

МЕТОДИКА ВНЕДРЕНИЯ ВОДЯНЫХ ЗНАКОВ В ПРОЕКТНЫЕ ОПИСАНИЯ ЦИФРОВЫХ УСТРОЙСТВ С ЦЕЛЬЮ ДОКАЗАТЕЛЬСТВА АВТОРСТВА

В данной статье рассматривается методика внедрения водяных знаков в IP-компоненты с использованием свободных запоминающих ячеек в LUT-блоках FPGA.

Защита цифровых устройств на базе ПЛИС сейчас является очень важной задачей для разработчиков. Для решения этой задачи предлагается внедрение водяного знака в проектное описание с целью обеспечения возможности в дальнейшем доказать свое право интеллектуальной собственности на данный объект [1]. В общем случае водяной знак – некоторая последовательность бит, которая не будет присутствовать в описании явным образом, однако проектировщик, осуществивший внедрение будет иметь возможность извлечь эту последовательность бит.

На физическом уровне FPGA в качестве основных элементов кроме всего прочего имеют так называемые LUT-блоки (см. рис. 1), с помощью которых осуществляется реализация любой логической функции 4-х переменных. Каждый LUT-блок содержит запоминающие ячейки, в которых хранятся значения таблицы истинности для функции реализуемой этим блоком. Ввиду того, что не всегда используются все ячейки LUT-блоков, оставшиеся ячейки можно использовать для хранения водяного знака.

Предлагается изменять хранимые в неиспользуемых запоминающих ячейках значения таким образом, чтобы логическая функция реализуемая LUT-блоком оставалась неизменной, однако при этом в ячейках хранились биты водяного знака. Данные LUT-блоки будут представлены в виде линейной памяти. В каждый из блоков будет внедрена часть водяного знака. Для адресации по памяти предлагается использовать генератор псевдослучайных последовательностей. По соответствующему адресу будет внедряться часть битов водяного знака. Инициализирован генератор будет секретным ключом автора-проектировщика. Фактически для внедрения битов в свободные запоминающие ячейки необходимо добавить к свободному входу LUT-блока некое константное значение и изменить его инициализационную константу. Константное значение подаваемое на свободный вход будет использоваться для извлечения водяного знака. Существует два способа его добавления: 1) добавить на входную шину устройства дополнительный вход, сигнал которого будет передаваться

в LUT-блок; 2) добавить константное значение внутри схемы.

После внедрения водяного знака, необходимо провести анализ свободного места в проекте. В случае возможности – продублировать водяной знак. Адреса для его дублирования предлагается получить продолжив генерацию псевдослучайной последовательности. В противном случае оставшееся место необходимо заполнить случайными битами, для запутывания схемы. Таким образом водяной знак не будет присутствовать в схеме в прямом виде.

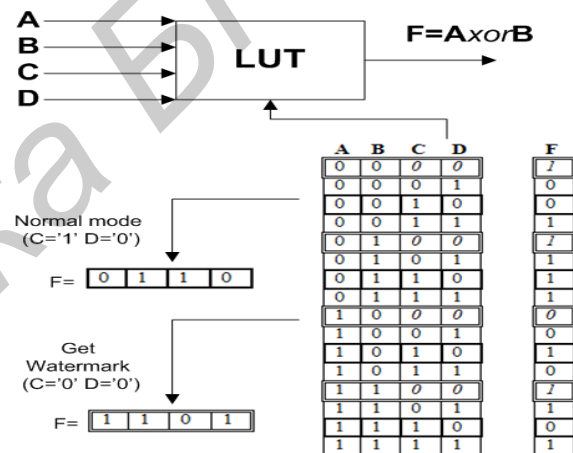


Рис. 1 – LUT-блок

Для изучения возможности внедрения водяного знака в проектное описание был проведен анализ свободных LUT-блоков в произвольно выбранных проектах для FPGA Spartan-3E. Среднее количество LUT2-блоков относительно всех LUT-блоков составляет 33%, LUT3 – 27%. Таким образом среднее количество свободного места в проектах составило 3439 бит, что показывает возможность внедрения в проект водяного знака соответствующей длины без использования дополнительных аппаратных ресурсов.

1. Иванюк, А. А. Проектирование встраиваемых цифровых устройств и систем / А. А. Иванюк – Минск : Бестпринт, 2012. – 337 с.

Николаенко Владимир Владимирович, студент 5 курса кафедры программного обеспечения информационных технологий БГУИР nickangel.blr@gmail.com.

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