АППАРАТНАЯ ЗАЩИТА ЦИФРОВЫХ УСТРОЙСТВ

***Л.А. Золоторевич*[1]**

[1]*Белорусский государственный университет информатики и радиоэлектроники, г. Минск, Беларусь*

В последнем десятилетии стала актуальной проблема защиты и дополнительного контроля проектов СБИС с целью обнаружения несанкционированного стороннего вмешательства в проект с разными основополагающими целями. Подобные действия являются преднамеренными и тщательно скрываемыми, что осложняет и без того достаточно сложную проблему верификации проектов и препятствует прямому применению существующих методов тестирования и функционального контроля СБИС [1,2].

Как развитие теории контролепригодного проектирования (Design-for-Testability - DfT) в работе [3] предлагается подход к проектированию Design for-Trust - DfTr, который дополнительно включает средства для контроля и предотвращения аппаратных атак при проектировании и изготовлении СБИС.

В работе [4] проанализированы различные модели процесса злонамеренного искажения проекта, описывающие условия, при которых подобное искажение может внедриться в цифровую систему. В числе возможных источников искажений рассматриваются поставщики базовых функциональных блоков интеллектуальной собственности (IP's), которые приобретаются разработчиками СнК, собственно разработчики СнК, а также кремниевые фабрики – изготовители СнК.

В докладе предлагается алгоритм логической обфускации и кодирования цифровых устройств, представленных на структурном уровне, на основе применения методов и средств тестового контроля.

Обфускация и логическое кодирование цифрового устройства на структурном уровне

Для блокирования попыток внешнего вмешательства в проект цифровой системы на структурном уровне одним из методов является логическое кодирование структурной реализации, которое обеспечивает доступ к объекту только авторизованным пользователям [5]. Метод обеспечивает сокрытие функциональности проекта на основе использования ключа, применение которого выводит систему в область правильного функционирования.

Чтобы защитить комбинационную схему с помощью k-разрядного ключа, предлагается простая процедура, которая требует включения в схему k дополнительных вентилей [5]. Во-первых, выбираются и сопоставляются с битами {y} ключа k линий схемы $\{w_i\}$. Каждая выбранная линия w_i отключается от приемников сигнала, а на место обрыва подключается вентиль XOR или вентиль XNOR с выходной линией связи w_i', на которой формируется сигнал, управляющий соответствующими приемниками сигнала вентиля w_i. При подключении вентиля XOR (XNOR) $w_i' = w_i \oplus y_i$ ($w_i' = w_i \overline{\oplus} y_i$), где y_i - соответствующий бит ключа. Выбор вентиля XOR или XNOR зависит от выбранного значения бита ключа: если выбранное значение y_i равно 0, то $w_i' = w_i \oplus y_i$, если y_i равно 1, то $w_i' = w_i \overline{\oplus} y_i$.

На рис. 1, а приведен фрагмент логической схемы, а на рис.1,б проиллюстрирована основная идея логического кодирования. Выход элемента C_1 отключен от нагрузки (элементы D_1 и D_2), и подключен к одному из входов дополнительного «ключевого» элемента типа XOR CC_1, на второй вход которого поступает внешний входной сигнал K_1 однобитового ключа. Схема будет работать в требуемом режиме только в том случае, если сигнал на входе K_1 будет равен 0. В противном случае на выходе элемента XOR CC_1 будет формироваться сигнал, инверсный правильному.

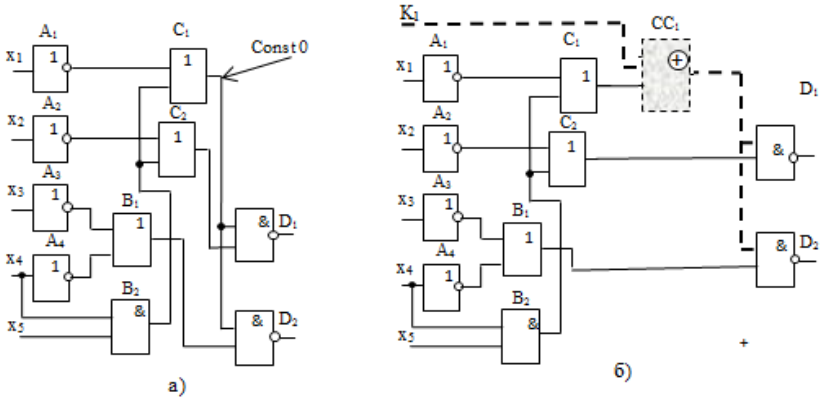

Рис. 1. Фрагмент логической сети; а) - исходная комбинационная схема; б) - схема с однобитовым ключом

