УДК 519.725, 625.7, 681.3

Применение методов помехоустойчивого кодирования для компактного тестирования цифровых схем

О.Н. Дяченко, Ю.Е. Зинченко, В.О. Дяченко
Донецкий национальный технический университет
do@donntu.org

Дяченко О.Н., Зинченко Ю.Е., Дяченко В.О. Применение методов помехоустойчивого кодирования для компактного тестирования цифровых схем. *Выполнен анализ эффективности компактного тестирования комбинационных схем, учитывающего структуру генератора тестовых последовательностей, анализатора тестовых реакций, построенных на основе методов циклического кодирования, и характер распределения ошибок в тестовой реакции. Предложен метод расчета сигнатур, отличающийся от известного, в выборе степенного обозначения тестовых наборов вместо двоичного. Показано, что главное достоинство аналитического вычисления сигнатур являются не столько значения компактных оценок, а вывод о сигнатурной тестируемости комбинационных схем. Этот вывод распространяется на многовходовые анализаторы тестовых реакций; для структур с посимвольным перемежением; для порождающих полиномов, как в конфигурации Галуа, так и в конфигурации Фибоначчи. Предложены рекомендации по выбору порождающих полиномов регистров сдвига с линейными обратными связями для различных вариантов компактного тестирования.*

Ключевые слова: *Генератор тестовых последовательностей, анализатор тестовых реакций, регистр сдвига с линейными обратными связями, порождающий полином, циклические коды.*

Введение

Всемирная паутина разрастается стремительными темпами: если в 2000 году было 359 млн. пользователей сети Интернет, то в марте 2017 года количество пользователей уже 3732 млн. – это половина населения земного шара. Наша планета постепенно оказывается в своеобразном информационном “коконе”. Увеличение количества информации, которая передается, хранится и обрабатывается, приводит к требованиям обеспечения ее достоверности и надежности используемых аппаратных и программных средств. От успешного решения этих задач, с одной стороны, зависит процветание нынешней цивилизации, или, с другой стороны – ее саморазрушение, например, из-за случайного или намеренного сбоя в военных приложениях. Поэтому для устранения последствий возможных ошибок или дефектов аппаратных средств используется весь арсенал методов и средств помехоустойчивого кодирования, встроенного самотестирования [1-8].

Одним из способов повышения тестопригодности СБИС микропроцессоров, устройств на ПЛИС является применение встроенных средств контроля, реализующих методы компактного тестирования. Метод сквозного сдвигового регистра (LSSD - level sensitive scan design) - другой широко известный способ снижения трудоемкости тестирования дискретных устройств. Метод LSSD сводит задачу тестирования к проверке нескольких регистров сдвига и комбинационных схем. Наиболее совместимым с методом LSSD, из широкого ряда методов компактного тестирования, является сигнатурный анализ, поскольку основой анализатора тестовых реакций (АТР) в этом случае является регистр сдвига с линейными обратными связями (РСЛОС). С помощью незначительных аппаратных затрат сдвиговые регистры преобразуются в РСЛОС, которые выполняют роль генераторов тестовых последовательностей (ГТП) и АТР для тестирования комбинационных схем (КС).

Реализация методов компактного тестирования ставит задачу определения достоверности результатов контроля. В работе [3] рассматриваются вопросы комплексной оценки достоверности тестирования КС при применении ГТП и АТР в виде РСЛОС, которая учитывает не только обнаруживающие способности АТР, но также структуру ГТП и характер тестовых реакций объекта диагностики. В частности, получен вывод о значительной зависимости

эффективности сигнатурного анализа от выбора того или иного сочетания порождающих полиномов РСЛОС ГТП и АТР.
Данная работа представляет собой продолжение исследований в этом направлении.

Цель статьи

Выполнить анализ эффективности компактного тестирования цифровых схем при предположении, что ГТП - РСЛОС с примитивным образующим полиномом, а АТР реализованы на основе циклических кодов. Особенностью таких анализаторов является их способность локализовать ошибки, кратность которых не превышает корректирующих способностей кодов, на основе которых они построены.

