УДК 681.3.06

Р.В. Королев

Харьковский университет Воздушных Сил им. И. Кожедуба, Харьков

ИССЛЕДОВАНИЕ ПЕРИОДИЧЕСКИХ СВОЙСТВ АЛГОРИТМА ПОТОЧНОГО ШИФРОВАНИЯ RC4

В работе проведены исследования периодичных свойств последовательностей псевдослучайных чисел, формируемых генератором RC4. Проведенные исследования показали, что рассмотренный генератор обладает "слабыми" ключами, использование которых приводит к формированию последовательностей псевдослучайных чисел с малым периодом, что, в свою очередь, может привести к успешным криптографическим атакам.

Ключевые слова: *шифрование, период, криптографическая атака, генератор псевдослучайных чисел.*

Введение

Постановка проблемы в общем виде и анализ литературы Алгоритм поточного шифрования RC4 разработан в 1987 г. Рональдом Линном Ривестом, известным американским специалистом в области криптографии для компании RSA Data Security [1 – 3]. В течении семи лет этот алгоритм был фирменным секретом и детали о его конструкции предоставлялось только после подписания договора о не разглашении, но в 1994 г. был анонимно опубликован [2]. Начиная с этого времени, он нашел широкое применение в целом ряде криптографических приложений, включая такие, как SSL и TLS – для шифрования данных, передаваемых по сетям ЭВМ, не предусматривающим защиты пользовательских данных, WPA и WEP-для защиты беспроводных соединений [4]. Таким широким распространением алгоритм обязан ряду свойств, не утратившим актуальности за двадцать лет с его существования. Одно из них – высокое быстродействие. В настоящее время прогресс в развитии вычислительной техники существенно увеличил возможности применения более ресурсоемких методов шифрования, одновременно с этим значительно выросли и объемы обрабатываемых данных, что до известной степени нивелирует указанное преимущество. Помимо этого появилось множество мобильных устройств для которых главной характеристикой является низкое энергопотребление, а следовательно к ним предъявляются требования экономности используемых алгоритмов в плане вычислений (малое количество операций). К ним можно отнести смарт-карты, в которых может быть необходима функция шифрования, мобильные устройства и т.д.

В статье [4] были исследованы ключевые пространства и соответствующие им длины периодов формируемых псевдослучайных последовательностей, частично выявлены “слабые” ключи, которые могут привести к эффективным криптографическим атакам. На наш взгляд данные исследования носят ограниченный характер и являются не полными. В своей работе мы ставим задачу исследования периодических свойств и выявление всех “слабых” ключей мини-версии генератора RC4, обобщении полученных результатов для полной версии алгоритма.

Основной раздел

1. Структура и особенности реализации генератора ПСЧ RC4

Описание алгоритма поточного шифрования RC4 наиболее полно представлено в [1 – 3]. Алгоритм функционирует независимо от открытого текста, формируемая им последовательность накладывается на открытый текст, тем самым можно утверждать, что в сущности, алгоритм RC4 является генератором псевдослучайных чисел (ГПСЧ). RC4 содержит подстановочную таблицу (S -бокс): $S_0, S_1, ... S_{255}$ где $S_k \in GF(2^n)$ $n = 8$, $k \in 0 \div 255$ и представляет собой перестановку от 0 до 255. Внутреннее состояние алгоритма, оперирующего элементами из n бит, определяется двумя индексными элементами i и j такой же длины (при начальной инициализации $i, j = 0$).

Для генерации псевдослучайного бита последовательности выполняются следующие операции:

$$i = (i + 1) \bmod 256;$$

$$j = (j + S_i) \bmod 256;$$

$$S_i \leftrightarrow S_j;$$

$$t = (S_i + S_j) \bmod 256;$$

$$gamma = S_t.$$

Значение gamma складывается операцией $\oplus$ (сложение по $\bmod 2$) с открытым текстом для формирования шифротекста, либо операции $\oplus$ с шифротекстом для получения открытого текста. Шифрование происходит весьма быстро – примерно в 10 раз быстрее шифра DES [1]. RC4 формирует псевдослучайные последовательности с длинной периода

$< 2^{1700} = (256! \times 256^2)$ (возможные состояния шифра). S -бокс медленно изменяется в процессе работы: параметр i обеспечивает изменение каждого элемента, а j отвечает за то, чтобы эти элементы изменялись псевдослучайным образом.

