УДК 621.391.7

# Реализация новой статистической атаки на блочный шифр

В. А. Монарев[1]

В работе описана модификация атаки на блочный шифр RC6, предложенной В.А. Монаревым и А.М. Лубкиным в 2010 году. Новый метод позволяет найти ключ для 5-раундового шифра на персональном компьютере за приемлемое время. В частности, вычислительная сложность для 5-го и 6-го раунда составляет $2^{40}$ и $2^{50}$ соответственно.

*Ключевые слова*: криптография, криптоанализ, блочный шифр, криптоаналитическая атака

## 1. Введение

Шифр RC6 был разработан группой исследователей как один из претендентов на звание AES. В данной работе приводится описание модификация атаки, описанной в [1], которая позволяет существенно сократить количество операций при поиске ключа, что делает возможным проведение атаки на 5-раундовую версию шифра RC6 на персональном компьютере. Предложенная атака относится к статистическим атакам и была впервые предложена в [2]. Самые лучшие варианты этой атаки на шифр RC6 описаны в [3], [4] и [1].

Результаты, приведённые в работе, можно считать лучшими на сегодняшний день для шифра RC6 с уменьшенным числом раундов. Поскольку ранее существовавшие алгоритмы поиска ключа имели большую сложность, то ни в одной опубликованной ранее работе не приводятся результаты реализации такого вида атак на шифр RC6. В данной работе приводятся результаты реализации атаки на 5-ый раунд и оценка эффективности этой атаки для 5- и 6-раундовых версий шифра.

## 2. Краткое описание шифра RC6

В экспериментальной части рассматривался 128-битный вариант шифра RC6, когда на вход шифра подаются 4 блока по 32 бита. Перед описанием схемы шифрования введём необходимые обозначения.

$\mathrm{lbs}_n(X)$ : младшие $n$ бит в числе $X$;

$\oplus$ : операция XOR

$a <<< b$ : циклический сдвиг $a$ на $b$ бит влево;

$a >>> b$ : циклический сдвиг $a$ на $b$ бит вправо;

[1] Работа выполнена при финансовой поддержке РФФИ (грант N 14-01-31484-мол_а).

$S_i$ : $i$-ый подключ;

$r$ : число раундов шифрования;

$(A_i, B_i, C_i, D_i)$ : вход $i$-го раунда четыре 32-битных блока (128 бит);

$f(x)$ : $x(2x+1)$;

$F(x)$ : $f(x) <<< 5$;

$x \| y$ : конкатенация $x$ и $y$.

На начальном этапе секретный 128 (192, 256)-битный ключ преобразуется в массив размера $(2r+4)$ 32-битных подключей $S_0, S_1, \ldots$ С помощью этого массива происходит шифрование данных по следующему алгоритму.

Алгоритм 1 (шифрования)

1. $A_1 = A_0; B_1 = B_0 + S_0; C_1 = C_0; D_1 = D_0 + S_1$

2. *for* $i = 1$ *to* $r$ *do*

$t = F(B_i); u = F(D_i); A_{i+1} = B_i;$

$B_{i+1} = ((C_i \oplus u)) <<< (t \bmod 32)) + S_{2i+1};$

$C_{i+1} = D_i;\ D_{i+1} = ((A_i \oplus t)) <<< (u \bmod 32)) + S_{2i};$

3. $A_{r+2} = A_{r+1} + S_{2r+2}; B_{r+2} = B_{r+1}; C_{r+2} = C_{r+1} + S_{2r+3}; D_{r+2} = D_{r+1}.$

## 3. Алгоритм поиска секретного ключа шифра RC6

Напомним основную идею поиска секретного ключа по алгоритму, предложенному в [1]. Для того чтобы расшифровать информацию, необходимо найти все секретные подключи $S_0, S_1, \ldots$ Их поиск осуществляется по отдельности, начиная с $S_0$. Для выбора правильного подключа используется статистический тест хи-квадрат (более подробно в [1]).

Алгоритм 2 (вычисление статистики)

1. На вход шифра подаётся последовательность 128-битных блоков данных (четыре 32-битных блока).

$$(0,0,0,0),(1,0,0,0),\ldots(2^{32}-1,0,0,0),(0,0,1,0),(1,0,1,0),\ldots \qquad (1)$$

2. Каждый блок из (2) шифруется по алгоритму 1 на r раундов. После шифрования вычисляется статистика $x^2$ (хи-квадрат) для $lbs_5(A_{r+2}) \| lbs_5(C_{r+2})$ (1023 степени свободы), то есть объединяются два 5-битных блока и рассматривается выборка из 10-битных чисел.

Для того чтобы найти секретный ключ $S_0$, необходимо применить Алгоритм 3.

