РАЗРАБОТКА ПАРАЛЛЕЛЬНОГО АЛГОРИТМА ШИФРОВАНИЯ ГОСТ 28147-89 НА ПЛАТФОРМЕ СОПРОЦЕССОРОВ INTEL XEON PHI

М.С. Миниахметова

Введение

В настоящее время все большее значение приобретают технологии обработки и передачи больших объемов данных. При этом в случае, если эти данные составляют тайну какого-либо уровня, появляется дополнительное требование к защищенности таких данных.

Традиционные подходы к разработке средств криптографической защиты информации обеспечивают информационную безопасность, но при этом могут в значительной степени влиять на скорость ее обработки и передачи по защищенным vpn-каналам и корпоративным сетям передачи данных.

Таким образом, в настоящее время одной из актуальных проблем информационной безопасности является создание эффективных, криптостойких и относительно недорогих аппаратно-программных средств защиты данных.

Как ожидают эксперты, в ближайшем будущем высокопроизводительная обработка данных будет базироваться на использовании гетерогенных архитектур, включающих центральный процессор и использующих ускорители (или сопроцессоры) для достижения высокой скорости вычислений [1].

В настоящее время ведутся исследования, посвященные разработке параллельного алгоритма шифрования ГОСТ 28147-89 для платформ с графическими ускорителями: технологии CUDA[2], OpenGL, DirectX[3]. Однако на сегодня, по-видимому, отсутствуют даннфе об исследованиях, посвященных разработке параллельных криптографических алгоритмов для сопроцессоров Intel Xeon Phi, преимуществом которых является переносимость и универсальность программ, написанных для этой платформы.

Описание алгоритма

ГОСТ 28147-89 [4] – симметричный алгоритм блочного шифрования; размер блока 64 бит, размер ключа 256 бит, количество раундов сети Фейстеля – 32 [5]. Также в процессе обработки используется дополнительный ключ, называемый S-блоком и представляющий собой перестановку чисел от 0 до 15. Способ генерации S-блоков в стандарте не оговаривается. Обычно они генерируются разработчиками с помощью генератора случайных чисел. S-блоки являются дополнительным ключевым материалом и должны храниться в секрете.[6] Существуют четыре режима работы данного алгоритма: режим простой замены, режим гаммирования, гаммирование с обратной связью и режим выработки имитовставки. Режим простой замены предполагает разбиение сообщения на 64-битные блоки с последующей независимой обработкой каждого блока. Таким образом, данный режим алгоритма шифрования ГОСТ 28147-89 позволяет выполнить распараллеливание обработки по данным. На рис. 1 представлена схема раунда сети Фейстеля для алгоритма ГОСТ 28147-89.

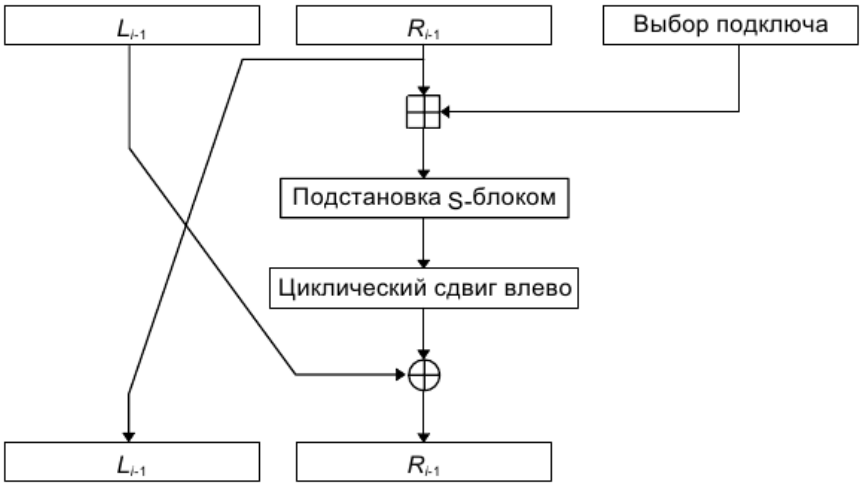

Рис. 1. Схема шифрования по алгоритму ГОСТ 28147-89

Архитектура Intel Xeon Phi

Intel Xeon Phi – сопроцессоры корпорации Intel с архитектурой Intel Many Integrated Core (Intel MIC), предназначенные для массивно-параллельных вычислений. Архитектура Intel MIC предполагает объединение 60 процессорных ядер x86, размещенных на общей плате. Каждая плата оснащена собственной оперативной памятью, объем которой составляет 8 Гбайт, а также имеет собственную полноценную операционную систему – специализированную сборку Linux, что, в частности, позволяет организовать доступ к плате сопроцессора из сети, как к отдельному вычислительному узлу. Каждое ядро имеет собственный кэш 1 и 2 уровня, при этом обеспечивается когерентность кэшей всех ядер. Архитектура сопроцессоров Intel Xeon Phi представлена на рис. 2.

