ПРИМЕНЕНИЕ ЗАПОМИНАЮЩИХ УСТРОЙСТВ В КАЧЕСТВЕ КРИПТОГРАФИЧЕСКИХ ПРИМИТИВОВ ДЛЯ ИНТЕГРАЛЬНЫХ СХЕМ ПРОГРАММИРУЕМОЙ ЛОГИКИ

А. В. Пучков, А. А. Иванюк
ООО «Софтек Флеш Солюшнс»
Кафедра информатики, Белорусский государственный университет информатики и радиоэлектроники
Минск, Республика Беларусь
E-mail: alexander.v.puchkov@gmail.com, ivaniuk@bsuir.by

Рассматриваются проблемы защиты цифровых систем от несанкционированного использования, в частности проблема идентификации и использование для ее решения таких криптографических примитивов, как физически неклонируемые функции (ФНФ). Представлены актуальные проблемы ФНФ. Показана целесообразность использования для ПЛИС реализаций ФНФ на основе запоминающих устройств.

Введение

Стремительное развитие рынка цифровых устройств и систем, в частности заказных интегральных схем, ставило и продолжает ставить перед разработчиками множество сложных задач, часто не имеющих однозначно приемлемого решения, и связанных с защитой разработанных аппаратных средств. Понимая защиту в широком смысле, отнесем к этой категории методы не только защиты от неблагоприятных условий окружающей среды, но и от несанкционированных действий человека. Последние обретают все большую актуальность, поскольку как произведенные аппаратные средства, так и их проектные описания в любом виде являются потенциальным объектом для противоправных действий, таких как обратное проектирование и производство копий устройства вне рамок соглашений с автором. Это приносит убытки, не только сопоставимые, но значительно превосходящие те, которые могут быть вызваны техническими проблемами надежности, не связанными напрямую с человеческим фактором, и решаемые в той или иной мере методами проектирования контролепригодных и ремонтопригодных устройств.

Усложняет проблему и тот факт, что ее решение не может быть осуществлено исключительно программными средствами. Ответом на данную проблему стало возникновение в начале 2000-х годов физической криптографии [1]. Ее подходы вместо того, чтобы полагаться на некие защищенные компоненты в виде запоминающих устройств, хранящих ключи шифрования для применения в аутентификации, основываются на присущих физическим системам вообще, и цифровым системам в частности, уникальных и невоспроизводимых характеристиках. Это позволяет приблизиться к тому, чтобы цифровая криптосистема была физически невзламываемой, что само по себе является важнейшей целью, достижение которой решило бы целый ряд актуальных задач в проектировании устройств, защищенных от несанкционированных действий человека. И хотя в физической криптографии в настоящее время существует множество нерешенных проблем, ее достижения могут быть применены в настоящее время и уже применяются крупнейшими производителями аппаратных средств.

Одним из ключевых понятий физической криптографии является физически неклонируемая функция (ФНФ, англ. Physical Unclonable Function, PUF). Применимо к цифровым системам ФНФ предстставляет собой устройство, в основе функционирования которого лежит тот факт, что при современных технологических нормах цифровые устройства подвержены влиянию вариаций технологического процесса, которое приводит к тому, что физические параметры интегральных схем в некоторой их выборке оказываются случайно распределенными. Это не оказывает существенного влияния на работоспособность цифровых схем, но является по своей природе близким к идеальному источником как энтропии при построении генераторов истинно случайных последовательностей, так и стабильных уникальных идентификаторов в рамках решения задачи идентификации и аутентификации. Последнее возможно потому, что физические параметры интегральных схем, испытывающие влияние вариаций технологического процесса, остаются принципиально уникальными для каждого из кристаллов, причем не представляется возможным управлять их значениями. Формально ФНФ можно описать значениями пар входных сигналов запроса $c \in C$ (Challenge) и соответствующих им выходных выходных сигналов ответа $r \in R$ (Response). С математической точки зрения ФНФ является функцией, отображающей множество запросов C на множество ответов R: $r = PUF(c)$.

I. Актуальные проблемы ФНФ

Поскольку ФНФ, разработанные в рамках цифровых устройств, основываются в своем функционировании на физических вариаци-

ях технологического процесса производства интегральных схем, то генерируемые с их помощью пары запрос-ответ имеют двойственную природу: с одной стороны они теоретически уникальны для каждого устройства и ими невозможно управлять, с другой же стороны они являются потенциальным источником энтропии даже в рамках серии измерении ответов на один и тот же запрос. Это приводит к тому, что на практике всегда существует некоторое множество нестабильных пар запрос-ответ, которые являются крайне нежелательными для решения задачи идентификации цифровых устройств и систем. Поэтому в рамках данной задачи так или иначе решают проблему стабилизации пар запрос-ответ. Это можно делать как с помощью схемотехнических решений, так и управляя последовательностью запросов [2]. Отметим, что данная проблема принципиально не актуальна для задачи генерации псевдослучайных последовательностей, а даже улучшает свойства построенных на ФНФ подобных генераторов.

