В. П. Клыбик
(БГУИР, Минск)

РЕАЛИЗАЦИЯ PUF ТИПА АРБИТР НА FPGA

Физически неклонируемые *(слитно)* функции (от англ. Physically Unclonable Functions, PUF) широко применяются для аутентификации и идентификации экземпляров цифровых устройств [1, 2].

Для PUF типа арбитр (A-PUF) [1] наблюдается низкая эффективность при их реализации на кристаллах программируемой логики типа FPGA, связанная в первую очередь с непредсказуемой длиной и заведомой асимметричностью путей. Кроме этого реализации A-PUF на FPGA характеризуются наличием нестабильных откликов при многократной подаче одного запроса.

Перечисленные проблемы вызывают трудности использования выходных значений A-PUF для аутентификации и идентификации экземпляров цифровых устройств [2].

Для решения проблем предлагаются следующие подходы:

1) Новые схемные реализации A-PUF для FPGA. Применение реверсивных счетчиков и методов компенсации статической временной составляющей асимметричности путей тестирующего сигнала.

2) Новые варианты генераторов тестовых импульсных последовательностей. Использование конечных последовательностей тестирующих импульсов вместо одиночных.

3) Повышение стабильности A-PUF за счет перехода от оценки прямого значения единичного отклика простого арбитра к оценке статистических характеристик множества последовательных откликов. Использование в качестве метрики идентичности цифровых устройств подмножеств входных значений с устойчиво стабильными выходными значениями арбитра, нестабильными значениями, и их комбинаций.

Для проверки практической эффективности предложенных решений и их комбинаций в промышленном применении необходимо проведение натурных экспериментов для FPGA. В результате возможна разработка схемы идентификации цифровых устройств, реализованных на FPGA, дающей стабильные результаты и достаточную степень защиты.

Литература

1. An Analysis of Delay Based PUF Implementations on FPGA. Mode of access: http://rijndael.ece.vt.edu/puf/paper/arc2010.pdf. Date of access: 11.01.2013.

2. Physical Unclonable Functions for Device Authentication and Secret Key Generation. Mode of access: http://people.csail.mit.edu/devadas/pubs/puf-dac07.pdf. Date of access: 01.02.2013.