ПОСТАНОВКА ЦИФРОВЫХ ВОДЯНЫХ ЗНАКОВ ВСТРОЕННЫМ СРЕДСТАВМИ САМОТЕСТИРОВАНИЯ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Сергейчик В. В.

Иванюк А. А. – д-р. техн. наук, доцент, проф.

В работе предлагается метод постановки водяных знаков в ходе самотестирования схемы оперативного запоминающего устройства (ОЗУ).

Память является неотъемлемой частью большинства современных вычислительных систем. По данным [1] доля памяти на кристалле составляет порядка 50 – 90%. При этом отказы ОЗУ составляют до 70% отказов вычислительных систем. Поэтому обнаружение неисправностей ОЗУ представляет актуальную проблему. Другой важной проблемой является защита цифровых устройств от несанкционированного использования. Ущерб от пиратства и подделок в индустрии оценивается в 169 млрд. долларов в год [2]. Подходы защиты включают: шифрование компонент интеллектуальной собственности, активное и пассивное измерение, идентификацию, обфускацию, постановку цифровых водяных знаков (ЦВЗ) и отпечатков пальцев.

Суть технологии ЦВЗ состоит во встраивании информации в проект цифрового устройства, осуществляемом с определенной целью, например для идентификации и защиты авторского права. Различают статические и динамические ЦВЗ [3]. Статические ЦВЗ хранятся непосредственно в проектном описании некоторого уровня абстракции. Динамические могут быть обнаружены в ходе функционирования защищаемого цифрового устройства, например, по изменению выходных сигналов. Динамические ЦВЗ особенно эффективны в силу того, что они проявляются только при подаче определенных входных данных.

Распространенным методом тестирования ОЗУ являются маршевые тесты, в ходе которых для каждой ячейки памяти выполняется последовательность операций (чтение/запись 0 и 1). Неразрушающее маршевое тестирование позволяет сохранить содержимое ячеек памяти благодаря использованию операций чтения прямого или инвертированного значения во временный буфер и записи прямого или инвертированного значения из буфера в память. Для анализа реакции ОЗУ на тестовые воздействия используются методы получения компактных оценок, например, сигнатурный анализ [1]. При этом сначала для содержимого памяти вычисляется эталонная сигнатура, а затем в ходе тестирования вычисляется рабочая сигнатура. Неравенство эталонной и рабочей сигнатур свидетельствует о наличии неисправности.

Предлагаемый метод постановки ЦВЗ реализуется на базе неразрушающего тестирования. Сигнатурный анализ осуществляется с использованием сдвигового регистра с линейной обратной связью (LFSR). Данный метод постановки ЦВЗ относится к классу динамических ЦВЗ.

Схема, выполняющая самотестирование и постановку ЦВЗ, состоит из следующих элементов (рисунок 1, *а*): RAM (Random Access Memory) – тестируемое ОЗУ, BIST (Built-In Self-Test) – устройство самотестирования, осуществляющее генерацию последовательностей адресов, чтение, запись и инверсию данных, SA (Signature Analyzer) – сигнатурный анализатор, на котором сжимается последовательность значений памяти, Start – сигнал извлечения водяного знака, OTP Reg (One-Time Programmable Register) – ПЗУ, содержащее фиксированную последовательность извлечения водяного знака, Key Reg – регистр, в котором содержится начальное значение сигнатурного анализатора, требуемое для извлечения водяного знака, wm – регистр для хранения водяного знака. В режиме тестирования (Start = ‘0’) на сигнатурном анализаторе осуществляется сжатие значений из RAM, в режиме извлечения (Start = ‘1’) – сжимаются значения, содержащиеся в OTP Reg.

Процесс постановки ЦВЗ состоит из нескольких шагов. Сначала выбирается последовательность символов, идентифицирующая автора (т. н. пользовательское сообщение), например название компании изготовителя. С помощью хэш-функции рассчитывается дайджест этого сообщения. Первая часть дайджеста, соответствующая по длине размерности SA, используется в качестве ключа извлечения ЦВЗ. Она держится в секрете и передается извне в Key Reg при извлечении. Вторая часть используется в качестве водяного знака.

Последовательность состояний, в которые переходит SA при сжатии значений ОЗУ, можно рассматривать как ориентированный граф, вершинами которого являются значения SA. Переходы между вершинами помечаются значением бита, переводящим SA в следующее состояние.

На следующем шаге формируется последовательность извлечения ЦВЗ. Для этого в графе выбирается путь, обладающий специальным свойством. Начальным состоянием при обходе графа выступает первое слово дайджеста. Затем от него строится путь, в котором четность количества единиц каждого посещаемого состояния соответствует очередному биту ЦВЗ (четное – 0, нечетное – 1). Значение бита над переходом в очередное состояние становится частью последовательности извлечения. Такое построение возможно из-за того, что для любого состояния два следующих всегда отличаются одним битом, а значит имеют различное число единиц. ЦВЗ относится к классу динамических, т. к. в явном виде ЦВЗ не присутствует в защищаемом компоненте, а проявляется в процессе его функционирования.

