УДК 621.391:519.2

Алексейчук А. Н., Игнатенко С.М.

НИЖНЯЯ ГРАНИЦА ВЕРОЯТНОСТИ ВОССТАНОВЛЕНИЯ ИСТИННОГО РЕШЕНИЯ СИСТЕМЫ ЛИНЕЙНЫХ УРАВНЕНИЙ С ИСКАЖЕННОЙ ПРАВОЙ ЧАСТЬЮ НАД КОЛЬЦОМ ВЫЧЕТОВ ПО МОДУЛЮ 2^N

Системы уравнений (СУ) с искаженной правой частью (относительно неизвестных, принимающих значения в некотором конечном множестве) являются классическим объектом исследования в современной криптографии [1, 2]. Как правило, такие системы уравнений используются при построении статистических или корреляционных методов криптоанализа симметричных криптосистем (генераторов псевдослучайных последовательностей, блочных шифров; см., например, [3 – 5]). Основной задачей исследования указанных систем уравнений является разработка эффективных, с точки зрения надежности и трудоемкости, алгоритмов восстановления истинного решения системы.

Наиболее изученный класс СУ с искаженной правой частью образуют булевы системы уравнений, обзор известных алгоритмов решения которых приведен в [6]. В посление годы, в связи с развитием методов синтеза и расширением сферы применения недвоичных программно-ориентированных поточных шифров, наблюдается повышенный интерес специалистов к системам уравнений с искаженной правой частью над конечными кольцами (полями) мощности $q>2$. Необходимость исследования таких систем уравнений продиктована современными задачами криптоанализа и алгебраической теории кодирования, о чем свидетельствуют, например, работы [4, 5, 7].

Универсальным методом решения СУ с искаженной правой частью является хорошо известный в теории статистических решений и ее приложениях метод максимума правдоподобия (ММП) [8]. В случае, когда истинное решение СУ выбирается случайно и равновероятно из некоторого конечного множества, ММП является оптимальной статистической процедурой восстановления этого решения. Нахождение аналитических оценок надежности метода максимума правдоподобия (то есть вероятности правильного восстановления истинного решения СУ указанным методом) относится к числу важнейших задач анализа систем уравнений с искаженной правой частью [1].

В [1] получены аналитические границы надежности ММП для случая булевой СУ соответственно со случайной равновероятной и фиксированной левой частью. Системы линейных уравнений (СЛУ) с искаженной правой частью над кольцом вычетов по модулю 2^N исследовались в [9 – 11]. В частности, в [10] получена нижняя оценка вероятности восстановления истинного решения СЛУ с искаженной правой частью и фиксированной матрицей коэффициентов над кольцом $\mathbf{Z}/(2^N)$, обобщающая аналогичную оценку, приведенную в [1]. Метод построения подобных оценок обобщен и развит в [12] при анализе эффективности статистических процедур нахождения начального состояния конечного автомата по известному входу и выходу, полученному при случайном искажении функции переходов автомата.

Перечисленные выше результаты не дают ответ на вопрос о том, как оценить вероятность восстановления истинного решения СЛУ с искаженной правой частью над произвольным конечным кольцом, матрица коэффициентов которой выбирается случайно и равновероятно из множества всех матриц заданного размера.

В настоящей статье получена нижняя граница надежности метода максимума правдоподобия решения СЛУ с искаженной правой частью и случайной равновероятной матрицей коэффициентов над кольцом вычетов по модулю 2^N. (Отметим, что ограничение, связанное с выбором кольца, не является существенным, и основные результаты статьи почти дословно переносятся на системы линейных уравнений с искаженной правой частью над произвольным конечным кольцом). Показано, что при определенных условиях оценка

истинного решения рассматриваемой СЛУ методом максимума правдоподобия является асимптотически состоятельной, если распределение искажений в правой части системы уравнений отлично от равномерного распределения вероятностей.

Установлена также приближенная нижняя граница надежности ММП, основанная на нормальной аппроксимации распределения вероятностей суммы независимых одинаково распределенных случайных величин. Изложены результаты экспериментального исследования надежности ММП для различных СЛУ с искаженной правой частью над кольцом $\mathbf{Z}/(32)$, показывающие, что последняя граница является достаточно точным приближением надежности метода максимума правдоподобия.

Перейдем к подробному изложению полученных результатов.

