УДК 621.391: 519.2

А. Н. Алексейчук[1], **С. М. Игнатенко**[2]
[1]Специальный факультет СБ Украины в составе Военного института телекоммуникаций и информатизации НТУУ «КПИ»
[2]В/ч А 1906

Метод оптимизации алгоритмов решения систем линейных уравнений с искаженной правой частью над кольцом вычетов по модулю 2^N

Предложен метод построения новых алгоритмов решения систем линейных уравнений с искаженной правой частью над кольцом вычетов по модулю 2^N по произвольной конечной совокупности исходных таких алгоритмов. Показано, что в ряде случаев предложенный метод позволяет существенно повысить эффективность известных алгоритмов решения указанных систем уравнений.

Ключевые слова: *корреляционный криптоанализ, система линейных уравнений с искаженной правой частью, оптимизация вычислительных алгоритмов.*

Введение

Одной из актуальных задач современного криптоанализа является разработка эффективных, с точки зрения надежности и трудоемкости, методов решения систем линейных уравнений (СЛУ) с искаженной правой частью над конечными коммутативными кольцами по аналогии с известными методами решения таких СЛУ над полем из двух элементов [1–3]. К разработке и анализу алгоритмов решения систем линейных уравнений с искаженной правой частью приводят задачи корреляционного криптоанализа поточных шифров, декодирования блоковых кодов, восстановления искаженных линейных рекуррентных последовательностей и ряд других [1, 4–8].

В настоящее время известны два универсальных метода решения СЛУ с искаженной правой частью над кольцом $R_N = \boldsymbol{Z}/(2^N)$: метод максимума правдоподобия (ММП) [1, 9] и метод последовательного решения N вспомогательных булевых СЛУ с искаженными правыми частями и одинаковыми матрицами коэффициентов [10]. В [11, 12] показано, что при выполнении определенных условий трудоемкость ММП можно уменьшить, заменяя процедуру вычисления, так называемых векторов ошибок, вычислением (с использованием «быстрых» алгоритмов [13]) комплексного преобразования Фурье или, соответственно, числового преоб-

разования Ферма некоторых вспомогательных функций, заданных на множестве $R_N^{(n)}$, где n — число неизвестных исходной СЛУ. На практике применение ММП или указанных его модификаций становится невозможным уже при умеренных значениях n или N в силу большой временной или емкостной сложности соответствующих алгоритмов решения СЛУ. С другой стороны, метод последовательного решения булевых СЛУ с искаженными правыми частями [10] часто не позволяет восстанавливать истинное решение системы уравнений с требуемой (высокой) надежностью.

В настоящей статье предлагается метод построения новых алгоритмов решения СЛУ с искаженной правой частью над кольцом R_N по произвольной конечной совокупности исходных таких алгоритмов. Метод основывается на идее последовательного решения статистических задач, примененной к решению булевых систем уравнений с мешающими параметрами Г.В. Балакиным и Ю.Б. Никольским [2], а также формальном подходе к построению оптимальных по трудоемкости вычислительных алгоритмов, предложенном М.В. Гаврилкевичем и В.И. Солодовниковым [14]. Установлены аналитические выражения оценок надежности и временной сложности, получаемых по предложенному методу алгоритмов решения СЛУ с искаженной правой частью через соответствующие характеристики исходных алгоритмов. Описана процедура построения оптимальных (в определенном классе) алгоритмов решения СЛУ с искаженной правой частью над кольцом R_N.

При $N = 5$ проведено экспериментальное исследование эффективности алгоритмов, получаемых из исходных алгоритмов решения СЛУ с искаженными правыми частями (над различными кольцами вычетов) по методу максимума правдоподобия. Полученные результаты свидетельствуют о том, что в большинстве случаев новые алгоритмы являются более эффективными по сравнению с ранее известными алгоритмами решения СЛУ с искаженной правой частью над кольцом R_N [1, 9–12].

Определения основных понятий

Для заданных натуральных t и n обозначим $(R_N)_{t\times n}$ кольцо матриц размера $t \times n$ над кольцом R_N. Символом P_N обозначим совокупность всех распределений вероятностей (РВ) на R_N. Каждое РВ $p_N \in P_N$ представляет собой стохастический вектор длины 2^N с координатами $p_N(a)$, где $a \in R_N$.

Система линейных уравнений с искаженной правой частью над кольцом R_N определяется как упорядоченный набор $(A,\ x_0,\ b,\ p_N)$, где $A \in (R_N)_{t\times n}$, $x_0 \in R_N^{(n)}$ — неизвестный вектор длины n над кольцом R_N, $p_N \in P_N$, $b = Ax_0 + \varepsilon$, ε — случайный вектор с независимыми в совокупности координатами, распределенными на множестве R_N по закону p_N [1, 9].

