Russian Technological Journal.
2026;14(2):80–102

ISSN 2782-3210 (Print)
ISSN 2500-316X (Online)

Микро- и наноэлектроника. Физика конденсированного состояния

Micro- and nanoelectronics. Condensed matter physics

УДК 004.832.32
https://doi.org/10.32362/2500-316X-2026-14-2-80-102
EDN LLZOKJ

ОБЗОРНАЯ СТАТЬЯ

Физически неклонируемые функции в цифровых интегральных схемах

Е.Ф. Певцов [@], Т.А. Деменкова, Ю.А. Коротаев [@], А.С. Сигов

MIREA – Russian Technological University, Moscow, 119454 Russia
[@] Авторы для переписки, e-mail: pevtsov@mirea.ru, korotaevya@yandex.ru

• **Поступила:** 16.09.2025 • **Доработана:** 23.09.2025 • **Принята к опубликованию:** 12.02.2026

Резюме

Цели. Преимуществом модулей, реализующих физически неклонируемые функции (ФНФ) и встроенных в цифровой чип, является то, что отклики на запросы могут быть напрямую использованы другими приложениями устройства. Устройство способно запрашивать и считывать ФНФ без привлечения внешних инструментов и вывода запроса и ответа за пределы чипа. ФНФ может быть реализована с использованием технологических операций и компонентов, применяемых при изготовлении самого устройства. Статья является первой из двух обзорных публикаций, посвященных ФНФ как компонентам инфраструктуры аппаратной безопасности. Данная статья фокусируется на формальном описании ФНФ и их конструкциях, основанных на модулях памяти и анализе временных характеристик сигналов.

Методы. Использованы методы определения количественных показателей и признаков для формального описания ФНФ: вычислимость, уникальность, возможность реализации, сложность клонирования, защита от несанкционированного доступа.

Результаты. Рассмотрены реализации ФНФ как физических устройств, обладающих уникальной сигнатурой. Предложена их классификация: ФНФ на основе временных характеристик сигналов, ФНФ на основе схем памяти и аналоговые ФНФ. Приведены наиболее типичные примеры реализаций первых двух типов. Показано, что решения на основе задержек сигналов обеспечивают широкое пространство пар «запрос – ответ», но требуют симметрии и/или калибровки, тогда как ФНФ на базе памяти проще реализуются в интегральных схемах и при корректной постобработке достигают высокой воспроизводимости, что делает их практичным выбором для многих приложений. Описаны подходы к компенсации влияния вариаций напряжения и температуры. Приведены примеры «сильных» память-ориентированных ФНФ и схемотехнические приемы повышения их стойкости к атакам.

Выводы. Технология обеспечения безопасности на основе ФНФ обладает значительным потенциалом, особенно для применения в устройствах интернета вещей. Проведенный анализ показывает, что в сочетании с методами постобработки и компенсации эксплуатационных факторов ФНФ является зрелым инструментом обеспечения аппаратной безопасности.

Ключевые слова: физически неклонируемая функция, ФНФ, интегральные схемы, аппаратная безопасность, ФНФ типа «арбитр», ФНФ на основе памяти, SRAM, DRAM, интернет вещей

Для цитирования: Певцов Е.Ф., Деменкова Т.А., Коротаев Ю.А., Сигов А.С. Физически неклонируемые функции в цифровых интегральных схемах. *Russian Technological Journal*. 2026;14(2):80–102. https://doi.org/10.32362/2500-316X-2026-14-2-80-102, https://www.elibrary.ru/LLZOKJ

Прозрачность финансовой деятельности: Авторы не имеют финансовой заинтересованности в представленных материалах или методах.

Авторы заявляют об отсутствии конфликта интересов.

REVIEW ARTICLE

Physically unclonable functions in digital integrated circuits

Evgenii Ph. Pevtsov [@], Tatyana A. Demenkova, Yuri A. Korotaev [@], Alexander S. Sigov

MIREA – Russian Technological University, Moscow, 119454 Russia
[@] Corresponding authors, e-mail: pevtsov@mirea.ru, korotaevya@yandex.ru

• **Submitted:** 16.09.2025 • **Revised:** 23.09.2025 • **Accepted:** 12.02.2026

Abstract

Objectives. Modules that implement physically unclonable functions (PUFs) within a digital chip facilitate the direct use of challenge–response pairs by device applications that can query and read the PUF without external tools or exposing data outside the chip. A PUF can be implemented using technological processes and components already applied in device fabrication. The first of two reviews on PUFs as elements of hardware security infrastructure, the present paper focuses on the formal description of PUFs and designs based on memory modules and timing analysis.

Methods. The following quantitative indicators were applied to formally describe PUFs: computability, uniqueness, feasibility, cloning resistance, and protection against unauthorized access.

Results. PUFs are considered as physical devices with unique signatures. A classification into three PUF groups is proposed: delay-based, memory-based, and analog. Typical examples of the first two groups are outlined. While delay-based solutions provide a large challenge–response space, they require symmetry and/or calibration. In contrast, memory-based PUFs are easier to implement in integrated circuits. With suitable post-processing, they can achieve high reproducibility, making them practical for many applications. Approaches to mitigating voltage and temperature variations are described along with examples of strong memory-oriented PUFs and circuit techniques that enhance resistance to attacks.

Conclusions. PUF-based security technologies demonstrate significant potential, particularly for the Internet of Things. When combined with post-processing and compensation methods, PUFs constitute a mature and effective tool for hardware security.

Keywords: physically unclonable function, PUF, integrated circuits, hardware security, arbiter PUF, memory-based PUF, SRAM, DRAM, Internet of Things

For citation: Pevtsov E.Ph., Demenkova T.A., Korotaev Yu.A., Sigov A.S. Physically unclonable functions in digital integrated circuits. *Russian Technological Journal.* 2026;14(2):80–102. https://doi.org/10.32362/2500-316X-2026-14-2-80-102, https://www.elibrary.ru/LLZOKJ

Financial disclosure: The authors have no financial or proprietary interest in any material or method mentioned.

The authors declare no conflicts of interest.

ВВЕДЕНИЕ

Наличие конфиденциальной и интеллектуальной информации в аппаратных устройствах, предназначенных для выполнения специализированных задач искусственного интеллекта, делает их выгодной мишенью для хакерских атак. Злоумышленник может нарушить безопасность аппаратных средств, перехватить информацию для получения финансовой выгоды и украсть интеллектуальную собственность для проведения обратного проектирования с целью производства поддельных клонированных устройств. Помимо клонированных подделок, переработанные и восстановленные устройства могут продаваться как новые, что приводит к потере доходов производителями и возникновению проблем с безопасностью из-за сокращения срока их службы и надежности.

Одно из возможных решений для обеспечения безопасности оборудования заключается в физическом внедрении защищенных схем для аутентификации устройства, генерации случайного ключа доступа и других, все более усложняющихся способов защиты от подделок. Схемы защиты обладают уникальной сигнатурой, аналогичной отпечаткам сетчатки/пальцев человека и ДНК[1]. Эти сигнатуры являются случайными, их трудно предсказать и достаточно сложно клонировать, что предотвращает несанкционированный доступ к данным. Таким образом, актуальной является тема реализации надежных аппаратных платформ для безопасной связи, аутентификации устройств и защиты от разнообразных программных и аппаратных рисков и атак хакеров.

Физически неклонируемая функция (ФНФ) представляет собой физический объект, работа которого не может быть воспроизведена («клонирована») физическим способом (путем создания другой системы с использованием той же технологии), который для заданных входных данных и условий (запроса) обеспечивает физически определенный выходной сигнал (ответ) «цифрового отпечатка пальца», являющийся уникальным идентификатором конкретного экземпляра устройства. Это актуально для применения в приложениях с высокими требованиями к безопасности, например, в криптографии, устройствах интернета вещей и для защиты конфиденциальности.

Согласно определению, ФНФ выполняет функциональную операцию, т.е. при запросе с определенными входными данными она выдает результат, поддающийся измерению или оценке. Следует рассматривать ФНФ как функцию в инженерном смысле, т.е. процедуру, выполняемую конкретной (физической) системой или воздействующую на нее. Как правило, входные данные для ФНФ называются запросом, на который на выходе формируется некий ответ. Выполненный запрос и измеренный ответ на него обычно называются парой «запрос – ответ» (challenge to response pair, CRP), а соотношение, устанавливаемое между запросами и ответами с помощью конкретной реализации ФНФ, описывает процедуру реализации CRP.

Тема ФНФ широко освещается в научной литературе, в частности, из-за очевидной необходимости обеспечения безопасности устройств интернета вещей [1]. В настоящей работе обобщаются результаты, изложенные в основном в последних публикациях о современных ФНФ и их реализациях [2–4].

КОЛИЧЕСТВЕННЫЕ ПОКАЗАТЕЛИ ФНФ

Наиболее полное описание свойств, по которым можно оценивать различные реализации ФНФ, приведено в работах [5–7]. Как в рамках одного типа ФНФ, так и для сравнения разных типов ФНФ между собой применяются понятия теории классификации и идентификации.

Для набора мгновенных воздействий конкретной конструкции ФНФ применяются следующие два типа количественных показателей.

- Количественная оценка между двумя различными экземплярами, реализующими конкретную ФНФ – это разность между двумя ответами, полученными в результате однократного применения запроса к обеим реализациям ФНФ. Согласно классификации, предложенной в работе [7], соответствующее обозначение этой метрики – inter-distance. Следовательно, это случайная величина, описывающая расстояние между двумя ответами ФНФ от разных экземпляров ФНФ, использующих один и тот же вызов.
- Количественная характеристика, описывающая отличия между двумя оценками в одном экземпляре ФНФ – это разность между двумя разными ответами, полученными в результате двухкратного применения запроса к одной реализации ФНФ. В этом случае метрика обозначается как intra-distance. Это случайная величина, описывающая расстояние между двумя ответами ФНФ, полученными от одного и того же экземпляра ФНФ и использующими один и тот же вызов.
- Воспроизводимость и уникальность ФНФ определяются этими показателями. Для обеих метрик применяется один и тот же запрос. При этом конкретное значение количественных характеристик для одного экземпляра или для разных

[1] Дезоксирибонуклеиновая кислота. [Deoxyribonucleic acid.]

экземпляров ФНФ может варьироваться в зависимости от сложности и количества испытаний, т.е. используемая мера количественных оценок может варьироваться в зависимости от характера реакции. В частности, в случаях, когда ответом является битовая строка, в качестве критерия используется расстояние Хэмминга (inter-Hamming distance, inter-HD).

Для конкретного типа ФНФ характеристики inter-distance и intra-distance часто обобщаются в виде гистограмм, иллюстрирующих результаты выполнения нескольких запросов для одного устройства с ФНФ и результаты, наблюдаемые при выполнении ряда различных запросов для нескольких однотипных устройств с ФНФ. Как указано в работе [6], во многих случаях обе гистограммы могут быть аппроксимированы гауссовым распределением с указанием их средних значений, соответственно μ_{inter} и μ_{intra}, и, при наличии, их стандартных отклонений, соответственно σ_{inter} и σ_{intra}.

Из определения следует, что μ_{intra} выражает средний уровень шума в ответах, т.е. характеризует воспроизводимость измеренного ответа по сравнению с другими наблюдениями того же ответа. Очевидно, что чем меньше значение μ_{intra}, тем более надежные ответы реализует данная ФНФ. С другой стороны, μ_{inter} выражает понятие уникальности, т.е. измеряет среднюю различимость двух систем на основе их ответов ФНФ. Если ответы представляют собой битовые строки, то наилучшая различимость, которой можно достичь – это если отличается в среднем половина битов. В частности, если μ_{inter} выражается как относительное значение расстояния Хэмминга, наилучшим результатом является значение, близкое к 50%. На практике одновременная реализация минимума μ_{intra} и 50% μ_{inter} является задачей компромисса применяемых методов реализации ФНФ. Практическое применение обоих понятий иллюстрируется рис. 1 [6], на котором показан пример использования ФНФ для целей идентификации.

Получение ответа ФНФ, как правило, связано с физическим измерением, следовательно, существует ряд нежелательных побочных физических эффектов, которые могут повлиять на результат. Очевидными причинами является случайный шум и погрешности измерений. В результате один и тот же запрос не обязательно вызывает один и тот же ответ, что приводит к так называемой внутренней дистанции (см. определение intra-distance) между ответами ФНФ. Внешние факторы также оказывают систематическое влияние на измерение отклика, например, температура или напряжение питания в случае, когда ФНФ реализуется в интегральной схеме (ИС). Таким образом, для корректного сравнения различных результатов из литературных источников необходимо учитывать, в каких условиях получены значения μ_{intra}. Пример влияния температуры на воспроизводимость ФНФ приведен в работе [8]. Если воздействие окружающей среды носит систематический характер, могут быть применены методы, позволяющие снизить его влияние на реакцию ФНФ. Другими возможными вариантами являются введение компенсирующих коэффициентов [9] и специальные стратегии реализации ФНФ, минимизирующие зависимость от окружающей среды [7, 10].