Рассмотрим систему линейных уравнений

$$Ax = b = Ax_0 + \varepsilon^{(t)} \tag{1}$$

над кольцом $R = \mathbf{Z}/(2^N)$, где A – матрица размера $t \times n$ с элементами из R, $x_0 \in R^{(n)}$, $\varepsilon^{(t)} = (\varepsilon_1, \ldots, \varepsilon_t) \in R^{(t)}$. Предположим, что A, x_0 и $\varepsilon^{(t)}$ являются независимыми случайными элементами, причем A имеет равномерное распределение вероятностей на множестве всех $(t \times n)$-матриц над кольцом R, вектор x_0 равномерно распределен на множестве $R^{(n)}$, а координаты вектора $\varepsilon^{(t)}$ являются независимыми случайными величинами, распределенными по закону

$$\mathbf{P}(\varepsilon_i = a) = p(a),\ a \in R,\ i \in \overline{1,t}. \tag{2}$$

Ниже символом $\mathbf{P}$ обозначается совместное распределение вероятностей на множестве всех упорядоченных наборов $(A, x_0, \varepsilon^{(t)})$,

$$\mathbf{P}(A, x_0, \varepsilon^{(t)}) = |R|^{-nt} |R|^{-n}\ p(\varepsilon^{(t)}),$$

а символом $\mathbf{P}_z$ – условное распределение $\mathbf{P}$ при условии $\{x_0 = z\}$, $z \in R^{(n)}$.

Положим $p_M = \max\limits_{a \in R} p(a)$, $p_m = \min\limits_{a \in R} p(a)$. Предположим, что выполняется условие

$$p_M > p_m > 0. \tag{3}$$

Для любого $x \in R^{(n)}$ обозначим

$$\varepsilon(x) = b - Ax,\ \ \lambda(x) = \sum_{a \in R} n(a \mid \varepsilon(x)) \log \frac{p_M}{p(a)},$$

где $n(a \mid \varepsilon(x))$ – частота встречаемости элемента $a \in R$ в векторе $\varepsilon(x)$.

Введем ряд дополнительных обозначений. Обозначим

$$D(\bar{q}_1 \,\|\, \bar{q}_2) = \sum_{a \in R} q_1(a) \log \frac{q_1(a)}{q_2(a)}$$

информационную дивергенцию между произвольными распределениями вероятностей $\bar{q}_1 = (q_1(a) : a \in R)$ и $\bar{q}_2 = (q_2(a) : a \in R)$ на множестве R, где $q_2(a) > 0$ для любого $a \in R$ [13]. Символом $\bar{\omega} = (|R|^{-1} : a \in R)$ обозначим равномерное распределение на R, а символом $\bar{p} = (p(a) : a \in R)$ – распределение вероятностей вида (2).

Известно [10], что восстановление истинного решения x_0 СЛУ (1) методом максимума правдоподобия равносильно нахождению вектора $x^* = x^*(b)$, удовлетворяющего условию

$$\lambda(x^*) = \min_{x \in R} \lambda(x). \tag{4}$$

Надежность ММП определяется по формуле

$$\pi_{n,t} = \mathbf{P}\{x^* = x_0\} = |R|^{-n} \sum_{z \in R^{(n)}} \mathbf{P}_z\{x^* = z\},$$

а средняя вероятность ошибки – по формуле

$$1-\pi_{n,t} = |R|^{-n} \sum_{z\in R^{(n)}} \mathbf{P}_z\{x^* \neq z\}. \tag{5}$$

Ниже для построения верхней границы параметра (5) используется следующий результат (см. [14]; [15], стр. 93).

Лемма. Пусть $\xi_1, \ldots, \xi_t$ – независимые случайные величины такие, что $\alpha_i \le \xi_i \le \beta_i$, где $\alpha_i, \beta_i \in \mathbf{R}$, $i \in \overline{1,t}$. Тогда для любого $u > 0$

$$\mathbf{P}\{\sum_{i=1}^{t}(\xi_i - E\xi_i) \ge tu\} \le \exp\left\{-\frac{2t^2u^2}{\sum_{i=1}^{t}(\beta_i-\alpha_i)^2}\right\}. \tag{6}$$

Основным результатом статьи является следующая теорема, устанавливающая при указанных выше предположениях нижнюю границу вероятности правильного восстановления истинного решения СЛУ (1) методом максимума правдоподобия.

