ВНЕДРЕНИЕ ЦИФРОВЫХ ВОДЯНЫХ ЗНАКОВ В LFSR-СТРУКТУРЫ

А. А. Иванюк, В. В. Сергейчик
Кафедра информатики, Белорусский государственный университет информатики и радиоэлектороники
Минск, Республика Беларусь
E-mail: vovasq@mail.ru, ivaniuk@bsuir.by

Рассматривается защита авторского права на IP-компоненты с помощью цифровых водяных знаков (ЦВЗ). Предлагается метод постановки динамических ЦВЗ в кодировке переключения для многополиномиальных LFSR, входящих в состав схем тестирования.

Введение

ЦВЗ представляет собой метод встраивания информации, применяемый с определенной целью, например для идентификации и защиты авторского права [1]. Процедура использования ЦВЗ состоит из двух этапов: встраивания и извлечения. В ходе этапа встраивания из исходного проектного описания с помощью метода постановки ЦВЗ и сообщения, идентифицирующего автора, получают новое описание, содержащее некоторое свойство, которое позволяет доказать авторство. В ходе извлечения ЦВЗ процедурой обнаружения определяется присутствие или отсутствие сообщения схеме.

I. Существующие подходы

Разработано большое количество методов ЦВЗ, работающих на различных уровнях абстракции, начиная с бит-образа [2] или технологического описания [1] и заканчивая системным уровнем [3]. Описываемый в данной работе метод совмещает задачу защиты IP-компонента с задачей тестирования. Методы ЦВЗ, связанные с тестированием: ЦВЗ в кодировке состояний тестовых автоматов в методологии проектирования для тестирования [4], ЦВЗ в перестановке ячеек сканирующей цепи [3], инверсия значений ячеек сканирующих цепей в зависимости от битов ЦВЗ.

II. Variable-Rank LFSR

В задачах контроля и диагностики средств вычислительной техники регистры сдвига с линейной обратной связью (Linear Feedback Shift Register, LFSR) используются в качестве генераторов псевдослучайных тестовых и адресных последовательностей, схем сжатия результатов – сигнатурных анализаторов [5]. LFSR строится на базе неприводимого полинома. Распространены конструкции, использующие несколько полиномов. Одна из них, Variable-Rank LFSR (VR-LFSR) [6], предлагается в качестве основы для постановки ЦВЗ, рис. 1. Схема включает декодер, который коммутирует разряды цепи обратной связи LFSR, соответствующие полиному с заданным кодом.

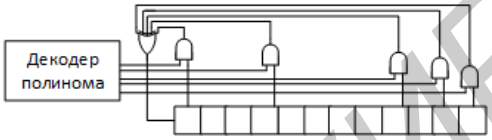

Рис. 1 – VR-LFSR

Кодирование полиномов в декодере зависит от реализации. Наложив ограничения на выбор кодирования, в частности на отображение полином/код, можно получить несколько вариантов ЦВЗ. В простейшем случае код представляет собой m-разрядное число, уникально идентифицирующее один из 2^m полиномов в VR-LFSR. ЦВЗ разбивается на фрагменты также по m бит каждый. При извлечении ЦВЗ VR-LFSR инициализируется полиномом в определенном начальном состоянии, которое играет роль ключа. Далее LFSR функционирует на протяжении $2n$ тактов (где n – максимальная разрядность VR-LFSR). После этого часть битов очередного состояния определяет новый код полинома. Транслируя код на выход можно получить очередную порцию ЦВЗ явно. Очевидным недостатком будут аппаратные затраты на извлечение: потребуется канал шириной m бит и дополнительная логика трансляции заданных значений на выход. Другим вариантом будет хранение всех позиций переключения на извлекающей стороне. Однако, возможно и неявное определение кодов по генерируемой последовательности длиной $2n$. В этом случае извлекающей стороне должно быть известно соответствие полином/код. С помощью алгоритма Берлекампа-Месси по $2n$ битам порожденной последовательности можно восстановить полином [7]. Далее из таблицы соответствия полином/код по полиному определяется его кодировка, в свою очередь являющаяся порцией ЦВЗ.

III. Пример

Дан VR-LFSR с отображением код/полином: $00 \longrightarrow x^4 + x^3 + 1$, $01 \longrightarrow x^4 + x + 1$, $10 \longrightarrow x^5 + x^3 + 1$, $11 \longrightarrow x^8 + x^6 + x^5 + x + 1$. Стартовое состояние (ключ извлечения) 11000110. ЦВЗ 1010 0110 1101 1011. Схема приведена на рис. 2 и включает следующие основные элементы: контроллер, декодер и LFSR. Контроллер трансли-

рует на декодер биты из состояния LFSR на позициях, заданных отображением в зависимости от значения счетчика порций. Контроллер генерирует сигнал переключения значения полинома (switch). Декодер в зависимости от принятого кода выдает на LFSR требуемый полином и индекс его старшего бита (msbIndex). LFSR функционирует в соответствии с текущим полиномом и значением максимального индекса.

