УДК 681.3.06

Р.В. Корольов, Д.А. Волков

*Харківський університет Повітряних Сил ім. І. Кожедуба, Харків*

# ОЦІНКА ПЕРІОДИЧНОСТІ АЛГОРИТМУ ПОТОКОВОГО ШИФРУВАННЯ ПРИ НЕНУЛЬОВИХ ЗНАЧЕННЯХ ІНДЕКСНИХ ЕЛЕМЕНТІВ

*В роботі проведені дослідження алгоритму поточного шифрування RC4 при ненульових значеннях індексних елементів. Визначаються довжини періодів псевдовипадкових чисел з обмеженим періодом. Доведено що існує залежність розташування одиничного елемента у S-блоці зі значеннями індексних елементів, при яких формується послідовність з обмеженим періодом.*

***Ключові слова:*** *генератор псевдовипадкових чисел, алгоритм поточного шифрування, RC4.*

## Вступ

**Постановка проблеми.** RC4 (англ. Rivest Cipher 4 або англ. Ron's Code, також відомий як ARCFOUR або ARC4 (англ. Alleged RC4 )) - це алгоритм потокового шифрування, який широко застосовується в різних системах захисту інформації в комп'ютерних мережах ( наприклад, в протоколах SSL і TLS, алгоритмі безпеки бездротових мереж WEP, для шифрування паролів в Windows NT).

Шифр RC4 застосовується в деяких широко поширених стандартах і протоколах шифрування таких, як WEP, WPA і TLS.

Алгоритм працює в режимі OFB. Для формування ключів використовується S - блок розміром $8 \times 8$ ($S_0, S_1, ...S_{255}$). Елементи становлять перестановку чисел від 0 до 255 , перестановка є функцією ключа змінної довжина. У алгоритмі застосовуються два індексних елемента $i, j = 0$. Для генерації випадкового байта виконуються наступні обчислення:

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

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

$S_i \leftrightarrow S_j;$

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

$Key = S_t.$

використовується в операції XOR з відкритим текстом для одержання шифротексту або в XOR із шифротекстом для одержання відкритого тексту. Головними факторами, що сприяли широкому застосуванню RC4, були простота його апаратної та програмної реалізації, а також висока швидкість роботи алгоритму в обох випадках. Алгоритм компактний в термінах розміру коду і особливо зручний для процесорів з побайтно - орієнтованою обробкою. Швидкість шифрування досягає 10 Мбайт/с на процесорах з тактовою частотою 330 Мгц. Компанія RSA Data Security, Inc стверджує, що алгоритм стійкий до диференційного и лінійного крипто аналізу.

У США довжина ключа для використання всередині країни рекомендується рівний 128 бітів, але угода, укладена між Software Publishers Association (SPA ) і урядом США дає RC4 спеціальний статус, який означає, що дозволено експортувати шифри довжиною ключа до 40 біт. 56 - бітові ключі дозволено використовувати закордонним відділенням американських компаній[1-4].

**Мета статті** є оцінка періодичності алгоритму поточного шифрування при значеннях індексних елементів $i, j <> 0$.

## Вирішення поставленого завдання

Методика дослідження періодичних властивостей алгоритму потокового шифрування RC4 над його міні-версією запропонована в статтях [5], вона полягає в побудові зменшеної версії алгоритму RC4, яка створюється, за допомогою масштабування із збереженням всіх базових операцій алгоритму. Дослідження періодичних властивостей міні-версій алгоритму потокового шифрування RC4 показала, що існує залежність розташування в S - блоці $S_0, S_1, ...S_n$ одиничного значення і початковими значеннями індексних елементів $i, j$, яке призводить до формування псевдовипадкових послідовностей обмеженого періоду.

Для проведення досліджень протестована робота алгоритму потокового шифрування RC4 для поля $GF(2^4)$ на повній множині ненульових ключових даних. Визначалися значення індексних елементів $i, j$ при яких довжина періоду була обмеженою.

У ході проведених досліджень було встановлено, що для кожного значення S -блоку (для поля $GF(2^4)$ існує значення індексних елементів $i, j <> 0$, при якому довжина періоду буде відповідати 240 елементам псевдовипадкової послідовності. У табл. 1 частково представлені результати проведеного експерименту.

Таблиця 1

Значення S-блоку та індексних елементів i, j,
що призводять до формування послідовності обмеженого періоду

