УДК 519.17

В. Г. Скобелев

Оценки сложности экспериментов с блоками управляемых перестановок

(Представлено академиком НАН Украины А. А. Летичевским)

Для базових типів блоків керованих перестановок (матричних, пошарових та рекурсивних) отримано асимптотичні оцінки складності експериментів, призначених для виявлення або локалізації поодиноких несправностей. Встановлено, що для матричних та рекурсивних блоків керованих перестановок складність цих експериментів не є істотною порівняно зі складністю самого блоку.

1. Представив семейство перестановок n-битовых последовательностей, используемое при построении блочных шифров [1, 2], отображением $\mathbf{f}\colon \mathbf{E}^{n+m} \to \mathbf{E}^n$ ($\mathbf{E} = \{0,1\}$; $m \in \mathbf{N}$), т. е. $\mathbf{y} = \mathbf{f}(\mathbf{x}, \mathbf{v})$, где $\mathbf{x} \in \mathbf{E}^n$ — информационный, а $\mathbf{v} \in \mathbf{E}^m$ — управляющий вектор, получим, что отображение $\mathbf{g}_{\mathbf{v}_0}\colon \mathbf{E}^n \to \mathbf{E}^n$ ($\mathbf{v}_0 \in \mathbf{E}^m$), где $\mathbf{g}_{\mathbf{v}_0}(\mathbf{x}) = \mathbf{f}(\mathbf{x}, \mathbf{v}_0)$, является перестановкой компонент вектора $\mathbf{x} \in \mathbf{E}^n$. Комбинационная схема (КС) $S_{\mathbf{f}}$, реализующая отображение $\mathbf{f}$, определена в [3] как блок управляемых перестановок (БУП). В [3] исследована скорость функционирования основных типов БУП и осуществляемое ими рассеяние компонент информационного вектора, но не исследованы задачи обнаружения и локализации неисправностей. Последние должны быть решены стандартными методами технической диагностики [4], но получаемые при этом тесты существенно сложнее оптимальных (так как в них не учтены ни функциональные, ни структурные характеристики КС $S_{\mathbf{f}}$). Оценим сложность обнаружения и локализации неисправностей для основных типов БУП.

2. Пусть $\mu(C)$ — общее число ножек функционального элемента C. Определим сложность КС $S_{\mathbf{f}}$ равенством $\mu(S_{\mathbf{f}}) = \sum \mu(C)$, где сумма берется по всем функциональным элементам КС $S_{\mathbf{f}}$. Неисправностью КС $S_{\mathbf{f}}$ назовем одиночную неисправность ее функционального элемента (константную неисправность ножки или короткое замыкание двух соседних ножек), а тест представим матрицей, строки которой — вход-выходные пары эталона. Пусть A_d и A_l — минимальные тесты для обнаружения и локализации неисправностей КС $S_{\mathbf{f}}$. Положим $\mu_a(S_{\mathbf{f}}) = (2n+m)\alpha_a$ ($a \in \{d, l\}$), где α_a — число строк матрицы A_a. Величину $\nu_a(S_{\mathbf{f}}) = \mu^{-1}(S_{\mathbf{f}})\mu_a(S_{\mathbf{f}})$ ($a \in \{d, l\}$) назовем сложностью обнаружения ($a = d$) и локализации ($a = l$) неисправностей КС $S_{\mathbf{f}}$.

3. Матричный БУП — это КС $M^{(1)}_{n,m}$, содержащая дешифратор D_m с m входами и элементы P_i ($i = 1, \ldots, 2^m - 2$), реализующие такие отображения $\mathbf{h}_{P_i}\colon \mathbf{E}^n \times \mathbf{E} \to \mathbf{E}^n$, что отображение $\mathbf{f}^{\alpha}_{P_i}\colon \mathbf{E}^n \to \mathbf{E}^n$ ($\alpha \in \mathbf{E}$), где $\mathbf{f}^{\alpha}_{P_i}(\mathbf{x}) = \mathbf{h}_{P_i}(\mathbf{x}, \alpha)$, при $\alpha = 1$ осуществляет перестановку компонент вектора $\mathbf{x} \in \mathbf{E}^n$, а при $\alpha = 0$ является тождественным отображением. При этом: 1) для КС $M^{(1)}_{n,m}$ информационные входы — это информационные входы элемента P_1, управляющие входы — это входы дешифратора, а выходы — это 0-й и $(2^m - 1)$-й выходы дешифратора (используются только в процессе эксперимента), а также выходы элемента P_{2^m-2}; 2) i-й выход ($i = 1, \ldots, 2^m - 2$) дешифратора D_m подсоединен к управляющему входу элемента P_i; 3) выходы элемента P_i ($i = 1, \ldots, 2^m - 3$) подсоединены к информационным входам элемента P_{i+1}.

