УДК 004.312
DOI: 10.21122/2309-4923-2023-1-54-62

ИВАНЮК А.А., ШАМЫНА А.Ю.

ФИЗИЧЕСКИ НЕКЛОНИРУЕМАЯ ФУНКЦИЯ ТИПА АБИТР С НЕЛИНЕЙНЫМИ ПАРАМИ ПУТЕЙ

Белорусский государственный университет информатики и радиоэлектроники,
Минск, Республика Беларусь

Физически неклонируемые функции (ФНФ) являются базовыми элементами физической криптографии, позволяющие решать такие задачи как, неклонируемая идентификация, аутентификация и доказательство авторства на цифровые устройства, генерирование случайных последовательностей и т.п. Отличительными особенностями ФНФ являются их случайность, непредсказуемость и невоспроизводимость, обусловленные неконтролируемыми, случайными вариациями исходных материалов и технологических процессов при их изготовлении. По своей сути ФНФ представляют собой цифровые схемы, позволяющие извлекать подобные вариации и преобразовывать их в двоичную форму для дальнейшего использования. Среди всего многообразия ФНФ выделяют ФНФ типа арбитр (АФНФ), которая представляет собой цифровую схему, которая принимает на входы двоичное значение N-разрядного запроса и вырабатывает однобитный ответ. Функционирование схемы АФНФ основано на сравнении времени прохождения двух копий тестового сигнала по паре конфигурируемых путей, выбранной значением запроса из множества 2N всех возможных пар. Результат сравнения и определяет двоичное значение ответа АФНФ. Множество всех пар запрос-ответ является случайным, непредсказуемым и невоспроизводимым в случае реализации копий схемы ФНФ как на одном, так и на других кристаллах, в том числе с использованием различных технологий. В данной статье предлагается новый подход к синтезу схем АФНФ, основанный на применении элементов перестановочных сетей и позволяющий формировать нелинейные конфигурации пар путей, что потенциально усложняет построение модели АФНФ с целью осуществления атаки на ее реализации. Приводятся новые схемотехнические решения для построения АФНФ и результаты экспериментальных исследований их основных характеристик, полученных при реализации на FPGA серии Zynq-7000.

Ключевые слова: *физически неклонируемая функция, арбитр, перестановочные сети.*

Введение

Физически неклонируемые функции (ФНФ) представляют собой реализованные цифровые схемы, принимающие на свои входы значение запроса *CH* (*Challenge*) и вырабатывающие значение ответа *R* (*Response*) в качестве реакции на поданный запрос [1]. Формально поведение схемы ФНФ можно описать как отображения множества запросов на множество ответов: $PUF: CH \rightarrow R$, при этом $y = PUF(x)$ ($y \in R$, $x \in CH$), где функция *PUF* не известна и не определена до момента изготовления экземпляра схемы. При попытке изготовить идентичную копию схемы ФНФ, в том числе с применением иных технологий, происходит изменение множества *R* при использовании одного и того же множества *CH*. Другими словами идентичная копия будет иметь функцию $PUF' \neq PUF$, что определяет свойство уникальности (неклонируемости). При изготовлении схем физически невозможно создать две идентичные копии, имеющие одинаковые параметры и характеристики, вариации которых случайны и неконтролируемы. К таким параметрам можно отнести неоднородное распределение примесей в применяемых при изготовлении схем материалов, геометрические размеры используемых элементов и сигнальных линий и т.п. Перечисленные параметры непосредственно влияют на основные характеристики структурных элементов цифровых устройств, такие как временные задержки распространения сигналов. Извлечение уникальных физических параметров и трансформация их в цифровое представление и есть основная задача проектирования схем ФНФ. Наиболее удачной схемой, позволяющей оценивать различия задержек распространения сигналов через симметричные пути цифровых устройств, является схема ФНФ типа арбитр (АФНФ) [1, 2].

Помимо уникальности к ФНФ предъявлю ряд других требований, среди которых можно выделить непредсказуемость, случайность и стабильность. Под непредсказуемостью можно понимать не возможность предсказать, смоделировать либо иным способом оценить значение функции $y' = PUF(x')$, при известном значении $y = PUF(x)$, $x' \neq x$. Среди многих характеристик, оценивающих случайность ФНФ выделяют единообразие, определяющее соотношение числа единичных $R1$ и нулевых ответов $R0$ на множестве уникальных запросов $CH \rightarrow R = \{R0, R1\}$. В идеальном случае $|R0| = |R1|$. Под стабильностью ФНФ понимают способность схемы к генерированию одинаковых ответов на многократно повторяемые запросы: $CH \rightarrow R^t$, $CH \rightarrow R^{t+1}$, …, $CH \rightarrow R^{t+W}$, где R^t – множество ответов, полученное в дискретный отсчет времени t, W – число повторений. Для идеальной ФНФ $R^t = R^{t+1} = \ldots = R^{t+W}$.

Исследователи и разработчики, осуществляющие модернизации существующих и разработку новых схем ФНФ, действуют в стремлении обеспечивать высокие показатели описанных выше свойств в зависимости от области применения и технологических ограничений. В данной работе рассматривается решение проблемы увеличения непредсказуемости ответов АФНФ путем построения нелинейных пар симметричных путей.

Классическая схема АФНФ

Физически неклонируемая функция типа арбитр (АФНФ) впервые была предложена в работе [2]. Структурно схема АФНФ состоит из трех основных блоков: генератора тестовых импульсов (ГТИ), блока симметричных путей (БСП) и арбитра (АРБ). Схема ГТИ, как правило, вырабатывает одиночный тестовый импульс s, две копии которого s^a и s^b одновременно поступают на два входа БСП a и b соответственно. Помимо этого, БСП имеет N-разрядный вход запроса $CH = [ch_0, ch_1, ch_2, \ldots, ch_{N-1}] = [ch_0{:}ch_{N-1}]$, значение которого выбирает уникальную конфигурацию пары внутренних путей (p_0, p_1), которые коммутируют два входа a и b с двумя выходами x и y: $(a, b)\rightarrow(p_0, p_1)^{CH}\rightarrow(x, y)$. В итоге на выходах появляются импульсы s^x и s^y, являющиеся копиями исходных s^a и s^b. В зависимости от значения запроса CH может происходить как прямая, так и обратная коммутация входов с выходами. Под путем, который проходит одиночный импульс, будем понимать последовательность структурных элементов и соединительных линий, обеспечивающих связь между исходным входом и соответствующим выходом БСП. Для АФНФ кране важно соблюдать симметричность (структурную идентичность) двух путей, по которым проходят две копии тестовых импульсов [1, 2].

