ИССЛЕДОВАНИЕ СТАБИЛЬНОСТИ ПРОМЫШЛЕННОЙ SRAM ПАМЯТИ, ИСПОЛЬЗУЕМОЙ ДЛЯ НЕКЛОНИРУЕМОЙ ИДЕНТИФИКАЦИИ

Кайкы М. Н., Иванюк А. А.
Кафедра информатики, Белорусский государственный университет информатики и радиоэлектроники
Минск, Республика Беларусь
E-mail: kaikymykhailo@gmail.com, ivaniuk@bsuir.by

Данная работа посвящена изучению стабильности промышленных ячеек статической памяти, используемых для неклонируемой идентификации. В работе рассматривается изменение характеристик стабильности ячеек в зависимости от напряжения питания промышленного образца статической памяти.

Введение

В основе источников энтропии и идентификаторов обычно лежат физически неклонируемые функции (ФНФ), являющиеся сущностями, воплощёнными в физической структуре, которые легко оценить, но, в силу неконтролируемых человеком процессов, невозможно воспроизвести, смоделировать или охарактеризовать [1].

I. Статическая память

Современная статическая память — полупроводниковая энергозависимая структура, ячейка которой построена при помощи двух инверторов с перекрёстной обратной связью на базе КМОП-транзисторов работающих в ключевом режиме [2] (см. рис. 1). В силу асимметрии такой структуры, ячейки статической памяти при инициализации заполняются случайными значениями, которые зависят от многих факторов, в том числе и от величины задержек на линиях обратной связи.

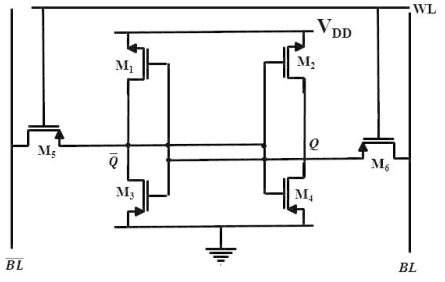

Рис. 1 – Ячейка статической памяти на 6 КМОП-транзисторах

II. Цель работы

Природа инициализации ячеек и простота исполнения статической памяти определяют большой интерес к исследованию её применимости в качестве генератора уникальных последовательностей для систем идентификации и аутентификации [3]. На практике, изменение характеристик окружающей среды вносит свои коррективы в работу не только цифровых идентификаторов но и всех устройств в целом, что отрицательно влияет на их надёжность. Данная работа направлена на изучение поведения статической памяти в качестве идентификатора с целью определить зависимость стабильности и уникальности ячеек от девиации напряжения питания.

III. Экспериментальная установка

Для проведения экспериментов, была использована плата быстрого прототипирования Nexys-4 компании Digilent с размещённым на ней кристаллом ПЛИС Artix-7 xc7a100tscg384–1 компании Xilinx. В качестве исследуемой статической памяти была применена микросхема компании MicroChip — 23K256 размером 256 Кбит и рабочим диапазоном напряжений от 2.7В до 3.6В. Напряжение на микросхеме изменялось при помощи 12-ти разрядного ЦАП MCP4921, той же фирмы, и последовательно включённым операционным усилителем с обратной связью по напряжению AD8041 (Analog Devices). Контроль напряжения и хода эксперимента осуществлялся при помощи разработанного блока-сопряжения и софт-процессора Microblaze, размещённых в ПЛИС. В ходе проведения эксперимента на цифро-аналоговом преобразователе устанавливалось желаемое напряжение питания, после чего из микросхемы памяти считывались значения её ячеек с циклами перезагрузок (выключение питания на достаточный срок — 2 секунды [4]), всего таких циклов насчитывалось 100 для каждого напряжения. Затем, напряжение питания изменялось и процесс повторялся. В результате проведения экспериментов были получены наборы данных для значений напряжения питания микросхемы в диапазоне от 1.72 В до 4.45 В с шагом 5.5 мВ.

IV. Анализ полученных данных

Проведём анализ стабильности памяти для каждого напряжения питания по отдельности, для этого посчитаем количество переключений каждой ячейки между циклами перезагрузки и разделим эту сумму на количество проведённых экспериментов (см. формулу 1).

$$S = 100\% \cdot \frac{\sum_{j=1}^{M} \sum_{i=0}^{N-1} x_{ij} \oplus x_{(i+1)j}}{N \cdot M}, \quad (1)$$

где N — количество экспериментов, M — количество ячеек, x_{ij} – значение j-той ячейки в i-том эксперименте. Результаты проведённого анализа стабильности ячеек изображены на рис. 2.