С точки зрения эффективности применения ФНФ могут быть классифицированы как «слабые» и «сильные». ФНФ считается «слабой», если существует всего несколько комбинаций CRP с реакциями, которые, как правило, мало

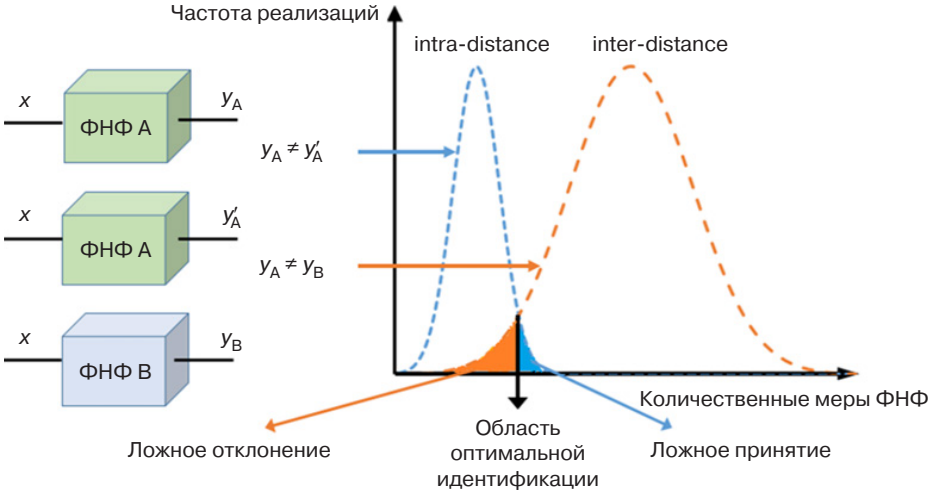


Рис. 1. Количественные характеристики ФНФ [6].
x – запрос, y_A, y'_A – ответы конкретного экземпляра ФНФ на запрос;
y_B – ответ другого экземпляра ФНФ на тот же запрос

чувствительны к изменениям окружающей среды. Хотя в «слабых» ФНФ относительно мала устойчивость к атакам хакеров, они используются для создания секретных ключей из-за их высокой стабильности. В случае «сильной» ФНФ, реализующее ее устройство имеет достаточно большое количество CRP, так что злоумышленник не сможет в реальное время разрушить систему идентификации. В связи с этим при физической реализации ФНФ следует повышенное внимание уделять защите от атак на вскрытие ФНФ, в частности, применяющих методы машинного обучения.

Стандартной процедурой характеризации ФНФ является прохождение статистических тестов, целью которых является определение меры случайности двоичных последовательностей, порожденных либо аппаратными, либо программными генераторами случайных чисел. Эти тесты разработаны Лабораторией информационных технологий (Information Technology Laboratory), являющейся главной исследовательской лабораторией Национального института стандартов и технологий[2], и основаны на различных статистических свойствах, присущих только случайным последовательностям.

ФОРМАЛЬНОЕ ОПИСАНИЕ ФНФ

Одна из попыток формального описания ФНФ, основанная на описании физической процедуры реагирования на запросы, предпринята в работе [7]. Создание экземпляра ФНФ не может быть просто абстрактным понятием, но всегда связано с конкретным физическим объектом. ФНФ – это процедура П, представимая некоторой функциональностью ввода-вывода, которую формально можно выразить как преобразование «запрос – ответ» ФНФ $П: X \rightarrow Y: П(x)$. Формально процедуру «запрос – ответ» можно отнести к ФНФ, если она характеризуется следующими свойствами:

1. Вычислимость: при заданных процедурах П и аргументах x из множества X есть способ вычислить $Y = П(x)$ за полиномиальное алгоритмическое время. Это означает, что необходимо, чтобы создание ФНФ было возможно с минимальными усилиями, например, в условиях ограниченного времени, площади, мощности и энергопотребления при интегрировании в чип. Ясно, что если ФНФ поддается вычислению, то подразумевается, что она может быть сконструирована. Также, очевидно, что все варианты ФНФ, которые предоставляют экспериментальные результаты, могут быть сконструированы и, по крайней мере, теоретически оценены.
2. Уникальность: $П(x)$ содержит некоторую информацию об идентичности физического объекта, реализующего П. Если рассматривается четко определенный набор или совокупность экземпляров ФНФ, то информация, содержащаяся в ответе $П(x)$ ФНФ, позволяет осуществить идентификацию, которую можно произвести из совокупности на основе этого ответа. Последовательные ответы позволяют создавать все меньшие и меньшие неопределенности идентификации до тех пор, пока оптимально не останется объект с одним экземпляром ФНФ, и в этом случае рассматриваемый набор «запрос – ответ» будет уникальным для идентификации ФНФ в рассматриваемом множестве объектов. Исходя из размера множества и характеристик ответов ФНФ, такая уникальная идентификация может быть возможной, а может и не быть. Одним из возможных показателей уникальности, который приводится в большинстве экспериментальных результатов, является гистограмма промежуточных метрик inter-distance, суммируемая по их среднему значению μ_{inter}.
3. Воспроизводимость: $y = П(x)$ воспроизводится с погрешностью, достаточной для идентификации ФНФ. Ответы на различные запросы x в одной и той же П ФНФ должны быть близки по рассматриваемому показателю метрики различий ответов. При интерпретации экспериментальных результатов они в основном измеряются с помощью гистограммы внутренней метрики intra-distance и суммируются по его среднему значению μ_{intra}. Воспроизводимость – это свойство, которое отличает ФНФ от настоящих генераторов случайных чисел (true random number generator, TRNGs).
4. Неклонируемость: для заданной процедуры П не существует другой процедуры Г, не эквивалентной П, такой, чтобы $\forall x \in X\ Г(x) \approx П(x)$ с точностью до погрешности реализации. Следует принять во внимание, что процедура клонирования Г необязательно физически реализуема, т.е. различаются физическая и математическая неклонируемости. Если трудно найти физический объект, содержащий другую ФНФ $П_Г \neq П$, такой, что $\forall x \in X\ П_Г(x) \neq П(x)$, утверждается, что реализация П физически невозможна. Сложность создания физического клона сохраняется даже для производителя оригинальной ФНФ. В этом случае она называется стойкостью производителя. Если трудно придумать (абстрактную) математическую процедуру $f_Г$, такую, что $\forall x \in X\ f_Г(x) \approx П(x)$,

[2] The National Institute of Standards and Technology, NIST. https://www.nist.gov/. Дата обращения 19.07.2025. / Accessed July 19, 2025.

утверждается, что П математически неопределима. Физическая и математическая неклонируемости – это принципиально разные свойства, конструкция может быть легко клонирована физически, но не математически, или наоборот. Для того, чтобы ФНФ была действительно неклонируемой, процедура реализации П должна быть как физически, так и математически неклонируемой. Следует отметить, что физическое клонирование может быть очень трудным или неосуществимым, при этом теоретически доказать неклонируемость очень сложно. Очевидно, что системы, основанные на квантовой физике, теоретически не поддаются клонированию.

5. Непредсказуемость: для набора процедур $Q = \{f(x_i, y_i) = П(x_i)\}$, с точностью до погрешности, нельзя определить $y_c \approx П(x_c)$ для случайного запроса x_c (random challenge), такого, что $(x_c) \notin Q$. Если возможно точно предсказать ответ ФНФ для случайного запроса, просто наблюдая за набором CRP, то легко создать математический клон при наличии доступа к полному каталогу вариантов ответов ФНФ.
6. Односторонность: для аргументов y и процедур П с точностью до погрешности нельзя найти x, такое, чтобы $П(x) = y$. В некоторых работах ФНФ упрощенно описываются как физический вариант односторонних функций, применяемый для объектов криптографии [11].
7. Очевидность вмешательства: изменение физического объекта, описываемого процедурой П при внедрении преобразующего $П \rightarrow П'$ таким образом, что с высокой вероятностью справедливо $\forall x \in X\ П(x) \neq П'(x)$ даже с точностью до погрешности реализации П. Следует различать системы защиты от несанкционированного доступа, т.е. системы, в которых вмешательство не приводит к получению какой-либо полезной информации, и системы, в которых вмешательство очевидно и вредоносно, т.е. системы, в которых вмешательство в физический объект, содержащий ФНФ, изменяет поведение CRP.

РЕАЛИЗАЦИИ ФНФ, ОСНОВАННЫЕ НА АНАЛИЗЕ ВРЕМЕННЫХ ХАРАКТЕРИСТИК СИГНАЛОВ

Большим преимуществом ФНФ, встроенной в цифровой чип, является то, что отклики на запросы могут быть напрямую использованы другими приложениями, работающими на том же устройстве. В частности, устройство может запрашивать и считывать свою собственную ФНФ без необходимости использования внешних инструментов и без необходимости того, чтобы запрос и ответ покидали устройство. С другой стороны, ФНФ может быть реализована с использованием только технологических операций и компонентов, которые применяются при изготовлении самого устройства, в котором размещен узел ФНФ, что практически не требует дополнительных затрат.

В обзорных публикациях [2, 3, 12–18] приведено несколько вариантов классификаций ФНФ: по времени появления первых разработок, по физическим конструктивным (гибридным или полностью электронным) свойствам и технологиям реализации (электронные, оптические, радиочастотные, магнитные), размерам пар CRP, области применения и т.д. Обобщая эти классификации, условно реализации ФНФ в ИС можно разделить на три основных типа: 1) на основе временных характеристик сигналов; 2) на основе схем памяти; 3) аналоговые и пассивные.

ФНФ на основе кольцевых осцилляторов (RO-PUF[3])

В этих устройствах для формирования ФНФ используется эффект рассогласования частот кольцевых генераторов, построенных на инверторах [19]. Из-за производственных вариаций два номинально идентичных кольцевых генератора, реализованные на одном кристалле, будут иметь фиксируемую разность частот. Как показано на рис. 2, в RO-PUF закладывается массив из N таких осцилляторов.

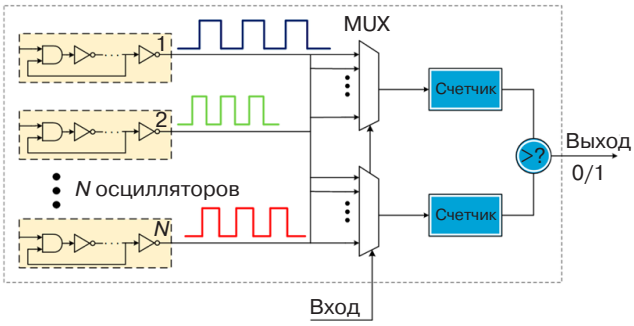


Рис. 2. Пример реализации ФНФ на основе кольцевого осциллятора [3]. MUX – мультиплексор

Результат сравнения частот двух кольцевых генераторов формирует бит ответа. Запрос заключается в количестве или расположении кольцевых генераторов, а ответной реакцией является результат разности частот их колебаний. Для надежного сравнения частот применяются счетчики, подсчитывающие число импульсов каждого осциллятора за заданный временной интервал. Альтернативный подход – подключать выходы двух генераторов на входы RS-триггера[4].

[3] Ring oscillator physical unclonable function (PUF).
[4] R (reset) – сброс, S (set) – установка.

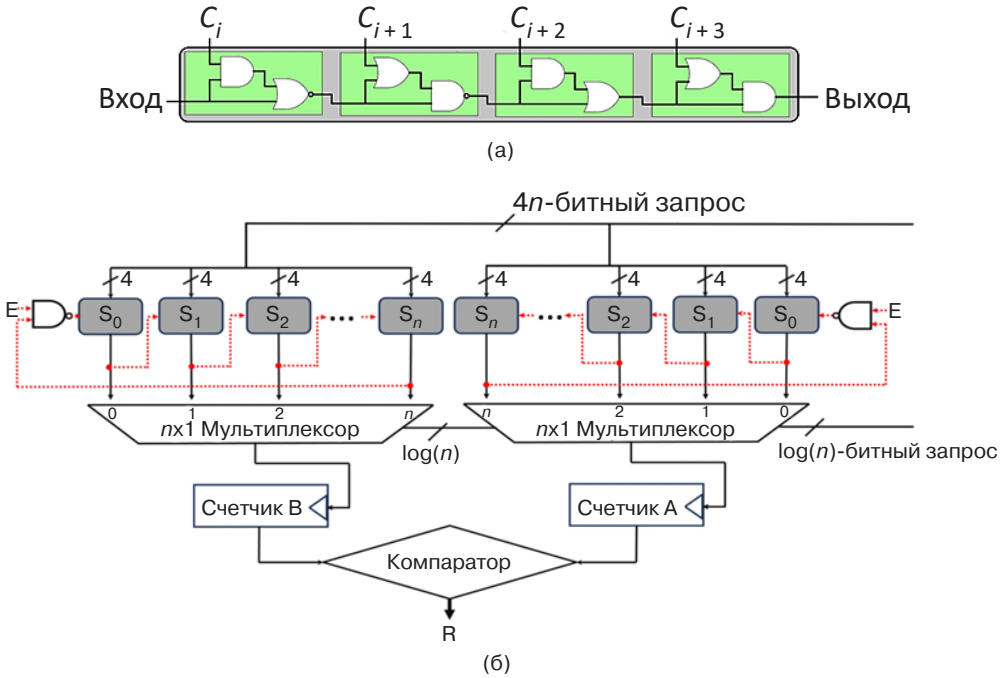


Рис. 3. Микроархитектура RO-PUF: (а) модуль формирования задержки, (б) устройство формирования бита ответа на конфигурируемый 4-разрядный запрос [24]. C_i, …, C_{i+3} – challenges (запросы); E – enable (сигнал разрешения); nx1 – мультиплексор с n входами и 1 выходом; R – response (ответ)

Реализации RO-PUF демонстрируют умеренную сложность: схема состоит из повторяющихся блоков генераторов и простых цифровых счетчиков/компараторов. Для получения N бит необходимо, по меньшей мере, порядка $2N$ генераторов (каждый бит требует уникальной пары RO[5]). Часто используют более экономичные схемы, например, сортируют частоты множества RO и генерируют множество бит, сравнивая различные пары в упорядоченном списке – это позволяет получить несколько бит из N генераторов, но может усложнить анализ. Согласно [3] уникальность хорошо спроектированного RO-PUF близка к 50% – случайные разбросы частот дают равновероятное превосходство одного генератора над другим. Повторяемость также может быть высокой: если разница частот выбранных пар достаточно велика, то порядок их сравнения сохраняется даже при изменениях температуры и напряжения. В экспериментах достигается надежность 95–99%. Тем не менее, при неблагоприятных условиях (например, при сближении частот из-за температурного дрейфа) некоторые биты ответов могут инвертироваться, поэтому для повышения надежности вводят запас по частоте или используют кодирование ответов.