Под алгоритмом решения СЛУ с искаженной правой частью над кольцом R_N будем понимать произвольную частичную вычислимую функцию $\wp$, заданную на некотором подмножестве множества всех упорядоченных наборов $(A,\ b,\ p_N)$, та-

ких, что $A \in (R_N)_{t\times n}$, $p_N \in P_N$, $b = Ax_0 + \varepsilon$, и ставящую в соответствие каждому указанному набору некоторый вектор $x_0{}^* \in R_N{}^{(n)}$ — оценку истинного решения x_0 СЛУ:

$$Ax = b = Ax_0 + \varepsilon . \tag{1}$$

Запись $x_0{}^* = \wp(A,b,p_N)$ означает, что вектор $x_0{}^*$ есть результат применения алгоритма $\wp$ к входным данным $(A,b,p_N) \in D_\wp$, где $D_\wp$ — область определения функции $\wp$.

Обозначим Λ_N класс всех алгоритмов решения систем линейных уравнений с искаженной правой частью над кольцом R_N. Символами

$$\pi_\wp = \pi_\wp(A, x_0, p_N), \quad T_\wp = T_\wp(N, n, t, p_N)$$

будем обозначать соответственно функции надежности и трудоемкости алгоритма $\wp \in \Lambda_N$.

Надежность алгоритма $\wp$ определяется по формуле:

$$\pi_\wp = \Pr\{\wp(A, b, p_N) = x_0\}, \tag{2}$$

где вероятность в правой части равенства (2) определяется относительно закона распределения p_N координат случайного вектора ε. Отметим, что заданная таким образом надежность зависит от матрицы $A \in (R_N)_{t\times n}$ и вектора $x_0 \in R_N{}^{(n)}$. Можно определить среднюю надежность $\overline{\pi_\wp}$ алгоритма $\wp$, положив

$$\overline{\pi_\wp} = 2^{-Ntn} \sum_{A\in(R_N)_{t\times n}} \Pr\{\wp(A,b,p_N) = x_0\}.$$

Наконец, можно усреднить значения (2) по всем $A \in (R_N)_{t\times n}$, $x_0 \in R_N{}^{(n)}$ и получить таким образом среднюю надежность алгоритма $\wp$ решения СЛУ (1), которая формируется путем случайного равновероятного, не зависящего от вектора ε выбора истинного решения и матрицы коэффициентов.

Трудоемкость $T_\wp$ алгоритма $\wp \in \Lambda_N$ определим как битовую временную сложность (в худшем случае, при равномерном весовом критерии) этого алгоритма, рассматривая в качестве модели вычислительного устройства, на котором реализуются алгоритмы, равнодоступную адресную машину [15].

Метод построения новых алгоритмов решения систем линейных уравнений с искаженной правой частью над кольцом R_N

Пусть заданы произвольные натуральные числа N_1, N_2. Положим $N = N_1 + N_2$ и определим отображение

$$\theta_{N_1,N_2} : \Lambda_{N_1} \times \Lambda_{N_2} \to \Lambda_N, \tag{3}$$

ставящее в соответствие каждой упорядоченной паре $(\wp_1, \wp_2)$ алгоритмов решения систем линейных уравнений с искаженными правыми частями над кольцами R_{N_1}, R_{N_2} соответственно новый алгоритм:

$$\wp = \theta_{N_1,N_2}(\wp_1, \wp_2), \quad \wp \in \Lambda_N. \tag{4}$$

Дадим точное определение алгоритма (4). Предварительно введем ряд обозначений.

Отождествим элементы кольца R_N с N-мерными двоичными векторами, полагая

$$r = \sum_{i=0}^{N-1} 2^i r_i = (r_{N-1},...,r_1,r_0),\ r_i \in \{0,1\},\ i \in \overline{0,N-1}.$$

Для заданных N_1, N_2 определим отображения $\delta_0, \delta_1 : R_N \to R_N$ по формулам:

$$\begin{gathered}\delta_0(r) = (0,...,0,r_{N_1-1},...,r_0),\ \delta_1(r) = (0,...,0,r_{N-1},...,r_{N_1}),\\ r = (r_{N-1},...,r_1,r_0) \in R_N.\end{gathered} \tag{5}$$