После прохождения выбранных путей $(p_0, p_1)^{CH}$ тестовые импульсы s^x и s^y появляются на выходах БСП с различными значениями задержек $\delta(p_0^{CH})$ и $\delta(p_1^{CH})$, обусловленными технологическими неконтролируемыми вариациями выбранных симметричных путей. Схема арбитра осуществляет сравнение значений $\delta(p_0^{CH})$ и $\delta(p_1^{CH})$ с выработкой бинарного значение ответа R^{CH}. Одной из наиболее используемых схем АРБ является схема синхронного D-триггера, на входы синхронизации и данных которого подаются сигналы с выходов БСП, при этом сравнению подвергаются передние фронты тестовых импульсов s^x и s^y [1]. В свою очередь сама схема БСП строится из последовательно подключенных базовых блоков α_i, $i\in[0,2^N\text{-}1]$, обеспечивающих прямую и перекрестную коммутацию сигналов с двух входов a_i и b_i на два выхода x_i и y_i. При $ch_i = 0$ осуществляется прямая коммутация α_i^0 $((a_i, b_i)\rightarrow(x_i, y_i))$, если $ch_i = 1$ – перекрестная коммутация α_i^1 $((a_i, b_i)\rightarrow(y_i, x_i))$. На рисунке 1 приведена общая структура классической схемы АФНФ с коммутационным элементом БСП, реализованным при помощи двух мультиплексоров m_{i0} и m_{i1}.

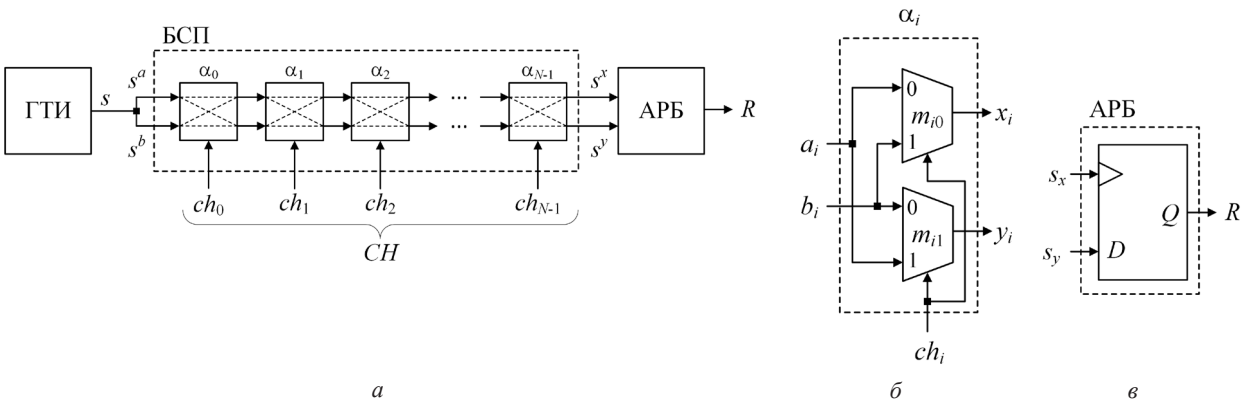


Рисунок 1. Структурная схема классической АФНФ (*а*), схема коммутационного элемента (*б*) и схема арбитра (*в*)

Рассмотрим пример структуры АФНФ для $N = 2$. При этом БСП состоит из двух элементов α_0 и α_1, а значение запроса $CH = [ch_0\, ch_1]$ и определяет конкретную конфигурацию пары путей $(p_0, p_1)^{CH}$ из четыре возможных. Так, при $CH_0 = [00]$ (здесь и далее для произвольного CH_M $M\in[0,2^N\text{-}1]$ является десятичным индексом запроса) конфигурируется следующая пара путей $(p_0, p_1)^0$: $\alpha_0^0 \rightarrow \alpha_1^0 = (m_{00}^0, m_{01}^0)\rightarrow(m_{10}^0, m_{11}^0)$, где m_{ij}^r обозначает часть пути, проходящего от r-го входа мультиплексора m_{ij} до его выхода $(r, j\in\{0,1\})$. При $CH_3 = [11]$ пути для тестовых импульсов будут выглядеть следующим образом $(p_0, p_1)^3$: $\alpha_0^1\rightarrow\alpha_1^1 = (m_{01}^1, m_{00}^1)\rightarrow(m_{11}^1, m_{10}^1)$. В общем случае значение i-го бита запроса и определяет конфигурацию части пути, проходящего через элемент $\alpha^{ch_i} : (m_{ich_i}^{ch_i}, m_{ich_i}^{\overline{ch_i}})$, где $\overline{ch_i}$ есть инверсное значение $ch_i\in\{0,1\}$.

В обоих рассмотренных вариантах пары путей $(p_0, p_1)^0$ и $(p_0, p_1)^3$ являются симметричными, так как проходят через одинаковое число структурных однотипных элементов и соединительных проводников, незначительные уникальные отличия которых приводят к различным, непредсказуемым значениям $\delta(p_0^{CH})$ и $\delta(p_1^{CH})$, что в итоге влияет на конечный результат R^{CH}.

Как видно из представленного (рис. 1) БСП имеет линейную структуру последовательно соединенных блоков α_i, которые являются базовыми блоками перестановочных сетей (*permutation networks*) [3]. Линейная природа БСП классической схемы АФНФ является уязвимой к атакам, как правило осуществляемым методами машинного обучения, с целью создания точной модели, воспроизводящей значения множества ответов, идентичным ее физической реализации [4]. Для предотвращения подобных действий предлагается много подходов, среди которых можно выделить методы, нацеленные на нелинейном преобразовании значений запросов [5], что усложняет проведение атак на АФНФ.