Масштабирование RO-PUF на более высокие частоты в современных техпроцессах требует учета увеличения флуктуаций периода, поскольку на нанометровых нормах шум может вносить ошибки, сравнимые с разницей частот кольцевых генераторов.

В работах [20, 21] продемонстрирована успешная реализация RO-PUF в FPGA[6]. В настоящее время предложено несколько разработок, направленных на улучшение характеристик RO-PUF, переводящих их в разряд сильных ФНФ [22]. В работах [23, 24] описывается архитектура конфигурируемого RO-PUF, в которой используются изменения частоты и фазового сдвига, а каждый блок задержки S_0, …, S_n выполнен из логических элементов, сформированных парами n- и p-MOS[7] транзисторов так, что суммарное время задержки возрастает в соответствии с ужесточением технологических допусков на их изготовление. На примере, приведенном на рис. 3а, каждый блок задержки S сконфигурирован для формирования 4-разрядного запроса. На рис. 3б N каскадов задержки включены последовательно, причем выходные данные каждого из них применяются для переключения сигналов запуска счетчиков, значения которых сравниваются компаратором для выдачи сигнала ответа.

Предлагаемая конструкция устраняет дублирование кольцевых генераторов, снижает коммутационную активность и вносит межкаскадную задержку в качестве дополнительного источника случайности. Предложенный ФНФ был реализован в 22-нм режиме

[5] Ring oscillator – кольцевой осциллятор.

[6] Field-programmable gate array – программируемая пользователем вентильная матрица.

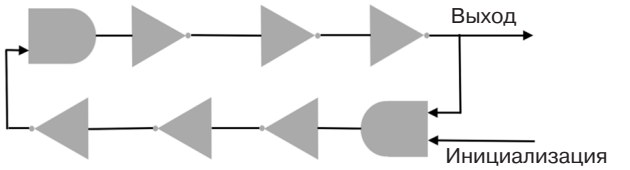
[7] Metal-oxide-semiconductor – металл-оксид-полупроводник.

по технологии FD SOI[8] с использованием инструментов Synopsys[9]. Результаты испытаний на 8 чипах успешно прошли тесты NIST, значения intra-HD и inter-HD (внутреннее и внешнее расстояния Хэмминга соответственно) составили 9.95% и 45.5% соответственно.

Другой вариант ФНФ с конфигурируемым кольцевым осциллятором (ККО ФНФ) предложен в работе [25]. ФНФ выполнена как модификация базовой схемы из элементов XOR2, выполняющих роль элементов управляемой задержки, для которой возможно применение полного множества запросов. Показано, что задержка зависит не только от значения запроса, но и от конфигурации межсоединений структурных элементов схемы с конфигурируемым кольцевым генератором. Предлагается временная модель модифицированной ККО ФНФ, позволяющая аналитически доказать влияние межсоединений на частоту вырабатываемого сигнала, что экспериментально подтверждено с использованием FPGA Xilinx серии Zynq-7000 (Xilinx, США).

Проблема компенсации влияния температуры на ФНФ рассмотрена в статьях [26, 27]. Авторы проанализировали влияние температурных характеристик MOSFET[10] на свойства RO-PUF без изменения исходной структуры схемы. Моделирование 55-нм процесса инструментами Cadence Virtuoso[11] выполненное методом Монте-Карло, показало, что применение в блоке генерации *n*-MOS-транзистора с высоким пороговым напряжением (NHVT[12]) приводит к тому, что изменение температуры оказывает наименьшее влияние на частоту генерации. В этом случае изменение частоты кольцевого генератора в диапазоне рабочих температур от 50 до 200 °C составляет 7.83%, что меньше, чем 14.35% у классического RO-PUF. Параллельно реализуются несколько кольцевых генераторов, измерение частоты путем подсчета фронтов нарастания остается тем же, но при запросе ФНФ выбирается произвольная пара генераторов, а ответ формируется как логическая функция результата сравнения двух полученных значений счетчиков (рис. 3).

В работах [28, 29] также продемонстрирована успешная реализация RO-PUF в FPGA: эксперименты



n = 3 (нечетное) для обеих цепей, четное в сумме

Рис. 4. Кольцевой генератор с переходным эффектом [30]

проводились на 15 программируемых логических интегральных схемах (ПЛИС) с 1024 контурами, получены значения μ_{inter} = 46.15% и μ_{intra} = 0.48%. Авторы применили методику устранения состояний метастабильности, которая учитывает только наиболее стабильный бит отклика из 8 пар циклов генераторов. Источником вариации является случайная разность в задержке распространения сигнала по номинально идентичным путям. Авторы [29] предложили архитектуру Pseudo-LFSR PUF[13], в которой структура LFSR реализована как замкнутая цепочка инверторов и XOR-элементов, формирующая единый контур, позволяющий надежно извлекать уникальные для каждого кристалла вариации задержек распространения сигнала.

В ФНФ на основе кольцевого генератора с переходным эффектом (transient effect ring oscillator physical unclonable function, TERO-PUF) анализируется изменение частоты и длительности сигнала в сигнальной линии и компонентах логических элементов в зависимости от типа их изготовления [30]. Кольцевой генератор с переходным эффектом состоит из двух последовательно соединенных бистабильных кольцевых генераторных цепей, как показано на рис. 4.

Кольцевой генератор с переходным эффектом формируется с четным числом инверторов, поэтому выходной сигнал ячейки переходит в стабильное состояние (аналогично бистабильному кольцу или ячейке памяти bus keeper), но не раньше, чем стабилизируются некоторые временные (переходные) колебания цепи. Подсчитывается количество колебаний, которые происходят в каждой ячейке TERO перед переходом в устойчивое состояние, при этом значения для нескольких ячеек объединяются для формирования характерного отклика для TERO-PUF. Здесь запрос заключается в номере или местоположении ячейки TERO (если существует несколько таких ячеек), а ответной реакцией являются временные колебания, возникающие при остановке системы.

[8] Fully depleted silicon-on-insulator – полностью обедненный кремний на изоляторе.

[9] Synopsis Electronic Design Automation Solutions. https://www.synopsys.com/silicon-design.html. Дата обращения 19.07.2025. / Accessed July 19, 2025.

[10] Metal-oxide-semiconductor field-effect transistor – полевой транзистор с изолированным затвором.

[11] https://cadence-ds.ru/virtuoso/. Дата обращения 19.07.2025. / Accessed July 19, 2025.

[12] *N*-type high voltage transistor – транзистор *n*-типа с повышенным пороговым напряжением.

[13] Pseudo-feedback linear shift register PUF – ФНФ на основе псевдо-регистра сдвига с линейной обратной связью.

Ячейки TERO должны быть спроектированы и реализованы с симметричной структурой, которая требует специального выбора используемых элементов управления и задержек всех соединений. Внедрение таких компонентов в ПЛИС является специфической задачей, поскольку структура ПЛИС не позволяет разработчикам автоматически выбирать соединения между элементами. Задавая ограничения вручную и используя специфические особенности целевого семейства ПЛИС, можно добиться требуемой симметрии. В работе [30] описывается конструкция TERO-PUF для двух различных технологий FPGA (45-нм Xilinx Spartan 6[14] и 28-нм Altera Cyclone V[15]). Статистическая обработка TERO-PUF с помощью двух целевых ПЛИС привела к тому, что уникальность Spartan 6 составила 48.46%, а Cyclone V – 47.62%. Результат по устойчивости составляет 2.63% при использовании Spartan 6 и 1.8% при использовании Cyclone V. Эти результаты близки к результатам, полученным в нескольких работах, где используется кольцевой генератор RO-PUF, который считается лучшим кандидатом для реализации PUF на ПЛИС. Отмечается, что TERO-PUF менее чувствителен к атакам на основе измерений побочных каналов, чем RO-PUF. Кроме того, в отличие от RO-PUF, TERO-PUF способен генерировать несколько битов для каждого запроса (от одного до трех). Авторы показали, что TERO-PUF обеспечивает от 0.85 до 1 бита энтропии на бит ответа. Эта работа демонстрирует, что TERO-PUF является перспективной альтернативой RO-PUF для реализации PUF на ПЛИС.

ФНФ с бистабильным кольцевым генератором (bistable ring physical unclonable function, BR-PUF) [22] имеет конструкцию, аналогичную кольцевому генератору PUF, но сохраняет стабильное состояние в течение определенного времени. Подобно ФНФ на основе кольцевого генератора, устройство состоит из цепочки вентилей NOT (или инвертора), однако в этой реализации имеется четное число вентилей, образующих бистабильную систему вместо колебательной (рис. 5).

При перезагрузке такая система через определенное время переходит в одно из стабильных состояний, определяемых уникальными технологическими вариациями при изготовлении кольца. Кольцо может иметь множество различных конфигураций, каждая из которых независимо стремится к предпочтительному состоянию. Это предпочтительное

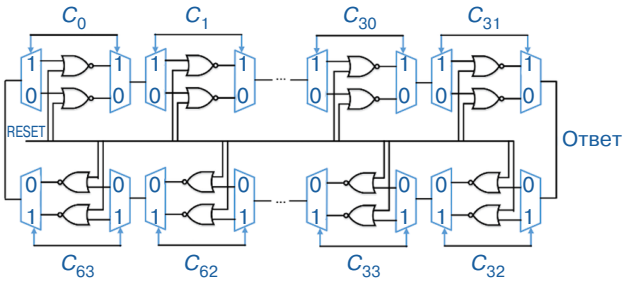


Рис. 5. Бистабильная кольцевая ФНФ.
C_0, C_1, C_{30}, C_{31}, C_{63}, C_{62}, C_{33}, C_{32} – запросы (challenges)

состояние действует как ответ, а конфигурация или бистабильное кольцо, в частности, определяется запросом (в данном случае – сигналом сброса) ФНФ.

Как впервые показано в оригинальной работе [22], где была предложена архитектура BR-PUF, число топологически различных колец составляет 2^n, что позволяет отнести данный примитив к классу «сильных» ФНФ, при этом естественный разброс технологических параметров обеспечивает хорошую межкристальную уникальность и широкий распределенный спектр времен сходимости кольца. В экспериментах на ПЛИС BR-PUF демонстрирует близкую к идеалу уникальность (~50%) и надежность порядка 97%, при этом длительные «хвосты» распределения времени стабилизации позволяют отбраковывать медленные либо нестабильные CRP, что повышает повторяемость. В то же время обнаружено, что одиночное кольцо поддается машинному моделированию: линейный алгоритм, обученный на миллионе пар «запрос – ответ», предсказывает ответы 64-, 128- и 256-стадийных экземпляров с ошибкой меньше 5%. Повысить устойчивость удается простым параллельным XOR-объединением более 4 независимых колец [31].

Дальнейшее усиление этой архитектуры предложено в гибридной схеме Chaotic-BR-PUF: выход базового BR-кольца подвергается обфускации через нелинейное логистическое отображение, за счет чего эффективность атак падает до уровня случайного угадывания (50–60%) при сравнимых ресурсах ПЛИС [32].

Актуальной тенденцией является переход к многозначной логике: тернарная BR-PUF на CNTFET[16]-транзисторах формирует троичные ответы, экспоненциально расширяя пространство CRP и повышая энтропию без существенного роста аппаратных затрат. Моделирование на 32-нм библиотеке стандартных элементов показало улучшение непредсказуемости и стойкости к атакам на основе

[14] Spartan 6 FPGAs. https://www.amd.com/en/products/adaptive-socs-and-fpgas/fpga/spartan-6.html. Дата обращения 19.07.2025. / Accessed July 19, 2025.

[15] Cyclone V FPGA and SoC FPGA. https://www.altera.com/products/fpga/cyclone/v. Дата обращения 19.07.2025. / Accessed July 19, 2025.

[16] Carbon nanotube field-effect transistor – транзистор на основе углеродных нанотрубок.

машинного обучения по сравнению с бинарным прототипом, а высокая температурная устойчивость CNTFET делает такой подход перспективным для IoT[17]-устройств [33].

ФНФ типа «арбитр» (A-PUF[18])

Принцип работы ФНФ этого типа основан на сравнении времен прохождения двух сигналов, распространяющихся по теоретически симметричным траекториям. Модуль A-PUF состоит из нескольких ячеек, соединяющих источник сигнала с компонентом-арбитром (рис. 6).

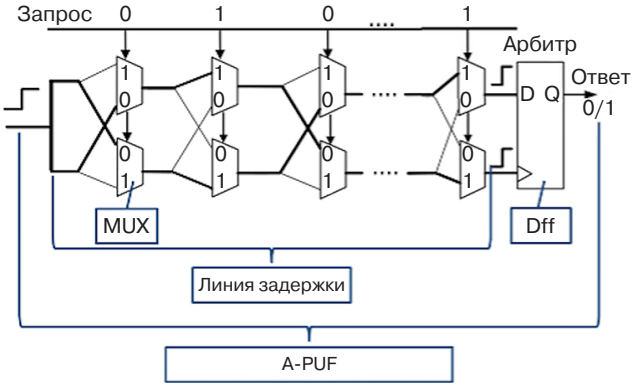


Рис. 6. Пример реализации ФНФ типа «арбитр». D – вход; Q – выход; Dff – D-триггер

Каждая ячейка имеет переключатель, который может направлять оба сигнала через другие сигнальные линии. Компонент-арбитр выдает двоичный выходной сигнал, значение которого зависит от того, какой из двух входных сигналов, отделенных от источника сигнала, достигает компонента первым. Из-за случайных изменений в проводнике и переключающих элементах, по которым проходит сигнал, скорость обоих сигналов будет варьироваться относительно друг друга. Таким образом запрос строится на основе характера включения/выключения маршрутизирующих коммутаторов (и кратности номера/положения арбитра в этих системах), а ответ формируется в зависимости от более быстрого пути после этого переключения.

