УДК 621.391:519.95

А. Н. Алексейчук, Е. В. Скрынник
Институт специальной связи и защиты информации НТУУ «КПИ»
ул. Московская, 45/1, 01011 Киев, Украина

Классы отображений с тривиальной линейной структурой над конечным полем

Получены допускающие простую практическую проверку условия, при которых отображение над конечным полем обладает свойством тривиальности линейной структуры, важным в криптографических приложениях.

Ключевые слова: *криптографическая защита информации, линейная структура дискретного отображения, конечное поле.*

Одним из известных требований к дискретным отображениям, используемым в современных симметричных системах шифрования, является условие отсутствия линейных трансляторов. Напомним (см., например, [1]), что ненулевой вектор $a \in \mathbf{GF}(2)^n$ называется линейным транслятором отображения $\varphi : \mathbf{GF}(2)^n \to \mathbf{GF}(2)^m$, если существует элемент $c \in \mathbf{GF}(2)^m$ такой, что равенство $\varphi(x+a)+\varphi(x)=c$ выполняется для всех $x \in \mathbf{GF}(2)^n$. Как правило, наличие линейных трансляторов (или, как говорят, нетривиальность линейной структуры) отображения φ свидетельствует о его криптографических слабостях. Отметим, например, работу [2], в которой показано, что нетривиальность линейной структуры функции усложнения генератора гаммы синхронной поточной шифрсистемы позволяет повысить эффективность атак на эту шифрсистему, основанных на реинициализации начального состояния генератора.

Исследованию строения множества линейных трансляторов булевых функций и подстановок на множестве $\mathbf{GF}(2)^n$, используемых при построении блочных шифров, посвящены работы [2–4] и [5, 6] соответственно. В [7] предложено обобщение понятия линейного транслятора для отображений векторных пространств над конечными полями и исследованы распределения ряда числовых характеристик множества аддитивных (линейных) трансляторов случайных равновероятных отображений указанного вида.

С криптографической точки зрения, более естественным (и более жестким) является требование, состоящее в отсутствии линейных трансляторов не только у данного отображения $\varphi : \mathbf{GF}(2)^n \to \mathbf{GF}(2)^m$, но и у всех ненулевых линейных ком-

бинаций его координатных функций. Формализация этого условия (применительно к более широкому классу отображений одной конечной абелевой группы в другую) приводит к понятию тривиальности линейной структуры дискретного отображения, введенному в [8]. Отметим, что это, более общее по сравнению с [7], понятие возникает естественным образом при обосновании достаточных условий стойкости блочных шифров относительно алгебраических атак, основанных на гомоморфизмах [8, 9].

Настоящая статья посвящена нахождению условий, гарантирующих тривиальность линейной структуры отображения $\varphi : F \to F$, где F — произвольное конечное поле. Каждое такое отображение может быть представлено полиномом с коэффициентами из F (см., например, [10], с. 438), и, как показано ниже, тривиальность линейной структуры отображения φ можно обеспечить, накладывая определенные ограничения на степень (или коэффициенты) данного полинома. В частности, показано, что тривиальную линейную структуру имеют все отображения степени $4k+3$, где $1 \le k \le 2^{n/2-2}-1$, над полем из 2^n элементов, а также (при $n = 2^t$, $t \ge 2$) известное отображение $x \mapsto x^{-1}$, $x \in \mathbf{GF}(2)^n$, используемое в конструкциях современных блочных шифров [11, 12].

Перейдем к подробному изложению полученных результатов. Прежде всего, напомним основное определение, приведенное в [8].

Пусть G_1 и G_2 — конечные абелевы группы, $\varphi : G_1 \to G_2$ — произвольное отображение. Будем говорить, что φ *имеет тривиальную линейную структуру*, если не существует элемента $a \in G_1 \setminus \{0\}$ и комплексного характера $\psi \ne 1$ группы G_2 таких, что функция $\psi(\varphi(x+a)-\varphi(x))$, $x \in G_1$, является константой. В случае невыполнения указанного условия будем говорить, что отображение φ имеет нетривиальную линейную структуру.

