ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ
INFORMATION TECHNOLOGIES

УДК 004.056.55

Исследование физически неклонируемых функций на основе статической памяти

А.Ю. Лосевской

Национальный исследовательский университет «МИЭТ»
АО «НИИ молекулярной электроники» (г. Москва)

Study on Characteristics of SRAM Based Physical Unclonable Functions

A.Y. Losevskoy

National Research University of Electronic Technology, Moscow
JSC Molecular Electronics Research Institute, Moscow

Рассмотрена конструкция физически неклонируемой функции на основе статической памяти. Исследованы характеристики физически неклонируемых функций, изготовленных в 0,18-мкм КМОП-процессе. Показана возможность использования физически неклонируемых функций для генерации ключей систем шифрования.

Ключевые слова: статическая память; физически неклонируемая функция; криптографический ключ; SRAM; PUF.

The construction of the SRAM based physical unclonable functions, implemented with 0.18 μm CMOS process, have been studied. The possibility of using the unique sequences of physical unclonable functions as the cryptographic keys has been shown.

Keywords: static random access memory; physical unclonable function; unique sequence; cryptographic key; SRAM; PUF.

Введение. Традиционно для хранения криптографических ключей используются такие виды энергонезависимой памяти, как постоянное запоминающее устройство (ПЗУ), электронно-стираемое программируемое постоянное запоминающее устройство (ЭСППЗУ), сверхоперативное запоминающее устройство (СОЗУ) с батарейным питанием и др. Однако данные виды памяти подвержены физическим атакам, которые позволяют злоумышленнику извлечь ключ из устройства [1]. Защитные контрмеры в большинстве случаев приводят к значительному удорожанию конечного устройства.

Перспективным является использование физически неклонируемых функций (ФНФ). ФНФ – физический объект, встраиваемый в физическую структуру другого

объекта и реализующий функцию, которую легко вычислить, но сложно охарактеризовать (по существу, данная физическая функция является аналогом математической односторонней функции). ФНФ, встраиваемые в интегральные схемы (ИС), позволяют «на лету» генерировать криптографические ключи, что существенно усложняет проведение злоумышленником физической атаки.

В процессе производства ИС неизбежные случайные технологические вариации приводят к тому, что на микроскопическом уровне все ИС уникальны. Уникальность проявляется в том, что у идентичных с точки зрения топологии ИС электрофизические параметры элементов слегка отличаются друг от друга вследствие вариации длины и ширины канала транзисторов, толщины подзатворного окисла, концентрации легирующих примесей и пр. [2].

ФНФ встраивается в ИС в виде функционального блока. Ввиду случайных технологических вариаций ФНФ разных ИС будут иметь уникальные электрофизические характеристики. ФНФ позволяет представить данную уникальность в виде бинарной последовательности, которую можно использовать в качестве криптографического ключа или затравки для алгоритма генерации ключей.

В литературе приводится описание нескольких типов ФНФ, которые могут быть реализованы в большинстве КМОП-технологий: ФНФ на основе задержек [3], ФНФ типа «бабочка» [4], ФНФ на основе статической памяти [5] и др.

В настоящей работе представлены результаты исследования характеристик ФНФ на основе статической памяти, изготовленных в 0,18-мкм КМОП-процессе ОАО «НИИМЭ и Микрон», подтверждающие возможность использования ФНФ для генерации криптографических ключей.

ФНФ на основе статической памяти. В основе ФНФ лежит шеститранзисторная ячейка статической памяти, состоящая из двух инверторов с перекрестной обратной связью и двух ключевых транзисторов, обеспечивающих доступ к ячейке (рис. 1).