Алгоритм 3 (атака со сложностью перебора $2^{32}$)

1. Для каждого $S'_0 \in \{0,1,2,\ldots,2^{32}-1\}$ вычисляем последовательность 128-битных блоков $(A'_0, B'_0, C'_0, D'_0)_n$, $n = 0,1,\ldots$ по формулам:
$D'_0 = c_n; B'_0 = a_n - S'_0; A'_0 = b_n \oplus t; C'_0 = d_n$, где $t = F(a_n)$, которую подаём на вход шифру, где $(a_n, b_n, c_n, d_n)$ последовательность вида (1).

2. Для каждой последовательности вычисляем статистику $x^2$, используя $lbs_5(A_{r+2}) \| lbs_5(C_{r+2})$. По аналогии с Алгоритмом 2 ( подробнее в [1]).

3. Находим значение $S'_0$, для которого значение $x^2$ максимально. Полагаем его равным искомому $S_0$.

## 4. Усовершенствованный алгоритм

Предлагаются два усовершенствования для того, что бы ускорить Алгоритм 3. Во-первых, изменить вид последовательности (1) таким образом, чтобы уменьшить длину последовательности, необходимую для подсчёта статистики $x^2$ и корректного поиска секретного ключа. Во-вторых, предлагается изменить схему подбора секретного подключа. Если в Алгоритме 3 предполагается перебор всех возможных значении подключа $S_0$, то есть перебор $2^{32}$ значений, то в новом алгоритме предлагается производить поиск ключа по частям. Например, сначала найти первые $L$ бит ключа, далее найти оставшиеся $32-L$, где $L$ – целочисленный параметр.

Для того чтобы уменьшить длину последовательности выбранного шифротекста, нужно отметить, что во втором раунде шифра (см. Алгоритм 1 и Алгоритм 3) циклический сдвиг зависит только от первого и третьего блока данных ($A_0$ и $C_0$) при условии, что подключ подобран правильно. Таким образом, предлагается подобрать последовательность выбранного шифротекста $(a_n, b_n, c_n, d_n)$, чтобы циклический сдвиг на втором раунде был равен нулю. Далее будет показано, что это существенно уменьшает длину последовательности, необходимую для правильного поиска ключа. Ниже приведён вид последовательности, который использовался в экспериментах

$$(0,0,0,0),(a_1,0,0,0),(a_2,0,0,0)\ldots, \qquad (1)'$$

где $a_i$ упорядочены по возрастанию и $F(a_i)\ mod\ 32 = 0$ для всех $i$.

Чтобы найти необходимое количество элементов искомой последовательности, нужно перебрать достаточное количество элементов последовательности (1), выбирая из них только те элементы, которые удовлетворяют заданному условию. Полагаем, что этот перебор нужно проводить только один раз для первого подключа, поскольку далее эта последовательность хранится в памяти.

Таблица 1. Оценки эффективности нового подхода

| $R$ | Размер выборки | Новый метод | | | Старый метод | | |
|---|---|---|---|---|---|---|---|
| | | $x^2 > Q_{0.99}$ | $x^2 > Q_{0.999}$ | $x^2 > Q_x$ | $x^2 > Q_{0.99}$ | $x^2 > Q_{0.999}$ | $x^2 > Q_x$ |
| 5 | $2^{16}$ | 49 | 28 | 12 | 10 | 1 | 0 |
| 5 | $2^{18}$ | 151 | 102 | 62 | 10 | 2 | 0 |
| 5 | $2^{20}$ | 276 | 231 | 181 | 20 | 3 | 0 |
| 5 | $2^{22}$ | 406 | 363 | 315 | 74 | 27 | 5 |
| 5 | $2^{24}$ | 502 | 459 | 423 | 253 | 163 | 78 |

В табл. 1 приведены результаты оценки эффективности нового подхода. В строке таблицы приведены числа превышений квантилей распределения хи-квадрат для 1000 случайных ключей в 6-раундовом шифре RC6 при правильно подобранном подключе $S_0$ (см. Алгоритм 3). Для подбора ключа на практике необходимо, чтобы при подсчёте статистики $x^2$ шифротекста получались значения, значительно превышающие $Q_{0.999}$. В ходе поиска секретного ключа выбирается множество подключей, для которых статистика $x^2$ максимальна. В [1] предложено выбрать $2^{16}$ ключей. Очевидно, что даже в случае, если последовательность шифротекста была бы «идеальной» псевдослучайной последовательностью, то из $2^{32}$ последовательностей для более $2^{22}$ последовательностей статистика $x^2$ превысила бы

$Q_{0.999}$. Поэтому самым важным столбцом в табл. 1 является столбец $Q_x$ ($Q_x$ = 1239, $x = 1 - 2^{-12}$). Из результатов следует, что для 6% подключей можно применить атаку при длине выбранного текста $2^{18}$, благодаря более эффективному выбору текста. Для предыдущего варианта атаки длина текста должна быть равна $2^{24}$.