Ниже рассматриваются исключительно преобразования φ аддитивной группы конечного поля: $G_1 = G_2 = (F, +)$, где $F = \mathbf{GF}(p^n)$, p — простое число, $n \in \mathbf{N}$. Обозначим $\mathrm{Tr}(x) = x + x^p + \ldots + x^{p^{n-1}}$ абсолютный след элемента $x \in F$, $\chi(x) = \exp\{\frac{2\pi i \mathrm{Tr}(x)}{p}\}$, $x \in F$ — канонический аддитивный характер поля F. Заметим, что поскольку каждый характер ψ группы $(F, +)$ имеет вид $\chi(bx)$, $x \in F$, для некоторого $b \in F$ (см. теорему 5.7 в [10]), то отображение $\varphi : F \to F$ тогда и только тогда имеет тривиальную линейную структуру, когда для любых $a, b \in F \setminus \{0\}$ выполняется соотношение $\mathrm{Tr}(b\varphi(x+a) - b\varphi(x)) \ne \mathrm{const}$.

Приведем два простых критерия тривиальности линейной структуры отображения $\varphi : F \to F$. Первый из них связан с представлением данного отображения набором его координатных функций: $\varphi = (\varphi_1, \ldots, \varphi_n)$, где $\varphi_i : F \to \mathbf{GF}(p)$, $i \in \overline{1,n}$, а второй — с его полиномиальным представлением над полем F:

$$\varphi(x) = \sum_{i=0}^{d} c_i x^i, \; c_i \in F, \; i \in \overline{0,d}. \qquad (1)$$

Зафиксируем пару дуальных базисов $\alpha = (\alpha_1, \ldots, \alpha_n)$, $\beta = (\beta_1, \ldots, \beta_n)$ поля F над полем $\mathbf{GF}(p)$ (см. [10], с. 78) и отождествим произвольный элемент $b \in F$ с вектором его координат в базисе α, а значения отображения φ — с векторами их координат в базисе β. Справедливо равенство $\mathrm{Tr}(b\varphi(x+a) - b\varphi(x)) = \\ = < b, \varphi(x+a) - \varphi(x) >$, $x \in F$, где $< u, v >$ обозначает скалярное произведение векторов u и v над полем $\mathbf{GF}(p)$. Отсюда следует, что отображение φ имеет тривиальную линейную структуру в том и только в том случае, когда все ненулевые линейные комбинации $b_1\varphi_1 + \ldots + b_n\varphi_n$ его координатных функций с коэффициентами из $\mathbf{GF}(p)$ не имеют аддитивных трансляторов (в терминологии [7]). Отметим, что при $p = 2$ приведенное утверждение позволяет установить необходимое и достаточное условие тривиальности линейной структуры отображения φ в терминах таблицы его линейных аппроксимаций, характеризующей его «устойчивость» относительно метода линейного криптоанализа.

Напомним [13], что таблица линейных аппроксимаций отображения $\varphi : \mathbf{GF}(2)^n \to \mathbf{GF}(2)^n$ определяется как квадратная матрица $LP^{(\varphi)}$ порядка 2^n с элементами

$$LP^{(\varphi)}(u, v) = (2\mathbf{P}\{< u, X > = < v, \varphi(X) >\} - 1)^2, \quad u, v \in \mathbf{GF}(2)^n, \tag{2}$$

где X — случайный вектор с равномерным распределением вероятностей на множестве $\mathbf{GF}(2)^n$. На основании равенства (2) для любого $v = (v_1, \ldots, v_n) \in \mathbf{GF}(2)^n$ v-й столбец матрицы $LP^{(\varphi)}$ состоит из квадратов нормированных коэффициентов Уолша-Адамара булевой функции $< v, \varphi > = v_1\varphi_1 + \ldots + v_n\varphi_n$:

$$LP^{(\varphi)}(u, v) = 2^{-2n}\left(\sum_{x \in \mathbf{GF}(2)^n} (-1)^{<u,x> + <v,\varphi(x)>}\right)^2, \; u, v \in \mathbf{GF}(2)^n. \tag{3}$$

Непосредственно из формулы (3) и теоремы 1, доказанной в [3] (см. также задачу 2.112 в [1]), вытекает следующее утверждение.

Утверждение 1. Отображение $\varphi : \mathbf{GF}(2)^n \to \mathbf{GF}(2)^n$ имеет тривиальную линейную структуру в том и только в том случае, когда для любого $v \in \mathbf{GF}(2)^n \setminus \{0\}$ множество $\{u \in \mathbf{GF}(2)^n : LP^{(\varphi)}(u, v) = 0\}$ не содержит ни одной гиперплоскости в пространстве $\mathbf{GF}(2)^n$. В частности, φ имеет тривиальную линейную структуру, если для любого $v \in \mathbf{GF}(2)^n \setminus \{0\}$ мощность множества $\{u \in \mathbf{GF}(2)^n : LP^{(\varphi)}(u, v) = 0\}$ меньше, чем 2^{n-1}.