На основании (5) имеем:

$$r = \delta_0(r) + 2^{N_1}\delta_1(r),\ r \in R_N. \tag{6}$$

Считая, что множества R_{N_1}, R_{N_2} канонически вложены во множество R_N, можно записать:

$$\delta_0(r) \in R_{N_1},\ \delta_1(r) \in R_{N_2}. \tag{7}$$

Отметим, что соотношения (6), (7) однозначно определяют функции δ_0, δ_1 в следующем смысле: для любых $a_0 \in R_{N_1}$, $a_1 \in R_{N_2}$ таких, что $r = a_0 + 2^{N_1}a_1$, имеют место равенства $a_0 = \delta_0(r)$, $a_1 = \delta_1(r)$. Это свойство функций δ_0, δ_1 будет использовано ниже.

Для любой матрицы $U = \| u_{\mu\nu} \|$ над кольцом R_N положим по определению $\delta_0(U) = \| \delta_0(u_{\mu\nu}) \|$, $\delta_1(U) = \| \delta_1(u_{\mu\nu}) \|$. Очевидно равенство $U = \delta_0(U) + 2^{N_1} \delta_1(U)$.

Перейдем к определению алгоритма $\wp = \theta_{N_1,N_2}(\wp_1, \wp_2)$. Рассмотрим СЛУ (1) над кольцом R_N. Для решения этой СЛУ с помощью определяемого алгоритма $\wp$, прежде всего, построим систему линейных уравнений с искаженной правой частью над кольцом R_{N_1} следующего вида:

$$\delta_0(A)y = \delta_0(b) = \delta_0(A)\delta_0(x_0) + \delta_0(\varepsilon). \tag{8}$$

Отметим, что закон распределения $p_{N_1} \overset{\text{def}}{=} \delta_0(p_N)$ координат случайного вектора $\delta_0(\varepsilon)$ определяется по формуле:

$$p_{N_1}(a_{N_1-1},...,a_0) = \sum_{(u_{N-1},...,u_{N_1}) \in R_{N_2}} p_N(u_{N-1},...,u_{N_1}, a_{N_1-1},...,a_0),\ (a_{N_1-1},...,a_0) \in R_{N_1}.$$

Если упорядоченный набор $(\delta_0(A), \delta_0(b), p_{N_1})$ принадлежит области определения $D_{\wp_1}$ алгоритма $\wp_1$ (то есть СЛУ (8) может быть решена с помощью этого алгоритма), то, решая ее, получим оценку

$$x_{0,1}^* = \wp_1(\delta_0(A), \delta_0(b), p_{N_1}) \tag{9}$$

вектора $x_{0,1} \overset{\text{def}}{=} \delta_0(x_0)$.

Итак, на первом шаге алгоритма $\wp$ вида (4) осуществляется построение СЛУ (8), проверка условия

$$(\delta_0(A), \delta_0(b), p_{N_1}) \in D_{\wp_1} \tag{10}$$

и вычисление оценки истинного решения $x_{0,1}$ СЛУ (8) по формуле (9).

На втором шаге алгоритма $\wp$ по системе уравнений (1) и вектору (9) составляется СЛУ над кольцом R_{N_2} следующего вида:

$$A_2 z = \delta_1(b) - \delta_1(Ax_{0,1}^* + \varepsilon_1^*), \tag{11}$$

где $A_2 = A \bmod(2^{N_2})$,

$$\varepsilon_1^* = \delta_0(b - Ax_{0,1}^*). \tag{12}$$

Отметим, что в общем случае СЛУ (11) не является системой уравнений с искаженной правой частью. Тем не менее, справедливо следующее утверждение.

Утверждение 1. При выполнении равенства

$$x_{0,1}{}^* = x_{0,1} \tag{13}$$

СЛУ (11) является системой линейных уравнений с искаженной правой частью над кольцом R_{N_2}, имеет истинное решение $x_{0,2} \stackrel{\text{def}}{=} \delta_1(x_0)$ и определяется упорядоченным набором $(A_2, x_{0,2}, d, p_{N_2})$, где вектор $d \stackrel{\text{def}}{=} \delta_1(b) - \delta_1(Ax_{0,1}{}^* + \varepsilon_1{}^*)$ удовлетворяет равенству над кольцом R_{N_2}

$$d = A_2 x_{0,2} + \varepsilon_2, \tag{14}$$

а закон распределения случайного вектора $\varepsilon_2 \stackrel{\text{def}}{=} \delta_1(\varepsilon)$ определяется по формуле:

$$p_{N_2}(a_{N_2-1},...,a_0) = \sum_{(u_{N_1-1},...,u_0)\in R_{N_1}} p_N(a_{N_2-1},...,a_0,u_{N_1-1},...,u_0), \quad (a_{N_2-1},...,a_0) \in R_{N_2}.$$

Доказательство. Достаточно показать, что при выполнении соотношений (1), (13) имеет место равенство (14).

