Russian Technological Journal.
2026;14(3):83–105

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-2026-14-3-83-105
EDN QIOHGI

ОБЗОРНАЯ СТАТЬЯ

Физически неклонируемые функции в аналоговых интегральных схемах

Е.Ф. Певцов [@], Т.А. Деменкова, М.И. Малето, А.С. Сигов, Ю.А. Коротаев [@], Н.Д. Евгеньев

МИРЭА – Российский технологический университет, Москва, 119454 Россия
[@] Авторы для переписки, e-mail: korotaevyua@yandex.ru, pevtsov@mirea.ru

• **Поступила:** 16.09.2025 • **Доработана:** 20.10.2025 • **Принята к опубликованию:** 27.03.2026

Резюме

Цели. Целью работы является комплексный обзор аналоговых и пассивных физически неклонируемых функций (ФНФ), анализ уязвимостей к атакам на основе машинного обучения и разбор практических сценариев применения в современных интегральных схемах и устройствах интернета вещей.

Методы. Использованы методы количественной оценки различий реализаций ФНФ и признаков их формального описания, включая вычислимость, уникальность, реализуемость, сложность создания клонов, защиту от несанкционированного доступа.

Результаты. Показано, что аналоговые ФНФ относятся к классу «сильных» ФНФ, но требуют специальных мер для подавления влияния факторов внешней среды и старения. Приведены примеры, демонстрирующие близкую к идеальной уникальность (inter-HD[1] ≈ 50%) при высокой стабильности (intra-HD[2] < 1%) и рекордные энергетические показатели (единицы – десятки фДж/бит). Пассивные ФНФ характеризуются высокой стабильностью, но относятся к «слабым» ФНФ. Рассмотрены атаки на основе машинного обучения, показано, что конволюционные нейронные сети и многослойные перцептроны превосходят классические подходы. Средства защиты на уровне протокола, ограничивающие объем доступной злоумышленнику информации, позволяют избежать модификации архитектуры ФНФ.

Выводы. Аналоговые и пассивные ФНФ расширяют спектр средств аппаратной аутентификации и защиты от подделок, особенно для маломощных и ресурсно-ограниченных устройств интернета вещей. Наиболее перспективны архитектуры с внутренней калибровкой и малыми накладными расходами по площади/потреблению, а также пассивные решения для задач однократной идентификации и контроля вмешательства. Остаются открытыми задачи стандартизации процедур чтения/оцифровки, повышения устойчивости к изменениям внешней среды и различным атакам, а также совмещения с коррекцией ошибок и постобработкой на кристалле. Для выбора архитектур ФНФ необходимо тщательное моделирование угроз и применение стратегий глубокой защиты с учетом будущих достижений машинного обучения.

Ключевые слова: физически неклонируемая функция, аналоговые ФНФ, пассивные ФНФ, ML-атаки, аппаратная безопасность, аутентификация устройств, интернет вещей

[1] Inter-Hamming distance – внешнее расстояние Хэмминга.
[2] Intra-Hamming distance – внутреннее расстояние Хэмминга.

Для цитирования: Певцов Е.Ф., Деменкова Т.А., Малето М.И., Сигов А.С., Коротаев Ю.А., Евгеньев Н.Д. Физически неклонируемые функции в аналоговых интегральных схемах. *Russian Technological Journal*. 2026;14(3):83–105. https://doi.org/10.32362/2500-316X-2026-14-3-83-105, https://www.elibrary.ru/QIOHGI

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 analog integrated circuits

Evgenii Ph. Pevtsov [@], Tatyana A. Demenkova, Mikhail I. Maleto, Alexander S. Sigov, Yuri A. Korotaev [@], Nikita D. Evgenev

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

• **Submitted:** 16.09.2025 • **Revised:** 20.10.2025 • **Accepted:** 27.03.2026

Abstract

Objectives. The paper provides a comprehensive overview of analog and passive physical unclonable functions (PUFs), analyzing their vulnerabilities to machine-learning (ML) attacks, and assessing their practical deployment in modern integrated circuits and Internet of Things (IoT) devices.

Methods. Quantitative metrics were used to compare PUF implementations and their formal properties, such as computability, uniqueness, implementability, difficulty of cloning, and protection against unauthorized access.

Results. Analog PUFs were shown to belong to the class of “strong” PUFs. However, special measures are required to counteract environmental and ageing effects. Examples are cited to demonstrate their near-ideal uniqueness (inter-Hamming distance ≈ 50%), high stability (intra-Hamming distance < 1%), and excellent energy performance (from units to tens of femtojoules per bit). While characterized by high stability, passive PUFs are classified as “weak” PUFs. A consideration of ML-based modeling attacks confirmed that convolutional neural networks and multilayer perceptrons outperform classical approaches. By limiting the amount of data available to an attacker, protocol-level protection prevents the PUF architecture from being modified.

Conclusions. Analog and passive PUFs expand the range of tools available for hardware authentication and anti-counterfeiting, particularly in low-power, resource-constrained IoT nodes. The most promising directions include architectures with on-chip self-calibration and minimal area/power overhead, as well as passive schemes for one-time identification and tamper evidence. However, open challenges remain in terms of standardizing readout and digitization procedures, increasing robustness to environmental variation and diverse attacks, and integrating error correction and post-processing on the chip. The practical adoption and selection of architectures requires conservative threat modeling and defense-in-depth strategies that account for current attack capabilities and likely future advances in ML.

Keywords: physically unclonable function, analog PUFs, passive PUFs, ML attacks, hardware security, device authentication, Internet of Things

For citation: Pevtsov E.Ph., Demenkova T.A., Maleto M.I., Sigov A.S., Korotaev Yu.A., Evgenev N.D. Physically unclonable functions in analog integrated circuits. *Russian Technological Journal.* 2026;14(3):83–105. https://doi.org/10.32362/2500-316X-2026-14-3-83-105, https://www.elibrary.ru/QIOHGI

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

The authors declare no conflicts of interest.

ВВЕДЕНИЕ

Физически неклонируемые функции (ФНФ) служат аппаратной основой доверия для аутентификации, защиты от подделок и безопасного вывода ключей. В первой части цикла [1] рассматривались цифровые ФНФ. Вторая часть посвящена аналоговым и пассивным ФНФ, а также современным атакам на основе машинного обучения (machine learning, ML) и практическим сценариям внедрения.

Аналоговые ФНФ используют непрерывные технологические разбросы параметров активных и пассивных элементов в качестве источника энтропии. В отличие от цифровых примитивов аппаратной безопасности, где наблюдаемый эффект формируется дискретной логикой, аналоговые ФНФ опираются на тонкие вариации пороговых напряжений, токов, емкостей и сопротивлений, которые после включения схемы приводят к воспроизводимым стационарным уровням напряжения/тока, уникальным для каждого кристалла. Оцифровка выполняется компаратором или аналого-цифровым преобразователем. Устойчивость откликов обеспечивается схемными приемами подавления дрейфа и шумов. Аналоговые реализации потенциально предоставляют более высокую плотность энтропии и больший набор пар «запрос – ответ» (challenge to response pairs, CRP), что позволяет относить многие из них к классу «сильных» ФНФ. Вместе с тем работа с характеристиками транзисторных и пассивных структур чувствительна к внешним факторам, что требует применения специальных мер для коррекции возможных ошибок.

Пассивные ФНФ – резистивные «отпечатки» силовых сетей, Via PUF[3] на вероятностном формировании контактов и Coating PUF[4] со специфическим «рисунком» случайного покрытия, отличающиеся минимальными накладными расходами по площади, высокой стабильностью и, в ряде случаев, с идеальной стабильностью, но ограниченным числом пар «запрос – ответ».

Бурное развитие сферы ML радикально изменило понимание безопасности ФНФ: вместо традиционного криптоанализа на первый план вышли атаки, ориентированные на извлечение закономерностей из пар «запрос – ответ». Исследовательское сообщество параллельно продвигает все более совершенные ML-подходы к моделированию ФНФ и контрмеры на уровне архитектуры и протоколов, уточняя фундаментальные границы стойкости. В работе дан сводный обзор текущего состояния: теоретические основы, классы атак на основе ML, практические контрмеры и их последствия для проектирования и развертывания ФНФ.

АНАЛОГОВЫЕ ФНФ

Измерение оригинальных параметров электрической или электронной величины может служить процедурой для идентификации устройств. Источником энтропии служат вариации пороговых напряжений транзисторов (TV[5]- / ICID[6]-PUF), токовые арбитры, диодные структуры, схемы квазиадиабатической логики (QUAL-PUF[7]) и адиабатические SRAM[8].

В наиболее простом варианте TV-PUF, который применяется для идентификации интегральных схем (ИС), обычно анализируется изменение пороговых напряжений интегральных транзисторов, имеющее место в результате неизбежных вариаций технологии на этапе производства. Запросом является номер или расположение транзисторного компонента, а ответом – значение соответствующего порогового напряжения.

Один из методов применения ФНФ, позволяющих присвоить уникальную идентификационную метку каждому отдельному экземпляру обычной ИС без необходимости специальных этапов обработки или программирования после изготовления, предложен в [2]. В устройстве, именуемом ICID-PUF, несколько транзисторов одинаковой конструкции объединены в адресуемую матрицу (рис. 1).

В ICID-PUF адресуемый транзистор управляет резистивной нагрузкой. Из-за особенностей изготовления пороговые напряжения этих транзисторов различаются, и ток, проходящий через эту нагрузку, будет частично случайным. Напряжение на нагрузке измеряется и преобразуется в последовательность битов с помощью компаратора с автоматическим обнулением. Этот метод был экспериментально проверен на 55 микросхемах, изготовленных по технологии 0.35 мкм КМОП[9]. При наибольших

[3] Via physically unclonable function (PUF) – технология ФНФ, основанная на использовании микроскопических отверстий (via) в металлических слоях полупроводников. [Via PUF is a technology based on the use of microscopic via holes in metallic layers of semiconductors.]

[4] ФНФ на основе защитного покрытия. [Coating PUF is a technology that utilizes a protective coating for its operation.]

[5] Threshold voltage – пороговое напряжение.

[6] Integrated circuit identification – идентификация интегральной схемы.

[7] Quasi-adiabatic logic based PUF.

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

[9] Комплементарная структура металл – оксид – полупроводник – набор полупроводниковых технологий построения интегральных микросхем и соответствующая ей схемотехника микросхем. [The complementary metal–oxide–semiconductor (CMOS) structure is a collection of semiconductor technologies used for the fabrication of integrated circuits and the related circuitry in microcircuits.]

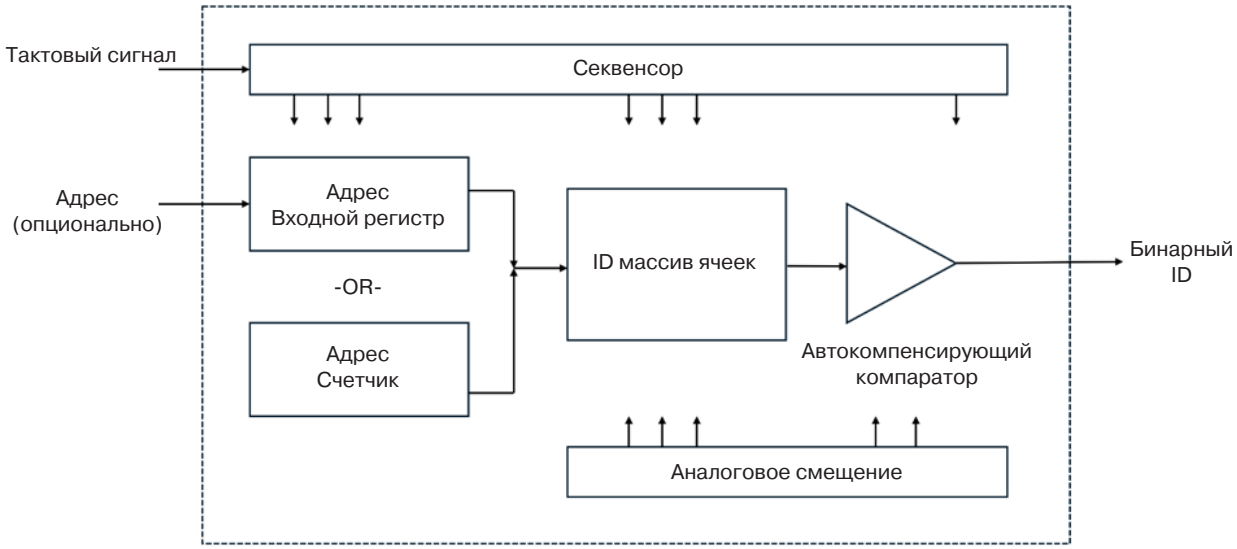


Рис. 1. Блок-схема устройства для идентификации ИС на основе ФНФ [2]. ID (identifier) – идентификатор

колебаниях окружающей среды получено значение intra-HD[10] μ_{intra} = 1.3%, в то время как inter-HD[11] μ_{inter} очень близко к 50%. При тактовой частоте 1 ГГц на входе усилителя конструкция ФНФ с 64-битными ключами на транзисторах потребляет мощность 0.18 мкВт/бит при 50% показателях уникальности и единообразия. Показано, что воспроизводимость этого варианта ФНФ не зависит от процессов старения ИС и уровня топологических норм 45-нм, 65-нм и 90-нм.