Пусть теперь φ — произвольное отображение вида (1) над полем F. Для любых $a, b \in F \setminus \{0\}$ обозначим

$$\varphi_{a,b}(x) = b\varphi(x+a) - b\varphi(x). \tag{4}$$

Назовем полином $f(x) \in F[x]$ *невырожденным*, если не существует элементов $g(x) \in F[x]$, $c \in F$, таких, что $f(x)$ представим в виде:

$$g(x)^p - g(x) + c. \tag{5}$$

Понятие невырожденности полинома над конечным полем связано с известной границей Карлица-Ушиямы (см., например, [10], с. 306), согласно которой для любого невырожденного полинома $f(x) \in F[x]$ степени $d \geq 1$ выполняется неравенство

$$\left| \sum_{x \in F} \chi(f(x)) \right| \leq (d-1) p^{n/2}. \tag{6}$$

Следующее утверждение устанавливает достаточное условие тривиальности линейной структуры отображения (1).

Утверждение 2. Пусть $\varphi(x)$ — полином вида (1) над полем $F = \mathbf{GF}(p^n)$ такой, что $\deg \varphi(x) = d$, $2 \leq d < p^{n/2} + 2$, и для любых $a, b \in F \setminus \{0\}$ полином (4) является невырожденным. Тогда отображение φ имеет тривиальную линейную структуру.

Доказательство. Предположим противное: существуют $a, b \in F \setminus \{0\}$ такие, что $\chi(\varphi_{a,b}(x)) \equiv \text{const}$. Тогда $\left| \sum_{x \in F} \chi(\varphi_{a,b}(x)) \right| = p^n$. С другой стороны, из условия утверждения и неравенства (6) следует, что

$$\left| \sum_{x \in F} \chi(\varphi_{a,b}(x)) \right| \leq (\deg \varphi_{a,b}(x) - 1) p^{n/2} \leq (d-2) p^{n/2} < p^n.$$

Полученное противоречие означает, что отображение φ имеет тривиальную линейную структуру, что и требовалось доказать.

Утверждение 3. Для любых $a, b \in F \setminus \{0\}$, $c \in F$, отображения $x \mapsto \varphi(x)$, $x \in F$ и $x \mapsto b\varphi(ax) + c$, $x \in F$, имеют тривиальную или нетривиальную линейную структуру одновременно. Кроме того, φ имеет тривиальную линейную структуру тогда и только тогда, когда отображение $x \mapsto \varphi(x^p)$, $x \in F$, имеет тривиальную линейную структуру.

Доказательство. Первая часть утверждения следует непосредственно из определения тривиальности линейной структуры. Вторая часть вытекает из равенства $(x+y)^p = x^p + y^p$, $x, y \in F$, и биективности отображения $x \mapsto x^p$, $x \in F$.

Итак, согласно утверждению 3, при построении отображений с тривиальной линейной структурой достаточно ограничиться такими полиномами (1), старшие

коэффициенты которых равны 1, а свободные члены — 0. При этом, принимая во внимание вторую часть утверждения, можно вначале исследовать полиномы, степени которых взаимно просты с числом p.

Утверждение 4. Пусть $\varphi(x)$ — полином вида (1) над полем $F = \mathbf{GF}(p^n)$, $\deg\varphi(x) = d$, $2 \le d < p^{n/2} + 2$. Тогда справедливы следующие утверждения.

1. Если p — нечетное число, $d \ge 3$, то при выполнении условия

$$(d, p) = (d-1, p) = 1 \tag{7}$$

отображение φ имеет тривиальную линейную структуру.

2. Если $p = 2$, $d \ge 7$ и

$$d \equiv 3 (\mathrm{mod}\, 4), \tag{8}$$

то отображение φ имеет тривиальную линейную структуру.

Доказательство. Предположим, не ограничивая общности рассуждений, что в выражении (1) $c_d = 1$. Пусть $a, b \in F \setminus \{0\}$. Из равенств (1) и (4) следует соотношение

$$\varphi_{a,b}(x) = abdx^{d-1} + (abc_{d-1}(d-1) + a^2 b\frac{d(d-1)}{2})x^{d-2} + h(x), \tag{9}$$

где $h(x) \in F[x]$, $\deg h(x) \le d-3$.

Если p — нечетное число, то на основании равенств (7), (9) полином $\varphi_{a,b}(x)$ имеет степень $d-1$, взаимно простую с p, и, следовательно, является невырожденным. Таким образом, согласно утверждению 2, отображение φ имеет тривиальную линейную структуру.

