ~1700 Мбайт/с. Графический ускоритель от Intel хоть и не показал выдающихся результатов (295 Мбайт/с), но по распространенности ему нет равных. Его скорости будет достаточно для шифрования одного жесткого диска.

Стоит отметить, что тестировались не самые производительные GPU, у Nvidia и AMD есть более производительные решения на аналогичных архитектурах: GeForce GTX 980 и FirePro W9100. Мы предполагаем, что скорость в этом случае увеличится пропорционально числу ALU этих GPU: в 4 раза для GTX 980 и 3 раза для FirePro W9100. При этом производительность шифрования на одном GPU не может превысить скорость передачи данных по шине PCI express v3 в одном направлении (12 Гбайт/с).

Заключение

По скоростным характеристикам шифрование ГОСТ 28147–89 приближается к AES и может стать ему хорошей альтернативой. Если комбинировать шифрование на CPU и GPU, можно достигнуть скорости шифрования на 1 узел в 53 Гбайт/с (платформа 2 CPU Intel Xeon E5-2697 v3 + 4 GPU Nvidia GeForce GTX 980). Кратко перечислим области, где могут быть востребованы такие скорости шифрования. Во-первых, для шифрования сетей стандарта 40 Гбит/с и 80 Гбит/с, что будет реализовано в следующих версиях АПКШ «Континент». Во-вторых, в распределенных сетевых дисковых хранилищах. В настоящий момент «Код Безопасности» разрабатывает проходной шифратор для протокола iSCSI. В-третьих, саму операцию шифрования можно продавать как услугу в облачных сервисах – клиент облака доплачивает за шифрование его данных или соединения. Можно пожертвовать высокой скоростью ради увеличения энергоэффективности и снижения себестоимости шифрующего оборудования для сетей стандарта 1 Гбит/с и 10 Гбит/с.

Кролевецкий Алексей,
ООО «Код Безопасности»