

А.С.Цурина

ЛИНЕЙНАЯ СЛОЖНОСТЬ ВОСЬМЕРИЧНЫХ СБАЛАНСИРОВАННЫХ БИНАРНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

В данной статье представлены результаты исследования линейной сложности восьмеричных бинарных последовательностей, сформированных на основе четырех циклотомических классов.

Ключевые слова: линейная сложность, восьмеричные последовательности, циклотомические классы

Введение

Проблема защиты информации путем ее преобразования, исключающего ее прочтение посторонним лицом, волновала человеческий ум с давних времен. Традиционным обеспечением конфиденциальности, целостности и аутентификации данных является шифрование. По правилу Керкхoffa, стойкость алгоритма шифрования должна определяться стойкостью ключа, то есть длиной используемого ключа.

Стандартное симметричное шифрование не является абсолютно стойким, так как имеет ключи небольшой длины, например, в IDEA применяются 128-разрядные ключи, в алгоритме Blowfish размер ключа варьируется от 32 до 448 бит, в DES используются 56-разрядные ключи.

Линейная сложность ключевого потока поточного шифра — важный показатель для оценки его устойчивости и безопасности. Чем выше линейная сложность псевдослучайной последовательности, тем выше стойкость этой последовательности к взлому. Поэтому последовательности, обладающие высокой линейной сложностью, важны для криптографических приложений. Отдельные сведения о линейной сложности восьмеричных бинарных последовательностей над полем второго порядка были получены в [1].

Цель настоящей работы заключается в исследовании линейной сложности восьмеричных сбалансированных бинарных периодических последовательностей. Линейная сложность последовательности будет определена посредством разложения периода последовательности на сумму квадратов целых чисел. Метод исследования основан на найденных в [2] соотношениях для многочлена последовательности, соответствующего классу восьмеричных вычетов.

Основные определения

Пусть $p = 1 + 8f$, обозначим через H_0 — класс вычетов 8 степени по модулю p , то есть $H_0 = \{q^{8t} \pmod p, t = 0, f-1\}$, здесь q — первообразный корень по модулю p . Положим $H_s = q^s H_0$, где $s = \overline{0,7}$ (все действия выполняются по модулю p), тогда $H_i \cap H_j = \emptyset, i \neq j$ и порядок $|H_i| = f$.

Рассмотрим последовательность $X = \{x_i\}$, сформированную по следующему правилу:

$$x_i = \begin{cases} 1, & \text{если } i \pmod p \in \bigcup_{k \in I} H_k, \\ 0, & \text{в остальных случаях.} \end{cases}, \quad (1)$$

где I — подмножество множества индексов $\{0, 1, K, 7\}$.

Обозначим через a примитивный корень степени p из единицы в поле разложения многочлена $t^p - 1$ над полем второго порядка. Пусть $S_8(a) = (S_8(a), S_8(a^q), K, S_8(a^{q^7}))$ и $T_X(a) = \sum_{k \in I} D^k S_8(a)$, где D — оператор циклического сдвига матрицы на единицу влево.

Тогда, согласно [3], линейная сложность последовательности, сформулированная на основе восьмеричных вычетов, будет определяться по следующей формуле:

$$L = p - \frac{p-1}{8} \Delta - 1, \quad (2)$$

где Δ — число нулей в $T_X(a)$.

Для $p = 1 + 8f$ справедливы разложения: $p = x^2 + 4y^2 = a^2 + 2b^2$, $x \equiv a \equiv 1 \pmod 4$, где x, a, y, b