Важно отметить, что в случае нарушения времени установки/удержания (setup/hold) возможна нежелательная ситуация метастабильности в арбитре и результат его работы не будет зависеть от результата сравнения времен прохождения сигналов, а будет определяться случайным шумом в откликах (см., например, [8]).

Преимуществом ФНФ этого типа является простота реализации и малая занимаемая площадь: одна n-ступенчатая A-PUF – это $2n$ мультиплексоров и один триггер-арбитр. При $n = 64$ схема занимает считанные сотни вентилей. Соответствующее устройство легко масштабируется на кремнии, т.к. разброс задержек, достаточный для генерации случайных различий, сохраняется с уменьшением норм техпроцесса. Практические реализации A-PUF демонстрируют уникальность, близкую к теоретически оптимальному значению 50%, особенно – при усложненных вариантах конструкции. Анализ публикаций, посвященных A-PUF, показывает множество вариаций их исполнения. В обзоре [3] кроме основной структуры A-PUF даны краткие описания модификаций этой архитектуры, в частности, двухканальных и многоканальных с элементами XOR, схем на основе мультиплексоров, комбинаций с RO-PUF и других. Уязвимость обычных функций A-PUF к атакам на основе моделирования на основе машинного обучения значительно ограничивает их применимость в безопасных средах с ограниченными ресурсами.

Архитектура ФНФ типа «арбитр» с улучшенными характеристиками представлена в работах [34–37]. Один из примеров реализации, в котором несколько независимых модулей объединяются функцией XOR для формирования единого ответа, приведен на рис. 7 [28].

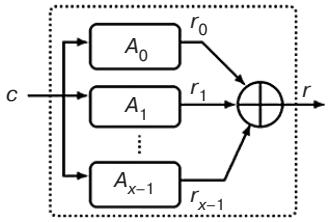


Рис. 7. Модификация A-PUF с объединением ответов функцией XOR. c – запрос; A_0, ..., A_{x-1} – экземпляры A-PUF; r_0, ..., r_{x-1} – ответы экземпляров A-PUF; r – ответ XOR A-PUF

В другой архитектуре[19] модуль на основе оперативной памяти (FF-MB-A-PUF[20]) объединяет слабые модули ФНФ на основе энергозависимой памяти с нелинейной логикой обратной связи для повышения энтропии и усиления устойчивости к атакам моделирования. Для оценки предложенного решения разработана комплексная экспериментальная

[17] Internet of things – интернет вещей.
[18] Arbiter PUF.

[19] Mishra A. *Enhancing the security scalability of Arbiter PUFs using memory-based weak PUFs*. Thesis. West Lafayette (IN): Purdue University; 2025. https://hammer.purdue.edu/articles/thesis/enhancing_the_security_scalability_of_arbiter_pufs_using_memory-based_weak_pufs/28899152. Дата обращения 19.07.2025. / Accessed July 19, 2025.
[20] Memory-based feed-forward arbiter PUF – ФНФ типа «арбитр» с опережающей связью на основе памяти.

система, использующая до 50 млн пар «запрос – ответ» (CRP). Результаты экспериментов показали, что как количество, так и точное расположение контуров обратной связи критически влияют на устойчивость моделирования. Для сопоставления полученных результатов с аналогичными реализациями в этой работе были внедрены и настроены самые современные стратегии моделирования, включая глубокие нейронные сети (deep neural networks, DNNs) и стратегию эволюции адаптации ковариационной матрицы. Оптимизированная конфигурация FF-MB-A-PUF, включающая 63 цикла обратной связи, продемонстрировала высокую устойчивость к атакам на основе моделирования, повышенную случайность (49.23%) и улучшенную уникальность между устройствами (49.20%), что привело к сбалансированному распределению выходных данных и высокой энтропии. Эти результаты позволяют считать FF-MB-A-PUF масштабируемым, аппаратно-эффективным и безопасным примитивом, идеально подходящим для встраиваемых систем нового поколения и маломощных IoT-систем.

В работе [37] описаны типовые методы стабилизации A-PUF от шума, старения, колебаний напряжения и температуры, в частности, усреднение и маскировка нестабильных битов.

ФНФ на основе задержек тактовых сигналов (Clock PUF)

ФНФ на основе задержек тактовых сигналов Clock PUF [38] в синхронных схемах анализирует изменение скорости распространения сигнала от тактового генератора к различным участкам самой схемы, основываясь на различиях в изготовлении при его физической реализации. В современных проектах ИС эти эффекты расфазировки являются паразитными, и их стремятся устранить, однако вариации и искажения все равно возникают. В этом варианте ФНФ сравниваются различия в задержках парных сигналов в предположительно схожих схемах, чтобы однозначно охарактеризовать схему, аналогично A-PUF. Здесь запросом являются линии тактового сигнала, а ответом – задержка в каждой соответствующей линии.

В работе [39] предлагается симметричный облегченный вариант ФНФ на основе трехфазного D-триггера с повышенной уникальностью, реализованный в ИС с использованием стандартной 40-нм КМОП[21]-технологии. Результаты моделирования после компоновки кристалла предсказывают, что уникальность устройства составляет 0.4994, что является самым высоким показателем среди всех рассмотренных архитектур. По сравнению с A-PUF устройство имеет на 73.3% меньшую потребляемую мощность, занимает на 93.6% меньшую площадь и потребляет на 95.7% меньше энергии на один бит. Аналогичные показатели при сравнении с RO-PUF составляют 98.3%, 96.9% и 99.9% соответственно. Кроме того, в отличие от других ФНФ на основе триггеров, предлагаемый вариант не требует блока постобработки для устранения напряжения смещения, что способствует экономии общей площади реализации и мощности системы. Для доказательства этой концепции выполнена реализация этого устройства на ПЛИС, а для сравнения производительности между рассмотренными архитектурами предложен новый коэффициент качества (figure of merit, FOM), учитывающий мощность, надежность, задержку, площадь кремния и уникальность. Отмечено, что предлагаемая архитектура обеспечивает самый высокий показатель FOM среди рассмотренных архитектур ФНФ.

В исследовании [38] представлены новые технологии ФНФ, которые извлекают биты из попарных искажений между доменами тактовой сети ИС. Реализован алгоритм, который выбирает равноудаленные приемники и маршрутизирует обратную сеть, затем извлекает случайные биты для конкретного чипа. Оценка тактовых импульсов на основе SPICE[22]-моделирования 45-нм КМОП-технологии подтверждает работоспособность, стабильность, уникальность, случайность и низкие накладные расходы данной реализации.

Вариант, основанный на анализе расфазировки тактового сигнала, рассмотрен также в работе [40]. Предлагается программный вариант ФНФ (S-PUF[23]), которая вызывает ненормальную работу схемы кодирования видео, с применением тактового сигнала. Ключ отклика с характеристиками схемы генерируется путем использования зависимости отклика от пути синхронизации. В качестве несущей схемы ФНФ используется схема кодирования видео, которая является частью IP-ядра[24] микросхемы кодирования видео с открытым исходным кодом. На основе анализа временного тракта схемы кодирования выбирается сигнал запуска, переводящий схему в ненормальный режим работы. Генерируются случайные данные, которые подвергаются операциям кодирования

[21] Комплементарная структура металл-оксид-полупроводник.

[22] Simulation program with integrated circuit emphasis – симулятор электронных схем общего назначения с открытым исходным кодом. [Simulation program with IC emphasis is an open-source simulator of general-purpose electronic circuits.]

[23] Software PUF – программная ФНФ.

[24] IP-ядра (intellectual property) – готовые блоки для проектирования микросхем. [IP cores (intellectual property) are ready-made blocks for designing microchips.]

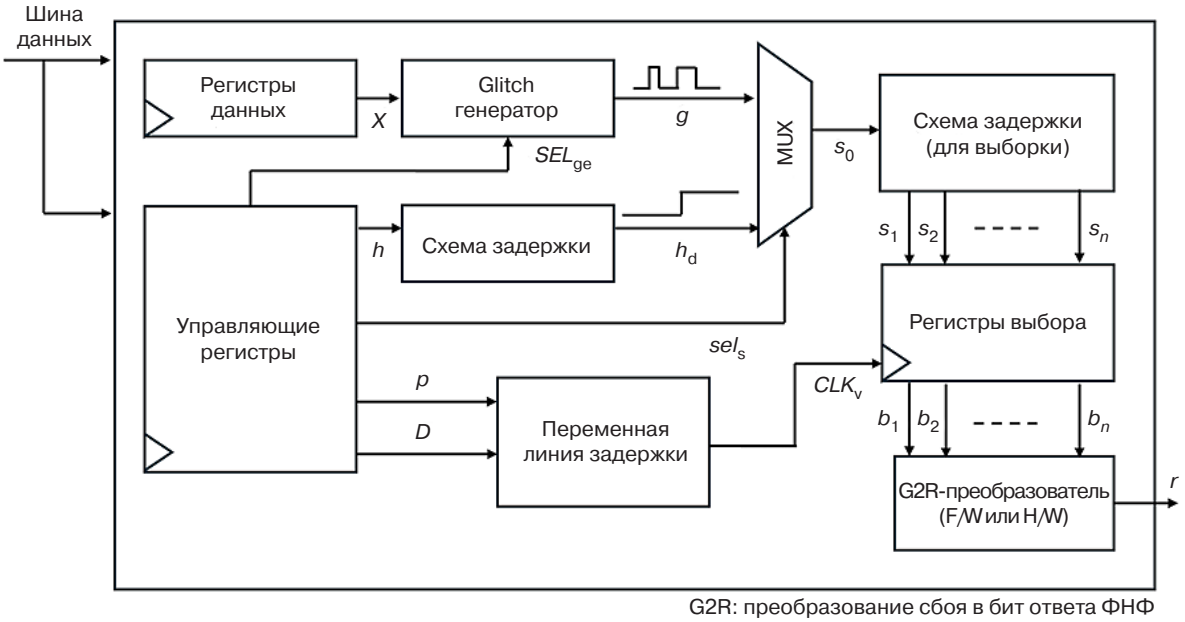


Рис. 8. Пример устройства с Glitch PUF [41].
X – входные данные, подаваемые на Glitch-генератор; SEL_{ge} – сигнал выбора выхода Glitch-генератора; g – выбранный выходной бит Glitch-генератора; s_0 – исходный Glitch-сигнал; s_1, ..., s_n – сигналы после схемы задержки (точки выборки); h – калибровочный импульс; h_d – калибровочный импульс после схемы задержки; sel_s – входной сигнал выбора; p – триггерный сигнал; D – код управления временной задержкой; CLK_v – тактовый сигнал после переменной задержки; b_1, ..., b_n – значения, считанные регистрами выбора и представляющие форму сбоев; G2R – Glitch-to-Response (устройство преобразования сбоя в ответ); F/W – firmware (прошивка); H/W – hardware (аппаратура); r – response (ответ)

и сжатия видео, которые затем маскируются с помощью кода Грея и операции исключения ложных битов. Результаты тестирования показывают, что предложенный вариант S-PUF проходит тест NIST с уникальностью 48.87% при коэффициенте автокорреляции этой реализации 0.0204 при 95%-й достоверности.

ФНФ на основе переходных процессов (Glitch PUF)

ФНФ на основе переходных процессов – это более сложные схемы, чем RO-PUF и A-PUF; они анализируют переходные характеристики сигналов, приводящие к сбоям работы устройства. Запросом для этой концепции ФНФ является сама схема, а ответом – конкретная реализация возникающих сбоев и эволюция их во времени (см. пример на рис. 8 [41, 42]).

В архитектуре Glitch PUF, описанной в [41], для формирования ФНФ используются сбои, которые возникают из-за изменения задержки между затворами транзисторов в схеме, влияющие на характеристики распространения импульса от каждого затвора. Описана процедура моделирования простой реализации такой схемы на этапе проектирования, результаты которой хорошо совпадают с данными, полученными при аппаратной реализации такой ФНФ в реальных микросхемах.

В [43] отмечается, что при аппаратной реализации Glitch PUF характерной проблемой является восприимчивость к шумам. Для снижения влияния шума предлагается модуль управления сбоями, который использует многоуровневую параллельную архитектуру для генерации многоразрядной стабильной информационной энтропии. Разработана схема шумоподавления, которая фильтрует шум, используя эффект гистерезиса и механизм обратной связи с триггерами Шмитта и схема широтно-импульсного детектирования для извлечения выходных данных сигналов сбоев при переходных процессах. В 65-нм КМОП-технологии TSMC[25] реализована 128-битная схема такой Glitch PUF. Результаты экспериментов показывают, что случайность (intra-distance = 0.01) составляет 99.9%, а уникальность (inter-distance) – 50.03%, что означает, что предложенная конструкция может широко использоваться для обеспечения безопасности устройств интернета вещей.

В [44] указано, что производительность таких ФНФ незначительно колеблется из-за изменений окружающей среды, и для устранения этих колебаний требуются методы исправления ошибок и предлагается один из вариантов такого метода.

[25] Taiwan Semiconductor Manufacturing Company – производитель интегральных схем и полупроводниковых пластин. [The Taiwan Semiconductor Manufacturing Company (TSMC) is a manufacturer of ICs and semiconductor wafers.]

Для количественной демонстрации эффективности предложенного метода проводятся оценочные эксперименты с использованием FPGA.