Теорема. При выполнении условий (2), (3) для любых натуральных n, t справедливо неравенство

$$\pi_{n,t} \ge 1-|R|^n \exp\left\{-\frac{2tD^2}{(\log p_M - \log p_m)^2}\right\}, \tag{7}$$

где $D = \min\{D(\bar{p}\,\|\,\bar{\omega}), D(\bar{\omega}\,\|\,\bar{p})\}$.

Доказательство. Зафиксируем вектор $z \in R^{(n)}$ и оценим сверху вероятность $\mathbf{P}_z\{x^* \neq z\}$. На основании равенства (4) для любого $c \in \mathbf{R}$ справедливо включение

$$\{x^* \neq z\} \subseteq \{\lambda(z) > c\} \cup \left(\bigcup_{x\neq z}\{\lambda(x) \le c\}\right),$$

из которого следует, что

$$\mathbf{P}_z\{x^* \neq z\} \le \mathbf{P}_z\{\lambda(z) > c\} + (|R|^n - 1)\max_{x\neq z}\mathbf{P}_z\{\lambda(x) \le c\}, \quad c \in \mathbf{R}. \tag{8}$$

Пусть выполняется равенство $x_0 = z$. Тогда для любого $x \in R^{(n)}$

$$\lambda(x) = \sum_{a\in R} n(a \mid A(z-x)+\varepsilon^{(t)}) \log\frac{p_M}{p(a)}. \tag{9}$$

При этом случайный вектор $A(z - x) + \varepsilon^{(t)}$ имеет равномерное распределение вероятностей на множестве $R^{(t)}$, если $x \neq z$, и совпадает с вектором $\varepsilon^{(t)}$ при $x = z$.

Для любых $x \in R^{(n)}$, $a \in R$, $i \in \overline{1,t}$ введем случайную величину $\xi_{i,a}(x)$, принимающую значение 1, если i-я координата случайного вектора $A(z - x) + \varepsilon^{(t)}$ равна a, и значение 0 – в противном случае. Согласно равенству (9),

$$\lambda(x) = \sum_{i=1}^{t}\eta_i(x), \tag{10}$$

где

$$\eta_i(x) = \sum_{a\in R}\xi_{i,a}(x)\log\frac{p_M}{p(a)}, \quad i \in \overline{1,t}. \tag{11}$$

Отметим, что для любого $x \in R^{(n)}$ случайные величины (11) независимы в совокупности и одинаково распределены.

Найдем математическое ожидание $\mathbf{E}_z\eta_i(x)$ случайной величины $\eta_i(x)$ относительно распределения $\mathbf{P}_z$ (то есть при условии $x_0 = z$), $x \in R^{(n)}$. Если $x = z$, то в силу равенства (11)

$$\mathbf{E}_z\eta_i(z) = \sum_{a\in R}\mathbf{E}_z\xi_{i,a}(z)\log\frac{p_M}{p(a)} = \sum_{a\in R}\mathbf{P}_z\{\varepsilon_i = a\}\log\frac{p_M}{p(a)} =$$

$$= \sum_{a\in R}p(a)\log\frac{p_M}{p(a)} = \log\left(\frac{p_M}{|R|^{-1}}\right) - D(\overline{p}\,\|\,\overline{\omega}).$$

С другой стороны, при $x \neq z$

$$\mathbf{E}_z\eta_i(x) = \sum_{a\in R}|R|^{-1}\log\frac{p_M}{p(a)} = \log p_M - |R|^{-1}\sum_{a\in R}\log p(a) = \log\left(\frac{p_M}{|R|^{-1}}\right) + D(\overline{\omega}\,\|\,\overline{p}).$$

Таким образом, принимая во внимание формулу (10), получим, что

$$\mathbf{E}_z\lambda(z) = t\log\left(\frac{p_M}{|R|^{-1}}\right) - tD(\overline{p}\,\|\,\overline{\omega}), \tag{12}$$

$$\mathbf{E}_z\lambda(x) = t\log\left(\frac{p_M}{|R|^{-1}}\right) + tD(\overline{\omega}\,\|\,\overline{p}), \quad x \neq z. \tag{13}$$

