МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИНСТИТУТ ОПТИКИ АТМОСФЕРЫ СО РАН им. В.Е. ЗУЕВА

НОВЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В ИССЛЕДОВАНИИ СЛОЖНЫХ СТРУКТУР

МАТЕРИАЛЫ
ДВЕНАДЦАТОЙ КОНФЕРЕНЦИИ С МЕЖДУНАРОДНЫМ УЧАСТИЕМ
4–8 июня 2018 г.

Мероприятие проведено при финансовой поддержке
Российского фонда фундаментальных исследований (проект № 18-07-20033)

Томск
Издательский Дом Томского государственного университета
2018

дится к выполнимости квантифицируемой конъюнктивной нормальной формы, решение которой является PSPACE-полной проблемой. Предлагаемый нами подход связан с перепрограммированием LUT на основе перестановки входных переменных.

Итак, задана комбинационная схема из вентилей (комбинационная часть последовательностной схемы). Необходимо покрыть некоторые ее подсхемы программируемыми блоками (LUTs), так чтобы иметь как можно больше возможностей восстановить корректное функционирование схемы. Предполагается, что сохранившиеся неисправности с большей вероятностью будут проявляться на линиях со слабой наблюдаемостью. Находится множество L таких линий. Предлагается несколько способов покрытия линий из этого множества вместе с соответствующим фрагментом подсхемы. Считается, что на рассматриваемой линии возможна произвольная, а не только константная как в работе [3], неисправность. В отличие от работы [3] мы допускаем неисправность нескольких линий одновременно. В результате покрытия фрагментов исходной схемы C из вентилей схема превращается в частично программируемую схему C_p, реализующую то же поведение, что и схема C. Заметим, что LUT со свободным входом программируется таким образом, что переменная, сопоставляемая свободному входу, является несущественной для запрограммированной функции.

Пусть m – число входов LUT, тогда функция C_{LUT} этого блока существенно зависит от (m-1) переменной. При обнаружении неисправности линии предполагается выполнить перепрограммирование связанного с ней программируемого блока, имеющего свободный вход. Пусть вход u_i блока связан с линией l, а u_m – свободный вход. Функция f_{LUT} извлекается из подсхемы покрываемой рассматриваемым LUT. При программировании LUT в отсутствии неисправности на линии l каждый единичный набор этой функции в пространстве (m-1) переменных заменяется двумя наборами в пространстве m переменных. В одном из них переменная u_m принимает значение 1, а в другом значение 0. При перепрограммировании LUT в случае обнаружения неисправности на линии реализуется функция:

$$f_{LUT}(u_i = 1) \wedge u_m \vee f_{LUT}(u_i = 0) \wedge \overline{u}_m .$$

Эта функция существенно зависит от (m-1) переменной: $u_1, \ldots, u_{i-1}, u_{i+1}, \ldots, u_m$. Новая функция получена из прежней перестановкой переменных: переменная u_i заменяется переменной u_m, в результате чего u_m становится существенной переменной. Каждый единичный набор новой функции в пространстве (m-1) переменных заменяется двумя наборами в пространстве m переменных. В одном из них переменная u_i принимает значение 1, а в другом значение 0. Переменная u_i становится несущественной, неисправность линии l маскируется.

Литература

1. *Matrosova A., Ostanin S., Kirienko I.* Increasing manufacturing yield using partially programmable circuits with clb implementation of incompletely specified boolean function of the corresponding sub-circuit // Proc. of IEEE 18th International Symposium on Design and Diagnostics of Electronic Circuits and Systems. Belgrade, Serbia, 2015. P. 267–270.
2. *Matrosova A., Ostanin S., Andreeva V.* Patching circuit design based on reserved CLBs // Proc. of 20th IEEE International Conference on Automation, Quality and Testing, Robotics. Cluj-Napoca, Romania, 2016. P. 49–54.
3. *Yamashita S., Yoshida H., Fujita M.* Increasing yield using partially-programmable circuits // Proc. of Workshop on Synthesis And System Integration of Mixed Information technologies (SASIMI). 2010. P. 237–242.
4. Jo S., Matsumoto T., Fujita M. SAT-based automatic rectification and debugging of combinational circuits with LUT insertions // Proc. Of IEEE Asian Test Symposium. 2012. P. 19–24.

ОБНАРУЖЕНИЕ И МАСКИРОВАНИЕ ВРЕДОНОСНЫХ ПОДСХЕМ, АКТИВИРУЕМЫХ ВНЕ РАБОЧЕЙ ОБЛАСТИ ФУНКЦИОНИРОВАНИЯ СХЕМЫ*

Е.В. Митрофанов

Национальный исследовательский Томский государственный университет, Томск, Россия
qvaz@ya.ru

Частое использование услуг сторонних компаний для производства спроектированных интегральных схем с целью экономии денежных средств приводит к увеличению риска встраивания вредоносных подсхем, которые могут лишить схему работоспособности или привести к краже конфиденциальной информации. Активация вредоносной подсхемы (Trojan Circuit, TC), как правило, происходит на малом подмножестве всех возможных входов, поэтому её присутствие практически невозможно обнаружить на стадиях верификации и тестирования интегральной схемы. TC состоит из двух частей. Триггерная подсхема (Trojan trigger) активируется, когда на входы TC поступает заранее определенная комбинация сигналов. В свою очередь, Trojan payload включается триггерной подсхемой и каким-либо образом изменяет работу схемы (получает доступ к защищенным данным, выводит из строя схему).