Практическая реализация самотестирования СБИС

Анализ диагностического обеспечения микропроцессорных СБИС ведущих зарубежных фирм: IBM (S/390, метод LSSD); Hewlett Packard (сигнатурный анализ); альянс компаний Apple, IBM и Motorola (Power PC); Motorola (MC 202-206); Intel Corporation (микропроцессоры 80386, Pentium Pro); Advanced Micro Devices (AMD-K6), показывает, что 5-8% площади кристалла СБИС занимают встроенные схемы тестирования, которые позволяют обнаружить практически 100% дефектов. Например, диагностическое обеспечение микропроцессора S/390 включает: ОЗУ, кэш, память, схемы их управления со встроенными схемами самотестирования; триггеры, регистровые сети, образующие в режиме тестирования сканируемый путь по методу LSSD; встроенные ГТП; встроенный АТР - многоканальный сигнатурный анализатор; порт JTAG в соответствии со стандартом IEEE 1149.1.
Методы исчерпывающего тестирования КС и сканирования позволяют вместе обнаруживать 95% неисправностей. Применение разных псевдослучайных последовательностей, обеспечивает 99,9% покрытия всех неисправностей СБИС.

Аналитический метод вычислений компактных оценок

Прежде всего, рассмотрим метод аналитического расчета сигнатур, альтернативный методу, предложенному в [3].
Предположим, что ГТП и АТР реализованы в виде РСЛОС с внутренними сумматорами в цепях обратной связи с порождающими полиномами соответственно h(X) и g(X), причем оба полинома примитивные, а их корни связаны равенством $\beta=\alpha^k$, m=degh(X)= =degg(X).
Тестовые наборы, которые поступают на входы исследуемой КС, представляют собой ненулевые элементы поля $GF(2^m)$, являющегося расширением поля GF(2) над полиномом h(X). Эти элементы поля могут быть представлены в двоичном, полиномиальном и степенном обозначениях. Каждому ненулевому элементу α^k поля $GF(2^m)$ соответствует минимальный полином, причем, если минимальный полином примитивный, то его степень равна m. Если в качестве порождающего полинома РСЛОС АТР выбрать минимальный полином, соответствующий элементу α^k, то между корнями полиномов h(X) и g(X) будет выполнено равенство $\beta=\alpha^k$. Анализ таблицы минимальных полиномов показывает, что для любой степени m<5 существует только два примитивных полинома, причем $\beta=\alpha^{-1}$, т. е. эти полиномы являются двойственными (взаимообратными) [6]. Поэтому для примеров, иллюстрирующих метод аналитического расчета сигнатур, будем рассматривать h(X) и g(X) степени m=5.
Основное отличие предлагаемого метода расчета сигнатур от известного [3] заключается в выборе степенного обозначения тестовых наборов вместо двоичного. В этом случае значение сигнатуры для конъюнкции с рангом m может быть вычислено согласно следующему выражению: $S=M_kX^{-Ak}$, где X^A - степенное обозначение тестового набора, M - матрица для перехода от значений РСЛОС ГТП к значениям РСЛОС АТР.
Рассмотрим порядок расчета сигнатур на примерах.
Пример. Пусть $F_1=\bar{x}_5\bar{x}_4x_3x_2x_1$, $g(X)=X^5+X^3+1$, т.е. k=-1.
Элемент поля $GF(2^5)$ над полиномом $h(X)=X^5+X^2+1$, соответствующий тестовому набору 00111, может быть представлен в полиномиальном обозначении X^2+X+1. Для перехода к степенному обозначению воспользуемся таблицей логарифмов Зеча (табл. 1). Согласно этой таблице $X^J=X^i+1$. Учитывая свойства $X^{2j}=(X^i+1)^2$ и $X^i=(X^{p-i}+1)$, где $p=2^m-1$, определим таблицу для нечетных значений i от 1 до 15.
Таким образом, $X^2+X+1=X\bullet(X+1)+1= =X\bullet X^{18}+1=X^{19}+1=X^{11}$. Значение сигнатуры $S(F_1)=M_{-1}X^{11}$.

Таблица 1. Логарифмы Зеча для $h(X)=X^5+X^2+1$

i	1	3	5	7	9	11	13	15
j	18	29	2	22	16	19	14	24

Несколько замечаний по поводу построения матрицы M_k . Прежде всего, следует отметить, что вид матрицы M_k зависит не только от k, но также от начального значения РСЛОС

ГТП, которое может быть выбрано любым ненулевым.