Пусть теперь $p = 2$, $d = 4k+3$, где $k \ge 1$. Тогда равенство (9) может быть записано в виде:

$$\varphi_{a,b}(x) = abx^{4k+2} + a^2 bx^{4k+1} + h(x),\ \deg h(x) \le 4k. \tag{10}$$

Предположим, что существуют $g(x) = \sum_{j \ge 0} g_j x^j \in F[x]$, $c \in F$, такие, что

$$\varphi_{a,b}(x) = g(x)^2 + g(x) + c. \tag{11}$$

Из формул (10), (11) следует, что $\deg g(x) = 2k+1$; в частности, $g_{4k+1} = 0$. С другой стороны, согласно тем же формулам, $g_{4k+1} = a^2 b \ne 0$. Полученное противоречие означает, что полином (4) является невырожденным, и на основании утверждения 2 отображение φ имеет тривиальную линейную структуру.

Утверждение доказано.

Итак, при выполнении неравенств $1 \le k \le 2^{n/2-2} - 1$ каждый полином нечетной степени $d = 4k + 3$ над полем $\mathbf{GF}(2^n)$ задает отображение φ с тривиальной линейной структурой. Случай, в котором $\deg \varphi = 4k + 1$, $k \ge 1$, оказывается более трудным для исследования. При $k = 1$ справедливо следующее, несколько неожиданное утверждение.

Утверждение 5. Пусть $n \ge 3$. Тогда каждое отображение, соответствующее полиному степени $d = 5$ над полем $F = \mathbf{GF}(2^n)$, имеет нетривиальную линейную структуру.

Доказательство. Пусть $\varphi(x) \in F[x]$ — полином вида (1), $\deg \varphi(x) = 5$, $c_5 = 1$. Положим $a = 1$ и покажем, что существуют $g(x) \in F[x]$, $c \in F$, $b \in F \setminus \{0\}$, для которых выполняется равенство (11).

Действительно, на основании равенств (1), (4) справедливо соотношение

$$\varphi_{1,b}(x) = bx^4 + bc_3x^2 + b(c_3 + 1)x + c,$$

где $c = c_1 + c_2 + c_3 + c_4 + 1$. Если $c_3 = 1$, то, полагая $b = 1$, получим, что $\varphi_{1,1}(x) = x^4 + x^2 + c$, и равенство (11) выполняется при $g(x) = x^2$. Пусть $c_3 \ne 1$. Положим

$$b = (c_3^{\,2} + 1)^{-1},\ g(x) = x^2(bc_3 + b^2(c_3^{\,2} + 1)) + xb(c_3 + 1).$$

Теперь, используя равенство $b = b^2 c_3^{\,2} + b^4(c_3^{\,4} + 1)$, нетрудно непосредственно убедиться в справедливости формулы (11) для указанных a, b, c и $g(x)$.

Утверждение доказано.

Широкий класс отображений с тривиальной линейной структурой, соответствующих полиномам степени $4k + 1$ над полем $\mathbf{GF}(2^n)$, описывает следующее утверждение.

Утверждение 6. Пусть $\varphi(x)$ — полином вида (1) над полем $F = \mathbf{GF}(2^n)$, $\deg \varphi(x) = 4k + 1 < 2^{n/2} + 2$, где $k = 2^t s$, $s \equiv 1 (\mathrm{mod}\, 2)$, $s \ge 3$. Тогда при выполнении условия

$$c_{4k} = c_{4k-1} = \ldots = c_{2k+2} = 0 \qquad (12)$$

отображение φ имеет тривиальную линейную структуру.

Доказательство. Предположим, не ограничивая общности рассуждений, что в выражении (1) $c_{4k+1} = 1$. Зафиксируем $a, b \in F \setminus \{0\}$. Допустим, что существуют $g(x) = \sum_{j \ge 0} g_j x^j \in F[x]$, $c \in F$, для которых выполняется равенство (11). Согласно формулам (1) и (4), справедливо соотношение $\varphi_{a,b}(x) = \sum_{j=0}^{4k} f_j x^j$, где

$$f_j = b\sum_{i=j+1}^{4k+1}\binom{i}{j}c_i a^{i-j},\ j \in \overline{0,4k}. \tag{13}$$