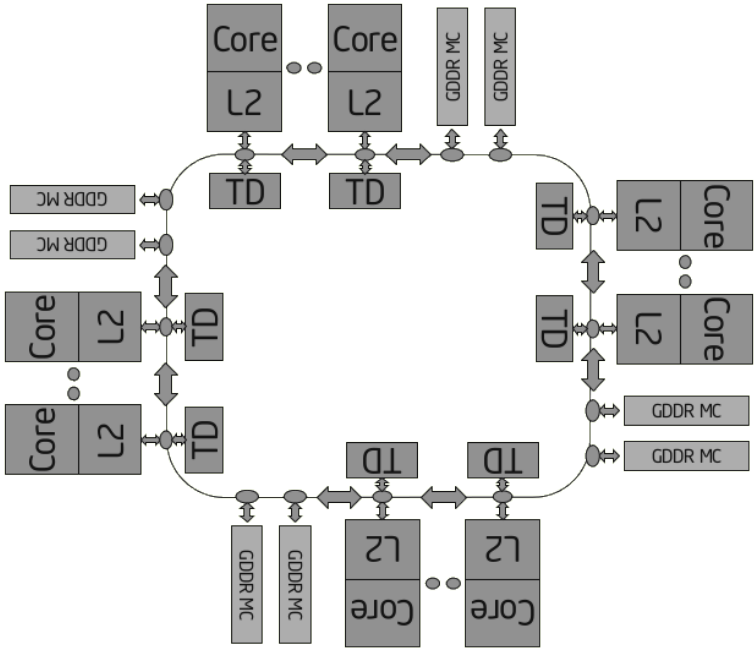

Рис. 2. Архитектура Intel Xeon Phi

Плата сопроцессора Intel Xeon Phi соединяется с центральным процессором Intel Xeon через шину PCI Express, по которой данные передаются от центрального процессора к плате ускорителя и в обратном направлении. На момент написания статьи сопроцессорами Intel Xeon Phi поддерживался стандарт PCI Express 2.0.

Для разработки программ для платформы Intel Xeon Phi используются стандартные языки программирования, такие как C, C++ и Fortran, а также стандартные технологии параллельной обработки данных: OpenMP, Intel MPI, Intel TBB, Intel Cilk , «встроенный» параллелизм функций библиотеки Intel MKL [7].

Проектирование и разработка алгоритма

Разработка параллельного алгоритма ГОСТ 28147-89 для платформы с многоядерными ускорителями Intel Xeon Phi предполагает реализацию последовательного алгоритма ГОСТ 28147-89 и последующее распараллеливание последовательного алгоритма по технологии многопоточного программирования для архитектуры Intel Xeon Phi.

Для написания программы, реализующей последовательный алгоритм ГОСТ 28147-89, нами был выбран язык программирования C и технология многопоточного программирования OpenMP.

Приложение состоит из двух основных модулей: модуля обработки сообщения и криптографического модуля.

В криптографическом модуле определяется набор ключей шифрования и реализуются функции генерации ключей шифрования и таблиц подстановок, а также функции шифрования и дешифрования сообщения.

Модуль обработки сообщения выделяет буфер памяти оптимального размера, считывает данные из входного файла в буфер и вызывает функции шифрования и дешифрования сообщения, реализованные в криптографическом модуле.

Для организации параллельной обработки при шифровании и дешифровании сообщения в данной работе была выбрана технология OpenMP. Такой выбор обусловлен, прежде всего, тем, что OpenMP является признанным стандартом параллельного программирования для систем с общей памятью.

При проектировании параллельного алгоритма был использован подход параллелизма поданным. В данной работе он заключается в следующем.

Обработка сообщения выполняется в режиме offload сопросцессора Intel Xeon Phi. В начале обработки заполненный буфер и набор ключей шифрования выгружаются на сопроцессор. Для каждого 8-байтового (64-

битового) блока буфера вызывается функция шифрования. При этом с помощью прагмы omp for инициализируется обработка каждого блока в отдельном потоке. По окончании шифрования буфер выгружается в основную память и записывается в выходной файл главным процессом.

На рис. 3 представлена UML-диаграмма деятельности разработанного алгоритма.

