МАТЕМАТИЧЕСКАЯ ОБРАБОТКА ДАННЫХ ФИЗИЧЕСКОГО ЭКСПЕРИМЕНТА

УДК 004.312 DOI: 10.17223/00213411/65/4/150

ПОСТРОЕНИЕ АППРОКСИМИРУЮЩИХ СХЕМ В РЕЖИМЕ ТРОИРОВАНИЯ

А.Ю. Матросова[1], С.А. Останин[1], Г.Г. Гошин[2]

[1] *Национальный исследовательский Томский государственный университет*, *г. Томск*, *Россия*
[2] *Томский государственный университет систем управления и радиоэлектроники*, *г. Томск*, *Россия*

Троирование является одним из широко используемых на практике подходов к обеспечению надежности функционирования логических схем. Однако появившиеся в последние годы возможности одновременного внесения в каждую копию и соответствующие линии вредоносных подсхем (Trojan Circuits) делают метод троирования уязвимым. Возникает необходимость противостоять таким угрозам. Одним из выходов в этой ситуации является использование вместо идентичных трех схем двух аппроксимирующих схем и одной рабочей схемы, выполняющей предписанное разработчиком функционирование. Этот подход приводит к появлению незащищенной области, в которой неисправность одной из трех схем может быть не обнаружена. Предлагается строить аппроксимирующие схемы, начиная с построения аппроксимирующих систем булевых функций, являющихся заданием на их синтез. Показано, что этот подход дает больше возможностей для сокращения незащищенной области, чем известные ранее методы. Приведены алгоритмы получения аппроксимирующих систем булевых функций из безызбыточной системы ДНФ рабочей схемы и алгоритм оценки величины незащищенной области.

Ключевые слова: *комбинационные схемы*, *безызбыточные системы ДНФ*, *аппроксимирующие схемы*, *троирование*, *константные неисправности*, *тестовые наборы*, *обнаруживающие константные неисправности.*

Введение

Надежность сложных физических систем зависит от надежности составляющих их компонент, в частности, от надежности управляющих компонент, которые, как правило, являются логическими схемами высокой производительности. Схемы троирования являются одним из широко распространенных подходов к обеспечению надежности функционирования логических схем. Предполагается, что одна из трех схем может быть неисправной. В этом случае в условиях подключения к одноименным выходам трех схем схемы голосования значение выхода определяется значением большинства одноименных выходов. Схемы голосования предполагаются исправными. Однако в современных условиях производство логической схемы может выполняться различными фирмами, в том числе, и в разных частях света. В связи с этим появляется возможность включения вредоносной подсхемы в каждую из идентичных схем, например, в соответствующую линию каждой из трех схем. Вредоносная подсхема (Trojan Circuit) может изменить в нужный момент значение сигнала на этих линиях на противоположное значение с целью искажения работы схемы или с целью извлечения конфиденциальной информации из устройства, содержащего рассматриваемую схему. Это значит, что технология троирования оказывается уязвимой в условиях возможности включения вредоносных подсхем. Одним из известных подходов к защите схемы троирования является использование аппроксимирующих схем, которые строятся из рабочей схемы, реализующей нужное разработчику поведение [1–3]. Аппроксимирующие схемы используются также при синтезе самопроверяемых логических схем [4–6]. В работе [1] аппроксимирующие схемы используются с целью сокращения аппаратурных затрат в условиях, когда функционирование самопроверяемой схемы может незначительно отклоняться от функционирования рабочей схемы, что менее важно, чем сокращение аппаратурных затрат. При использовании аппроксимирующих схем в схемах троирования отклонение от корректного функционирования возможно в присутствии неисправности в одной из трех схем в так называемой незащищенной области. В данной работе при построении аппроксимирующих схем основное внимание уделяется проблеме сокращения незащищенной области. С этой целью предлагается строить аппроксимирующие схемы из аппроксимирующих систем булевых функций. Это значит, что предлагается еще на этапе создания рабочей схемы учесть необходимость ее защиты от внедрения вредоносных подсхем при использовании троирования. Этот подход дает большие возможности для сокращения незащищенной области.