Таблица 2. Исследование эффективности подбора подключа для 6-го раунда

| *S* текст / *L* бит | $2^{18}$ | $2^{19}$ | $2^{20}$ | $2^{21}$ | $2^{22}$ | $2^{23}$ |
|---|---|---|---|---|---|---|
| 32 | 62 | 116 | 201 | 254 | 306 | 371 |
| 31 | 61 | 108 | 185 | 241 | 318 | 346 |
| 30 | 55 | 100 | 187 | 228 | 309 | 348 |
| 29 | 42 | 77 | 134 | 222 | 322 | 381 |
| 28 | 15 | 40 | 72 | 165 | 267 | 413 |
| 27 | 9 | 15 | 49 | 99 | 148 | 249 |
| 26 | 5 | 12 | 23 | 37 | 91 | 130 |
| 25 | 3 | 7 | 6 | 21 | 31 | 69 |

В табл. 2 приведены результаты экспериментального исследования эффективности подбора 32-битного подключа по частям для 6-раундовой версии шифра. Предлагается сначала подобрать L младших бит ключа, а после этого – остальные 32 – *L* бит, и производить поиск ключа полным перебором всех возможных $2^{32}$ значений. Таким образом, сложность перебора уменьшиться в $2^{32}/2^{L}$ раз, если размер необходимого текста не изменится. В таблице приведены значения превышения квантили $Q_x$, где $x = 1 - 2^{-12}$ при переборе *L* бит ключа (для 1000 случайных ключей). Отметим, что вычислительную сложность можно найти по формуле

$$S \cdot 2^{L},$$

где *S* – количество текста. Легко заметить, что значения по диагоналям соответствуют атакам на шифр с одинаковой сложностью. Например, если подбирается 32 бита подключа и используется $2^{18}$ текста (сложность $2^{49}$), то эффективность атаки можно повысить, если подбирать 27 бит ключа при длине текста $2^{21}$ (сложность $2^{48}$).

В табл. 3 приведены результаты для 5-раундовой версии. Из таблицы следует, что если вместо подбора 32-бит подключа при $2^{12}$ текста использовать перебор 27 бит ключа и $2^{13}$ текста, то сложность уменьшится в 16 раз, а эффективность возрастёт. Таким образом, данный подход даёт существенное повышение эффективности атаки при уменьшении сложности.

Таблица 3. Исследование эффективности подбора подключа для 5-го раунда

| Текст / *L* бит | $2^{12}$ | $2^{13}$ | $2^{14}$ | $2^{15}$ | $2^{16}$ |
|---|---|---|---|---|---|
| 32 | 797 | 967 | 996 | 1000 | 1000 |
| 31 | 807 | 978 | 997 | 1000 | 1000 |
| 30 | 819 | 973 | 998 | 1000 | 1000 |
| 29 | 746 | 942 | 994 | 1000 | 1000 |
| 28 | 665 | 889 | 976 | 1000 | 1000 |
| 27 | 470 | 807 | 927 | 979 | 1000 |
| 26 | 250 | 412 | 480 | 621 | 900 |
| 25 | 139 | 206 | 242 | 315 | 482 |

## 4. Реализация атаки

Обобщая результаты, приведённые в табл. 2 и 3, можно сделать вывод, что наиболее эффективно подбирать 27 младших бит ключа, а уже после того, как для каждого из двух подключей будут найдены 27 младших бит, производить поиск оставшихся 5-ти бит. В результате экспериментальной работы было выяснено, что для эффективного нахождения последних 5 бит подключа необходимо изменить вид входной последовательности текста. Было предложено использовать последовательность вида:

$$(0,0,0,0),(1,0,1,0),\ldots(2^{32}-1,0,2^{32}-1,0),(0,1,0,1),(1,1,1,1),\ldots \qquad (2)$$

В табл. 4 приведены результаты экспериментов для 5-раундовой версии шифра. Производился подбор последних пяти бит у каждого из двух подключей одного раунда (итого 10 бит), при фиксированных (правильно подобранных) 27 битах в каждом из подключей. В первом столбце указано количество использованного текста. Во втором столбце – количество рассмотренных случайных ключей. В третьем столбце – количество ключей, при использовании которых статистика шифротекста $x^2$ превысила $Q_x$ ($Q_x$ = 1239, $x = 1 - 2^{-12}$); такие ключи назовём «подходящими», поскольку для них можно применить статистическую атаку. В четвёртом указан вид последовательности (или последовательность вида (1)' или (2)). В пятом – количество пар подключей, которые были найдены с ошибкой. То есть для некоторых неправильных подключей статистика $x^2$ превысила статистику для правильного подключа. Из табличных значений следует, что даже сильное увеличение количества текста не улучшает эффективность подбора последних бит подключей, если выбрана последовательность текста вида (1)'. Изменение же вида последовательности даёт существенное улучшение. Почти все пары ключей будут найдены правильно. Отметим, что сложность нахождения последних 5 бит у каждого из подключа составит $2^{33}$, что заметно меньше, чем сложность нахождения первых 27 бит у каждого из подключей.