— целые числа. Согласно [4, 5], формулы для циклотомических чисел зависят от f, y . Здесь рассмотрим только случай, когда $(p-1)/8$ — нечетное. Как показано в [2], для $y \equiv 0 \pmod{4}$ справедливы следующие соотношения:

$$S_d(\alpha) = (\omega, \omega+1, 0, \omega+1, \omega+1, \omega, 0, \omega), \text{ если } x \equiv 5 \pmod{16} \text{ и } y \equiv 0 \pmod{8}, \text{ и } b \equiv 2 \pmod{8}, p = 41, 137, 281, \dots$$

$$S_d(\alpha) = (\omega, \omega, 0, \omega, \omega+1, \omega+1, 0, \omega+1), \text{ если } x \equiv 5 \pmod{16} \text{ и } y \equiv 0 \pmod{8}, \text{ и } b \equiv 6 \pmod{8}, p = 313, 409, 457, \dots$$

$$S_d(\alpha) = (\omega, \omega+1, 1, \omega+1, \omega+1, \omega, 1, \omega), \text{ если } x \equiv 13 \pmod{16} \text{ и } y \equiv 0 \pmod{8}, \text{ и } b \equiv 2 \pmod{8}, p = 521, 569, 617, \dots$$

$$S_d(\alpha) = (\omega, \omega, 1, \omega, \omega+1, \omega+1, 1, \omega+1), \text{ если } x \equiv 13 \pmod{16} \text{ и } y \equiv 0 \pmod{8}, \text{ и } b \equiv 6 \pmod{8}, p = 761, 809, 857, \dots$$

$$S_d(\alpha) = (1, 0, 1, 0, 0, 1, 1, 1), \text{ если } x \equiv 5 \pmod{16} \text{ и } y \equiv 4 \pmod{8}, \text{ и } b \equiv 2 \pmod{8}, p = 73, 89, 233, \dots$$

$$S_d(\alpha) = (1, 1, 1, 1, 0, 0, 1, 0), \text{ если } x \equiv 5 \pmod{16} \text{ и } y \equiv 4 \pmod{8}, \text{ и } b \equiv 6 \pmod{8}, p = 601, 937, 1289, \dots$$

$$S_d(\alpha) = (1, 0, 0, 0, 0, 1, 0, 1), \text{ если } x \equiv 13 \pmod{16} \text{ и } y \equiv 4 \pmod{8}, \text{ и } b \equiv 2 \pmod{8}, p = 1433, 1609, 1721, \dots$$

$$S_d(\alpha) = (1, 1, 0, 1, 0, 0, 0, 0), \text{ если } x \equiv 13 \pmod{16} \text{ и } y \equiv 4 \pmod{8}, \text{ и } b \equiv 6 \pmod{8}, p = 1801, 1913, 2089, \dots$$

Воспользовавшись методом, предложенным в [2], аналогично получаем следующие соотношения для $y \equiv 2 \pmod{4}$:

$$S_d(\alpha) = (\eta, \omega+1, \omega\eta+\omega, \omega, \omega+\eta, \omega+1, \omega\eta+1, \omega), \text{ если } x \equiv 5 \pmod{16} \text{ и } y \equiv 2 \pmod{8}, \text{ и } b \equiv 4 \pmod{8}, p = 953, 2633, 2729, \dots$$

$$S_d(\alpha) = (\eta, \omega, \omega\eta+\omega, \omega+1, \omega+\eta, \omega, \omega\eta+1, \omega+1), \text{ если } x \equiv 5 \pmod{16} \text{ и } y \equiv 2 \pmod{8}, \text{ и } b \equiv 0 \pmod{8}, p = 2953, 1129, 2297, \dots$$

$$S_d(\alpha) = (\eta+1, \omega+1, \omega\eta+\omega+1, \omega, \omega+\eta+1, \omega+1, \omega\eta, \omega), \text{ если } x \equiv 13 \pmod{16} \text{ и } y \equiv 2 \pmod{8}, \text{ и } b \equiv 0 \pmod{8}, p = 1321, 2377, 1657, \dots$$

$$S_d(\alpha) = (\eta+1, \omega, \omega\eta+\omega+1, \omega+1, \omega+\eta+1, \omega, \omega\eta, \omega+1), \text{ если } x \equiv 13 \pmod{16} \text{ и } y \equiv 2 \pmod{8}, \text{ и } b \equiv 4 \pmod{8}, p = 2521, 1993, 2137, \dots$$

Линейная сложность последовательности на основе четырех циклотомических классов

В этом подразделе исследуем линейную сложность сбалансированных бинарных последовательностей.