В работе [3] предложен каскад из трех ступеней по 20 КМОП-инверторов и транзисторов в диодном включении, формирующих делитель напряжения, выходное напряжение которого зависит от вариаций порогового напряжения. Данная ФНФ продемонстрировала inter-HD ≈ 50.65%, intra-HD ≈ 6.96%. За счет работы ниже порогового напряжения схема демонстрирует низкое энергопотребление (не более 0.43 пДж/бит), однако чувствительна к шуму компаратора. Для повышения надежности распознавания авторы использовали усреднение по 15-кратным выборкам.

Следует отметить, что эти характеристики могут быть изменены в условиях повышенного шума, например, из-за изменения параметров библиотечных элементов («характеризация по углам»: вариации технологического процесса, рабочего напряжения и температуры – process, voltage, temperature, PVT) или из-за старения активного устройства, что приводит к проблемам с надежностью ответов ФНФ.

Точное измерение разности номинально идентичных токов при открытии транзисторов выполнено в [4] при помощи специализированного элемента аппаратной реализации искусственных нейронных сетей WTA (winner takes all), выступающего в роли арбитра. Получены значения intra-HD ≈ 1.57%, inter-HD ≈ 49.8% и надежности 97.7% в диапазоне температур от −20°C до +120°C и варьировании напряжения питания ±300 мВ. Энергия потребления схемы составила 5.67 пДж/бит. В усовершенствованном варианте этой схемы, реализованной в топологии 130 нм, для надежного поддержания рабочей точки на уровне около 50 нА применяется пара каскодных токовых зеркал с двукратным gain-boosting[12] усилением, что увеличивает выходное сопротивление. В результате нестабильность бита не превышает 1.56% в диапазоне изменений питающих напряжений 0.6–2 В и температуры 0–75 °C, а intra-HD в среднем не превышает 0.49% при практически идеальной уникальности (inter-HD ≈ 50%), что вместе с энергией 5.36 фДж/бит и площадью 72 мкм²/бит делает ячейку особенно привлекательной для встраивания в модули интернета вещей. Эксперименты на 21 кристалле по 128 бит подтверждают статистическую устойчивость решения и демонстрируют один из лучших совокупных показателей обобщающего фактора качества ФНФ FOM[13] = 17 отн. ед., сохраняя простоту интеграции в ИС и возможность дальнейшего масштабирования.

[10] Intra-Hamming distance – внутреннее расстояние Хэмминга.
[11] Inter-Hamming distance – внешнее расстояние Хэмминга.
[12] Gain-boosting – прием аналоговой схемотехники, при котором вспомогательное усиление в петле обратной связи повышает эффективное усиление каскодного узла, что приводит к увеличению его выходного сопротивления. [Gain-boosting is an analog circuit technique in which auxiliary gain in the feedback loop increases the effective gain of the cascade node, thereby increasing its output resistance.]
[13] Figure of merit.

В работе [5] реализован другой вариант аналоговой диодной ФНФ, в котором сигнатура устройства формируется из диодов, присутствующих в выходных портах ИС. Для повышения уникальности сигнатур предусмотрены меры компенсации перепадов температуры и потерь в подводящих проводниках.

В другой работе [6], также посвященной реализации ФНФ на основе диодных структур в ИС, продемонстрировано, что вызванные технологическим процессом нелинейные изменения проводимости диодов Шоттки на основе оксидных полупроводников обеспечивают подходящий источник энтропии для реализации ФНФ без операции переключения. Показано, что, используя мягкую обработку кислородной плазмой, можно частично устранить область накопления электронов, которая естественным образом образуется в оксидной полупроводниковой пленке, что приводит к значительному изменению нелинейности как экзотического источника энтропии. Диоды Шоттки, обработанные мягкой плазмой, показали почти идеальную однородность и уникальность в среднем на 50%, а также идеальное значение энтропии без необходимости в дополнительной площади оборудования и затратах электроэнергии. Подчеркивается, что эти результаты являются перспективными вариантами для разработки встроенных в аппаратное обеспечение ФНФ, обеспечивающих реализацию энергоэффективного криптографического оборудования.

ФНФ на основе схем с квазиадиабатической логикой (QUAL-PUF) формируется из составных конденсаторных и транзисторных компонентов адиабатической логической схемы (энергоэффективной системы, которая основана на преобразовании в сигнал заряда, накопленного в нагрузочном конденсаторе после выполнения операций), обусловленной изменениями в технологии на этапе производства. Схемы, допускающие такую полную рециркуляцию, как правило, сложны и имеют большую площадь, поэтому в работе [7] используется квазиадиабатическая схема, которая восстанавливает только большую часть заряда конденсатора. Как показано на рис. 2, в этой реализации ФНФ к двум теоретически идентичным транзисторным элементам в схеме подается повышающееся напряжение.

Различия, возникающие при производстве, приводят к несоответствию параметров транзисторов, в результате чего один из них обладает большей проводимостью и быстрее заряжает нагрузочный конденсатор. Это создает устойчивый бит отклика каждой элементарной ячейки схемы, аналогично эффекту рассогласования МОП-транзисторов в традиционных ФНФ. Поскольку адиабатическая логика работает в определенных циклах зарядки/разрядки, уникальной особенностью данной реализации является то, что любая ячейка ФНФ оценивается только на одном из четырех одинаковых временных интервалов. Чтобы учесть это, каждая битовая единица ФНФ состоит из четырех таких ячеек, работающих с временным сдвигом на четверть такта. Сказанное иллюстрируется рис. 3, где изображена реализация модуля 4-разрядной адиабатической ФНФ, составленной из четырех QUAL-PUF.

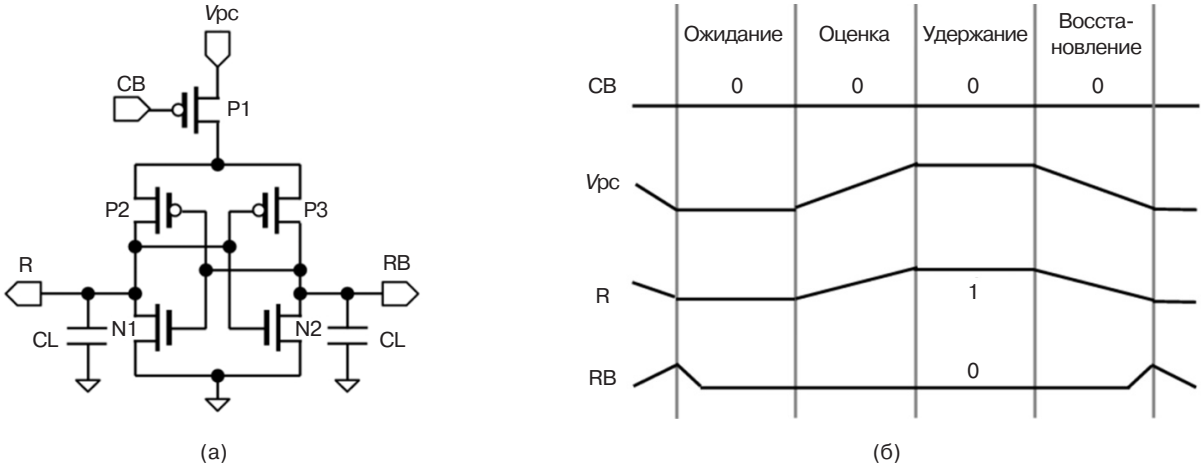


Рис. 2. ФНФ на основе схем QUAL-PUF [7].
(а) QUAL-PUF; (б) временная диаграмма.
*V*pc (power clock) – питающий тактовый сигнал, CB (challenge bit) – бит запроса, P1 – управляющий транзистор, P2 и P3 – *p*-МОП[14]-транзисторы бистабильного элемента, R (response) – основной бит отклика, RB (response bit) – комплементарный выход бита отклика, N1 и N2 – *n*-МОП-транзисторы бистабильного элемента, CL – эквивалентная нагрузочная емкость выходного узла

[14] Металл – оксид – полупроводник. [Metal–oxide–semiconductor.]

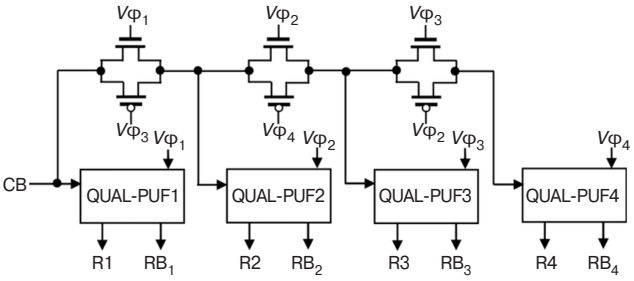


Рис. 3. Модуль 4-разрядной адиабатической ФНФ, составленной из четырех QUAL-PUF [7]

Каждая элементарная ячейка управляется битом запроса CB, задающим процесс инициализации, и четырьмя тактовыми импульсами $V\varphi_1$ – $V\varphi_4$, представляющими собой трапецеидальные power-clock сигналы квазиадиабатической логики, сдвинутые по фазе на 90°. Эти фазы соответствуют состояниям ожидания, оценки, удержания и восстановления. Каждый локальный блок QUAL-PUF1 – QUAL-PUF4 формирует пару выходных сигналов – основной бит отклика R1 – R4 и его комплементарный выход RB_1 – RB_4. Связи между блоками осуществляются проходными ключами, управляемыми соответствующими фазовыми сигналами $V\varphi_i$, что обеспечивает последовательные циклы зарядки и восстановления энергии нагрузки.

Если первая ячейка, как показано на рис. 3, работает в фазе удержания, то следующая – в фазе восстановления, а две остальные – в фазах ожидания и оценки соответственно. Одновременная выборка всех четырех выходов позволяет получить четыре бита отклика. При выборке в разные фазы тактового сигнала формируются различные комбинации битов, что дает возможность четырем модулям ФНФ генерировать до 16 бит отклика, при этом в каждом модуле содержится четыре повторяющихся случайных бита. Такая структура значительно усложняет моделирование ФНФ потенциальным злоумышленником.

В работе [7] приведен пример такой реализации ФНФ 4-разрядного маломощного чипа с памятью по схеме 6T адиабатической ячейки памяти, изготовленной по стандартному КМОП-процессу 0.18 мкм с напряжением питания 1.8 В. Размеры модуля – 58.7 × 5.7 мкм. Результаты моделирования показывают, что значение inter-HD составляет 47.58%, надежность – 95.10%, а рассеиваемая энергия – 29.73 фДж/бит/цикл .

Эти результаты подтверждены в более поздних реализациях аналогичной схемы [8], в которых показано, что при моделировании такая ФНФ обеспечивает среднюю надежность в 98.51% при колебаниях температуры и напряжения питания, при уникальности 49.75% и потреблении 15.92 фДж/бит/цикл. Эти оценки хорошо согласуются с результатами измерений изготовленных образцов, которые продемонстрировали требуемую функциональность ФНФ и надежность 96.92% при комнатной температуре.

Пример схемы на основе адиабатической SRAM с использованием КМОП-технологии 0.18 мкм, которая потребляет меньше энергии, чем обычные ФНФ на основе памяти, и обладает хорошей уникальностью и надежностью, приведен также в работе [9]. При моделировании SPICE[15] потребление энергии предложенной схемы составляет 13.88 фДж/бит/цикл, а значения уникальности и надежности при подключении схемы ФНФ в 4-битном каскоде составляют 50.07% и 99.51% соответственно.

ФНФ НА ОСНОВЕ ПАССИВНЫХ УСТРОЙСТВ

К аналоговым ФНФ можно также отнести пассивные устройства, в которых используются статистические вариации пассивных элементов или структур, формирующие постоянный уникальный «отпечаток» устройства. Пассивные ФНФ обычно не требуют подачи специального стимулирующего сигнала, их случайные параметры заложены в структуре изначально и считываются напрямую.

Ниже рассматриваются три примера пассивных ФНФ: 1) на основе вариаций сопротивления проводников, 2) на основе переходных отверстий (Via PUF) и 3) ФНФ с использованием защитного покрытия (Coating PUF).

Различия в картах распределения мощности в ИС, вызванные вариациями при изготовлении соединений компонентов, также могут служить признаками уникальности конкретного экземпляра. Для реализации ФНФ в этом случае в устройство добавляют дополнительные компоненты, так что каждая ветвь сети распределения электроэнергии может быть подсоединена к шине земли, минуя уже существующие компоненты. Чтобы сформировать сигнатуру устройства, измеряются падения напряжений этих участков цепи (или значения сопротивления). Незначительные флуктуации толщины, ширины и зернистости металла при производстве приводят к тому, что сопротивления сегментов питающей шины слегка различаются от кристалла к кристаллу. Считывание может осуществляться путем подачи тестовых токов через определенные участки силовой сети и измерения возникающих падений напряжения, которые зависят от суммарного сопротивления цепи. Комбинируя результаты нескольких таких

[15] Simulation program with integrated circuit emphasis – симулятор электронных схем общего назначения с открытым исходным кодом. [Simulation Program with Integrated Circuit Emphasis (SPICE) is an open-source simulator for general-purpose electronic circuits.]