2. Методика исследований и основные полученные результаты

Методика исследования периодических свойств генератора псевдослучайных чисел RC4 над его мини-версией предложена в статье [4], она состоит в построении уменьшенной версии алгоритма RC4 которая, получается, посредством масштабирования с сохранением всех базовых операций алгоритма. Мини версия подвергается тестированию и эмпирической оценки длин периодов на различных входных ключевых данных.

Для проведения исследований периодических свойств ГПСЧ RC4 разработаны программные реализации мини-версий над $GF(2^2), GF(2^3)$, т.е используются S -боксы $S_0^1, S_1^1, ...S_3^1$ и $S_0^2, S_1^2, ...S_7^2$ соответственно.

Ожидаемые длины периодов должны были составлять $L^1 < 4!*4^2 = 384$ и $L^2 < 8!*8^2 = 2580480$ возможных состояний.

Для проведения исследований протестирована работа ГПСЧ RC4 на полном множестве ненулевых ключевых данных и при начальной инициализации $i, j = 0$ (всего 4! ключей для поля $GF(2^2)$ и 8! ключей для поля $GF(2^3)$). В каждом тесте оценивалась длина периода L .

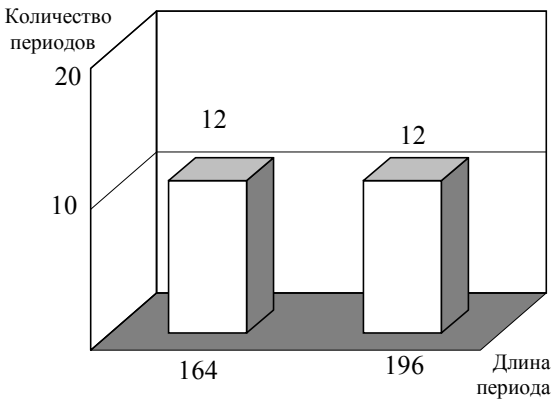

Рис. 1. Распределения числа периодов мини-версии RC4 для $GF(2^2)$

В результате проведения эксперимента подсчитаны распределения числа периодов и их количество, которые представлены на рис. 1, 2.

Как следует из приведенных на рис. 1, 2 данных, генератор RC4 формирует последовательности с длинной периода ниже максимального. Особый интерес представляют результаты исследования периодических свойств мини-версии RC4 для версии поля $GF(2^3)$. Существуют “аномально” плохие начальные состояния S -бокса, которые порождают псевдослучайные последовательности с длинной периода на несколько порядков ниже максимально допустимого.

Например, начальные перестановки $S_0 = 3, S_1 = 5, S_2 = 6, S_3 = 2, S_4 = 7, S_5 = 0, S_6 = 4, S_7 = 1$ и $S_0 = 5, S_1 = 4, S_2 = 1, S_3 = 7, S_4 = 6, S_5 = 2, S_6 = 0, S_7 = 3$ формируют псевдослучайные последовательности с длинной периода 24 элемента, а перестановки $S_0 = 5, S_1 = 3, S_2 = 6, S_3 = 4, S_4 = 0, S_5 = 7, S_6 = 1, S_7 = 2$, $S_0 = 5, S_1 = 3, S_2 = 6, S_3 = 4, S_4 = 1, S_5 = 7, S_6 = 0, S_7 = 2$, $S_0 = 6, S_1 = 4, S_2 = 3, S_3 = 2, S_4 = 7, S_5 = 0, S_6 = 5, S_7 = 1$ и $S_0 = 6, S_1 = 4, S_2 = 3, S_3 = 2, S_4 = 7, S_5 = 1, S_6 = 5, S_7 = 0$ формируют псевдослучайные последовательности с длинной периода 120 элемента.