Каждому элементу поля α^0, $\alpha^1,\ldots,\alpha^{m-1}$ ставится в соответствие строка матрицы M_k, которая определяется следующим образом. Для элемента α^j отыскивается значение степени j эквивалентного элемента $\alpha^j=\alpha^i$, которое нацело делится на -k. Значение j определяется на основании равенства $\alpha^i=\alpha^{i+pd}$, где d - любое целое число. Строка матрицы M_k представляет собой остаток от деления полинома $X^{p+j/k+(s-1)}$ на полином g(X) (α^s - начальное состояние РСЛОС ГТП).

Для рассматриваемого примера при начальном состоянии РСЛОС ГТП, равном 00001, для строки, соответствующей α^0, значение равно остатку от деления полинома $X^{31-0-1}=X^{30}$ на полином $g(X)=X^5+X^3+1$.

Для начального состояния РСЛОС ГТП, равного α^0, и k=-1, матрица M_{-1} представляет собой последние m состояний РСЛОС АТР.

Для начального состояния РСЛОС ГТП равного α^m и k=-1 матрица M_{-1} представляет собой единичную матрицу, например, при m=5 значение сигнатуры конъюнкции с рангом m будет равно двоичному обозначению соответствующего элемента поля, записанному в обратном порядке.

Два варианта матрицы M_{-1} будут иметь вид:

$$M_{-1}=\begin{pmatrix}01011\\10110\\00101\\01010\\10100\end{pmatrix},\quad M_{-1}=\begin{pmatrix}00001\\00010\\00100\\01000\\10000\end{pmatrix}$$ - единичная матрица.

Итак, $S(F_1)=M_{-1}X^{11}$.

Для умножения на матрицу необходимо перейти от степенного обозначения тестового набора к двоичному (или полиномиальному). Такое преобразование можно упростить, используя заранее вычисленные значения X^1, X^2, X^4, X^8, X^{16} и т.д. по модулю h(X) (эффективность такого упрощения увеличивается с ростом значения m): $X^1 \bmod h(X)=X^1$, $X^2 \bmod h(X)=X^2$, $X^4 \bmod h(X)=X^4$, $X^8 \bmod h^8(X)=X^3+X^2+1$, $X^{16} \bmod h(X)=X^4+X^3+X+1$.

Произвольный элемент Xj можно представить в виде произведения полиномов со степенями степени 2: $X^{11}=X^8\bullet X^2\bullet X^1$. Остаток от деления X^{11} на h(X) будет равен остатку от деления на h(X) произведения остатков сомножителей: $(X^3+X^2+1)\bullet X^2\bullet X^1 \bmod h(X)=$
$=(X^6+X^5+X^3)\bmod(X^5+X^2+1)=X^2+X+1$, или в двоичном обозначении 00111.

При начальном значении РСЛОС ГТП α^5 значение сигнатуры $S(F_1)$=11100.

Пример. Пусть $F_2=\bar{x}_5\bar{x}_4x_3x_2$ при тех же значениях h(X), g(X) и том же начальном состоянии РСЛОС ГТП.

$S(F_2)=M_{-1}(X^{19})+M_{-1}(X^{19}+1)=$
$=M_{-1}(X^{19}+X^{19}+1)=M_{-1}(00001)=10000$.

Пусть $F_3=\bar{x}_5\bar{x}_4x_3x_1$, $F_4=\bar{x}_4x_3x_2x_1$, $F_5=\bar{x}_5\bar{x}_4x_3$.

$S(F_3)=M_{-1}(X^5+X^5+X)=M-1(X)=$
$=M_{-1}(00010)=01000$.
$S(F_4)=M_{-1}(X^{11}+X^{11}+X^4)=M_{-1}(X^4)=$
$=M_{-1}(10000)=00001$.
$S(F_5)=M_{-1}(X^2+X^2+1+X^2+X+X^2+X+1)=M_{-1}(0)=0$.

Таким образом, в общем случае для k=-1 сигнатура конъюнкции с рангом r=m-1 равна произведению матрицы M_{-1} и X^i , где i - индекс отсутствующей переменной, уменьшенный на единицу; сигнатура конъюнкции с r<m-1 равна нулю.