РЕАЛИЗАЦИЯ ФНФ НА ОСНОВЕ ПАМЯТИ SRAM[26]

ФНФ на основе статической памяти SRAM

Реализация ФНФ на основе статической памяти SRAM [45, 46] основана на том, что случайное распределение состояний ячеек памяти 6T (рис. 9), определяющее их поведение при включении, непосредственно связано с условиями производства и допусками на технологически режимы их формирования. Случайное стартовое состояние ячеек SRAM служит «отпечатком» кристалла и может выступать либо непосредственно как ключ, либо как основа для генерации ответов на запросы. Таким образом, относительно стандартного массива SRAM она требует лишь контролируемого сброса/включения питания памяти или спецрежима и не вносит дополнительных энергозатрат в режиме покоя.

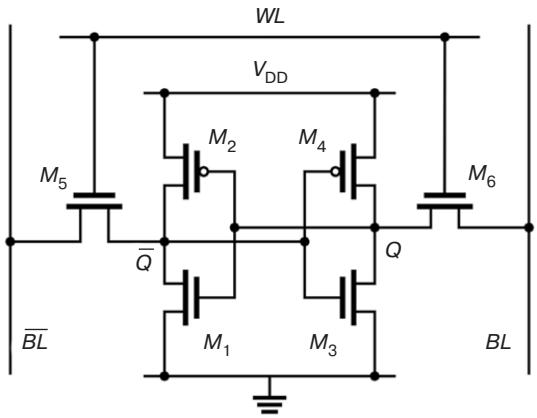


Рис. 9. Ячейка 6T SRAM.
WL – word line (управляет двумя транзисторами доступа); V_{DD} – питание; $M_1, \ldots, M_6$ – MOS-транзисторы; $Q, \overline{Q}$ – комплементарные узлы хранения данных; $BL, \overline{BL}$ – bit line (комплементарные битовые линии, используемые для записи и чтения данных)

Исследования показывают, что SRAM-PUF могут обеспечивать близкую к идеальному значению уникальность. Надежность же ограничена влиянием шумов и условий среды: без коррекции она составляет ~88–90% [16]. Для повышения надежности выхода применяют схемы усреднения (многократное считывание при включении) и алгоритмы исправления ошибок (например, код Рида – Соломона или нечеткий экстрактор) [17].

SRAM-PUF успешно поддается масштабированию: реализации на техпроцессах вплоть до 7-нм показывают сохранение работоспособности [18, 47], хотя уменьшение размера транзисторов снижает абсолютные величины рассогласований, потенциально требуя более продвинутой обработки бит (например, отбраковки нестабильных ячеек) для поддержания надежности. Данные экспериментов с ФНФ на основе SRAM, основанные на изучении включения 8190 байт SRAM из разных блоков памяти на разных ПЛИС, показали, что среднее различие между двумя разными блоками составляет $\mu_{inter} = 49.97\%$, а среднее различие между несколькими измерениями в одном блоке составляет $\mu_{intra} = 3.57\%$ для фиксированных условий окружающей среды. Однако μ_{intra} увеличивается до 12% для больших отклонений температуры. Авторы оценивают энтропийное содержание состояний включения SRAM как 0.76 бит на ячейку SRAM.

Аналогичные результаты приведены в [46, 48], в которых изучено поведение SRAM при включении на двух разных платформах. Для 5120 блоков по 64 ячейки SRAM, измеренных на 8 коммерческих микросхемах SRAM, получено значение $\mu_{inter} = 43.16\%$ и $\mu_{intra} = 3.8\%$, а для 15 блоков по 64 ячейки SRAM из встроенной памяти на 3 микросхемах микроконтроллера авторы получили значение $\mu_{inter} = 49.34\%$ и $\mu_{intra} = 6.5\%$ соответственно.

Недостатком подобной реализации ФНФ на ПЛИС является то обстоятельство, что в наиболее распространенных ПЛИС все ячейки SRAM принудительно сбрасываются в ноль непосредственно после включения питания и, следовательно, теряется всякая случайность. Для устранения этого в ФНФ предложены схемы типа «бабочки» и схемы с защелками. Схема типа «бабочка» (butterfly), предложенная в [49], структурно состоит из двух перекрестно-связанных защелок (latch) с тактовым сигналом, установленным в единицу для симуляции комбинационного бистабильного элемента (рис. 10).

Сигнал excite устанавливает на выходах обоих элементов различные уровни сигнала (0/1), переводя ячейку в метастабильное состояние. При снятии сигнала схема переходит в стабильное случайное состояние, конкретное значение которого также определяется физическими причинами реализации триггеров и перекрестной связью, формируя бит ответа. Результаты измерений, приведенные в работе [50], получены на 64 схемах с ФНФ типа «бабочка» на 36 ПЛИС. Получены значения $\mu_{inter} = 50\%$ и $\mu_{intra} < 5\%$ при больших колебаниях температуры. Аналогично другим ФНФ, при использовании данного вида ФНФ применяются методы коррекции ошибок.

[26] Static random access memory – статическая память с произвольным доступом.

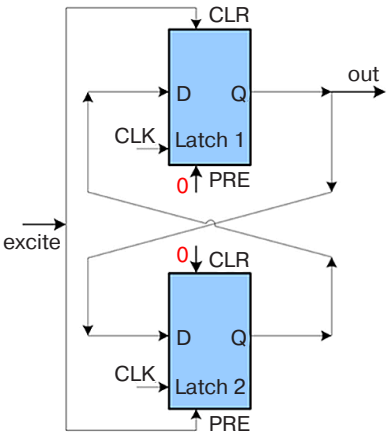


Рис. 10. ФНФ типа «бабочка» [49].
Latch 1/2 – защелка; excite – сигнал инициализации;
CLR (clear) – вход асинхронного сброса защелки;
PRE (preset) – вход асинхронной установки защелки;
CLK (clock) – вход тактового сигнала;
D – вход данных защелки; Q – выход защелки;
out – выход схемы

Другой вариант идентификации ИС предложен в работе [51]. Вместо перекрестного соединения двух инверторов или двух триггеров-защелок перекрестно соединены два NOR-вентиля, образуя NOR-триггер. При подаче сигнала сброса этот триггер переходит в нестабильное состояние и возвращается в то или иное стабильное состояние в зависимости от внутреннего несоответствия между электронными компонентами. Эксперименты с 128 NOR-триггерами были проведены на 19 сверхбольших интегральных схемах, изготовленных при КМОП-технологии с топологическими нормами 0.130 мкм, получены значения μ_{inter} = 50.55% и μ_{intra} = 3.04%.

ФНФ на основе динамической памяти DRAM[27]

Другим видом ФНФ на основе энергозависимой памяти является DRAM-PUF, которая присутствует практически во всех современных вычислительных устройствах, включая ресурсно-ограниченные встраиваемые системы и IoT-платформы, что делает ее привлекательной основой для встроенных аппаратных примитивов безопасности. Большой объем ячеек обеспечивает значительный пул энтропии и потенциально широкое пространство пар «запрос – ответ», а доступ к DRAM возможен как на этапе загрузки, так и во время работы системы. Такие свойства особенно важны там, где невозможно или дорого применять классические отдельные защитные модули. Кроме того, по сравнению с SRAM, DRAM обычно потребляет меньше энергии при сопоставимой емкости.

Типичная ячейка на основе 1T1C[28] DRAM представляет собой комбинацию «транзистор – конденсатор» (рис. 11) и требует периодического регенерирования (refresh) из-за утечки заряда[29].

Вариации емкости, токов утечки и пороговых напряжений, возникающие при производстве, создают отличия между ячейками, которые можно использовать как уникальную сигнатуру. Утечки могут происходить как в пределах строки, так и в соседние строки/линии. Активное воздействие соседних строк друг на друга усиливает перетекание заряда

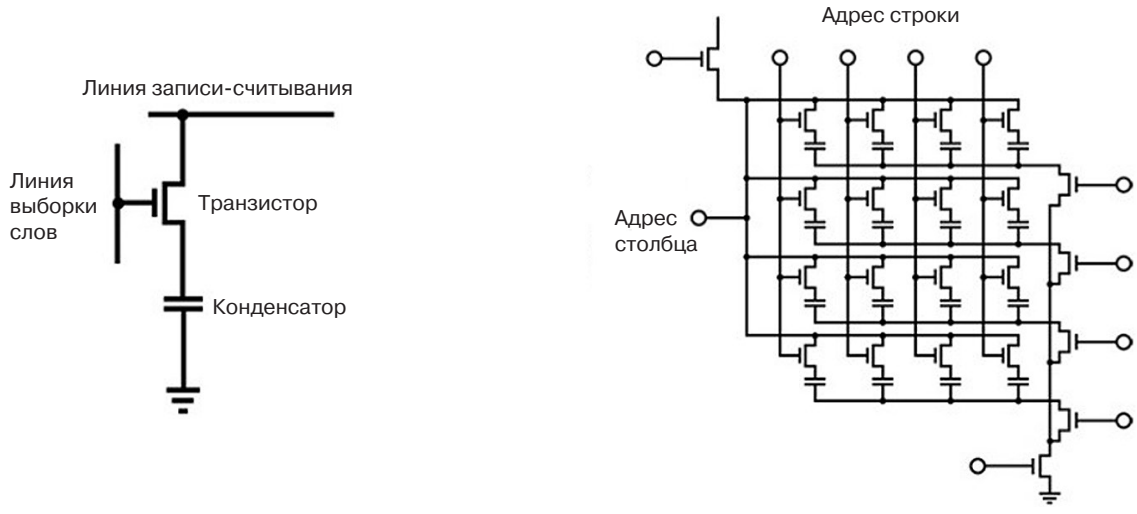


Рис. 11. Память DRAM и ячейка 1T1C

[27] Dynamic random access memory – динамическая память с произвольным доступом.
[28] One-transistor, one-capacitor – ячейка оперативной памяти, состоящая из одного полевого транзистора и одного конденсатора. [One-transistor, one-capacitor is a RAM cell consisting of one field-effect transistor and one capacitor.]
[29] DRAM Scaling Challenges Grow. https://semiengineering.com/dram-scaling-challenges-grow/. Дата обращения 19.07.2025. / Accessed July 19, 2025.

и приводит к битовым инверсиям, повышающим энтропию. Также наблюдается явление переменного времени удержания (variable retention time, VRT): одна и та же ячейка может непредсказуемо переключаться между состояниями с высокой и низкой удерживающей способностью. Наконец, укороченные задержки операций чтения/записи (например, tRCD[30], tRP[31]) приводят к тому, что часть ячеек не успевает корректно установиться, формируя характерный паттерн ошибок. Эти механизмы различной стабильности позволяют строить как воспроизводимые ФНФ (при отбраковке нестабильных битов и/или коррекции ошибок), так и высокоэнтропийные генераторы случайных чисел (TRNG) при работе в режимах, где результат максимально нестабилен.

Исследования DRAM-PUF традиционно группируют по используемому физическому эффекту: стартовые значения при включении питания, распад (retention/decay) при остановке refresh или отключении питания (Start-Up DRAM-PUF, Retention based DRAM-PUF), и нарушения таймингов (Latency-Based DRAM-PUF). Также изучаются более специфические эффекты, например, Rowhammer-PUF и комбинированные решения.

Работа Start-Up DRAM-PUF базируется на начальном распределении зарядов ячеек после подачи питания. В [52] исследовали устойчивость такой ФНФ к температуре (0–80 °C), питанию (4.5–5.5 В) и ускоренному старению, формируя 2048-битные ответы (16 × 128-битных ключей) и повышая надежность за счет алгоритма выбора ячеек с устойчивыми соседями. Последующий анализ показал, что понижение температуры и снижение напряжения питания сильнее ухудшают стабильность, чем повышение; эффект старения (negative bias temperature instability, NBTI) оказался умеренным.

Другие аналогичные работы использовали весь массив DRAM как «изображение» (преобразование в градации серого) с последующим извлечением признаков искусственной нейронной сетью для идентификации; достигнута точность классификации порядка ~98.8%, хотя классические метрики устойчивости ФНФ подробно не оценивались [53]. Также обсуждалась попытка улучшать случайность постобработкой LFSR (linear-feedback shift register).

Retention based DRAM-PUF использует вариации времени удержания заряда при отключении авто-refresh (или питания) и чтения массива через заданный интервал. Получаемый паттерн битовых инверсий уникален для сегмента памяти. В работе [54] показано, что время ожидания ФНФ можно сократить до 20–60 с, если ответ формируется как карта местоположений битовых инверсий. Была показана уникальность не только на уровне микросхемы, но и между блоками памяти внутри одного DRAM-модуля. Надежность сохранялась при изменении температуры в пределах ±10 °C (20–40 °C); также изучено влияние старения (85 °C, 48 ч).

В Latency-Based DRAM-PUF энтропия извлекается из различий в скоростях доступа к ячейкам. Для реализации ФНФ контроллер намеренно занижает тайминги (tRCD, tRP и т.д.), и отдельные ячейки начинают давать ошибки чтения/записи в характерных позициях. Такая архитектура сильно ускоряет работу ФНФ: сообщалось о времени порядка ~0.875 мс, что более чем в 10000 раз быстрее типичных retention DRAM PUF (около 10 с). Пример реализации [54] использует варьирование tRP/tRCD, запись известного шаблона, чтение с нарушенными таймингами и построение «энтропийных карт». После этого XNOR-фильтрация применяется для удаления нестабильных бит.

Эффект Rowhammer – намеренное многократное чередование обращений к тем строкам DRAM, к которым процессор намеренно обращается множество раз **в** очень коротком промежутке времени, вызывающее ускоренную утечку заряда в соседних строках и детерминированные битовые инверсии. В работе [28] этот феномен впервые применен для реализации ФНФ. Суть метода Rowhammer-PUF состоит в том, что из массива DRAM выделяются две ФНФ-строки памяти, которые заранее заполняют противоположными шаблонами: 0x55 и 0xAA. В определенный момент происходит отключение обновления (refresh) этих строк, которые начинают быстро разряжаться под действием активно работающих (активация + предзарядка) двух соседних Rowhammer-строк, формируя уникальный шаблон.