измерений, формируется уникальный вектор ответов, характеризующий данный экземпляр микросхемы. Запрос заключается в количестве или расположении участков схемы, а ответ – в соответствующем значении падения напряжения или сопротивления. Пример такой разработки представлен в [10], где приводятся результаты измерения изменений эквивалентных сопротивлений в системе распределения питания двадцати четырех идентичных микросхем, изготовленных по 65-нм технологии.

Поскольку в основе лежат пассивные металлические структуры, резистивная ФНФ обладает высокой стабильностью к внешним условиям. Вариации сопротивления металла линейно зависят от температуры и слабо зависят от напряжения питания, что упрощает компенсацию внешних воздействий по сравнению с транзисторными эффектами. В частности, транзисторным (активным) ФНФ обычно требуются калибровки или алгоритмы коррекции для учета изменений PVT-параметров, тогда как пассивная металлическая сеть обеспечивает более воспроизводимые результаты без сложной подстройки. Кроме того, использование уже существующей в каждом чипе распределенной сети питания означает минимальные накладные расходы по площади – добавляются лишь схемы для опроса и оцифровки отклика. Распределенный характер металлической решетки создает широкий разброс статистических вариаций по разным участкам, что повышает уникальность: вероятность того, что два чипа случайно дадут одинаковый «резистивный» отпечаток, пренебрежимо мала. Преимущество такой ФНФ и в аппаратной устойчивости – правильно спроектированная металлизация не деградирует со временем (электромиграция устранена подбором размеров проводников). Сложность подделки тоже высока: попытаться скопировать сопротивления во всех узлах питания «клона» практически невозможно без воспроизведения полного технологического процесса оригинала. К ограничениям данного подхода можно отнести относительно небольшой объем генерируемых данных (как правило, получается уникальный ключ/ID, хотя можно варьировать точки измерения для получения нескольких бит), а также необходимость прецизионных аналоговых измерений малых разниц сопротивлений. Тем не менее, экспериментальные образцы резистивной ФНФ показали жизнеспособность: например, в 65-нм КМОП по разбросам силовой сети удалось надежно различать все 36 испытанных кристаллов.

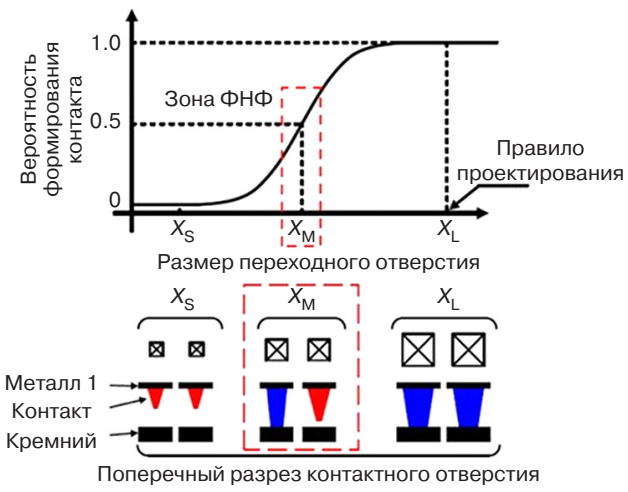
В работе [10], описывающей аналоговую ФНФ, предложено фиксировать перепады напряжения и эквивалентные сопротивления в цепях питания микросхем, поскольку на эти электрические параметры влияют случайные факторы технологии изготовления. Результаты экспериментов на чипах, изготовленных по 65-нм КМОП-технологии, показали, что при измерениях эквивалентных сопротивлений количественные характеристики μ_{intra} и μ_{inter} составляют примерно 0.04 и 1.5 Ом соответственно.

Идея ФНФ на основе вариаций формирования переходных отверстий (Via PUF) состоит в преднамеренном нарушении проектных норм переходных отверстий в топологии ИС: используются размеры немного меньше минимально допустимых. При точном размере каждое отверстие имеет порядка 50% шанса успешно заполниться металлом и образовать соединение между слоями либо остаться разомкнутым [11]. Эти события происходят случайно вследствие неконтролируемых флуктуаций технологического процесса. В результате после изготовления чипа множество заложенных в него соединений оказываются либо проводящими («1»), либо обрывом («0»), формируя уникальный для кристалла шаблон. Считывание Via PUF осуществляется посредством измерения сопротивления заложенных контактов: высокое сопротивление свидетельствует об отсутствии металлического соединения («0»), низкое – о сформированном контакте («1»). Важным достоинством данного подхода является исключительная надежность: контакт либо сформировался, либо нет, и металлическое соединение не подвержено влиянию изменений температуры или напряжения питания. Экспериментально показано, что битовая ошибка (bit error rate, BER) практически нулевая, поэтому для ФНФ на основе формирования переходных отверстий не требуется коррекция ошибок с помощью избыточных кодов. Дополнительная обработка, например, двухступенчатое XOR-преобразование, применяется для устранения смещений и достижения лучшей равномерности битов. Преимущества Via PUF включают также высокую уникальность отпечатков (межкристальные расстояния Хэмминга ~50%) и устойчивость к старению. Благодаря тому, что подобные «случайные» контакты можно распределить по всему кристаллу среди обычных переходных отверстий, затрудняется их обнаружение при обратном проектировании чипа злоумышленником. Кроме того, реализация не требует нестандартных технологических процессов – используются стандартные слои и материалы КМОП, добавляются лишь «заложенные» контакты особого размера. К ограничениям Via PUF можно отнести то, что число генерируемых бит фиксировано схемой (обычно выступает как уникальный идентификатор, а не многоразовый challenge-response), а также необходимость калибровать размер отверстий под конкретный техпроцесс для обеспечения ~50% вероятности заполнения и отбраковывать пограничные случаи во избежание нестабильных битов.

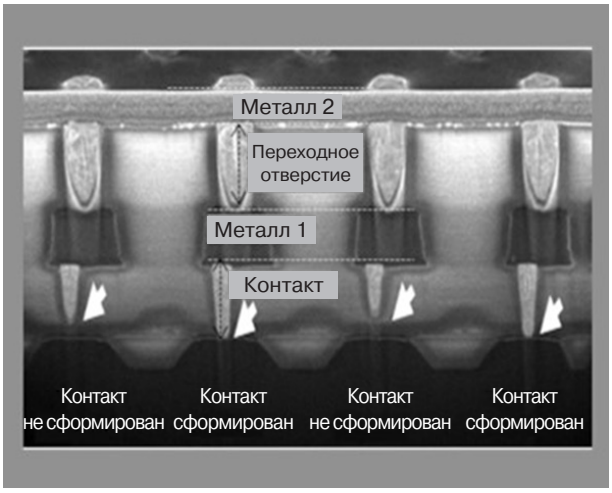
В работе[16], посвященной способам повышения доверенности системы на кристалле на базе микропроцессоров на базе ядра Arm Cortex-M4 (производитель – Arm, Великобритания), в обосновании выбранного способа формирования ФНФ отмечается, что существует средняя по размеру зона (условно именуемая как зона ФНФ), в которой вероятность образования сквозного отверстия или контакта составляет 50%, если размер сквозного отверстия или контактного отверстия меньше, чем обычно задается при проектировании (рис. 4а).

Микроскопическое изображение кремния Via PUF в поперечном сечении показано на рис. 4б, где отчетливо видны контактные отверстия разного качества: 1) контакт разомкнут если не обеспечивает соединения с кремниевой подложкой; 2) контакт закорочен, если он обеспечивает электрическое соединение между слоями. Для формирования ФНФ после завершения изготовления требуется исключение из рассмотрения отверстий, которые являются слабыми с точки зрения надежности, путем измерения сопротивления сквозного или контактного соединения. Например, в одном технологическом узле сопротивление более 1 МОм идентифицируется как «разрыв цепи», а сопротивление менее 50 кОм – как «замыкание», в то время как все отверстия, которые находятся между этими двумя значениями, отсекаются. При этом значения отключения подбираются отдельно для каждого технологического процесса. Как только соединение классифицируется как короткое замыкание или обрыв, оно остается неизменным независимо от изменения PVT, что гарантирует нулевое значение битовых ошибок (BER). Это важная характеристика Via PUF, подтверждающая надежность технологии.

Как отмечено выше, достижение полной случайности имеет решающее значение для ФНФ, где идеальная случайность определяется расстоянием Хэмминга, равным 0.5 или 50%. Для повышения надежности в этой работе применен двухэтапный отбор по критерию XOR (рис. 5). Было изготовлено 405 тестовых чипов, в которых было сформировано 16 различных размеров отверстий по 7680 бит на каждый размер отверстия, что в общей сложности составляет 122800 бит исходных данных для ФНФ. Первый этап XOR сокращает их до 7680 бит, которые проходят через второй этап XOR, генерируя 640 бит в качестве конечного результата, при котором достигается значение μ_{inter} = 0.4972 при стандартном отклонении σ_{inter} = 0.0205. Рисунок 5 иллюстрирует отбор чипов с Via PUF по результатам стандартных тестов на случайность SP 800-22 и SP 800-90B Национального института стандартов и технологий США[17].



(а)



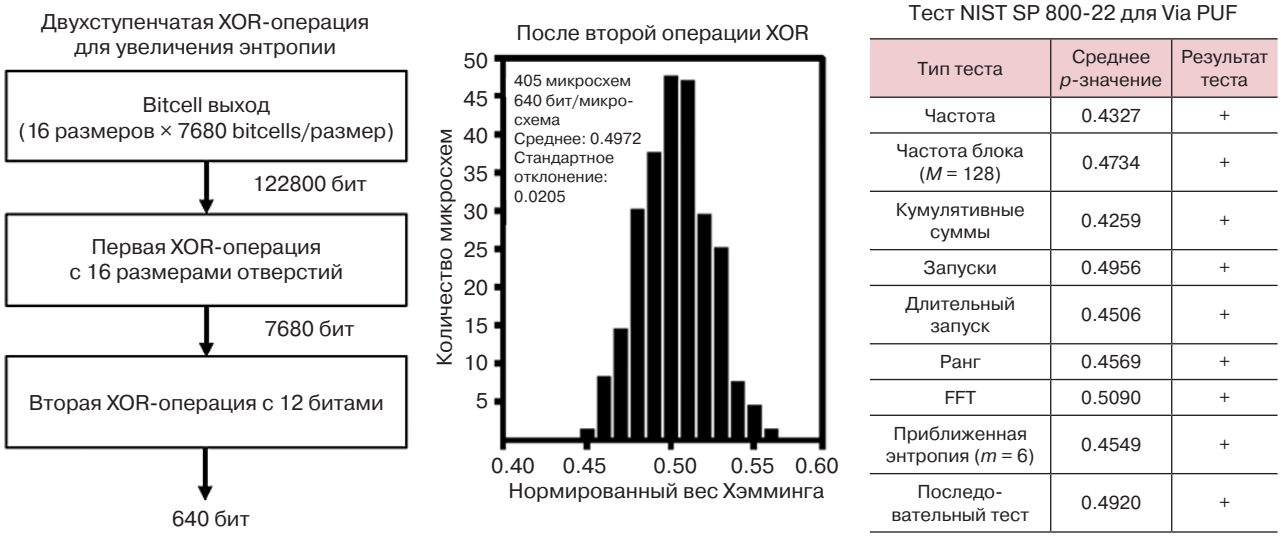
(б)

Рис. 4. Реализация ФНФ на основе вариаций формирования переходных отверстий:
(а) вероятности формирования контакта в зависимости от размера переходного отверстия;
(б) поперечный разрез микроскопического изображения Via PUF[18].
X_S – размер переходного отверстия, при котором контакт не формируется;
X_L – размер переходного отверстия, определенный правилами проектирования;
X_M – промежуточный размер переходного отверстия,
при котором формирование контакта имеет вероятностный характер

[16] Lee T.K. *Via PUF technology as a root of trust in IoT supply chain*. Global Semiconductor Alliance; 2024. https://www.gsaglobal.org/forums/via-puf-technology-as-a-root-of-trust-in-iot-supply-chain. Дата обращения 16.06.2025. / Accessed June 16, 2025.

[17] The National Institute of Standards and Technology, NIST. https://www.nist.gov/. Дата обращения 16.06.2025. / Accessed June 16, 2025.

[18] Там же. [*Ibid.*]



Тест NIST SP 800-22 для Via PUF

Тип теста	Среднее *p*-значение	Результат теста
Частота	0.4327	+
Частота блока (M = 128)	0.4734	+
Кумулятивные суммы	0.4259	+
Запуски	0.4956	+
Длительный запуск	0.4506	+
Ранг	0.4569	+
FFT	0.5090	+
Приближенная энтропия (m = 6)	0.4549	+
Последо-вательный тест	0.4920	+

(в)

Рис. 5. Алгоритм двухэтапного отбора Via PUF по критерию XOR и результаты тестов NIST[19]. FFT (fast Fourier transform) – быстрое преобразование Фурье, M – длина блока в тесте частоты в пределах блока, m – длина битового шаблона в тесте приблизительной энтропии. Блок представляет собой фрагмент битовой последовательности фиксированной длины, на которые тест NIST делит всю проверяемую последовательность

Аналогичная ФНФ, использующая бинарный ответ на уникальность (LRR-DPUF[20]), основана на вариациях литографии межсоединений, также используется в работе [12].