Положим в формуле (8) $c = t\log\left(\frac{p_M}{|R|^{-1}}\right)$. Тогда на основании соотношений (12), (13) получим следующие равенства:

$$\mathbf{P}_z\{\lambda(z) > c\} = \mathbf{P}_z\{\lambda(z) - \mathbf{E}_z\lambda(z) > c - \mathbf{E}_z\lambda(z)\} = \mathbf{P}_z\{\lambda(z) - \mathbf{E}_z\lambda(z) > tD(\overline{p}\,\|\,\overline{\omega})\}, \tag{14}$$

$$\mathbf{P}_z\{\lambda(x) \le c\} = \mathbf{P}_z\{-\lambda(x) + \mathbf{E}_z\lambda(x) \ge -c + \mathbf{E}_z\lambda(x)\} = \mathbf{P}_z\{-\lambda(x) + \mathbf{E}_z\lambda(x) \ge tD(\overline{\omega}\,\|\,\overline{p})\}. \tag{15}$$

Для оценки выражения в правой части равенства (14) применим лемму к случайным величинам $\xi_i = \eta_i(z)$, $i \in \overline{1,t}$. Заметим, что, согласно равенству (11), $0 \le \eta_i(z) \le \log\frac{p_M}{p_m}$, $i \in \overline{1,t}$, и, следовательно, на основании формул (6) и (14)

$$\mathbf{P}_z\{\lambda(z) > c\} \le \exp\left\{-\frac{2t(D(\overline{p}\,\|\,\overline{\omega}))^2}{(\log p_M - \log p_m)^2}\right\}. \tag{16}$$

Аналогично, для оценки сверху выражения в правой части равенства (15) применим лемму к случайным величинам $\xi_i = -\eta_i(x)$, $i \in \overline{1,t}$. Поскольку $-\log\frac{p_M}{p_m} \le -\eta_i(x) \le 0$, $i \in \overline{1,t}$, то, согласно формулам (6) и (15), получим

$$\mathbf{P}_z\{\lambda(x) \le c\} \le \exp\left\{-\frac{2t(D(\overline{\omega}\,\|\,\overline{p}))^2}{(\log p_M - \log p_m)^2}\right\}. \tag{17}$$

Итак, на основании соотношений (5), (8), (16) и (17) справедливы неравенства

$$1 - \pi_{n,t} \le \exp\left\{-\frac{2t(D(\overline{p}\,\|\,\overline{\omega}))^2}{(\log p_M - \log p_m)^2}\right\} + (|R|^n - 1)\exp\left\{-\frac{2t(D(\overline{\omega}\,\|\,\overline{p}))^2}{(\log p_M - \log p_m)^2}\right\} \le \le |R|^n\exp\left\{-\frac{2tD^2}{(\log p_M - \log p_m)^2}\right\}.$$

Тем самым теорема доказана.

Непосредственно из формулы (7) вытекает следующее утверждение.

Следствие 1. Пусть при выполнении условий (2), (3) параметры t и $n = n(t)$ изменяются так, что

$$\frac{t}{n} \ge N\left(\frac{2D^2}{(\log p_M - \log p_m)^2} - \theta\right)^{-1}, \quad \theta = \text{const}, \quad 0 < \theta < \frac{2D^2}{(\log p_M - \log p_m)^2}.$$

Тогда оценка x^* истинного решения СЛУ (1), полученная методом максимума правдоподобия, является асимптотически состоятельной: $\lim\limits_{t\to\infty}\pi_{n,t}=1$.

Заметим, что, несколько огрубляя оценку (7), можно получить более удобную для вычисления нижнюю границу вероятности правильного восстановления истинного решения СЛУ (1) методом максимума правдоподобия.

Следствие 2. Обозначим $d(\overline{p})=\sum\limits_{a\in R}|\,p(a)-|\,R\,|^{-1}|$ расстояние по вариации между распределениями вероятностей $\overline{p}$ и $\overline{\omega}$ на множестве R [13]. Тогда при выполнении условий (2), (3) справедливо неравенство

$$\pi_{n,t}\ge 1-|\,R\,|^{n}\exp\left\{-\frac{tp_m^2(d(\overline{p}))^2}{2}\right\}. \tag{18}$$

Доказательство. Прежде всего, заметим, что

$$D\ge\frac{1}{2\ln 2}(d(\overline{p}))^2 \tag{19}$$

(см. [13], стр. 61). Далее, в силу определения параметра $d(\overline{p})$ справедливо неравенство

$$d(\overline{p})\ge(p_M-|\,R\,|^{-1})+|\,p_m-|\,R\,|^{-1}|=p_M-p_m. \tag{20}$$

Наконец, поскольку $\ln(1+x)<x$ для любого $x>0$, то

$$\log p_M-\log p_m=\log\left(1+\frac{p_M-p_m}{p_m}\right)<\frac{p_M-p_m}{p_m\ln 2}. \tag{21}$$

Непосредственно из формул (7) и (19) – (21) следует неравенство (18).