Теорема 1. Пусть последовательность X сформирована по (1) для $I=\{0,1,2,3\}$, $p = x^2 + 4y^2 = a^2 + 2b^2$, $x \equiv a \equiv 1 \pmod{4}$, $y \equiv 0 \pmod{4}$ и $(p-1)/8$ — нечетное число. Тогда:

$$L = \frac{(p-1)}{2}, \text{ если } y \equiv 4 \pmod{8};$$

$$L = p-1, \text{ если } y \equiv 0 \pmod{8}.$$

Доказательство. Рассмотрим первый случай, когда $x \equiv 5 \pmod{16}$ и $y \equiv 0 \pmod{8}$, и $b \equiv 2 \pmod{8}$.

Здесь $S_8(\alpha) = (\omega, \omega+1, 0, \omega+1, \omega+1, \omega, 0, \omega)$, тогда

$$T_X(\alpha) = S_8(\alpha) + DS_8(\alpha) + D^2S_8(\alpha) + D^3S_8(\alpha) = (\omega, \omega+1, \omega, \omega, \omega+1, \omega, \omega+1, \omega+1).$$

Таким образом, в этом случае $\Delta = 0$, и утверждение теоремы следует из формулы (2).

Если $x \equiv 5 \pmod{16}$, $y \equiv 0 \pmod{8}$ и $b \equiv 6 \pmod{8}$, то $S_8(\alpha) = (\omega, \omega, 0, \omega, \omega+1, \omega+1, 0, \omega+1)$ и

$T_x(\alpha) = S_8(\alpha) + DS_8(\alpha) + D^2S_8(\alpha) + D^3S_8(\alpha) = (\omega, \omega+1, \omega, \omega, \omega+1, \omega, \omega+1, \omega+1)$. Здесь, как и в первом случае, $\Delta = 0$.

Покажем, что $\Delta = 0$ в третьем и четвертом случаях.

Если $x \equiv 13 \pmod{16}$, $y \equiv 0 \pmod{8}$, и $b \equiv 2 \pmod{8}$, то $S_8(\alpha) = (\omega, \omega+1, 1, \omega+1, \omega+1, \omega, 1, \omega)$ и $T_x(\alpha) = S_8(\alpha) + DS_8(\alpha) + D^2S_8(\alpha) + D^3S_8(\alpha) = (\omega+1, \omega, \omega+1, \omega+1, \omega, \omega+1, \omega, \omega)$ и, как мы видим, $\Delta = 0$.

В четвертом случае, когда $x \equiv 13 \pmod{16}$, $y \equiv 0 \pmod{8}$ и $b \equiv 6 \pmod{8}$, имеем, что $S_8(\alpha) = (\omega, \omega, 1, \omega, \omega+1, \omega+1, 1, \omega+1)$ и $T_x(\alpha) = (\omega+1, \omega, \omega+1, \omega+1, \omega, \omega+1, \omega, \omega)$. Здесь также $\Delta = 0$.

Таким образом, если $y \equiv 0 \pmod{8}$, то $\Delta = 0$ и $L = p - 1$.

Рассмотрим оставшиеся четыре случая.

Если $x \equiv 5 \pmod{16}$ и $y \equiv 4 \pmod{8}$ и $b \equiv 2 \pmod{8}$, то $S_8(\alpha) = (1, 0, 1, 0, 0, 1, 1, 1)$, тогда $T_x(\alpha) = (0, 1, 1, 0, 1, 0, 0, 1)$ и, следовательно, $\Delta = 4$.

Если $x \equiv 5 \pmod{16}$ и $y \equiv 4 \pmod{8}$ и $b \equiv 6 \pmod{8}$, то $S_8(\alpha) = (1, 1, 1, 1, 0, 0, 1, 0)$, тогда $T_x(\alpha) = (0, 1, 0, 0, 1, 0, 1, 1)$ и $\Delta = 4$.