Комбинированные решения (например, объединение SRAM-PUF и DRAM-PUF) позволяют свести преимущества разных видов памяти и частично компенсировать недостатки каждой: показаны реализации с высокой энтропией, большим числом CRP и устойчивой аутентификацией в широком температурном диапазоне (20–60 °C).

Сравнение типов DRAM-PUF показывает, что в большинстве работ достигается значение inter-HD, близкое к идеальным 50%, тогда как надежность варьируется в зависимости от класса. Retention based DRAM-PUF оказываются более чувствительны к температуре/напряжению, Latency Based DRAM-PUF обычно более воспроизводимы при правильно выбранных порогах таймингов, Start-Up DRAM-PUF занимает промежуточное положение и требует алгоритмов выбора стабильных ячеек [55].

[30] Time row address to column address delay – задержка активации строки. [Time row address to column address delay is row activation delay.]

[31] Row precharge time – время обновления строки. [Row precharge time is row refresh time.]

Большой объем DRAM потенциально обеспечивает широкое пространство CRP, однако на практике число пригодных стабильных бит резко сокращается после фильтрации по надежности и случайности, поэтому большинство DRAM-PUF в прикладных системах относят к «слабым» ФНФ (ограниченное число устойчивых CRP), подходящим прежде всего для генерации ключей и эпизодической аутентификации.

ФНФ на основе энергонезависимой памяти

ФНФ на основе энергонезависимой памяти (non-volatile memory, NVM) также используют случайные вариации характеристик ячеек памяти для формирования уникальных «отпечатков» микросхем. Ключевыми физическими эффектами, определяющими уникальность и стабильность ФНФ, построенных на энергонезависимой памяти, являются вариации материалов и токов утечки, а также стохастические процессы переключения.

В ReRAM-PUF[32] [56] источником случайности служит стохастический процесс образования проводящих участков в диэлектрике: пороги переключения и сопротивление high/low состояния слегка разнятся от ячейки к ячейке из-за технологических допусков. В других вариантах ReRAM-PUF измеряется разброс сопротивлений в заранее сформированном массиве без его перезаписи [57].

Аналогично, в MRAM[33] уникальные различия обусловлены вариациями сопротивления магнитных туннельных переходов (magnetic tunnel junction, MTJ), возникающими при производстве [58]. В MRAM на вариативность влияет толщина барьера и магнитная анизотропия MTJ: малые разбросы вызывают различие сопротивлений ячеек в одном состоянии. Эти вариации, обусловленные технологией, очень стабильны во времени, что улучшает воспроизводимость ответа.

В PCM (phase-change memory, память на изменении фазы) за основу берутся различия в состояниях материала: при заводском изготовлении или после переключения в аморфное состояние каждая ячейка имеет слегка разный уровень проводимости из-за флуктуаций структуры, что позволяет считывать это состояние памяти как случайный шаблон [59]. Для достаточной воспроизводимости необходимо учитывать явление дрейфа сопротивления аморфного состояния со временем. В исследованиях показано, что грамотный выбор режима считывания (например, дифференциального) и калибровка позволяют минимизировать влияние дрейфа и получать стабильные биты [60].

Физические эффекты, создающие случайность – случайное зарождение проводящих каналов, вариации туннельного сопротивления, разброс фазового состояния обеспечивают высокую энтропию, а инженерные решения стремятся сгладить нестабильность этих эффектов для воспроизводимости. Таким образом, ReRAM-, MRAM- и PCM-PUF формируют бит ответа либо непосредственным считыванием неконтролируемого начального состояния ячеек, либо путем специального режима чтения/записи, выделяющего разброс характеристик ячеек. За последние годы предложено множество архитектур ФНФ на этих типах энергонезависимой памяти, нацеленных на улучшение их характеристик. Базовая схема – «слабая» ФНФ на основе массива памяти, когда ответы формируются из состояния большого числа ячеек (например, считывается N-битный стартовый вектор из неинициализированной памяти). Такой подход прост и экономичен, но дает ограниченное число пар «запрос – ответ» (фиксированный отпечаток) [61].

Для расширения пространства «запрос – ответ» применяют модифицированные архитектуры, переводящие их в класс «сильных» ФНФ: например, в ReRAM реализованы 2T2R- и 1T4R-ячейки с возможностью задавать разные пути чтения и сравнения сопротивлений, формируя экспоненциально большое число возможных ответов [59]. В одном из подходов, также предложенных в этой работе, массив ReRAM работает в режиме вычисления «in-memory», когда сочетание нескольких ячеек (через XOR или считывание по специальному шаблону) создает выход, нечувствительный к моделированию и устойчивый к атакам на основе машинного обучения.

С точки зрения схемотехники внимание также уделяется подавлению побочных каналов. В частности, симметричные структуры (например, зеркально переключаемые дифференциальные пары ячеек) устраняют систематический перекос и усложняют предсказание ответа атакующим [57]. Современные реализации включают также режим самоуничтожения: в ReRAM-PUF можно предусмотреть подачу повышенного напряжения, которое необратимо уничтожает часть ячеек при попытке вскрытия злоумышленником, тем самым уничтожая ключ [56].

Архитектуры энергонезависимых ФНФ охватывают спектр от компактных встроенных ячеек памяти, выдающих один зашитый ключ, до крупноразмерных перестраиваемых массивов, способных генерировать множество ответов и противостоять моделирующим атакам. ФНФ на энергонезависимой памяти способны обеспечивать показатели, близкие к идеальным. Уникальность в экспериментах с ReRAM, MRAM, PCM обычно составляет ~50%, Разница между повторными чтениями составляет менее 1–2%, а в ряде

[32] Resistive random-access memory PUF.

[33] Magnetoresistive random-access memory – магниторезистивная память с произвольным доступом.

работ заявлено ~0.01–0.1% битовых ошибок без коррекции. Например, в MRAM-PUF на основе массива MTJ получены значения inter-HD ~ 49.96% и intra-HD ~ 0.98%. Энтропия генерируемых ответов близка к максимальной: распределение 0/1 обычно около 50% (uniformity ~50%), что подтверждается прохождением статистических тестов NIST на случайность для битовых последовательностей ФНФ. В обзорах отмечается, что современные ReRAM-PUF после отбраковки нестабильных бит обеспечивают информационную насыщенность ~1 бит энтропии на ячейку или очень близкую к этому.

Надежность ФНФ на базе энергонезависимой памяти характеризуется способностью сохранять стабильный ответ при различных помехах – изменениях температуры, напряжения питания, старении компонентов. Поскольку состояние энергонезависимой памяти физически закреплено (проводящие участки в ReRAM, магнитный вектор в MRAM, фазовая структура в PCM), такие ФНФ менее чувствительны к внешним воздействиям. Так, MRAM-PUF демонстрирует стабильность от −40 до 150 °C [59]. ReRAM-PUF при температурных циклах (например, от 25 до 125 °C) показывает лишь незначительное увеличение разброса сопротивлений; экспериментально подтверждено сохранение >91% бит без ошибок при 125 °C [56]. Вопрос старения также исследован: медленная деградация оксидных проводящих участков или туннельных барьеров за время службы устройства может повысить битовую ошибку, но заложенный запас по порогу и алгоритмы коррекции позволяют обеспечить многолетнюю стабильность.

Постобработка в схемах на основе памяти может уменьшать смещение и повышать статистические показатели, но добавляет накладные расходы и потенциальные уязвимости при неверном применении [55].

СВОДНЫЕ РЕЗУЛЬТАТЫ ПО ОБОЗРЕВАЕМЫМ ФНФ

Ниже приведена сводная таблица характеристик некоторых ключевых вариантов ФНФ, рассмотренных в данной части цикла статей (таблица). Отражены работы, в которых приводятся оригинальные результаты после реализации одной или нескольких ФНФ. В качестве ключевых метрик выбраны inter-distance, intra-distance. В ряде публикаций они имеют названия уникальность (uniqueness) и надежность (reliability) соответственно.

Чувствительность к внешним условиям показывает, при каких вариациях напряжения/температуры проводились измерения характеристик и насколько они изменяются (в скобках указывается насколько изменяется intra-distance), если такие данные приводятся.

Столбец «Оценочная сложность реализации (высокая, средняя, низкая)» призван продемонстрировать относительные аппаратные затраты на реализацию того или иного вида ФНФ, а также техническую сложность (необходимость балансировки путей, подбора параметров элементов, изменения техпроцессов и т.д.).

Таблица. Сводные результаты по обозреваемым ФНФ

Тип ФНФ/работа	Год публикации	Характеристики ФНФ					
		Inter-distance	Intra-distance	Платформа	Inter-distance		Оценочная сложность реализации
					Температура	Напряжение	
RO [7]	2007	46.15%	0.48%	15 × Xilinx Virtex-4 LX25 FPGA	−20–120 °C	1.2 В ± 10%	средняя
Arbiter [7]	2007	23%	0.7%	ASIC TSMC 180-нм	20–70 °C (+4.8%), 20–120 °C (+9%)	±2% (+3.7%), ±33% (+9%)	средняя
RO [10]	2009	47.8%	~0%	SPICE model 90-нм КМОП	−15–65 °C	0.2–1.0 В (+7% при 0.5 В)	средняя
SRAM PUF (FinFET[34] 16-нм) [17]	2022	–	14%	NVIDIA Jetson, 16-нм LP FinFET	0–85 °C	–	низкая

[34] Fin field-effect transistor – транзистор с трехмерной структурой. [Fin field-effect transistor is a 3D-structured transistor.]

Таблица. Продолжение

Тип ФНФ/работа	Год публикации	Характеристики ФНФ					
		Inter-distance	Intra-distance	Платформа	Inter-distance		Оценочная сложность реализации
					Температура	Напряжение	
SRAM PUF (FinFET 14-нм) [17]	2022	–	10%	NXP LPC, 14-нм LP FinFET	0–85 °C	–	низкая
SRAM PUF (FinFET 7-нм) [17]	2022	–	11%	Xilinx Versal, 7-нм HP FinFET	0–85 °C	–	низкая
TERO [19]	2014	48.07%	1.73%	FPGA (Altera Cyclone II)	–	–	средняя
BR [22]	2011	49.8%	0.7%	FPGA (Xilinx Virtex-II Pro)	5–45 °C (+2.7%)	±10% (+2.2%)	средняя
CRO[35] [23]	2024	45.5%	9.95%	ASIC 22-нм FDSOI	−40–70 °C	0.72–0.88 В	средняя
RO [26]	2025	–	0.38%	SPICE-model 55-нм КМОП	−50–200 °C (+9.38%)	–	средняя
Rowhammer [27]	2017	–	<5%	DDR3/4 DRAM	−40–60 °C	–	низкая
XOR Arbiter [28]	2022	48.69%	0.59%	FPGA (Xilinx Artix 7)	0–85 °C	0.95–1.05 В	средняя
Pseudo-LFSR [29]	2011	65.6%	1.8%	FPGA (Xilinx Virtex 5)	–	1 В	средняя
TERO [30]	2016	47.22%	2.36%	FPGA (Xilinx Spartan 6)	−15–65 °C	1.1–1.3 В	средняя
TERO [30]	2016	48.58%	2.66%	FPGA (Altera Cyclone V)	−15–65 °C	1.05–1.15 В	средняя
XOR BR [31]	2015	14.8%	0.8%	FPGA (Xilinx Spartan 6)	27–75 °C	–	средняя
BR [32]	2021	48.0%	–	FPGA (Xilinx Artix 7)	–	–	средняя
BR [33]	2024	66.26%	1.58%	SPICE-model CNTFET 32-нм КМОП	0–100 °C	0.8–1.0 В	средняя
Eye-Opening Arbiter[36] [37]	2025	44.99%	3.49%	FPGA (Xilinx Zynq-7010)	−40–125 °C	0.81–0.99 В	средняя
Clock [38]	2013	50.11%	1.19%	SPICE-model 45-нм КМОП	–	–	средняя
Tri-state Flip-Flop[37] [39]	2020	~49%	~2%	FPGA (Altera Cyclone)	–	–	низкая
Overclocking clock software[38] [40]	2025	48.87%	–	SPICE model TSMC 65-нм КМОП	−25–125 °C	1.0–1.4 В	низкая

[35] Configurable ring oscillator PUF – конфигурируемая ФНФ на основе кольцевого осциллятора.
[36] ФНФ типа «арбитр» с фазовым окном. [Arbiter PUF with a phase window.]
[37] ФНФ на основе триггеров с высокоимпедансным выходом. [PUF based on high-impedance flip-flops.]
[38] Программная ФНФ на основе разгона тактового сигнала. [S-PUF based on overclocking.]

Таблица. Продолжение

Тип ФНФ/работа	Год публикации	Характеристики ФНФ					
		Inter-distance	Intra-distance	Платформа	Inter-distance		Оценочная сложность реализации
					Температура	Напряжение	
Glitch [41]	2010	~32%	1.3%	FPGA Xilinx XC3S400A–4FTG256C (16 boards)	100 °C (+5.3%)	–	средняя
Glitch PUF с триггером Шмитта [43]	2021	50.03%	–	ASIC TSMC 65-нм КМОП	−25–125 °C	0.8–1.4 В	средняя
SRAM [45]	2007	49.97%	3.57%	FPGA	−20–80 °C	–	низкая
Butterfly [49]	2007	~50%	~10%	FPGA (Xilinx Virtex-5)	−20–80 °C	–	средняя
MRAM [58]	2024	49.96%	0.98%	MRAM (STT[39]-MRAM массив)	−25–100 °C	0.65–0.85 В	средняя
3D ReRAM [60]	2022	49.4%	0.014%	ReRAM (8-слойный 3D-массив)	0–80 °C (+1.93%)	1.65–2.2 В (+1.93%)	высокая
Dual-Mode[40] ReRAM [61]	2025	~50%	~1%	ReRAM (1T1R ячейки + логика)	–	–	высокая

ЗАКЛЮЧЕНИЕ

ФНФ на основе временных характеристик сигналов – это класс устройств, где для формирования откликов, обусловленных вариациями изготовления, используется анализ частоты, фазы и переходных процессов. Для получения устойчивого ответа таким решениям обычно требуются тщательно сбалансированная компоновка, калибровка и модули постобработки. Их преимуществом является практически неограниченное пространство пар «запрос – ответ», что делает их удобными кандидатами для протоколов аутентификации, однако они уязвимы к атакам на основе моделирования.

