ИСПОЛЬЗОВАНИЕ СУБТАКТОВЫХ ЛИНИЙ ЗАДЕРЖКИ ДЛЯ АНАЛИЗА ВРЕМЕННЫХ ХАРАКТЕРИСТИК ФИЗИЧЕСКИ НЕКЛОНИРУЕМОЙ ФУНКЦИИ ТИПА АРБИТР

Шамына А. Ю., Иванюк А. А.
Кафедра программного обеспечения информационных технологий, кафедра информатики, Белорусский государственный университет информатики и радиоэлектроники
Минск, Республика Беларусь
E-mail: {shamyna, ivaniuk}@bsuir.by

Произведен анализ временных характеристик физически неклонируемой функции типа арбитр классической структуры с использованием субтактовых линий задержек. Кратко изложены концепции построения времяизмерительной системы и способы ее калибровки. Описано построение экспериментальной установки. Экспериментальные исследования проводились на плате быстрого прототипирования Digilent z7-10 с SoC Zynq-7000.

Введение

Актуальным и востребованным является использование средств физической криптографии. Эти средства применяются в протоколах аутентификации и проверки подлинности, а также в различных криптосистемах как источник энтропии. Многие из них основаны на использовании физически неклонируемых функций (ФНФ) [1]. Широкое применение получили физически неклонируемые функции типа арбитр (АФНФ). Основополагающая идея их работы базируется на уникальности и неповторимости временных характеристик распространения сигналов через пути цифрового устройства. В схеме АФНФ предполагается наличие блока симметричных путей (БСП), через который распространяются тестовые импульсы и арбитра, задача которого сводится к определению очередности прохождения фронтов этих импульсов через БСП. Однако при реализации данных схем на современных платформах (таких как ПЛИС типа FPGA) возникают сложности с оценкой их временных характеристик. Консервативные оценки задержек с использованием параметрических моделей зачастую не подходят для измерения уникальных временных характеристик задержек конкретного экземпляра устройства. Подходы для измерения, основанные на применении принципов кольцевого осциллятора также обладают ограничениями с точки зрения подбора времени и окна измерения, а также их реализации [2].

В настоящей работе для оценки временных характеристик АФНФ предлагается использовать времяизмерительную систему (англ. time to digital convertion, TDC), построенную на основе субтактовых линий задержки (англ. tapped delay line, TDL) [3-4]. Данный вид времяизмерительных систем широко применяется в тех областях, где требуются измерения между физическими событиями (рис. 1) с высокой точностью и производительностью. Например, в масс-спектрометрии, позитронно-эмиссионной томографии, экспериментах по ядерной и квантовой физике и т.п.

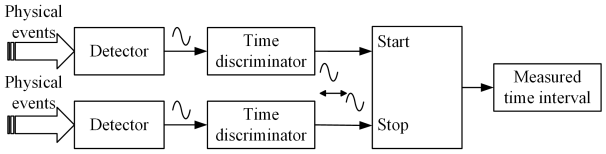

Рис. 1 – Концепция TDC

I. Конфигурация TDC

За основу при реализации времяизмерительной системы была выбрана методика интерполяции, описанная в [4]. Ее суть заключается в совместном использовании счетчиков «грубого» подсчета тактов TDC и TDL при измерениях. Это позволяет значительно расширить окно измерений, а также синхронизировать события между несколькими независимыми каналами (при условии тактирования одним синхросигналом).

Составными частями канала TDC являются: вход измеряемого сигнала «Hit», линия задержки «Delay line», счетчик тактов «Counter», каскадный счетчик единиц «Encoder» и блок управления «Control unit» (рис. 3).

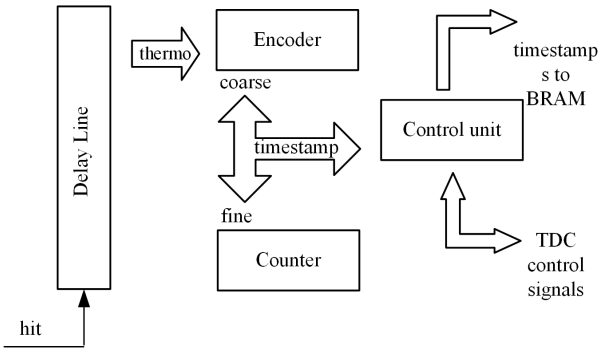

Рис. 2 – Схема канала TDC

Ключевым элементом канала измерения TDC является субтактовая линия задержки

TDL. Принцип ее работы заключается в формировании цепи последовательно соединенных звеньев, через которую пропускается измеряемый сигнал. Проходя через элементы задержки, фронт сигнала переключает подключенные к ним триггеры, которые синхронизированы одним тактовым сигналом (рисунок 3). Задержка данной линии должна быть несколько больше, чем период тактового сигнала TDC. Данная структура TDL является автономной и не требует дополнительной логики сброса, т.к. выход линии заведен на входы портов сброса триггеров. Для уменьшения задержки между элементами линии задержки и увеличения точности измерений были использованы линии логики быстрого переноса (англ. fast carry logic), которые напрямую соединяют SLICE-блоки столбца FPGA. Однако несмотря на такое решение, задержка на каждом шаге имеет разное значение. Поэтому такая схема нуждается в процедуре калибровки и вычислении задержки каждого шага линии задержки. Для калибровки был использован метод коррелированных событий [5].

