УДК 621.658.012.531

В.А. Василенко, ст. преподаватель
В.В. Кудрявченко
Севастопольский национальный технический университет
Студгородок, г. Севастополь, Украина, 99053
E-mail: root@sevgtu.sebastopol.ua

ОРГАНИЗАЦИЯ ПОТОКОВЫХ ШИФРОВ НА БАЗЕ РЕГИСТРОВ С ОБРАТНОЙ СВЯЗЬЮ ПО ПЕРЕНОСУ

Рассматриваются возможные пути построения потоковых шифров с помощью регистров с обратной связью различных модификаций.

Потоковые шифры преобразуют открытый текст в шифротекст побитово. Простейшая реализация потокового шифра изображена на рисунке 1.

Генератор гаммы выдает поток битов: $K_1, K_2, \ldots, K_i$. Эта гамма шифра или просто гамма и поток битов открытого текста $P_1, P_2, \ldots, P_i$, подвергаются операции XOR (сложению по модулю два). В результате создается поток битов шифротекста

$$C_i = P_i \oplus K_i .$$

При расшифровывании, для восстановления битов открытого текста, над битами шифротекста и той же самой гаммой выполняется операция XOR: $P_i = C_i \oplus K_i$, т.е. $P_i \oplus K_i \oplus K_i = P_i$.

Надежность системы полностью зависит от свойств генератора гаммы. Чем ближе выход генератора гаммы к истинно случайному, тем больше времени потребуется криптоаналитику для вскрытия шифра.

Дальнейшим развитием методов получения потоковых шифров явилось использование регистров сдвига с линейной обратной связью (РСЛОС). Регистр сдвига с обратной связью состоит из двух частей: регистра сдвига и функции обратной связи.

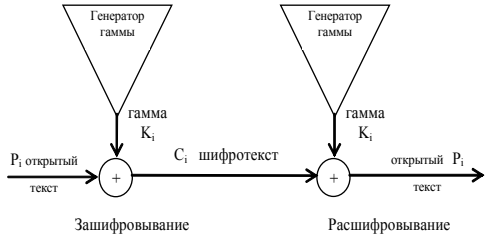

Рисунок 1 – Потоковый шифр

Регистр сдвига представляет собой последовательность битов. Если длина регистра равна n битам, регистр называется n-битовым. При каждом извлечении бита все биты сдвигаются на одну позицию. Новый старший бит рассчитывается как функция всех остальных битов регистра. Периодом регистра называют длину получаемой последовательности до начала ее повторения. Потоковые шифры на базе регистров сдвига легко реализуются с помощью цифровой аппаратуры.

К простейшему типу регистров сдвига с обратной связью относят РСЛОС. Обратная связь представляет собой операцию XOR над некоторыми битами регистра. Перечень этих битов называется последовательностью отводов. Благодаря простоте последовательности обратной связи, для анализа РСЛОС можно использовать довольно развитую математическую теорию. В криптографии РСЛОС используются чаще, чем другие.

В настоящее время существует множество описаний алгоритмов построения потоковых шифров на базе РСЛОС, таких как шифр A5, Rambutan, Fish, Pike, Mush, алгоритм Джиффорда и др. Описание алгоритмов потоковых шифров на базе регистров сдвига с обратной связью по переносу (РСОСП) встречаются крайне редко и носят неконкретный характер. В данной работе предлагается ряд подходов к построению таких шифров. В общем случае РСОСП напоминает РСЛОС. В обоих использованы регистр сдвига и функция обратной связи (ОС), однако, в РСОСП предусмотрен ещё регистр переноса (рисунок 2).

В регистрах с линейной ОС выполняется операция XOR (сложение по модулю два) над всеми битами последовательности отводов, в РСОСП эти биты складываются друг с другом и содержимым регистра переноса. Новым битом становится результат по модулю два. В регистр переноса заносится результат, поделённый на 2, этот результат становится новым содержимым регистра переноса.

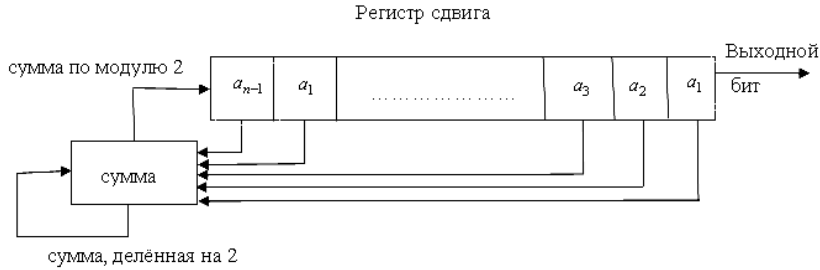

Рисунок 2 – Регистр сдвига с обратной связью по переносу

Регистром переноса служит не бит, а число. Размер этого регистра должен быть не менее $\log_2 m$, где m – число отводов. РСОСП с некоторой начальной задержкой переходит в циклический режим, максимальный период которого равен не $2^n - 1$ (n – длина регистра сдвига), а q-1 (где q – число обратной связи). Число q задаётся отводами и определяется так [1,2]:

$$q = 2q_1 + 2^2 q_2 + ... + 2^n q_n - 1$$

(q должно быть простым числом, для которого 2 – примитивный корень).

