УДК 004.432

А.Я. Белецкий, А.А. Белецкий

Национальный авиационный университет, Киев

СИНХРОННЫЙ АЛГОРИТМ ПОТОЧНОГО ШИФРОВАНИЯ ЦИФРОВОЙ ИНФОРМАЦИИ

Введение и постановка задачи

При шифровании больших объемов данных в реальном времени (таких, например, как речь или «живое видео») применяются *поточные* криптографические системы (шифры, генераторы, алгоритмы). Суть поточных шифров заключается в сложении по модулю 2 битов потока ключей с битами сообщений. В современных криптосистемах поток ключей (*поточный ключ*) генерируется из короткого основного (*базового*) ключа с помощью однозначно определенных детерминированных правил, осуществляющих так называемую процедуру *разворачивания ключа*.

Поточные шифры принято разделять на *синхронные* и *самосинхронизирующиеся* (или *асинхронные*) шифраторы. В синхронных поточных шифрах поточный ключ (*гаммирующая функция* или *гамма*) формируется независимо от входной последовательности, каждый элемент (бит, байт и т.п.) которой таким образом шифруется независимо от других элементов. Если же поточный ключ зависит от исходных данных и результата их криптопреобразования, то шифрование называют самосинхронизирующимся. Большинство реализаций поточного шифрования являются синхронными.

К настоящему времени разработано большое количество разнообразных по способу генерирования псевдослучайных последовательностей и по техническим характеристикам генераторов ПСП [1 – 3]. В поточных шифрах осуществляется, как правило, последовательное шифрование битов данных. Реже используются поточные шифры, в которых элементами шифрования выступают байты и другие (по размеру) элементы входного текста.

В докладе предлагается синхронный SPB поточный криптографический алгоритм, размер секретного ключа в котором составляет 128 бит. Отличительная особенность SPB генераторов состоит в том, что за один шаг шифрования в системе формируется блок гаммы длиною 128 бит, образующейся в результате стохастических операций нелинейной подстановки (*Substitution*) и перестановки (*Permutation*), дополненные стохастической прокруткой блока (*Blok*) поточной гамма-функции.

Краткая характеристика алгоритма

Основу алгоритма составляют шенноновские криптопримитивы подстановок и перестановок (*Substitution – Permutation*), дополненные операцией стохастического циклического сдвига (*Shift*). Схема функционирования алгоритма показана на рис. 1.

На этапе инициализации шифратора секретный 128-битный ключ (*Key* 128) размещается в регистре ключевого поля *RKF*. В блоке *Shift* осуществляется круговой сдвиг содержимого регистра *RKF* на нечетное число $Z \in [1,63]$, которое вычисляется следующим образом. Все 16 байтов регистра *RKF* поразрядно суммируются по mod 2 и в младший разряд результирующего байта B заносится 1 (для обес-

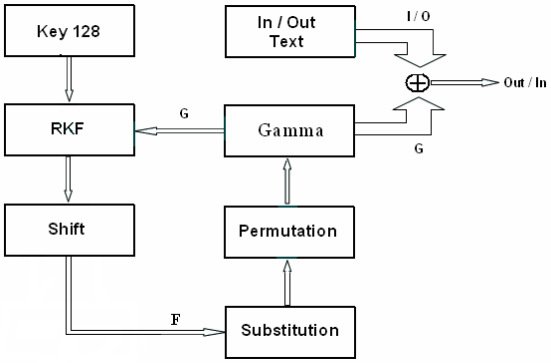

Рис. 1. Обобщенная структурная схема SPB-шифратора

Таблица 1

Последовательности перестановок байтов в операторе *Per*

p	Десятичный номер ячейки X															
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	0	11	8	15	1	10	14	4	13	6	3	12	7	9	5	2
1	9	0	4	11	7	13	3	14	12	15	2	5	10	1	6	8
2	4	5	0	8	15	14	10	13	2	9	7	11	6	12	1	3
3	12	7	9	0	3	8	15	10	4	1	6	13	5	11	2	14
4	5	8	1	9	0	3	13	2	7	12	15	14	11	6	10	4
5	14	3	5	12	4	0	11	7	1	10	13	6	8	2	9	15
6	11	9	15	6	10	7	0	12	3	13	5	8	2	14	4	1
7	2	6	12	4	8	5	1	0	9	14	10	15	13	3	7	11
8	3	10	7	14	5	2	4	1	0	8	12	9	15	13	11	6
9	1	14	10	3	6	9	8	11	5	0	4	2	12	7	15	13
10	7	2	11	1	13	4	6	3	8	5	0	10	14	15	12	9
11	10	15	14	7	9	12	2	8	6	3	11	0	1	4	13	5
12	6	4	2	13	14	1	7	15	10	11	9	3	0	5	8	12
13	13	1	3	10	11	6	12	5	15	2	8	4	9	0	14	7
14	15	12	13	5	2	11	9	6	14	4	1	7	3	8	0	10
15	8	13	6	2	12	15	5	9	11	7	14	1	4	10	3	0

печения нечетности). Младшие шесть разрядов байта B как раз и определяют значение параметра прокрутки Z.

Нелинейная подстановка реализуется по классической схеме и отвечает преобразованию байтов x регистра ключевого поля соотношением

$$y = (x^{-1} \cdot A)_2,$$

где $(a)_2 = a \bmod 2$ – операция приведения результатов матричных вычислений к остатку по $\bmod 2$; x^{-1} – мультипликативное обратное значение байта x над неприводимым полиномом g, двоичная форма которого имеет вид: $g = 100011101$; и, наконец, A – невырожденная в кольце вычетов по $\bmod 2$ матрица, в качестве которой выбрана матрица

$$A = \begin{bmatrix} 1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{bmatrix}.$$

Перестановка байтов выполняется по следующей схеме. Байт, находящийся по адресу X в регистре оператора *Sub*, перемещается в ячейку Y регистра оператора *Per*. Значения Y выбираются из p-й строки табл. 1, причем номер p определяется содержимым четырех младших разрядов регистра оператора *Sub*.

Выводы

Испытания, проведенные с использование пакета NIST STS [4], подтвердили высокое качество статистических свойств псевдослучайных последовательностей, формируемых предлагаемым поточным шифратором.

Разработанный SPB алгоритм имеет четкую и ясную структуру, достаточно простой как в программной, так и аппаратной реализациях, доставляет высокую скорость криптогафических преобразований и может быть рекомендован для разработки систем поточного шифрования.

Список литературы

1. Асосков А.В. Поточные шифры / А.В. Асосков, М.А. Иванов, А.А. Мирский и др. – М.: КУДИЦ-ОБРАЗ, 2003. – 336 с.

2. Шнайер Б. Прикладная криптография / Б. Шнайер. – М.: ТРИУМФ, 2003. – 816 с.

3. Поточные шифры. Результаты зарубежной открытой криптологии. – 390 с. – [Электронный ресурс]. – Режим доступа к ресурсу: http://www.ssl.stu.neva.ru/psw/crypto.html

4. Random Number Generation and Testing. – [Электронный ресурс]. – Режим доступа к ресурсу: http://www.csrc.nist.gov/rng/