Micro- and nanoelectronics. Condensed matter physics

Микро- и наноэлектроника. Физика конденсированного состояния

UDC 004.832.32
https://doi.org/10.32362/2500-316X-2026-14-3-83-105
EDN QIOHGI

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.

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

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.

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

INTRODUCTION

Physically unclonable functions (PUFs) provide a hardware basis for trust, offering authentication and protection against counterfeiting, as well as enabling secure key derivation. The first part of the study [1] considers digital PUFs. The second part focuses on analog and passive PUFs, as well as their role in countering contemporary machine learning (ML) attacks and practical implementation scenarios.

Analog PUFs use continuous technological variations in the parameters of active and passive elements as a source of entropy. Unlike digital hardware security primitives, which are formed using discrete logic, analog PUFs rely on subtle variations in threshold voltages, currents, capacitances, and resistances. Once the circuit is switched on, these variations result in reproducible steady-state voltage and current levels that are unique to each chip. Here, digitization is performed by a comparator or analog-to-digital converter, while response stability is ensured by circuit techniques for drift and noise suppression. Due to their potentially providing higher entropy density and a larger set of challenge–response pairs (CRPs), many analog implementations are classified as "strong" PUFs. However, the characteristics of transistors and passive structures are sensitive to external factors, necessitating special measures to correct possible errors.

Passive PUFs include resistive imprints of power networks, Via PUFs[3] based on probabilistic contact formation, and Coating PUFs[4] which are provided with a specific pattern of random coating. While such passive PUFs are characterized by minimal overhead in terms of area, high stability, and—in some cases—ideal stability, this comes at the cost of a limited number of CRPs.

Due to the rapid development of ML having radically changed the understanding of PUF security, contemporary attacks are more frequently focused on extracting patterns from CRPs rather than traditional cryptanalysis. Concurrently, the research community is advancing increasingly sophisticated ML approaches to PUF modeling and countermeasures at the architecture and protocol levels, thereby refining the fundamental boundaries of resilience. The present work therefore sets out a comprehensive overview of the current state of the art, including the theoretical foundations, ML-based attack classes, and practical countermeasures, as well as their implications for PUF design and deployment.

ANALOG PUFS

Individual devices can be identified by measuring the original parameters of an electrical or electronic quantity. Sources of entropy include variations in transistor threshold voltages (TV-) and integrated circuit identification (ICID-) PUF, current arbiters, diode structures, quasi-adiabatic logic based (QUAL-) PUF, and adiabatic static random-access memory (SRAM).

The simplest TV-PUF variant, which is used to identify integrated circuits (ICs), involves analyzing the change in threshold voltages of integrated transistors resulting from inevitable technological variations during manufacturing. Here the challenge consists in the number or location of the transistor component, while the response is the corresponding threshold voltage value.

The approach to applying PUF proposed in [2] involves the assignation of a unique identification tag to each instance of a conventional IC without requiring special processing or programming after manufacture. Here several transistors of the same design are combined into an addressable matrix in an ICID-PUF device (Fig. 1).

In the described ICID-PUF, an addressable transistor controls a resistive load. Due to manufacturing variations, the threshold voltages of these transistors fluctuate, resulting in an unpredictable current flowing through the load. The voltage across the load is then measured and converted into a sequence of bits using an auto-zero comparator. This method has been verified via experimentation on 55 microchips manufactured using 0.35-μm complementary metal–oxide–semiconductor (CMOS)[5] technology. At the highest environmental fluctuations, an intra-Hamming distance (intra-HD) μ_{intra} = 1.3% is obtained, while the inter-Hamming distance (inter-HD) value of μ_{intra} is very close to 50%. With an input clock frequency of 1 GHz, the PUF design featuring 64-bit keys on transistors consumes 0.18 μW/bit while achieving uniqueness and uniformity indices of 50%. Reproducibility of this PUF variant has been demonstrated to be independent of IC ageing processes, as well as 45 nm-, 65 nm-, and 90 nm process nodes.

In [3], a cascade comprising three stages of 20 CMOS inverters and diode-connected transistors is proposed. This forms a voltage divider whose output voltage depends on variations in the threshold voltage. This PUF demonstrates an

[3] Via PUF is a technology based on the use of microscopic via holes in metallic layers of semiconductors.

[4] Coating PUF is a technology that utilizes a protective coating for its operation.

[5] 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.

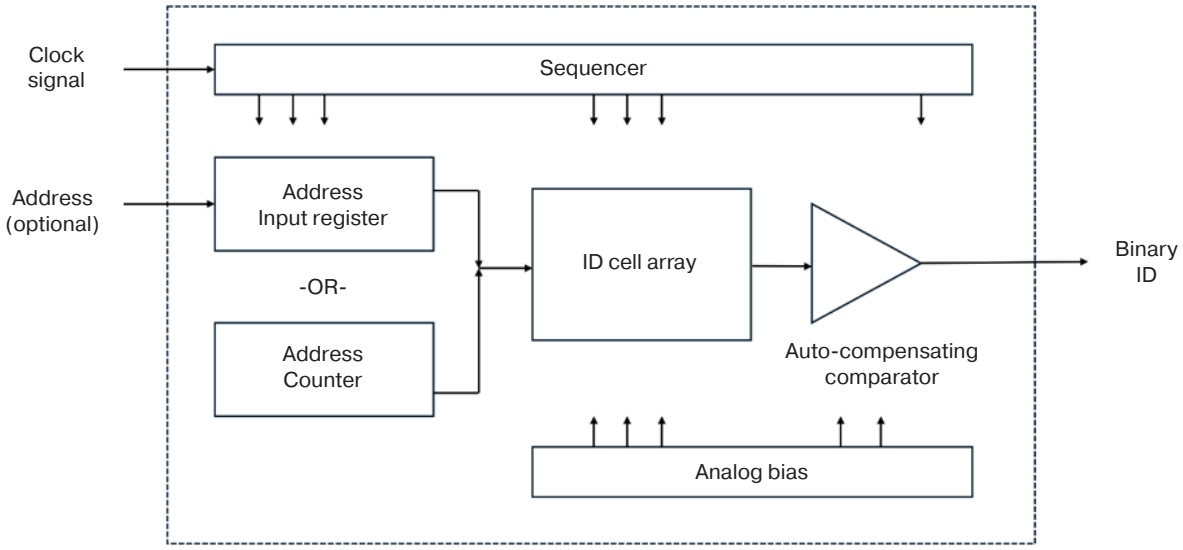


Fig. 1. Block diagram of a device for IC identification based on PUF [2]. ID is identifier

inter-HD of approximately 50.65% and an intra-HD of approximately 6.96%. Due to operating below the threshold voltage, the circuit demonstrates low power consumption (no more than 0.43 pJ/bit); however, it is sensitive to comparator noise. Reliability of recognition is enhanced by averaging 15 samples.

It should be noted that these characteristics may change in the event of increased noise due to changes in the library element parameters (characterization by PVT corners: process, voltage, and temperature variations) or the ageing of the active device, which can affect the reliability of PUF responses.

As described in [4], the difference between nominally identical currents is accurately measured when transistors are turned on. This is achieved using a specialized hardware element of an artificial neural winner-takes-all network, which acts as an arbiter. The obtained values are intra-HD ≈ 1.57%, inter-HD ≈ 49.8% and 97.7% reliability in the temperature range from −20°C to +120°C, with a ±300 mV variation in supply voltage. The circuit's energy consumption is 5.67 pJ/bit. An improved version of this circuit, which is implemented in a 130 nm technology node, uses a pair of cascode current mirrors with double gain-boosting[6] amplification to reliably maintain the operating point at around 50 nA, thereby increasing the output resistance. Consequently, bit instability does not exceed 1.56% across a supply voltage range of 0.6–2 V and a temperature range of 0–75°C. Intra-HD does not exceed 0.49% on average, with virtually perfect uniqueness (inter-HD ≈ 50%). Together with an energy consumption of 5.36 fJ/bit and an area of 72 μm^2/bit, these characteristics render the cell highly attractive for integration into Internet of Things (IoT) modules. Experiments on 21 128-bit chips confirm the statistical stability of the solution, as well as demonstrating one of the best aggregate quality factor indicators (figure of merit is 17 relative units) while maintaining ease of integration into ICs and potential for further scaling.

