УДК 004.056.53

ИДЕНТИФИКАЦИЯ ЦИФРОВЫХ УСТРОЙСТВ С ПОМОЩЬЮ БИСТАБИЛЬНЫХ ЭЛЕМЕНТОВ, РЕАЛИЗОВАННЫХ НА FPGA

Кайкы М.
Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь
Иванюк А.А. - д.т.н., профессор кафедры информатики

Аннотация. Данная работа посвящена изучению внутрикристальных и межкристальных статических ячеек памяти, построенных на двух инверторах с обратной связью. Приведён пример расчёта расстояний по Хэммингу в троичной и пятеричной системах счисления для анализа различия нестабильных идентификаторов. Построены тепловые карты ячеек статической памяти с учётом нестабильных элементов, рассмотрены возможности применения подобных физически неклонируемых функций в системах защиты цифровых схем и идентификации.

Ключевые слова. Физически неклонируемая функция, кристалл, статическая память, FPGA.

Введение.

Согласно отчету Организации экономического сотрудничества и развития, за 2020 год во всем мире было продано контрафактных товаров на сумму около 2 триллионов долларов [1]. Данный факт является плохим признаком для потребителей и компаний, которые заказывают детали из разных источников по всему миру для создания своих продуктов, которые в большинстве случаев должны обладать высокой надёжностью и точностью выполнения работ. Изготовители контрафакта, как правило, используют сложные механизмы изменения, включающие множество стадий копирования и редактирования внутренней структуры продукта, в частности, микросхемы, что затрудняет проверку её происхождения и подлинности. Следовательно, компании могут получить имитационные детали, а их продукты станут менее надёжны и эффективны. В результате борьбы с контрафактной продукцией были предложены несколько технологий, среди них – усложнение структуры товара, применение водяных знаков, специальных рельефов, меток, системы маркировки и прослеживания товаров. Так, например, компания Intel для подтверждения авторских прав на этапе фотолитографического процесса наносила на кристаллы своих процессоров Intel 8086 специализированную метку. Одной из технологий защиты авторских прав при изготовлении микросхем является внедрение в структуру специализированных идентификаторов, единожды программируемых на одном из этапов производства, а затем считываемых при инициализации устройства или в процессе подтверждения соответствия при закупке комплектующих. Однако, данный метод защиты имеет большой недостаток – в случае утечки данных об алгоритме программирования идентификаторов злоумышленник может воспользоваться данным алгоритмом и внедрить его в контрафактную продукцию. Так, например, в январе 2022 года компания-производитель графических адаптеров Nvidia стала жертвой кибератаки, ответственность за которую взяла на себя хакерская группировка LAPSUS$, которая похитила с серверов около 1 Тбайт конфиденциальной информации, в частности, были получены ключи идентификации видеоадаптеров в системе, а также методы обхода ограничений для процессов получения криптовалюты. Впоследствии хакерская группировка обнародовала сертификаты для подписи кода, и злоумышленники уже начали использовать их для подписи вредоносных программ. Украденные сертификаты использовались для подписи, бэкдоров и троянов удаленного доступа. Подобные случаи указывают на необходимость разработки уникальных, неповторимых идентификаторов, получение которых не должно зависеть от методов разработки цифровой системы.

Защита цифровых устройств:

Как указывается в [2], одним из методов схемной обфускации как инструмента защиты цифровых устройств является внедрение генераторов констант (ГК). ГК — разновидность непрозрачных предикатов. ГК представляют собой схемы, генерирующие одно логическое значение постоянно. Сложность реализации ГК заключается в создании нераспознаваемых и неминимизируемых средством синтеза схем. Вариации технологических процессов изготовления интегральных схем вносят в их физическую структуру случайные, непредсказуемые изменения, делающие каждый экземпляр цифрового устройства уникальным, неповторимым и невоспроизводимым [3]. Использование физически неклонируемых функций позволяет решить данный класс задач с необходимыми условиями уникальности. Физически неклонируемая функция (англ. Physical Unclonable Function (PUF)) – это функция, воплощенная в физической

структуре, которую просто оценить, но трудно охарактеризовать, смоделировать или воспроизвести [4].

