Родинко М.Ю.

АНАЛИЗ ЦИКЛОВЫХ ФУНКЦИЙ БЛОЧНЫХ СИММЕТРИЧНЫХ ШИФРОВ

Блочные симметричные шифры (БСШ) часто строятся путем итеративного повторения нелинейных функций несколько раз. Оправданием этому является тот факт, что несколько итераций простой нелинейной функции могут привести к сложной нелинейной функции, которая, однако, все еще остается достаточно простой для анализа, описания и реализации. Одна итерация называется циклом, а итеративная функция – цикловой функцией.

В основе цикловых функций многих современных БСШ лежат принципы путаницы и диффузии, заложенные еще К. Шенноном [1]. Простой способ реализации принципа путаницы состоит в применении нелинейной подстановки (замены) к шифруемому блоку. Нелинейная функция часто реализуется с помощью таблицы подстановки, называемой S-блоком. Одним из способов достижения эффекта диффузии является использование перестановки для перемешивания разных частей шифруемого блока. В качестве перестановки часто используется линейная функция. Применение более общих или аффинных функций, чем простая перестановка, увеличивает мощность диффузионного преобразования. Этот шаг гарантирует, что изменение одного бита в открытом тексте приведет к изменению приблизительно половины битов шифртекста.

Одним из наиболее популярных цикловых преобразований является преобразование, используемое в шифре Rijndael, где последовательное применение нелинейной и линейной функций реализует т.н. стратегию широкого следа [2]. В качестве линейной функции здесь используется умножение на МДР матрицу. Такое линейное преобразование обладает высоким коэффициентом ветвления и на сегодняшний день считается наиболее оптимальным.

Мы хотим рассмотреть две схемы цикловых преобразований, в которых нет четкого разделения на линейную и нелинейную составляющие, т.е. стратегия широкого следа реализуется в рамках единого преобразования.

Первое цикловое преобразование, названное нами преобразованием на основе управляемых подстановок, представлено на рис. 1.

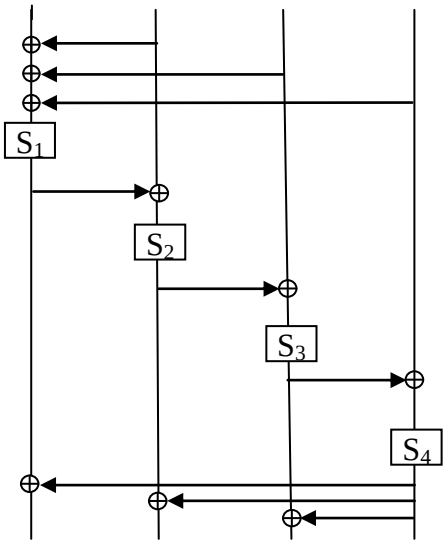

Рис. 1. Цикловая функция на основе управляемых подстановок

Как следует из этого рисунка, 32-х битный входной блок данных делится на четыре байта, каждый из которых проходит через цепочку из S-блоковых преобразований. При этом на вход первого S-блока подаётся сумма по модулю два всех четырёх байтовых сегментов. Второй, третий и четвёртый байтовые сегменты поступают на соответствующие входы других S-блоков, где они предварительно объединяются через сумматоры по модулю два с выходами предыдущих S-блоков. Кроме того, выход последнего S-блока складывается по модулю два с выходами всех предыдущих S-блоков, формируя выходы SL преобразования.

Число ветвлений, определяемое как число активных S-блоков в смежных циклах, в данной конструкции теряет смысл, так как она обеспечивает с большой вероятностью

активизацию сразу всех S-блоков смежных циклов (в этой конструкции при активизации одного байта входа принудительно активизируются все четыре входящих в неё S-блока).

Второе преобразование – цикловое преобразование на основе латинского квадрата. В этом случае таблицу подстановок представляют в виде латинского квадрата, размерность которого определяется размером шифруемого подблока. Преобразование осуществляется путем выбора в качестве выходного байта значения ячейки таблицы, которая определяется по строке – значением шифруемого подблока, а по столбцу – значением выхода подстановки на предыдущем шаге. Недостаток метода заключается в том, что в случае использования байтовой подстановки таблица будет иметь размер равный 64 Кб. В случае ограничения на размер доступной памяти целесообразно использовать полубайтовую подстановку, для которой необходимо всего 256 байт памяти. Для сравнения – оптимизированное цикловое преобразование с умножением на МДР матрицу требует 1 Кб памяти для хранения таблицы предвычислений.

В табл. 1 приведены полученные нами результаты эффективности предложенных схем цикловых преобразований и оптимизированного преобразования с умножением на МДР матрицу. Как видно из таблицы, пока нам не удалось достичь эффективности, сравнимой с преобразованием из шифра Rijndael. Однако эффективность преобразования во многом зависит от его конкретной программной реализации. Мы планируем оптимизировать реализацию предложенных методов и уточнить полученные результаты по скоростным характеристикам.

Таблица 1

Результаты измерения скоростных характеристик цикловых функций

	Оптимизированная цикловая функция с умножением на МДР матрицу	Цикловая функция на основе управляемых подстановок	Цикловая функция на основе латинского квадрата
Время шифрования константного блока 100 млн. раз, сек	$4{,}052\times10^{-7}$	0,978	0,046
Время шифрования 100 млн. различных блоков, сек	0,258	1,642	1,268

Список использованных источников

1. Shannon, C.E. Communication Theory of Secrecy Systems / C.E Shannon // Bell System Technical Journal. - 1949. - Vol. 28. – pp. 656-715.

2. Landau, S. Polynomials in the Nation’s Service: Using Algebra to Design the Advanced Encryption Standard. – February, 2004.

Бурлака А.А., Килимник О.В.

МЕТРОЛОГІЧНЕ ЗАБЕЗПЕЧЕННЯ ЗАСОБІВ ВИМІРЮВАННЯ, ЩО ЗАСТОСОВУЮТЬСЯ ПРИ ПОБУДОВІ, НАЛАШТУВАННІ ТА ОБСЛУГОВУВАННІ ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖ

Сучасний рівень розвитку телекомунікаційних мереж характеризується використанням високотехнологічного автоматизованого обладнання на базі останніх досягнень радіотехніки та мікроелектроніки, а також мікропроцесорної техніки та електронно-обчислювальних машин, що дозволяє реалізувати високоефективні системи для вирі-