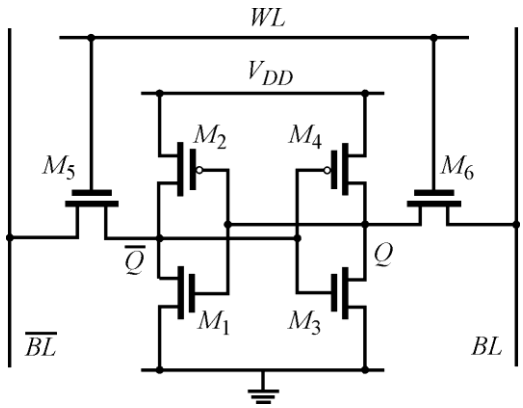

Рис.1. Шеститранзисторная ячейка СОЗУ

После подачи питания исходное состояние ячейки установится в одно из двух устойчивых логических состояний, что определяется технологическими вариациями и шумами внутри схемы. Если параметры транзисторов инверторов ячейки вследствие технологических вариаций отличаются существенно, то при повторных подачах питания исходное логическое состояние ячейки будет воспроизводимым. В противном случае на его выбор будут оказывать влияние как шумы внутри схемы (локальные флуктуации токов и напряжений), так и внешние параметры функционирования (напряжение питания, температура окружающей среды). Корреляции исходных логических состояний ячеек памяти разных ИС будут отсутствовать в том случае, если технологические вариации будут носить случайный характер. На основе исходных логических состояний ячеек могут быть сформированы бинарные последовательности, которые можно использовать как ключи, пароли и идентификаторы ИС.

ФНФ на основе статической памяти представляет собой массив шеститранзисторных ячеек. Для генерации бинарной последовательности необходимо произвести чтение массива после подачи на него питания.

Характеристики ФНФ. Основные характеристики ФНФ на основе статической памяти – уникальность и надежность. Для численной оценки характеристик используется понятие расстояния Хэмминга для двух последовательностей:

$$HD = \sum_{i=1}^{n} \left(2^{|a_i - b_i|} - 1\right),$$

где n – длина последовательности; a_i и b_i – значения i-х битовых позиций последовательностей a и b.

Уникальность ФНФ показывает, насколько бинарные последовательности разных ИС отличаются друг от друга. В идеальном случае, когда технологические вариации носят чисто случайный характер, среднее значение *HD* для уникальности ФНФ составляет величину, равную половине длины последовательности. На практике систематические вариации могут привести к снижению уникальности ФНФ. Связано это с тем, что транзисторы ячеек памяти разных ИС, имеющие одинаковое топологическое расположение, будут иметь схожие отклонения электрофизических параметров. Как следствие, исходные логические состояния таких ячеек будут совпадать, что негативно скажется на уникальности ФНФ.

Надежность ФНФ указывает на ее способность воспроизводить последовательность в случае повторных генераций при наличии внутрисхемных шумов, а также при изменении внешних параметров функционирования ИС. В идеальном случае последовательность должна быть полностью воспроизводимой при повторных генерациях. В действительности слишком малое различие параметров транзисторов инверторов некоторых ячеек приводит к тому, что в результате влияния внутрисхемных шумов и внешних параметров функционирования такие ячейки могут случайным образом выбирать одно из двух устойчивых логических состояний при повторных генерациях, что приводит к снижению надежности ФНФ.

Экспериментальное исследование характеристик ФНФ. В качестве образцов исследования использованы семь ИС, изготовленные в 0,18-мкм КМОП-процессе ОАО «НИИМЭ и Микрон». ИС представляет собой систему на кристалле, имеющую в своем составе массив статической памяти объемом 2048 байт. Результаты чтения массива сохранялись на ПК для дальнейшей обработки. Для оценки надежности ФНФ массив повторно считывался 21 раз. Для исследования влияния температуры на характеристики ФНФ чтение проводилось при температурах 25, 50 и 70 °С.

Длина бинарной последовательности выбрана равной 16 байт (128 бит). Таким образом, для каждой ИС было получено 128 бинарных последовательностей.

На рис. 2 представлены гистограммы уникальности ФНФ для различных значений температуры окружающей среды (здесь и далее N – число попаданий в интервал; u – среднее значение *HD*; *std* – стандартное отклонение *HD*). Из рисунка следует, что температура не оказывает заметного влияния на уникальность. Среднее значение *HD* близко к идеальному (половина длины последовательности, т.е. 64 бита), что указывает на преимущественно случайный характер технологических вариаций.