Another version of an analog diode PUF is implemented in [5], where the device signature is formed from diodes present in the output ports of the IC. Measures are provided to increase the uniqueness of the signatures, as well as compensating for temperature differences and losses in the supply conductors.

The study [6] examines the use of PUFs based on diode structures in ICs. The authors demonstrate that changes in the conductivity of oxide-based Schottky diodes as a result of the technology process provide an effective source of random numbers for using PUFs without the need for switching operations. It is demonstrated that the naturally occurring electron accumulation region in an oxide semiconductor film can be partially eliminated using a mild oxygen plasma treatment. This leads to a significant change in nonlinearity, thus providing an exotic source of entropy. In general, soft plasma-treated Schottky diodes demonstrate near-perfect uniformity, uniqueness, and an ideal entropy value, thus eliminating the need for additional equipment, as well as reducing space requirements and energy costs. These results are promising for the development of hardware-embedded PUFs that enable the implementation of energy-efficient cryptographic equipment.

A QUAL-PUF is formed from the composite capacitor and transistor components of an adiabatic logic circuit (an energy-efficient system that converts

[6] 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.

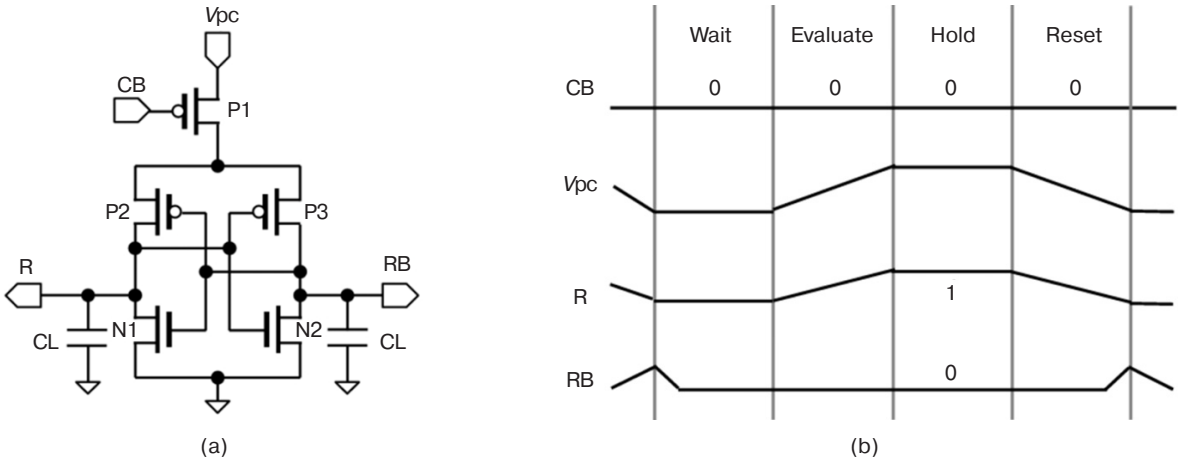


Fig. 2. QUAL-PUF circuits [7]:
(a) QUAL-PUF; (b) timing diagram.
*V*pc (power clock) is supply clock signal; CB is challenge bit;
P1 is control transistor; P2 and P3 are *p*-MOS[7] transistors of the bistable element;
R (response) is main response bit; RB (response bit) is complementary response bit output,
N1 and N2 are *n*-MOS transistors of the bistable element;
and CL is equivalent load capacitance of the output node

the charge accumulated in the load capacitor after operations into a signal) due to technological changes during the manufacturing process. Circuits that allow for such complete recycling are usually complex and occupy a large area. In [7], however, a quasi-adiabatic circuit is used which only recovers most of the capacitor charge. As shown in Fig. 2, this PUF implementation involves applying an increasing voltage to two theoretically identical transistor elements in the circuit.

Mismatches in transistor parameters are caused by differences that occur during production. This results in one transistor having greater conductivity and charging the load capacitor faster. This creates a stable response bit for each elementary cell of the circuit, which is similar to the effect of MOS transistor mismatch in traditional PUFs. Since adiabatic logic operates within specific charge/discharge cycles, a distinctive feature of this implementation is the evaluation of each FIFO (First-In, First-Out) cell at only one of four identical time intervals. To account for this, each PUF bit unit consists of four cells operating with a time shift of a quarter of a clock cycle. The implementation of a 4-bit adiabatic PUF module composed of four QUAL-PUFs is shown in Fig. 3.

Each elementary cell is controlled by a challenge bit (CB), which initiates the process, along with four clock pulses ($V\varphi_1$–$V\varphi_4$), which are trapezoidal power-clock signals of quasi-adiabatic logic shifted by 90° in phase. These phases correspond to the wait, evaluate, hold, and reset states. Each local block (QUAL-PUF1–QUAL-PUF4) generates a pair of output signals comprised of the main response bit (R1–R4) and its complementary output (RB_1–RB_4). Connections between the blocks are made via pass keys, which are controlled by the corresponding phase signals $V\varphi_i$ to ensure sequential cycles of charging and restoration of load energy.

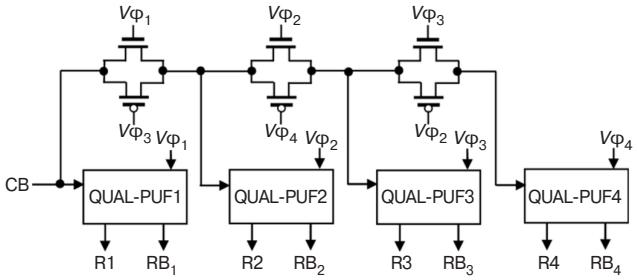


Fig. 3. 4-bit adiabatic PUF module composed of four QUAL-PUFs [7]

[7] Metal–oxide–semiconductor.

As shown in Fig. 3, if the first cell operates in the hold phase, the next cell operates in the reset phase, while the remaining two cells operate in the wait and evaluate phases, respectively. By sampling all four outputs simultaneously, four bits of response can be obtained. Sampling at different phases of the clock signal forms different combinations of bits, thus enabling the four PUF modules to generate up to 16 bits of response. Since each module contains four repeating random bits, this structure significantly complicates the PUF modeling process for a potential attacker.

Study [7] provides an example of implementing a 4-bit low-power chip with memory based on a 6T adiabatic memory cell manufactured using a standard 0.18 μm CMOS process with a supply voltage of 1.8 V, whose module dimensions measure 58.7 × 5.7 μm. The simulation results show an inter-HD value of 47.58%, a reliability of 95.10%, and a dissipated energy of 29.73 fJ/bit/cycle.

These results are confirmed in later implementations of a similar circuit [8], which demonstrate that such a PUF, when simulated, provides an average reliability of 98.51% under temperature and supply voltage fluctuations. The circuit offers a uniqueness of 49.75% and a power consumption of 15.92 fJ/bit/cycle. These estimates are consistent with measurements taken on manufactured samples, which confirm the PUF's required functionality with a reliability of 96.92% at room temperature.

An example of a circuit based on adiabatic SRAM using 0.18 μm CMOS technology is given in [9]. As well as consuming less energy than conventional memory-based PUFs, this circuit offers good uniqueness and reliability. When simulated using simulation program with integrated circuit emphasis (SPICE)[8], the proposed circuit consumes 13.88 fJ/bit/cycle, and the uniqueness and reliability values when the PUF circuit is connected in a 4-bit cascode are 50.07% and 99.51%, respectively.

PASSIVE PUFS

Analog PUFs include passive devices that use statistical variations in passive elements or structures to create a unique "fingerprint" for the device. Passive PUFs typically do not require a special stimulus signal due to their random parameters being embedded in the structure from the outset and thus capable of being read directly.