В данной статье предлагается альтернативный подход к синтезу схем БСП на основе схемотехнических элементов перестановочных сетей, позволяющий формировать нелинейные комбинации пар путей для прохождения тестовых импульсов, что потенциально может усложнить последовательности вырабатываемых ответов.

Новые элементы блока симметричных путей

Введем следующие ограничения на построения новых элементов БСП, которые характерны в том числе и для классической схемы (см. рис. 1).

1. Минимальное число входов и выходов – два. Данное ограничение обусловлено применением одной пары конфигурируемых путей и одного арбитра.

2. Пара путей во всех конфигурациях элемента должна быть симметричной. Это означает, что произвольно выбранные пути должны проходить через одинаковое число однотипных элементов и сигнальных линий. В противном случае сильная асимметрия путей может приводить к заведомо постоянному значению ответа R.

3. На выходах произвольной пары путей должны наблюдаться как прямая, так и перекрестная коммутация входных сигналов.

Пусть $P^{k,k}$ есть перестановочная сеть, обеспечивающая все возможные $k!$ коммутации k входов с k выходами. Очевидно, что $P^{2,2} = \alpha$, удовлетворяющая описанным выше требованиям. Введем нотацию, позволяющую описывать последовательную линейную структуру классической схемы БСП на основе таких элементов: $\{P_0^{2,2}, P_1^{2,2}, P_2^{2,2}, ..., P_{N-1}^{2,2}\} = \{\alpha_0, \alpha_1, \alpha_2, ...\alpha_{N-1}\}$; и сокращенную нотацию: $\{P^{2,2}\}^N = \{\alpha\}^N$, где N это число идентичных элементов, последовательно соединенных друг с другом.

Первым предлагаемым структурным элементом БСП будет являться элемент перестановочной сети $P^{2,k} = \beta^k$, обеспечивающий прямую и перекрестную коммутацию двух своих входов с произвольной парой из k имеющихся выходов. Для $k = 2$ элемент β^2 эквивалентен элементу α. Для произвольного значения k необходимо и достаточно k конфигураций, удовлетворяющих вышеописанному условию. На рисунке 2 приведены графические обозначения элементов β^k, β^4 и структурная схема элемента β^4, построенная на двух элементах α.

Приведенная схема является одной из возможных, которая удовлетворяет описанным требованиям и имеет четыре конфигураций, которые обеспечивают прямую и перекрестную коммутацию входов (a_i, b_i) с произвольной парой выходов из четырех возможных $(w_i, x_i, y_i, z_i,)$.

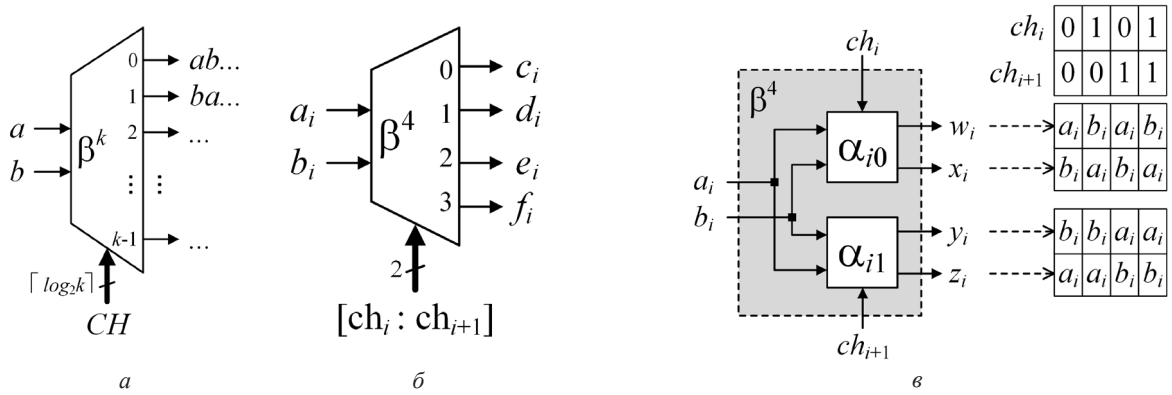
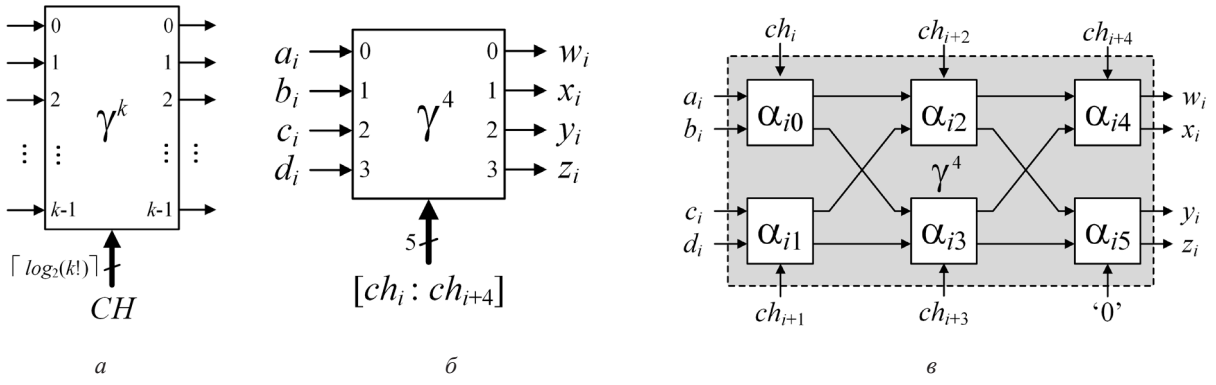


Рисунок 2. Графическое обозначение элемента β^k (*а*), элемента β^4 (*б*) и структурная схема элемента β^4 (*в*)

Схемотехническую реализацию перестановочной сети $P^{k,k}$ для произвольного значения k обозначим как элемент γ^k, обладающий k входами и k выходами и позволяющий осуществлять число возможных коммутаций близкое к $k!$. Например, для $k = 4$ элемент γ^4 может быть построен на основе пяти элементов α [3]. На рисунке 3 представлена модифицированная схема элемента γ^4, которая содержит дополнительный элемент α_{i5} с фиксированным значением бита запроса, необходимый для обеспечения топологической симметрии путей.