Аналогично, для произвольных примитивных полиномов h(X) и g(X) степени m, корни которых связаны равенством $\beta=\alpha^{-3}$, для конъюнкции с рангом r<m-2 $S=M_{-3}(0)=0$. Сигнатура равна нулю в следующих случаях: k=-5, r<m-3; k=-7, r<m-4; k=-9, r<m-3; k=-11, r<m-4; k=-13, r<m-4; для произвольного k r<m-1-w, где w - вес двоичной записи -k.

Если рассматривать полученный результат при конкретных значениях m, условие равенства сигнатуры нулю можно сформулировать иначе: r<w[(k_o)], где w[(k_o)] - вес двоичной записи k в обратном коде.

Таким образом, если неисправность в КС, описываемой функцией F, приводит к тестовой реакции $F_н$, и в представлении $F+F_н$ в виде полинома Жегалкина присутствуют только конъюнкции с рангом r<w[$(k)_o$], то $S(F+F_н)=S(F)+S(F_н)=0$, или $S(F)=S(F_н)$, т.е. неисправность будет необнаруженной.

Итак, число w (вес двоичной записи -k) представляет собой параметр, с помощью которого можно оценить эффективность сигнатурного анализа при применении в качестве ГТП и АТР РСЛОС с порождающими примитивными полиномами одинаковой степени. Параметр w принимает минимальное значение 1 при k=-1, и максимальное значение m-1 при k=1.

Этот вывод также справедлив для многовходовых АТР и РСЛОС ГТП и АТР с альтернативной реализацией (с внешними сумматорами в цепях обратной связи).

Учитывая, что структура РСЛОС с приводимым образующим полиномом, который представляет собой произведение различных неприводимых полиномов, эквивалентна совокупности структур РСЛОС с неприводимыми полиномами - сомножителями, получаются следующие выводы. Максимальная эффективность компактного тестирования КС достигается для следующих вариантов:

1) АТР на основе кодов Хэмминга (локализация одиночных ошибок) - одинаковые образующие полиномы РСЛОС ГТП и АТР;

2) АТР на основе кодов БЧХ (локализация кратных независимых ошибок) - первый сомножитель образующего полинома РСЛОС АТР (минимальный полином, соответствующий элементу поля Галуа с наименьшей степенью j) должен быть равен примитивному образующему полиному РСЛОС ГТП. Остальные сомножители - минимальные полиномы, соответствующие элементам поля Галуа со степенями j+2, j+4 и т.д.

3) многовходовый АТР на основе кодов Бартона (локализация одиночного ошибочного вектора) - сомножитель образующего полинома РСЛОС АТР, соответствующий неприводимому полиному, должен быть равен примитивному образующему полиному РСЛОС ГТП;

4) многовходовый АТР на основе кодов Рида-Соломона, исправляющего одиночные ошибки (локализация одиночного ошибочного вектора) - корень первого сомножителя образующего полинома РСЛОС АТР должен быть равен корню примитивного образующего полинома РСЛОС ГТП;

5) многовходовый АТР на основе кодов Рида-Соломона, исправляющего ошибки кратности t (локализация t ошибочных векторов) - корень первого сомножителя образующего полинома РСЛОС АТР (элемент поля Галуа со степенью j) должен быть равен корню примитивного образующего полинома РСЛОС ГТП; корни остальных сомножителей - элементы поля Галуа со степенями j+1, j+2, j+3 и т.д.

Выводы

Выполнен анализ эффективности компактного тестирования с локализацией ошибок в выходной тестовой реакции проверяемой комбинационной схемы. Предложен метод аналитического расчета сигнатур для исчерпывающего тестирования комбинационных схем при реализации генератора тестовых последовательностей и анализатора тестовых реакций на основе регистров сдвига с линейными обратными связями. Рассматриваются анализаторы тестовых реакций, построенные на основе циклических кодов Хэмминга, Боуза-Чоудхури-Хоквингема, Бартона, Рида-Соломона, позволяющие локализовать ошибки в тестовой реакции. Получена оценка меры эффективности компактного тестирования комбинационных схем, на основе которой предложены рекомендации по выбору порождающих полиномов регистров сдвига с линейными обратными связями для различных вариантов компактного тестирования с локализацией ошибок. Полученные результаты могут найти применение для встроенного самотестирования или внешнего тестового оборудования средств вычислительной техники.

