В. В. Сергейчик

ПРЕОБРАЗОВАНИЯ ПРОЕКТНЫХ ОПИСАНИЙ ЦИФРОВЫХ УСТРОЙСТВ С ЦЕЛЬЮ СХЕМНОЙ ОБФУСКАЦИИ

Рассматривается функциональная обфускация: назначение, методы, перспективы применения.

Пиратство в области аппаратных средств по наносимому материальному ущербу существенно превышает пиратство в области программного обеспечения, однако ему всё еще уделяют меньше внимания.

Обфускация служит для запутывания понимания функционирования устройства с целью защиты от обратного проектирования. Также широко применяется для сокрытия водяных знаков и отпечатков пальцев.

Существует множество методов лексической обфускации, но их недостатком является то, что их результаты удаляются при синтезе [1]. Функциональные методы обфускации базируются на эквивалентном изменении схемы с сохранением исходной функциональности. Выгодно использовать лексические методы совместно с функциональными. Это увеличивает сложность понимания функционирования на всех стадиях проектирования и производства устройства. Рассмотрим несколько методов:

- Переименование идентификаторов, хранивших семантику функционирования устройства, на бессмысленные сочетания символов [2], обычно одинаковой длины и похожего написания.
- Перестановка объявлений и параллельных операторов – удаляется смысловая близость операций [2].
- Разрушение структуры кода – изменение исходного форматирования, которое несёт важную смысловую нагрузку [2].
- Схемы, исчезающие при синтезе. При этом внедряются схемы, заведомо минимизируемые до схем, являющихся источниками констант ‘0’ или ‘1’.
- Схемы, генерирующие константы. Суть в замене выводов ‘0’ и ‘1’ на схему, которая всегда генерирует постоянное значение. При этом схема будет синтезирована и обратному проектировщику потребуется время, чтобы понять, что она эквивалентна константе. Примеры на рисунке 1.

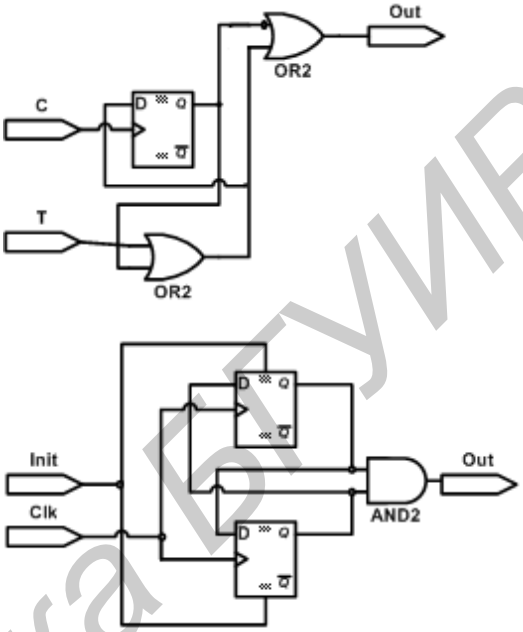

Рис. 1 – Генераторы констант ‘1’ и ‘0’

Замена логических операций на таблицы истинности. При этом логика таблиц может быть произвольной сложности. Например, операцию xor можно заменить таблицей “0000“, “0110“, “0101“, “1000“, адресацию осуществлять комбинацией входных сигналов. Например, в FPGA логические операции реализуются с помощью LUT-блоков, поэтому при хорошем подборе функций аппаратные расходы не увеличатся, зато повысится сложность понимания схемы.

Обфускация усложняет обратное проектирование схем. Важно проводить обфускацию так, чтобы результирующая схема устройства существенно отличалась от исходной, но функциональность оставалась эквивалентной прежней.

1. Проектирование встраиваемых цифровых устройств и систем / А. А. Иванюк. – Минск : Бестпринт, 2012. — 337с.
2. A Taxonomy of obfuscation transformations [Electronic resource] / C. Collberg [et al.] // Dept. of CS, – Univ. of Auckland, 1997. – Mode of access: collberg.pdf. – Date of access: 20.10.2012.

Сергейчик Владимир Валентинович, студент 5 курса ФКСиС кафедры ПОИТ БГУИР, vovasq@mail.ru.

Научный руководитель: Иванюк Александр Александрович, заведующий кафедрой вычислительных методов и программирования БГУИР, доктор технических наук, доцент, ivaniuk@bsuir.by.