КОНТРОЛЬ ЭФФЕКТИВНОСТИ КОДИРОВАНИЯ ИНТЕГРАЛЬНЫХ СХЕМ

Л.А. Золоторевич, В.А. Ильинков

В последние годы для защиты проектов интегральных схем применяются методы и средства аппаратного кодирования комбинационных блоков интегральных схем (ИС) [1]. Для совершенствования подобной защиты проектов необходимы средства контроля эффективности применяемых методов кодирования. Предлагается метод взлома кода при наличии информации о структуре закодированного объекта и возможности доступа к физической модели. Задача решается на основе описания закодированной структуры в виде КНФ функции разрешения, решения задачи выполнимости (SAT) и физического моделирования объекта.

Исходными данными для декодирования структуры цифрового устройства является структурная реализация закодированной схемы, которая может быть получена методом обратного проектирования (проектирования по прототипу), а также активированный физический образец интегральной схемы, в защищенную от несанкционированного доступа память которой заказчик загрузил правильное значение ключа. Этот образец может использоваться в виде модели черного ящика Y = eval (X). Основная идея SAT – атаки взлома ключа состоит в том, чтобы определить правильный ключ, не прибегая к исследованиям на большом интервале входно-выходных переменных. Два ключа $\vec{K}_1$ и $\vec{K}_2$ являются эквивалентными ($\vec{K}_1 = \vec{K}_2$), тогда и только тогда, когда для входного значения $\vec{X}_i$ закодированная схема выдает одинаковое выходное значение $\vec{Y}_i$ для ключей $\vec{K}_1$ и $\vec{K}_2$. Для определения правильного ключа итеративно исключаются ключи из класса эквивалентности, которые выдают неправильные значения выходов, в крайней мере для одного входного шаблона. Класс эквивалентных ключей определяется на некотором входно-выходном векторе

решением выполнимости функции $Cir_b(\vec{X}_j, \vec{K}, \vec{Y}_j)$ полным методом. Входной вектор $\vec{X}^d$ называется различающим, если реакция схемы при использовании ключа $\vec{K}_1$ равна $\vec{Y}_1^d$ и отличается от реакции $\vec{Y}_2^d$ при использовании ключа $\vec{K}_2$. При наличии различающего набора можно проверить реакцию активированной схемы для входа $\vec{X}^d$ и использовать ее, чтобы исключить ключ $\vec{K}_1$ или $\vec{K}_2$ как не входящий в класс эквивалентности правильных ключей.

Литература

1. 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.