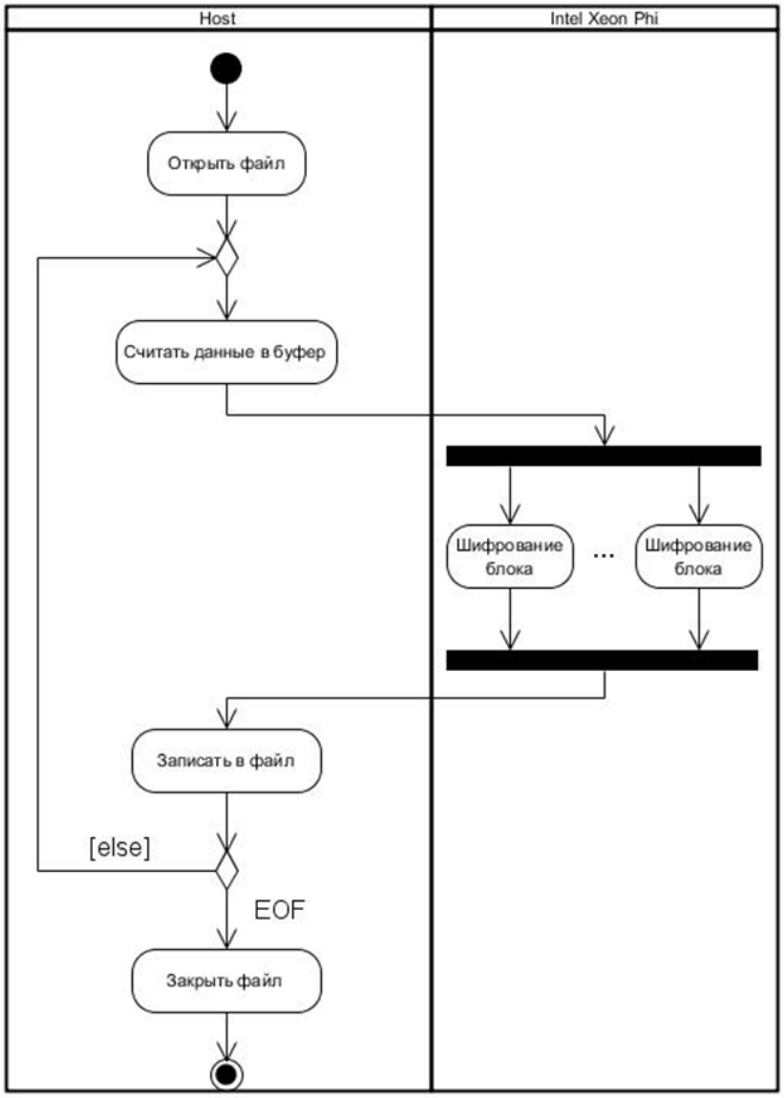

Рис. 3. Диаграмма деятельности параллельного алгоритма ГОСТ 28147-89

Вычислительные эксперименты

Для исследования эффективности разработанного алгоритма нами были проведены вычислительные эксперимента на суперкомпьютере «Торнадо ЮУрГУ». Для тестирования был выделен один узел с установленным сопроцессором Intel Xeon Phi.

Технические характеристики узла:

Процессор Intel Xeon X5680 (6 ядер, 3.33 ГГц)

Оперативная память 24ГБ

Сопроцессор Intel Xeon Phi SE10X:

Основными целями вычислительных экспериментов были: определение зависимости скорости шифрования от объема шифруемых данных и определение зависимости скорости шифрования от числа потоков, запущенных на сопроцессоре.

Для определения зависимости скорости шифрования от объема входных данных были взяты файлы размером 64, 128, 256, 512, 1024, 2048, 4096 и 5120 МБ. На рис. 4 представлен график зависимости скорости шифрования от объема входного файла.