Если $x \equiv 13 \pmod{16}$ и $y \equiv 4 \pmod{8}$ и $b \equiv 2 \pmod{8}$, то $S_8(\alpha) = (1, 0, 0, 0, 0, 1, 0, 1)$, тогда $T_x(\alpha) = (1, 0, 1, 1, 0, 1, 0, 0)$ и $\Delta = 4$.

Если $x \equiv 13 \pmod{16}$ и $y \equiv 4 \pmod{8}$ и $b \equiv 6 \pmod{8}$, то $S_8(\alpha) = (1, 1, 0, 1, 0, 0, 0, 0)$, тогда $T_x(\alpha) = (1, 0, 1, 1, 0, 1, 0, 0)$ и $\Delta = 4$.

Следовательно, если $y \equiv 4 \pmod{8}$, то $\Delta = 4$, тогда утверждение теоремы следует из формулы (2).

Таким образом, теорема 1 доказана.

В таблице 1 приведены результаты непосредственного вычисления линейной сложности последовательностей.

Таблица 1.

Линейная сложность последовательности X для $I=\{0,1,2,3\}$ при $y \equiv 0 \pmod{4}$

p	L	p	L	p	L	p	L
41	40	313	312	521	520	761	760
137	136	409	408	569	568	809	808
281	280	457	456	617	616	857	856
p	L	p	L	p	L	p	L
73	36	601	300	1433	716	1801	900
89	40	937	468	1609	804	1913	956
233	116	1289	644	1721	860	2089	1044

Анализ результатов, представленных в табл. 1, подтверждает справедливость теоремы 1.

Доказательство нижеприведенных теорем проводится с применением этого же метода.

Теорема 2. Пусть последовательность X сформирована по (1) для $I=\{0,1,2,3\}$, где $p = x^2 + 4y^2 = a^2 + 2b^2$, $x \equiv a \pmod{4}$, $y \equiv 2 \pmod{4}$ и $(p-1)/8$ — нечетное число.

Тогда $L = p - 1$.

Ниже приведена таблица, иллюстрирующая теорему 2 на числовых значениях.

Таблица 2

Линейная сложность последовательности X для I={0,1,2,3} при $y \equiv 2 \pmod{4}$

p	L	p	L	p	L	p	L
953	952	2953	2952	1321	1320	2521	2520
2633	2632	1129	1128	2377	2376	1993	1992
2729	2728	2297	2296	1657	1656	2137	2136

Рассмотрим еще два варианта I={0,1,2,5} и I={0,1,3,4}. Для $y \equiv 0 \pmod{4}$ случай I={0,1,2,5} уже был рассмотрен в [3].

Теорема 3. Пусть последовательность X сформирована по (1) для I={0,1,2,5}, где $p = x^2 + 4y^2 = a^2 + 2b^2$, $x \equiv a \equiv 1 \pmod{4}$, $y \equiv 2 \pmod{4}$ и $(p-1)/8$ — нечетное число. Тогда $L = p - 1$.

Ниже приведена таблица, поясняющая теорему 3 на числовых значениях.

Таблица 3

Линейная сложность последовательности X для I={0,1,2,5} при $y \equiv 2 \pmod{4}$

p	L	p	L	p	L	p	L
953	952	2953	2952	1321	1320	2521	2520
2633	2632	1129	1128	2377	2376	1993	1992
2729	2728	2297	2296	1657	1656	2137	2136

Теорема 4. Пусть последовательность X сформирована по (1) для I={0,1,3,4}, $p = x^2 + 4y^2 = a^2 + 2b^2$, $x \equiv a \equiv 1 \pmod{4}$, $y \equiv 0 \pmod{4}$ и $(p-1)/8$ — нечетное число. Тогда:

$L = p - 1$, если $y \equiv 0 \pmod{8}$;

$L = \frac{3(p-1)}{4}$, если $y \equiv 4 \pmod{8}$.