ФНФ на основе защитного покрытия (Coating PUF) использует внешнее случайное диэлектрическое покрытие, наносимое поверх кристалла, для формирования уникального отпечатка. Классическая реализация была предложена в работах [13, 14]: поверх ИС располагается решетка из металлических проводников (например, гребенчатая структура электродов), а все пространство между ними заливается оптически непрозрачным полимером, в который заранее добавлены случайно распределенные диэлектрические наночастицы. Благодаря хаотичному расположению, размерам и диэлектрическим свойствам этих частиц, электрическая емкость между каждой парой проводников является случайной величиной. Иными словами, номинально одинаковые конденсаторы, образованные верхними проводниками, приобретают разброс значений емкости, уникальный для каждого экземпляра микросхемы. Считывая множество таких конденсаторов (например, с помощью измерения токов утечки или временных постоянных заряда/разряда), можно получить набор случайных бит, зависящий от локальных вариаций диэлектрической проницаемости покрытия. Эти биты составляют уникальный идентификатор устройства, физически неклонируемый ввиду неповторимости распределения частиц в слое покрытия.

В работе [15] показано, что при нанесении непрозрачного и химически инертного слоя диэлектрика на верхний слой металлизации ИС измерения значений электрических емкостей участков цепи относительно других участков или земли питания носят случайный характер, индивидуальный для каждого экземпляра чипа. Схему реализации и принцип работы ФНФ на основе покрытия иллюстрирует рис. 6.

Оцифрованные результаты измерения на 36 изготовленных чипах, в каждом из которых тестировался 31 емкостный датчик, показали высокую степень случайности ($\mu_{inter} \approx 50\%$) и низкий уровень шума ($\mu_{intra} < 5\%$).

ФНФ на основе защитного покрытия обладает двумя важными достоинствами. Во-первых, улучшается аппаратная защищенность кристалла: непрозрачный верхний слой препятствует прямому оптическому изучению и считыванию внутренних схем, действуя как защитная маска. Любая попытка снять или повредить этот слой неизбежно изменит распределение частиц и емкости, что уничтожит исходный «отпечаток» устройства. Таким образом, Coating PUF не только предоставляет уникальный ключ, но и служит своего рода сенсором вскрытия – при вмешательстве оригинальный идентификатор теряется, выявляя факт взлома. Во-вторых, благодаря крупномасштабному случайному процессу

[19] Lee T.K. Via PUF technology as a root of trust in IoT supply chain. Global Semiconductor Alliance; 2024. https://www.gsaglobal.org/forums/via-puf-technology-as-a-root-of-trust-in-iot-supply-chain. Дата обращения 16.06.2025. / Accessed June 16, 2025.

[20] Learning resilient and reliable digital PUF – устойчивая к обучению надежная цифровая ФНФ.

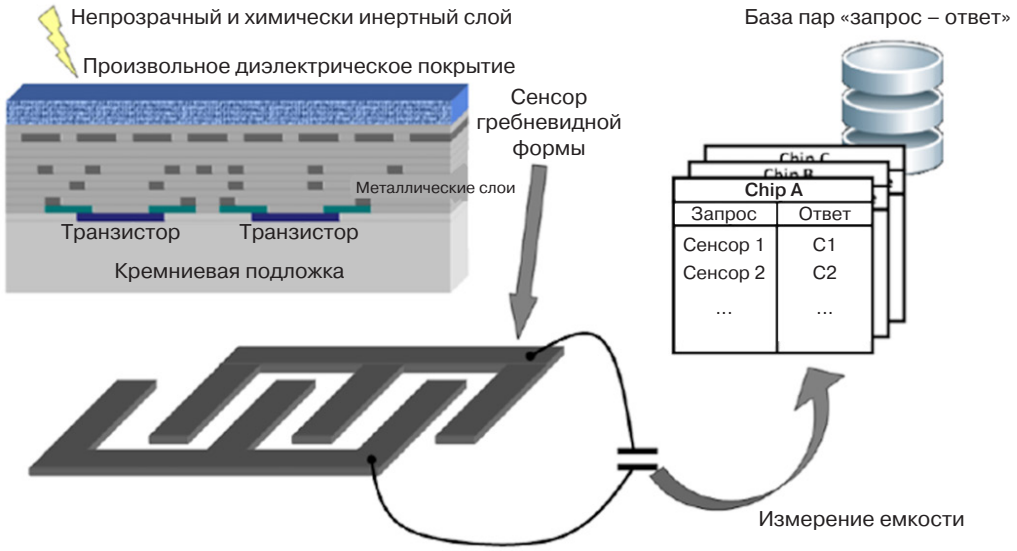


Рис. 6. Пример реализации пассивной ФНФ на основе инертного слоя диэлектрика [14]

формирования (смешивание миллионов частиц), вероятность совпадения двух таких ФНФ крайне мала, а воспроизведение требует копирования процессов на атомарном уровне, что практически невыполнимо. Из недостатков отмечается необходимость дополнительной технологической стадии при изготовлении – нанесение и отверждение специального покрытия, что увеличивает себестоимость. Кроме того, для чтения отпечатка нужны аналоговые схемы или внешние измерения с высокой точностью, а сами измерения могут зависеть от внешних условий (например, температуры, влияющей на диэлектрик). Устройства с Coating PUF продемонстрировали жизнеспособность в системах аутентификации, в частности, при реализации метки RFID[21], где случайное эпоксидное покрытие используется как источник 128-битного ключа, уничтожающегося при попытке физического доступа.

В таблице обобщены данные публикаций, в которых приводятся оригинальные результаты по реализации ФНФ на основе аналоговых схем и схем с вариациями переходных отверстий. В качестве ключевых метрик выбраны: расстояние между двумя ответами ФНФ от разных экземпляров ФНФ, использующих один и тот же вызов – inter-HD, и расстояние между двумя ответами ФНФ, полученными от одного и того же экземпляра ФНФ и использующими один и тот же вызов – intra-HD. В ряде публикаций они имеют названия уникальность (uniqueness) и надежность (reliability), соответственно.

Таблица. Характеристики аналоговых и пассивных ФНФ

Тип ФНФ / ссылка	Год публикации	Характеристики ФНФ					
		Inter-HD	Intra-HD	Платформа	Чувствительность к внешним условиям		Оценочная сложность реализации
					Температура	Напряжение	
Subthreshold[22] [3]	2019	50.65%	~7%	SPICE model TSMC 65 нм КМОП	От −20°C до 85°C	0.75–0.9 В	Высокая
Current Mirror[23] [4]	2023	49.84%	1.57%	SPICE model TSMC 65 нм КМОП	От −20°C до 120°C	±300 мВ	Высокая
Adiabatic SRAM[24] [7]	2020	47.58%	4.9%	ASIC 180 нм КМОП	От −40°C до 100°C	1.8 В	Средняя
6T Adiabatic[25] [8]	2024	49.75%	1.49%	ASIC 180 нм КМОП	От −40°C до 100°C	0.9–1.8 В	Средняя

[21] Radio frequency identification – радиочастотная идентификация.
[22] Субпороговая ФНФ.
[23] ФНФ, основанные на реализации массива токовых зеркал. [PUF based on the use of an array of current mirrors.]
[24] Тип SRAM, в котором используется технология адиабатического восстановления энергии. [A type of SRAM that employs adiabatic energy recovery methods.]
[25] 6-транзисторная ФНФ, основанная на принципах адиабатической логики. [A six-transistor PUF that operates on adiabatic logic principles.]

Таблица. Продолжение

Тип ФНФ / ссылка	Год публикации	Характеристики ФНФ					
		Inter-HD	Intra-HD	Платформа	Чувствительность к внешним условиям		Оценочная сложность реализации
					Температура	Напряжение	
Adiabatic Logic[26] [9]	2024	50.07%	0.49%	ASIC 180 нм КМОП	От −50°C до 100°C	–	Средняя
Via[27] [11]	2020	49.99%	~0%	ASIC 130 нм КМОП	От −55°C до 125°C	1.65 В	Низкая

В данной таблице 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. Оценочная сложность реализации (высокая, средняя, низкая) характеризует 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.).

НАРУШЕНИЕ БЕЗОПАСНОСТИ ФНФ НА ОСНОВЕ МЕТОДОВ ML

Стремительное развитие методов ML в корне изменило представление о безопасности ФНФ. Уязвимость ФНФ к атакам на основе ML послужила причиной обширных исследований как методологий атак, так и механизмов защиты [3, 16–19]. Эти атаки представляют собой смену парадигмы в анализе безопасности ФНФ, переход от традиционных криптоаналитических подходов к методам моделирования на основе данных, которые используют закономерности, присущие парам «запрос – ответ» ФНФ.

Исследователи разрабатывают все более сложные стратегии атак с использованием методов ML противника [17, 20], одновременно предлагая новые архитектуры и протоколы ФНФ, предназначенные для противостояния таким атакам [3, 18, 19]. В данном разделе представлен анализ текущего состояния атак и защиты от ML в системах ФНФ на основе последних достижений как в методологии атак, так и в стратегиях противодействия. Рассматриваются теоретические основы безопасности ФНФ, анализируются различные категории атак на основе ML, оцениваются предложенные механизмы защиты и обсуждаются последствия для будущих разработок и стратегий развертывания ФНФ.

Архитектуры ФНФ и свойства безопасности

ФНФ можно разделить на две категории, основываясь на их поведении в режиме «запрос – ответ»: сильные и слабые [21]. Сильные ФНФ характеризуются способностью генерировать большое количество пар «запрос – ответ», что делает их подходящими для протоколов аутентификации, в которых можно использовать несколько CRP без исчерпания доступного пространства запросов. В качестве примеров можно привести ФНФ типа «арбитр», ФНФ с кольцевым генератором и различные композитные архитектуры [17–19]. Слабые ФНФ, напротив, имеют ограниченное пространство запросов и обычно используются для генерации ключей, где извлекается один или несколько ответов и обрабатывается через механизмы коррекции ошибок [22].

ФНФ типа «арбитр» (Arbiter PUF, A-PUF) представляет собой одну из наиболее изученных архитектур сильных ФНФ, использующих разницу в задержках между двумя номинально идентичными путями передачи сигнала для генерации ответа [16, 18]. Биты запроса управляют переключающими элементами, которые определяют конфигурацию пути, а схема арбитра в конце определяет, какой путь быстрее, создавая двоичный ответ. Несмотря на концептуальную простоту, ФНФ этого типа оказалась уязвимой для различных атак с применением машинного обучения (ML-атак) из-за линейной аддитивной модели задержки [17, 19]. Для повышения безопасности от ML-атак разработаны более сложные архитектуры [18, 19, 22], которые представляют собой попытки фундаментально изменить математические отношения между входами и выходами, чтобы предотвратить эффективное моделирование ML.

Важнейшим аспектом реализации ФНФ является обработка шумов, присущих ответам ФНФ, вызванных колебаниями окружающей среды, старением и погрешностями измерений [16, 22]. Механизмы исправления ошибок, обычно реализуемые с помощью

[26] ФНФ, основанная на принципах адиабатической логики. [PUF based on adiabatic logic.]

[27] ФНФ, основанная на вариациях процесса формирования переходных отверстий. [PUF derived from variations in the formation of vias.]

нечетких экстракторов или алгоритмов вспомогательных данных, необходимы для надежной генерации ключей и аутентификации. Наиболее распространенный подход заключается в хранении вспомогательных данных, которые позволяют корректировать зашумленные ответы ФНФ без раскрытия фактических значений ответов. Однако недавние исследования показали, что вспомогательные данные могут способствовать утечке значительной информации об ответах ФНФ, позволяя осуществлять ML-атаки даже в тех случаях, когда фактические значения ответов недоступны [22]. Это представляет собой фундаментальную уязвимость в системах на основе ФНФ, использующих стандартные подходы к исправлению ошибок, особенно при использовании линейных блочных кодов, таких как коды повторения.

Применение ML для атак на ФНФ

Уязвимость ФНФ к атакам с применением ML впервые была продемонстрирована на примере классических методов ML, примененных к A-PUF и их разновидностям [3, 17]. Эффективность этих атак обусловлена фундаментальными математическими соотношениями, лежащими в основе конструкций ФНФ. Для A-PUF разница задержек может быть смоделирована как линейная функция битов запросов и параметров задержки, что делает их восприимчивыми к методам линейной классификации [16, 17]. Даже если сложность увеличивается за счет операций XOR или других нелинейных преобразований, базовая структура часто остается изучаемой с помощью соответствующих алгоритмов ML. Классические A-PUF, как правило, можно смоделировать с точностью более 95%, используя менее 10000 пар «запрос – ответ» и стандартные методы логистической регрессии. Линейный характер модели задержки делает эти ФНФ особенно уязвимыми для математического анализа и ML-моделирования.

Модели глубокого обучения могут автоматически обнаруживать релевантные признаки и нелинейные взаимосвязи в данных об ответах на запросы, устраняя необходимость в ручном подборе признаков. Атаки на основе глубокого обучения демонстрируют превосходную производительность на всех протестированных архитектурах по сравнению с классическими подходами ML. Конволюционные нейронные сети (convolutional neural networks, CNN) и многослойные перцептроны (multilayer perceptrons, MLP) также продемонстрировали более высокую производительность по сравнению с классическими подходами ML, особенно против сложных архитектур ФНФ, разработанных для защиты от традиционных атак [3, 17]. Конволюционные нейронные сети достигают точности моделирования выше 90% для различных типов ФНФ, требуя при этом меньшего количества обучающих образцов, чем традиционные методы. Это говорит о том, что сложность современных алгоритмов ML опережает защитные возможности текущих конструкций ФНФ.

