ШЕВЧЕНКО Д.А., ДЕРБУНОВИЧ Л.В.

МОДЕЛИРОВАНИЕ ЦИФРОВЫХ СХЕМ ОБРАБОТКИ ИНФОРМАЦИИ НА ЯЗЫКЕ VHDL. АЛГОРИТМ КРИПТОРГАФИЧЕСКОЙ ЗАЩИТЫ AES

Описан итерационный блочный шифр AES и его реализация средствами языка VHDL. Показаны достоинства данной реализации.

Проблема защиты информации была актуальна во все времена. В настоящее время, кода информация все чаще представлена в электронном виде и передается преимущественно через сеть Internet, существует высокая вероятность несанкционированного доступа к ней посторонних лиц. Наверное, наиболее эффективным способом защиты информации является ее шифрование. На протяжении нескольких десятков лет военные, политические, коммерческие организации разных стран мира используют определенные алгоритмы криптографической защиты, которые стали стандартами для этих стран. Среди них наиболее совершенными и широко применяемыми являются: ГОСТ 28147-89 - отечественный стандарт, AES – американский стандарт. Среди этих двух алгоритмов наиболее совершенным и наиболее стойким является второй – AES. В его основе лежит алгоритм *RIJNDAEL*, который разработан бельгийскими учеными Йоаном Дэменом и Винсентом Райменом. *RIJNDAEL*- это итерационный блочный шифр, имеющий архитектуру "Квадрат". Шифр имеет переменную длину блоков и различные длины ключей. Длина ключа и длина блока могут быть равны независимо друг от друга 128, 192 или 256 битам. В стандарте *AES* определена длина блока данных, равная 128 битам. Промежуточные результаты преобразований, выполняемых в рамках криптоалгоритма, называются *состояниями (State).* Состояние можно представить в виде прямоугольного массива байтов (рис. 2.1). При размере блока, равном 128 битам, этот 16-байтовый массив имеет 4 строки и 4 столбца (каждая строка и каждый столбец в этом случае могут рассматриваться как 32-разрядные слова).

Алгоритм имеет N число раундов в зависимости от размера блока входных данных и блока ключа.

Раунд состоит из четырех различных преобразований:

• замены байтов *SubBytesQ* - побайтовой подстановки в 5-блоьах с фиксированной таблицей замен размерностью 8 x 256;

• сдвига строк *ShiftRowsQ* - побайтового сдвига строк массива *State* на различное количество байт;

• перемешивания столбцов *MixCoIumnsQ* - умножения столбцов состояния, рассматриваемых как многочлены над *GF(2*), на многочлен третьей степени *g(x)* по модулю $x^4 + 1$;

• сложения с раундовым ключом *AddRoundKeyQ* - поразрядного *XOR* с текущим фрагментом развернутого ключа.

State

a_0	a_4	a_8	a_{12}
a_1	a_5	a_9	a_{13}
a_2	a_6	a_{10}	a_{14}
a_3	a_7	a_{11}	a_{15}

Рис. 2.1. Пример представления 128-разрядного блока данных в виде массива *State*, где a - байт блока данных, а каждый столбец - одно 32-разрядное слово

При этом преобразование происходит по правилам умножения в полях Галуа с использованием регистров сдвига с линейными обратными связям*и* - LFSR (Linear Feedback Shift Register). Эти устройства являются идеальным средством защиты от случайных деструктивных воздействий. Основными достоинствами *LFSR* являются:

• простота аппаратной и программной реализации;

• высокое быстродействие;

• хорошие статистические свойства формируемых последовательностей в режиме генерации псевдослучайных последовательностей (ПСП);

• возможность построения на их основе генераторов, обладающих свойствами, ценными при решении специфических задач защиты информации (формирование последовательностей произвольной длины, формирование последовательностей с пред-периодом, формирование ПСП с произвольным законом распределения, построение генераторов, обладающих свойством самоконтроля и т. п.).

Была поставлена проблема реализации алгоритма AES на кристалле ПЛИС (фирмы Xilinx), используя средства языка VHDL. С помощью VHDL были описаны все блоки алгоритма и сгруппированы в единую структуру. В результате получилось устройство зашифрования и дешифрования данных.

Реализация алгоритма шифрования на языке VHDL имеет множество преимуществ. Во-первых, такая программно-аппаратная реализация имеет большую стойкость к взлому по сравнению с только программной реализацией. Во-вторых, она требует меньше ресурсов. Тип кристалла позволяет в любое время внести изменения в структуру устройства, если требования к шифрованию будут изменены (например, разная длина ключа). В результате моделирования было показано, что устройство успешно шифрует блоки длиной 128 бит и 128 бит для ключа и данных соответственно.