ВЗЛОМ КЛЮЧЕВОГО КОДА СТРУКТУРЫ ЦУ НА ОСНОВЕ РЕШЕНИЯ ЗАДАЧИ SAT

Л.А. Золоторевич, А.В. Павлова

В связи с проблемами пиратства, перепроизводства и контрафакции в последние годы стала актуальной необходимость защиты проектов СБИС, СнК от несанкционированного доступа в цикл проектирования и производства интегральных схем на основе создания общего подхода к их контролю. По оценкам Technology Information Handling Services (IHS), финансовый риск из-за контрафактных и несанкционированных микросхем оценивается в более чем 169 миллиардов долларов в год [1]. Кроме больших финансовых потерь существует реальная проблема обеспечения национальной безопасности.

В работе [2] 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. Одним из методов борьбы с вышеупомянутыми угрозами является логическая блокировка. Основная идея блокировки 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 конечным пользователям. Одновременно с исследованиями по повышению эффективности кодирования разрабатываются и исследуются методы взлома кода [3].

В докладе рассматривается возможность раскрытия кода злоумышленником на основе описания зашифрованной схемы в виде КНФ булевой функции разрешения и решения выполнимости данной функции.

Литература

1. Subramanyan P., Ray S., Malik S. Evaluating the security of logic encryption algorithms // Hardware Oriented Security and Trust (HOST), 2015 IEEE International Symposium. – IEEE, 2015. – P. 137–143.

2. Золоторевич Л.А. Аппаратная защита цифровых устройств // Вестник Томского государственного университета. Управление, вычислительная техника, информатика. – 2020. – № 50. – С. 69–78. – DOI: 10.17223/19988605/50/9.

3. Weighted Logic Locking: A New Approach for IC Piracy Protection / N. Karousos [et al.] // IEEE 23rd International Symposium on On-Line Testing and Robust System Design (IOLTS). – 2017. – P. 221–226.