На рис. 3 представлена надежность ФНФ для различных значений температуры окружающей среды. Как видно из рисунка, повышение температуры приводит к незначительному снижению надежности. Это связано с тем, что рост температуры обусловливает увеличение внутрисхемных шумов и, как следствие, увеличивается число ячеек памяти, устойчивое состояние которых определяется шумами (как уже отмечалось, это актуально для ячеек, параметры транзисторов инверторов которых отличаются незначительно).

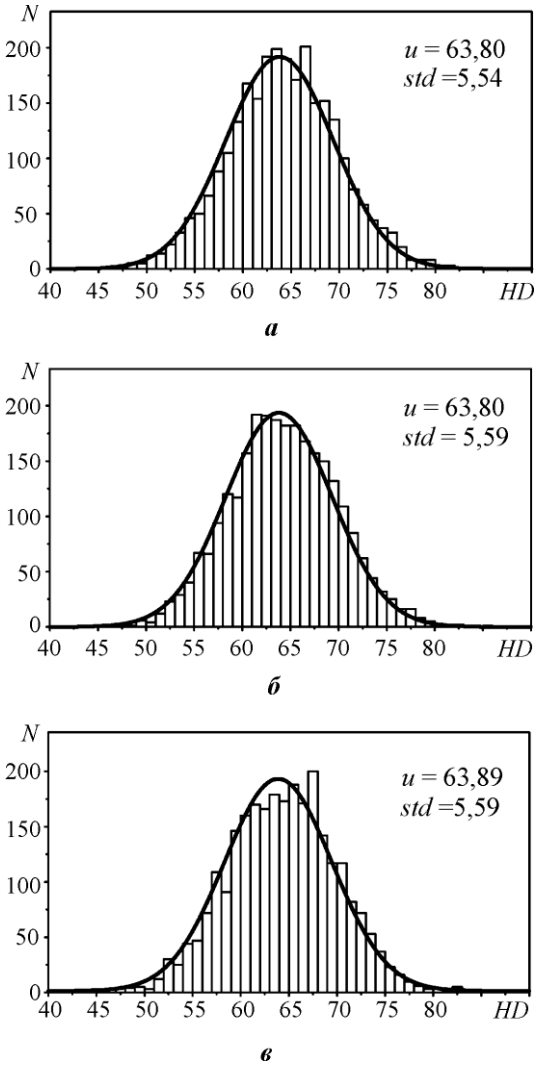

Рис.2. Уникальность ФНФ для различных значений температуры: *а* – 25 °С; *б* – 50 °С; *в* – 70 °С