Согласно определению вектора d и равенства (12), при выполнении (13) справедливо следующее равенство над кольцом R_{N_2}:

$$d = \delta_1(b) - \delta_1(Ax_{0,1}{}^* + \delta_0(\varepsilon)). \tag{15}$$

С другой стороны, на основании (1)

$$\begin{gathered} b = Ax_0 + \varepsilon = A(x_{0,1} + 2^{N_1} x_{0,2}) + \delta_0(\varepsilon) + 2^{N_1}\delta_1(\varepsilon) = \\ = Ax_{0,1} + \delta_0(\varepsilon) + 2^{N_1}(Ax_{0,2} + \delta_1(\varepsilon)) = \delta_0(Ax_{0,1} + \delta_0(\varepsilon)) + \\ + 2^{N_1}(Ax_{0,2} + \delta_1(\varepsilon) + \delta_1(Ax_{0,1} + \delta_0(\varepsilon))), \end{gathered}$$

откуда согласно отмеченному выше свойству функций δ_0, δ_1, вытекает равенство:

$$\delta_1(b) \equiv Ax_{0,2} + \delta_1(\varepsilon) + \delta_1(Ax_{0,1} + \delta_0(\varepsilon)) \pmod{2^{N_2}}. \tag{16}$$

Из (15), (16) находим, что $d \equiv Ax_{0,2} + \delta_1(\varepsilon) \pmod{2^{N_2}}$, то есть над кольцом R_{N_2} выполняется равенство (14), что и требовалось доказать.

Полученное утверждение показывает, что в случае, когда оценка (9) истинного решения $x_{0,1}$ СЛУ (8) совпадает с этим решением, СЛУ (11) представляет собой систему уравнений с искаженной правой частью над кольцом R_{N_2}. Эта система уравнений определяется набором $(A_2, x_{0,1}, d, p_{N_2})$, заданным в формулировке утверждения 1.

Итак, на основании вышеизложенного, второй шаг алгоритма $\wp$ описывается следующим образом. Вначале строится СЛУ (11), которая интерпретируется как система уравнений с искаженной правой частью над кольцом R_{N_2}. Затем проверяется условие:

$$(A_2, d, p_{N_2}) \in D_{\wp_2}. \tag{17}$$

Если соотношение (17) выполняется, то СЛУ (11) решается с помощью алгоритма $\wp_2$, то есть вычисляется оценка

$$x_{0,2}{}^* = \wp_2(A_2, d, p_{N_2}) \tag{18}$$

истинного решения $x_{0,2}$ СЛУ с искаженной правой частью

$$A_2 z = d = A_2 x_{0,2} + \varepsilon_2 \tag{19}$$

над кольцом R_{N_2}.

Наконец, на третьем шаге алгоритма $\wp$ вычисляется оценка $x_0{}^* = \wp(A, b, p_N)$ истинного решения СЛУ (1), которая находится по формуле:

$$x_0{}^* = x_{0,1}{}^* + 2^{N_1} x_{0,2}{}^*.$$

Отметим, что в соответствии с приведенным описанием алгоритма $\wp$ его область определения $D_\wp$ состоит из тех и только тех упорядоченных наборов (A, b, p_N), для которых выполняются условия (10) и (17). Таким образом, отображение θ_{N_1,N_2} вида (3) корректно определено.

Приведем аналитические выражения оценок надежности и трудоемкости алгоритма $\wp = \theta_{N_1,N_2}(\wp_1, \wp_2)$ через соответствующие характеристики алгоритмов $\wp_1$ и $\wp_2$.

Утверждение 2. Пусть (A, x_0, b, p_N) — СЛУ вида (1) над кольцом R_N, и пусть $(A, b, p_N) \in D_\wp$, где алгоритм $\wp$ определяется равенством (4). Обозначим

$$\pi_{\wp_1} = \pi_{\wp_1}(\delta_0(A), x_{0,1}, p_{N_1}),\ \pi_{\wp_2} = \pi_{\wp_2}(A_2, x_{0,2}, p_{N_2})$$

значения функций надежности и трудоемкости алгоритмов $\wp_1$, $\wp_2$ соответственно (от аргументов $(\delta_0(A), x_{0,1}, p_{N_1})$ и $(A_2, x_{0,2}, p_{N_2})$, определяемых системами линейных уравнений с искаженными правыми частями (8) и (19) соответственно).