Начиная со стартового LFSR проходит следующие состояния: 8d, 1a, 35, 6b, d6, ac, 58, b1, 62, c5, 8a, 15, 2a, 55, aa. В состоянии aa (**10**101010) в соответствии со значением счетчика порций (0) выбирается отображение $0 \longrightarrow (7, 6)$. Биты с этими индексами представляют собой код (10) полинома, на который произойдет переключение. После переключения LFSR генерирует следующие биты: 0,1,0,1,1,0,0,1,1,1,1,1,0,0,0,1. С помощью алгоритма Берлекампа-Месси можно убедиться, что последовательность соответствует полиному x^5+x^3+1 с кодом 10. Оставшиеся биты ЦВЗ извлекаются подобным образом.

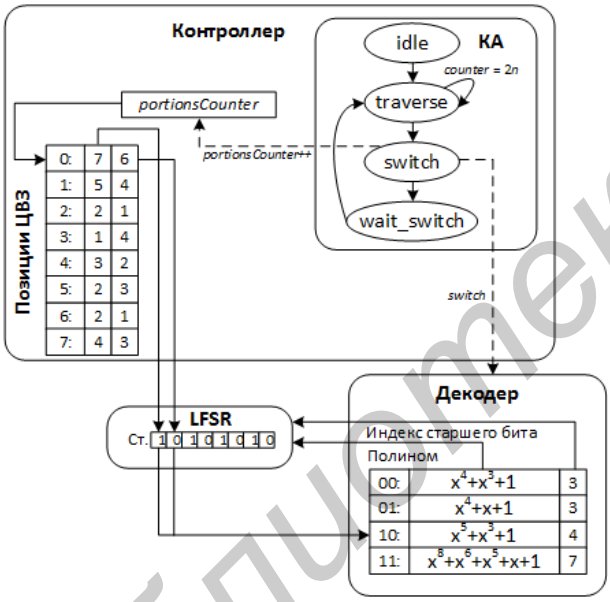

Рис. 2 – Пример

Оценить вероятность ложного обнаружения P_u можно следующим образом. Вероятность конкретного m-битового кода в М-последовательности длины 2^{n-1} битов составляет $2^{n-m}/2^n$. Вероятность обнаружить незапланированный ЦВЗ длины $L_{wm} = m \cdot z$ (z — количество порций) в случае перебора всех начальных состояний равна: 2^{n-m*z}. Вероятность выбора последовательности двух бит из последовательности длины n будет: $2^{n-2}/2^n = 1/4$. Для примера вероятность совпадения будет порядка $2^8 \cdot (1/4)^8 = 2^8 \cdot 1/(2^{16}) = 1/2^8$.

IV. Результаты реализации

Для проверки использовалась IDE Xilinx 14.4 WebPack, синтез проводился для бюджетной FPGA xc6slx75. Эксперименты ставились для разного количества полиномов. Результаты приводятся в табл. 1, где n — это максимальная разрядность VR-LFSR; L_{wm} — длина ЦВЗ; 5, 6, 7-й столбцы указывают результаты синтеза: регистры, LUT, частоту в МГц; 8-й указывает вероятность ложного обнаружения. Звездочками помечены случаи, в которых полный перебор ключей трудно достижим.

Таблица 1 – Результаты экспериментов

№	n	L_{wm}	2^m	Рег.	LUT	F	P_u
1	8	16	4	28	42	347	2^{-8}
2	32	160	32	94	212	237	2^{-128}
3	64	160	32	134	349	177	2^{-96*}
4	128	160	32	204	672	176	2^{-32*}

Наиболее перспективным представляется поиск способов совмещения подобного ЦВЗ с тестами с высокой покрывающей способностью. В результате, при попытке удаления ЦВЗ будет разрушено ценное свойство всего модуля тестирования – высокая обнаруживающая способность. Тестирование в смешанном режиме [6] – один из вероятных кандидатов. Сначала LFSR функционирует в автономном режиме достаточно продолжительное время (порядка 10000 тактов), в ходе которого обнаруживается большинство неисправностей. Для оставшихся используются целенаправленные тесты, которые строятся на основе стартового значения *seed*, выбранного порцией ЦВЗ полинома и значений, порождаемых LFSR за $2n$ тактов.

1. G. Qu, M. Potkonjak, Intellectual Property Protection in VLSI Design Theory and Practice – Dor-drecht: Kluwer Publishing, 2003. – 203 p.
2. Ziener, D. Techniques for Increasing Security and Reliability of IP Cores Embedded in FPGA and ASIC Designs / D. Ziener. – Erlangen, 2010. – 325 p.
3. Cui, A. A Hybrid Watermarking Scheme for Sequential Functions / A. Cui, C. H. Chang, L. Zhang // IEEE ISCAS, 2011. – Rio de Janeiro, 2011. – P. 2333 – 2336.
4. Zhang, L. State Encoding Watermarking for Field Authentication of Sequential Circuit Intellectual Property / L. Zhang, C. H. Chang // IEEE ISCAS, 2012. – Seoul, 2012. – P. 3013 – 3016.
5. Ярмолик, С. В. Маршевые тесты для самотестирования ОЗУ / С. В. Ярмолик, А. П. Занкович, А. А. Иванюк // Монография. – Минск, «Издательский центр БГУ», 2009. – 269 с.
6. Kim, H. Increasing Encoding Efficiency of LFSR Reseeding Based Test Compression / H. Kim, S. Kang // IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems. – 2006. – Vol. 25. – Pp. 913 – 917.
7. Блейхут, Р. Теория и практика кодов, контролирующих ошибки – М.: Мир, 1986. – 576 с.