Также были исследованы методы трансферного обучения, когда модели, обученные на одном экземпляре ФНФ или архитектуре, адаптируются для атак на различные ФНФ [21]. Такой подход позволяет сократить объем обучающих данных, необходимых для успешных атак, и продемонстрировать обобщенность моделей ФНФ, обученных на схожих архитектурах.

Эволюционные стратегии, в частности, стратегия эволюции адаптации ковариационной матрицы, доказали свою эффективность ML-атак в борьбе с более сложными конструкциями ФНФ [17, 21]. Эти методы позволяют моделировать поведение ФНФ путем эволюции популяций моделей-кандидатов и отбора тех, которые лучше всего соответствуют наблюдаемым данным о реакции на запрос. Гибкость эволюционных подходов делает их особенно опасными для ФНФ со сложной внутренней структурой.

Один из особенно сложных подходов включает использование сиамских нейронных сетей для моделирования ФНФ путем использования вспомогательных данных [22]. Эта техника использует избыточность, присущую кодам коррекции ошибок, для извлечения обучаемых характеристик и меток без прямого доступа к ответам ФНФ. Применяя отношения XOR в линейных блочных кодах, злоумышленники могут обучать модели для предсказания поведения ФНФ, используя только общедоступные вспомогательные данные и задачи.

Продвинутые стратегии атак вышли за рамки простого моделирования «запрос – ответ» и используют дополнительные источники информации. Атаки на основе надежности используют тот факт, что ответы ФНФ вблизи границ принятия решений более чувствительны к шуму и колебаниям окружающей среды [16, 17]. Анализируя стабильность отклика в ходе многочисленных измерений, злоумышленники могут получить представление о внутренней структуре и параметрах схем ФНФ.

Еще один значительный вектор угроз представляют атаки по побочным каналам, когда физическая информация, такая как энергопотребление, электромагнитные излучения или вариации синхронизации, используется для усиления атак на моделирование ML [21]. Эти атаки могут быть особенно эффективны в сочетании с традиционными подходами ML, обеспечивая дополнительные ограничения и информацию для повышения точности модели.

Объединение нескольких векторов атаки создает особенно мощные угрозы. Например, объединение

информации о частичном ответе с измерениями побочных каналов может значительно сократить количество пар «запрос – ответ», необходимых для успешных ML-атак. Такой мультимодальный подход подчеркивает важность учета всех потенциальных источников утечки информации при анализе безопасности ФНФ.

Потенциальную угрозу будущего, которая может кардинально изменить уровень безопасности ФНФ, представляют собой квантовые вычисления. Хотя текущие квантовые алгоритмы могут не применяться непосредственно к моделированию ФНФ, расширенные вычислительные возможности могут позволить использовать новые стратегии атак или сделать невозможные в настоящее время атаки практическими.

Способы защиты от ML-атак

Для повышения устойчивости ФНФ к атакам, реализуемым с помощью ML, предложено несколько архитектурных инноваций.

Конструкция Cyclic Redundancy Check PUF (CRC-PUF) представляет собой фундаментальный подход, который нарушает прямое сопоставление между запросами и ответами посредством криптографических преобразований [18]. Применяя операции проверки циклической избыточности со случайно выбранными полиномами, CRC-PUF гарантирует, что вероятность восстановления преобразованного запроса криптографически мала, эффективно предотвращая традиционные атаки ML.

В другой архитектуре ФНФ используется механизм двухраундовой обработки запросов, при котором промежуточные ответы используются для модификации последующих запросов [17]. Такой подход скрывает прямую связь между входными запросами и конечными ответами, что значительно усложняет создание предсказательных моделей алгоритмами ML. Рандомизация, вносимая промежуточными этапами обработки, увеличивает эффективное пространство запросов и уменьшает корреляцию между различными парами «запрос – ответ».

Инновации на аппаратном уровне также показали перспективность в противостоянии ML-атакам. Подпороговый ФНФ с делителем напряжения работает в слабых инверсионных областях, где большие колебания порогового напряжения обеспечивают повышенную случайность [3]. Благодаря каскадному соединению нескольких ступеней и тщательному контролю смещения эта конструкция обладает сильными статистическими свойствами, сохраняя устойчивость к различным алгоритмам ML, включая машины опорных векторов, логистическую регрессию и искусственные нейронные сети.

Защитные средства на уровне протокола направлены на ограничение информации, доступной потенциальным злоумышленникам, а не на модификацию базовой архитектуры ФНФ. Стратегии ограничения запросов ограничивают количество пар «запрос – ответ», которые можно наблюдать, не позволяя злоумышленникам накапливать достаточное количество обучающих данных для эффективных ML-атак [16, 21]. Однако такой подход по своей сути ограничивает возможности сильных ФНФ и может оказаться нецелесообразным для приложений, требующих многочисленных операций аутентификации. Для минимизации утечки информации на этапах настройки и эксплуатации ФНФ были разработаны усовершенствованные протоколы регистрации [21, 23]. Эти протоколы тщательно управляют распределением пар «запрос – ответ» и реализуют безопасные методы вычислений для предотвращения несанкционированного доступа к обучающим данным. Многосторонние вычисления и гомоморфное шифрование могут быть использованы для обеспечения работы ФНФ без раскрытия конфиденциальной информации потенциальным злоумышленникам.

Продвинутые методы (рис. 7) предлагают новый подход к защите ФНФ за счет намеренного внесения ошибок в процесс «запрос – ответ» [20]. Отравляя обучающие данные, доступные потенциальным злоумышленникам, эти методы могут значительно снизить точность ML-моделей, сохраняя при этом корректную работу для легитимных пользователей, которые понимают стратегию отравления. Подход заключается в периодическом предоставлении неправильных ответов на запросы, создавая набор данных, который не может быть эффективно изучен стандартными алгоритмами ML.

Последствия использования вспомогательных данных в системах ФНФ для безопасности привели к разработке специализированных подходов к исправлению ошибок [16, 22]. Здесь показано, что традиционные схемы конкатенированного кодирования, особенно использующие коды повторения в качестве внутренних кодов, очень уязвимы для ML-атак с помощью анализа вспомогательных данных. Избыточность таких кодов предоставляет злоумышленникам достаточно информации для обучения эффективных моделей без доступа к реальным ответам ФНФ. Коды с более высокими кодовыми частотами и более сложной структурой лучше противостоят атакам на вспомогательные данные, в то время как простых кодов, такие как коды с повторением, следует избегать в критически важных приложениях [22]. Анализ различных семейств кодов показывает, что количество и сложность отношений XOR в структуре кода напрямую влияют на уязвимость к ML-атакам.

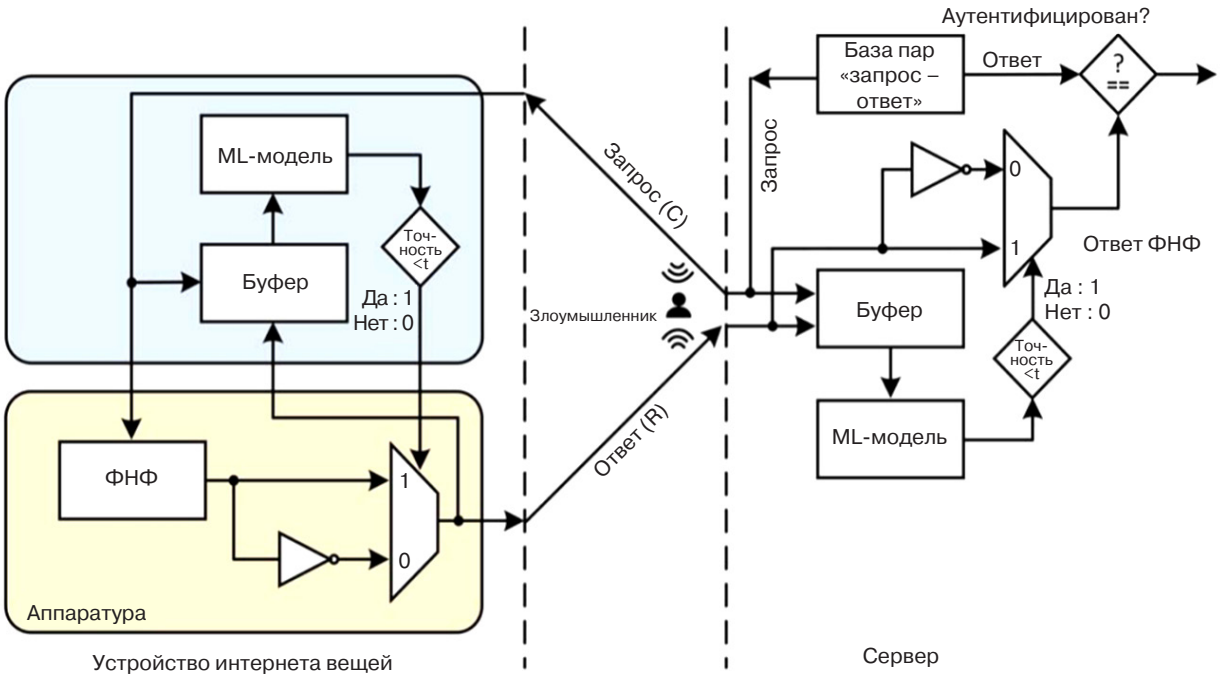


Рис. 7. Блок-схема метода внесения ошибок

Безопасные подходы к исправлению ошибок включают использование методов построения синдромов, систематическое кодирование с низкой утечкой информации и специализированные полярные коды, которые минимизируют утечку информации, сохраняя при этом возможность исправления ошибок [22]. Эти методы направлены на уменьшение корреляции между вспомогательными данными и ответами ФНФ, что затрудняет злоумышленникам извлечение полезной обучающей информации.

Исследования физической реализации позволяют понять практическую эффективность как атак, так и защиты [3, 18, 19]. Так эмпирические исследования различных архитектур ФНФ выявили значительные различия в показателях успешности ML-атак и требуемых объемах обучающих данных. В частности, FPGA[28]-реализация CRC-PUF демонстрирует устойчивость к ML-атакам при сохранении разумных затрат площади и мощности. При разработке были достигнуты нормированные значения inter-HD и intra-HD, равные 0.5065 и 0.0696 соответственно, что свидетельствует о хороших статистических свойствах для приложений безопасности.

Анализ площади и мощности показывает, что ФНФ, устойчивые к ML, могут быть реализованы с разумными затратами по сравнению с классическими архитектурами. Для CRC-PUF требуется 1032 эквивалента вентилей по сравнению с 646 для базового Arbiter PUF, что представляет собой скромное увеличение при значительном повышении безопасности. Аналогично, архитектура MARPUF[29] достигает устойчивости к ML при площади, значительно превышающей практические пределы для встраиваемых приложений.

Более сложные архитектуры демонстрируют разную степень устойчивости ФНФ. Функции типа «арбитр» с несколькими XOR-каскадами требуют экспоненциально возрастающего числа CRP для успешных атак, но остаются уязвимыми к продвинутым техникам при наличии достаточного количества данных [17, 19, 20]. При этом частота успешных атак падает ниже 60% даже в случае применения наборов обучающих данных значительного размера, что представляет собой значительное улучшение по сравнению с классическими конструкциями.

Реализация ФНФ на основе массива подпороговых делителей напряжения в 65-нм КМОП-технологии показывает многообещающие результаты с энергопотреблением всего 0.43 пДж/бит [3]. При воздействии различных ML-атак, включая логистическую регрессию, искусственные нейронные сети и машины опорных векторов с нелинейными RBF[30]-ядрами, точность предсказания остается на уровне около 60%, демонстрируя практическую устойчивость к ML.

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

[29] Physical unclonable function with improved machine learning attack resistance – ФНФ, обеспечивающая устойчивость к атакам машинного обучения.

[30] Radial basis function – радиальная базисная функция.

Направления исследований методов защиты от ML-атак

Разработка ФНФ, устойчивых к ML, связана с компромиссами между безопасностью и практическими соображениями, такими как площадь, мощность, надежность и производительность [3, 18, 19]. Конструкции с высокой степенью защиты часто требуют дополнительной аппаратной сложности, увеличения возможностей коррекции ошибок или снижения производительности, что может быть неприемлемо для приложений, чувствительных к стоимости.

Анализ ML-атак на ФНФ выявляет фундаментальные ограничения в безопасности, обеспечиваемой текущими архитектурами. Многие практические реализации не достигают теоретического максимума энтропии, оставляя место для ML-атак, использующих статистические закономерности [16, 17, 22]. Математические модели, лежащие в основе большинства конструкций ФНФ, по своей сути содержат обучаемые шаблоны, которые могут быть использованы достаточно сложными алгоритмами ML. Это позволяет предположить, что для достижения истинной устойчивости к ML могут потребоваться принципиально иные подходы к проектированию ФНФ, а не постепенные усовершенствования существующих архитектур.

