УДК 519.873:519.718.7

ПОДГОТОВКА КОНТЕНГЕНТА ДЛЯ СОЗДАНИЯ И РАЗВИТИЯ ТЕХНИЧЕСКОЙ БАЗЫ ЦИФРОВИЗАЦИИ

Золоторевич Л.А., к.т.н, доцент,
Белорусский государственный университет информатики и радиоэлектроники
Минск, Республика Беларусь

Аннотация: Акцентируется внимание на непрерывной подготовке специалистов для создания и развития методов и средств проектирования цифровых систем. Анализируются новые аспекты проектирования интегральных схем (ИС). Рассматриваются задачи обеспечения защиты структурных решений ИС кодированием. Предлагается алгоритм декодирования структур цифровых устройств. Применяются методы и средства тестового диагностирования, выполнимости булевых функций.

Ключевые слова: проектирование интегральных схем, выполнимость булевых функций, кодирование, декодирование.

PREPARATION OF CONTINTGENT FOR CREATION AND DEVELOPMENT OF THE TECHNICAL BASE OF DIGITALIZATION

Zolotorevich L.A., PhD, docent,
Belarusian State University of Informatics and Radioelectronics,
Minsk, Republic of Belarus

Abstract: The focus is on the continuous training of specialists for the creation and development of methods and tools for designing digital systems. New aspects of integrated circuits (IC) design are analyzed. Problems of ensuring the protection of structural solutions of IS by coding are considered. An algorithm for decoding structures of digital devices is proposed. Methods and means of test diagnostics, feasibility of Boolean functions are used.

Keywords: design of integrated circuits, feasibility of Boolean functions, encoding, decoding.

Процесс современной цифровизации можно рассматривать как развитие на новой технической базе (СБИС, СнК) процессов создания АСУ (60-е годы), компьютеризации (80-е годы) и информатизации (90-е годы). Наличие собственной технологии микроэлектроники является важнейшим звеном цифровизации. Общеизвестно, что микроэлектроника и электронная отрасли промышленности являются стратегическими отраслями любой современной индустриально развитой страны. Они обеспечивают большую часть их национального дохода, превышающую доход от всех остальных отраслей народного хозяйства. Мировой опыт показывает, что указанные отрасли играют роль своеобразного катализатора развития всех отраслей человеческой жизнедеятельности. Электроника «контролирует в 3 раза больше рабочих мест, чем создаёт». Поэтому успехи, достигнутые в этих отраслях, являются необходимым условием создания новых конкурентоспособных товаров практически во всех отраслях.

Необходимость развития собственной микроэлектроники обусловлена, в первую очередь, потребностями оборонной промышленности. Приобретение зарубежной электроники стало проблематичным из-за возможных санкций на поставку, но более важно то, что в целях обеспечения безопасности применения зарубежной электроники необходим наукоемкий контроль на предмет несанкционированного внедрения в интегральные схемы троянов с разными основополагающими целями. Подобные действия в последние годы являются преднамеренными и тщательно скрываемыми, что препятствует прямому применению для их обнаружения существующих методов тестирования и функционального контроля СБИС [1-3].

В связи с тем, что задачи проектирования цифровых систем являются наукоемкими, для разработки собственных проектов для их решения и применения в реальном секторе необходима подготовка квалифицированного персонала. К сожалению, наиболее высококвалифицированная молодежь работает в IT-сфере, выполняет заказы по постановкам частных задач зарубежных работодателей, что не направлено на создание и внедрение наукоемкой технологии создания технической базы цифровизации.

В работах [4,5] 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 рассматриваются задачи, связанные с развитием теории контролепригодного проектирования (Design-for-Testability - DfT).

Одним из методов борьбы с вышеупомянутыми угрозами является логическое шифрование. Основная идея шифрования состоит в том, чтобы изменить конструкцию ИС, добавив в нее дополнительные логические элементы и новые входы, называемые ключевыми. Ключевые входы подключаются к защищенной от несанкционированного доступа памяти, а закодированная схема будет работать правильно только в том случае, если поданы правильные значения на ее ключевые входы. Значения ключевых входов передаются после изготовления микросхем конечным пользователям.

Логическое шифрование [1] основывается на предположении, что производитель не знает и не может вычислить правильные значения ключевых входов. В противном случае, злоумышленник мог бы просто запрограммировать эти значения, и перепроизводство не могло быть предотвращено.

Однако производитель может попытаться вычислить значения ключевых входов при условии, что ему доступна структура закодированной логической схемы, которая передается проектировщиком. Кроме того, злоумышленник может приобрести на рынке активированную микросхему, в защищенную от несанкционированного доступа память которой заказчик загрузил правильное значение ключа.

Если $Cir_a(\vec{X})$ - КНФ-представление булевой функции разрешения, реализуемой исходной схемой, а КНФ функции разрешения закодированной схемы $Cir_b(\vec{X},\vec{K})$; $\vec{X}$ - первичные входы схемы, $\vec{X}=(x_1,x_2,...,x_n)$; $\vec{K}$ - ключевые входы зашифрованной схемы, $\vec{K}=(k_1,k_2,...,k_m)$, то задача получения ключа сводится к описанию закодированной схемы КНФ булевой функции разрешения и определению выполнимости данной функции. Решение задачи применением программы решения выполнимости (SAT-solver) ограничивается большим объемом вычислительных процедур, определяемым числом 2^n, где n – число первичных входов схемы.

Предлагается следующее решение проблемы: вместо того, чтобы анализировать значения ключей индивидуально, предлагается рассмотреть классы эквивалентности ключей. Два ключа $\vec{K}_1$ и $\vec{K}_2$ являются эквивалентными ($\vec{K}_1 = \vec{K}_2$) тогда, когда для каждого входного значения $\vec{X}_i$ зашифрованная схема выдает одинаковое выходное значение $\vec{Y}_i$ для ключей $\vec{K}_1$ и $\vec{K}_2$.

Предложен алгоритм и проведено его исследование на основе применения программных средств моделирования, тестового диагностирования и SAT-решателей.

Список использованных источников

1. Золоторевич, Л.А. Аппаратная защита цифровых устройств / Л.А. Золоторевич // Вестник Томского государственного университета. Управление, вычислительная техника, информатика. 2020, №50. – С. 69-78. DOI: 10.17223/19988605/50/9.
2. 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.
3. Золоторевич, Л.А. Обфускация комбинационных схем цифровых устройств от несанкционированного доступа /L.A. Zolotorevich // Информатика. – 2019. – Т. 16, № 3. – С. 89–100.
4. Shakya, B. Benchmarking of *hardware* Trojans and maliciously affected circuits / B. Shakya, T. H. Salmani, D. Forte, S. Bhunia, M. Tehranipoor *// J. Hardw. Syst. Secur. (HaSS) 1(1). – 2017. – P. 85–102.*
5. 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. 221-22.