Положим $\pi_{\wp} = \pi_{\wp}(A, x_0, p_N)$. Тогда справедливы неравенства:

$$\pi_{\wp_1} + \pi_{\wp_2} - 1 \le \pi_{\wp} \le \min\{\pi_{\wp_1}, \pi_{\wp_2}\}. \tag{20}$$

Кроме того, если случайные векторы $\varepsilon_1 = \delta_0(\varepsilon)$ и $\varepsilon_2 = \delta_1(\varepsilon)$ независимы, то

$$\pi_{\wp} = \pi_{\wp_1}\pi_{\wp_2}. \tag{21}$$

Доказательство. Рассмотрим события U_1 и U_2, определяемые по формулам:

$$U_1 = \{\varepsilon \in R_N{}^{(t)} : \wp_1(\delta_0(A), \delta_0(b), p_{N_1}) = x_{0,1}\},\ U_2 = \{\varepsilon \in R_N{}^{(t)} : \wp_2(A_2, d, p_{N_2}) = x_{0,2}\}.$$

Обозначим символом $\Pr^{(t)}$ РВ на множестве $R_N{}^{(t)}$ значений случайного вектора ε. Из определения параметров $\pi_{\wp_1}$, $\pi_{\wp_2}$ следуют равенства:

$$\pi_{\wp_1} = \Pr^{(t)}\{U_1\},\ \pi_{\wp_2} = \Pr^{(t)}\{U_2\}. \tag{22}$$

С другой стороны, согласно определению алгоритма $\wp$, выполняется равенство:

$$\pi_{\wp} = \Pr^{(t)}\{U_1U_2\}. \tag{23}$$

Непосредственно из формул (22), (23) следуют соотношения (20), (21). Утверждение доказано.

Получим оценку трудоемкости $T_{\wp} = T_{\wp}(N, n, t, p_N)$ алгоритма $\wp$. На первом шаге этого алгоритма построение СЛУ (8) не требует вычислений (за исключением, быть может, нахождения распределения вероятностей p_{N_1} по распределению p_N). Следовательно, трудоемкость первого шага равна $T_{\wp_1}(N_1, n, t, p_{N_1})$.

На втором шаге для вычисления вектора ε_1* по формуле (12) достаточно выполнить *nt* умножений и $(n-1)t + t = nt$ сложений (вычитаний) в кольце R_{N_1}. Далее, вычисление вектора *d* в правой части СЛУ (11) потребует выполнения *nt* умножений и $(n+1)t$ сложений (вычитаний) в кольце R_N.

Таким образом, суммарная сложность второго шага алгоритма $\wp$ составит не более

$$T_2 = T_{\wp_2}(N_2, n, t, p_{N_2}) + 2ntT_{\text{УМ}}(N) + 2(n+1)tT_{\text{СЛ}}(N)$$

двоичных операций (символы $T_{\text{УМ}}(N)$ и $T_{\text{СЛ}}(N)$ обозначают соответственно временные сложности алгоритмов умножения и сложения (вычитания) N-разрядных двоичных целых чисел). Наконец, на третьем шаге алгоритма $\wp$ вычислений фактически не производится.

Итак, доказано следующее утверждение.

Утверждение 3. Трудоемкость алгоритма $\wp = \theta_{N_1,N_2}(\wp_1, \wp_2)$, определяемого по формуле (4), оценивается сверху величиной:

$$T_{\wp} = T_{\wp_1}(N_1, n, t, p_{N_1}) + T_{\wp_2}(N_2, n, t, p_{N_2}) + 2(n+1)t(T_{\text{УМ}}(N) + T_{\text{СЛ}}(N)). \qquad (24)$$

Оптимизация алгоритмов решения систем линейных уравнений с искаженной правой частью над кольцом R_N

Следуя общей идее предложенного в [14] подхода к построению оптимальных вычислительных алгоритмов, определим рекурсивно отображения

$$\theta_{N_1,N_2,\ldots,N_k} : \Lambda_{N_1} \times \Lambda_{N_2} \times \ldots \times \Lambda_{N_k} \to \Lambda_N,$$

где $k \geq 3$, $N = N_1 + N_2 + \ldots + N_k$, $N_i \geq 1$, $i \in \overline{1,k}$, полагая для любых $\wp_i \in \Lambda_{N_i}$ ($i \in \overline{1,k}$):

$$\theta_{N_1,N_2,\ldots,N_k}(\wp_1, \wp_2, \ldots, \wp_k) = \theta_{N-N_k,N_k}(\theta_{N_1,N_2,\ldots,N_{k-1}}(\wp_1, \wp_2, \ldots, \wp_{k-1}), \wp_k).$$