Масштабируемость атак ML представляет собой особую проблему для будущих реализаций ФНФ. По мере того, как алгоритмы ML становятся все более мощными и доступными, барьер для проведения успешных атак продолжает снижаться. Эта тенденция говорит о том, что безопасность ФНФ не может зависеть только от вычислительной сложности моделирования атак, а должна быть направлена на фундаментальные информационно-теоретические принципы безопасности.

Подход с ограничением запроса, хотя и является теоретически обоснованным, сильно ограничивает возможности сильных ФНФ и может оказаться непрактичным для приложений, требующих частой аутентификации или генерации ключей [16, 21]. Это ограничение фактически сводит сильные ФНФ к функциональности слабых ФНФ, устраняя многие из преимуществ, которые изначально мотивировали их разработку.

Требования к исправлению ошибок представляют собой еще одно существенное ограничение. Уязвимость вспомогательных данных, обнаруженная в недавнем исследовании [22], показывает, что даже кажущиеся безопасными подходы к исправлению ошибок могут создавать векторы атак. При выборе подходящих кодов коррекции ошибок теперь необходимо учитывать не только традиционные показатели, такие как возможности коррекции и сложность реализации, но и безопасность от атак ML с помощью анализа вспомогательных данных.

Анализ протоколов аутентификации и обмена ключами на основе ФНФ также показывает различную степень уязвимости к ML-атакам [21, 23]. Традиционные протоколы, основанные на прямом обмене запросами и ответами, очень уязвимы для атак моделирования, если наблюдается достаточное количество CRP. Безопасность этих протоколов в основном зависит от устойчивости ФНФ к ML-атакам, а не от защиты на уровне протокола.

Последние инновации в области протоколов направлены на минимизацию информации, доступной злоумышленникам, при сохранении функциональных требований [23]. Такие методы, как безопасные многосторонние вычисления, гомоморфное шифрование и доказательства с нулевым знанием, позволяют использовать ФНФ без раскрытия пар «запрос – ответ» потенциальным злоумышленникам. Однако эти подходы часто требуют значительных вычислительных затрат, что может быть нецелесообразно для устройств с ограниченными ресурсами. Более сложные протоколы используют обфускацию запросов, маскировку ответов и механизмы временной безопасности для ограничения возможностей злоумышленников [20, 21]. Однако многие из этих подходов оказались недостаточными для борьбы с решительными противниками, имеющими доступ к современным методам ML. Основная проблема заключается в том, чтобы сбалансировать безопасность с практическими ограничениями, такими как затраты на связь, вычислительные требования и устойчивость к ошибкам.

Интеграция ФНФ в сложные системы создает дополнительные направления для атак через анализ побочных каналов, внедрение неисправностей и уязвимости на уровне системы [21]. По мере того, как ФНФ все шире внедряются в критически важные приложения, растет мотивация для сложных атак, что требует более надежного анализа безопасности и механизмов защиты. Таким образом, быстрое развитие методов ML создает постоянные проблемы для безопасности ФНФ. Появляющиеся подходы, такие как ML противника, трансферное обучение и мета-обучение, могут создавать новые стратегии атак, которые не смогут отразить существующие средства защиты [20, 23].

Разработка стандартизированных методик оценки безопасности ФНФ имеет решающее значение для справедливого сравнения различных конструкций и методов атаки [17, 21]. Будущие исследования ФНФ должны быть направлены на разработку архитектур с доказуемыми свойствами безопасности, а не на эмпирическую устойчивость к существующим методам

атак [16, 18]. В существующих оценках часто используются различные наборы данных, параметры атак и метрики успеха, что затрудняет объективную оценку относительных уровней безопасности. Информационно-теоретические подходы, которые могут гарантировать безопасность даже против вычислительно неограниченных противников, обеспечивают более прочный фундамент для долгосрочной безопасности.

Динамика развития систем доверенного проектирования позволяет предположить, что для достижения долгосрочной безопасности необходимо перейти от постепенных улучшений текущих архитектур к принципиально иным подходам, основанным на информационно-теоретических принципах безопасности [24, 25]. Результаты исследования подчеркивают важность тщательного моделирования угроз, консервативных предположений о безопасности и стратегий глубокой защиты для практиков, внедряющих системы на основе ФНФ [26–29].

ПРИМЕРЫ ПРИМЕНЕНИЯ ФНФ

Модули ФНФ используются в широком спектре применений для защиты устройств в зависимости от класса защиты (слабого или стойкого) чипа, встроенного в устройство. Ответы ФНФ могут быть использованы непосредственно для идентификации аналогично тому, как это делается при биометрической идентификации. Как было показано в первой части цикла статей [1], пороговое значение, используемое для принятия решения о положительной идентификации, зависит от гистограмм intra-HD и inter-HD. В общем случае перекрытия соответствующих гистограмм задание порогового значения равносильно компромиссу между частотой ложного подтверждения (false-acceptance rate, FAR) и частотой ложного отклонения (false-rejection rate, FRR), аналогично тому, как это применяется в метрологии. Оптимальный выбор, сводящий к минимуму сумму значений FAR и FRR, достигается путем установки порогового значения на пересечении обеих гистограмм, но для конкретных приложений могут быть желательны и другие компромиссы. Кроме того, очевидно, что уникальная идентификация возможна с высокой вероятностью только в том случае, если ответ содержит достаточную энтропию по отношению к размеру выборки.

ФНФ применяются, в частности, для: 1) взаимной аутентификации устройств интернета вещей [30, 31]; 2) идентификации потока сообщений с запросами аутентификации мобильных беспилотных летательных аппаратов, оснащенных ФНФ и наземными станциями [32, 33]; 3) обеспечения связи между устройствами, датчиками и системой мониторинга состояния здоровья, в которой сервер также оснащен соответствующим ФНФ и используется защищенная база данных для хранения собранных вариантов пар CRP [34]; 4) оснащения средствами защиты и безопасности транспортных средств [35, 36]; 5) обеспечения безопасности и конфиденциальности при передаче данных в сетях [37–39].

Идентификация устройств

На этапе регистрации в базе данных сохраняется CRP от каждой ФНФ, а также идентификационные данные физической системы, в которую она встроена. Как было показано в [1], во время идентификации проверяющий сравнивает случайную пару CRP с хранящимися в базе данных ответами ФНФ для представленной системы. Если наблюдаемый отклик достаточно близок к отклику в базе данных, идентификация выполняется успешно, в противном случае происходит сбой. Чтобы предотвратить повторные атаки, каждая пара CRP должна использоваться только один раз для каждого экземпляра ФНФ и должна быть удалена из базы данных после идентификации (рис. 8 и [40]).

Генерация ключей шифрования

ФНФ генерируется на основе случайности, обусловленной технологическими допусками, и при генерации и хранении секретных ключей на ее основе не требуется ее программирование. Поскольку эта случайность постоянно фиксируется в (суб)микроскопических физических деталях чипа, ключ остается неизменным, может воспроизводиться несколько раз, и не требуется энергонезависимая память ключей, что также обеспечивает дополнительную защиту от атак по сторонним каналам.

Однако ответы ФНФ обычно зашумлены и для извлечения криптографического ключа из ответов требуется промежуточный этап обработки. Эта проблема известна в теории информации как извлечение ключа шифрования из сигнала с шумом и, как правило, решается с помощью двухэтапного алгоритма. На начальном этапе генерации запрашивается ФНФ, и алгоритм создает секретный ключ вместе с некоторой дополнительной информацией, составляющей вспомогательные данные. Ключ и эти данные хранятся в защищенной базе данных независимо от устройства. На этапе воспроизведения эти вспомогательные данные сообщаются алгоритму, который использует их для извлечения из ФНФ того же самого ключа, что был создан на этапе генерации. Эти алгоритмы можно сконструировать таким образом, чтобы ключ был совершенно секретным, даже если вспомогательные данные могут быть открыто переданы. Чтобы обеспечить надежность этого способа генерации ключей, применяются

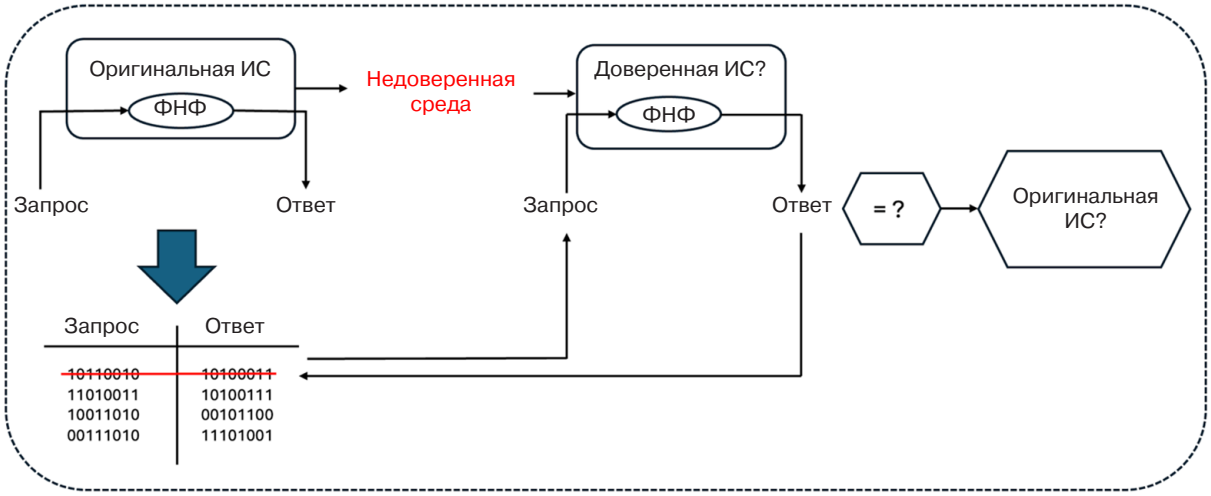


Рис. 8. Применение ФНФ в протоколе аутентификации [40]

специальные способы устранения ошибок [41, 42], в частности, алгоритмы генерации (Gen) и воспроизведения (Rep), обеспечивающие извлечения стабильной воспроизводимой информации из ответов ФНФ, основой которых является сравнение двух сообщений, составленных из зашумленных зашифрованных случайных данных и эталонных, к которым для распознавания присоединены несекретные вспомогательные данные. Практические примеры этих алгоритмов предложены, например, в [43–45].

Таким образом, применение ФНФ позволяет реализовать аппаратно-запутанную криптографию как специальный метод, в котором цифровой ключ шифра не хранится в памяти, а секретным элементом является полное уникальное поведение экземпляра ФНФ во встраиваемом устройстве. Это в значительной степени не позволяет злоумышленникам, использующим энергонезависимую память, получить полезную информацию. Аппаратно-запутанная криптография тесно связана с областью доказуемой физической безопасности, поскольку применение ФНФ может также послужить для доказательства несанкционированного доступа к хранилищу ключей (см, например, [46]).

Защита от реинжиниринга ИС (intellectual property protection)

Объекты интеллектуальной собственности (intellectual property), входящие в состав микросхем, крайне важно защитить от многочисленных угроз безопасности, наносящих финансовые потери полупроводниковым компаниям. Такими угрозами являются, в частности, подделка, клонирование, обратный инжиниринг и зависимость от некачественных компонентов. Примерами исследований в этой области являются работы, посвященные аппаратной защите блока ФНФ SRAM на программируемой логической интегральной схеме, и способ предотвращения копирования IP[31]-адреса программного обеспечения для защиты от несанкционированного доступа к встроенному программному обеспечению, основанные на применении ФНФ и моделей нейронных сетей [47–49].

Генерация случайных чисел

Кремниевые ФНФ используются в качестве источника генерации случайных чисел, формирование которых необходимо для криптографических систем. Характерными примерами исследований в этой области служат работы [50, 51], в которых авторы использовали ответы ФНФ для формирования исходных данных генератора случайных чисел.

Защита платежных систем (payment)

В работах [52, 53] ответы ФНФ используются в битовых строках аутентификации, ключах шифрования и генерации токенов электронной наличности (PUF-Cash) для разработки архитектуры приложений, которую можно использовать в схемах электронных платежей, гарантируя при этом анонимность идентификационных данных пользователей для других организаций, таких как банки и продавцы. В работе [54] предложено снабжать кредитную/дебетовую карту встроенным чипом с ФНФ, обеспечивающим закрытый ключ, безопасную связь и аутентификацию данных.

Защита памяти и программ и обеспечение безопасности коммуникаций

В настоящее время ряд компаний и исследовательских центров специализируются в разработке

[31] Internet protocol – уникальный числовой идентификатор устройства в компьютерной сети.

специальных мер по обеспечению повышенной доверенности оборудования и программного обеспечения. В частности, характерным примером служит техническая документация ассоциации [54], созданной для разработки, определения и продвижения открытых, независимых от поставщиков, глобальных отраслевых стандартов, поддерживающих аппаратную основу доверия для взаимозаменяемых доверенных вычислительных платформ, в которой указывается, что масштабные угрозы безопасности, обусловленные геополитическими проблемами и проблемами, связанными с суверенитетом данных, угрожают замедлить внедрение и рост индустрии интернета вещей и стимулируют необходимость создания надежных экосистем цепочки поставок в Азии, Европе и Северной и Южной Америке. Подчеркивается, что ключи, используемые для цифровой подписи и верификации, а также криптографические функции, обеспечивающие безопасный процесс загрузки операционных систем, являются важным средством обеспечения безопасности всей системы в целом. Отмечается, что главным и единственным эффективным средством, обеспечивающим безопасное функционирование, следует признать применение микросхем, снабженных ФНФ, в частности ФНФ нового типа, разработанного компанией eMemory Technology Inc[32]. Технология NeoPUF, разработанная этой компанией, использует различия в туннельном эффекте оксидного слоя для достижения высоких характеристик ФНФ (inter-HD = 50%; intra-HD ~ 0%)[33].