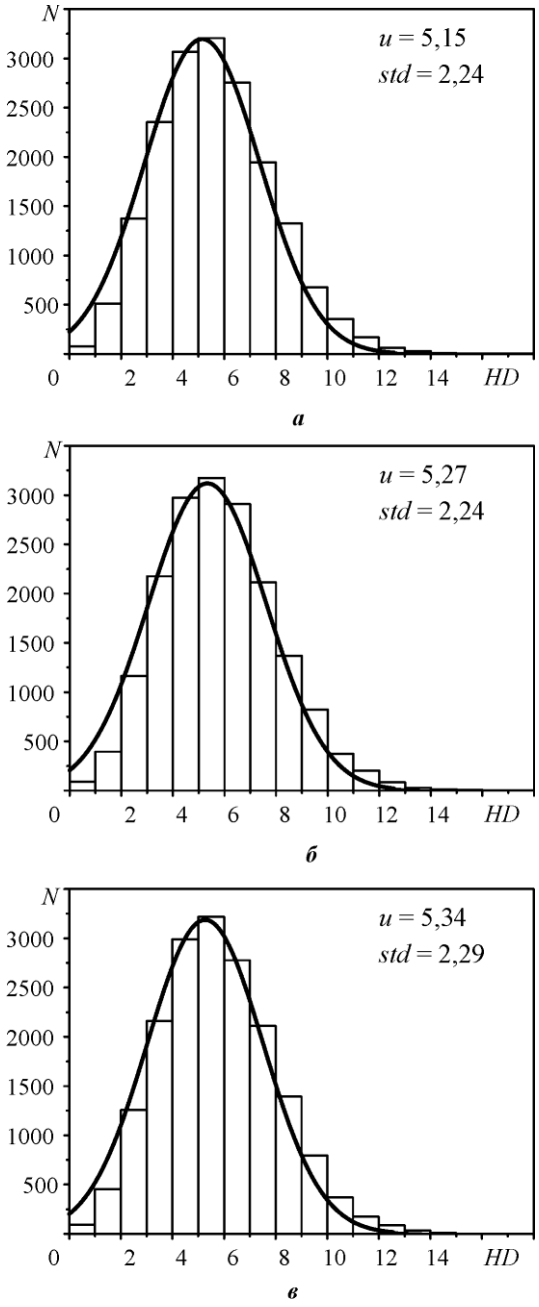

Рис.3. Надежность ФНФ для различных значений температуры: *а* – 25 °С; *б* – 50 °С; *в* – 70 °С

На рис. 4 представлены гистограммы надежности ФНФ в диапазоне температур от 25–70 °С без и с использованием усреднения. Последовательности, полученные при 25°С, приняты за опорные, относительно которых рассчитывались значения *HD* для тех же последовательностей, но сгенерированных при температурах 50 и 70 °С. Из рисунка следует, что усреднение позволяет несколько улучшить надежность ФНФ, однако при этом увеличивается время генерации последовательности ввиду необходимости проведения повторных считываний массива памяти.

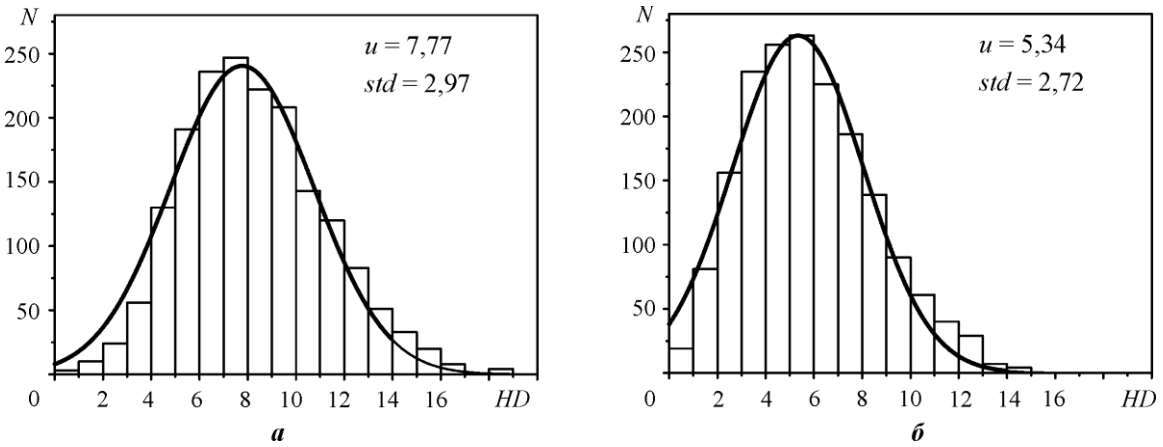

Рис.4. Надежность ФНФ в диапазоне температур 25–70 °С: *а* – без усреднения; *б* – с усреднением 1 из 21

Генерация криптографических ключей. Бинарные последовательности могут быть использованы для генерации криптографических ключей при условии их полной воспроизводимости во всем рабочем диапазоне, чего на практике добиться крайне сложно. Для исправления неустойчивых битов последовательности могут быть использованы схемы коррекции ошибок. При этом получение полностью воспроизводимой последовательности разбивается на два этапа: инициализация и регенерация (рис.5).