ФНФ на основе памяти формируют «отпечаток» из стартовых состояний и/или характеристик массивов SRAM/DRAM/NVM. Их сильная сторона – простая интеграция в уже имеющиеся на кристалле блоки и высокая воспроизводимость при умеренных накладных расходах. При этом пространство пар «запрос – ответ» обычно ограничено, что ориентирует их на задачи генерации ключей и идентификации устройства.

Для обоих классов важны меры стабилизации к условиям эксплуатации (температура, питание, старение) и использование вспомогательных данных, коррекции ошибок и/или модулей анализа. Выбор конкретной ФНФ должен исходить из требований приложения и целевой платформы.

БЛАГОДАРНОСТИ

Работа выполнена при поддержке Министерства науки и высшего образования РФ (Государственное задание для университетов № FSFZ-2026-0003) и с применением оборудования Центра коллективного пользования РТУ МИРЭА (соглашение от 01.09.2021 № 075-15-2021-689, уникальный идентификационный номер 2296.61321X0010).

ACKNOWLEDGMENTS

This work was supported by the Ministry of Science and Higher Education of the Russian Federation (State task for universities No. FSFZ-2026-0003) and using the equipment of the Center for Collective Use of RTU MIREA (agreement dated September 01, 2021, No. 075-15-2021-689, unique identification number 2296.61321X0010).

Вклад авторов

Е.Ф. Певцов – концепция исследования, разработка структуры обзора, написание текста статьи.

Т.А. Деменкова – концепция исследования, разработка структуры обзора, обобщение результатов.

Ю.А. Коротаев – анализ и систематизация литературы, написание текста статьи, обобщение результатов.

[39] Spin-torque-transfer – передача спинового момента. [Spin-torque-transfer.]

[40] Dual mode – двухканальный режим работы оперативной памяти. [Dual-channel RAM mode.]

А.С. Сигов – научное консультирование, научное редактирование статьи, утверждение финальной версии рукописи.

Все авторы прочитали и одобрили опубликованную версию рукописи.

Authors' contributions

E.Ph. Pevtsov – study conceptualization, review outline and structure, manuscript writing.

T.A. Demenkova – study conceptualization, review outline and structure, synthesis of the results.

Yu.A. Korotaev – literature analysis and systematization, manuscript writing, synthesis of the results.

A.S. Sigov – scientific consulting, scientific editing, final approval of the manuscript.

All authors have read and approved the published version of the manuscript.

СПИСОК ЛИТЕРАТУРЫ / REFERENCES

1. Khalil K., Idris H., Idriss T., Bayoumi M. *Lightweight Hardware Security and Physically Unclonable Functions: Improving Security of Constrained IoT Devices*. Cham: Springer Nature Switzerland; 2025, 152 p.
2. McGrath T., Bagci I.E., Wang Z.M., Roedig U., Young R.J. A PUF taxonomy. *Appl. Phys. Rev.* 2019;6(1):011303. https://doi.org/10.1063/1.5079407
3. Zerrouki F., Ouchani S., Bouarfa H. A survey on silicon PUFs. *J. Syst. Archit.* 2022;127:102514. https://doi.org/10.1016/j.sysarc.2022.102514
4. Alhamarneh R.A., Mahinderjit Singh M. Strengthening Internet of Things Security: Surveying Physical Unclonable Functions for Authentication, Communication Protocols, Challenges, and Applications. *Appl. Sci.* 2024;14(5):1700. https://doi.org/10.3390/app14051700
5. Tehranipoor M., Pundir N., Vashistha N., Farahmandi F. *Hardware Security Primitives*. Cham: Springer; 2023, 350 p.
6. Maes R., Verbauwhede I. Physically Unclonable Functions: A Study on the State of the Art and Future Research Directions. In: Sadeghi A.-R., Naccache D. (Eds.). *Towards Hardware-Intrinsic Security: Foundations and Practice*. Berlin: Springer; 2010. P. 3–37. https://doi.org/10.1007/978-3-642-14452-3_1
7. Suh G.E., Devadas S. Physical Unclonable Functions for Device Authentication and Secret Key Generation. In: *Proceedings of the 44th ACM/IEEE Design Automation Conference* (*DAC 2007*), San Diego, CA, USA, June 4–8, 2007. New York: ACM; 2007. P. 9–14. https://doi.org/10.1145/1278480.1278484
8. Лебедев В.Р., Певцов Е.Ф., Деменкова Т.А., Малето М.И., Филимонов В.В. Метод исследования реализации физически неклонируемых функций в информационных системах. *International Journal of Open Information Technologies*. 2024;12(1):28–36. URL: http://injoit.org/index.php/j1/article/view/1712. Дата обращения 10.07.2025. / Accessed July 10, 2025. [Lebedev V.R., Pevtsov E.F., Demenkova T.A., Maleto M.I., Filimonov V.V. Method for studying the implementation of Physical Unclonable Function in information systems. *Int. J. Open Inf. Technol.* 2024;12(1):28–36 (in Russ.). Available from URL: http://injoit.org/index.php/j1/article/view/1712. Accessed July 10, 2025.]
9. Gassend B., Clarke D., van Dijk M., Devadas S. Silicon physical random functions. In: *Proceedings of the 9th ACM Conference on Computer and Communications Security* (*CCS 2002*), Washington, DC, USA, November 18–22, 2002. New York: ACM; 2002. P. 148–160. https://doi.org/10.1145/586110.586132
10. Vivekraja V., Nazhandali L. Circuit-level techniques for reliable physically unclonable functions. In: *Proceedings of the 2009 IEEE International Workshop on Hardware-Oriented Security and Trust* (*HOST 2009*), San Francisco, CA, USA, July 27, 2009. Piscataway, NJ: IEEE; 2009. P. 30–35. https://doi.org/10.1109/HST.2009.5225054
11. Pappu R., Recht B., Taylor J., Gershenfeld N. Physical one-way functions. *Science*. 2002;297(5589):2026–2030. https://doi.org/10.1126/science.1074376
12. Anandakumar N.N., Hashmi M.S., Tehranipoor M. FPGA-based Physical Unclonable Functions: A comprehensive overview of theory and architectures. *Integration*. 2021;81:175–194. https://doi.org/10.1016/j.vlsi.2021.06.001
13. Cao Y., Xu J., Wu J., Wu S., Huang Z., Zhang K. Advances in Physical Unclonable Functions Based on New Technologies: A Comprehensive Review. *Mathematics* (*Basel*). 2024;12(1):77. https://doi.org/10.3390/math12010077
14. Vatalaro M., De Rose R., Lanuzza M., Crupi F. Weak physically unclonable functions in CMOS technology: A review. *Chips*. 2025;4(1):3. https://doi.org/10.3390/chips4010003
15. Sklavos N., Chaves R., Di Natale G., Regazzoni F. *Hardware Security and Trust: Design and Deployment of Integrated Circuits in a Threatened Environment*. Cham: Springer; 2017, 254 p. https://doi.org/10.1007/978-3-319-44318-8
16. Lata K., Cenkeramaddi L.R. FPGA-Based PUF Designs: A comprehensive review and comparative analysis. *Cryptography*. 2023;7(4):55. https://doi.org/10.3390/cryptography7040055
17. Masoumian S., Selimis G., Wang R., Schrijen G-J., Hamdioui S., Taouil M. Reliability analysis of FinFET-based SRAM PUFs for 16 nm, 14 nm and 7 nm technology nodes. In: *Proceedings of the 2022 Design, Automation & Test in Europe Conference & Exhibition* (*DATE 2022*), Antwerp, Belgium, March 14–23, 2022. Piscataway, NJ: IEEE; 2022. P. 1189–1192. https://doi.org/10.23919/DATE54114.2022.9774735
18. Eiroa S., Baturone I., Acosta A.J., Dávila J. Using physical unclonable functions for hardware authentication: A survey. In: *Proceedings of the 25th Conference on Design of Circuits and Integrated Systems* (*DCIS 2010*), Lanzarote, Canary Islands, Spain, November 17–19, 2010. Lanzarote; 2010. URL: https://digital.csic.es/bitstream/10261/96029/1/Using%20Physical.pdf

19. Bossuet L., Ngo X.T., Cherif Z., Fischer V. A PUF based on a transient effect ring oscillator and insensitive to locking phenomenon. *IEEE Trans. Emerg. Top. Comput.* 2014;2(1):30–36. https://doi.org/10.1109/TETC.2013.2287182
20. Brzuska C., Fischlin M., Schröder H., Katzenbeisser S. Physically uncloneable functions in the universal composition framework. In: Rogaway P. (Ed.). *Advances in Cryptology – CRYPTO 2011*, Santa Barbara, CA, USA, August 14–18, 2011. Book Series: Lecture Notes in Computer Science. Berlin: Springer; 2011. V. 6841. P. 51–70. https://doi.org/10.1007/978-3-642-22792-9_4
21. Tuyls P., Schrijen G-J., Škorić B., van Geloven J., Verhaegh N., Wolters R. Read-proof hardware from protective coatings. In: Goubin L., Matsui M. (Eds.). *Cryptographic Hardware and Embedded Systems. CHES 2006*, Yokohama, Japan, October 10–13, 2006. Book Series: Lecture Notes in Computer Science. Berlin: Springer; 2006. V. 4249. P. 369–383. https://doi.org/10.1007/11894063_29
22. Chen Q., Csaba G., Lugli P., Schlichtmann U., Rührmair U. The bistable ring PUF: a new architecture for strong physical unclonable functions. In: *Proceedings of the 2011 IEEE International Symposium on Hardware-Oriented Security and Trust* (*HOST 2011*), San Diego, CA, USA, June 5–6, 2011. Piscataway, NJ: IEEE; 2011. P. 134–141. https://doi.org/10.1109/HST.2011.5955011
23. Abulibdeh E., Saleh H., Mohammad B., Al-Qutayri M., Veeran A. Area and power efficient implementation of configurable ring oscillator PUF. *TechRxiv Preprint*; April 2, 2024. https://doi.org/10.36227/techrxiv.171207533.30573247/v1
24. Abulibdeh E., Saleh H., Mohammad B., Al-Qutayri M., Hussain A. Kernel-based response extraction approach for efficient configurable ring oscillator PUF. *Sci. Rep.* 2025;15:5938. https://doi.org/10.1038/s41598-025-89769-5
25. Иванюк А.А., Ярмолик В.Н. Конфигурируемый кольцевой осциллятор с управляемыми межсоединениями. *Безопасность информационных технологий*. 2024;31(2):121–133. https://doi.org/10.26583/bit.2024.2.08
[Ivaniuk A.A., Yarmolik V.N. Configurable ring oscillator with controlled interconnections. *Bezopasnost' informatsionnykh tekhnologii = IT Security* (*Russia*). 2024;31(2):121–133 (in Russ.). https://doi.org/10.26583/bit.2024.2.08]
26. Du H., Guo C., Cui S. Optimization design of the RO PUF temperature reliability based on MOSFET temperature characteristics. In: *The International Conference Optoelectronic Information and Optical Engineering* (*OIOE 2024*), Wuhan, China, October 18–20, 2024. Proc. SPIE 13513; 2025. Art. 1351324. https://doi.org/10.1117/12.3045630
27. Schaller A., Xiong W., Anagnostopoulos N.A., Saleem M.U., Gabmeyer S., Katzenbeisser S., Szefer J. Intrinsic Rowhammer PUFs: Leveraging the Rowhammer effect for improved security. In: *Proceedings of the 2017 IEEE International Symposium on Hardware-Oriented Security and Trust* (*HOST 2017*), McLean, VA, USA, May 1–5, 2017. Piscataway, NJ: IEEE; 2017. P. 1–7. https://doi.org/10.1109/HST.2017.7951729
28. Anandakumar N.N., Hashmi M.S., Chaudhary M.A. Implementation of efficient XOR arbiter PUF on FPGA with enhanced uniqueness and security. *IEEE Access*. 2022;10:129832–129842. https://doi.org/10.1109/ACCESS.2022.3228635
29. Hori Y., Kang H., Katashita T., Satoh A. Pseudo-LFSR PUF: A compact, efficient and reliable physical unclonable function. In: *Proceedings of the 2011 International Conference on Reconfigurable Computing and FPGAs* (*ReConFig'11*), Cancun, Mexico, November 30 – December 2, 2011. Cancun: IEEE; 2011. P. 223–228. https://doi.org/10.1109/ReConFig.2011.72
30. Marchand C., Bossuet L., Cherkaoui A. Enhanced TERO-PUF implementations and characterization on FPGAs. In: *Proceedings of the 2016 ACM/SIGDA International Symposium on Field-Programmable Gate Arrays* (*FPGA 2016*), Monterey, CA, USA, February 21–23, 2016. New York: ACM; 2016. P. 282. https://doi.org/10.1145/2847263.2847298
31. Xu X., Rührmair U., Holcomb D.E., Burleson W.P. Security evaluation and enhancement of bistable ring PUFs. In: Mangard S., Schaumont P. (Eds.). *Radio Frequency Identification. RFIDSec 2015*. Book Series: Lecture Notes in Computer Science. Cham: Springer; 2015. V. 9440. P. 3–16. https://doi.org/10.1007/978-3-319-24837-0_1
32. Thirumoorthi M., Jovanovic M., Mirhassani M., Khalid M.A.S. Design and evaluation of a hybrid chaotic-bistable ring PUF. *IEEE Trans. Very Large Scale Integr.* (*VLSI*) *Syst.* 2021;29(11):1912–1921. https://doi.org/10.1109/TVLSI.2021.3111588
33. Sharifi F., Momeni H., Hosseini A. Ternary bistable ring PUF for high-secure applications. *J. Supercomput.* 2024;80: 12663–12685. https://doi.org/10.1007/s11227-024-05935-y
34. Rührmair U., van Dijk M. On the practical use of physical unclonable functions in oblivious transfer and bit commitment protocols. *J. Cryptogr. Eng.* 2013;3(1):17–28. https://doi.org/10.1007/s13389-013-0052-8
35. Rührmair U. Oblivious transfer based on physical unclonable functions. In: Acquisti A., Smith S.W., Sadeghi A.-R. (Eds.). *Trust and Trustworthy Computing. TRUST 2010*. Berlin: Springer; 2010. V. 6101. P. 430–440. https://doi.org/10.1007/978-3-642-13869-0_31
36. Roy A., Roy D., Stănică P. On combining Arbiter based PUFs. *Cryptogr. Commun.* 2025;17(2):493–510. https://doi.org/10.1007/s12095-024-00769-0
37. Driemeyer B., Mandry H., Wiens D.-P., Becker J., Kauffman J.G., Ortmanns M. An eye-opening Arbiter PUF for fingerprint generation using auto-error detection for PVT-robust masking and bit stabilization achieving a BER of 2e-8 in 28 nm CMOS. In: *Proceedings of the 2025 IEEE International Solid-State Circuits Conference* (*ISSCC 2025*), San Francisco, CA, USA, February 16–20, 2025. Piscataway, NJ: IEEE; 2025. P. 300–302. https://doi.org/10.1109/ISSCC49661.2025.10904785
38. Yao Y., Kim M., Li J., Markov I., Koushanfar F. ClockPUF: physical unclonable functions based on clock networks. In: *Proceedings of the Design, Automation & Test in Europe Conference & Exhibition* (*DATE 2013*), Grenoble, France, March 18–22, 2013. Piscataway, NJ: IEEE; 2013. P. 422–427. https://doi.org/10.7873/DATE.2013.095
39. Khan S., Shah A.P., Chouhan S.S., Roy A., Roy D., Stănică P. Utilizing manufacturing variations to design a tri-state flip-flop PUF for IoT security applications. *Analog Integr. Circ. Sig. Process.* 2020;103:477–492. https://doi.org/10.1007/s10470-020-01642-9

