
УДК 681.3.06

Р.В. Королев

Харьковский университет Воздушных Сил им. Ивана Кожедуба, Украина

АНАЛИЗ АЛГОРИТМА ПОТОЧНОГО ШИФРОВАНИЯ RC4

В работе проведены исследования зависимости расположения единичного элемента в S-блоке с значениями индексных элементов i, j , использование которых приводит к формированию псевдослучайных последовательностей малого периода.

Ключевые слова: генератор псевдослучайных чисел, RC4.

Введение

Постановка проблемы. Существенное повышение производительности микропроцессоров в 90-е годы обусловило в криптографии усиление интереса к программным методам реализации шифроалгоритмов — как к возможной альтернативе аппаратным

схемам на регистрах сдвига. Одним из самых первых программных криптоалгоритмов, получивших широкое распространение, стал алгоритм RC4.

Алгоритм RC4 — это поточный шифр с переменной длиной ключа, разработанный в 1987 году Рональдом Райвистом для компании RSA Data Security. Как и его «компаньон», блочный шифр RC2,

RC4 представляет собой шифр с переменной длиной ключа, пригодный для быстрого магистрального шифрования. Он очень компактен в терминах размера кода и особенно удобен для процессоров с побайтно-ориентированной обработкой. RC4 может шифровать со скоростью около 10 Мбайт/с на процессоре с тактовой частотой 330 МГц и, подобно RC2, имеет особый статус, значительно упрощающий получение разрешения на экспорт (схема позволяет безболезненно редуцировать длину ключа). Шифр RC4 применяется в некоторых широко распространённых стандартах и протоколах шифрования таких, как WEP, WPA и TLS, также алгоритм RC4 реализован в десятках коммерческих криптопродуктов, включая Lotus Notes, Apple Computer's AOCE, Oracle Secure.

Главными факторами, способствовавшими широкому применению RC4, были простота его аппаратной и программной реализации, а также высокая скорость работы. Хотя прогресс в развитии вычислительной техники в настоящее время существенно увеличил возможности применения более ресурсоемких методик шифрования, одновременно с этим значительно выросли и объемы данных, что до известной степени нивелирует указанное преимущество. Помимо этого, возник целый класс мобильных и встраиваемых устройств, для которых ключевой характеристикой является низкое энергопотребление, а следовательно, к ним предъявляются повышенные требования экономности алгоритмов в плане вычислений. Среди таких устройств можно выделить смарт-карты, в которых может быть необходима функция шифрования данных, и мобильные устройства, подключающиеся к беспроводным сетям. Оба этих класса устройств переживают в настоящее время расцвет, что привлекает внимание к таким алгоритмам, как RC4.

В США длина ключа для использования внутри страны рекомендуется равной 128 битам, но соглашение, заключённое между Software Publishers Association (SPA) и правительством США даёт RC4 специальный статус, который означает, что разрешено экспортировать шифры длиной ключа до 40 бит. 56-битные ключи разрешено использовать заграничным отделением американских компаний [1 – 4].

Целью статьи является исследование зависимостей расположения единичного элемента в S-блоке и значениями индексных элементов i, j . Использование этих зависимостей дает возможность формировать псевдослучайные последовательности малого периода, которые могут использоваться для эффективного криптографического взлома.

Результаты исследований

Методика исследования периодических свойств алгоритма поточного шифрования RC4 над его мини-версией предложена в статьях [5, 6], она состоит

в построении уменьшенной версии алгоритма RC4, которая получается, посредством масштабирования с сохранением всех базовых операций алгоритма. Исследование периодических свойств мини-версий алгоритма поточного шифрования RC4 показала, что существует зависимость расположения в S-блоке (S_0, S_1, \dots, S_n) единичного значения и начальными значениями i, j которое приводит к формированию псевдослучайных последовательностей малого периода.

Для проведения исследований протестирована работа генератора псевдослучайных чисел RC4 для поля $GF(2^4)$ на полном множестве ненулевых ключевых данных. Вычислялись значения i, j , при которых длина периода была минимальной.

В ходе проведенных исследований было установлено, что при любом значении S-блока существует значение i, j , при которых длина периода составляет 240 элементов псевдослучайной последовательности (для поля $GF(2^4)$). В табл. 1 частично представлены результаты проведенного эксперимента.

Как следует из приведенных в табл. 1 данных, существует зависимость расположения единичного элемента $(S_i = 1)$ в S-блоке и значениями i, j при которых формируется псевдослучайная последовательность с гарантировано малым периодом.