Любое начальное состояние завершается одной из четырёх ситуаций:

1) оно может быть частью максимального периода;

2) после начальной задержки оно может породить бесконечную последовательность нулей;

3) оно может перейти в последовательность максимального периода после начальной задержки;

4) после начальной задержки это состояние может породить бесконечную последовательность единиц.

Идея использования в криптографии РСОСП всё ещё не имеют серьёзных практических реализаций. Впервые она была выдвинута Энди Клаппером и Марком Горески [3]. Однако чёткой математической теории этих регистров до сих пор в литературе не появилось. Так же как анализ РСЛОС основан на сложении примитивных полиномов по модулю два, анализ РСОСП основан на суммировании неких чисел, называемых 2-адическими (2-adic). Существует также 2-адический аналог алгоритма Берлекэмпа [4]. Это означает, что на базе РСОСП можно строить потоковые шифры по аналогии с РСЛОС. Можно строить шифры и на комбинации РСЛОС и РСОСП.

Пример каскада для получения потокового шифра приведен на рисунке 3. Алгоритм функционирования каскада РСЛОС/РСОСП (рисунок 3) предполагает, что тактируется первый массив РСЛОС, а результаты объединяются сложением с переносом. Если выход функции объединения равен 1, то тактируется следующий массив (из РСОСП), и выход этих РСОСП объединяется с выходом предыдущей функцией объединения операцией XOR. Если выход первой функции объединения равен 0, то массив РСОСП не тактируется, а выход просто складывается с переносом, полученным на предыдущем раунде. Если выход этой второй функции объединения равен 1, то тактируется третий массив (из РСЛОС) и т.д. Генератор использует множество регистров $n = m \times k$, где m – число этапов, k – число регистров на этап. Чередуя эти величины, получим разные потоковые шифры.

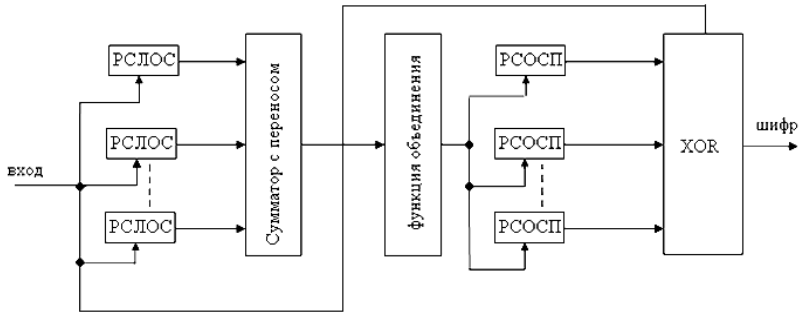

Рисунок 3 – Каскад РСЛОС/РСОСП

Для большей криптостойкости шифров можно предложить чередующийся генератор с комбинированными регистрами (рисунок 4).

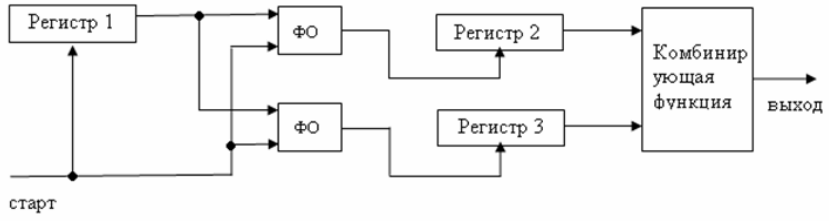

Рисунок 4 – Чередующийся генератор потоковых шифров

Для удобства изложения было взято число регистров равное 3, которое, в принципе, может быть любым.

У генератора, представленного на рисунке 7 возможны следующие режимы шифрования:

1. Регистр 1, Регистр 2 и Регистр 3 – это РСОСП. Комбинирующая функция – XOR.
2. Регистр 1 – РСЛОС; Регистр 2 и Регистр 3 – РСОСП. Комбинирующая функция – XOR.
3. Регистр 1 – РСОСП, а Регистр 2 и регистр 3 – РСЛОС. Комбинирующая функция – сложение с переносом.
4. Регистр 2 – РСЛОС, Регистр 3 – РСОСП, а в качестве Регистра 1 может выступать любой из них. Комбинирующая функция – сложение с переносом.

Предложенный путь построения потоковых шифров в рамках системно-теоретического подхода представляется весьма перспективным для создания разнообразных и достаточно криптостойких образований.

Перспективы дальнейшего исследования потоковых шифров на базе РСОСП состоят в развитии математического аппарата для таких систем, что позволит аналитически определять их стойкость и надежность.

Библиографический список

1. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си / Б. Шнайер. — М.: Изд-во “Триумф”, 2003. — 816 с.
2. Петров А.А. Компьютерная безопасность. Криптографические методы защиты / А.А. Петров. — М.: Изд-во “ДМК”, 2000. — 448 с.
3. Klapper A. 2-adic Shift Registers / A.Klapper, M. Goresky // Cambridge Security Workshop Proceedings. Fast Software Encryption. — 1994. — P. 174 – 178.
4. Klapper A., Feedback Registers Based on Ramfield Extension of the 2-adic Numbers / A. Klapper, M. Goresky // Springer-Verlag. Advances in Cryptology. — 1995. — P. 215 – 222.

Поступила в редакцию 15.06.2005 г.