ПРИМЕНЕНИЕ ФИЗИЧЕСКОЙ КРИПТОГРАФИИ В УСТРОЙСТВАХ НА БАЗЕ FPGA

Карбовский Д.В.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Иванюк А.А. – д-р. техн. наук, доцент

Данная работа описывает применение методов физической криптографии для защиты софт-процессоров на базе FPGA от нелицензированного использования. Проводится исследование результатов применения физически неклонируемой функции типа арбитр. Приводятся значения метрик для различных конфигураций.

Роль вычислительных устройств на базе полупроводниковых технологий неоценима в современном мире. Разработка и производство полупроводниковых кристаллов, однако, являются крайне дорогими процессами и связаны с большими рисками. Это привело к потребности в создании платформы для прототипирования полупроводниковых устройств, а также поиска альтернативных способов создания устройств. Таким решением стали устройства на базе FPGA (Field-Programmable Gate Array – программируемая логическая матрица). В отличие от устройств типа ASIC (Application-Specific Integrated Circuit – интегральные схемы конкретного предназначения), где архитектура микропроцессора предопределена его архитектурой, устройства типа FPGA содержат набор базовых элементов (элементы логики, памяти, коммуникации и т.д.), соединения между которыми устанавливаются конфигурацией. Такой подход позволяет использовать кристаллы с готовым набором элементов, лишь меняя конфигурацию устройства, но не его топологию. Это позволяет дешёвое прототипирование вычислительных устройств и даже использование FPGA в качестве базы для готовых устройств.

Одной из проблем такого подхода является проблема распространения файла конфигурации кристалла FPGA. Одна и та же конфигурация, загруженная в аналогичный кристалл, приведёт к созданию логической копии выпускаемого устройства. Поскольку конфигурация не хранится кристаллом, а передаётся из внешнего источника, такая архитектура устройства является крайне уязвимой к нелегальному копированию. Для защиты конфигурации устройства от нелегального использования применяются методы физической криптографии, в частности, физически неклонируемые функции (ФНФ). Такие функции используют особенности физических объектов для формирования ответов для набора запросов. Набор таких пар запросов-ответов является уникальным для каждого устройства. Для определения качеств ФНФ были разработаны метрики оценки, такие как стабильность и уникальность.

Примером физически неклонируемой функции является ФНФ типа арбитр. Данная функция использует разницу в длине физических путей на кристалле. Даже топологически одинаковые пути ввиду технологической несовершенности будут отличаться по длине. Это приводит к тому, что чаще всего по одному из путей сигнал будет проходить быстрее, чем по другому.

Разработка устройств на базе FPGA происходит в автоматизированных средах разработки. Инженер пользуется языками описания аппаратуры, код на которых транслируется в бинарный файл. Среда проектирования выбирает базовые элементы и линии для соединения на кристалле, используя алгоритмы оптимизации, длины путей и использования кристалла. Внесение даже незначительных изменений в описание устройства может повлечь создание совершенно другой конфигурации с отличным использованием элементов чипа. Как следствие этого, выбор соединительных линий может значительно измениться в сравнении с предыдущим описанием.

Нелегальное использование конфигурации устройства подразумевает различные способы копирования. Помимо обычного копирования злоумышленник может использовать дополнительный инструментарий для восстановления проекта из битового файла, внести изменения в проект и синтезировать устройство с собственным функционалом.

Использование физически неклонируемых функций позволяет устройству на базе FPGA производить самоверификацию. ФНФ позволяет получить уникальный отпечаток для данного кристалла. Отпечаток представляет собой набор битов, которые устройство сравнивает с контрольным значением. Если значения не совпадают, устройство может не включаться. В таком случае, простое копирование описания на другой кристалл не позволит клонировать продукт.

В случае, если злоумышленник меняет описание устройства, повторный синтез конфигурации приведёт к изменению соединительных путей, и, как следствие, изменению времени прохода сигнала по ним. Это влечёт изменения в работе всех физически неклонируемых функций. Как итог, множество их ответов изменяется и перестаёт совпадать с контрольными значениями. Это является эффективным методов защиты от нелегального копирования устройств на базе FPGA.