Кроме того, в ходе проведенных экспериментов выявлены частные результаты, полученные ранее другими авторами в работе [4], что согласует и дополняет известные положения. Таким образом можно утверждать что существуют значения секретного ключа (значения S -бокса) при которых формируемые псевдослучайные последовательности имеют период на несколько порядков меньше максимального, что в свою очередь может привести к появлению эффективных криптографических атак.

В ходе проведенных исследований были оценены все длины периодов формируемой последовательности для полей $GF(2^3), GF(2^2)$ при всех возможных состояниях i и j для всех значений S -боксов, результаты исследований приведены на рис. 3, 4.

Таким образом, в ходе проведенных исследований выявлено что для каждого S -бокса существует значения i и j , при которых длина периода строго определена.

Так для S -боксов из поля $GF(2^2)$ (их количество равно $4! = 24$) длина периода составляет 12 элементов последовательности, а для S -боксов из поля $GF(2^3)$ (их количество равно $8! = 40320$) длина периода составляет 56 элементов последовательности.

Выводы

Проведенные исследования показали, что генератор ППСЧ RC4 обладает плохими периодическими свойствами (период формирования ППСЧ на несколько порядков ниже максимального) обладает “слабыми” ключами, которым соответствуют “плохим” начальным перестановкам (значениям S -боксов). Их использование приводит к формированию псевдослучайных последовательностей с малой длиной периода.