Положив $\mathbf{f}^0_{P_i}(\mathbf{x}) \equiv \mathbf{0}$ ($\mathbf{x} \in \mathbf{E}^n$) для всех $i = 1, \ldots, 2^m - 2$ и изменив структуру КС $M^{(1)}_{n,m}$ так, что ее информационные входы подсоединены к информационным входам каждого элемента P_i ($i = 1, \ldots, 2^m - 2$), а выходы этих элементов через элемент ИЛИ подсоединены к внешним выходам, получим КС $M^{(2)}_{n,m}$, эквивалентную КС $M^{(1)}_{n,m}$.

Представляет интерес и следующее изменение структуры КС $M^{(1)}_{n,m}$. Удалив D_m и ограничившись элементами P_i ($i = 1, \ldots, m$), подсоединим i-й управляющий вход КС к управляющему входу элемента P_i. Получим КС $M^{(3)}_{n,m}$, реализующую семейство перестановок $\mathbf{f}^{\alpha_1}_{P_1} \circ \cdots \circ \mathbf{f}^{\alpha_m}_{P_m}$ ($\alpha_1, \ldots, \alpha_m \in \mathbf{E}$), где $\circ$ — операция суперпозиции.

Анализ этих КС дает возможность доказать следующую теорему.

Теорема 1. *Если $m = O(n \log n)$ ($n \to \infty$), то для КС $S_{\boldsymbol{f}} \in \{M^{(i)}_{n,m} \mid i = 1, 2, 3\}$ истинны следующие асимптотические равенства:*

$$\nu_d(S_{\boldsymbol{f}}) = O(\log n) \qquad (n \to \infty), \tag{1}$$

$$\nu_l(S_{\boldsymbol{f}}) = O(n \log n) \qquad (n \to \infty). \tag{2}$$

4. Послойный БУП — это КС $P_{n,m}$ (n — четное число, $m = 0{,}5n(k-1)$ ($k \in \mathbf{N}$)), содержащая элементы π_i ($i = 1, \ldots, k$) и m элементов δ. Элемент π_i ($i = 1, \ldots, k$) реализует перестановку $\mathbf{f}_i$ компонент вектора $\mathbf{x} \in \mathbf{E}^n$, а элемент δ — такое отображение $\mathbf{g}\colon \mathbf{E}^2 \times \mathbf{E} \to \mathbf{E}^2$, что $\mathbf{g}((\alpha, \beta), 1) = (\beta, \alpha)$ и $\mathbf{g}((\alpha, \beta), 1) = (\alpha, \beta)$ для всех $(\alpha, \beta) \in \mathbf{E}^2$. При этом: 1) для КС $P_{n,m}$ информационные входы — это входы элемента π_1, управляющие входы — это управляющие входы всех элементов δ, а выходы — это выходы элемента π_k; 2) выходы элемента π_i ($i = 1, \ldots, k-1$) разбиты на пары, каждая из которых подсоединена к информационным входам соответствующего элемента δ; 3) выходы элементов δ, информационные входы которых соединены с выходами элемента π_i ($i = 1, \ldots, k-1$), подсоединены к соответствующим входам элемента π_{i+1}.

Анализ КС $P_{n,m}$ дает возможность доказать следующую теорему.