Further on, three examples of passive PUFs are considered: (1) based on variations in conductor resistance; (2) based on via holes (Via PUF); and (3) based on using a protective coating (Coating PUF).

[8] Simulation Program with Integrated Circuit Emphasis (SPICE) is an open-source simulator for general-purpose electronic circuits.

Differences in the manufacture of component connections can result in variations in power distribution maps in ICs, which can also serve as indicators of the uniqueness of a particular instance. In this case, a PUF is implemented by adding extra components to the device to enable the connection of each branch of the power distribution network to the ground bus, thus bypassing the existing components. The device signature is formed by measuring the voltage drops (or resistance values) across these sections of the circuit. Fluctuations in the thickness, width, and grain size of the metal during production cause slight variations in the resistance of the busbar segments from crystal to crystal. This can be achieved by applying test currents through specific sections of the power network and measuring the resulting voltage drops, which depend on the circuit's total resistance. By combining the results of several such measurements, a unique response vector is created that characterizes a given instance of the microcircuit. The challenge specifies the number or location of the circuit sections, while the response specifies the corresponding voltage drop or resistance value. An example of this process is presented in [10], which provides the results of measuring changes in equivalent resistances in the power distribution systems of 24 identical microcircuits manufactured using 65 nm technology.

A resistive PUF is highly stable to external conditions due to being based on passive metal structures. Variations in metal resistance depend linearly on temperature and weakly on supply voltage, making compensation for external influences simpler than with transistor effects. In particular, transistor (active) PUFs typically require calibrations or correction algorithms to account for changes in PVT parameters, whereas a passive metal network provides more reproducible results without complex adjustments. Since the only necessary additional circuits are those required for readout and digitizing the response, the use of a distributed power network already presents in each chip results in minimal overhead in terms of area. The distributed nature of the metal grid creates statistical variation across different areas to increase uniqueness; as such, the probability of two chips producing the same resistive fingerprint by chance is negligible. Another advantage of this PUF is its hardware stability, which is achieved by designing the metallization in such a way as to ensure it does not degrade over time (electromigration is eliminated by selecting the dimensions of the conductors). Since it is practically impossible to copy the resistances in all the power nodes of a clone without replicating the entire technological process of the origin, the counterfeiting of such devices is highly complex. This approach has two main limitations: (1) the relatively small

amount of data generated (usually a unique key/ID is obtained, although varying the measurement points can produce several bits); (2) the need for precise analog measurements of small resistance differences. Nevertheless, experimental samples of resistive PUF have proven viable; for instance, in 65 nm CMOS, all 36 tested crystals could be reliably distinguished based on power network variations.

In [10], which considers analog PUFs, it is proposed that voltage drops and equivalent resistances be recorded in microcircuit power supply circuits due to these electrical parameters being affected by random factors in manufacturing technology. Experiments carried out on chips manufactured using 65 nm CMOS technology demonstrate that, when measuring equivalent resistances, the quantitative characteristics μ_{intra} and μ_{inter} are approximately 0.04 and 1.5 Ohm, respectively.

The idea behind Via PUF, which is based on variations in the formation of via holes, is to deliberately violate the design standards for via holes in IC layout by using sizes that are slightly smaller than the permissible minimum. The exact size of each via gives it about a 50% chance of successfully forming a connection between the layers by being filled with metal or of remaining open [11]. Such events occur randomly due to uncontrollable fluctuations in the manufacturing process. Consequently, once the chip is manufactured, many of the embedded connections in it turn out to be either conductive ("1") or open ("0"), forming a pattern unique to the crystal. Via PUF is read by measuring the resistance of the embedded contacts: high resistance indicates an absence of a metal connection ("0"), while low resistance indicates a formed contact ("1"). An important advantage of this approach is its exceptional reliability: either the contact is formed or it is not, and the metal connection is unaffected by changes in temperature or supply voltage. Experiments have shown that the bit error rate for PUFs based on the formation of vias is practically zero, thus obviating the need for error correction using redundant codes. Additional processing, such as two-stage XOR conversion, is employed to eliminate offsets and improve bit uniformity. The main advantages of Via PUFs include high fingerprint uniqueness (with inter-codeword Hamming distances of around 50%) and resistance to ageing. Such random contacts can be distributed throughout the crystal among conventional vias, which makes them difficult to detect when an attacker reverse engineers the chip. Since standard CMOS layers and materials are used with the sole addition of "embedded" contacts of a specific size, the implementation does not require non-standard technological processes. However, the number of bits generated by Via PUF is fixed by the circuit (usually acting as a unique identifier rather than a reusable CRP); for this reason, the size of the vias must be calibrated for a specific technical process to ensure a ~50% probability of filling and any borderline cases rejected to avoid unstable bits.

A study of methods to increase the reliability of a system on a chip based on ARM Cortex-M4 microprocessors (ARM, United Kingdom) conducted by Lee[9] justifies the chosen method of forming a PUF. It notes that there is a medium-sized area, conventionally referred to as the PUF zone, in which the probability of contact forming is 50% if the size of the via is smaller than that specified in the design (Fig. 4a).

A microscopic image of a silicon Via PUF in cross section is shown in Fig. 4b. Contact vias of varying quality are clearly visible, with the following definitions: (1) the contact is open if it does not provide a connection to the silicon substrate; (2) the contact is shorted if it provides an electrical connection between the layers. In order to form the PUF after manufacturing is complete, it is necessary to exclude unreliable contacts by measuring the resistance of the through or contact connection.

For example, in one process node, resistance greater than 1 MOhm is identified as an open circuit, while resistance less than 50 kOhm is identified as a short circuit. All vias between these two values are cut off, these cut-off values being selected separately for each process. Once classified as a short circuit or open circuit, the connection remains unchanged regardless of PVT variations to ensure a zero-bit error rate. This important feature of Via PUF confirms the basic reliability of the technology.

As mentioned previously, achieving complete randomness is essential for PUFs, where ideal randomness is defined as an HD of 0.5, or 50%. To increase reliability, this work used a two-stage selection based on the XOR criterion (Fig. 5). A total of 405 test chips were manufactured with 16 different via sizes, each having 7680 bits, thus providing a total of 122800 bits of input data for the PUF. The first XOR stage reduces this to 7680 bits, which then pass through the second XOR stage to generate the final result of 640 bits, achieving a value of μ_{inter} = 0.4972 at a standard deviation σ_{inter} = 0.0205. Figure 5 shows the selection of Via PUF chips based on the results of the United States National Institute of Standards and Technology's[10] standard randomness tests SP 800-22 and SP 800-90B.

A similar PUF using a binary response to uniqueness (learning resilient and reliable digital PUF) based on variations in interconnection lithography is also used in [12].

[9] 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. Accessed June 16, 2025.

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

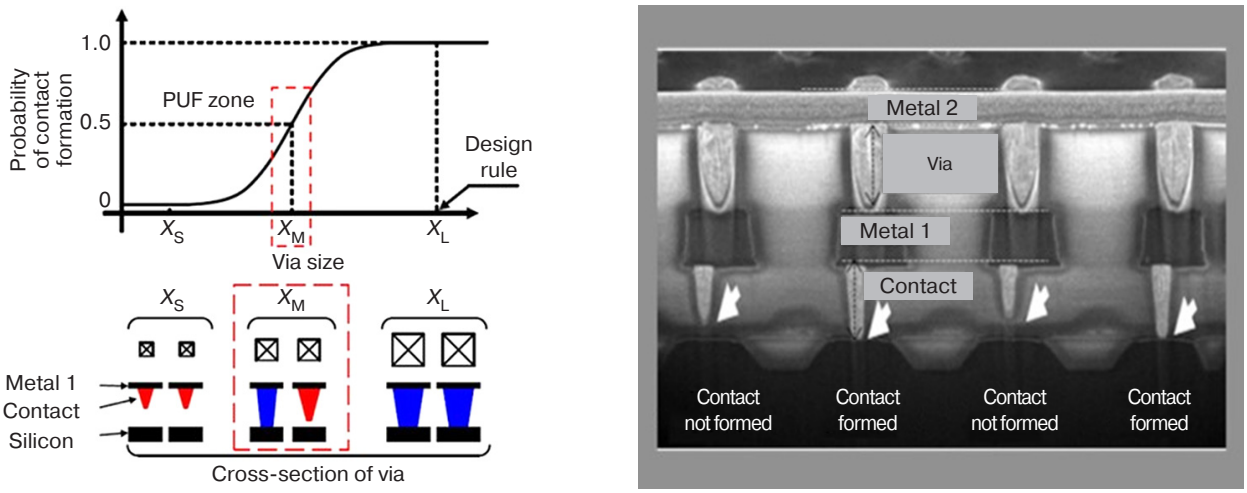


Fig. 4. Implementation of a PUF based on variations in via formation:
(a) probability of contact formation depending on the size of the via;
(b) cross-section[11] of a microscopic image of a Via PUF.
X_S is the size of the via at which no contact is formed; X_L is the size of the via determined by the design rules;
X_M is the intermediate size of the via at which contact formation is probabilistic