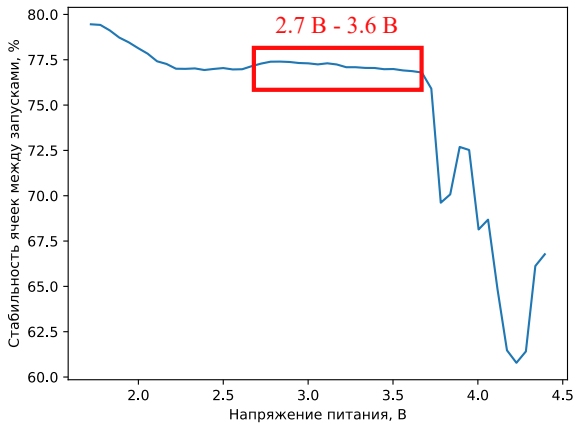

Рис. 2 – Стабильность ячеек статической памяти в зависимости от напряжения питания

Важным критерием при оценке физически неклонируемых функций является соотношение количества нулей и единиц в её ответах. Для расчёта данного соотношения использована метрика единообразия (см. формулу 2) для каждого из напряжений питания (см. рис. 3), разрядность вектора выбрана исходя из ширины шины данных в микросхеме ($B = 8$).

$$U = 100\% \cdot \frac{\sum_{j=1}^{K} (1 - 2 \cdot |\frac{WH(V)}{B} - 0.5|)}{K}, \quad (2)$$

где $WH(V)$ — вес бинарного вектора V по Хэммингу, B — разрядность вектора, K — количество векторов.

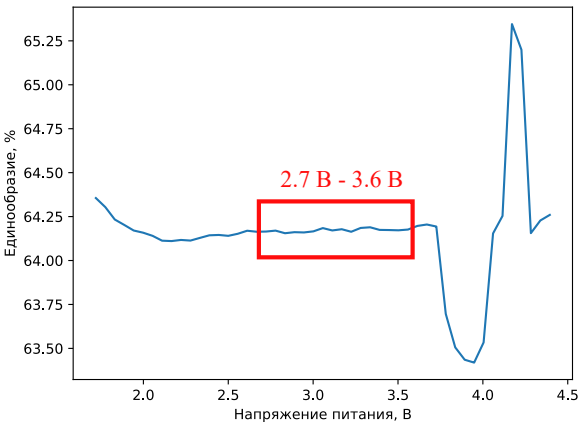

Рис. 3 – Единообразие ячеек статической памяти

Стоит отметить, что после превышения значения питающего напряжения равного 4.15 В, микросхема статической памяти перестала полноценно функционировать как оперативное запоминающее устройство. Для проверки работоспособности микросхемы был применён маршевый тест ОЗУ MATS [5] (см. формулу 3).

$$\{\uparrow\downarrow (w0); \uparrow (r0, w1); \downarrow (r1)\} \quad (3)$$

В результате проведения данного маршевого теста, из доступного объёма — 256 Кбит, функции оперативного запоминающего устройства выполняли всего 23.74% ячеек статической памяти.

Для оценки изменения характеристик памяти от напряжения питания был произведён расчёт среднеквадратичного отклонения для всего диапазона напряжений и для выделенных диапазонов работы (ниже рабочего, рабочий, выше рабочего). Смотрите таблицу 1.

Таблица 1 – Среднеквадратичное отклонение для диапазонов напряжения питания

Напряжение, В	1,72-2,71	2,76-3,59	3,64-4,15
σ_S	0.44		
	0.87	0.17	4.94
σ_U	0.309		
	0.06	0.01	0.57

V. Заключение

В результате проведённого эксперимента и анализа полученных данных были сделаны следующие выводы:

1. С увеличением напряжения питания статической памяти стабильность ячеек при инициализации снижается на 20%.
2. При превышении рабочего диапазона напряжений питания соотношение нулей и единиц при инициализации снижается на 0,75%.
3. Использование статической памяти как физически неклонируемой функция для систем идентификации без коррекции на практике не представляется возможным.
4. Методы коррекции для использования статической памяти как физически неклониуремая функция для систем идентификации нуждаются в дальнейших исследованиях.

1. Pappu, R. Physical One-Way Functions: Ph.D. thesis / R. Pappu // MIT. — Boston, USA, 2001.
2. Угрюмов, Е.П. Цифровая схемотехника : учеб.-метод. пособие / Угрюмов, Е.П. – СПб.: БХВ-Петербург, 2001. - 221 С.
3. Phyo Aung, Pyi & Mashiko, Koichiro & Ismail, Nordinah & Ooi, Chia-Yee. (2020). Evaluation of SRAM PUF Characteristics and Generation of Stable Bits for IoT Security.
4. Skorobogatov, S. Hardware Security Implications of Reliability, Remanence, and Recovery in Embedded Memory. J Hardw Syst Secur 2, 314–321 (2018).
5. Ярмолик В.Н. Неразрушающее тестирование запоминающих устройств. //Ярмолик В.Н. Мурашко И.А., Куммерт А., Иванюк А.А. Минск: Бестпринт; 2005, —52 - 82 С.