Следствие доказано.

Покажем теперь, что, исходя из формулы (8), можно получить приближенную оценку параметра $\pi_{n,t}$, основанную на нормальной аппроксимацию вероятностей в левых частях неравенств (16), (17).

Обозначим $D_x=\mathbf{D}_z\eta_i(x)$ дисперсию случайной величины $\eta_i(x)$ относительно распределения $\mathbf{P}_z$, $x,z\in R^{(n)}$, $i\in\overline{1,t}$. На основании формул (11) – (13) справедливы равенства

$$D_z=\sum_{a\in R}p(a)\left(\log\frac{p_M}{p(a)}\right)^2-\left(\sum_{a\in R}p(a)\log\frac{p_M}{p(a)}\right)^2, \tag{22}$$

$$D_x=\sum_{a\in R}|\,R\,|^{-1}\left(\log\frac{p_M}{p(a)}\right)^2-\left(\sum_{a\in R}|\,R\,|^{-1}\log\frac{p_M}{p(a)}\right)^2,\ x\ne z. \tag{23}$$

Следствие 3. Пусть $\alpha,\beta>0$,

$$t=\left(\frac{u_\alpha\sqrt{D_z}+u_\beta\sqrt{D_x}}{D(\overline{p}\,\|\,\overline{\omega})+D(\overline{\omega}\,\|\,\overline{p})}\right)^2, \tag{24}$$

где u_α, u_β – квантили нормального распределения, определяемые с помощью соотношений

$$\alpha=1-\Phi(u_\alpha),\ \beta=\Phi(-u_\beta),\ \Phi(u)=\frac{1}{\sqrt{2\pi}}\int_{-\infty}^{u}e^{-\frac{t^2}{2}}dt,\ u\in\mathbf{R}. \tag{25}$$

Тогда при выполнении условий (2), (3) для надежности ММП справедлива приближенная оценка

$$\pi_{n,t}\ge 1-(\alpha+(|\,R\,|^{n}-1)\beta). \tag{26}$$

Доказательство. Положим в формуле (8)

$$c = t\mathrm{E}_z\eta_1(z) + u_\alpha\sqrt{tD_z}\,. \qquad (27)$$

На основании равенства (24) и соотношений

$$\mathbf{E}_z\eta_1(z) = \log\left(\frac{p_M}{|R|^{-1}}\right) - D(\bar{p}\,\|\,\bar{\omega}),\ \mathbf{E}_z\eta_1(x) = \log\left(\frac{p_M}{|R|^{-1}}\right) + D(\bar{\omega}\,\|\,\bar{p}),\ x \neq z,$$

получим, что

$$c = t\mathrm{E}_z\eta_1(x) - u_\beta\sqrt{tD_x}\,. \qquad (28)$$

Заметим теперь, что, поскольку слагаемые в формуле (10) являются независимыми одинаково распределенными случайными величинами, то на основании центральной предельной теоремы и формул (25), (27), (28) справедливы следующие (приближенные) равенства:

$$\mathbf{P}_z\{\lambda(z) > c\} = \mathbf{P}_z\{\frac{\lambda(z) - t\mathbf{E}_z\eta_1(z)}{\sqrt{tD_z}} > \frac{c - t\mathbf{E}_z\eta_1(z)}{\sqrt{tD_z}}\} = 1 - \Phi(u_\alpha) = \alpha, \qquad (29)$$

$$\mathbf{P}_z\{\lambda(x) \le c\} = \mathbf{P}_z\{\frac{\lambda(x) - t\mathbf{E}_z\eta_1(x)}{\sqrt{tD_x}} \le \frac{c - t\mathbf{E}_z\eta_1(x)}{\sqrt{tD_x}}\} = \Phi(-u_\beta) = \beta. \qquad (30)$$

Подставляя выражения (29), (30) в формулу (8), получим неравенство (26).

Следствие доказано.

