УДК 004.312

Q-БИТНАЯ ФИЗИЧЕСКИ НЕКЛОНИРУЕМАЯ ФУНКЦИЯ ТИПА КОНФИГУРИРУЕМЫЙ КОЛЬЦЕВОЙ ОСЦИЛЛЯТОР И ОЦЕНКА ЕЕ ХАРАКТЕРИСТИК

Бурко Л.А., Иванюк А.А.

Белорусский государственный университет информатики и радиоэлектроники, Минск, Республика Беларусь, burkoliana@gmail.com

Аннотация: в работе исследуются основные характеристики q-битной физически неклонируемой функции (ФНФ) типа конфигурируемый кольцевой осциллятор (ККО). На поданный n-битный запрос данная ФНФ формирует q-битный ответ. Решается задача оценки характеристик стабильности, уникальности и единообразия сформированных ответов для q-битной ФНФ. Стабильность характеризует способность ФНФ воспроизводить один и тот же ответ при многократной подаче одного и того же запроса. Уникальность отражает степень различия ответов, формируемых для различных экземпляров ФНФ на различных ПЛИС (межкристальная уникальность) и внутри одной ПЛИС (внутрикристальная уникальность). Единообразие характеризует равномерность распределения получаемых ответов по множеству всех возможных значений. Приводятся результаты экспериментальных оценок q-битных ФНФ ККО, реализованных на ПЛИС Xilinx ZYNQ 7000.

Ключевые слова: физически неклонируемая функция, конфигурируемый кольцевой осциллятор, стабильность, уникальность, единообразие, ПЛИС.

I. ВВЕДЕНИЕ

Физически неклонируемые функции (ФНФ) представляют собой аппаратный механизм формирования уникального ответа на основе индивидуальных физических особенностей конкретного экземпляра электронного устройства. Эти особенности возникают вследствие технологического разброса параметров при изготовлении и практически невозможно полностью воспроизвести их в другом экземпляре устройства. Поэтому при подаче одинакового входного воздействия на различные экземпляры ФНФ они могут формировать различные ответы, в то время как один и тот же экземпляр при повторном измерении должен сохранять свой ответ. ФНФ применяются для идентификации и аутентификации электронных устройств, защиты аппаратуры и данных, а также в задачах формирования криптографических ключей. Исследование стабильности и уникальности ответов является актуальной задачей при разработке и оценке ФНФ. Особый интерес представляет формирование многобитного ответа, поскольку увеличение его разрядности позволяет расширить множество возможных значений ответа и повысить количество информации, получаемой при одном считывании. В предыдущих исследованиях [1, 2] был проведен анализ характеристик ФНФ на основе конфигурируемого кольцевого осциллятора (ККО). В настоящей работе рассматриваются особенности q-битной архитектуры ФНФ ККО и предлагается оценка ее характеристик с использованием метрик стабильности, уникальности и единообразия сформированных ответов.

В классической архитектуре ФНФ [3] каждому входному воздействию (многобитному запросу) CH соответствует однобитный ответ $R = PUF(CH) \in \{0,1\}$. Такой подход обеспечивает минимальный объем информации, получаемой в результате одного измерения. Для формирования q-битного результата необходимо либо использовать несколько независимых экземпляров ФНФ, либо применять несколько различных запросов и объединять полученные однобитные ответы.

В отличие от классического подхода, в новой предлагаемой архитектуре одному запросу CH_i соответствует q-битный ответ $R_i^q = PUF(CH_i)$, где $CH_i = \{ch_i, MW\}, i \in [0, 2^{n-1}]$, ch_i – n-битный запрос, MW – фиксированное окно измерения в периодах системного сигнала синхронизации [1]. В свою очередь $R_i^q = (r_i^{q-1}, r_i^{q-2}, \dots, r_i^0)$, где $r_i^l \in \{0,1\}$, $l \in [0, q-1]$, q – количество разрядов сформированного ответа. При этом различные значения q-битного ответа могут рассматриваться как символы некоторого алфавита $R_i^q = PUF(CH_i) \in \{0,1,\dots,2^q - 1\}$. Следовательно, при q-битном ответе одному запросу может соответствовать один из 2^q возможных символов алфавита.

II. МЕТРИКИ ОЦЕНКИ q-БИТНОЙ ФНФ ККО

Для оценки качества ФНФ ККО используются три основные метрики: стабильность, уникальность, единообразие. Метрики оценки характеристик однобитных ФНФ являются известными и хорошо изученными. В данной работе предлагается их адаптация для оценки ФНФ ККО, формирующей многобитный ответ.