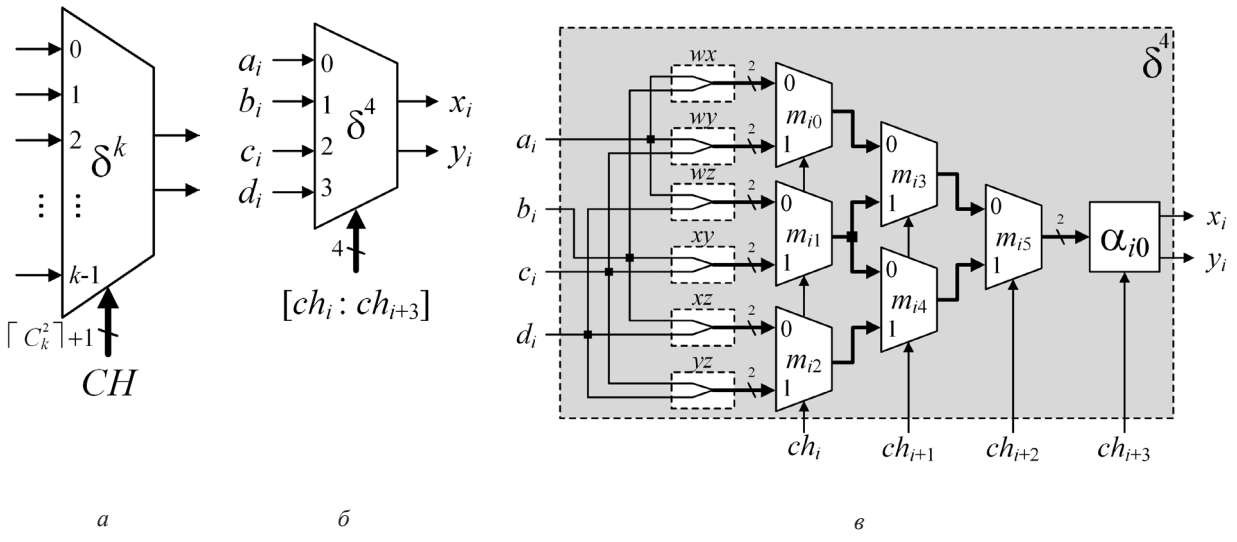
а *б* *в*

Рисунок 3. Графическое обозначение элемента γ^k (*а*), элемента γ^4 (*б*) и структурная схема элемента γ^4 (*в*)

В случае отсутствия элемента α_5 фронты тестовых сигналов на выходах y_i и z_i могут заведомо быстрее формироваться в сравнении с сигналами на выходах w_i и x_i. Для представленного элемента существует 32 конфигурации внутренних путей, 24 из которых приводят к всевозможным коммутациям входов (a_i, b_i, c_i, d_i) с выходами (w_i, x_i, y_i, z_i,). Восемь значений запроса $CH = [ch_i{:}ch_{i+4}]$ приводят к одинаковому значению на выходах схемы, однако с использованием различных конфигураций внутренних путей. Например, при подаче запросов CH_{16} = [10000] и CH_1 = [00001] на выходах схемы будет наблюдаться одна и та же комбинация значений входных сигналов (b_i, a_i, c_i, d_i). При этом два пути, связывающие входы c_i и d_i с выходами y_i и z_i останутся неизменными, а пути, связывающие входы a_i и b_i с выходами w_i и x_i, будут разными: для CH_{16} это пара путей $a_i \to \alpha_0^1 \to \alpha_3^0 \to \alpha_4^0 \to x_i$ и $b_i \to \alpha_0^1 \to \alpha_2^0 \to \alpha_4^0 \to w_i$, а для CH_1 это пути $a_i \to \alpha_0^0 \to \alpha_2^0 \to \alpha_4^1 \to x_i$ и $b_i \to \alpha_0^0 \to \alpha_3^0 \to \alpha_4^1 \to w_i$.

Данный пример показывает возможность использования дополнительного бита запроса ch_{i+5}, управляющего элементом α_5, что в свою очередь обеспечивает 64 уникальные конфигурации внутренних путей элемента γ^4.

Элементом обратным β^k будет являться перестановочная сеть $P^{k,2} = \delta^k$, осуществляющую прямую и перекрестную коммутацию произвольной пары из k входов с двумя выходами. Подобный элемент может быть синтезирован на основе C_k^2 мультиплексоров 2×1, коммутирующих две двухразрядные шины с одной выходной двухразрядной шиной, и одного элемента α. На рисунке 4 приведен пример структуры элемента δ^4, состоящего из шести двухразрядных мультиплексоров $m_{i0} - m_{i5}$ и одного элемента α_{i0}, обеспечивающего 16 конфигураций внутренних путей, которые обеспечивают прямую и перекрестную коммутацию произвольной пары из четырех входов (a_i, b_i, c_i, d_i) с двумя выходами (x_i, y_i).



а *б* *в*

Рисунок 4. Графическое обозначение элемента δ^k (*а*), элемента δ^4 (*б*) и структурная схема элемента δ^4 (*в*)

Для приведенного элемента δ^4 существует 12 уникальных конфигураций, при которых на двух выходах (x_i, y_i) появятся все возможные комбинации двух различных символов из входного набора (a_i, b_i, c_i, d_i). Четыре значения запроса $CH = [ch_i{:}ch_{i+3}]$ приводят к одинаковым значениям на выходах схемы, но при этом активируются различные пары путей. Так, два запроса $CH_{10} = [1010]$ и $CH_{12} = [1100]$ приведут к появлению на выходах (x_i, y_i) одного и того же значения (b_i, c_i). При подаче запроса CH_{10} будет активирован путь для пары тестовых импульсов $(b_i, c_i) \to m^1_{i1} \to m^0_{i4} \to m^1_{i5} \to \alpha^0_{i0} \to (x_i, y_i)$, а при запросе $(b_i, c_i) \to m^1_{i1} \to m^1_{i3} \to m^0_{i5} \to \alpha^0_{i0} \to (x_i, y_i)$ (рис. 4, *в*). Таким образом, все возможные 16 конфигураций δ^4 элемента будут являться уникальными для произвольной пары путей.