Пусть теперь для каждого натурального $j \in \overline{1,N}$ задан некоторый алгоритм $\wp(j)$ решения систем линейных уравнений с искаженной правой частью над кольцом R_j. Функции надежности π_j и трудоемкости T_j алгоритма $\wp(j)$ ($j \in \overline{1,N}$) предполагаются известными. Обозначим через $\Theta = \Theta(\wp(1), \ldots, \wp(N))$ класс всех алгоритмов $\wp \in \Lambda_N$ вида $\wp = \theta_\nu \overset{\text{def}}{=} \theta_{N_1,N_2,\ldots,N_k}(\wp(N_1), \wp(N_2), \ldots, \wp(N_k))$, где $\nu = (N_1, N_2, \ldots, N_k)$ пробегает всевозможные композиции (упорядоченные разбиения) числа N.

Зафиксируем СЛУ вида (1) над кольцом R_N и предположим, что двоичные разряды координат случайного вектора ε являются независимыми в совокупности случайными величинами. Рассмотрим задачу построения алгоритма $\wp^* \in \Theta$, имеющего при заданной верхней границе трудоемкости наибольшую надежность среди всех алгоритмов решения СЛУ (1), принадлежащих классу Θ:

$$\pi_{\wp}(A, x_0, p_N) \to \max,\ T_{\wp}(N, n, t, p_N) \leq T_0,\ \wp \in \Theta. \qquad (25)$$

Заметим, что, поскольку Θ содержит ровно 2^{N-1} различных алгоритмов, то тривиальная процедура решения задачи (25) сводится к перебору этих алгоритмов

и вычислению их надежностей и трудоемкостей с использованием соотношений (21), (24).

Отметим, что при определенных дополнительных ограничениях на РВ координат случайного вектора ε задача (25) может быть решена более эффективно. Рассмотрим, например, частный случай, в котором

$$p_N(a) = p^{\|a\|}(1-p)^{N-\|a\|}, a = (a_{N-1},...,a_0) \in R_N, \qquad (26)$$

где $\|a\| = a_0 + ... + a_{N-1}$, $0 < p < 1/2$. Обозначим φ_j канонический гомоморфизм кольца R_N в кольцо R_j, $j \in \overline{1,N}$. Отображение φ_j стандартным образом продолжим до отображений, заданных на множестве всех матриц над кольцом R_N и распределений вероятностей на этом кольце соответственно.

Заметим, что на основании утверждений 2, 3 и равенства (26) для любой композиции ν числа N надежность и трудоемкость алгоритма $\wp = \theta_\nu$ определяются соответственно по формулам:

$$\pi_\wp(A, x_0, p_N) = \prod_{j=1}^{N} (\pi_j)^{\alpha_j},$$

$$T_\wp(N, n, t, p_N) = \sum_{j=1}^{N} \alpha_j T_j + 2(n+1)t(T_{\text{УМ}}(N) + T_{\text{СЛ}}(N))(\sum_{j=1}^{N} \alpha_j - 1),$$

где α_j — число слагаемых, равных j, в композиции ν, $\pi_j = \pi_j(\varphi_j(A), \varphi_j(x_0), \varphi_j(p_N))$, $T_j = T_j(N, n, t, \varphi_j(p_N))$, $j \in \overline{1,N}$. Отсюда следует, что при выполнении условия (26) задача (25) равносильна следующей задаче целочисленного линейного программирования:

$$\sum_{j=1}^{N} \alpha_j \ln \pi_j \to \max, \sum_{j=1}^{N} \alpha_j (T_j + 2(n+1)t(T_{\text{УМ}}(N) + T_{\text{СЛ}}(N))) \le T_0 + 2(n+1)t(T_{\text{УМ}}(N) + T_{\text{СЛ}}(N)),$$

$$\alpha_j \in \mathbf{Z}, \alpha_j \ge 0, j \in \overline{1,N}, \alpha_1 + 2\alpha_2 + \ldots + N\alpha_N = N.$$

Для решения последней задачи можно применять известные алгоритмы [16].

