В. Л. Касперович

ПРИМЕНЕНИЕ ФИЗИЧЕСКИ НЕКЛОНИРУЕМЫХ ФУНКЦИЙ ДЛЯ ЗАЩИТЫ ЦИФРОВЫХ УСТРОЙСТВ ОТ НЕСАНКЦИОНИРОВАННЫХ ИЗМЕНЕНИЙ

В данной работе рассматривается проблема защиты цифровых устройств как объектов интеллектуальной собственности от несанкционированного копирования и (или) модификации. Предлагается усовершенствованный метод защиты цифровых устройств, основанный на применении физически неклонируемых функций, а именно кольцевых осцилляторов.

В настоящее время актуальной является проблема защиты устройств на ПЛИС от несанкционированного использования. Наиболее эффективным является метод, основанный на внедрении уникального идентификатора, напрямую связанного с устройством, т.е. физически неклонируемой функции.

В качестве физически неклонируемой функции был выбран кольцевой осциллятор. Его структура состоит из цепи задержки с обратной связью и инверсией выходного значения. Кольцевой осциллятор генерирует последовательность типа меандр определенной частоты, которая зависит от следующих параметров: средняя величина задержки элементов кольцевого осциллятора; задержка, вызванная дискретными случайными вариациями и задержка, вызванная системными случайными расхождениями [1]. Кроме цепи самого осциллятора, необходимы также такие элементы, как счетчик количества тактов кольцевого осциллятора, регистр, хранящий заранее измеренной значение относительной частоты, а также механизм сравнения этих значений.

В рамках данного исследования была поставлена задача максимальной интеграции структуры кольцевого осциллятора со структурой исходного устройства. Для этого элементами кольцевого осциллятора выбраны компоненты исходного устройства, и введены два режима работы: штатное функционирование и проверка.

Алгоритм модификации предполагает разрыв цепи сигнала, соединяющей два компонента, и внедрение вместо нее структуры, как показано на рисунке 1. Возможны модификации данной структуры, например, использование вместо нее элемента XOR, однако показанная структура является предпочтительной, т.к. существуют примитивы проектирования, соответствующие ей. Преобразуются все сигналы, входящие в самую длинную цепь, соединяющую входной и выходной порты устройства. Полученная цепь замыкается обратной связью, выход которой и будет представлять собой выход кольцевого осциллятора. В штатном режиме функционирование не будет нарушено.

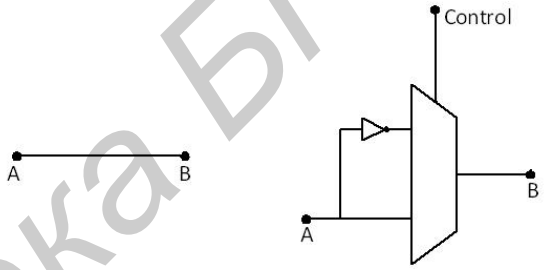

Рис. 1 – Процедура внедрения цифрового компонента

Результатом данной разработки является метод защиты цифровых устройств на ПЛИС. Его преимуществами являются:

- возможность предотвратить как модификацию, так и тиражирование устройства;
- защищенность от удаления осциллятора из проекта;
- основанный на внутренней структуре устройства метод идентификации;
- отсутствие необходимости производить трудоемкие операции по анализу схем.

1. Tehranipoor, M. Hardware Trojan Detection Solutions and Design-for-Trust Challenges / M. Tehranipoor et al. // Computer – 2011. – № 7. – P. 66–74.

Касперович Вячеслав Леонидович, студент 5 курса факультета КСиС Белорусского государственного университета информатики и радиоэлектроники, vaclav1990@tut.by

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