S. V. Sukhanov

Analysis of Physical Unclonable Functions Based on Memory

Key words: *physical unclonable function (PUF), SRAM, latch*

The article discusses the constructions of physical unclonable functions (PUF) based on memory. The analysis of different constructions and conclusion is given.

С. В. Суханов

АНАЛИЗ ФИЗИЧЕСКИ НЕКЛОНИРУЕМЫХ ФУНКЦИЙ НА ОСНОВЕ ЭЛЕМЕНТОВ ПАМЯТИ

В настоящее время электронные устройства получили широкое распространение во многих сферах жизни человека. Для защиты конфиденциальной информации используются системы шифрования, позволяющие ограничить к ней доступ третьим лицам. При создании таких систем предполагается, что информация о секретных ключах злоумышленнику недоступна. Проблема хранения секретных ключей систем шифрования является одной из важнейших проблем как с теоретической, так и с практической точки зрения [1].

К инновационным способам безопасного хранения ключей относится использование физически неклонируемых функций (ФНФ). ФНФ позволяет создавать ключи для систем шифрования на основе уникальной информации, содержащейся в сложной физической структуре интегральной схемы (ИС), при этом ключи «существуют» только во время работы ИС, что позволяет отказаться от их хранения в постоянной памяти.

Для оценки надежности ФНФ используются два показателя:

- *внутричиповое отклонение* — изменение выходного сигнала, в процентном исчислении, при повторяющемся запросе на одной ФНФ. В идеальной ФНФ данный показатель должен быть равен 0 %.

- *междучиповое отклонение* — изменение выходного сигнала, в процентном исчислении, при повторяющемся запросе на двух ФНФ, выполненных на одном или разных кристаллах. В идеале, когда обе ФНФ представляют абсолютно симметричные схемы, данная вероятность равняется 50 %.

Сравнение различных конструкций было произведено в [2]. В данной статье будут рассматриваться подходы к реализации ФНФ на основе элементов памяти.

1. ФНФ на основе СОЗУ

Статические оперативные запоминающие устройства (СОЗУ) широко используются в вычислительной технике для хранения данных. Непосредственно запоминающий элемент СОЗУ (ячейка) состоит из четырех транзисторов, реализующих два инвертора с перекрестными обратными связями. Подобная ячейка всегда находится в одном из двух состояний, что, в свою очередь, позволяет использовать ее для хранения 1 бита информации. Реализация ФНФ на основе ячейки СОЗУ изображена на рис. 1.

Экспериментально подтверждено, что большинство ячеек СОЗУ при включении питающего напряжения преимущественно переходят в одно из двух состояний [3]. Причиной этого является то, что каждая ячейка СОЗУ, представляющая собой *RS*-триггер, в силу особенностей технологии изготовления имеет множество несимметричных элементов. К таким элементам можно отнести длины соединительных проводников, их геометрические размеры, неоднородность физических и химических свойств кремния, девиацию задержек сигналов и др.

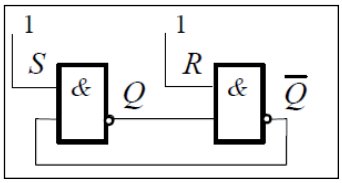

Рис. 1. ФНФ на базе ячейки СОЗУ, реализованной в виде RS-триггера

2. ФНФ на основе одноступенчатого триггера (latch)

Данная ФНФ является технологией, основанной на оседающем состоянии двух парно-пересекающихся логических элементов ИЛИ-НЕ, которая представляет собой простой RS одноступенчатый триггер (latch). Утверждением сигнала сброса триггер вынужденно переходит в нестабильное состояние, и, когда освобождается, он сходится в стабильном состоянии, в зависимости от внутреннего несоответствия между элементами ИЛИ-НЕ. Возможна эквивалентная схема ФНФ со структурой ячеек, основанных на парно-пересекающихся элементах И-НЕ, как показано на рис. 2.