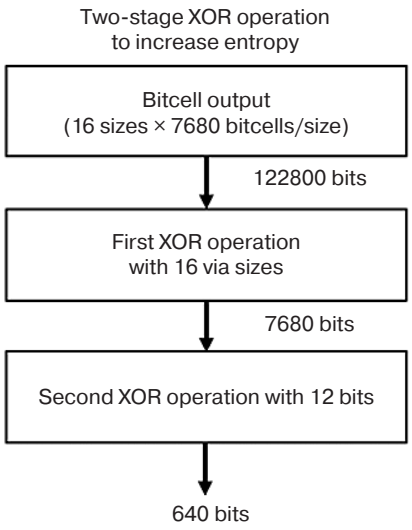
The protective Coating PUF uses an external, random, dielectric coating that is applied over the crystal in order to form a unique fingerprint. The classic implementation, as described in references [13, 14], involves placing a grid of metal conductors (e.g., a comb-like electrode structure) on top of the IC and filling the space between them with an optically opaque polymer containing randomly distributed dielectric nanoparticles. Due to the chaotic arrangements, sizes, and dielectric properties of these particles, the electrical capacitance between each pair of conductors becomes a random variable. In other words, nominally identical capacitors formed by the upper conductors acquire a range of capacitance values that is unique to each microcircuit instance. By reading a set of such capacitors (for example, by measuring leakage currents or charge/discharge time constants), it a set of random bits can be obtained depending on local variations in the dielectric permeability of the coating. These bits constitute a unique device identifier that is physically unclonable due to the unique distribution of particles in the coating layer.

As shown in [15], when an opaque, chemically inert dielectric layer is applied to the upper layer of IC metallization, the electrical capacitance values measured for each chip are random and unique. The implementation scheme and operation principle of the Coating PUF are shown in Fig. 6.

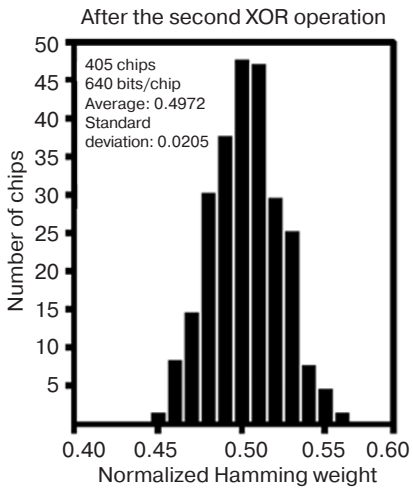
The results of digitized measurement carried out on 36 manufactured chips, in which each chip is used to test 31 capacitive sensors, show a high degree of randomness ($\mu_{inter} \approx 50\%$) and low noise ($\mu_{intra} < 5\%$).

A protective Coating PUF offers two key advantages. Firstly, it enhances the hardware security of the crystal by preventing direct optical examination and reading of the internal circuits. The opaque top layer acts as a protective mask. As such, any attempt to remove or damage this layer inevitably changes the distribution of particles and capacitance, destroying the device's original "fingerprint." Thus, Coating PUF not only provides a unique key, but also serves as a kind of tamper sensor. If tampered with, the original identifier is lost, thus revealing the hack. Secondly, due to the large-scale random formation process involving the mixing of millions of particles, the probability of two such PUFs coinciding is extremely low. Reproduction would require copying processes at the atomic level, which is practically impossible. However, a key disadvantage in this approach is the need for an additional manufacturing process, namely the application and curing of a special coating, which increases the cost. Additional analog circuits or high-precision external measurements required for reading the imprint may be affected by external conditions (e.g., temperature affecting the dielectric). Devices with Coating PUF have demonstrated their effectiveness in authentication systems, particularly in the implementation of radio frequency identification tags, where a random epoxy coating is used as a source of a 128-bit key that is destroyed when physical access is attempted.

[11] 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. Accessed June 16, 2025.



(a)



(b)

NIST SP 800-22 test for Via PUF

Test type	Average *p*-value	Test result
Frequency	0.4327	+
Block frequency (*M* = 128)	0.4734	+
Cumulative sums	0.4259	+
Runs	0.4956	+
Long run	0.4506	+
Rank	0.4569	+
FFT	0.5090	+
Approximate entropy (*m* = 6)	0.4549	+
Sequential test	0.4920	+

(c)

Fig. 5. Two-stage Via PUF selection algorithm based on the XOR criterion and NIST test results[12].
FFT is fast Fourier transform. *M* is the length of the block in the frequency test within the block,
m is the length of the bit pattern in the approximate entropy test. A block is a fragment of a fixed-length bit sequence into which the NIST test divides the entire sequence being tested

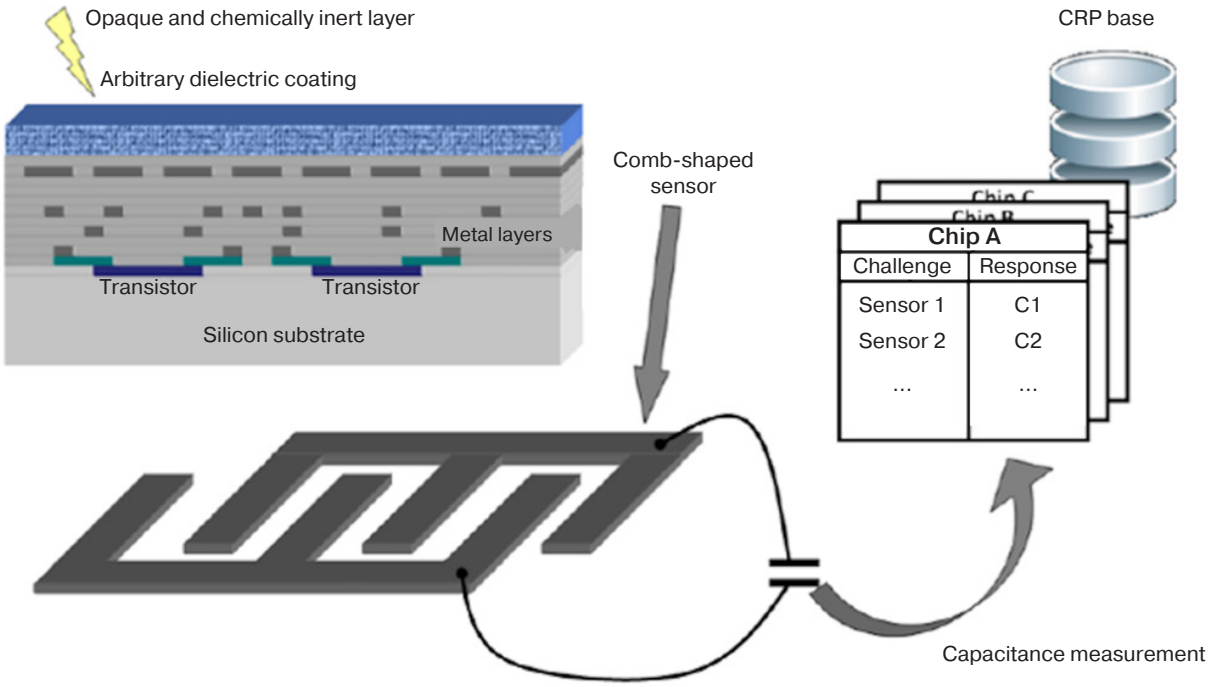


Fig. 6. Example of passive PUF implementation based on an inert dielectric layer [14]

[12] 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. Accessed June 16, 2025.