Результаты экспериментального исследования эффективности алгоритмов решения СЛУ с искаженной правой частью над кольцом R_5

Ниже в таблице представлены численные оценки средней надежности и трудоемкости семи программно реализованных алгоритмов решения СЛУ с искаженной правой частью над кольцом вычетов по модулю 32, соответствующих семи композициям числа $N = 5$. Данные в таблице получены с использованием про-

граммы для ПЭВМ типа Celeron 1100 MHz, 256 Mb ОЗУ, которая для каждой пары значений *n*, *t* (числа неизвестных и уравнений соответственно) решает 100 систем линейных уравнений с искаженной правой частью над кольцом R_5.

Характеристики эффективности алгоритмов решения СЛУ
с искаженными правыми частями над кольцом вычетов по модулю 32

		(1,1,1,1,1)		(2, 2, 1)		(2, 3)		(3, 1, 1)		(3, 2)		(4, 1)		(5)	
n	*t*	*P*	*T*	*P*	*T*	*P*	*T*	*P*	*T*	*P*	*T*	*P*	*T*	*P*	*T*
3	7	0,01	0	0,01	0	0,01	0	0,03	0	0,03	0	0,03	1	0,09	20
	25	0,04	0	0,10	0	0,13	0	0,22	0	0,39	0	0,39	2	0,86	28
	40	0,15	0	0,21	0	0,27	0	0,34	0	0,59	0	0,78	3	0,99	34
	60	0,17	0	0,38	0	0,48	0	0,48	1	0,79	0	0,94	4	1	42
	80	0,30	0	0,57	0	0,64	0	0,63	1	0,88	0	0,95	6	1	50
	100	0,47	0	0,66	0	0,78	0	0,77	1	0,99	0	1	7	1	58
	150	0,67	0	0,88	0	0,92	1	0,90	2	1	1	1	10	1	79
4	25	0	0	0,02	0	0,04	1	0,08	2	0,20	1	0,22	42	0,72	919
	80	0,18	0	0,33	1	0,45	3	0,38	5	0,79	3	0,93	98	1	1717
	150	0,49	0	0,81	1	0,88	4	0,81	10	1	5	1	168	1	2744

Истинное решение и элементы матрицы коэффициентов каждой системы линейных уравнений формируются с использованием линейного конгруэнтного генератора по модулю 32. Векторы искажений в правых частях СЛУ состоят из символов, представленных в коде ASCII, которые выбираются последовательно, с интервалом в 10 знаков, из осмысленного текста, составленного из русскоязычных и англоязычных фраз. В качестве исходного алгоритма $\wp(j)$ решения СЛУ с искаженной правой частью над кольцом R_j ($j \in \overline{1,5}$) используется стандартный алгоритм, основанный на методе максимума правдоподобия [11]. Параметры *P* и *T* в таблице обозначают соответственно отношение числа правильно решенных СЛУ к общему числу (100) систем уравнений и суммарное время (в секундах) решения всех систем уравнений без учета времени их формирования.

Как видно из таблицы, диапазон изменения значений характеристик эффективности рассматриваемых алгоритмов достаточно широк. Так, средняя надежность решения системы из 25 уравнений от трех неизвестных, с искаженными правыми частями, изменяется от 0,04 до 0,86. При этом на решение 100 таких систем затрачивается от 1 до 28 секунд. Система от того же числа неизвестных, состоящая из 60 уравнений с искаженными правыми частями, решается со средней надежностью от 0,17 до 1. Время решения 100 указанных СЛУ составляет от 1 до 42 секунд. Очевидно, что с ростом отношения *t*/*n* надежность каждого из семи алгоритмов увеличивается.

Результаты экспериментальных исследований, приведенные в таблице, позволяют упорядочить рассматриваемые алгоритмы по убыванию их средней надежности. Так, при всех значениях параметров *n* и *t*, указанных в таблице, наибольшую среднюю надежность имеет алгоритм $\theta_{(5)}$; далее следуют алгоритмы $\theta_{(4,1)}$ и $\theta_{(3,2)}$. При умеренных (по сравнению с *n*) значениях *t* следующими в списке

оказываются алгоритмы $\theta_{(3,1,1)}$ и $\theta_{(2,3)}$. С ростом t средние надежности этих алгоритмов выравниваются, и при $t >> n$ порядок их расположения меняется на противоположный: $\theta_{(2,3)}$, $\theta_{(3,1,1)}$. Наконец, замыкают список алгоритмы $\theta_{(2,2,1)}$ и $\theta_{(1,1,1,1,1)}$.