Синтез схемы ФНФ основанной на ячейках статической памяти в FPGA:

При реализации идентификаторов мы использовали ФНФ на основе поведения стандартной памяти SRAM, доступной в любом цифровом чипе. Для получения ячеек статической памяти на базе ПЛИС использовалось описание двух последовательно соединённых инверторов с обратной связью, которые в процессе синтеза преобразовываются в две ячейки LUT-1 (Рисунок 1). Каждая ячейка SRAM имеет свое собственное предпочтительное состояние при подаче питания на логический блок, т.е. при конфигурации ПЛИС. Эта случайность выражается в начальных значениях «неинициализированной» памяти SRAM. Следовательно, ответ SRAM дает уникальный и случайный набор нулей и единиц. Этот шаблон подобен отпечатку пальца, поскольку он уникален для конкретной SRAM и, следовательно, для конкретного чипа. Проводя экспериментальную часть работы в совместной с БГУИР учебной лаборатории компании SK hynix memory solutions Eastern Europe, авторы упаковывали такие идентификаторы в массивы 32-ух разрядных регистров численностью в 512 слов на 4-ех различных кристаллах отладочной платы Nexys-4 компании Digilent. Извлечение значений из ячеек производилось при помощи тридцати двух 512-ти разрядных мультиплексоров и 32-ух разрядного софт-процессора MicroBlaze в виде IP-ядра компании Xilinx. При проведении эксперимента, каждая из плат конфигурировалась, отправляла на хост-машину последовательность из 512 слов, затем процесс повторялся 99 раз. Стоит отметить, что в процессе конфигурации ПЛИС, происходит её сброс, соответственно ячейки статической памяти возвращаются к исходному состоянию. Для обеспечения независимости измерений и недопущения перегрева ячеек, каждому процессу конфигурации предшествовала пауза длительностью в 20 секунд, что позволило нивелировать влияние переходных процессов и повышений температуры в кристалле на результаты тестирования.

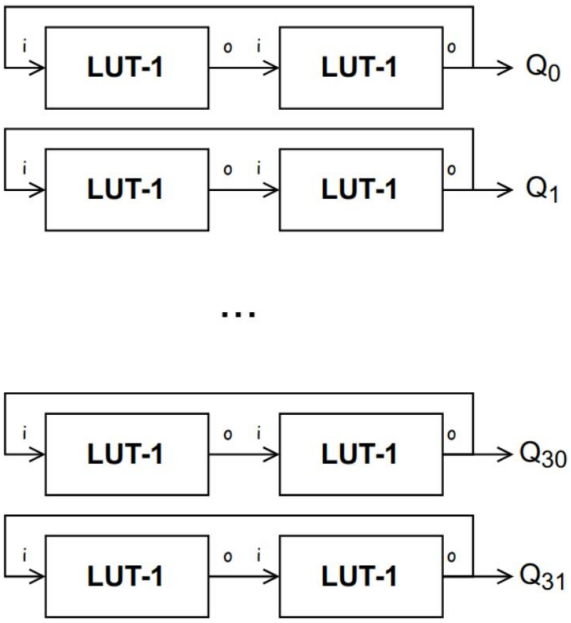

Рисунок 1. Схемотехническое исполнение ячейки статической памяти на двух инверторах с обратной связью с использованием элементной базы ПЛИС 7 серии компании Xilinx

Анализ основных характеристик, полученных ФНФ:

Проведенные исследования показывают, что каждая ячейка статической памяти при инициализации может принимать либо значение логического «0», либо логической «1», однако, как показывает мировая практика [5], часть ячеек не имеет чётких значений при инициализации между сбросами и может вести себя нестабильно, что приводит к невозможности использования в ГК и, как в следствие в системах идентификации. Для обеспечения надёжности и уникальности идентификаторов необходимо исключить из реализации нестабильные ячейки, для этого на этапе производства статическая память проходит проверку на пригодность к использованию в качестве идентификатора, затем полученная информация используется для программирования либо конфигурирования систем коррекции ФНФ [5]. Используя полученные данные в результате эксперимента, мы определили нестабильные ячейки памяти, рассчитали их распределения относительно логической единицы и нанесли полученные данные на тепловые карты для каждого из кристаллов. На рисунке 2 изображена одна полная тепловая карта и четыре фрагмента карт,

взятых из одного расположения, различных кристаллов. На рисунке крестиками обозначены нестабильные ячейки, черными – стабильные нули, белыми – стабильные единицы.