Вместо элемента CC_1 типа XOR может быть установлен элемент XNOR. В этом случае однобитовый правильный ключ, поступающий на вход K_1, равен 1. Заметим, что применение неправильного ключа равносильно появлению неисправности константного типа «const 0» («const 1») на выходе элемента C_1 в зависимости от входного набора и истинного значения сигнала на C_1, равного 1 (0). Этот факт является важным, так как позволяет формализовать задачу обфускации на основе применения методов и средств тестового контроля цифровых устройств.

При воздействии входного набора X = (00000) и неправильного ключа $K_1 = 1$ (рис.1) на выходах схемы D_1, D_2 формируются сигналы (11), в то время как при правильном ключе $K_1 = 0$ - (00). Так же поведет себя схема (рис. 1) при неисправности «const 0» на выходе элемента C_1. Таким образом, входной набор X = (00000) является тестом контроля данной неисправности и в то же время при отсутствии неисправности искажает выходное состояние схемы при подаче неправильного ключа.

Таким образом, для сокрытия функциональности схемы необходимо добавить в некоторые линии схемы дополнительные элементы и определить правильный код, искажение которого выводит схему из области правильного функционирования. Заметим, что при воздействии входно-

го набора X = (01110) и неправильного ключа $K_1 = 1$ (рис.1) на выходах схемы D_1, D_2 появятся сигналы (11) как и при правильном ключе, так как входной набор X = (01110) не является тестом контроля неисправности «const 0» на выходе элемента C_1.

Основная задача, которая должна быть решена при эффективной практической реализации данной общей идеи, заключаются в том, чтобы определить оптимальное множество внутренних линий схемы и количество ключевых элементов для создания максимальных трудностей для злоумышленника по поиску правильного ключа.

Для определения степени защищенности устройства при его кодировании принимается расстояние Хэмминга (HD), которое позволяет количественно определить степень отличия правильной реакции устройства от ошибочной реакции. Для того, чтобы затруднить восстановление правильного ключа, необходимо обеспечить наименьшую корреляцию между правильными и не правильными выходными векторами, что достигается при HD = 0,5.

Применение методов и средств тестового диагностирования для защиты цифровых устройств от вредоносных искажений

При выборе и включении очередного вентиля при кодировании логических устройств необходимо проводить анализ на влияние эффекта маскирования неисправностей, который способен блокировать эффект кодирования. Кроме того, целесообразно учитывать, что для некоторых линий отсутствует возможность активизации пути от данной линии к выходам устройства.

Сведем задачу кодирования к поиску неисправностей константного типа кодируемой структуры, обнаруживаемых на большем количестве выходных линий на максимальном количестве входных векторов. В отличие от решения, принятого в работе [6], рассмотрим более эффективный подход, основанный на применении метода сквозного вычисления неисправностей, покрываемых рассматриваемым входным вектором (конкурентно-дедуктивного моделирования) вместо моделирования каждой неисправной модификации схемы на определенном множестве случайных входных наборов с целью оценки степени влияния неисправностей на выходы схемы [7]. Метод конкурентно-дедуктивного

моделирования неисправностей основан на моделировании исправной схемы и позволяет за один проход моделирования определять все неисправности константного типа, обнаруживаемые на моделируемом входном наборе. За счет того, что моделируется только исправная схема, эффективность решения существенно повышается по сравнению с моделированием одиночной неисправности на множестве входных векторов.