Построение БСП на предложенных элементах

Рассмотренные элементы могут быть использованы в различных сочетаниях для построения БСП. Рассмотрим некоторые из вариантов сочетаний элементов α, β^k, γ^k, δ^k для $k = 4$. Так, выходы элемента α могут быть сопряжены со входами элемента β^4, выходы β^4 – со входами элементов γ^4 и δ^4, выходы γ^4 – со входами элементов γ^4 и δ^4, выходы δ^4 – со входами элемента α. Даже такие простые примеры сочетаний позволяют конструировать БСП многими способами. В таблице 1 приведены описания некоторых шаблонных структур БСП.

Таблица 1

Примеры различных конфигураций БСП для $k = 4$

№	Символьное описание БСП	Разрядность запроса *CH*
1	$\{\alpha\}^e$	e
2	$\{\beta^4\delta^4\}^e$	$6e$
3	$\{\alpha\}e\{\beta^4\delta^4\alpha\}^g$	$7g+e$
4	$\{\alpha\}^e\beta^4\{\gamma^4\}^g\delta^4\{\alpha\}^h$	$5g+e+h+6$
5	$\{\{\alpha\}^e\{\beta^4\delta^4\}^g\{\alpha\}^h\}^q$	$q(6g+e+h)$

Применяя целочисленные значения коэффициентов *e, g, h, q* и *k* можно синтезировать структуру БСП с различной разрядностью запроса *CH*. На рисунке 5 приведены примеры двух структур (№ 3 и № 4, см. табл. 1) с размерностью запроса равной 16. Данные структуры являются одномерными, построенными последовательным соединением элементов α, β, γ и δ, и обладающие различной структурной сложностью. Так, если классическая схема БСП для $N = 16$ $\{\alpha\}^{16}$ состоит из 32 мультиплексоров, то схема на рис. 1 а – из 44 мультиплексоров, а схема на рис. 1 б – из 40 мультиплексоров. Увеличенная структурная сложность вместе с неоднородностью БСП может потенциально усложнить связь подаваемых запросов с генерируемыми ответами АФНФ.

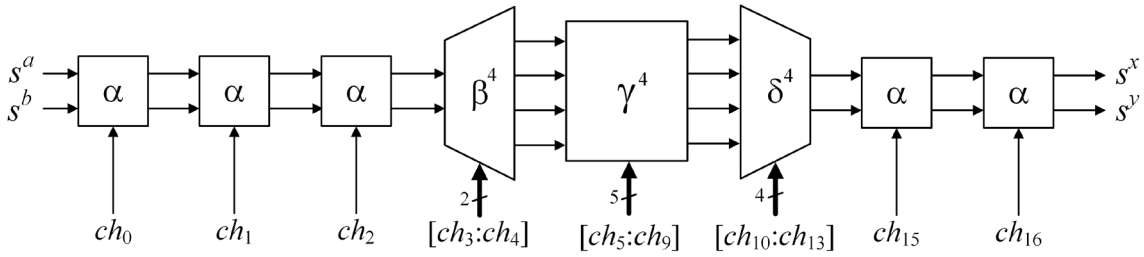


Рисунок 5. Структуры БСП, сформированные по следующим символьным описаниям: $\{\alpha\}^2\{\beta^4\delta^4\alpha\}^2$ (*а*), $\{\alpha\}^3\beta^4\gamma^4\delta^4\{\alpha\}^2$ (*б*)

Для еще большего увеличения структурной сложность и с учетом требования симметрии всех пар выбираемых путей возможно построение многомерных структур БСП с использованием разнообразных сочетаний базовых элементов, например:

$$\alpha\beta^k \begin{Bmatrix} \alpha_0 \\ \dots \\ \alpha_{k-1} \end{Bmatrix}^e \{\gamma^k\}^g \begin{Bmatrix} \delta_0^{k/2} \\ \delta_1^{k/2} \end{Bmatrix} \delta^4.$$

Для оценки нелинейности БСП, сформированных на основе предложенных элементов, проведем анализ значений $\delta(p_0^{CH})$ и $\delta(p_1^{CH})$ в зависимости от множества различных запросов *CH*.