При этом, поскольку $\deg\varphi_{a,b}(x) = 4k$, то $\deg g(x) = 2k$ и, следовательно, $g_{2l+1} = 0$ для любого $l \in \overline{k,2k-1}$. Отсюда на основании равенства (11) вытекает, что

$$f_{2l+1} = 0,\ l \in \overline{k,2k-1}. \tag{14}$$

Заметим теперь, что, согласно равенствам (12), (13), соотношения (14) могут быть записаны следующим образом:

$$f_{2l+1} = b\binom{4k+1}{2l+1}a^{4k-2l} = 0,\ l \in \overline{k,2k-1}. \tag{15}$$

Представим число $k = 2^t s$ в виде $k = 2^{t+1}s' + 2^t$, где $s' \geq 1$, и положим $l = 2k - 2^{t+1}$. Тогда

$$4k+1 = 1 + 2^{t+2} + 2^{t+3}s',\ 2l+1 = 1 + 2^{t+3}s',$$

и на основании теоремы Лукаса (см. [14], с. 121) $\binom{4k+1}{2l+1} \equiv 1 (\mathrm{mod}\,2)$, откуда следует, что при указанном значении l коэффициент f_{2l+1} отличен от нуля. Полученное противоречие с равенствами (14) свидетельствует о том, что полином (4) является невырожденным.

Итак, на основании утверждения 2 отображение φ имеет тривиальную линейную структуру, что и требовалось доказать.

В заключение рассмотрим отображение

$$\theta(x) = x^{-1},\ x \in \mathbf{GF}(2^n)\setminus\{0\},\ \theta(0) = 0, \tag{16}$$

широко используемое в конструкциях современных блочных шифров [11, 12].

Утверждение 7. Пусть $n = 2^t$, $t \geq 2$. Тогда отображение (16) имеет тривиальную линейную структуру.

Доказательство. На основании равенства $\theta(x) = \varphi(x^2)$, где $\varphi(x) = x^{2^{n-1}-1}$, $x \in F = \mathbf{GF}(2^n)$, и утверждения 3 достаточно показать, что при указанных значениях n отображение φ имеет тривиальную линейную структуру.

Пусть $a,b \in F\setminus\{0\}$. По теореме Лукаса биномиальные коэффициенты $\binom{2^{n-1}-1}{j}$, $j \in \overline{0,2^{n-1}-1}$, являются нечетными числами. Следовательно,

$$\varphi_{a,b}(x) = b((x+a)^{2^{n-1}-1} + x^{2^{n-1}-1}) = b\sum_{j=0}^{2^{n-1}-2} x^j a^{2^{n-1}-1-j} = u\sum_{j=0}^{2^{n-1}-2} z^j , \qquad (17)$$

где $u = ba^{2^{n-1}-1}$, $z = xa^{-1}$. Из формулы (17) следует, что условие $\mathrm{Tr}(\varphi_{a,b}(x)) \equiv \mathrm{const}$ равносильно условию

$$\mathrm{Tr}(u(z + z^2 + ... + z^{2^{n-1}-2})) = 0 , \; z \in F . \qquad (18)$$

Покажем, что множество

$$H = \{\omega(z) \overset{\text{def}}{=} z + z^2 + ... + z^{2^{n-1}-2} : z \in F\} \qquad (19)$$

содержит некоторый базис поля F над полем $\mathbf{GF}(2)$. Тогда из условия (18) следует, что $\mathrm{Tr}(u\omega) = 0$ для любого $\omega \in F$, то есть (см. теорему 2.24 в [10]) $u = 0$. Однако последнее равенство противоречит выбору элементов a и b, откуда вытекает, что отображение φ имеет тривиальную линейную структуру.

Заметим, что, поскольку n является степенью двойки, то на основании Теоремы 2.39 в [10] элементы $\omega(z), \omega(z)^2, ..., \omega(z)^{2^{n-1}}$ образуют базис поля F при выполнении равенства $\mathrm{Tr}(\omega(z)) = 1$. Таким образом, для завершения доказательства утверждения остается убедиться в том, что множество (19) содержит элемент, след которого равен 1.