Вначале вычисляются неисправности, обнаруживаемые на моделируемом ограниченном множестве случайных входных наборов. Затем по результатам анализа определяются те неисправности, которые обнаруживаются наибольшим числом наборов и указывают преимущественные линии схемы для вставки ключевых вентилей. В то же время численное ограничение количества моделируемых входных воздействий [8] ограничивает возможность поиска наиболее эффективного решения.

В докладе предлагается подход, основанный на построении теста в классе неисправностей константного типа [7] и его применении на первом этапе кодирования. В рамках данного подхода вместо использования заранее определенного числа случайных входных воздействий (как, например, 100 в работе [8]), применятся тестовая последовательность входных векторов, которая обеспечивает близкое к полному покрытию неисправностей константного типа кодируемой структуры.

По результатам сквозного моделирования неисправностей определяются наиболее подходящие линии для подключения ключевых вентилей. Для повышения эффективности кодирования кроме указанных ключевых вентилей добавляются управляющие вентили. Если ключевой вентиль управляется одним битом ключевого кода, то вероятность того, что данный вентиль будет приведен в действие $P = 0{,}5$. Это означает, что только половина ключевых вентилей повлияет на результат функционирования схемы при применении неправильного ключа. Для того, чтобы увеличить вероятность P и усилить влияние неправильного бита кодового слова на результат функционирования схемы, применим управляющие вентили, с помощью которых можно объединить биты кодового слова в группы, использовав при этом их выходы в качестве входов ключевых вентилей. В таком случае будет реализовано групповое воздействие нескольких битов кодового слова на активизацию клю-

чевого вентиля. Если хотя бы один из ключевых входов, включенных в группу, принимает неправильное значение, ключевой вентиль окажется активированным. Для этого с каждым ключевым вентилем используется управляющий вентиль. При этом, если применяется двухвходовый управляющий вентиль, то вероятность активизации ключевого вентиля возрастает с 0,5 до 0,75, в случае трехвходового вентиля - 0,88, а при пятивходовом – 0,97 (только один ключевой вектор из 32 векторов данной группы является правильным).

ЛИТЕРАТУРА

1. *Zolotorevich L.A.* Project verification and construction of superchip tests at the RTL level // Automation and Remote Control. – USA, NY, Plenum Press 2013. – Vol. 74, Issue 1. P. 113-122.
2. *Zolotorevich L.A., Il'inkova A.V.* Development of tests for VLSI circuit testability at the upper design levels // Automation and Remote Control. – USA, NY, Plenum Press. –-Vol. 71 Issue 9. – September 2010. – P. 1888-1898.
3. *Rajendran J., Sam M., Sinanoglu O., Karri R.* Security analysis of integrated circuit camouflaging //ACM SIGSAC conference on Computer & communications security. – Germany, Berlin. 04 - 08 November 2013.– P. 709-720.
4. *Xiao K., Forte D., Jin Y., Karri R., Bhunia S., Tehranipoor M.* Hardware Trojans: Lessons learned after one decade of research // ACM transactions on design automation of electronic system. – Vol. 22. – No.1. – 2016.
5. *Roy J., Koushanfar A. F., Markov I. L.* EPIC: Ending Piracy of Integrated Circuits // IEEE Computer. – 2010. – Vol. 43. – No. 10. – P. 30-387.
6. *Karousos N., Pexaras K., Karybali I. G., Kalligeros E.* Weighted Logic Locking: A New Approach for IC Piracy Protection // IEEE 23rd International Symposium on On-Line Testing and Robust System Design (IOLTS). – 2017. – P. 221-226.
7. *Золоторевич Л.А.* Исследование методов и средств верификации проектов и генерации тестов МЭС // Сборник научных трудов всероссийской научно-технической конференции "Проблемы разработки перспективных микроэлектронных систем – МЭС-2006". Под общ. Ред. А.Л. Стемпковского. – М.: ИППМ РАН. 2006. – С. 163-168.
8. *Yasin M., Rajendran J., Sinanoglu O., Karri R.* On Improving the Security of Logic Locking // Computer-Aided Design of Integrated Circuits and Systems. IEEE Transactions on 2016. –Vol. 35. – No. 9. – P. 1411-1424.