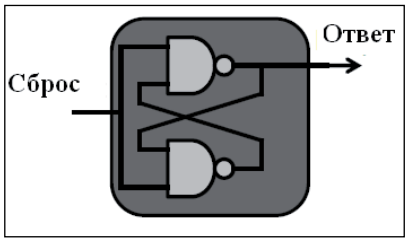

Рис. 2. ФНФ на базе одноступенчатого триггера «Защелка»

Реальное преимущество такой конструкции ФНФ над СОЗУ ФНФ в том, что поведение ФНФ не полагается на состояние подачи питания, а может вызываться в любое время, когда устройство работает. Это означает, что секретные ключи, генерируемые ФНФ, не обязательно должны постоянно храниться в течение активного времени устройства, но могли бы быть воссозданы в любое время. Кроме того, это позволяет измерять множественные вычисления каждого ответа, что дает возможность повысить надежность с помощью методов постобработки, таких как «мажоритарное решение» [4].

3. ФНФ типа бабочка

Данная конструкция основывается на формировании перекрестных обратных связей с использованием стандартных триггеров (рис. 3), применяемых в программируемых логических матрицах. В результате структура запоминающей ячейки ФНФ типа бабочка оказывается настолько симметричной, насколько это возможно. Подобная ячейка строится как схема с перекрестными обратными связями, которые используются в ФНФ на базе запоминающих ячеек СОЗУ. Используя функциональность: предустановка/сброс триггера, эта схема может быть принудительно переведена в нестабильное состояние и вновь сойтись только после сброса. Следует отметить, что в связи с дискретными опциями маршрутизации FPGA не так просто реализовать ячейку таким образом, чтобы несоответствие конструирования было мало. Это является необходимым условием, если кто-то хочет случайного несоответствия, вызванного вариациями производства [5].

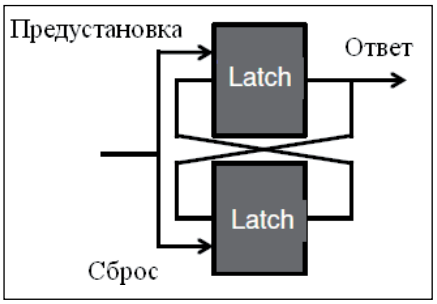

Рис. 3. ФНФ типа бабочка

4. ФНФ типа бускипер (Buskeeper)

Бускипер — слабая схема «защелки», которая хранит последнее значение шины с тремя состояниями.

Схемой, в основном, является элемент задержки с выходом, соединенным со входом через относительно высокий импеданс. Это обычно достигается с помощью двух инверторов, подключенных «спиной к спине» (рис. 4). Сопротивление проходит по шине слабо, поэтому другие схемы могут перекрыть значение шины, когда она не в режиме с тремя состояниями.

Бускипер используется для препятствия получения КМОП (комплементарный металлооксидный полупроводник) транзисторов переменных значений, когда они соединены в сеть с тремя состояниями. В противном случае оба транзистора в затворе могут возбудиться, и, таким образом, происходит короткое замыкание между источником питания и заземления, что приводит к разрушению затвора транзистора. Этому препятствует бускипер, извлекая на входе последний действующий логический уровень (0 или 1) в сети. Схема обычно размещается параллельно с сетью с тремя состояниями.

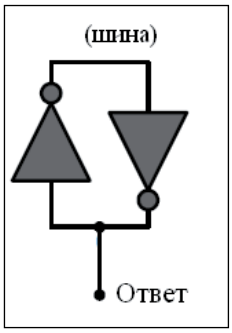

Рис. 4. Ячейка ФНФ типа бускипер

Преимущество этих ФНФ над другими бистабильными ячейками памяти ФНФ в том, что основная ячейка бускипера очень мала, например, по сравнению с обычным одноступенчатым триггером.

5. ФНФ MECCA

MECCA ((ME)mory (C)ell-based (C)hip (A)uthentication) — ФНФ, основанная на концепции механизмов отказа в массиве памяти. Это наблюдается более чем в 50 % однокристальных систем, которые используются для памяти [6].

Механизмы ошибок, наблюдаемые в ячейках памяти, приведены ниже:

- ошибки записи: происходят, когда внутренний узел в ячейке СОЗУ не может быть выпущен через проход транзисторов в течение активной продолжительности числовой шины;
- ошибки чтения: переброс данных в ячейки памяти во время операции чтения;

- ошибки доступа: происходят, когда разница напряжений между битовыми строками меньше, чем напряжение смещения усилителя считывания, когда он активен;
- ошибки занятости линии: когда напряжение питания снижается во время ожидания, утечка тока через n-МОП транзисторы может вызвать снижение внутреннего узлового напряжения ниже порога переключения инвертора для переброса данных.

