УДК 519.873:519.718.7

КОДИРОВАНИЕ ЛОГИЧЕСКИХ СХЕМ ДЛЯ ЗАЩИТЫ ОТ НЕАВТОРИЗОВАННОГО ПОЛЬЗОВАТЕЛЯ

Л.А. Золоторевич
Белорусский государственный университет информатики и радиоэлектроники, Минск, Беларусь, zolotorevichla@bsuir.by

Наиболее сложными проблемами проектирования современных систем на кристалле (СнК), требующими разработки эффективных методов и средств, являются проблемы верификации проектов, построения тестов и создания систем контроля [1,2]. Эти проблемы являются достаточно сложными, но естественными, возникающими непреднамеренно и должны решаться в режиме благоприятствующего проектирования. В то же время в последние годы возникла потребность в дополнительном контроле проектов с целью обнаружения последствий несанкционированного вмешательства в проекты. Целью подобного вмешательства может быть внедрение троянов, ухудшение характеристик, экономические преступления и др. Подобные действия являются преднамеренными и тщательно скрываемыми, что ограничивает возможности существующих методов тестирования и функционального контроля СБИС. 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 докладе дается сравнительный анализ методов кодирования цифровых устройств на уровне их структурного представления с целью предотвращения хищения и злонамеренного искажения проектов. Предлагается метод управляемого логического кодирования на основе использования методов и средств тестового диагностирования.

Логическое кодирование обеспечивает доступ к объекту только авторизованным пользователям [3,4]. Этот подход предполагает сокрытие функциональности проекта на основе применения ключа, который переводит систему в область правильного функционирования. Кроме логического шифрования комбинационной схемы в литературе известен метод внедрения новых внутренних состояний в граф перехода для последовательностных устройств, но на сегодняшний день эффективность практического применения этого метода не установлена.

Подход, основанный на логическом кодировании структуры, базируется на включении в логическую сеть дополнительных вентилей, управляемых внешними логическими ключами, и применении обфускации струк-

туры объекта [5]. В такой постановке, если злоумышленник не владеет ключом, то ему недоступна внутренняя реализация структуры объекта.

Важнейшая задача структурной обфускации и логического кодирования заключается в том, чтобы максимально затруднить или сделать невозможным получение правильного ключа неавторизованным пользователем.

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 (в докладе обсуждаются известные в литературе предложения с использованием других типов вентилей). 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 $w_i' = w_i \overline{\oplus} y_i$.

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. Основная задача, которая должна быть решена при 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.

В работах [6,7] для определения множества линий структуры для кодирования применяется моделирование кодируемой схемы с последовательно вносимыми неисправностями и вычислении признаков $P_i = X_i * Y_i$, характеризующих моделируемую неисправность линии с точки зрения эффективности ее выбора при кодировании схемы. Здесь X_i – количество входных наборов, которые покрывают анализируемую неисправность, Y_i – количество выходных переменных, которые искажаются при появлении данной неисправности. По результатам анализа полученных признаков определяется множество внутренних линий схемы для кодирования.

В докладе предлагается свести задачу кодирования к поиску неисправностей константного типа кодируемой структуры, обнаруживаемых на большем количестве выходных линий и на максимальном количестве входных векторов [4]. Предложен алгоритм управляемого кодирования описаний цифровых устройств комбинационного типа на структурном уровне на основе применения средств тестового диагностирования. Пред-

ложенный алгоритм по сравнению с известными в литературе требует меньших вычислительных затрат и времени и проявляет устойчивость к восстановлению правильного ключа на основе «атаки SAT» [8]. Это обусловлено тем, что ключевые входы не связаны напрямую с ключевыми вентилями, а ключевые вентили активизируются не одним ключевым входом.

Применение метода сквозного вычисления множества покрываемых неисправностей на основе моделирования исправной схемы существенно сокращает объем вычислительных процедур.

Список литературы

1. Zolotorevich, L.A. Project verification and construction of superchip tests at the RTL level /L.A. Zolotorevich // Automation and Remote Control. – USA, NY, Plenum Press 2013. – Vol. 74, Issue 1. P. 113-122.
2. Zolotorevich, L.A. Development of tests for VLSI circuit testability at the upper design levels/ L.A. Zolotorevich, A.V. Il'inkova // Automation and Remote Control. – USA, NY, Plenum Press. –-Vol. 71 Issue 9. – September 2010.- P. 1888-1898.
3. Rajendran, J. Security analysis of integrated circuit camouflaging / J. Rajendran, M. Sam, O. Sinanoglu, R. Karri //ACM SIGSAC conference on Computer & communications security. – Germany, Berlin. 04 - 08 November 2013.– P. 709-720.
4. Золоторевич, Л.А. Модели неисправностей при верификации проектов и контроле цифровых систем / Л.А. Золоторевич // Компьютерные науки и информационные технологии: Материалы Междунар. науч. конф. – Саратов: Издат. центр «Наука», 2018. – ISBN 978-5-9999-2651. – С. 160-163. https://elibrary.ru/item.asp?id=35694605 (РИНЦ).
5. Roy, J. A. EPIC: Ending Piracy of Integrated Circuits / J. A. Roy, F. Koushanfar, I. L. Markov // IEEE Computer. – 2010. – Vol. 43. – No. 10. – P. 30-387.
6. Chakraborty, R. S. Security against Hardware Trojan through a Novel Application of Design Obfuscation / R. S. Chakraborty, S. Bhunia // IEEE/ACM International Conference on Computer-Aided Design. – 2009. – P. 113-116.
7. Karousos, N. Weighted Logic Locking: A New Approach for IC Piracy Protection / N. Karousos, K. Pexaras, I. G. Karybali, E. Kalligeros // IEEE 23rd International Symposium on On-Line Testing and Robust System Design (IOLTS). – 2017. – P. 221-226.
8. Yasin, M. On Improving the Security of Logic Locking / M.Yasin, J. Rajendran, O. Sinanoglu// Computer-Aided Design of Integrated Circuits and Systems. IEEE Transactions . – 2016. –Vol. 35. –No. 9. – P. 1411-1424.