Стабильность характеризует способность ФНФ ККО воспроизводить один и тот же ответ при многократных запросах в рамках одной конфигурации. Для каждого запроса CH_i выполняется $M > 1$ измерений выходного значения ККО. Для однобитного ответа вероятность появления значения «1» определяется как $p(R_i = 1) = \frac{1}{M}\sum_{j=0}^{M-1} R_i$, где R_i – значение ответа при j-ом измерении для запроса CH_i. Тогда стабильность однобитного ответа определяется как вероятность воспроизведения его наиболее встречаемого значения: $Stability_1(R_i) = max(p(R_i = 1), 1 - p(R_i = 1))$.

Для q-битного ответа $R_i^q = PUF(CH_i) = (r_i^{q-1}, r_i^{q-2}, \dots, r_i^0)$ сначала определяется вероятность появления значения «1» для каждого l-го ($l \in [0, q-1]$) бита $p(r_i^l = 1) = \frac{1}{M}\sum_{j=0}^{M-1} r_i^l$. Тогда стабильность l-го бита определяется как $Stab(r_i^l) = max(p(r_i^l = 1), 1 - p(r_i^l = 1))$. Итоговая стабильность q-битного ответа для запроса CH_i ($Stability_q(R_i^q)$) вычисляется как среднее арифметическое стабильностей его отдельных битов, а общая стабильность ФНФ ККО определяется как среднее значение по рассматриваемым запросам:

$$Stability_q(R_i^q) = \frac{1}{q}\sum_{l=0}^{q-1} Stab(r_i^l), \qquad Stability_q = \frac{1}{T}\sum_{i=0}^{T-1} Stability_q(R_i^q),$$

где T – количество поданных различных запросов.

При этом число рассматриваемых запросов существенно меньше полного пространства возможных значений ($T << 2^n$). Поэтому для экспериментальной оценки стабильности выбирается ограниченное количество запросов, например $T \approx 1000$. При этом высокая средняя побитовая стабильность не гарантирует полного совпадения всего q-битного ответа при каждом измерении. Поэтому для оценки возможности непосредственного воспроизведения ответов дополнительно может использоваться вероятность полного совпадения ответа:

$$P_q^{full}(R_i^q) = \frac{N_{full}(R_i^q)}{M}, \qquad \overline{P_q^{full}} = \frac{1}{T}\sum_{i=0}^{T-1} P_q^{full}(R_i^q)$$

где $N_{full}(R_i^q)$ – количество измерений, при которых сформированный q-битный ответ полностью совпал с эталонным ответом (наиболее встречаемым) для данного запроса.

Уникальность характеризует способность ФНФ ККО формировать уникальные ответы для различных входных воздействий и, соответственно, отсутствие коллизий между ответами на различных экземплярах. Пусть имеются два экземпляра ФНФ ККО a и b. Для одного запроса CH_i формируются однобитные ответы: $R_{a,i}, R_{b,i}$. Тогда уникальность определяется как удельное расстояния Хэмминга: $Uniq_1(R_{a,i}, R_{b,i}) = \frac{1}{T}\sum_{i=0}^{T-1}[R_{a,i} \oplus R_{b,i}]$.

Пусть для одного запроса CH_i два экземпляра ФНФ формируют q-битные ответы: $R_{a,i}^q, R_{b,i}^q$. Тогда уникальность определяется как среднее между удельными расстояниями Хэмминга:

$$Uniq_q(R_{a,i}^q, R_{b,i}^q) = \frac{1}{T \cdot q}\sum_{i=0}^{T-1} HD[R_{a,i}^q, R_{b,i}^q].$$

В идеальном случае значения ответов должны распределяться равномерно по диапазону всех возможных значений ($N = 2^n$), без выраженных пиков и провалов. Единообразие характеризует равномерность появления всех символов алфавита. Данная характеристика позволяет оценить, насколько равновероятно формируются различные значения ответов при изменении запроса.