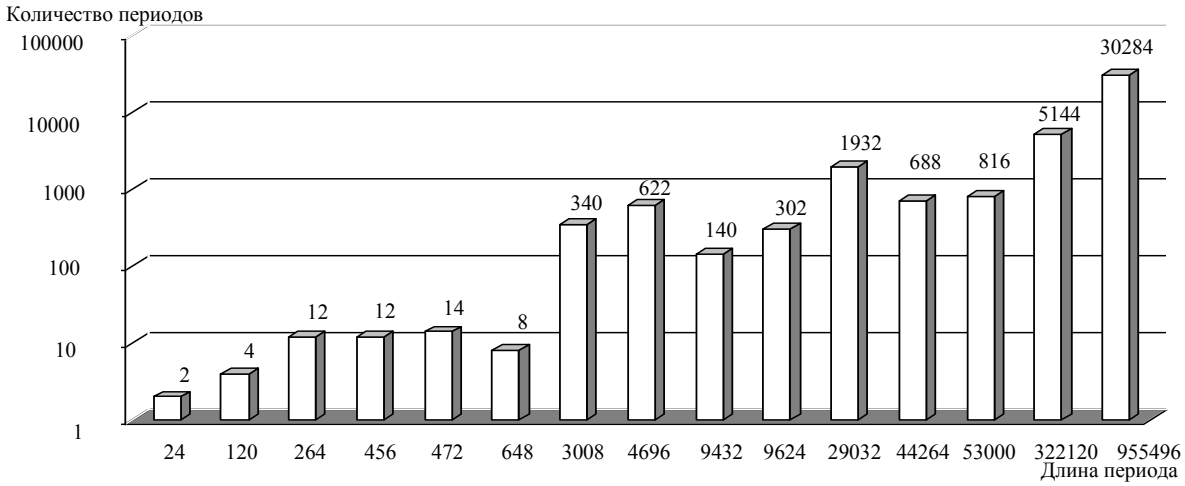

Рис. 2. Распределения числа периодов мини-версии RC4 для поля $GF(2^3)$

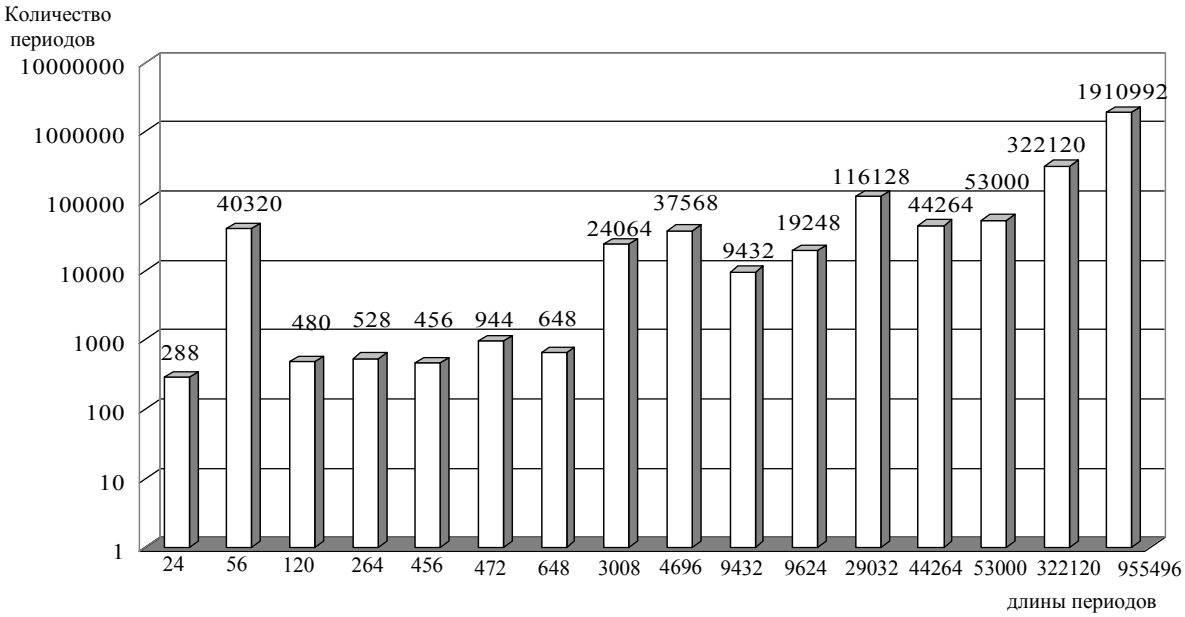

Рис. 3. Распределения числа периодов для поля $GF(2^3)$ при полном переборе значений i и j

Рис. 4. Распределения числа периодов для поля $GF(2^2)$ при полном переборе значений i и j

Список литературы

1. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си / Б. Шнайер. – М.: Издательство ТРИУМФ, 2002 – 816 с.

2. Поточные шифры Результаты зарубежной открытой криптологии. [Электронный ресурс]. – Режим доступа к источнику: www.ssl.stu.neva.ru/psw/crypto/potok/str_ciph.htm. – М., 1997.

3. Рябко Б.Я. Криптографические методы защиты информации /Б.Я.Рябко, А.Н.Фионов. – М.: Гарячая линия-Телеком, 2005.– 229 с.

4. Анализ обобщения алгоритма RC4 [Электронный ресурс]. – Режим доступа к источнику: www.vniipvti.ru/data/file/sbor3_11.pdf. – М., 2009.

Поступила в редколлегию 16.11.2009

Рецензент: д-р техн. наук, проф. А.А. Кузнецов, Харьковский университет Воздушных Сил им. И. Кожедуба, Харьков.

ДОСЛІДЖЕННЯ ПЕРІОДИЧНИХ ВЛАСТИВОСТЕЙ АЛГОРИТМУ ПОТОКОВОГО ШИФРУВАННЯ RC4

Р.В. Корольов

У роботі проведені дослідження періодичних властивостей послідовностей псевдовипадкових чисел, що формуються генератором RC4. Проведені дослідження показали, що розглянутий генератор володіє "слабкими" ключами, використання яких приводить до формування послідовностей псевдовипадкових чисел з малим періодом, що, у свою чергу, може привести до успішних криптографічних атак.

Ключові слова: *шифрування, період, криптографічна атака, генератор псевдовипадкових чисел.*

PERIODIC PROPERTIES RESEARCH OF ALGORITHM RC4 STREAMING ENCIPHERING

R.V. Korolev

Researches of periodic properties of sequences of pseudocasual numbers which are formed the generator of RC4 are in-process conducted. The conducted researches rotined that the considered generator owned the "weak" keys the use of which leads to forming of sequences of pseudocasual numbers with a small period, that, in same queue, can result in successful cryptographic attacks.

Keywords: *encipherement, period, cryptographic attack, generator of pseudocasual numbers.*