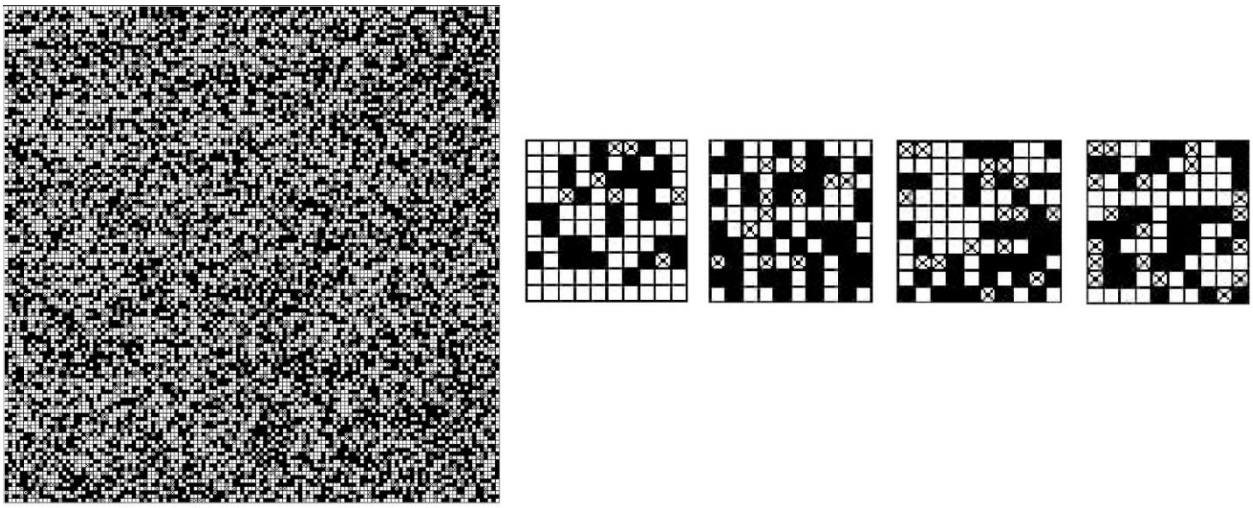

Рисунок 2. Тепловая карта сборок статической памяти на различных кристаллах.

Проанализировав полученные данные, мы пришли к выводу, что нестабильные ячейки более склонны к установке в логическую единицу, чем в ноль, а их количество относительно общей массы ячеек не превышает 15%, при этом, стоит отметить, что стабильными ячейками мы считали только те, которые на протяжении всех 100 опытов не изменяли свой логический уровень.

Метрики различия и уникальности идентификаторов:

При проведении анализа метрик различия нами были применены три различные функции расстояний по Хэммингу, одна для троичного и две для пятеричного алфавитов, так, каждый символ в алфавите соответствует диапазону вероятностей выпадения единицы в каждой из ячеек памяти. В троичном алфавите (0, X, 1) за единицу либо ноль принимались лишь те ячейки, которые не изменяли свои значения во всех экспериментах, остальные принимали значение X в пятеричном алфавите, каждый из символов соответствовал 20% приращению вероятности появления единичного символа (Таблица 2). Веса второй целевой функции расстояний по Хэммингу в случае 5-ричного алфавита были подобраны исходя из наблюдений, что среди ячеек имеют место быть элементы, стремящиеся к одному из двоичных уровней, но не принимающие однозначного значения на протяжении всех тестов.

Таблица 2 – Коэффициенты целевой функции расстояния по Хэммингу для пятизначного алфавита.

	0	L	X	H	1
0	0	0,25	0,5	0,75	1
L	0,25	0	0,25	0,5	0,75
X	0,5	0,25	0	0,25	0,5
H	0,75	0,5	0,25	0	0,25
1	1	0,75	0,5	0,25	0

Приведём пример расчёта удельного расстояния по Хэммингу для пятизначного алфавита:

Слово 1:	0	0	X	1	0	L	1	H
Слово 2:	L	0	1	X	0	1	0	L
Частичное расстояние:	0,25	0	0,5	0,5	0	0,75	1	0,5

Общее расстояние: 0,25 + 0 + 0,5 + 0,5 + 0 + 0,75 + 1 + 0,5 = 3,5/8 = 0,4375

Исходя из полученных расстояний по Хэммингу (Таблица 3), можно сделать вывод: среднее удельное расстояние стремится к значению в 0,49, при этом ни в одной из тепловых карт не было получено абсолютно одинаковых или противоположных друг другу слов.