Для каждого символа k алфавита выходной последовательности определяется число его появлений на T запросах: $C(k) = |\{R_i^q = k\}|$, где $k \in \{0, \dots, 2^q - 1\}, i \in [0, T-1]$. Далее вычисляется информационная энтропия:

$$H = -\sum_{t=0}^{T-1} \frac{C(k)}{T} \log_2 \frac{C(k)}{T}.$$

Максимальное значение энтропии будет равно числу бит в генерируемых символах, т.е. q. Тогда единообразие можно определить как:

$$\overline{Uniformity} = \frac{H}{q} \in [0,1].$$

В рамках эксперимента для каждого экземпляра ФНФ ККО рассматривалось $T = 1024$ различных значений запроса $ch_i \in [0{,}1023]$. Для каждого значения $CH_i = \{ch_i, MW = 5 \times 10^5\}$ на каждом экземпляре ФНФ ККО производилось $M = 1024$ регистраций выходного значения. В эксперименте были использованы четыре ПЛИС (ПЛИС$_1$, ПЛИС$_2$, ПЛИС$_3$, ПЛИС$_4$) на каждой из которых реализовано по четыре ККО (ККО$_1$, ККО$_2$, ККО$_3$, ККО$_4$). Ответ каждого экземпляра ФНФ ККО имеет длину $q = 21$ бит.

Для формирования воспроизводимого ответа ФНФ ККО проведен побитовый анализ стабильности исходного 21-битного ответа. На основании полученных вероятностей выделялись наиболее стабильные битовые позиции. В результате для дальнейшего формирования ответа использовалась стабильная старшая часть, состоящая из 7 бит ($R_i^7 \in \{64, \ldots, 127\}$). После исключения одного бита, не содержащего дополнительной различающей информации, формировался шестибитный ответ в диапазоне $R_i^{7^*} \in \{0, \ldots, 63\}$. Сокращение разрядности при сохранении наиболее стабильных битов позволяет повысить воспроизводимость ответа и использовать его для последующей уникальной идентификации ФНФ. Результаты метрик стабильности представлены в таблице 1.

Таблица 1. Результаты метрик стабильности для $q = 21$ бит и $q = 7$ бит

	ККО$_1$		ККО$_2$		ККО$_3$		ККО$_4$	
	$\overline{Stability_{21}}$	$\overline{Stability_7}$	$\overline{Stability_{21}}$	$\overline{Stability_7}$	$\overline{Stability_{21}}$	$\overline{Stability_7}$	$\overline{Stability_{21}}$	$\overline{Stability_7}$
ПЛИС$_1$	0,761	0,996	0,760	0,995	0,761	0,997	0,762	0,997
ПЛИС$_2$	0,763	0,996	0,765	0,998	0,762	0,996	0,765	0,997
ПЛИС$_3$	0,762	0,997	0,761	0,997	0,761	0,996	0,763	0,997
ПЛИС$_4$	0,761	0,997	0,760	0,996	0,760	0,996	0,760	0,996

	$\overline{P_{21}^{full}}$	$\overline{P_7^{full}}$	$\overline{P_{21}^{full}}$	$\overline{P_7^{full}}$	$\overline{P_{21}^{full}}$	$\overline{P_7^{full}}$	$\overline{P_{21}^{full}}$	$\overline{P_7^{full}}$
ПЛИС$_1$	0,0067	0,9913	0,0067	0,9863	0,0067	0,9912	0,0066	0,9905
ПЛИС$_2$	0,0068	0,9869	0,0067	0,9925	0,0067	0,9890	0,0067	0,9894
ПЛИС$_3$	0,0067	0,9907	0,0066	0,9899	0,0066	0,9890	0,0065	0,9920
ПЛИС$_4$	0,0068	0,9914	0,0066	0,9882	0,0065	0,9896	0,0065	0,9872

Далее была проведена оценка уникальности шестибитных ответов, формируемых на основе различных ККО, размещенных как внутри одной ПЛИС, так и на разных ПЛИС. При внутри-кристальном анализе для каждой ПЛИС рассматривались шесть возможных пар ККО. При межкристальном анализе для каждого ККО сравнивались ответы, полученные на четырех различных ПЛИС. Результаты внутрикристального анализа показали, что средние значения уникальности для исследуемых ПЛИС находятся в достаточно узком диапазоне: ПЛИС$_1$ – 0,427734, ПЛИС$_2$ – 0,420058, ПЛИС$_3$ – 0,419027, ПЛИС$_4$ – 0,427544. При межкристальном сравнении получены более высокие значения: ККО$_1$ – 0,482964, ККО$_2$ – 0,478217, ККО$_3$ – 0,479791, ККО$_4$ – 0,482322. Сопоставление результатов показывает, что межкристальная уникальность выше внутрикристальной, что в дальнейшем может быть использовано для задач неклонируемоей идентификации.

Для визуальной оценки единообразия полученные ответы группировались по их числовому значению, после чего строилась гистограмма их распределения. На рисунке 1 по оси абсцисс откладывается значение символа алфавита k, а по оси ординат – количество его появлений $C(k)$ на T запросах. По графику видно, что в исследуемой схеме распределение неравномерное, что требует дальнейшего исследования. Полученные результаты $\overline{Uniformity}$ показывают, что для всех исследованных ПЛИС значения единообразия находятся в диапазоне от 0,860 до 0,924 ($H \in [5{,}16; 5{,}54]$), что может быть приемлемо для генерации истинно случайных последовательностей.