Отметим, что алгоритм $\theta_{(1,1,1,1,1)}$ совпадает с последовательным методом решения систем линейных уравнений с искаженной правой частью над кольцом R_5 [10]. Как видно из таблицы, этот алгоритм имеет наименьшую среднюю надежность и наименьшую трудоемкость среди семи рассматриваемых алгоритмов. С другой стороны, алгоритм $\theta_{(5)}$ по существу представляет собой метод максимума правдоподобия решения СЛУ с искаженной правой частью над кольцом R_5 и характеризуется среди рассматриваемых алгоритмов наибольшими значениями средней надежности и трудоемкости.

В целом, как видно из данных, представленных в таблице, предложенный метод оптимизации алгоритмов решения СЛУ с искаженной правой частью над кольцом R_N позволяет обеспечить хороший «баланс» между основными показателями эффективности (надежностью и трудоемкостью) алгоритмов путем выбора подходящей композиции числа N. Ясно также, что с расширением совокупности исходных алгоритмов появляется дополнительная возможность целенаправленно варьировать значения указанных показателей в зависимости от условия конкретной прикладной задачи, приводящей к решению систем линейных уравнений с искаженной правой частью над кольцом вычетов по модулю 2^N.

1. *Балакин Г.В.* Введение в теорию случайных систем уравнений // Труды по дискретной математике. — М.: ТВП. — 1997. — Т. 1. — С. 1–18.

2. *Балакин Г.В., Никольский Ю.Б.* Последовательное применение метода максимума правдоподобия к решению систем уравнений с мешающими параметрами // Обозрение прикл. промышл. матем. — 1995. — Т. 2. — Вып. 3. — С. 468–476.

3. *Балакин Г.В.* Эффективно решаемые классы систем булевых уравнений // Обозрение прикл. промышл. матем. — 1995. — Т. 2. — Вып. 3. — С. 494–501.

4. *Meier W., Staffelbach O.* Fast Correlation Attacs on Stream Ciphers // J. Cryptology. — 1989. — Vol. 1, N 3. — P. 159–176.

5. *Kovalenko I.N., Savchuk M.N.* Some Methods of Decoding Corrupted Linear Codes // Реєстрація, зберігання і оброб. даних. — 1999. — Т. 1, № 2. — С. 62–68.

6. *Johansson T., Jonsson F.* Fast Correlation Attacks Through Reconstruction of Linear Polynomials // Advances in Cryptology — Crypto'00, Proceedings. — Springer Verlag, 2000. — P. 300–315.

7. *Chepyzhov V., Johansson T., Smeets B.* A Simple Algorithm for Fast Correlation Attacks on Stream Ciphers // FSE'2000. — Springer Verlag, 2001. — Vol. 547. — P. 181–195.

8. *Смирнов В.Г.* Системы булевых уравнений рекуррентного типа // Обозрение прикл. промышл. матем. — 1995. — Т. 2. — Вып. 3. — С. 477–482.

9. *Балакин Г.В.* Оценка истинного решения системы уравнений над кольцом вычетов при аддитивной помехе // Проблемы теоретической кибернетики: Тез. докл. XII Междунар. конф. — Нижний Новгород, 1999. — С. 15.

10. *Алексейчук А.Н.* Системы линейных уравнений с искаженной правой частью над кольцом вычетов по модулю 2^N // Захист інформації. — 2001. — № 4. — С. 12–19.

11. *Алексейчук А.Н., Игнатенко С.М.* Оценки эффективности универсальных методов восстановления искаженных линейных рекуррент над кольцом вычетов по модулю 2^N // Зб. наук. пр. ІПМЕ НАН України. — Вып. 20. — К., 2003. — С. 40–48.

12. *Игнатенко С.М., Алексейчук А.Н.* Алгоритм восстановления искаженной линейной рекурренты над кольцом вычетов по модулю 2^N с использованием быстрого преобразования Ферма // Тез. докл. VI Междунар. научно-практич. конф. «Безопасность информации в информационно-телекоммуникационных системах». — К., 2003. — С. 53–54.

13. *Блейхут Р.* Быстрые алгоритмы цифровой обработки сигналов: Пер. с англ. — М.: Мир, 1989. — 448 с.

14. *Гаврилкевич М.В., Солодовников В.И.* Эффективные алгоритмы решения задач линейной алгебры над полем из двух элементов // Обозрение прикл. промышл. матем. — 1995. — Т. 2. — Вып. 3. — С. 400–437.

15. *Ахо А., Хопкрофт Дж., Ульман Дж.* Построение и анализ вычислительных алгоритмов: Пер. с англ. — М.: Мир, 1979. — 535 с.

16. *Мину М.* Математическое программирование: Пер. с фр. — М.: Наука, 1990. — 488 с.

Поступила в редакцию 07.02.2005