Экспериментальное исследование характеристик различных реализаций АФНФ

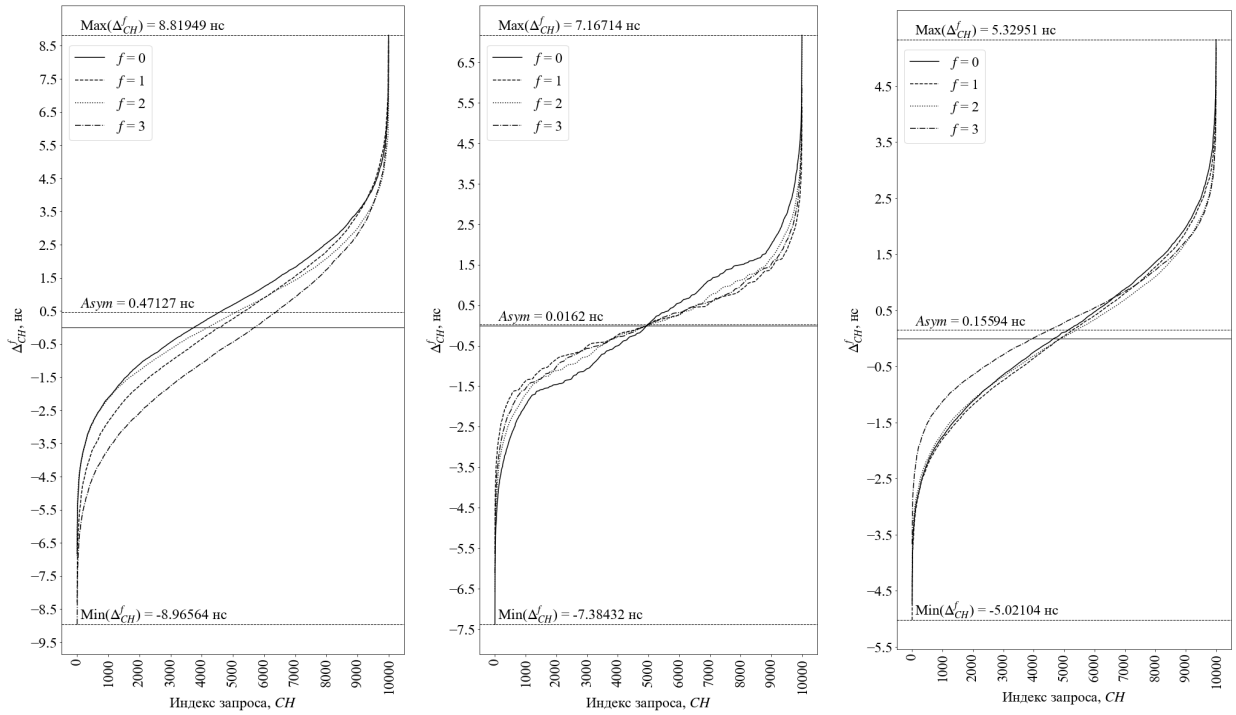
Для исследования схемных реализаций АФНФ была использована плата быстрого прототипирования *Digilent ZYBO Z7* с программируемой логической интегральной схемой *FPGA Xilinx ZYNQ* [6]. Исследованию подверглись три реализации АФНФ для $N = 32$, БСП которых имеют следующие описания: BSP1: $\{\alpha\}^{32}$, BSP2: $\{\alpha\}^4\{\beta^4\delta^4\alpha\}^4$ и BSP3: $\alpha\beta^4\{\gamma^4\}^5\delta^4$. Проектирование схем АФНФ было осуществлено при помощи языка *VHDL* и САПР цифровых устройств *Xilinx Vivado/Vitis*. На кристалле *FPGA* было реализовано четыре идентичных схемы для каждого типа

БСП. Кроме этого, дополнительно были реализованы управляющие схемы и схемы, позволяющие измерять значения $\delta(p_0^{CH})$ и $\delta(p_1^{CH})$. Управление передачей данных, генерирование значений запроса было осуществлено программных способом при помощи встроенного в *FPGA* процессора *ARM Cortex-A9*. Вычисление результирующего значения ответа АФНФ производилось на рабочей станции на основе собранных данных в процессе экспериментов.

В ходе технологического синтеза была оценена структурная сложность каждого из вариантов БСП, которая оценивалась в количестве *LUT*-блоков кристалла *FPGA*. Сложность классической схемы BSP1 составила 64 блока, для BSP2 – 88 блоков и для BSP3 – 80 блоков.

В первом эксперименте вычислялись значения $\Delta^f_{CH} = \delta(p_0^{CH}) - \delta(p_1^{CH})$ для $K = 10^4$ уникальных запросов **CH**, полученных генератором *M*-последовательностей, где $f \in [0,3]$ является индексом исследуемой схемы. На рисунке 6 приведены графики отсортированных значений Δ^f_{CH}, полученных на одном кристалле *FPGA* для трех описанных выше конфигураций БСП. Графики также содержат данные о диапазонах изменения значений Δ^f_{CH} и о параметре *Asym*, являющийся среднеквадратичным значением математических ожиданий $\mu(\Delta^f_{CH}), \forall f \in [0,3]$.

Последний параметр может быть использован для оценки степени асимметрии множеств значений Δ^f_{CH}, что непосредственно влияет на мощность подмножеств нулевых и единичных ответов АФНФ.



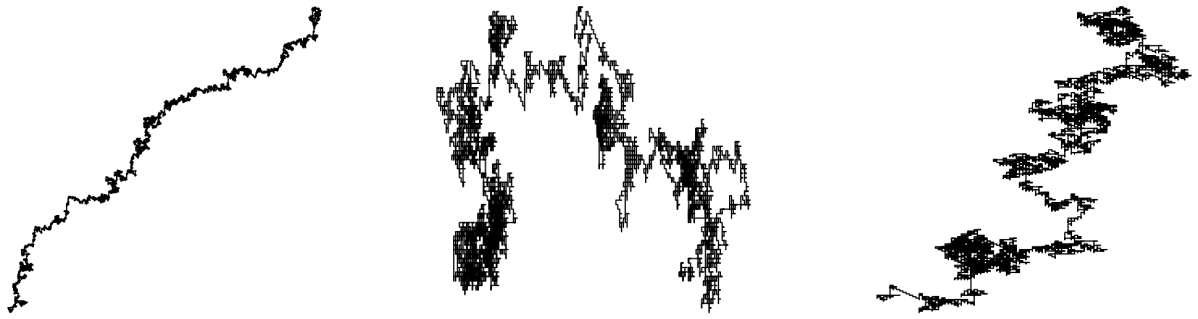
а *б* *в*

Рисунок 6. Графики значений Δ^f_{CH} для различных модификаций БСП: BSP1 (*а*), BSP2 (*б*), BSP3 (*в*)

Как видно, нелинейная природа значений задержек ярко выражена для BSP2, которая также обладает меньшим значением *Asym* (0,0162 нс) (рис. 6 б), а большей (0,47127 нс) – классическая реализация БСП (рис. 6 а). Увеличение структурной сложности, в том числе, повлияло на диапазон разброса значений Δ^f_{CH}, который для BSP2 уменьшился на 18,18 %, а для BSP3 – на 41,8 % в сравнении с классической схемой. Помимо этого, были вычислены усредненные значения среднеквадратичных отклонений $\sigma\Delta^f_{CH}$. Для схемы BSP1 этот показатель равен 2,2642 нс, для BSP2 – 1,3925 нс, и для BSP3 – 1,3145 нс.