* Исследование выполнено за счет гранта Российского научного фонда (проект № 14-19-00218).

Предлагаемый в данной работе метод обнаружения вредоносных подсхем (TCs) заключается в поиске возможных мест их включения, основанный на использовании точных оценок управляемости и наблюдаемости элементов комбинационной части схемы. Оценки управляемости вычисляются для нерабочей области функционирования последовательностной схемы. Алгоритмы получения оценок основаны на использовании структурного описания комбинационной части и функциональном представлении схемы с памятью в виде графа переходов состояний (State Transition Graph или STG). Вычисления выполняются в виде операций над Reduced Ordered Binary Decision Diagrams (ROBDDs). В методе также используется алгоритм определения существования установочной последовательности в заданное множество внутренних состояний, который, в свою очередь, также производит вычисления над ROBDD (BDD). Помимо метода обнаружения ТС, предлагается способ маскирования ТС. Проведенные экспериментальные оценки показали применимость рассматриваемых подходов и невысокую вводимую избыточность, необходимую для маскирования TCs.

Принцип вычисления точных оценок управляемости и наблюдаемости полюсов элементов схемы и их использование для обнаружения возможных мест включения вредоносных подсхем описаны в работе [1]. В данном случае рассматривается вариант вычисления управляемости вне рабочей области функционирования схемы. Такой подход оправдан, так как активация ТС может происходить вне рабочей области, а классические методы тестирования сконцентрированы на поиске дефектов в рабочей области, следственно такие методы никогда не обнаружат факт включения ТС в схему. Для вычисления управляемости вне рабочей области, помимо получения BDD графа управляемости [1], необходимо также построить BDD граф рабочей области функционирования схемы, который несложно получить из STG описания поведения схемы. Построив два графа, BDD искомых оценок получается путем перемножения BDD графа управляемости из [1] и инверсии BDD графа рабочей области. Оценки наблюдаемости всегда строятся на основе структурного описания комбинационной части схемы [1] и не используют STG представление.

Множество полюсов V, в которых возможно включение ТС, представляет собой все полюсы, управляемость которых больше 0, но меньше заданного порога. Полученное множество можно сократить, исключив полюсы с высокой наблюдаемостью (выше определенного порогового значения), а также полюсы, в которых активация ТС требует слишком длинной установочной последовательности. В работе [2] описаны алгоритмы обнаружения факта существования установочной последовательности и построения такой последовательности. Эти алгоритмы полезны как для сокращения множества V, так и для активации вредоносных подсхем (TCs) на этапе их обнаружения.

Для устранения вредоносного воздействия ТС предлагается добавление маскирующей подсхемы вне площади основной схемы и дальнейшая коммутация с необходимыми полюсами с помощью мультиплексора. Таким образом, маскирующая схема не требует внесения больших изменений в первоначальную схему, но добавляет некоторую избыточность. Экспериментальные результаты, полученные на наборе бенчмарков MCNC, говорят об избыточности в районе от 0.8% до 5%.

Литература

1. *Матросова А.Ю., Кириенко И.Е., Томков В.В., Мирютов А.А.* Обеспечение надежности физических систем: выявление мест возможного включения вредоносных подсхем (trojan circuits) в последовательностных схемах // Известия вузов. Физика. 2016. Т. 59, № 8. С. 140–147.
2. *Matrosova A., Andreeva V., Melnikov A.* ROBDDs Application for Finding the Shortest Transfer Sequence of Sequential Circuit or Only Revealing Existence of this Sequence without Deriving the Sequence itself // Proceedings of IEEE East-West Design & Test Symposium (EWDTS'2016). Kharkov : IEEE Computer Society, 2016. P. 513–516.

СИНТЕЗ ОТКАЗОУСТОЙЧИВЫХ АВТОМАТНЫХ СЕТЕЙ ДЛЯ НЕИСПРАВНОСТЕЙ ЗАДЕРЖЕК ПУТЕЙ*

С.А. Останин, В.А. Лавров, Д.А. Третьяков

Национальный исследовательский Томский государственный университет, Томск, Россия
sergeiostanin@yandex.ru, neverlva@gmail.com, agronya@gmail.com

Использование современных высокоскоростных электронных схем в высокотехнологичных производствах требует высокой надежности этих схем. Внешние факторы, такие как радиация, высокая температура и др., часто приводят к появлению так называемых «мягких» неисправностей (soft faults) кратковременных или перемежающихся. Такие неисправности не вызывают необратимых изменений аппаратуры, и их проявление длится ограниченное время, как правило, не больше одного такта. В высокоскоростных схемах накопление даже небольших задержек элементов вдоль пути от входа схемы к выходу может привести к некорректному сигналу на выходе. Такие неисправности называются неисправностями задержек путей. В данной работе предлага-

* Исследование выполнено за счет гранта Российского научного фонда (проект № 14-19-00218).