Для оценки работы физически неклонируемых функций используются различные метрики. Самые важные метрики в данном контексте – это стабильность работы и уникальность функции. Стабильность работы необходима для обеспечения одинаковых ответов на запросы для большинства ситуаций. Она выражается относительной величиной и означает долю корректных ответов. Уникальность может быть разделена на две категории: внутрикристальную и межкристальную. Для расчёта уникальности анализируется набор ФНФ, реализованных в аппаратуре. Набор, расположенный на одном кристалле, используется для получения внутрикристальной уникальности, а на различных – межкристальной. Уникальность ФНФ рассчитывается как сумма удельных хеммингових расстояний между наборами ответов на один и тот же запрос.

Одна из реализаций ФНФ типа арбитр использует цепочку мультиплексоров и линии соединения между ними [1]. Изменение значения управляющего сигнала переключает используемые линии, изменяя длину полного пути. Схема ФНФ типа арбитр представлена на рисунке 1.

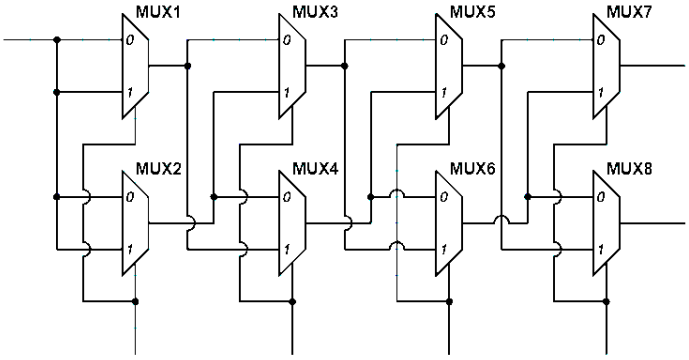

Рисунок 1 – Схема физически неклонируемой функции типа арбитр на базе цепочки из мультиплексоров.

Данная схема была реализована на языке VHDL с использованием софт-процессора Microblaze в среде проектирования Vivado. Тесты производились на плате Nexys 4 на базе кристалла Artix 7. Описание аппаратуры было синтезировано в различных конфигурациях (количество реализованных ФНФ на кристалле, длина арбитра) и протестировано с различными параметрами. Целью тестов было исследование изменения метрик для разных конфигураций. Стабильность для всех конфигураций составила более 0.99 для всех тестов. Результаты тестов приведены в таблице 1.

Таблица 1 – Результаты тестирования

Длина арбитра (ширина запроса)	Количество запросов при тестировании	Внутрикристальная уникальность	Межкристальная уникальность
8	256	0.38 (38%)	0.0156 (1.56%)
10	256	0.40 (40%)	0.0195 (1.95%)
12	256	0.35 (35%)	0.0008 (0.08%)
14	256	0.35 (35%)	0.0040 (0.40%)
16	1024	0.36 (36%)	0.0156 (1.56%)
18	1024	0.37 (37%)	0.0137 (1.37%)
20	1024	0.43 (43%)	0.0117 (1.17%)
22	1024	0.44 (44%)	0.0186 (1.86%)
24	1024	0.38 (38%)	0.0117 (1.17%)
26	1024	0.41 (41%)	0.0225 (2.25%)
28	1024	0.41 (41%)	0.0225 (2.25%)
30	1024	0.41 (41%)	0.0098 (0.98%)
32	1024	0.38 (38%)	0.0215 (2.15%)

Полученная межкристальная уникальность для простой реализации низкая. Эксперименты показали, что увеличение длины ФНФ типа арбитр не приводят к однозначным улучшениям показателей, в то время как внутрикристальная уникальность достаточно высокая. Выгоднее всего использовать несколько копий более дешёвой реализации для достижения лучшей защиты.

Проектирование и производство вычислительных устройств – дорогостоящие процессы. Некоторые устройства выпускаются на базе FPGA и нуждаются в защите от нелегального копирования. Методы физической криптографии позволяют защитить конфигурацию от использования на нелицензированном кристалле. ФНФ типа арбитр требует подбора длины и других параметров для получения высокой уникальности, но недорога в реализации и обладает хорошей стабильностью, пригодной для уникальной идентификации полупроводниковых кристаллов.

Список использованных источников:

1. Ярмолик, В.Н. Физически неклонируемые функции / В.Н. Ярмолик, Ю.Г. Вашинко // Информатика. -- 2011. – № 2 (30). – С. 92-103.