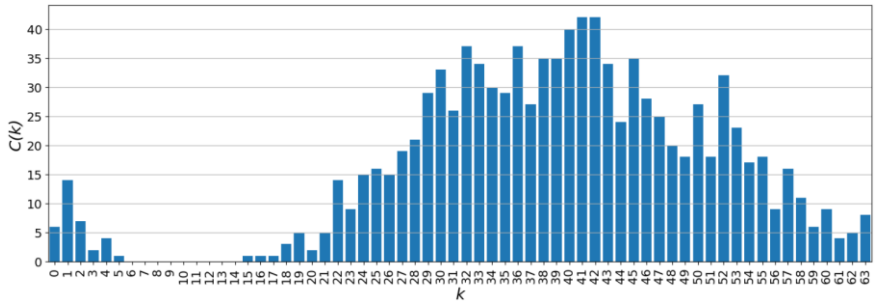


Рисунок 1. Распределение ответов от q-мерного ФНФ ККО

III. ЗАКЛЮЧЕНИЕ

В работе рассмотрена архитектура ФНФ ККО, формирующая многобитный ответ на одно входное воздействие. В отличие от классического однобитного представления, использование многобитного ответа позволяет за одно измерение получить больше информации и сформировать расширенный алфавит возможных ответов. Для рассматриваемой архитектуры исходный 21-битный результат был проанализирован с точки зрения стабильности отдельных разрядов, после чего для формирования воспроизводимого ответа была выделена наиболее стабильная часть и сформирован шестибитный ответ. Для оценки полученных ответов были адаптированы метрики стабильности, уникальности и единообразия, позволяющие учитывать особенности многобитного представления. Побитовая оценка стабильности позволяет определить вклад отдельных разрядов в воспроизводимость ответа, а дополнительная оценка полного совпадения позволяет непосредственно характеризовать вероятность получения всего многобитного ответа без изменений при повторных измерениях.

БЛАГОДАРНОСТЬ

Авторы выражают искреннюю благодарность резиденту ПВТ компании «Инженерный Центр Ядро», которая является одним из центров разработки YADRO, за предоставленное оборудование для проведения экспериментов в рамках работы совместной учебной лаборатории с Белорусским государственным университетом информатики и радиоэлектроники.

ЛИТЕРАТУРА

[1] Иванюк А.А., Бурко Л.А. Генерирование детерминированных идентификаторов и случайных чисел на основе схемы конфигурируемого кольцевого осциллятора. Информатика. 2025;22(4):65-81. https://doi.org/10.37661/1816-0301-2025-22-4-65-81.

[2] Ivaniuk, A. Unclonable Identification and True Random Number Generation Based on CRO PUF / A. Ivaniuk, L. Burko // Pattern Recognition and Information Processing (PRIP2025): Proceedings of the 17th International Conference, September 16-18, 2025, Minsk, Belarus / UIIP NASB. – Minsk, 2025.– pp. 103-107.

[3] Deng D., Hou S., Wang Z., Guo Y. Configurable ring oscillator PUF using hybrid logic gates. IEEE Access, 2020, vol. 8, pp. 161427–161437. DOI: 10.1109/ACCESS.2020.3021205.

Q-BIT PHYSICALLY UNCLONABLE FUNCTION BASED ON A CONFIGURABLE RING OSCILLATOR AND EVALUATION OF ITS CHARACTERISTICS

L.A. Burko, A.A. Ivaniuk

Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus,
burkoliana@gmail.com

Abstract: this paper examines the main characteristics of a q-bit physically unclonable function (PUF) based on a configurable ring oscillator (CRO). For a given n-bit challenge, the PUF generates a q-bit response. The stability, uniqueness, and uniformity of the generated responses are evaluated for the q-bit PUF. Stability characterizes the ability of the PUF to reproduce the same response when the same challenge is applied repeatedly. Uniqueness reflects the degree of difference between responses generated by different PUF instances on different FPGAs (inter-chip uniqueness) and within a single FPGA (intra-chip uniqueness). Uniformity characterizes how evenly the generated responses are distributed over the set of all possible values. Experimental evaluation results for q-bit CRO-based PUFs implemented on Xilinx ZYNQ 7000 FPGAs are presented.

Keywords: physically unclonable function, configurable ring oscillator, stability, uniqueness, uniformity, FPGA.