40. Yuan T., Wang P., Zhang Y., Zhou Z. An overclocking clock software PUF circuit with no additional hardware resource overhead based on video coding circuit. *Integration*. 2025;101:102319. https://doi.org/10.1016/j.vlsi.2024.102319
41. Suzuki D., Shimizu K. The Glitch PUF: a new Delay-PUF architecture exploiting glitch shapes. In: Mangard S., Standaert F.-X. (Eds.). *Cryptographic Hardware and Embedded Systems. CHES 2010*, August 17–20, 2010. Santa Barbara, CA, USA. Book Series: Lecture Notes in Computer Science. Berlin: Springer; 2010. V. 6225. P. 366–382. https://doi.org/10.1007/978-3-642-15031-9_25
42. Anderson J. A PUF design for secure FPGA-based embedded systems. In: *Proceedings of the 15th Asia South Pacific Design Automation Conference* (*ASP-DAC 2010*), Taipei, Taiwan, January 18–21, 2010. Piscataway, NJ: IEEE; 2010. P. 1–6. https://doi.org/10.1109/ASPDAC.2010.5419927
43. Ni L., Wang P., Zhang Y., Chen J., Li L., Zhang H. A reliable multi-information entropy glitch PUF using Schmitt trigger sampling method for IoT security. In: *2021 IEEE 14th International Conference on ASIC* (*ASICON 2021*), Kunming, China, October 26–29, 2021. Piscataway, NJ: IEEE; 2021. P. 1–4. https://doi.org/10.1109/ASICON52560.2021.9620406
44. Nozaki Y., Takemoto S., Yoshikawa M. Error correction method for lightweight cipher PRINCE-based physically unclonable function. In: *Proceedings of the 6th International Conference on Information Technology and Computer Communications* (*ITCC 2024*), Xi'an, China, July 5–7, 2024. New York: ACM; 2024. P. 38–42. https://doi.org/10.1145/3704391.3704397
45. Guajardo J., Kumar S.S., Schrijen G-J., Tuyls P. FPGA intrinsic PUFs and their use for IP protection. In: Paillier P., Verbauwhede I. (Eds.). *Cryptographic Hardware and Embedded Systems – CHES 2007*, Vienna, Austria, September 10–13, 2007. Lecture Notes in Computer Science. Berlin: Springer; 2007. V. 4727. P. 63–80. https://doi.org/10.1007/978-3-540-74735-2_5
46. Holcomb D.E., Burleson W.P., Fu K. Initial SRAM state as a fingerprint and source of true random numbers for RFID tags. *Proceedings of the Conference on RFID Security*. 2007;7(2):01–012.
47. Gebali F., Mamun M. Review of physically unclonable functions (PUFs): Structures, models, and algorithms. *Front. Sens.* 2022;2:751748. https://doi.org/10.3389/fsens.2021.751748
48. Holcomb D.E., Burleson W.P., Fu K. Power-up SRAM state as an identifying fingerprint and source of true random numbers. *IEEE Trans. Comput.* 2009;58(9):1198–1210. https://doi.org/10.1109/TC.2008.212
49. Kumar S., Guajardo J., Maes R., Schrijen G-J., Tuyls P. The butterfly PUF: protecting IP on every FPGA. In: *Proceedings of the IEEE International Workshop on Hardware-Oriented Security and Trust* (*HOST 2008*), Anaheim, CA, USA, June 3–4, 2008. Piscataway, NJ: IEEE; 2008. P. 67–70. https://doi.org/10.1109/HST.2008.4559053
50. Farha F., Ning H., Ali K., Chen L., Nugent C. SRAM-PUF-based entities authentication scheme for resource-constrained IoT devices. *IEEE Internet Things J.* 2021;8(7):5904–5913. https://doi.org/10.1109/JIOT.2020.3032518
51. Su Y., Holleman J., Otis B. A 1.6 μJ/bit stable chip-ID generating circuit using process variations. In: *Proceedings of the IEEE International Solid-State Circuits Conference* (*ISSCC 2007*), San Francisco, CA, USA, February 11–15, 2007. Piscataway, NJ: IEEE; 2007. P. 606–611. https://doi.org/10.1109/ISSCC.2007.373466
52. Tehranipoor F., Karimian N., Yan W., Chandy J.A. Investigation of DRAM PUFs reliability under device accelerated aging effects. In: *Proceedings of the 2017 IEEE International Symposium on Circuits and Systems* (*ISCAS 2017*), Baltimore, MD, USA, May 28–31, 2017. Piscataway, NJ: IEEE; 2017. P. 1–4. https://doi.org/10.1109/ISCAS.2017.8050629
53. Yue M., Karimian N., Yan W., Anagnostopoulos N.A., Tehranipoor F. DRAM-based authentication using deep convolutional neural networks. *IEEE Consum. Electron. Mag.* 2021;10(4):8–17. https://doi.org/10.1109/MCE.2020.3002528
54. Sutar S., Raha A., Raghunathan V. D-PUF: an intrinsically reconfigurable DRAM PUF for device authentication in embedded systems. In: *Proceedings of the 2016 International Conference on Compilers, Architectures and Synthesis of Embedded Systems* (*CASES 2016*), Pittsburgh, PA, USA, October 2–7, 2016. New York: ACM; 2016. P. 1–10. https://doi.org/10.1145/2968455.2968519
55. Chew Y.Y., Lim W.L., Tan J.L., Ooi C.Y. In-depth review and comparative analysis of DRAM-based PUFs. *IEEE Access*. 2025;13:79367–79384. https://doi.org/10.1109/ACCESS.2025.3566068
56. Wilson T., Cambou B. Tamper-sensitive pre-formed ReRAM-based PUFs: Methods and experimental validation. *Front. Nanotechnol.* 2022;4:1055545. https://doi.org/10.3389/fnano.2022.1055545
57. Napolean A., Sivamangai N.M., Sharon N., Naveen Kuma R. Review on resistive random access memory based physical unclonable function circuits for high security. *Procedia Environ. Sci. Eng. Manag.* 2023;10(1):41–52. URL: http://www.procedia-esem.eu/pdf/issues/2023/no1/5_Napolean_22.pdf. Дата обращения 10.07.2025. / Accessed July 10, 2025.
58. Adel M.J., Rezayati M.H., Moaiyeri M.H., et al. A robust deep learning attack immune MRAM-based physical unclonable function. *Sci. Rep.* 2024;14:20649. https://doi.org/10.1038/s41598-024-71730-7
59. Go S.X., Wang Q., Lim K.G., Lee T.H., Bajalovic N., Loke D.K. Ultrafast near-ideal phase-change memristive physical unclonable functions driven by amorphous state variations. *Adv. Sci.* (*Weinh.*) 2022;9(36):e2204453. https://doi.org/10.1002/advs.202204453
60. Yang J., Lei D., Chen D., Li J., Jiang H., Luo Q., et al. Machine-learning-resistant 3D PUF with 8-layer stacking vertical RRAM and 0.014% bit error rate using in-cell stabilization scheme for IoT security applications. In: *2020 IEEE International Electron Devices Meeting* (*IEDM*), San Francisco, CA, USA, December 12–18, 2020. Piscataway, NJ: IEEE; 2020. P. 28.6.1–28.6.4. https://doi.org/10.1109/IEDM13553.2020.9372107
61. Li J., Cui Y., Gu C., Wang C., Liu W., Kvatinsky S. A highly reliable dual-mode RRAM PUF with key concealment scheme. *IEEE Trans. Comput.-Aided Des. Integr. Circuits Syst.* 2025. https://doi.org/10.1109/TCAD.2025.3536376

Об авторах

Певцов Евгений Филиппович, к.т.н., директор структурного подразделения «Центр проектирования интегральных схем, устройств наноэлектроники и микросистем», ФГБОУ ВО «МИРЭА – Российский технологический университет» (119454, Россия, Москва, пр-т Вернадского, д. 78). E-mail: pevtsov@mirea.ru. Scopus Author ID 6602652601, ResearcherID M-2709-2016, SPIN-код РИНЦ 1410-2483, https://orcid.org/0000-0001-6264-1231

Деменкова Татьяна Александровна, к.т.н., доцент, кафедра вычислительной техники, Институт информационных технологий, ФГБОУ ВО «МИРЭА – Российский технологический университет» (119454, Россия, Москва, пр-т Вернадского, д. 78). E-mail: demenkova@mirea.ru. Scopus Author ID 57192958412, ResearcherID AAB-3937-2020, SPIN-код РИНЦ 3424-7489, https://orcid.org/0000-0003-3519-6683

Коротаев Юрий Александрович, аспирант, кафедра наноэлектроники, Институт перспективных технологий и индустриального программирования, ФГБОУ ВО «МИРЭА – Российский технологический университет» (119454, Россия, Москва, пр-т Вернадского, д. 78). E-mail: korotaevyua@yandex.ru. SPIN-код РИНЦ 7428-6831, https://orcid.org/0009-0000-3976-7872

Сигов Александр Сергеевич, академик Российской академии наук, д.ф.-м.н., профессор, президент ФГБОУ ВО «МИРЭА – Российский технологический университет» (119454, Россия, Москва, пр-т Вернадского, д. 78). E-mail: sigov@mirea.ru. Scopus Author ID 35557510600, ResearcherID L-4103-2017, SPIN-код РИНЦ 2869-5663, https://www.researchgate.net/profile/A_Sigov

About the Authors

Evgenii Ph. Pevtsov, Cand. Sci. (Eng.), Director of Center for the Design of Integrated Circuits, Nanoelectronics Devices and Microsystems, MIREA – Russian Technological University (78, Vernadskogo pr., Moscow, 119454 Russia). E-mail: pevtsov@mirea.ru. Scopus Author ID 6602652601, ResearcherID M-2709-2016, RSCI SPIN-code 1410-2483, http://orcid.org/0000-0001-6264-1231

Tatyana A. Demenkova, Cand. Sci. (Eng.), Associated Professor, Computer Technology Department, Institute of Information Technologies, MIREA – Russian Technological University (78, Vernadskogo pr., Moscow, 119454 Russia). E-mail: demenkova@mirea.ru. Scopus Author ID 57192958412, ResearcherID AAB-3937-2020, RSCI SPIN-code 3424-7489, http://orcid.org/0000-0003-3519-6683

Yuri A. Korotaev, Postgraduate Student, Department of Nanoelectronics, Institute for Advanced Technologies and Industrial Programming, MIREA – Russian Technological University (78, Vernadskogo pr., Moscow, 119454 Russia). E-mail: korotaevyua@yandex.ru. RSCI SPIN-code 7428-683, https://orcid.org/0009-0000-3976-7872

Alexander S. Sigov, Academician at the Russian Academy of Sciences, Dr. Sci. (Phys.–Math.), Professor, President, MIREA – Russian Technological University (78, Vernadskogo pr., Moscow, 119454 Russia). E-mail: sigov@mirea.ru. Scopus Author ID 35557510600, ResearcherID L-4103-2017, RSCI SPIN-code 2869-5663, https://www.researchgate.net/profile/A_Sigov