Ниже, в табл. 1, приведены, полученные с использованием ЭВМ, статистические оценки надежности решения различных СЛУ вида (1) с $n = 3$ неизвестными над кольцом $\mathbf{Z}/(32)$. Для каждого значения t, указанного в таблице, составлялись и решались методом максимума правдоподобия 100 систем линейных уравнений с искаженной правой частью. Надежность ММП оценивалась как отношение числа правильно решенных СЛУ к общему их числу.

Таблица 1.

Зависимость надежности ММП от числа уравнений и распределения вероятностей искажений в правой части СЛУ (1)

	text1	text2	text3	text4	text5
$t = 10$	0,00	0,00	0,03	0,22	0,47
$t = 30$	0,00	0,00	0,66	0,86	1
$t = 50$	0,00	0,00	0,97	1	1
$t = 100$	0,01	0,02	1	1	1
$t = 150$	0,07	0,14	1	1	1
$t = 200$	0,16	0,24	1	1	1
$t = 250$	0,22	0,30	1	1	1
$t = 300$	0,34	0,44	1	1	1
$t = 350$	0,43	0,55	1	1	1
$t = 400$	0,58	0,68	1	1	1
$t = 450$	0,64	0,70	1	1	1
$t = 500$	0,70	0,77	1	1	1
$t = 550$	0,75	0,86	1	1	1
$t = 600$	0,88	1	1	1	1
$t = 650$	0,95	1	1	1	1
$t = 700$	1	1	1	1	1

Для формирования истинных решений и матриц коэффициентов указанных СЛУ использовался линейный конгруэнтный генератор, а для внесения искажений в их правые части – выбранные с шагом 10 символы пяти текстов, статистические характеристики которых приведены в табл. 2. Среди них text3, text4 и text5 являются осмысленными текстами на русском и английском языках, а text1 и text2 получены в результате посимвольного сложения по модулю 32 двух других (различным образом закодированных) осмысленных текстов.

Таблица 2.
Статистические характеристики используемых текстов

	text1	text2	text3	text4	text5
$d(\overline{p})$	0,156907	0,185852	0,722783	0,797595	0,878946
p_m	0,019670	0,019315	0,001020	0,000903	0,000789
p_M	0,043325	0,044813	0,098578	0,233062	0,362668
D	0,027279	0,033987	0,529636	0,815186	1,050974

Как видно из табл. 1, надежность метода максимума правдоподобия достаточно быстро стремится к 1 с ростом числа уравнений системы. При фиксированном числе уравнений надежность возрастает с увеличением значений параметра $D = \min\{D(\overline{p} \,\|\, \overline{\omega}), D(\overline{\omega} \,\|\, \overline{p})\}$, характеризующего статистическую различимость между распределением вероятностей искажений и равномерным распределением.

В табл. 3 приведены верхние оценки t_1 и t_2 наименьшего числа уравнений системы (1) ($n = 3$, $R = \mathbf{Z}/(32)$), достаточного для восстановления ее истинного решения с заданной надежностью $\pi_{3,t}$. Значения t_1 и t_2 расчитаны соответственно по формулам (7) и (24) (при $\alpha = 0{,}05$).

Сравним данные табл. 3 с результатами экспериментальных исследований (см. табл. 1). Пусть, например, $\pi_{3,t} = 0{,}7$ и в качестве вектора искажений в правой части СЛУ (1) используется text1. В этом случае $t_1 = 10120$, $t_2 = 944$. Вместе с тем, на практике указанное значение надежности ММП достигается уже для систем из 500 линейных уравнений, правые части которых искажены символами text1, а при наличии 700 уравнений все такие СЛУ решаются правильно.

Таблица 3.
Оценки наименьшего числа уравнений, достаточного для решения СЛУ (1) с заданной надежностью

	text1		text2		text3		text4		text5	
$\pi_{3,t}$	t_1	t_2	t_1	t_2	t_1	t_2	t_1	t_2	t_1	t_2
0,1	9158	858	6704	687	814	44	507	30	372	19
0,2	9261	867	6779	694	823	45	513	31	376	20
0,3	9377	877	6864	702	833	45	519	31	381	20
0,4	9512	889	6963	711	845	46	527	31	386	21
0,5	9671	903	7079	723	860	47	536	32	393	21
0,6	9865	921	7221	737	877	48	546	33	401	21
0,7	10120	944	7405	756	899	49	560	34	411	22
0,8	10471	980	7664	784	931	51	580	35	425	23
0,9	11075	1056	8106	845	984	55	613	38	449	24
0,94	11520	1168	8432	934	1024	62	638	42	468	27

Как видно из табл. 1 и табл. 3, значение t_2, расчитанное по формуле (24), является достаточно точной оценкой наименьшего числа уравнений СЛУ (1), при котором достигается

заданная надежность ее решения методом максимума правдоподобия. При этом абсолютная погрешность данной оценки уменьшается с ростом параметра D.

