УДК 004.272, 004.31

РАСПАРАЛЛЕЛИВАНИЕ АЛГОРИТМА БЛОЧНОГО ШИФРОВАНИЯ ДАННЫХ СО СЦЕПЛЕНИЕМ БЛОКОВ

М. В. Качинский, А. В. Станкевич, А. И. Шемаров
Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», г. Минск, Республика Беларусь

Аннотация. Блочные алгоритмы шифрования находят широкое применение для решения задач в области практической криптографии. Ряд модификаций алгоритмов блочного шифрования, например, при реализации алгоритмов со сцеплением блоков, требуют значительного времени шифрования большого потока данных за счет последовательной обработки блоков. Предлагается режим распараллеливания алгоритма блочного шифрования данных со сцеплением блоков путем линейной декомпозиции входного потока данных.
Ключевые слова: Шифрование, алгоритм блочного шифрования, сцепление блоков, блок, ключ, синхропосылка, декомпозиция потока данных, распараллеливание, программируемое логическое устройство.

PARALLELIZATION OF A BLOCK CIPHER ALGORITHM WITH CIPHER BLOCK CHAINING

M.V. Kachinsky, A.V. Stankevich, A.I. Shemarov
Educational Institution "Belarusian State University of Informatics and Radioelectronics", Minsk, Republic of Belarus

Abstract. Block encryption algorithms are widely used to solve problems in practical cryptography. Some modifications of block encryption algorithms, such as those cipher block chaining algorithms, require significant time to encrypt a large data stream due to sequential processing of blocks. A mode for parallelizing a block encryption algorithm with block chaining through linear decomposition of the input data stream is proposed.
Keywords: Encryption, block cipher algorithm, block chaining, block, key, initialization vector, data flow decomposition, parallelization, programmable logic device.

Введение

Блочные алгоритмы шифрования находят широкое применение для решения задач в области практической криптографии. Оборудование, использующее блочные алгоритмы для шифрования данных с симметричным ключом, появилось достаточно давно. Применение специализированных вычислительных аппаратных средств позволило увеличить эффективность систем безопасности. Эволюция аппаратных комплексов шифрования определялась в первую очередь элементной базой. Коренным образом подход к решению задач шифрования изменился в связи с появлением программируемых логических устройств.

С повышением количества элементов в программируемой логической микросхеме появляется возможность использования все более и более сложных алгоритмов. Алгоритмы блочного шифрования обычно хорошо распараллеливаются и конвейеризируются, что позволяет легко масштабировать аппаратное решения, но только для тех модификаций алгоритма, которые не используют предыдущий зашифрованных блок для обработки следующего блока.

Основная часть

Прогресс в области создания и совершенствования оборудования в итоге приводит к увеличению размеров обрабатываемых потоков данных. Ряд модификаций алгоритмов блочного шифрования, позволяющих получать хорошую криптостойкость, например, при реализации алгоритмов со сцеплением блоков, требуют значительного времени шифрования большого потока данных за счет последовательной обработки блоков. Это связано не с тем, что не существует теоретической возможности распараллеливания процесса шифрования в этих режимах, а определяется жесткой регламентацией процессов шифрования, регулируемых действующими стандартами. Стандарты, в итоге модифицируются и изменяются в соответствии с новыми требованиями, предъявляемыми развитием информационной инфраструктуры и задачами, решаемыми на конкретном этапе создания и развития информационных систем, но этот процесс достаточно медленный.

В работе предлагается режим распараллеливания алгоритма блочного шифрования со сцеплением блоков. Идея способа заключается в возможности декомпозиции шифруемого потока на отдельные потоки. В стандартах блочного шифрования не накладываются жесткие ограничения на количество потоков данных, которые могут быть зашифрованы с помощью одного ключа. Поэтому шифрование разделенных потоков может осуществляться параллельными структурами. Количество одновременно обрабатываемых потоков определяется только существующей в конкретный момент времени технологией создания микросхем требуемой степени интеграции. Однако для реализации алгоритмов блочного шифрования со сцеплением блоков требуется задание начального вектора или синхропосылки. На количество используемых одновременно синхропосылок обычно накладываются ограничения, так как это может теоретически приводить к дискредитации ключа при определенном наборе данных.

Для того чтобы не использовать несколько различных синхропосылок, что затрудняет реализацию алгоритма, или одну и туже

синхропосылку для шифрования различных потоков, что может снизить криптостойкость алгоритма в целом, предлагается следующий режим работы. Шифрование потока начинается как одного целого потока данных, а далее, после шифрования требуемого количества блоков, определяемого количеством подпотоков, на которые будет разделен исходный поток (определяется количеством параллельно работающих устройств шифрования), происходит декомпозиция потоков. Процесс шифрования в этос случае распараллеливается. Иллюстрация режима распараллеливания потока данных на восемь потоков при реализации алгоритма блочного шифрования со сцеплением блоков приведена в таблице «Распараллеливание потока данных для шифрования».

Заключение

Таким образом, путем декомпозиции входного потока данных, может быть достигнута возможность введения режима распараллеливания алгоритма блочного шифрования данных со сцеплением блоков. В работе приведен линейный алгоритм распределения блоков между устройствами шифрования. Для повышения криптостойкости можно использовать нелинейное распределение блоков по устройствам шифрования.

Распараллеливание потока данных для шифрования
Data flow parallelization for encryption

№ Итерации	УШ 0	УШ 1	УШ 2	УШ 3	УШ 4	УШ 5	УШ 6	УШ 7
0	Синхро-посылка							
1	Блок0							
2	Блок1							
3	Блок2							
4	Блок3							
5	Блок4							
6	Блок5							
7	Блок6							
8	Блок7							
9	Блок15	Блок14	Блок13	Блок12	Блок11	Блок10	Блок9	Блок8
10	Блок23	Блок22	Блок21	Блок20	Блок19	Блок18	Блок17	Блок16
11	…	…	…	…	…	…	…	…

УШ – Устройство шифрования

Сведения об авторах

Качинский М.В., канд. техн. наук, доц., доцент кафедры встраиваемых вычислительных систем, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», kachinsky@bsuir.by.

Станкевич А.В., канд. техн. наук, доц., доцент кафедры встраиваемых вычислительных систем, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», stankevich@bsuir.by.

Шемаров А.И., канд. техн. наук, доц., доцент кафедры встраиваемых вычислительных систем, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», shemarov@bsuir.by.

Information about the authors

Kachinsky M., Ph.D. in Computer Sciences, Associate Professor, department of electrical engineering, Educational Institution "Belarusian State University of Informatics and Radioelectronics", kachinsky@bsuir.by

Stankevich A., Ph.D. in Computer Sciences, Associate Professor, department of electrical engineering, Educational Institution "Belarusian State University of Informatics and Radioelectronics", stankevich@bsuir.by.

Shemarov A., Ph.D. in Computer Sciences, Associate Professor, department of electrical engineering, Educational Institution "Belarusian State University of Informatics and Radioelectronics", shemarov@bsuir.by