В связи с тем, что реализации ФНФ подвергаются усовершенствованию для снижения влияния присущих им недостатков, качественные характеристики ФНФ должны быть объектом количественного анализа. Для оценки полученных пар запрос-ответ применяют метрики, среди которых основную роль играют оценки уникальности, случайности, стабильности. Выраженные в общем виде через запросы и ответы ФНФ, они позволяют оценить качество тех или иных, порой различных по своей природе реализаций ФНФ [2]. Несмотря на существование в научной литературе общего понимания того, какими должны быть базовые характеристики и их значения, предлагались и продолжают предлагаются более сложные метрики, характеризующие качество реализаций ФНФ для конкретных приложений [2].

II. ФНФ для ПЛИС

В настоящее время программируемые логические интегральные схемы (ПЛИС) являются перспективной платформой для реализации цифровых устройств и систем. Изначально широко применявшиеся для прототипирования цифровых систем, которые в дальнейшем реализовывались в виде заказных интегральных схем, ПЛИС используются для построения сложных систем на кристалле (System on a Chip, SoC). В этой связи о них говорят как о программируемых системах на кристалле (Programmable SoC, PSoC).

Важным компонентом любой ПЛИС является статическое ОЗУ (SRAM), используемое для хранения ее конфигурации. Кроме данного ОЗУ, в распоряжении разработчика оказываются другие схемы памяти, такие как Block RAM, память LUT, и даже простые синхронные триггеры. Более того, используя базовую логику ПЛИС, можно реализовать элементы памяти, сымитировав с некоторой степенью приближения элементарную ячейку SRAM. Современные платы прототипирования на основе ПЛИС часто оснащаются внешними ОЗУ на базе динамической памяти (DRAM) большого объема, что еще больше расширяет спектр доступных видов схем памяти.

В этой связи удобной для ПЛИС представляется реализация ФНФ на основе запоминающих устройств SRAM или DRAM. В этом случае подобные схемы памяти после подачи на них питающего напряжения имеют случайное, но уникальное распределение нулей и единиц, что соответствует пониманию ФНФ. В этом случае говорят о таком виде ФНФ как ФНФ на основе статического ОЗУ (SRAM PUF). То же справедливо и для DRAM. Однако некоторая доля ячеек ОЗУ устанавливается при в включении питания в некоторое состояние только с определенной вероятностью, а значит подобным ФНФ также присущи проблемы стабилизации.

Для исследования данного вида ФНФ была разработано аппаратно-программное решение, позволяющие взаимодействовать с реализацией DRAM PUF. В состав данного комплекса входит 10 плат на основе ПЛИС Xilinx Artix-7, оснащенной 128 Мбит оперативного запоминающего устройства типа DRAM. При этом передача данных между рабочей станцией и ПЛИС осуществляется по протоколу UART. Задача комплекса состоит в получении текущего состояния DRAM с целью последующего анализа.

III. Заключение

Удобство использования ресурсов памяти современных интегральных схем программируемой логики делает весьма актуальным использование криптографических примитивов типа SRAM/DRAM PUF на их основе. В рамках работы был спроектирован аппаратно-программный комплекс, позволяющий получить состояние DRAM для последующего анализа, с помощью которого получен ряд экспериментальных результатов. Стоит отметить, что важной задачей в реализации данного комплекса является организация автоматизированного включения и выключения устройств для сброса схем памяти. В этом направлении продолжаются усовершенствования, что позволит максимально точно смоделировать подобные процессы в продуктах, выпускаемых на основе ПЛИС.

1. Pappu, R. Physical One-Way Functions / R. Pappu // PhD Thesis. – MIT, 2001. – 154 p.
2. Zalivaka, S.S. Multi-valued arbiters for quality enhancement of PUF responses on FPGA implementation / S.S. Zalivaka, A.V. Puchkov, V.P. Klybik, A.A. Ivaniuk, C.H. Chang // Special Session on Cyber-Physical Systems and Security, in Proc. 21st IEEE Asia and South Pacific Design Automation Conf. (ASP-DAC 2016), Macao, China, 26-28 Jan. 2016. – P. 533-538.