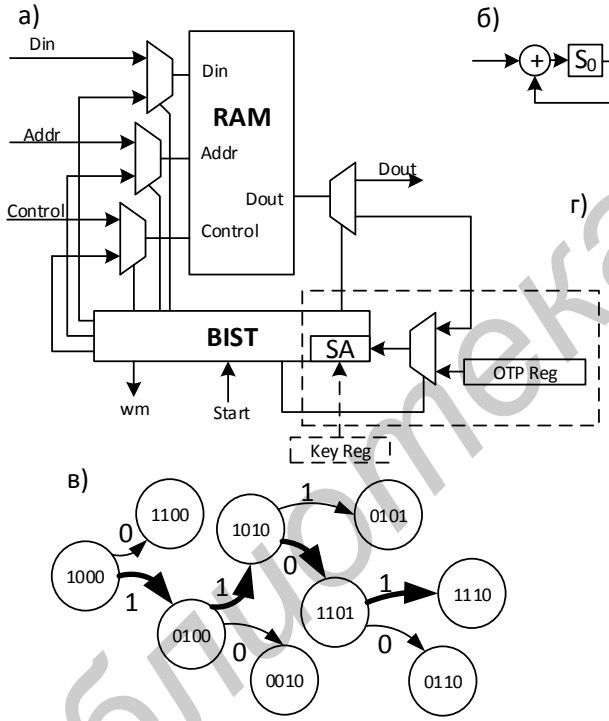
Рассмотрим пример: сигнатурный анализатор представляет собой LFSR с порождающим полиномом $1 + x + x^4$ (показан на рисунке 1, *б*), дайджест пользовательского сообщения: 1000 1011. Первая часть 1000

– будет использоваться в качестве ключа извлечения. Из состояния 1000 возможны два перехода: при 0 – 1100, при 1 – 0100. Первый бит ЦВЗ равен 1, поэтому выбирается состояние, имеющее нечетное число единиц: 0100. Таким образом, первый бит последовательности извлечения равен 1. Процесс повторяется до тех пор, пока не будет построена вся последовательность извлечения (1101). На рисунке 1, ***в)*** показан фрагмент графа и выделен путь при извлечении. На рисунке 1, *г)* показаны различные последовательности извлечения, соответствующие водяному знаку 1011 и произвольному начальному состоянию. Затем последовательность извлечения заносится в OTP Reg. Следует отметить, что для внедрения ЦВЗ весь граф строить не нужно.

Для запуска процесса извлечения устанавливается сигнал Start, после этого в SA в качестве начального значения записывается содержимое Key Reg, введенное пользователем. Затем происходит сжатие на SA содержимого OTP Reg. При этом значение четности количества единиц состояния SA на каждом такте заносится в регистр водяного знака или передается напрямую по сигнальной линии wm.

Важнейшей характеристикой ЦВЗ является вероятность совпадения P_u, указывающая на возможность того, что незапланированный ЦВЗ будет обнаружен в проектном описании [4]. В данном подходе P_u зависит от длины водяного знака. При этом, если длина ЦВЗ равна длине начального состояния, то для данной последовательности извлечения существуют все значения ЦВЗ, т. е. можно провести атаку Ghost Search стоимостью линейного перебора $m*2^N$ значений, где N – размерность состояния; m – число разрядов ЦВЗ. Однако если длина ЦВЗ превышает длину начального состояния, то присутствуют уже не все возможные комбинации, а только 2^N из 2^m возможных (см. рисунок 1, *д*). Таким образом, вероятность совпадения будет порядка $1/2^{m-N}$. Например, для m = 160 и N = 32 значение вероятности совпадения $P_u = 2{,}9*10^{-39}$.

Одним из усовершенствований может быть введение в схему модуля физически неклонируемой функции (ФНФ), например, с целью генерации ключа, уникального для каждой интегральной схемы.



г)

St/wm	1	0	1	1
0000	1	0	0	1
0001	0	0	0	1
0010	0	1	1	1
0011	1	1	1	1
0100	0	1	0	0
0101	1	1	0	0
0110	1	0	1	0
0111	0	0	1	0
1000	**1**	**1**	**0**	**1**
1001	0	1	0	1
1010	0	0	1	1
1011	1	0	1	1
1100	0	0	0	0
1101	1	0	0	0
1110	1	1	1	0
1111	0	1	1	0

д)

St/Ext	1	1	0	1	1
0000	1	1	1	0	0
0001	0	1	0	0	1
0010	0	0	1	1	0
0011	1	0	0	1	1
0100	0	0	0	0	1
0101	1	0	1	0	0
0110	1	1	0	1	1
0111	0	1	1	1	0
1000	**1**	**0**	**1**	**1**	**1**
1001	0	0	0	1	0
1010	0	1	1	0	1
1011	1	1	0	0	0
1100	0	1	0	1	0
1101	1	1	1	1	1
1110	1	0	0	0	0
1111	0	0	1	0	1

Рис. 1. *а)* схема BIST с возможностью постановки ЦВЗ; *б)* LFSR, заданный полиномом $1 + x + x^4$; ***в)*** фрагмент графа переходов и состояний SA; *г)* таблица соответствия начального состояния SA и последовательности извлечения для заданного ЦВЗ; *д)* таблица соответствия начального состояния и возможных ЦВЗ для заданной последовательности извлечения.

Широкое применение и растущая важность средств встроенного самотестирования в современных вычислительных системах открывает возможности для использования их в задачах защиты цифровых устройств от несанкционированного использования.

Список использованных источников:

1. 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.
2. Can EDA Combat the Rise of Electronic Counterfeiting? / F. Koushanfar [et al.] // Design Automation Conference. – San Francisco, USA, 2012. – P. 133–137.
3. A Public-Key Watermarking Technique for IP Designs / A. Abdel-Hamid [et al.] // Design, Automation and Test in Europe, Proceedings. – 2005. – Vol. 1. – P. 330–335.
4. Torunoglu, I. Watermarking-Based Copyright Protection of Sequential Functions / I. Torunoglu, E. Charbon // IEEE J. of Solid-State Circuits. – 2000. – Vol. 35. – P. 434–440.