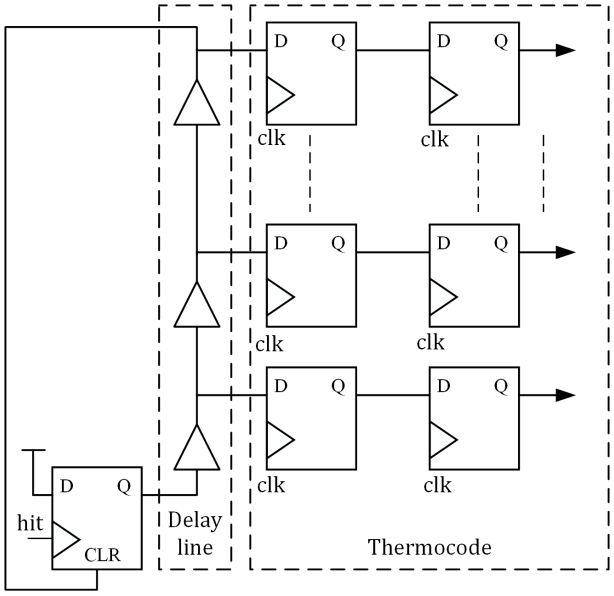

Рис. 3 – Схема TDL

II. Проведение эксперимента

Проект был создан и разработан в САПР Vivado 2018.2. Реализация канала TDC была выполнена в виде IP-ядра. Количество элементов для данной конфигураций было подобрано исходя из частоты для работы TDC. Для гибкого взаимодействия с ПК на платформе Zynq 7000 был развернут PetaLinux. Передача данных между ПК и экспериментальной установкой осуществлялась по протоколу TCP. Для этих целей было реализовано клиент-серверное приложение. Со стороны ПК было также разработано приложение для анализа поступающих данных измерений с использованием Matlab.

Для измерений была выбрана схема АФНФ, описанная в работе [2]. Конфигурация исследуемой АФНФ включала $N = 64$ звеньев блока симметричных путей. Всего было сгенерировано 10^5 запросов АФНФ и проведено столько же измерений. График распредления задержек для одного пути АФНФ выбранной конфирации предствлен на рисунке 4.

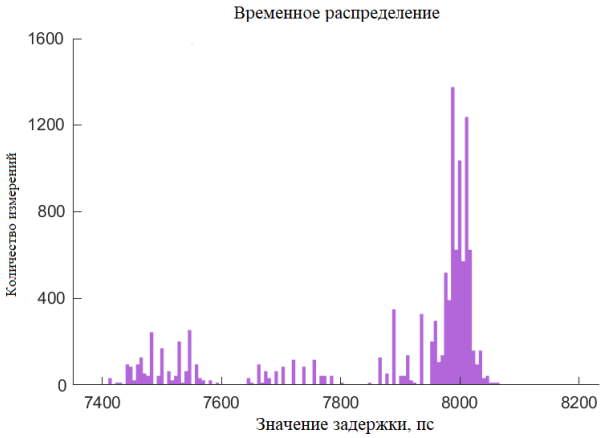

Рис. 4 – График распределение задержек АФНФ

Измерения соотвествуют полученным результатам в работе [2].

III. Заключение

Полученные результаты свидетельствуют о возможности и целесообразности использования подходов TDC для измерений внутренних задержек цифрового устройства. Концепция TDL может быть применена в качестве основы для разработки нового подхода при создании схемы арбитра АФНФ. В дальнейшем планируется сосредочить усилия над увеличении точности схемы TDC и снижения ее аппаратурных затрат.

IV. Список литературы

1. Pappu, R. Physical One-Way Functions: PhD Thesis in Media Arts and Sciences / R. Pappu. – Cambridge : Massachusetts Institute of Technology, 2001. – 154 p.
2. Шамына А.Ю., Иванюк А.А. Исследование временных параметров физически неклонируемой функции типа арбитр с использованием кольцевого осциллятора. Цифровая трансформация. 2022; 28(1): 27-38.
3. M. Adamič and A. Trost, "A Fast High-Resolution Time-to-Digital Converter Implemented in a Zynq 7010 SoC,"2019 Austrochip Workshop on Microelectronics (Austrochip), 2019, pp. 29-34, doi: 10.1109/Austrochip.2019.00017.
4. Jozef Kalisz, “Review of methods for time interval measurements with picosecond resolution,” Metrologia, vol. 41, no. 1, pp. 17–32, February 2004.
5. J. Wu, "Several Key Issues on Implementing Delay Line Based TDCs Using FPGAs,"in IEEE Transactions on Nuclear Science, vol. 57, no. 3, pp. 1543-1548, June 2010, doi: 10.1109/TNS.2010.2045901.