УДК 519.873:519.718.7

АЛГОРИТМЫ КОДИРОВАНИЯ И ВЗЛОМА КОДОВ СТРУКТУРНЫХ РЕАЛИЗАЦИЙ ЦИФРОВЫХ УСТРОЙСТВ

Л. А. Золоторевич[1], В. А. Ильинков[2]
Белорусский государственный университет информатики
и радиоэлектроники, Минск
e-mail: zolotorevichla@bsuir.by[1], v.ilyinkov@gmail.com[2]

Интегральные микросхемы (ИС) и системы на кристалле (СнК) являются ключевыми звеньями различных промышленных систем и систем обороноспособности государства. Появление контрафактных ИС, проблемы пиратства, перепроизводства, несанкционированное вмешательство в проект микросхемы, аппаратные трояны требуют развития методов и средств их своевременного обнаружения. Трояны могут быть внесены в структуру ИС в процессе как разработки, так и производства, включая этапы спецификации, проектирования, верификации и изготовления. Включение в структуру ИС дополнительных элементов ставит под угрозу функциональную пригодность и надежность системы в целом. С целью аппаратной защиты проектов в настоящее время применяются методы аппаратного кодирования. В работе рассматриваются особенности и надежность логического кодирования комбинационных схем. Предлагается алгоритм взлома кода комбинационных схем, основанный на исследовании ключа как элемента класса эквивалентности.

В литературе предложены различные методы кодирования комбинационной логики, в которых в качестве ключевых вентилей используются элементы XOR / XNOR [1, 2], AND / OR [3] или их комбинации [4]. Выбор линии для включения вентиля и тип применяемого вентиля существенно влияют на эффективность кодирования. Воздействие неправильного ключа можно сравнить с влиянием неисправности константного типа на данной линии. В отличие от вентилей OR, NOR, AND, NAND, при выборе в качестве ключевых вентилей XOR или NXOR применение неправильного ключа приводит к появлению неисправности константного типа в любом случае, на любом входном воздействии, что влияет в целом на эффективность кодирования.

Кроме выбора типа применяемого вентиля существуют еще два основных способа увеличить влияние кодовых вентилей на значения выходов схемы. Один из них заключается в выборе линий, сигналы в которых влияют на максимально возможное количество выходов схемы, второй – в повышении чувствительности схемы в ответ на применение не-

правильного ключа. Выбор линии для включения вентиля в большой степени влияет на эффективность кодирования. Один из подходов основан на случайном выборе линии схемы. В работе [1] показана недостаточная эффективность этого метода. Основная задача, которая должна быть решена при практической реализации идеи кодирования, заключается в том, чтобы определить оптимальное множество внутренних линий схемы и количество ключевых элементов для создания максимальных трудностей для злоумышленника по поиску правильного ключа. При включении очередного вентиля при кодировании логических устройств необходимо проводить анализ на появление эффекта маскирования неисправностей, который способен блокировать эффект кодирования [1, рис. 2]. При наличии избыточности некоторые линии схемы не могут быть активированы ни одним входным набором, поэтому вставка ключевого вентиля в данном случае может быть бесполезной [1, рис. 1]. В работе [1] предложен способ кодирования, основанный на сквозном моделировании неисправностей, построении теста в классе неисправностей константного типа и его применении на первом этапе кодирования.

Результат кодирования проявляется на выходах схемы в зависимости от числа неправильных битов кода [5]. Если ключевой вентиль управляется одним битом ключевого кода, то вероятность P того, что данный вентиль будет приведен в действие, равна 0,5. Это означает, что только половина ключевых вентилей может повлиять на результат функционирования схемы при применении неправильного ключа. Для увеличения вероятности P и усиления влияния неправильного бита кодового слова на результат функционирования схемы применяются управляющие вентили, с помощью которых можно объединить биты кодового слова в группы, использовав при этом их выходы в качестве входов ключевых вентилей. В таком случае будет реализовано групповое воздействие нескольких битов кодового слова на активацию ключевого вентиля. Если хотя бы один из ключевых входов, включенных в группу, принимает неправильное значение, ключевой вентиль окажется активированным. Для этого с каждым ключевым вентилем используется управляющий вентиль. Метод управляемого кодирования [1] позволяет повысить эффективность кодирования за счет увеличения числа применяемых вентилей.

В докладе рассматривается задача взлома кода, решение которой направлено на исследование надежности методов аппаратной защиты. Подход основан на сведении задачи к определению выполнимости булевой функции разрешения. Приводится алгоритм и особенности его практической реализации.

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 взлома ключа состоит в том, чтобы определить правильный ключ, не прибегая к исследованиям на большом интервале входно-выходных переменных [6]. Рассматривается класс эквивалентности ключей. 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 по крайней мере для одного входного шаблона. Класс эквивалентных ключей определяется на некотором входно-выходном векторе решением выполнимости функции закодированной схемы $Cir_b(\vec{X}_j, \vec{K}, \vec{Y}_j)$ полным методом. Определяется различающий входной набор. 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.

Список литературы

1. Золоторевич, Л. А. Аппаратная защита цифровых устройств / Л. А. Золоторевич // Вестник Томского гос. ун-та. Управление, вычислительная техника, информатика. – 2020. – № 50. – С. 69–78. DOI: 10.17223/19988605/50/9.

2. On Improving the Security of Logic Locking / M. Yasin [et al.] // IEEE TCAD. – 2016. – Vol. 35, no. 9. – P. 1411–1424.

3. A Novel Hardware Logic Encryption Technique for Thwarting Illegal Overproduction and Hardware Trojans / S. Dupuis [et al.] // IEEE IOLTS. – 2014. – P. 49–54.

4. Lee, Y.-W. Improving Logic Obfuscation via Logic Cone Analysis / Y.-W. Lee, N. A. Touba // Proc. of 16th Latin-American Test Symp., Puerto Vallarta, Mexico, 25–27 Mar. 2015. – Puerto Vallarta, 2015.

5. Weighted Logic Locking: A New Approach for IC Piracy Protection / N. Karousos [et al.] // IEEE 23rd Intern. Symp. on On-Line Testing and Robust System Design (IOLTS), Thessaloniki, Greece, 3–5 July 2017. – Thessaloniki, 2017. – P. 221–226.

6. Subramanyan, P. Evaluating the security of logic encryption algorithms / P. Subramanyan, S. Ray, S. Malik // IEEE Intern. Symp. on Hardware Oriented Security and Trust (HOST), Washington, DC, USA, 9–15 Nov. 2019. – Washington, 2019. – P. 137–143.