Table. Characteristics of analog and passive PUFs

PUF type / reference	Year of publication	PUF characteristics					
		Inter-HD	Intra-HD	Platform	Sensitivity to external conditions		Estimated implementation complexity
					Temperature	Voltage	
Subthreshold [3]	2019	50.65%	~7%	SPICE model TSMC 65 nm CMOS	From −20°C to 85°C	0.75–0.9 V	High
Current Mirror[13] [4]	2023	49.84%	1.57%	SPICE model TSMC 65 nm CMOS	From −20°C to 120°C	±300 mV	High
Adiabatic SRAM[14] [7]	2020	47.58%	4.9%	ASIC 180 nm CMOS	From −40°C to 100°C	1.8 V	Medium
6T Adiabatic[15] [8]	2024	49.75%	1.49%	ASIC 180 nm CMOS	From −40°C to 100°C	0.9–1.8 V	Medium
Adiabatic Logic[16] [9]	2024	50.07%	0.49%	ASIC 180 nm CMOS	From −50°C to 100°C	–	Medium
Via[17] [11]	2020	49.99%	~0%	ASIC 130 nm CMOS	From −55°C to 125°C	1.65 V	Low

The table below summarizes data from publications presenting original results on the implementation of PUFs based on analog circuits and circuits with variations in vias. The key metrics selected are inter-HD, i.e., the distance between two PUF responses from different PUF instances using the same call, and intra-HD, which is the distance between two PUF responses obtained from the same PUF instance and using the same call. These are referred to as "uniqueness" and "reliability" in a number of studies, respectively.

The table also shows the voltage/temperature variations at which the characteristics are measured, as well as the extent to which they change (the change in intra-HD is indicated in parentheses) if such data is provided. The estimated complexity of implementation (high, medium, or low) indicates the relative hardware costs and technical complexity involved in implementing a particular type of PUF (e.g., balancing paths, selecting element parameters, or change technical processes).

VIOLATION OF PUF SECURITY BASED ON ML METHODS

Recent advancements in ML techniques have significantly altered the perception of PUF security. The vulnerability of PUFs to ML-based attacks has led to extensive research on attack methodologies and defense measures [3, 16–19]. The paradigm shift in the approach to analyzing PUF security due to such attacks tends away from traditional cryptanalytic approaches and towards data-driven modeling techniques that exploit patterns inherent in PUF CRPs.

As well as developing more sophisticated attack strategies that use adversarial ML techniques [17, 20], researchers have proposed new PUF architectures and protocols designed to counter these attacks [3, 18, 19]. The following section presents an analysis of the current state of ML attacks and defenses in PUF systems, which is based on the latest advances in both attack methods and countermeasures. As well as examining the theoretical foundations of PUF security, it analyzes various categories of ML-based attack, evaluates proposed defense measures, and discusses the implications for future PUF development and deployment strategies.

PUF architectures and security properties

Based on their behavior in CRPs, PUFs can be categorized into two distinct types: strong and weak [21]. The possibility of using strong PUFs to generate a large

[13] PUF based on the use of an array of current mirrors.
[14] A type of SRAM that employs adiabatic energy recovery methods.
[15] A six-transistor PUF that operates on adiabatic logic principles.
[16] PUF based on adiabatic logic.
[17] PUF derived from variations in the formation of vias.

number of CRPs makes them suitable for authentication protocols that use multiple CRPs without exhausting the available challenge space. Examples include arbiter-type PUFs, ring oscillator PUFs, and various composite architectures [17–19]. In contrast, weak PUFs, which have limited challenge space, are generally employed for key generation, where one or more responses are extracted and processed using error correction procedures [22].

The Arbiter physical unclonable function (A-PUF) is one of the most widely studied strong PUF architectures. This architecture uses the difference in delays between two nominally identical signal transmission paths to generate a response [16, 18]. The challenge bits control the switching elements that determine the path configuration in such a way that the arbiter circuit can then evaluate which path is faster to produce a binary response. Despite its conceptual simplicity, this type of PUF has proven vulnerable to ML attacks due to its linear additive delay model [17, 19]. To improve security against ML attacks, more complex architectures have been developed that attempt to fundamentally change the mathematical relationships between inputs and outputs as a means of preventing effective ML modeling [18, 19, 22].

The most important aspect of PUF implementation is the processing of noise inherent in PUF responses. This noise is caused by environmental fluctuations, aging, and measurement errors [16, 22]. Reliable key generation and authentication relies on error correction mechanisms, which are typically implemented using fuzzy extractors or auxiliary data algorithms. Here, the most common approach is to store auxiliary data for enabling the correction of noisy PUF responses without disclosing the actual response values. However, recent research has shown that this auxiliary data can leak significant information about the PUF responses, enabling ML attacks even when the actual response values are unavailable [22]. This represents a fundamental vulnerability in PUF-based systems that use standard error correction approaches, particularly those using linear block codes, such as repetition codes.

Attacks on PUFs using ML

The vulnerability of PUFs to ML-based attacks has been demonstrated through the application of traditional ML techniques to A-PUFs and their variations [3, 17]. These attacks are successful due to the underlying mathematical relationships that underpin PUF designs. In the case of A-PUFs, the delay difference can be modeled as a linear function of challenge bits and delay parameters. This makes A-PUFs vulnerable to linear classification techniques [16, 17]. Despite increased complexity introduced by XOR operations or other nonlinear transformations, the fundamental structure is often still analyzable with appropriate ML algorithms. Typically, classic A-PUFs can be accurately modeled with over 95% accuracy using fewer than 10000 CRPs along with conventional logistic regression methods. Due to the linear nature of their delay model, these PUFs are particularly vulnerable to mathematical analysis and ML modeling.

Deep learning (DL) models can automatically detect relevant features and nonlinear relationships in CRPs, thus eliminating the need for manual feature selection. DL-based attacks demonstrate superior performance on all tested architectures compared to classical ML approaches. Convolutional neural networks and multilayer perceptrons also outperformed classical ML approaches, particularly against complex physical unclonable function (PUF) architectures designed to defend against traditional attacks [3, 17]. Convolutional neural networks achieve modeling accuracy above 90% for various types of PUFs while requiring fewer training samples than traditional methods. This suggests that the complexity of modern ML algorithms exceeds the defensive capabilities of current PUF designs.

Transfer learning methods have also been investigated, whereby models trained on a single PUF instance or architecture are adapted for use in attacks on different PUFs [21]. This approach reduces the amount of training data required for successful attacks at the same time as demonstrating the generalizability of PUF models trained on similar architectures.

Evolutionary strategies, particularly the covariance matrix adaptation evolution strategy, have been shown to be effective in ML attacks against more complex PUF designs [17, 21]. These methods enable the modeling of PUF behavior by evolving populations of candidate models and selecting those that best match the observed CRPs. The flexibility of evolutionary approaches makes them particularly dangerous for PUFs with complex internal structures.

One particularly challenging approach involves using Siamese neural networks to model a PUF using auxiliary data [22]. This technique exploits the redundancy inherent in error correction codes to extract trainable features and labels without direct access to PUF responses. By applying XOR relationships in linear block codes, attackers can train models to predict PUF behavior using only publicly available auxiliary data and tasks.

Advanced attack strategies, which have moved beyond simple CRP modeling, now utilize additional sources of information. Reliability-based attacks exploit the fact that PUF responses near decision boundaries are more sensitive to noise and environmental

fluctuations [16, 17]. By analyzing the stability of responses over multiple measurements, attackers can gain insights into the internal structure and parameters of PUF circuits.