Рассмотрим полиномиальное представление отображения $\mathrm{Tr}(\omega(z))$, $z \in F$:

$$\mathrm{Tr}(\omega(z)) = \sum_{i=0}^{n-1}\sum_{j=1}^{2^{n-1}-2} z^{j2^i} = \sum_{l=0}^{2^n-1} A_l z^l , \qquad (20)$$

где на основании тождества $z^{2^n} = z$, $z \in F$, коэффициент A_l равен числу упорядоченных пар (i, j) целых чисел, удовлетворяющих условиям

$$2^i j \equiv l \bmod(2^n - 1), \; i \in \overline{0, n-1}, \; j \in \overline{1, 2^{n-1} - 2} . \qquad (21)$$

Положим $l = 2$ и заметим, что для любого $i \in \overline{0, n-1}$ сравнение $2^i x \equiv 2 \bmod(2^n - 1)$ имеет единственное решение $x(i) \in \overline{0, 2^n - 2}$: $x(0) = 2$, $x(1) = 1$, $x(i) = 2^{n+1-i}$, $i \in \overline{2, n-1}$. При этом $x(i) \in \overline{1, 2^{n-1} - 2}$ для всех значений $i \in \overline{0, n-1}$, за исключением $i = 2$. Отсюда вытекает, что $A_2 = n - 1 \equiv 1 \,(\mathrm{mod}\, 2)$ и, следовательно, полином в правой части равенства (20) задает ненулевое преобразование поля F.

Таким образом, существует элемент $z \in F$, для которого $\mathrm{Tr}(\omega(z)) \neq 0$, что и требовалось доказать.

Изложенные выше результаты позволяют строить разнообразные отображения над конечными полями, имеющие тривиальную линейную структуру. Нахождение необходимых и достаточных условий тривиальности линейной структуры отображений специального вида (в частности, степенных) является задачей дальнейших исследований авторов статьи.

1. *Логачев О.А.* Булевы функции в теории кодирования и криптологии / О.А. Логачев, А.А. Сальников, В.В. Ященко. — М.: МЦНМО, 2004. — 470 с.

2. *Golic J.* On the Resynchronization Attack / J. Golic, G. Morgari // Fast Software Encryption. — FSE'03, Proceedings. — Springer-Verlag, 2003. — P. 100–110.

3. *Ященко В.В.* О критерии распространения для булевых функций и о бент-функциях / В.В. Ященко // Проблемы передачи информации. — 1997. — Т. 33. — Вып 1. — С. 75–86.

4. *Dawson E.* On the Linear Structures of Symmetric Functions / E. Dawson, Ch.-K. Wu // Australian J. of Combinatorics. — 1997. — Vol. 16. — P. 239–243.

5. *Evertse J.-H.* Linear Structures in Blockciphers / J.-H. Evertse // Advances in Cryptology — EUROCRYPT' 87, Proceedings. — Springer Verlag, 1988. — P. 249–266.

6. *Lai X.* Additive and Linear Structures of Cryptographic Functions / X. Lai // Fast Software Encryption. — FSE'94, Proceedings. — Springer-Verlag, 1995. — P. 75–85.

7. *Сачков В.Н.* Трансляторы и трансляции дискретных функций / В.Н. Сачков // Труды по дискретной математике. — М.: Гелиос АРВ, 2006. — Т. 9. — С. 253–268.

8. *Алексейчук А.Н.* Достаточные условия стойкости рандомизированных блочных систем шифрования относительно метода криптоанализа на основе коммутативных диаграмм / А.Н. Алексейчук // Реєстрація, зберігання і оброб. даних. — 2007. — Т. 9, № 2. — С. 61–68.

9. *Алексейчук А.Н.* Критерий примитивности группы подстановок, порожденной раундовыми преобразованиями Rijndael-подобного блочного шифра / А.Н. Алексейчук // Реєстрація, зберігання і оброб. даних. — 2004. — Т. 6, № 2. — С. 11–18.

10. *Лидл Р.* Конечные поля: В 2 т. / Р. Лидл, Г. Нидеррайтер; пер. с англ. — М.: Мир, 1988. — 818 с.

11. *Daemen J.* AES Proposal: Rijndael [Електронний ресурс] / J. Daemen, D. Rijmen: htpp://csrc.nist.gov/encription/aes/ rijndael/Rijndael.pdf.

12. Camellia: a 128-bit Block Cipher Suitable for Multiple Platforms — Design and Analysis / A. Aoki, T. Ichikawa, M. Kanda [at al.] // Selected Areas in Cryptography. — SAC 2001, Proceedings. — Springer Verlag, 2001. — P. 39–56.

13. *Chabaud F.* Links Between Differential and Linear Cryptanalysis / F. Chabaud, S. Vaudenay // Advances in Cryptology — EUROCRYPT' 94, Proceedings. — Springer Verlag, 1995. — P. 356–365.

14. *Берлекэмп Э.* Алгебраическая теория кодирования / Э. Берлекэмп; пер. с англ. — М.: Мир, 1971. — 477 с.

Поступила в редакцию 26.03.2008