Литература

1. Richard E.Blahut. Algebraic Codes for Data Transmission/ Cambridge University Press, 2012. – 498 p.
2. Дяченко О.Н., Дяченко В.О. Альтернативный метод укорачивания циклических кодов // Электронные информационные системы. 2017. №1 (12). С. 94–100.
3. Ярмолик В.Н., Калоша Е.П. Эффективность сигнатурного анализа в самотестирующихся СБИС // Электрон. моделирование. 1992. 14, №3. С.51-56.
4. Дяченко О.Н. Анализ сигнатурной тестируемости комбинационных схем // Автоматика и вычислительная техника. - 1990. - №5. С.85-89.
5. Ярмолик В.Н., Калоша Е.П. Эффективность сигнатурного анализа в самотестирующихся СБИС // Электрон. моделирование. 1992. 14, №3. С.51-56.
6. Ершов А.Н., Петров С. В., Пятошин Ю.П., Коханько Д. В., Зяблов В.В. и др. Улучшение радиационной стойкости памяти с помощью помехоустойчивых кодов // Ракетно-космическое приборостроение и информационные системы. 2014, том 1, выпуск 4, С. 42–49.
7. Дяченко В.О., Дяченко О.Н. Циклическое кодирование цифровой информации на основе двойственных полиномов // Современные тенденции развития и перспективы внедрения инновационных технологий в машиностроении, образовании и экономике: материалы II Международной научно-практической конференции (Азов, 19 мая 2015 г.) – Ростов н/Д, ДГТУ, 2015. С. 71-76.
8. Дяченко В.О., Зинченко Ю.Е., Дяченко О.Н. Исследование способов проектирования кодов Рида-Соломона // Інформаційні управляючі системи та комп'ютерний моніторинг (ІУС КМ-2014): V Всеукраїнська науково-технічна конференція студентів, аспірантів та молодих вчених, 22-23 квітня 2014 р., м. Донецьк : зб. доп. / Донец. національний. техн. ун-т; редкол. В.А.Світлична. – Донецьк: ДонНТУ, 2014. – в 2 тт. – т.2. – С. 72-78.

9. Питерсон У., Уэлдон Э. Коды, исправляющие ошибки. – М.: Мир, 1976. – 595 с.: ил.

Дяченко О.Н., Зинченко Ю.Е., Дяченко В.О. Применение методов помехоустойчивого кодирования для компактного тестирования цифровых схем. *Выполнен анализ эффективности компактного тестирования комбинационных схем, учитывающего структуру генератора тестовых последовательностей, анализатора тестовых реакций, построенных на основе методов циклического кодирования, и характер распределения ошибок в тестовой реакции. Предложен метод расчета сигнатур, отличающийся от известного, в выборе степенного обозначения тестовых наборов вместо двоичного. Показано, что главное достоинство аналитического вычисления сигнатур являются не столько значения компактных оценок, а вывод о сигнатурной тестируемости комбинационных схем. Этот вывод распространяется на многовходовые анализаторы тестовых реакций; для структур с посимвольным перемежением; для порождающих полиномов, как в конфигурации Галуа, так и в конфигурации Фибоначчи. Предложены рекомендации по выбору порождающих полиномов регистров сдвига с линейными обратными связями для различных вариантов компактного тестирования.*

Ключевые слова: *Генератор тестовых последовательностей, анализатор тестовых реакций, порождающий полином, циклические коды.*

Dyachenko O. N., Zinchenko Y.E., Dyachenko V. O. Application of methods of antinoise coding for compact testing of digital circuits. *The efficiency of compact testing of combinational circuits that takes into account the structure of the generator of test sequence, analyzer of test reactions based on the methods of cyclic encoding and the distribution of errors in a test response, under study. The calculation method signatures differ from the well-known in the selection of a power notation of test cases instead of binary is proposed. It is shown that the main advantage of the analytical evaluation of the signatures are not so much values compact evaluations, and the conclusion of signature testability of combinational circuits. This conclusion is extended to multi-analyzers test reactions; for structures with symbol-by-symbol interleaving; for the generator polynomials, in Galois configuration and the configuration of the Fibonacci. Recommendations on the choice of the generator polynomials of linear feedback shift register for different variants of compact testing are proposed.*

Keywords: *Generator of test sequences, analyzer of test reactions, linear feedback shift register, generator polynomial, cyclic codes.*

Статья поступила в редакцию 20.09.2017
Рекомендована к публикации д-ром техн. наук В.Н. Павлышом