Another significant threat vector is side-channel attacks, in which physical information such as power consumption, electromagnetic emissions, or synchronization variations is exploited to strengthen attacks on ML models [21]. Such attacks can be highly effective when combined with traditional ML approaches due to the provision of additional constraints and information that can improve model accuracy.

The combination of multiple attack vectors can create especially powerful threats. For example, by combining partial response data with side-channel measurements, the number of CRPs required for successful ML attacks is substantially decreased. Such multimodal approaches underline the importance of considering all potential sources of information leakage when analyzing the security of PUF models.

Quantum computing poses a potential threat in the future that could radically alter the security level of PUF. While current quantum algorithms may not be directly applicable to PUF modeling, advanced computing capabilities could facilitate new attack strategies or render currently impractical attacks feasible.

Defense methods against ML attacks

Several architectural improvements have been proposed for enhancing the resistance of PUFs against attacks implemented using ML. One such fundamental approach is the cyclic redundancy check PUF (CRC-PUF) design, which breaks the direct correlation between challenges and responses using cryptographic transformations [18]. By applying CRC operations with randomly chosen polynomials, the CRC-PUF ensures that the likelihood of recovering the transformed challenge is cryptographically small, thus circumventing traditional ML attacks.

Another PUF architecture employs a two-round challenge processing mechanism in which subsequent challenges are modified using intermediate responses [17]. By concealing the direct connection between input challenges and final responses, this approach significantly complicates the creation of predictive models by ML algorithms. Here, the randomization introduced by the intermediate processing stages increases the effective challenge space to reduce the correlation between different CRPs.

Innovations at the hardware level have also shown promise in countering ML attacks. Subthreshold PUF with a voltage divider operates in weak inversion regions, in which large threshold voltage fluctuations increase randomness [3]. The cascading connection of several stages combined with careful bias control provide this design with strong statistical properties that maintain its resistance to various ML algorithms. These properties include support vector machines, logistic regression, and artificial neural networks.

Rather than modifying the underlying architecture of the PUF, protocol-level defenses aim to limit the information available to potential attackers. Challenge restriction strategies limit the number of CRPs that can be observed, thereby preventing attackers from accumulating sufficient training data for effective ML attacks [16, 21]. However, due to inherently restricting the capabilities of strong PUFs, this approach may not be feasible for applications requiring numerous authentication operations. To minimize information leakage during the configuration and operation phases of PUFs, improved logging protocols have been developed [21, 23]. These protocols prevent unauthorized access to training data by carefully controlling the distribution of CRPs and implementing secure computation methods. Multilateral computation and homomorphic encryption can ensure that PUFs operate without revealing confidential information to potential attackers.

Advanced methods (Fig. 7) offer a new approach to protecting PUFs by deliberately introducing errors into the CRP process [20]. These methods can significantly reduce the accuracy of ML models by poisoning the training data available to potential attackers while maintaining correct operation for legitimate users who understand the poisoning strategy. This involves periodically providing incorrect responses to challenges, thereby creating a dataset from which standard ML algorithms cannot effectively learn.

The security implications of using auxiliary data in PUF systems have led to the development of specialized error correction approaches [16, 22]. It has been demonstrated that traditional concatenated coding schemes, particularly those employing repetition codes as inner codes, are highly vulnerable to ML attacks involving auxiliary data analysis. The redundancy of these codes gives attackers enough information to create effective models without needing to access the actual PUF responses. Codes with higher frequencies and more complex structures are more resistant to auxiliary data attacks, whereas simple codes such as repetition codes should be avoided in critical applications [22]. The analysis of various code families confirms that vulnerability to ML attacks is directly affected by the number and complexity of XOR relationships in the code structure.

Safe error correction approaches include syndrome construction methods, systematic coding with low data leakage, and specialized polar codes that minimize

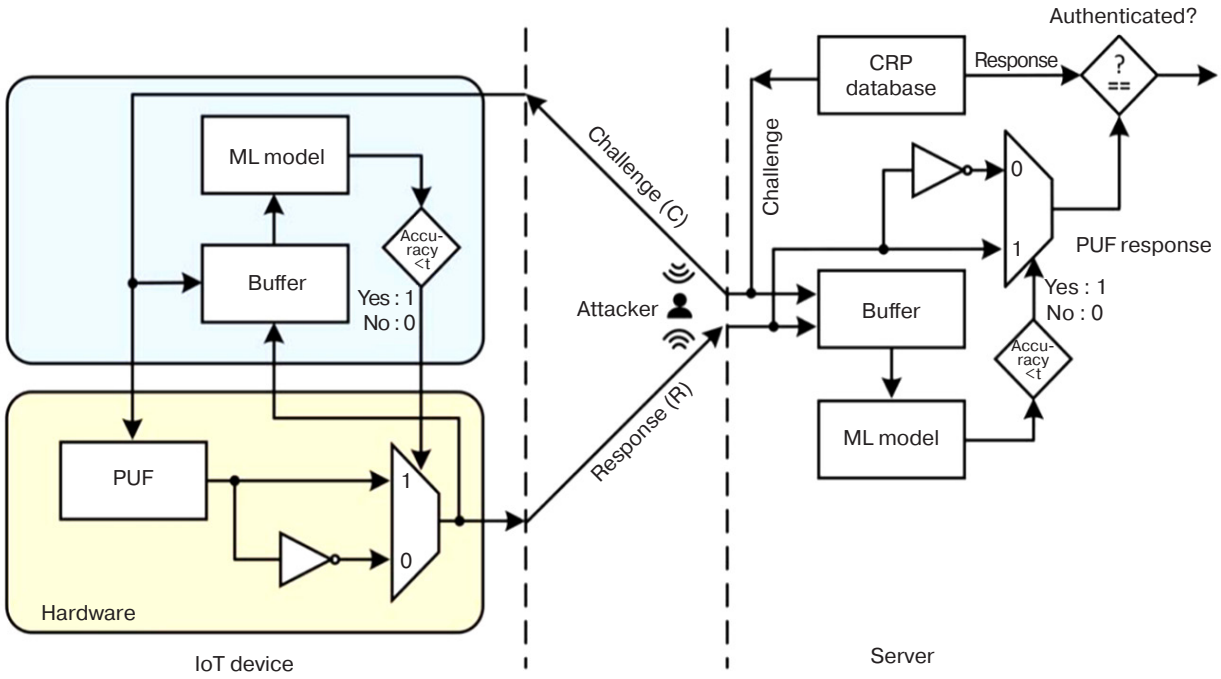


Fig. 7. Block diagram of the error injection method

data leakage while preserving the ability to correct errors [22]. These methods aim to reduce the correlation between auxiliary data and PUF responses, thereby making it more difficult for attackers to extract useful training data.

The practical effectiveness of both attacks and defenses can be understood through research into physical implementation [3, 18, 19]. Significant differences in the success rates of ML attacks and the required amounts of training data have been revealed by empirical studies of various PUF architectures. The field-programmable gate array implementation of CRC-PUF is particularly noteworthy for its ability to withstand ML attacks while still maintaining efficient area and power consumption. The achievement during development of normalized inter-HD and intra-HD values of 0.5065 and 0.0696, respectively, indicates favorable statistical properties for security applications.

Area and power analyses confirm the possibility of implementing ML-resistant PUFs at a reasonable cost as compared to classical architectures. For example, the requirement of 1032 equivalent gates in CRC-PUF as compared to 646 for the base Arbiter PUF is a modest increase, but one that results in a significant improvement in security. Similarly, while the ML resistant PUF architecture achieves ML resistance, its area significantly exceeds the practical limits for embedded applications.

More complex architectures demonstrate varying degrees of PUF resistance. Arbiter-type functions using multiple XOR cascades require an exponentially increasing number of CRPs to mount a successful attack, yet remain vulnerable to advanced techniques when sufficient data is available [17, 19, 20]. Conversely, reducing the frequency of successful attacks to below 60% even when using large training data sets represents a significant improvement over classical design.