Таблица 4. Результаты оценки эффективности атаки на 5-ый раунд

| Текст | Всего ключей | Подходящих ключей | Тип текста | Ошибок |
|---|---|---|---|---|
| $2^{13}$ | 1026 | 1000 | (1)' | 994 |
| $2^{16}$ | 100 | 100 | (1)' | 99 |
| $2^{23}$ | 100 | 100 | (1)' | 100 |
| $2^{16}$ | 491 | 100 | (2) | 0 |
| $2^{23}$ | 191 | 100 | (2) | 9 |

Далее приведём результаты реализации атаки на 5-ый раунд для 10 случайных ключей. В табл. 5 приведены результаты атаки, проведённой по следующему алгоритму:

1. Подбираем множество возможных значений 27 первых бит подключа $S_0$. Размер выборки $2^{13}$ текста.
2. Подбираем множество возможных значений 27 первых бит подключа $S_1$.
3. Из двух множеств подбираем правильную пару 27 битных частей $S_0$ и $S_1$.
4. Подбираем оставшиеся 10 бит подключей $S_0$ и $S_1$ (по 5 бит каждого подключа). Размер выборки $2^{26}$.

В ячейке стоит плюс, если искомая часть ключа была найдены верно. Минусы в столбцах 2 и 3 соответствуют, так называемым, «сильным ключам». Для этого множества ключей выборки $2^{13}$ недостаточно, чтобы найти правильный ключ. Из результатов следует, что 4 из 10

ключей были найдены правильно, что говорит об эффективности нового подхода.

Таблица 5. Оценка эффективности поиска ключа для 5-го раунда

| Номер ключа | 27 бит $S_0$ | 27 бит $S_1$ | 10 бит | Пара подключей $S_0$ и $S_1$ |
|---|---|---|---|---|
| 1 | + | + | + | + |
| 2 | - | - | - | - |
| 3 | + | + | + | + |
| 4 | + | + | + | + |
| 5 | - | - | - | - |
| 6 | - | + | - | - |
| 7 | - | - | - | - |
| 8 | + | - | - | - |
| 9 | + | - | - | - |
| 10 | + | + | + | + |

## Литература


1. *Монарев В.А., Лубкин А.М.* Эффективная атака на блоковый шифр RC6 // Вестник СибГУТИ. № 4, 2010, с.55- 60.
2. *Knudsen L., Meier W.* Correlations in RC6 whith a reduce number of rounds // FSE 2000, LNCS 1978 (2000), Springer Verlag, P. 94–108.
3. *Miyaji A., Nonaka M.* Evaluation of the security of RC6 against the $\chi^2$ – attack // IEICE Trans. Fundamentals, vol. E88–A, No.1, 2005.
4. *Isogai N., Matsunaka T., Miyaji A.* Optimized $\chi^2$ –attack against RC6 // ACNS 2003, LNCS 2846 (2003), Springer Verlag, P. 199–211.
5. *Рябко Б.Я., Монарев В.А., Шокин Ю.И.* Новый тип атак на блоковые шифры // Проблемы передачи информации, т. 41, н. 4, 2005, с.181– 128.
6. *Miyaji A. and Nonaka M.* Cryptanalysis of the Reduced–Round RC6 // Proc. ICICS 2002, LNCS 2513, P. 480–494.


*Статья поступила в редакцию 20.12.2013*

**Монарев Виктор Александрович**
к.ф.-м.н., научный сотрудник ИВТ СО РАН, (630090, Новосибирск, пр. Академика Лаврентьева, 6) тел. (383) 330-61-50, e-mail: viktor.monarev@gmail.com

**Implementation of a new statistical attack on block encryption**

**V.A. Monarev**

In this paper, modification of attack on block encryption RC6 suggested by V.A. Monarev and A.M. Lubkin in 2010 is described. This new method enables to find a key for a five round encryption on PC in acceptable time. In particular, computational complexity for 5 and 6 round is $2^{40}$ and $2^{50}$ respectively.

*Keywords*: cryptography, cryptoanalysis, block encryption, cryptoanalytic attack.