| Значення S -блоку | | | | | | | | | | | | | | | | i | j | Довжина періоду | Розмірність поля |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $S_0$ | $S_1$ | $S_2$ | $S_3$ | $S_4$ | $S_5$ | $S_6$ | $S_7$ | $S_8$ | $S_9$ | $S_{10}$ | $S_{11}$ | $S_{12}$ | $S_{13}$ | $S_{14}$ | $S_{15}$ | | | | |
| 0 | 2 | 7 | 5 | 4 | 1 | 3 | 6 | - | - | - | - | - | - | - | - | 4 | 5 | 56 | $GF(2^3)$ |
| 7 | 0 | 6 | 1 | 2 | 3 | 4 | 5 | - | - | - | - | - | - | - | - | 2 | 3 | 56 | $GF(2^3)$ |
| 4 | 3 | 0 | 2 | 5 | 6 | 7 | 1 | - | - | - | - | - | - | - | - | 6 | 7 | 56 | $GF(2^3)$ |
| 1 | 2 | 4 | 6 | 7 | 3 | 5 | 8 | 10 | 11 | 12 | 13 | 0 | 14 | 9 | 15 | 15 | 0 | 240 | $GF(2^4)$ |
| 4 | 9 | 5 | 2 | 3 | 12 | 10 | 8 | 11 | 7 | 15 | 13 | 1 | 6 | 0 | 14 | 11 | 12 | 240 | $GF(2^4)$ |
| 8 | 13 | 12 | 14 | 7 | 1 | 3 | 6 | 2 | 5 | 4 | 0 | 15 | 10 | 11 | 9 | 4 | 5 | 240 | $GF(2^4)$ |
| 15 | 13 | 11 | 9 | 7 | 5 | 3 | 0 | 1 | 2 | 4 | 6 | 8 | 10 | 12 | 14 | 7 | 8 | 240 | $GF(2^4)$ |
| 1 | 15 | 3 | 5 | 7 | 4 | 2 | 0 | 6 | 14 | 13 | 12 | 11 | 10 | 9 | 8 | 15 | 0 | 240 | $GF(2^4)$ |
| 8 | 10 | 9 | 5 | 7 | 15 | 6 | 0 | 2 | 14 | 13 | 11 | 12 | 3 | 4 | 1 | 14 | 15 | 240 | $GF(2^4)$ |
| 3 | 6 | 5 | 2 | 4 | 7 | 10 | 1 | 11 | 12 | 15 | 14 | 8 | 9 | 0 | 13 | 6 | 7 | 240 | $GF(2^4)$ |

Як випливає з наведених у табл. 1 даних, існує залежність розташування одиничного елемента ($S_i = 1$) в $S$-блоці і значеннями індексних елементів $i, j$, при яких формується послідовність з обмеженою довжиною періоду.

Висунемо припущення, що гарантовано обмежений період має місце коли значення збігається з номером розташування одиничного елемента в $S$-блокі, а $i = j - 1$ (тільки для випадку коли одиничний елемент розташований в діапазоні $S_1 \div S_n$).

Для випадку коли значення і дорівнює номеру останнього елемента $S$-блоку, а $j = 0$.

Для перевірки висунутого припущення протестована робота алгоритму потокового шифрування RC4 для полів $GF(2^5), GF(2^6)$. У ході проведених досліджень довжина періоду при запропонованих значеннях $i, j$ склала 992 і 4032 елемента послідовності, що підтвердило висунуте припущення. Надалі були оцінені всі довжини обмежених періодів, формованої послідовності для полів $GF(2^n)$ де $n = 3 \div 10$, результати досліджень представлені в табл. 2.

Як видно з наведених у табл. 2 даних, для кожної розмірності поля $GF(2^n)$ існує своя довжина обмеженого періоду.

## Висновки

Проведенні дослідження показали, що в алгоритмі поточного шифрування RC4 в якості навчальних значень індексних елементів $i, j$ можливо брати не тільки значення $i, j = 0$, но і інші значення $i, j <> 0$. Виключенням являються значення $i = j - 1$ та $i = n, j = 0$, використання яких приводить до формування послідовностей з обмеженим періодом значно меншим в порівнянні з максимально можливим. Використання даних досліджень дає можливість збільшити кількість ключових даних, що в свою чергу збільшує криптостійкість.

Таблиця 2

Довжини гарантовано обмежених періодів дляполів $GF(2^n)$ при $n = 3 \div 10$

| № р/п | Розмірність поля | Максимальна довжина періоду | Довжина гарантовано обмеженого періоду |
|---|---|---|---|
| 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 |

## Список літератури

*1. Методи та алгоритми симетричної криптографії: Навч. пос. / О.О. Кузнецов, С.П. Євсеєв, О.А. Смірнов, Є.В. Мелешко, О.Г. Король. – Кіровоград: КНТУ, 2012. – 316 с.*

*2. Шнаер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си / Б.Шнаер. – М.: ТРИУМФ, 2002 – 816 с..*

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

*4. RC4 [Електроний ресурс]. – Режим доступу: http://dic.academic.ru/.*

*5. Анализ обобщения алгоритма RC4 [Електронний ресурс]. – Режим доступу: http://vniipvti.ru/data/file/sbor3_11.pdf.*

*Надійшла до редколегії 10.12.2013*

**Рецензент:** д-р техн. наук, проф. О.О. Кузнецов, Харківський національний університет ім. В.Н. Каразіна, Харків.

### ОЦЕНКА ПЕРИОДИЧНОСТИ АЛГОРИТМА ПОТОЧНОГО ШИФРОВАНИЯ ПРИ НЕНУЛЕВЫХ ЗНАЧЕНИЯХ ИНДЕКСНЫХ ЭЛЕМЕНТОВ

Р.В. Королев, Д.А. Волков

*В работе проведены исследования алгоритма поточного шифрования RC4 при ненулевых значениях индексных элементов. Определяются длины периодов псевдослучайных чисел с ограниченным периодом. Установлено, что существует зависимость размещения единичного элемента в S-блоке с значениями индексных элементов, при которых формируется последовательность с ограниченным периодом.*

***Ключевые слова:*** *генератор псевдослучайных чисел, алгоритм текущего шифрования, RC4.*

### ESTIMATION OF PERIODICITY OF ALGORITHM OF ENCIPHEREMENT AT UNZERO VALUES OF INDEX ELEMENTS

R.V. Korolev, D.A. Volkov

*Researches of algorithm of stream encipherement of RC4 are in-process conducted at unzero values of index elements. Lengths of periods of pseudocasual numbers are determined with the limited period. It is set that exists dependence of placing of single element in S-blok with the values of index elements at which is formed sequence with the limited period.*

***Keywords:*** *generator of pseudocasual numbers, algorithm of current encipherement, RC4.*