Полученные результаты можно объяснить более плотной компоновкой структурных элементов схемных реализаций BSP2 и BSP3, что привело к уменьшению числа протяженных соединительных линий, которые, как известно, вносят значительную асимметрию в сравнении со структурными элементами БСП при их реализации на FPGA [7].

Другим примером, подтверждающим степень нелинейности значений задержек, может служить графический тест «Случайное двумерное блуждание» [8], приведенный для схемы $f = 1$ (рис. 7).



а *б* *в*

Рисунок 7. Результаты графического теста для схемы $f = 1$: BSP1 (*а*), BSP2 (*б*), BSP3 (*в*)

Помимо графических иллюстраций оценим нелинейность рассматриваемых схем БСП при помощи теста на линейную сложность [9], в основе которого лежит алгоритм Берлекэмпа-Мэсси [10]. В таблице 2 приведены значения уровня значимости (*P-value*), вычисляемого в ходе реализации описанного теста, большее значение которого свидетельствует о большей линейной сложности последовательности данных, полученных на выходах исследуемых схем БСП.

Как видно из данных, представленных в таблице 2, последовательности ответов для схем BSP2 и BSP3 обладают большей нелинейностью в сравнении с классической реализацией БСП АФНФ.

Таблица 2

Результаты теста на линейную сложность (значения *P-value*)

Тип БПС	Индекс схемы, f				Среднее
	0	1	2	3	
BSP1	0.2237	0.2608	0.3694	0.1125	0.2416
BSP2	0.8453	0.6360	**0.7960**	0.5565	0.7084
BSP3	**0.8683**	**0.7170**	0.4842	**0.8793**	**0.7372**

Проведем оценку одних из основных характеристик схемных реализаций ФНФ как единообразие *Un* (соотношение единичных и нулевых ответов), U_{intra} – внутикристальная уникальность (степень различия множества пар запрос-ответ для копий ФНФ, реализованных на одном кристалле) и *St* – стабильность (удельное значение многократно повторяющихся запросов, при которых наблюдаются стабильные ответы) [11]. Все перечисленные характеристики вычислялись на описанном выше наборе уникальных запросов и нормированы в диапазоне [0,1] от худшего к наилучшему значению (табл. 3).

Таблица 3

Значения характеристик АФНФ с различными схемами БСП

Тип БПС	*Un*	*Uintra*	*St*
BSP1	0.8416	0.8151	0.9920
BSP2	0.9918	0.6697	0.9952
BSP3	0.9202	0.9008	0.9975

Как видно из приведенных данных рассмотренные модификации БСП обладают сравнимыми, а иногда и превосходящими, значениями основных характеристик ФНФ по отношению к классической схеме БСП. Меньшая степень асимметрии множества значений Δ^f_{CH} для BSP2 и BSP3 (рис. 6) подтвердилась на полученных значениях единообразия *Un*.

Заключение

В данной статье были предложены схемотехнические модификации блока симметричных путей физически неклонируемой функции типа арбитр, основанные на реализации элементов перестановочных сетей. Усложнение базовых элементов БСП привело к увеличению линейной сложности последовательности ответов, что потенциально затрудняет построение математической модели АФНФ с целью осуществления атак на ее реализацию. Рассмотренные новые базовые элементы БСП могут быть применены для построения более сложных структур АФНФ. Как показали поведенные экспериментальные исследования предложенные модификации БСП обладают лучшими показателями единообразия и сравнимыми значениями стабильности по отношению к классической схеме АФНФ.

ЛИТЕРАТУРА

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

2. **Gassend, B.** Silicon physical random functions / B. Gassend [et al.] // Proc. of 9th Computer and Communications Security Conf. (CCS'02), Washington, DC USA, 18–22 Nov. 2002. – Washington, 2002. – P. 148-160.

3. **Waksman, A.** A Permutation Network / A. Waksman // Journal of the ACM. – 1968. – №1(15). – P. 159-163.

4. **Santikellur, P.** Deep Learning based Model Building Attacks on Arbiter PUF Compositions / P. Santikellur, A. Bhattacharyay, R.S. Chakraborty // IACR Cryptol. ePrint Arch. – 2019. – 10 p. – (Preprint / Paper 2019/566).

5. **Zhang, J.** Set-Based Obfuscation for Strong PUFs Against Machine Learning Attacks / J. Zhang, C. Shen // IEEE Transactions on Circuits and Systems I: Regular Papers. – 2021. – № 1(68). – P. 288-300.

6. **ZyboZ7: Zynq-7000 ARM/FPGA SoC Development Board** [Electronic resource]. – Mode of access: https://digilent.com/reference/programmable-logic/zybo-z7/start. – Date of access: 19.01.2023.

7. **Morozov, S.** An Analysis of Delay Based PUF Implementations on FPGA / S. Morozov, A. Maiti, P. Schaumont // Proc. of International Symposium on Applied Reconfigurable Computing: Tools and Applications (ARC 2010), Los Angeles, CA, US, 25–27 Mar. 2010. – Los Angeles, 2010. – P. 382-387.

8. **Costa, L.F.** Exploring complex networks through random walks [Electronic resource] / L.F. Costa, G. Travieso. – Physical Review E, 2007. – Mode of access: https://arxiv.org/pdf/ physics/ 0604193.pdf. – Date of access: 19.01.2023.

9. **Rukhin, A.** A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications [Electronic resource] / A. Rukhin [et al.] – NIST Special Publication 800-22, 2010. – Mode of access: https://www.nist.gov/publications/statistical-test-suite-random-and-pseudorandom-number-generators-cryptographic. – Date of access: 19.01.2023.

10. **Martin-Navarro, J.L.** Review of the Lineal Complexity Calculation through Binomial Decomposition-Based Algorithms / J.L. Martin-Navarro, F.S. Amparo // Mathematics. – 2021. - №5 (9) – P. 1-22.