Теорема 2. *Для КС $P_{n,m}$ истинны следующие асимптотические равенства*

$$\nu_d(P_{n,m}) = O(n) \qquad (n \to \infty,\ k \to \infty), \tag{3}$$

$$\nu_l(P_{n,m}) = O(\mu^2(P_{n,m})) \qquad (n \to \infty,\ k \to \infty). \tag{4}$$

5. Рекурсивный БУП — это 2-уровневая КС R_n ($n = rs$): 1-й уровень состоит из КС $W^{(i)}_r = Z_r$ ($i = 1, \ldots, s$), а 2-й уровень — из КС U_n, где U_n и Z_r — это БУП, соответственно, n-элементных и r-элементных битовых последовательностей. При этом: 1) для КС R_n информационные входы — это информационные входы КС $W^{(i)}_r$ ($i = 1, \ldots, s$), управляющие входы — это управляющие входы КС U_n и $W^{(i)}_r$ ($i = 1, \ldots, s$), а выходы — это выходы КС U_n; 2) выходы КС $W^{(i)}_r$ ($i = 1, \ldots, s$) подсоединены к соответствующим информационным входам КС U_n.

Такая структура рекурсивного БУП R_n дает возможность строить для него тесты в соответствии со следующей схемой:

1) для каждого $i = 1, \ldots, s$ тестируем КС $W^{(i)}_r$ при находящихся в фиксированных режимах КС U_n и $W^{(1)}_r, \ldots, W^{(i-1)}_r, W^{(i+1)}_r, \ldots, W^{(s)}_r$;

2) тестируем КС U_n.

Отметим, что именно такая схема была применена в [5] при анализе сложности 2-уровневых и 3-уровневых сетей Клоса.

Так как рассматриваются только одиночные неисправности БУП, то при такой схеме тестирования для $a \in \{d, l\}$ истинно следующее асимптотическое равенство:

$$\mu_a(R_n) = O(s\mu_a(Z_r) + \mu_a(U_n)) \qquad (s \to \infty,\ r \to \infty).$$

Отсюда вытекает

Теорема 3. *Если* $\mu(U_n) = O(s\mu(Z_r))$ $(s \to \infty,\ r \to \infty)$, *то для* $a \in \{d, l\}$ *истинно такое асимптотическое равенство:*

$$\nu_a(R_n) = O(\nu_a(Z_r) + \nu_a(U_n)) \qquad (s \to \infty,\ r \to \infty). \tag{5}$$

6. В заключение отметим следующее. Равенства (1), (4) и (5) показывают, что асимптотическая сложность эксперимента, предназначенного для обнаружения или локализации одиночных неисправностей в матричных и рекурсивных БУП, не является существенной в сравнении со сложностью самой БУП. Выделение классов послойных БУП, обладающих такими же характеристиками, представляет возможное направление исследований. Другое направление состоит в более тонком анализе различных типов рекурсивных БУП, а третье направление — в исследовании сложности экспериментов, предназначенных для обнаружения и локализации кратных неисправностей в основных типах БУП.

1. *Menezis A., van Oorschot, Vanstone S.* Handbook of applied cryptography. – New York: CRC Press, 1997. – 780 p.
2. *Харин Ю. С., Берник В. И., Матвеев Г. В. и др.* Математические и компьютерные основы криптологии. – Минск: Новое знание, 2003. – 382 с.
3. *Молдовян А. А., Молдовян Н. А., Гуц Н. Д. и др.* Криптография: скоростные шифры. – Ст.-Петербург: БХВ-Петербург, 2002. – 496 с.
4. *Пархоменко П. П.* Основы технической диагностики. – Москва: Энергия, 1981. – 320 с.
5. *Скобелев В. В., Скобелев В. Г.* Анализ шифрсистем. – Донецк: Изд-во Ин-та прикл. механ. и матем. НАН Украины, 2009. – 479 с.

Институт прикладной механики и математики НАН Украины, Донецк

Поступило в редакцию 17.06.2010

V. G. Skobelev

Estimates of the complexity of experiments with controlled blocks of permutations

For basic types of controlled blocks of permutations (namely, matrix, stratum, and recursive ones), the asymptotic estimations of complexity of experiments intended to detect or to localize simple faults are established. It is shown that, for matrix and stratum controlled blocks of permutations, the complexity of above-mentioned experiments is not essential relative to the complexity of the corresponding block.