Выдвинем предположение, что гарантированно малый период появляется когда значение j совпадает с номером расположения единичного элемента в S-блоке, а $i = j - 1$ (только для случая когда единичный элемент расположен в диапазоне $S_1 \div S_{15}$). Для случая когда $S_0 = 1$ значение i равно номеру последнего элемента S-блока, а $j = 0$.

Для проверки выдвинутого предположения протестирована работа алгоритма поточного шифрования RC4 для полей $GF(2^5)$ и $GF(2^6)$, т.е. когда S-блоки находятся в диапазоне от $S_0 \div S_{31}$ и $S_0 \div S_{63}$ соответственно. В ходе проведенных исследований длина периода при предложенных значениях i, j составила 992 и 4032 элемента последовательности, что подтвердило выдвинутое предположение.

В дальнейшем, были оценены все длины гарантировано малых периодов, формируемой последовательности для полей $GF(2^n)$ где $n = 3 \div 10$, результаты исследований представлены в табл. 2.

Как видно из приведенных в табл. 2 данных, для каждой размерности поля $GF(2^n)$ существует только своя длина гарантированного малого периода.

Так для поля $GF(2^6)$ длина периода составляет 4032 элемента последовательности, а для поля $GF(2^{10})$ 1047552 элемента, что на порядок меньше чем максимальный период.

Значение S-блока и индексных элементов i, j , приводящие к формированию псевдослучайной последовательности малого периода для поля $GF(2^4)$

Значение S-блока																i	j	Длина периода ПСП
S ₀	S ₁	S ₂	S ₃	S ₄	S ₅	S ₆	S ₇	S ₈	S ₉	S ₁₀	S ₁₁	S ₁₂	S ₁₃	S ₁₄	S ₁₅			
3	6	5	2	4	7	10	1	11	12	15	14	8	9	0	13	6	7	240
4	9	5	2	3	12	10	8	11	7	15	13	1	6	0	14	11	12	240
15	13	11	9	7	5	3	0	1	2	4	6	8	10	12	14	7	8	240
8	13	12	14	7	1	3	6	2	5	4	0	15	10	11	9	4	5	240
1	2	4	6	7	3	5	8	10	11	12	13	0	14	9	15	15	0	240
1	15	3	5	7	4	2	0	6	14	13	12	11	10	9	8	15	0	240
8	10	9	5	7	15	6	0	2	14	13	11	12	3	4	1	14	15	240

Таблиця 2

Длины гарантировано малых периодов алгоритма RC4 для полей $GF(2^3) - GF(2^{10})$

№ п/п	Размерность поля	Максимальная длина периода	Длина гарантировано малого периода
1.	$GF(2^3)$	$< 8^2 \cdot 8!$	56
2.	$GF(2^4)$	$< 16^2 \cdot 16!$	240
3.	$GF(2^5)$	$< 32^2 \cdot 32!$	992
4.	$GF(2^6)$	$< 64^2 \cdot 64!$	4032
5.	$GF(2^7)$	$< 128^2 \cdot 128!$	16256
6.	$GF(2^8)$	$< 256^2 \cdot 256!$	65280
7.	$GF(2^9)$	$< 512^2 \cdot 512!$	261632
8.	$GF(2^{10})$	$< 1024^2 \cdot 1024!$	1047552

Выводы

Проведенные исследования показали, что существует гарантированная зависимость между значениями i, j и расположением единичного элемента в S-блоке, использование которых, приводит к формированию псевдослучайной последовательности с малым периодом. Эти исследования могут использоваться для проведения эффективного криптоанализа.

Поступила в редколлегию 21.09.2012

Рецензент: д-р техн. наук, проф. В.А. Краснобаев, Полтавский национальный технический университет имени Кондратюка, Полтава.

АНАЛІЗ АЛГОРИТМУ ПОТОКОВОГО ШИФРУВАННЯ RC4

Р.В. Королев

В роботі проведені дослідження залежності розташування одиничного елементу в S-блоці із значеннями індексних елементів i, j , використання яких приводить до формування псевдовипадкових послідовностей малого періоду.

Ключові слова: генератор псевдовипадкових чисел, RC4.

ANALYSIS OF DATA-FLOW ENCRYPTERMENT ALGORITHM RC4

R.V. Korolev

Researches of dependence of location of single element are in-process conducted in S-bloke with the values of index elements i, j the use of which results in forming of pseudocausal sequences of small period.

Keywords: generator of pseudocausal numbers, RC4.