Implementing PUF using an array of subthreshold voltage dividers in 65 nm CMOS technology achieves promising results with a power consumption of only 0.43 pJ/bit [3]. When exposed to various ML attacks, including logistic regression, artificial neural networks, and support vector machines with nonlinear radial basis function kernels, the prediction accuracy remains at around 60%, demonstrating practical resistance to ML.

Research directions for methods of protection against ML attacks

Developing ML-resistant PUFs requires a balance between security requirements and practical considerations such as size, power consumption, reliability, and performance [3, 18, 19]. High-security designs may require additional hardware, more advanced error correction mechanisms, or reduced performance, all of which may be unacceptable for cost-sensitive applications.

Analysis of ML attacks on PUFs reveals fundamental limitations in the security provided by current implementations. Many practical PUF implementations

do not achieve the maximum theoretical level of entropy, making them vulnerable to statistical, pattern-based ML attacks [16, 17, 22]. The mathematical models that underpin PUF designs often contain learnable patterns that can be exploited by sophisticated ML algorithms. Therefore, achieving true resilience against ML attack may require fundamentally distinct approaches to PUF design rather than incremental enhancements to existing systems.

The scalability of ML attacks poses a significant challenge for the implementation of PUFs in the future. As ML techniques continue to advance and become more accessible, the likelihood of successful attacks decreases. This trend indicates that PUF security should not rely solely on computational complexity, but rather focus on fundamental information-theoretic principles.

Although the challenge restriction approach is theoretically sound, it severely limits the potential of strong PUFs and thus may not be practical for applications requiring frequent authentication or key generation [16, 21]. By making strong PUFs as ineffective as weak PUFs, this approach negates many of the initial motivations for their development.

The error correction requirements present another significant challenge. Study [22] reveals that auxiliary data is vulnerable, suggesting that seemingly secure error correction approaches may introduce vulnerabilities. When selecting error correction codes, it is essential to consider traditional factors such as correction capability and implementation complexity, as well as security against ML attacks through the analysis of auxiliary data.

Analysis of PUF-based authentication and key exchange protocols reveals varying degrees of vulnerability to ML attacks [21, 23]. Protocols based on direct CRP exchange are particularly vulnerable to simulation attacks when there is a large number of CRPs. The security of these protocols primarily relies on PUF resilience against ML attacks rather than on protocol-level protections.

Recent advancements in protocol design aim to minimize the information available to intruders while maintaining functional requirements [23]. Methods such as secure multi-party computing, homomorphic encryption and zero-knowledge proofs enable the use of PUF without disclosing CRP to potential attackers. However, these approaches often incur significant computational costs, which may be impractical for devices with limited resources. More complex protocols use challenge obfuscation, response masking, and temporary security mechanisms to restrict intruders' capabilities [20, 21]. Nevertheless, many of these approaches have proven inadequate against determined opponents with access to modern ML techniques. The main challenge lies in balancing security with practical constraints such as communication costs, computational requirements, and error tolerance.

Integrating PUFs into complex systems creates additional opportunities for attacks through side-channel analysis to introduce malfunctions and vulnerabilities at the system level [21]. As PUFs become more widely adopted in mission-critical applications, the incentive for sophisticated attacks increases, necessitating more robust security analyses and protection mechanisms. The rapid development of ML methods poses ongoing challenges for PUF security. Emerging techniques such as meta-learning, transfer learning, and multitask learning have the potential to create attack strategies that can overwhelm existing defenses [20, 23].

In order to facilitate fair comparisons between different attack designs and techniques, it is essential to develop standardized methodologies for evaluating the security of PUFs [17, 21]. Future PUF research should focus on developing architectures with provably secure properties rather than simply relying on empirical resistance to current attack methods [16, 18]. Due to the use of different datasets, attack parameters, and success criteria in existing assessments, it is difficult to make an objective comparison of the relative security levels of different systems. Information-theoretic approaches capable of ensuring security even against unlimited computational resources provide a sounder basis for long-term security.

The dynamics of the evolution of trusted design systems suggest that in order to achieve long-term security, it may be necessary to transition from approaches based on incrementally improving current architectures to a fundamentally different approach that leverages information-theoretic security principles [24, 25]. The findings of this study emphasize the significance of careful threat modeling, conservative security assumptions, and robust protection strategies for professionals implementing PUF-based systems [26–29].

PUF IMPLEMENTATION EXAMPLES

Depending on the level of protection required by the embedded chip in the device (weak or strong), PUF modules are used in a variety of applications to safeguard devices. PUF responses can be used directly for authentication in a manner similar to biometric verification. As demonstrated in the first part of this publication series [1], the cutoff value used to determine positive authentication relies on intra-HD and inter-HD histograms. Typically, when the histograms overlap, the cutoff value is set by balancing the likelihood of

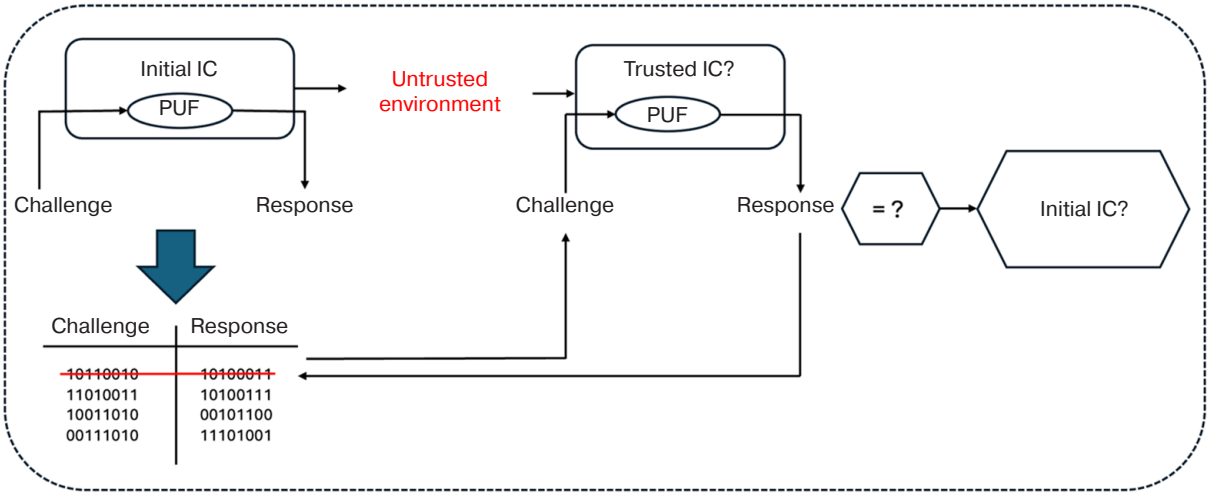


Fig. 8. PUF application in authentication protocol [40]

false positives (false acceptance rate, FAR) and false negatives (false rejection rate, FRR) using an approach similar to those employed in metrology. The optimal choice, which minimizes the sum of FARs and FRRs, is achieved by setting a threshold at the intersection of the two histograms. However, other trade-offs may be necessary for specific applications. Here it should also be noted that unique identification is only possible with a high degree of certainty if the response contains sufficient entropy relative to the sample size.

PUFs are used for the following:

1) the mutual authentication of IoT devices [30, 31];
2) the identification of message flows involving authentication requests from mobile unmanned aerial vehicles equipped with a PUF and ground stations [32, 33];
3) the communication between devices, sensors, and a health monitoring system in which the server is also equipped with an appropriate PUF, and a secure database is used to store the collected variants of CRPs [34];
4) the protection and safety of vehicles [35, 36];
5) the security and confidentiality of data transmission in networks [37–39].

Device identification

At registration, the CRP from each PUF is stored in the database along with the identification data of the physical system in which it is built. As outlined in [1], during the identification process, the verifier compares the random CRP pair with the PUF responses for the presented system stored in the database. If the observed response is close enough to the response in the database, authentication succeeds; otherwise, it fails. To prevent repeated attacks, each CRP should only be used once for each PUF instance and removed from the database after identification (Figs. 8 and [40]).