Пример применения ФНФ для защиты конфиденциальности и целостности инструкций и данных в памяти от физических и программных атак приведен в работах [38, 55].

Лицензирование программного обеспечения необходимо для защиты от несанкционированных модификаций и запуска на несанкционированных платформах. Идея применения ФНФ заключается в том, чтобы на основе сгенерированных ключей для выполнения некоторых критических операций, например, старт или перезапуск системы, программное обеспечение взаимодействовало с ФНФ [56]. Механизм лицензирования программного обеспечения, основанный на ФНФ, предложен в работе [57]. Компьютер пользователя оснащается ФНФ на основе схемы SRAM, что придает ему уникальную идентификацию. Когда пользователю необходимо приобрести необходимое программное обеспечение, компания устанавливает соединение с персональным компьютером пользователя, чтобы получить выходные данные ФНФ и сделать их доступными в программном обеспечении в виде лицензии. Клиент устанавливает программное обеспечение, и во время установки между программным обеспечением и персональным компьютером происходит механизм аутентификации. При этом встроенная лицензия сравнивается с выходными данными ФНФ, которая обеспечивает выполнение экземпляра программного обеспечения только на конкретном устройстве.

Недавно новый запатентованный подход применения ФНФ, названный Equipotential Timing, предложен компанией Granite Mountain Technologies[34]. Он предполагает использовать гигабайтные ФНФ (Giga-PUF) для проектирования функций, которые физически не могут быть отключены. Подход Equipotential Timing обеспечивает стабильные, синтезируемые реализации ФНФ, которые могут быть реализованы в виде «мягких» IP-блоков и интегрированы в любой дизайн по низкой цене. Эти Giga-PUF можно быстро и легко масштабировать для любых схем, во всех технологических узлах и кремниевых фабриках, предоставляя доступ всем компаниям к защите своих продуктов с помощью экспоненциальных решений ФНФ, которые обеспечивают подлинное доверие к оборудованию.

Еще одно применение модулей ФНФ, включенных в состав ИС – это обеспечение безопасной связи для аутентификации устройств интернета вещей в протоколе обмена ключами [58–60].

ЗАКЛЮЧЕНИЕ

Аналоговые и пассивные ФНФ образуют важный класс аппаратных примитивов безопасности, дополняя решения на основе задержек и памяти. Аналоговые схемы на транзисторных и диодных элементах обеспечивают высокую энтропию и низкую энергоемкость отклика, однако требуют продуманной стабилизации и калибровки для подавления влияния PVT-факторов и старения.

Пассивные подходы – резистивные «отпечатки» силовой сети, Via PUF и Coating PUF – привлекательны минимальными накладными расходами, высокой стабильностью и сложностью подделки.

Для практического применения рекомендуются:

- использование внутренних механизмов компенсации и автообнуления, а также отбракование/маскирование нестабильных элементов;

[32] eMemory Technology Inc. https://www.ememory.com.tw/. Дата обращения 19.07.2025. / Accessed July 19, 2025.

[33] PUFsecurity. NeoPUF® – A Reliable and Non-Traceable Quantum Tunneling PUF. https://www.pufsecurity.com/document/neopuf-a-reliable-and-non-traceable-quantum-tunneling-puf/. Дата обращения 19.07.2025. / Accessed July 19, 2025.

[34] Granite Mountain Technologies. Physical Unclonable Functions. https://gmt-semi.com/solutions/puf. Дата обращения 19.07.2025. / Accessed July 19, 2025.

- единая стандартизованная цепочка оцифровки (датчик – усилитель/компаратор – кодовая постобработка);
- интеграция с легкими техниками коррекции ошибок или фазовой фильтрацией там, где это оправдано;
- оценка устойчивости к атакам моделирования и побочным каналам с учетом аналоговой специфики (температура, питание, инжекция шумов).

Развитие ML выявило высокую уязвимость ряда классических ФНФ (особенно с линейными моделями задержек); усложнение конструкции (XOR, каскады) нередко недостаточно, а утечки вспомогательных/побочных данных позволяют проводить атаки без прямого доступа к ответам.

Защитные механизмы демонстрируют различную степень успеха, а такие архитектурные инновации, как CRC-PUF, демонстрируют повышенную устойчивость к ML-атакам. Однако фундаментальная проблема остается в том, что большинство современных конструкций ФНФ основано на математических моделях, которые по своей природе поддаются обучению достаточно сложными алгоритмами.

При выборе подходящих архитектур ФНФ, кодов коррекции ошибок и операционных протоколов необходимо учитывать не только текущие возможности атак, но и потенциальные будущие достижения в области методов ML. По мере развития этой области интеграция исследований в области безопасности ФНФ с более широкими достижениями в области ML, криптографии и аппаратной безопасности будет иметь важное значение для разработки надежных решений. Конечной целью остается разработка действительно неклонируемых функций, которые сохраняют свои защитные свойства даже перед лицом произвольно изощренных вычислительных атак.

ФНФ могут использоваться в качестве важных составляющих блоков в системах аутентификации, особенно в аппаратных токенах с ограниченными ресурсами и систем интернета вещей (см., в частности, услуги компании eMemory Technology Inc).

Будущие направления исследований:

1) стандартизация, развитие алгоритмов и инструментов анализа, повышение энергоэффективности;
2) повышение безопасности и защищенности от атак средствами анализа побочных каналов, атак на основе ML;
3) снижение эффектов влияния окружающей среды;
4) применение новых специальных алгоритмов, в частности, управляемых и реконфигурируемых ФНФ;
5) разработка ФНФ на перспективных физических эффектах, в частности квантовые ФНФ на основе ядерных магнитных моментов, резонансных туннельных диодов, плазмонной и лантаноидной люминесценции, джозефсоновских переходов, изменения потока электронов в нанокольцах (эффект Аронова – Бома), квантовой запутанности.

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.

М.И. Малето – анализ и систематизация литературы, обобщение результатов.

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

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

Н.Д. Евгеньев – анализ и систематизация литературы, написание текста статьи, обобщение результатов.

Все авторы прочитали и одобрили опубликованную версию рукописи.

Authors' contributions

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

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

M.I. Maleto – literature analysis and systematization, synthesis of the results.

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

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

N.D. Evgenev – literature analysis and systematization, manuscript writing, and synthesis of the results.

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

СПИСОК ЛИТЕРАТУРЫ / REFERENCES

1. 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 [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]
2. Lofstrom K., Daasch R., Taylor D. IC identification circuit using device mismatch. In: *Proceedings of the IEEE International Solid-State Circuits Conference* (*ISSCC 2000*). February 7–9, 2000. San Francisco, CA, USA. Piscataway, NJ: IEEE; 2000. P. 372–373. https://doi.org/10.1109/ISSCC.2000.839821
3. Venkatesh A., Sanyal A. A machine learning resistant strong PUF using subthreshold voltage divider array in 65nm CMOS. In: *Proceedings of the 2019 IEEE International Symposium on Circuits and Systems* (*ISCAS 2019*). May 26–29, 2019. Sapporo, Japan. Piscataway, NJ: IEEE; 2019. P. 1–5. https://doi.org/10.1109/ISCAS.2019.8702525
4. Mitchell-Moreno J.H., Espinosa Flores-Verdad G. A low bit instability CMOS PUF based on current mirrors and WTA cells. *J. Electron. Test.* 2023;39:611–620. https://doi.org/10.1007/s10836-023-06085-4
5. Jadhav V.D., Kalloor R., Poola L., Prabhakar T.V. Diode-PUF for intelligent electronic devices. In: *Proceedings of the 16th International Conference on Communication Systems & Networks* (*COMSNETS 2024*). January 2–6, 2024. Bengaluru, India. Piscataway, NJ: IEEE; 2024. P. 330–332. https://doi.org/10.1109/COMSNETS59351.2024.10427169
6. Kim N., Jeon S.-B., Jang B. Hardware-intrinsic physical unclonable functions by harnessing nonlinear conductance variation in oxide semiconductor-based diode. *Nanomaterials* (*Basel*). 2023;13(4):675. https://doi.org/10.3390/nano13040675
7. Takahashi Y., Koyasu H., Kumar S.D., et al. Quasi-adiabatic SRAM based silicon physical unclonable function. *SN Comput. Sci.* 2020;1:237. https://doi.org/10.1007/s42979-020-00253-5
8. Liu J., Takahashi Y. Design of low-power 6T adiabatic PUF circuit. In: *Proceedings of the 2024 IEEE Asia Pacific Conference on Circuits and Systems* (*APCCAS 2024*). October 27–30, 2024. Taipei, Taiwan. Piscataway, NJ: IEEE; 2024. P. 599–603. https://doi.org/10.1109/APCCAS62602.2024.10808318
9. Nagata S., Takahashi Y. A design of PUF circuit using adiabatic logic. In: *Proceedings of the 2024 IEEE Asia Pacific Conference on Circuits and Systems* (*APCCAS 2024*). October 27–30, 2024. Taipei, Taiwan. Piscataway, NJ: IEEE; 2024. P. 595–598. https://doi.org/10.1109/APCCAS62602.2024.10808900
10. Helinski R., Acharyya D., Plusquellic J. A physical unclonable function defined using power distribution system equivalent resistance variations. In: *Proceedings of the 46th ACM/IEEE Design Automation Conference* (*DAC 2009*). July 26–31, 2009. San Francisco, CA, USA. New York: ACM; 2009. P. 676–681. https://doi.org/10.1145/1629911.1630089
11. Jeon D., Baek J.H., Kim Y.-D., Lee J., Kim D.K., Choi B.-D. A physical unclonable function with bit error rate $<2.3 \times 10^{-8}$ based on contact formation probability without error correction code. *IEEE J. Solid-State Circuits*. 2020;55(3):805–816. https://doi.org/10.1109/JSSC.2019.2951415
12. Csaba G., Ju X., Chen Q., Porod W., Schmidhuber J., Schlichtmann U., Lugli P., Rührmair U. On-chip electric waves: an analog circuit approach to physical uncloneable functions [preprint]. *IACR Cryptology ePrint Archive*. 2009;2009/246.
13. 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
14. Skoric B., Maubach S., Kevenaar T., Tuyls P. Information-theoretic analysis of coating PUFs [preprint]. *IACR Cryptology ePrint Archive*. 2006;2006/101.
15. Aysu A., Farhady Ghalaty N., Franklin Z., Yali M., Schaumont P. Digital fingerprints for low-cost platforms using MEMS sensors. In: *Proceedings of the Workshop on Embedded Systems Security* (*WESS '13*). September 29, 2013. Montreal, QC, Canada. New York: ACM; 2013. Article 2. P. 1–6. https://doi.org/10.1145/2527317.2527319
16. Yu M.D., M'Raihi D., Sowell R., Devadas S. Lightweight and secure PUF key storage using limits of machine learning. In: Preneel B., Takagi T. (Eds.). *Cryptographic Hardware and Embedded Systems. CHES 2011.* Book Series: Lecture Notes in Computer Science. Berlin Heidelberg: Springer; 2011. V. 6917. P. 358–373. https://doi.org/10.1007/978-3-642-23951-9_24
17. Saadvikaa N., Saketi K.J., Gopishetti A., et al. PUF modeling attacks using deep learning and machine learning algorithms. *Eng. Proceedings.* 2023;56(1):187. https://doi.org/10.3390/ASEC2023-15948
18. Dubrova E., Näslund O., Degen B., et al. CRC-PUF: A machine learning attack resistant lightweight PUF construction. In: *2019 IEEE European symposium on security and privacy workshops* (*EuroS&PW*). IEEE; 2019. P. 264–271. https://doi.org/10.1109/EuroSPW.2019.00036
19. Tripathy S., Rai V.K., Mathew J. MARPUF: physical unclonable function with improved machine learning attack resistance. *IET Circuits, Devices & Systems*. 2021;15(5):465–474. https://doi.org/10.1049/cds2.12042
20. Ebrahimabadi M., Lalouani W., Younis M., et al. Countering PUF modeling attacks through adversarial machine learning. In: *2021 IEEE Computer Society Annual Symposium on VLSI* (*ISVLSI*). IEEE. 2021. P. 356–361. https://doi.org/10.1109/ISVLSI51109.2021.00071
21. Khalfaoui S., Leneutre J., Villard A., et al. Security analysis of machine learning-based PUF enrollment protocols: A review. *Sensors*. 2021;21(24):8415. https://doi.org/10.3390/s21248415
22. Strieder E., Frisch C., Pehl M. Machine learning of physical unclonable functions using helper data: Revealing a pitfall in the fuzzy commitment scheme. *IACR Transactions on Cryptographic Hardware and Embedded Systems.* 2021;2:1–36. https://doi.org/10.46586/tches.v2021.i2.1-36