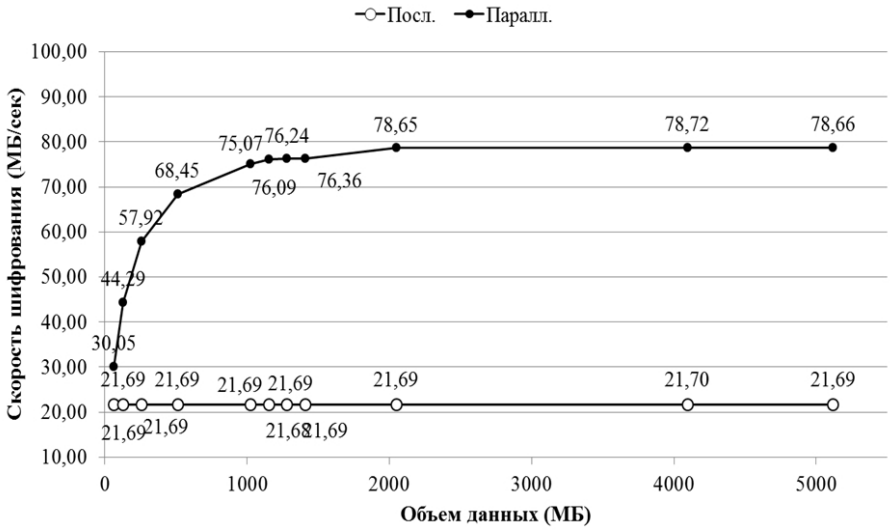

Рис. 4. Зависимость скорости шифрования от размера шифруемых данных

Из результатов данного эксперимента можно сделать вывод, что скорость шифрования разработанной параллельной реализацией алгоритма ГОСТ 28147-89 в среднем в 3,5 раза выше, чем скорость работы последовательной реализации этого алгоритма.

Для вычислительных экспериментов с целью определения зависимости скорости шифрования от числа запущенных на сопроцессоре потоков, был использован файл размером 1024 МБ. На рис. 5 представлен график зависимости скорости шифрования от числа запущенных на сопроцессоре потоков.

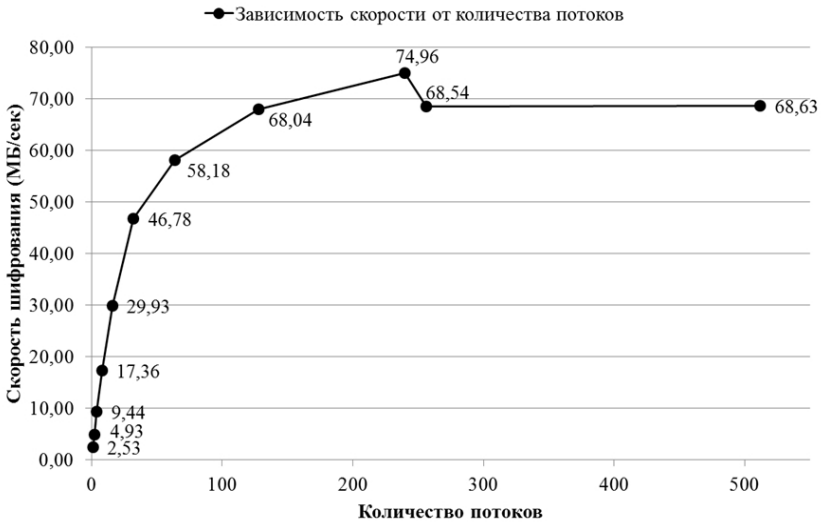

Рис. 5. Зависимость скорости шифрования от числа потоков на сопроцессоре

Из приведенных данных можно сделать вывод, что скорость обработки данных размером 1024 МБ одним потоком, почти в 29 раз меньше, чем при использовании максимального для Intel Xeon Phi количества количества потоков – 240.

Заключение

В работе описана параллельная реализация симметричного блочного криптографического алгоритма ГОСТ 28147-89.

При разработке данного алгоритма была использована модель распараллеливания по данным. Считывание данных и заполнение буфера выполняется центральным процессором, после чего буфер передается на сопроцессор, где происходит параллельная обработка всех блоков входных данных.

В завершение приведены результаты вычислительных экспериментов, подтверждающих результаты разработанного решения.

ЛИТЕРАТУРА:

1. Yelick K. Exascale Computing: More and Moore? // ACM Intl. Conf. on Computing Frontiers. 2011 г.

2. Коробицын В.В., Ильин С.С. Реализация симметричного шифрования по алгоритму ГОСТ 28147 на графическом процессоре с использованием технологии CUDA // Информационные технологии. 2011 г.. № 4. С.41-46.
3. Коробицын В.В., Ильин С.С. Реализация симметричного шифрования по алгоритму ГОСТ-28147 на графическом процессоре // Информационные технологии. 2008 г.. № 10. С.46-51.
4. ГОСТ 28147-89 Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования: государственный стандарт РФ от 30.06.1990, ИПК Издательство стандартов, 1990 г.. 28с.
5. Баричев С.Г., Серов Р.Е. Основы современной криптографии, Изд-во Горячая линия – Телеком, 2002. 122с.
6. Шнайер Б. Прикладная криптография, Изд-во Триумф, 2002 г., 816с.
7. Intel Xeon Phi Coprocessor – the Architecture. URL: http://software.intel.com/en-us/articles/intel-xeon-phi-coprocessor-codename-knights-corner.