Таблица 3 – Расстояния по Хэммингу.

	Плата 1	Плата 2	Плата 3	Плата 4	Среднее
Расстояние Хэмминга (0, X, 1) (0,5 – 0,5)					
Среднее,%	0,4886	0,4901	0,4867	0,4926	0,4895
Максимальное,%	0,8593	0,8906	0,8437	0,8750	0,8671
Минимальное,%	0,0781	0,0468	0,0781	0,0312	0,0585
Расстояние Хэмминга (0, L, X, H, 1) (0,25 – 0,25 – 0,25 – 0,25)					
Среднее,%	0,4932	0,4941	0,4920	0,4955	0,4937
Максимальное,%	0,8671	0,8984	0,8281	0,8750	0,8671
Минимальное,%	0,1171	0,0546	0,1015	0,0390	0,0782
Расстояние Хэмминга (0, L, X, H, 1) (0,1 – 0,4 – 0,4 – 0,1)					
Среднее,%	0,4945	0,4948	0,4942	0,4963	0,4949
Максимальное,%	0,8625	0,9031	0,8375	0,8750	0,8695
Минимальное,%	0,1125	0,0591	0,0968	0,0343	0,0757

Так как генераторы на основе ФНФ действительно случайны, что позволяет использовать их в аппаратных реализациях криптографических алгоритмов, например, в качестве генераторов секретных ключей [6], для использования ФНФ SRAM необходимо убедиться в характеристиках уникальности между разными идентификаторами как на одном кристалле, так и между несколькими. Для определения таких параметров авторами использовалась нормированная в диапазоне [0;1] метрика единообразия, которая вычислялась для каждого слова, при этом, была применена двоичная система счисления, где нулю соответствовали вероятности выпадения единицы от 0 до 0,5, а единице – от 0,51 до 1 (Формула 1). При этом, стоит отметить что при вычислении характеристики уникальности идентификаторов, имел место быть случай, с нулевой уникальностью. Такой случай возможен только тогда, когда идентификатор состоит полностью из единиц либо нулей. В результате проведения эксперимента был обнаружен всего один такой идентификатор из 2048 на 4-ех различных кристаллах. На рисунке 3 приведена гистограмма полученных значений уникальности идентификаторов среди 4-ех различных кристаллах.

$$U = 1 - 2 \times \left| \frac{WH(V)}{N} - 0.5 \right|, \quad (1)$$

где *V* – слово разрядности *N*.

Таблица 4 – Полученные значения внутрикристального единообразия идентификаторов.

	Плата 1	Плата 2	Плата 3	Плата 4	Среднее
Среднее	0,8244	0,8133	0,8211	0,8248	0,8209
Максимальное	1	1	1	1	1
Минимальное	0,1875	0,1250	0,1250	0	0,1093

Помимо подтверждения свойств уникальности и неповторимости идентификатора в одном кристалле необходимо также подтверждать их межкристальное различие. Для проверки последнего, нами были получены метрики различия в виде расстояний по Хэммингу между 4-мя кристаллами ПЛИС, при этом применялось вычисление расстояний «каждый с каждым», что позволило проверить все возможные сочетания идентификаторов. Межкристальное среднее удельное расстояние по Хэммингу для троичной системы счисления составило 0,491, максимальное – 0,875, минимальное – 0. Полученные расстояния указывают на то, что в среднем идентификаторы между кристаллами по-прежнему уникальны между собой, однако, имеют место

быть случаи, когда на двух различных кристаллах идентификаторы совпадают. При вычислениях для 4-ех различных кристаллов, мы получили всего 2 случая совпадения из 1572864, что составляет 0,000127% от общего количества сравнений.