23. Ali-Pour A., Afghah F., Hely D., et al. Secure PUF-based authentication and key exchange protocol using machine learning. In: *2022 IEEE Computer Society Annual Symposium on VLSI* (*ISVLSI*). IEEE. 2022. P. 386–389. https://doi.org/10.1109/ISVLSI54635.2022.00086
24. Yadav A., Kumar S., Singh J. A review of physical unclonable functions (PUFs) and its applications in IoT environment. In: Hu Y.C., Tiwari S., Trivedi M.C., Mishra K.K. (Eds.). *Ambient Communications and Computer Systems.* Book Series: Lecture Notes in Networks and Systems. Singapore: Springer; 2022. V. 356. P. 1–3. https://doi.org/10.1007/978-981-16-7952-0_1
25. Gao Y., Al-Sarawi S.F., Abbott D. Physical unclonable functions. *Nat. Electron.* 2020;3(2):81–91. https://doi.org/10.1038/s41928-020-0372-5
26. Wisiol N., Mühl C., Pirnay N., et al. Splitting the interpose PUF: A novel modeling attack strategy. *IACR Transactions on Cryptographic Hardware and Embedded Systems.* 2020;3:97–120. https://doi.org/10.13154/tches.v2020.i3.97-120
27. Arapinis M., Delavar M., Doosti M., et al. Quantum physical unclonable functions: Possibilities and impossibilities. *Quantum*. 2021;5:475. https://doi.org/10.22331/q-2021-06-15-475
28. Kayaci N., Ozdemir R., Kalay M., et al. Organic light-emitting physically unclonable functions. *Adv. Funct. Mater.* 2022;32(14):2108675. https://doi.org/10.1002/adfm.202108675
29. Awano H., Iizuka T., Ikeda M. PUFNet: A deep neural network based modeling attack for physically unclonable function. In: *2019 IEEE International Symposium on Circuits and Systems* (*ISCAS*). IEEE. 2019. P. 1–4. https://doi.org/10.1109/ISCAS.2019.8702431
30. Idriss T.A., Idriss H.A., Bayoumi M.A. A lightweight PUF-based authentication protocol using secret pattern recognition for constrained IoT devices. *IEEE Access*. 2021;9:80546–80558. https://doi.org/10.1109/ACCESS.2021.3084903
31. Shah A., Pandya H., Soni M., Karimov A., Maaliw R.R., Keshta I. PUF-based lightweight authentication protocol for IoT devices. In: Balas V.E., Semwal V.B., Khandare A. (Eds.). *Intelligent Computing and Networking. IC-ICN 2023*. Book Series: Lecture Notes in Networks and Systems. Singapore: Springer; 2023. V. 699. P. 401–412. https://doi.org/10.1007/978-981-99-3177-4_29
32. Alladi T., Deo M., Chamola V., Sikdar B., Chao H.C. SecAuthUAV: a novel authentication scheme for UAV-ground station and UAV-UAV communication. *IEEE Trans. Veh. Technol.* 2020;69(12):15068–15077. https://doi.org/10.1109/TVT.2020.3033060
33. Bansal G., Sikdar B. S-MAPS: scalable mutual authentication protocol for dynamic UAV swarms. *IEEE Trans. Veh. Technol.* 2021;70(11):12088–12100. https://doi.org/10.1109/TVT.2021.3116163
34. Yanambaka V.P., Mohanty S.P., Kougianos E., Puthal D. PMsec: physical unclonable function-based robust and lightweight authentication in the Internet of Medical Things. *IEEE Trans. Consum. Electron.* 2019;65(3):388–397. https://doi.org/10.1109/TCE.2019.2926192
35. Jiang Q., Zhang X., Zhang N., et al. Three-factor authentication protocol using physical unclonable function for IoV. *Comput. Commun.* 2021;173:45–55. https://doi.org/10.1016/j.comcom.2021.03.022
36. Mershad K., Cheikhrouhou O., Ismail L. Proof of accumulated trust: a new consensus protocol for the security of the IoV. *Veh. Commun.* 2021;32:100392. https://doi.org/10.1016/j.vehcom.2021.100392
37. Kaveh M., Aghapour S., Martín D., Mosavi M.R. A secure lightweight signcryption scheme for smart grid communications using reliable physically unclonable function. In: *2020 IEEE International Conference on Environment and Electrical Engineering & 2020 IEEE Industrial and Commercial Power Systems Europe* (*EEEIC/I&CPS Europe*). June 9–12, 2020. Madrid, Spain. Piscataway. NJ: IEEE; 2020. P. 1–6. https://doi.org/10.1109/EEEIC/ICPSEurope49358.2020.9160596
38. Cao Y.-N., Wang Y., Ding Y., Zheng H., Guan Z., Wang H. A PUF-based lightweight authenticated metering data collection scheme with privacy protection in smart grid. In: *2021 IEEE International Conference on Parallel & Distributed Processing with Applications, Big Data & Cloud Computing, Sustainable Computing & Communications, Social Computing & Networking* (*ISPA/BDCloud/SocialCom/SustainCom*). August 30 – September 3, 2021. New York, USA. Piscataway, NJ: IEEE; 2021. P. 876–883. https://doi.org/10.1109/ISPA-BDCloud-SocialCom-SustainCom52081.2021.00124
39. Maqsooq B., Qadri S., Shamshad S., Ayub M.F., Mahmood K., Kumar N. An identity-based authentication protocol for smart grid environment using physical unclonable function. *IEEE Trans. Smart Grid*. 2021;12(5):4426–4434. https://doi.org/10.1109/TSG.2021.3072244
40. Zerrouki F., Ouchani S., Bouarfa H. PUF-based mutual authentication and session key establishment protocol for IoT devices. *J. Ambient Intell. Human. Comput.* 2023;14:12575–12593. https://doi.org/10.1007/s12652-022-04321-x
41. Müelich S., Bossert M. *A New Error Correction Scheme for Physical unclonable Functions. arXiv*. arXiv:1611.01960 [cs.CR]. 2016. https://doi.org/10.48550/arXiv.1611.01960
42. Shamsoshoara A., Korenda A.R., Afghah F., Zeadally S. *A Survey on Hardware-Based Security Mechanisms for Internet of Things. arXiv*. arXiv:1907.12525 [cs.CR]. 2019. https://doi.org/10.48550/arXiv.1907.12525
43. 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. *Towards Hardware-Intrinsic Security*: *Foundations and Practice*. Book series: Information Security and Cryptography. Berlin: Springer; 2010. P. 3–37. https://doi.org/10.1007/978-3-642-14452-3_1
44. Dodis Y., Ostrovsky R., Reyzin L., Smith A. Fuzzy extractors: how to generate strong keys from biometrics and other noisy data. *SIAM J. Comput.* 2008;38(1):97–139. https://doi.org/10.1137/060651380
45. Muthammal R., Sindhuja N. VLSI architecture of turbo codes for dedicated short-range communication. *Int. J. Eng. Res. Online.* 2015;3(5):412–416. URL: https://www.researchgate.net/publication/321669464_VLSI_Architecture_of_Turbo_Codes-IP_Secure_With_PUF_for_DSRC_systems. Дата обращения 19.07.2025. / Accessed July 19, 2025.
46. Wong C.-W., Wu M. Counterfeit detection using paper PUF and mobile cameras. In: *Proceedings of the IEEE International Workshop on Information Forensics and Security* (*WIFS 2015*). November 16–19, 2015. Rome, Italy. Piscataway, NJ: IEEE; 2015. P. 1–6. https://doi.org/10.1109/WIFS.2015.7368579

47. Zheng J., Potkonjak M. A digital PUF-based IP protection architecture for network embedded systems. In: *Proceedings of the Tenth ACM/IEEE Symposium on Architectures for Networking and Communications Systems* (*ANCS'14*). 2014. P. 255–256. https://doi.org/10.1145/2658260.2661776
48. Zhang J., Lin Y., Lyu Y., Qu G. A PUF-FSM binding scheme for FPGA IP protection and pay-per-device licensing. *IEEE Trans. Inf. Forensics Secur.* 2015;10(6):1137–1150. https://doi.org/10.1109/TIFS.2015.2400413
49. Guo Q., Gong Y., Hu Y., Li X.-W. PUF-based pay-per-device scheme for IP protection of CNN model. In: *2018 IEEE Asian Test Symposium* (*ATS 2018*). December 10–13, 2018. Hefei, China. Piscataway, NJ: IEEE; 2018. P. 115–120. https://doi.org/10.1109/ATS.2018.00032
50. Kalanadhabhatta S., Kumar D., Anumandla K.K., Reddy A., Acharyya A. PUF-based secure chaotic random number generator design methodology. *IEEE Trans. Very Large Scale Integr.* (*VLSI*) *Syst.* 2020;28(9):1994–2004. https://doi.org/10.1109/TVLSI.2020.2979269
51. Kaya T. A true random number generator based on a Chua and RO-PUF: design, implementation and statistical analysis. *Analog Integr. Circ. Sig. Process.* 2020;102:577–588. https://doi.org/10.1007/s10470-019-01474-2
52. Calhoun J., Minwalla C., Helmich C., Saqib F., Che W., Plusquellic J. Physical Unclonable Function (PUF)-based e-cash transaction protocol (PUF-Cash). *Cryptography*. 2019;3(3):18. https://doi.org/10.3390/CRYPTOGRAPHY3030018
53. Zhang Y., Qin Y., Feng D., Yang B., Wang W. An efficient Trustzone-based in-application isolation schema for mobile authenticators. In: Lin X., Ghorbani A., Ren K., Zhu S., Zhang A. (Eds.). *Security and Privacy in Communication Networks. SecureComm 2017.* Book Series: Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering. Cham: Springer; 2018. V. 238. P. 585–605. https://doi.org/10.1007/978-3-319-78813-5_30
54. Kish L.B., Entesari K., Granqvist C.G., Kwan C. Unconditionally secure credit/debit card chip scheme and physical unclonable function. *Fluctuation Noise Lett.* 2017;16(1):1750002. https://doi.org/10.1142/S021947751750002X
55. Suh G.E., O'Donnell C., Devadas S. Aegis: a single-chip secure processor. *IEEE Des. Test Comput.* 2007;24(6):570–580. https://doi.org/10.1109/MDT.2007.179
56. Suresh V., Manimegalai R. SPIC-SRAM PUF integrated chip based software licensing model. In: Thampi S., Madria S., Wang G., Rawat D., Alcaraz Calero J. (Eds.). *Security in Computing and Communications. SSCC 2018. Communications in Computer and Information Science*. Springer; 2018. V. 969. P. 377–388. https://doi.org/10.1007/978-981-13-5826-5_29
57. Kohnhäuser F., Schaller A., Katzenbeisser S. PUF-based software protection for low-end embedded devices. In: Conti M., Schunter M., Askoxylakis I. (Eds.). *Trust and Trustworthy Computing. Trust 2015.* Book Series: Lecture Notes in Computer Science. Cham: Springer; 2015. V. 9229. P. 3–21. https://doi.org/10.1007/978-3-319-22846-4_1
58. Zheng Y., Liu W., Gu C., Chang C-H. *PUF-based Mutual Authentication and Key-Exchange Protocol for Peer-to-Peer IoT Applications* [preprint]. *TechRxiv*; 2021.
59. Mahmood K., Shamshad S., Rana M., et al. PUF-enabled lightweight key-exchange and mutual authentication protocol for multi-server-based D2D communication. *J. Inf. Secur. Appl.* 2021;61:102900. https://doi.org/10.1016/j.jisa.2021.102900
60. Bathalapalli V.K.V.V., Mohanty S.P., Pan C., Kougianos E. QPUF: quantum physical unclonable functions for security-by-design of industrial Internet-of-Things. In: *2023 IEEE International Symposium on Smart Electronic Systems* (*iSES 2023*). December 18–20, 2023. Hyderabad, India. Piscataway, NJ: IEEE; 2023. P. 296–301. https://doi.org/10.1109/iSES58672.2023.00067

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

Малето Михаил Иванович, к.т.н., ведущий инженер 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: maleto@yandex.ru. SPIN-код РИНЦ 2958-3989, http://orcid.org/0009-0006-3603-6322

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, www.researchgate.net/profile/A_Sigov

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

Евгеньев Никита Давидович, студент, кафедра вычислительной техники, Институт информационных технологий, ФГБОУ ВО «МИРЭА – Российский технологический университет» (119454, Россия, Москва, пр-т Вернадского, д. 78). E-mail: nikita.evgenev.10@gmail.com. SPIN-код РИНЦ 1034-0447, https://orcid.org/0009-0006-9073-8798

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.), Associate 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

Mikhail I. Maleto, Cand. Sci. (Eng.), Center for the Design of Integrated Circuits, Nanoelectronics Devices and Microsystems, MIREA – Russian Technological University (78, Vernadskogo pr., Moscow, 119454 Russia). E-mail: maleto@mirea.ru. RSCI SPIN-code 2958-3989, http://orcid.org/0009-0006-3603-6322

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

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 7428-6831, https://orcid.org/0009-0000-3976-7872

Nikita D. Evgenev, Student, Computer Technology Department, Institute of Information Technologies, MIREA – Russian Technological University (78, Vernadskogo pr., Moscow, 119454 Russia). E-mail: nikita.evgenev.10@gmail.com. RSCI SPIN-code 1034-0447, https://orcid.org/0009-0006-9073-8798