11. **Maiti, A.** A Systematic Method to Evaluate and Compare the Performance of Physical Unclonable Functions / A. Maiti, V. Gunreddy, P. Schaumont. In: Athanas, P., Pnevmatikatos, D., Sklavos, N. (eds.) Embedded Systems Design with FPGAs. Springer, New York, NY, 2013. – P. 245-267.

REFERENCES

1. **Yarmolik, V.N.** Fizicheski nekloniruemye funkcii / V.N. Yarmolik, Yu.G. Vashinko // Informatika. – 2011. – № 2(30). – PP. 92-103.

2. **Gassend, B.** Silicon physical random functions / B. Gassend [et al.] // Proc. of 9th Computer and Communications Security Conf. (CCS'02), Washington, DC USA, 18–22 Nov. 2002. – Washington, 2002. – PP. 148-160.

3. **Waksman, A.** A Permutation Network / A. Waksman // Journal of the ACM. – 1968. – № 1(15). – Pp. 159-163.

4. **Santikellur, P**. Deep Learning based Model Building Attacks on Arbiter PUF Compositions / P. Santikellur, A. Bhattacharyay, R.S. Chakraborty // IACR Cryptol. ePrint Arch. – 2019. – 10 p. – (Preprint / Paper 2019/566).

5. **Zhang, J.** Set-Based Obfuscation for Strong PUFs Against Machine Learning Attacks / J. Zhang, C. Shen // IEEE Transactions on Circuits and Systems I: Regular Papers. – 2021. – № 1(68). – Pp. 288-300.

6. **ZyboZ7: Zynq-7000 ARM/FPGA SoC Development Board** [Electronic resource] . – Mode of access: https://digilent.com/reference/programmable-logic/zybo-z7/start. – Date of access: 19.01.2023.

7. **Morozov, S.** An Analysis of Delay Based PUF Implementations on FPGA / S. Morozov, A. Maiti, P. Schaumont // Proc. of International Symposium on Applied Reconfigurable Computing: Tools and Applications (ARC 2010), Los Angeles, CA, US, 25–27 Mar. 2010. – Los Angeles, 2010. – P. 382–387.

8. **Costa, L.F.** Exploring complex networks through random walks [Electronic resource] / L.F. Costa, G. Travieso. – Physical Review E, 2007. – Mode of access: https://arxiv.org/pdf/ physics/ 0604193.pdf. – Date of access: 19.01.2023.

9. **Rukhin, A.** A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications [Electronic resource] / A. Rukhin [et al.] – NIST Special Publication 800-22, 2010. – Mode of access: https://www.nist.gov/publications/statistical-test-suite-random-and-pseudorandom-number-generators-cryptographic. - Date of access: 19.01.2023.

10. **Martin-Navarro, J.L.** Review of the Lineal Complexity Calculation through Binomial Decomposition-Based Algorithms / J.L. Martin-Navarro, F.S. Amparo // Mathematics. – 2021. – № 5(9) – Pp. 1-22.

11. **Maiti, A.** A Systematic Method to Evaluate and Compare the Performance of Physical Unclonable Functions / A. Maiti, V. Gunreddy, P. Schaumont. In: Athanas, P., Pnevmatikatos, D., Sklavos, N. (eds.) Embedded Systems Design with FPGAs. Springer, New York, NY, 2013. – Pp. 245-267.

IVANIUK A.A., SHAMYNA A.YU.

PHYSICALLY NON-CLONEABLE ARBITER -TYPE FUNCTION WITH NON-LINEAR PATH PAIRS

Belarusian state University of Informatics and Radioelectronics
Minsk, Republic of Belarus

Physically unclonable functions (PUFs) are basic physical cryptographical primitives, providing to solve tasks such as unclonable identification, digital device authentication and copyright authentication, true random sequence generation, etc. The major features of PUFs are stability, unpredictability and irreproducibility, due to uncontrollable random variations of distinctive features of the raw materials and technological processes used during their manufacturing. Generally, PUF are digital circuits that extract such variations and convert them into a binary format, which applied for further use. Among the variety of PUF types, an Arbiter PUF (APUF) is distinguished, which is a digital circuit with N-bit challenge input and single output for one-bit response generation. The functionality of APUF is based on comparison of transition time of two copies of the test signal along a pair of configurable paths, selected by the challenge value CH from a set of 2N all possible pairs. The result of the comparison is the binary value of the response. The set of all challenge-response pairs is a random, unpredictable and irreproducible in the cases of implementation of cloned PUF circuits both on single and/or on another chips, also using different technologies. This article presents a new approach to the synthesis of the APUF circuits, based on the permutation network elements, which allow to construct the nonlinear structures of pair of paths. This implies the potential complication of building an APUF model to attack its implemented instances. This article presents new schematic solutions for the synthesis of APUF circuits. Also, the main characteristics of the proposed APUF circuits implemented on the Xilinx Zynq-7000 FPGA is analyzed.

Keywords: *physically unclonable functions, arbiter, permutation networks.*

Иванюк Александр Александрович, доктор технических наук, доцент, профессор кафедры информатики БГУИР, заведующий совместной учебной лабораторией «СК хайникс мемори солюшнс Восточная Европа». Сфера научных интересов: физическая криптография, контролепригодное проектирование средств вычислительной техники. Автор более 150 научных работ и 8 патентов.

Alexander A. Ivaniuk, doctor of sciences, associated professor, professor at computer science department at the Belarusian State University of Informatics and Radioelectronics, head of the joint educational laboratory “SK hynix memory solutions Eastern Europe”. Research interests: physical cryptography, digital design and design for testability. He has published over 150 scientific articles and 8 patents.

E-mail: ivaniuk@bsuir.by

Шамына Артем Юрьевич, магистр технических наук, старший преподаватель кафедры ПОИТ БГУИР. Сфера научных интересов физическая криптография.

Artem Yu. Shamyna, Master of Engineering sciences, Senior Lecturer at the Belarusian State University of Informatics and Radioelectronics”. Research interests: physical cryptography

E-mail: shamyna@bsuir.by