Ниже приведена таблица, иллюстрирующая теорему 4 на числовых значениях.

Таблица 4

Линейная сложность последовательности X для I={0,1,3,4} при $y \equiv 0 \pmod{4}$

p	L	p	L	p	L	p	L
41	40	313	312	521	520	761	760
137	136	409	408	569	568	809	808
281	280	457	456	617	616	857	856
p	L	p	L	p	L	p	L
73	54	601	450	1433	1074	1801	1350
89	66	937	702	1609	1206	1913	1434
233	174	1289	966	1721	1290	2089	1566

Теорема 5. Пусть последовательность X сформирована по (1) для I={0,1,3,4}, где $p = x^2 + 4y^2 = a^2 + 2b^2$, $x \equiv a \equiv 1 \pmod{4}$, $y \equiv 2 \pmod{4}$ и $(p-1)/8$ — нечетное число. Тогда $L = p - 1$.

Ниже приведена таблица, поясняющая теорему на числовых значениях.

Таблица 5

Линейная сложность последовательности X для I={0,1,3,4} при $y \equiv 2(\text{mod } 4)$

p	L	p	L	p	L	p	L
953	952	2953	2952	1321	1320	2521	2520
2633	2632	1129	1128	2377	2376	1993	1992
2729	2728	2297	2296	1657	1656	2137	2136

Анализ результатов расчетов линейной сложности, представленных в таблицах 2—5, подтверждает справедливость теорем 2—5.

Заключение

Таким образом, получены теоретические сведения о линейной сложности восьмеричных сбалансированных бинарных последовательностей, формируемых по (1), в зависимости от разложения периода последовательности $p = x^2 + 4y^2 = a^2 + 2b^2$ при $x \equiv a \equiv 1(\text{mod } 4)$. Выделены регулярные правила кодирования последовательностей с высокой линейной сложностью.

1. Лидл Р., Нидеррайтер Г. Конечные поля. М.: Мир, 1988. 820 с.
2. Едемский В.А., Гантмахер В.Е. Синтез двоичных и троичных последовательностей с заданными ограничениями на их характеристики. Великий Новгород.: НовГУ, 2009. 189 с.
3. Едемский В.А. О линейной сложности двоичных последовательностей на основе классов биквадратичных и шестеричных вычетов // Дискретная математика. 2010. Т. 22. Вып. 1. С. 74-82.
4. Холл М. Комбинаторика. М.: Мир, 1970. 423 с.
5. Lehmer E. On the number of solutions of $u^k + D \equiv w^2(\text{mod } p)$ // Pacific J. Math. 1955. Vol. 5. P. 103-118.

References

1. Lidl R., Niderrayter G. Konechnye polya. M.: Mir, 1988. 820 s.
2. Edemskiy V.A., Gantmakher V.E. Sintez dvoichnykh i troichnykh posledovatel'nostey s zadannymi ograniceniyami na ikh kharakteristiki. Velikiy Novgorod.: NovGU, 2009. 189 s.
3. Edemskiy V.A. O lineynoy slozhnosti dvoichnykh posledovatel'nostey na osnove klassov bikvadratichnykh i shesterichnykh vychetov // Diskretnaya matematika. 2010. T. 22. Vyp. 1. S. 74-82.
4. Kholl M. Kombinatorika. M.: Mir, 1970. 423 s.
5. Lehmer E. On the number of solutions of $u^k + D \equiv w^2(\text{mod } p)$ // Pacific J. Math. 1955. Vol. 5. P. 103-118.

Tsurina A.S. Linear complexity of octal binary sequences. In this article we present research findings of the linear complexity of octal binary sequences formed on the basis of four cyclotomic classes.

Keywords: linear complexity, octal sequence, cyclotomic classes.

Сведения об авторе. А.С.Цурина — студент 3 курса ИЭИС НовГУ им. Ярослава Мудрого; направление «Прикладная математика и информатика»; aleksandra.curina@mail.ru.

Статья публикуется впервые. Поступила в редакцию 16.05.2016.