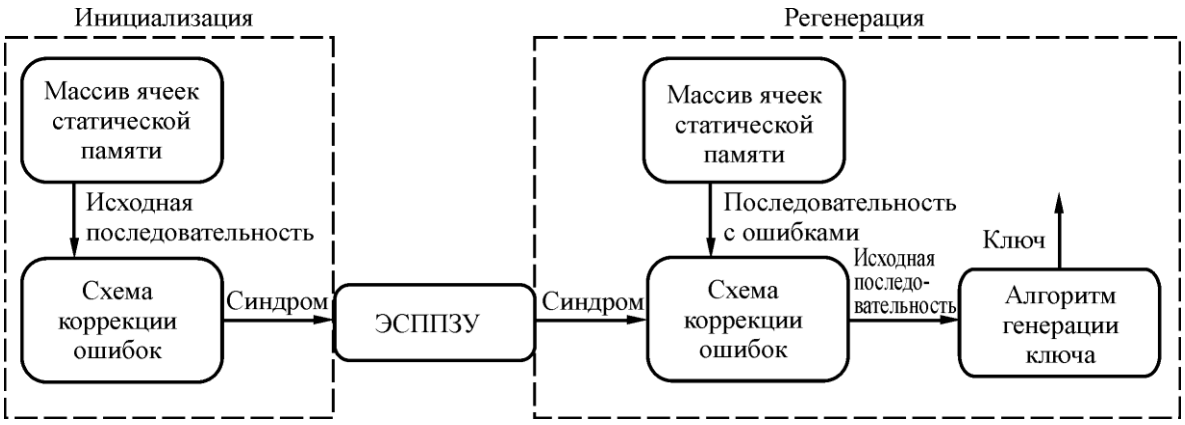

Рис.5. Этапы получения воспроизводимой последовательности

На этапе инициализации последовательность генерируется в нормальных условиях и признается истинной. Проводится вычисление избыточной информации (синдрома) для последовательности с использованием схемы коррекции ошибок. Избыточная информация сохраняется в энергонезависимой памяти. Для определения параметров схемы коррекции ошибок (количество исправляемых ошибок) могут быть использованы гистограммы надежности. Так, например, из рис.4,*б* следует, что исправление схемой коррекции 20-ти ошибок будет достаточным для восстановления исходной последовательности.

Когда возникает необходимость в ключе, осуществляется процесс регенерации. Последовательность генерируется при текущих условиях функционирования устройства. Для исправления неустойчивых битов последовательности используется сохраненная ранее избыточная информация.

Заключение. ФНФ на основе статической памяти позволяет использовать уникальность ИС на микроскопическом уровне для генерации криптографических ключей. В отличие от классического метода хранения ключей в энергонезависимой памяти, при использовании ФНФ ключи существуют только во время работы устройства, что значительно усложняет проведение злоумышленником физической атаки. Результаты эксперимента указывают на возможность использования ФНФ, полученной в рамках 0,18-мкм КМОП-процесса для безопасного хранения криптографических ключей.

Литература

1. ***Skorobogatov S.*** Optical surveillance on silicon chips: your crypto keys are visible. – URL: http://www.cl.cam.ac.uk/~sps32/SG_talk_OSSC_a.pdf (дата обращения: 15 мая 2015 г.)

2. ***Красников Г.Я.*** Конструктивно-технологические особенности субмикронных МОП-транзисторов. – Изд. 2-е, испр. – М.: Техносфера, 2011.

3. ***Suh G.E., Srinivas Devadas.*** Physical unclonable functions for device authentication and secret key generation // Design Automation Conference. IEEE. – 2007. – P. 9–14.

4. The butterfly PUF: Protecting IP on every FPGA / ***S.S. Kumar, J. Guajardo, R. Maes et al.*** // IEEE International Workshop on Hardware-Oriented Security and Trust. – 2008. – P. 67–70.

5. ***Guajardo J., Kumar S.S., Schrijen G.J., Tuyls P.*** Brand and ip protection with physical unclonable functions // IEEE International Symposium on Circuits and Systems. – 2008. – P. 3186–3189.

Статья поступила
4 июня 2015 г.

Лосевской Александр Юрьевич – аспирант кафедры интегральной электроники и микросистем МИЭТ, инженер-конструктор отдела разработки интегральных схем АО «НИИ молекулярной электроники» (г. Москва). *Область научных интересов:* разработка цифровых блоков ИС. **E-mail: alosevskoy@mikron.ru**