Такая ФНФ использует факт, что большинство конструкций уже содержат встроенный массив памяти СОЗУ для их работы, и, следовательно, может быть использована для генерации последовательностей.

Основная идея — в управлении числовой шины рабочего цикла ячеек ФНФ для определения их уязвимости к отказам во время доступа для записи/считывания. Управляемость числовой шины позволяет генерировать множественные ответы из массива, и, следовательно, увеличивается число пар «запрос — ответ». Случайные вариации процесса производства параметров ячеек по всей микросхеме определяют надежность (низкую или высокую) ячеек; надежность ячеек переводится в цифровые ответы.

Выводы

Результаты экспериментов [4] показали, что ФНФ на основе одноступенчатого триггера очень чувствительна к изменениям температуры и подаваемого напряжения, вследствие чего внутричиповое отклонение увеличивается до 10 %. ФНФ типа бускипер весьма стабильно работает при различных напряжениях питания [5], однако при изменении рабочей температуры выходные значения становятся весьма нестабильными. ФНФ MECCA, наоборот, стабильно работает при различной рабочей температуре и нестабильно — при вариациях напряжения [6]. Наилучшие результаты работы продемонстрировала ФНФ типа бабочка [5], у которой при различных вариациях работы междучиповое отклонение = 50 % и внутричиповое отклонение < 5 %.

Таким образом, ФНФ типа бабочка является наиболее стабильной ФНФ на основе элементов памяти.

СПИСОК ЛИТЕРАТУРЫ:

1. *Лосоевский А. Ю.* Исследование и анализ схем извлечения уникальной информации о кристалле физически неклонируемой функцией на кольцевых осцилляторах в приложении к генерации ключей для систем шифрования // Материалы МНТК «Научные исследования и их практическое применение. Современное состояние и пути развития». Киев, 2012. С. 23–45.
2. *Суханов С. В., Коваленко А. П., Игнатенко И. А.* Сравнительный анализ конструкций кремниевых физически неклонируемых функций // Известия Института инженерной физики. 2014. № 2 (32). С. 2–6.
3. *Ярмолик В. Н., Вашинко Ю. Г.* Физически неклонируемые функции // Информатика. 2011. № 2. С. 92–103.
4. *Maes R.* Physically Unclonable Functions: Constructions, Properties and Applications. PhD thesis. Belgien. Katholieke Universiteit Leuven, 2012. – 215 p.
5. *Deutschmann M.* Cryptographic Applications with Physically Unclonable Functions. PhD thesis. Klagenfurt. Alpen-Adria-Universitat Klagenfurt, 2010. – 93 p.
6. *Krishna A., Narasimhan S.* MECCA: A Robust Low-Overhead PUF Using Embedded Memory Array // Workshop on Cryptographic Hardware and Embedded Systems. Nara, Japan. 2011. P. 407–420.

REFERENCES:

1. *Losoevskiy A. Y.* Analysis of integrated circuit unique sequence extraction schemes for ring-oscillator physical unclonable functions in application for cryptographic keys generation // Research and their practical application. Current status and the ways of development. Kiev, 2012. P. 23–45.
2. *Sukhanov S. V., Kovalenko A. P., Ignatenko I. A.* Comparative analysis of the structures of silicon physical unclonable functions // Proceedings of the Institute of Engineering Physic. 2014. № 2 (32). P. 2–6.

3. *Yarmolik V. N., Vashinko Y. G.* Physical unclonable function // Information. 2011. № 2. P. 92–103.
4. *Maes R.* Physically Unclonable Functions: Constructions, Properties and Applications. PhD dissertation. Belgium. Katholieke Universiteit Leuven, 2012. – 215 p.
5. *Deutschmann M.* Cryptographic Applications with Physically Unclonable Functions. PhD dissertation. Klagenfurt. Alpen-Adria-Universitat Klagenfurt, 2010. – 93 p.
6. *Krishna A., Narasimhan S.* MECCA: A Robust Low-Overhead PUF Using Embedded Memory Array // Workshop on Cryptographic Hardware and Embedded Systems. Nara, Japan. 2011. P. 407–420.