Так, например, для вектора искажений text4 и надежности $\pi_{3,t} = 0{,}2$ число уравнений СЛУ оценивается значением $t_2 = 31$. На практике для правильного решения 22 из 100 подобных СЛУ достаточно 10 уравнений. Если в качестве вектора искажений используется text5, то надежность $\pi_{3,t} = 0{,}94$ достигается при $t_2 = 27$ уравнениях в системе. На практике оказывается достаточно 30 уравнений для правильного решения всех 100 аналогичных СЛУ.

Отметим также, что, согласно данным табл. 1 и табл. 3, оценка t_1, полученная на основе неравенства (7), является завышеной примерно в 20 раз по сравнению с фактическим количеством уравнений, соответствующим заданной надежности. Однако, в отличие от формулы (24), неравенство (7) устанавливает явную аналитическую зависимость нижней границы надежности ММП от конкретных параметров СЛУ с искаженной правой частью над кольцом вычетов по модулю 2^N.

Список литературы

1. *Балакин Г.В.* Введение в теорию случайных систем уравнений // Труды по дискретной математике. – М.: ТВП. – 1997. – Т. 1. – С. 1 – 18.
2. *Бабаш А.В., Шанкин Г.П.* Криптография. – М.: Солон-Р, 2002. – 511с.
3. *Смирнов В.Г.* Системы булевых уравнений рекуррентного типа // Обозрение прикл. промышл. матем. – 1995. – Т. 2. – Вып. 3. – С. 477 – 482.
4. *Golic J. Dj., Morgari G.* Vectorial fast correlation attaks // http://eprint.iacr.org/ 2004/247.
5. *Baigneres T., Junod P., Vaudenay S.* How far we go beyond linear criptanalysis? // Advances in Cryptology – ASIACRYPT'04, Proceedings. – Springer Verlag, 2004. – P. 432 – 450.
6. *Левитская А.А.* Системы случайных уравнений над конечными алгебраическими структурами // Кибернетика и системный анализ. – 2005. – Т. 41. – № 1. – С. 82 – 116.
7. *Babu N.S., Zimmermann K.-H.* Decoding of linear codes over Galois ring // IEEE Trans. on Inform. Theory. – 2001. – Vol. 47. – № 4. – P. 1599 – 1603.
8. *Леман Э.* Проверка статистических гипотез: Пер. с англ. – М.: Наука, 1964. – 498 с.
9. *Алексейчук А.Н.* Системы линейных уравнений с искаженной правой частью над кольцом вычетов по модулю 2^N // Захист інформації. – 2001. – № 4. – С. 12 – 19.
10. *Алексейчук А.Н., Игнатенко С.М.* Оценки эффективности универсальных методов восстановления искаженных линейных рекуррент над кольцом вычетов по модулю 2^N // Збірник наукових праць ІПМЕ НАН України – Вып. 20. – Киев, 2003. – С. 40 – 48.
11. *Алексейчук А.Н., Игнатенко С.М.* Метод оптимизации алгоритмов решения систем линейных уравнений с искаженной правой частью над кольцом вычетов по модулю 2^N // Реєстрація, зберігання і обробка даних. – 2005. – Т. 7. – № 1. – С. 21 – 29.
12. *Бабаш А.В.* Приближенные модели конечных автоматов // Обозрение прикл. промышл. матем. – 2005. – Т. 12. – Вып. 2. – С. 209 – 247.
13. *Чисар И., Кернер Я.* Теория информации. Теоремы кодирования для дискретных систем без памяти: Пер. с англ. – М.: Мир, 1985. – 397 с.
14. *Hoeffding W.* Probability inequalities for sums of bounded random variables // J. Amer. Statist. Assoc. – 1963. – Vol. 58. – № 301. – P. 13 – 30.
15. *Петров В.В.* Предельные теоремы для сумм независимых случайных величин. – М.: Наука, 1987. – 320 с.

Поступила 04.09.2006