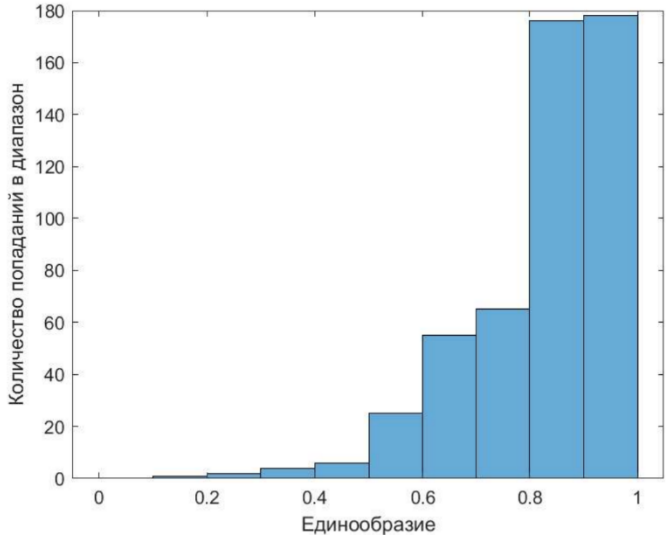

Рисунок 3. Гистограмма средней уникальности между 4-мя кристаллами.

Заключение:

Проведя исследование и анализ поведения ячеек статической памяти, реализованной на FPGA при инициализации, их метрик уникальности и различия мы получили данные о количестве стабильных и нестабильных ячеек, убедились в склонности к инициализации SRAM в уровень логической единицы, построили тепловые карты для 4-ех различных кристаллов ПЛИС, провели анализ межкристальной уникальности идентификаторов. Полученные данные свидетельствуют о том, что применение физически неклонируемых функций на основе статической памяти в силу характеристик случайности и уникальности пригоден для использования в механизмах защиты цифровых схем от несанкционированного использования, копирования, модификации, а также в системах идентификации устройств. Кроме этого, были выявлены повторяющееся межкристальные и нестабильные внутрикристальные идентификаторы, что указывает на необходимость разработки инструментов коррекции для достижения действительной уникальности и дальнейшего использования в системах идентификации.

Список использованных источников

1. *Counterfeiting and piracy in 2021 – the global impact Danny Grajales Pérez-y-Soto International Chamber of Commerce 11 May 2021*
2. *Сергейчик, В. В. Генераторы констант как базовые примитивы схемной обфускации / В. В. Сергейчик // Компьютерные системы и сети: материалы 50-й научной конференции аспирантов, магистрантов и студентов (Минск, 24-28 марта 2014 г.). – Минск: БГУИР, 2014. – С. 78 - 79.*
3. *Иванюк А. А. Синтез симметричных путей физически неклонируемой функции типа арбитр на FPGA / А. А. Иванюк // Информатика. - 2019. –Т.16, № 2. –С. 99-108.*
4. *Заливако С.С., Иванюк А.А. Схемная реализация комбинированной физически неклонируемой функции для генерирования действительно случайных числовых последовательностей. Доклады БГУИР. 2013; (7):37-43.*
5. *Farha, Fadi & Ning, Huansheng & Liu, Hong & Yang, Laurence & Chen, Liming. Physical Unclonable Functions Based Secret Keys Scheme for Securing Big Data Infrastructure Communication. Information Sciences (2019).*
6. *Иванюк, А. А. Физическая криптография и защита цифровых устройств / А. А. Иванюк, С. С. Заливако // Доклады*

БГУИР. – 2019. – №2 (120). – С. 50–58.

UDC 004.056.53

IDENTIFICATION OF DIGITAL DEVICES USING BISTABLE ELEMENTS IMPLEMENTED ON FPGA

Kaiky M.

Belarusian State University of Informatics and Radioelectronics[1], Minsk, Republic of Belarus

Ivaniuk A.A. – Doctor of Sciences in Technology

Annotation. This work is devoted to the study of on-chip and inter-chip static memory cells built on two feedback inverters. An example of calculating Hamming distances in ternary and quinary number systems is given to analyze the difference between unstable identifiers. Thermal maps of static memory cells are constructed considering unstable elements, and the possibilities of using such physically non-cloneable functions in digital circuit protection and identification systems are considered.

Keywords. Physically non-cloneable function, chip, static memory, FPGA.