Generating encryption keys

Since the PUF is based on randomness due to technological tolerances, no programming is required when generating or storing secret keys based on the PUF. Due to this randomness being fixed in the microscopic physical details of the chip, the key remains unchanged and can be reproduced several times. This eliminates the need for non-volatile key memory, providing additional protection against third-party channel attacks.

However, since PUF responses are typically noisy, an intermediate processing step is necessary to extract the cryptographic key. This problem, which is known in information theory as extracting an encryption key from a noisy signal, is typically solved using a two-stage algorithm. The PUF request during the first generation stage involves the algorithmic generation of a secret key and some additional auxiliary data. This key and the auxiliary data are then stored in a secure, device-independent database. During the reproduction stage, the auxiliary data is provided to the algorithm, which uses it to extract the same key from the PUF created during the generation stage. Such algorithms can be designed in such a way that the key remains top secret even if the auxiliary data are transmitted openly. To ensure the reliability of this method of key generation, special troubleshooting methods are employed [41, 42], such as the generation (Gen) and playback (Rep) algorithms. These algorithms ensure the extraction of stable, reproducible information from PUF responses by comparing two messages composed of noisy, encrypted, random data with unclassified auxiliary data

attached for identification purposes. Practical examples of these algorithms are provided in [43–45].

The use of PUF allows for the implementation of hardware-based cryptography as a special method. In this method, the digital cipher key is not stored in memory, while the secret element consists in the unique behavior of the PUF instance in the embedded device. This significantly hinders attempts by attackers to use non-volatile memory as a means of obtaining useful information. Since the PUF can also be used to detect unauthorized access to the key store, device-entangled cryptography is closely related to proven physical security (see, for example, [46]).

Intellectual property protection

Protecting the intellectual property of chips is a crucial issue for semiconductor companies due to numerous security threats that can result in financial losses. These threats include forgery, cloning, reverse engineering, and reliance on substandard components. Studies in this area include works on the hardware protection of SRAM PUF blocks on programmable logic ICs and methods of preventing the copying of IP addresses to protect against unauthorized access to firmware, based on PUF and neural network models [47–49].

Random number generation

Silicon PUFs are used as a source for generating random numbers, which are necessary for cryptographic systems. Exemplary studies in this domain include [50, 51], wherein the authors employ PUF responses to generate the primary data for random number generation.

Payment protection

In [52, 53], PUF responses are used in authentication bit strings, encryption keys, and electronic cash token generation (PUF-Cash). The aim is to develop an application architecture that can be used in electronic payment schemes. It also ensures the anonymity of user identities for organizations such as banks and sellers. It is proposed in [54] that private keys, secure communication and data authentication be provided by equipping credit/debit cards with built-in PUF chips.

Protection of memory and software integrity, ensuring secure communication

Currently, a number of companies and research centers specialize in developing special measures to increase the power of equipment and software. A typical example is the technical documentation of an association [54], which was created to develop, define and promote open, vendor-independent, global industry standards. These standards support a hardware trust framework for interchangeable trusted computing platforms. The specification of this framework refers to large-scale security threats arising from geopolitical and data sovereignty issues, which threaten to slow down the adoption and growth of the IoT industry. This in turn stimulates the need to create reliable supply chain ecosystems in Asia, Europe, and the Americas. Here, the importance of the keys used for digital signing and verification in ensuring the security of the entire system, along with cryptographic functions that provide a secure process for loading operating systems, is emphasized. The main and only effective means of ensuring safe operation is recognized as the use of microcircuits equipped with a PUF, in particular, a new type developed by eMemory Technology Inc.[18] The NeoPUF technology developed by this company exploits differences in the tunnel effect of the oxide layer to achieve high PUF performance (inter-HD = 50%; intra-HD ~ 0%).[19]

An example of using PUF to protect the confidentiality and integrity of instructions and data in memory from physical and software attacks is given in [38, 55].

Software licensing is required to protect against unauthorized modifications and usage on unauthorized platforms. The idea behind using the PUF is that critical operations such as starting or restarting the system are performed using the generated keys, while the software interacts with the PUF [56]. A software licensing mechanism based on PUF is proposed in [57]. The user's computer is equipped with a PUF based on the SRAM scheme to provide it with a unique identification. When a user needs to purchase the necessary software, the company establishes a connection to the user's computer to obtain the PUF output and make it available as a license in the software. During installation by the client, an authentication process occurs between the software and the personal computer. The built-in license is then compared with the PUF output to ensure that the software instance is only executed on a specific device.

Recently, a new patented PUF approach called equipotential timing has been proposed by Granite

[18] eMemory Technology Inc. https://www.ememory.com.tw/. Accessed July 19, 2025.

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

Mountain Technologies.[20] This approach uses gigabyte PUF (Giga-PUF) to design features that cannot be physically disabled. The equipotential timing approach provides stable, synthesized PUF implementations that can be implemented as soft IP blocks and integrated into any design at a low cost. Such Giga-PUFs can be quickly and easily scaled to any circuit, even across technology nodes and silicon fabricators. This gives all companies access to PUF exponential solutions that provide true trust in the hardware, thus enabling them to protect their products.

Another application of the PUF modules included in the IC is to enable secure communication for the authentication of IoT devices in the key exchange protocol [58–60].

CONCLUSIONS

As confirmed in this review, analog and passive PUFs represent an important class of hardware security primitive that complement latency- and memory-based solutions. While analog circuits made from transistors and diodes offer high entropy and low response power consumption, careful stabilization and calibration are required to counteract the effects of PVT factors and ageing.

Passive approaches, such as resistive fingerprints of the power grid Via PUF and Coating PUF, are attractive due to their minimal overhead, high stability and counterfeiting complexity.

For practical application, the following are recommended:

- use of internal compensation and auto-zero mechanisms, as well as rejection/masking of unstable elements;
- single standardized digitization chain (sensor—amplifier/comparator—code post-processing);
- integration with light error correction techniques or phase filtration where justified;
- assessment of resistance to simulation attacks and side channels, taking into account analog specifics (temperature, power supply, and noise injection).

The development of ML has revealed the vulnerability of many classic PUFs, particularly in linear delay models. The insufficient design complexity (e.g., XOR and cascades) results in leaks of auxiliary or side data to enable attacks without direct access to the responses.

Defense mechanisms demonstrate varying degrees of success, while architectural innovations such as the CRC-PUF offer increased resistance to ML attacks. However, the fundamental issue remains that most contemporary PUF designs are based on mathematical models that can be trained using complex algorithms.

When selecting suitable PUF architectures, error correction codes and operational protocols, it is important to consider not only current attack methods, but also potential future advances in ML techniques. As this area evolves, it will be essential to integrate PUF security research with broader developments in ML, cryptography, and hardware security in order to develop reliable solutions. Here, the ultimate goal is to develop truly unclonable functions that retain their protective properties even in the face of highly sophisticated computing attacks.

PUFs can be used as important building blocks in authentication systems, particularly in hardware tokens with limited resources and IoT systems (see the services of eMemory Technology Inc. in particular).

Promising future research directions include the following:

1) standardizing and developing algorithms and analysis tools, and increasing energy efficiency;
2) improving security and protection against attacks by analyzing side channels and ML attacks;
3) reducing environmental impact;
4) applying new special algorithms, particularly controlled and reconfigurable PUFs;
5) developing PUFs based on promising physical effects, particularly quantum PUFs utilizing nuclear magnetic moments, resonant tunnel diodes, plasmon and lanthanide luminescence, Josephson transitions, changes in electron flow in nanocells (Aaron–Bohm effect), and quantum entanglement.

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

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).

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.

REFERENCES

1. 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. Available from URL: https://www.researchgate.net/publication/321669464_VLSI_Architecture_of_Turbo_Codes-IP_Secure_With_PUF_for_DSRC_systems. 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

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

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

Translated from Russian into English by K. Nazarov
Edited for English language and spelling by Thomas A. Beavitt