A Review of Physical Unclonable Functions (PUFs) and Its Applications in IoT Environment

Aruna Yadav, Sanjeev Kumar, and Jagendra Singh

Abstract This paper describes various studies about physical unclonable functions, and it inspires use of physical unclonable functions over conventional security mechanisms and compares them in many aspects. It categorizes physical unclonable functions as strong physical unclonable functions and weak physical unclonable functions. For any communication in a network, authentication scheme for nodes, server, router, and network gateway is presented and procedure of communication is explained and presented through architecture. This paper explained problems faced by smart devices due to attacks on security. Finally, this paper reviews various emerging concepts of physical unclonable functions and its advancement.

Keywords Physical unclonable functions · Cryptographic hardware · Hash function · Authentication · FPGA (field programmable gate arrays) · Randomness

1 Introduction

Physical unclonable functions provide improved security in terms of low-cost authentication and in key creation applications. Physical unclonable functions are used for secret key storage without secured EEPROMS. Physical unclonable functions can do this because they do not store secret in digital memory rather; they find out some undisclosed features from physical characteristics of integrated circuit like manufacturing differences of gate delay as a physical characteristic. There are many reasons physical unclonable functions are better than standard secure digital storage. Physical

A. Yadav (✉) · J. Singh
Bennett University, Greater Noida, India
e-mail: e19soe808@bennett.edu.in

J. Singh
e-mail: jagendra.singh@bennett.edu.in

S. Kumar
KIET Group of Institutions, Delhi-NCR, Ghaziabad, India
e-mail: sanjeev.yadav@kiet.edu

Y.-C. Hu et al. (eds.), *Ambient Communications and Computer Systems*, Lecture Notes in Networks and Systems 356, https://doi.org/10.1007/978-981-16-7952-0_1

unclonable functions use cryptographic hardware which are nominal in price. Physical unclonable function consumes less power and easy to fabricate. Generally, invasive attacks are possible only if attacker able to change physical characteristic, that is main reason to secure physical unclonable functions continuous active anti-tamper mechanism is not needed. Physical unclonable functions derive secrets manufacturing variability of Integrated circuits. No two integrated circuits can be same even there must be some slight difference two integrated circuits even if manufacturing and masking process is same. There are many applications that integrate physical unclonable functions into integrated circuits. Physical unclonable functions can be categorized as: strong physical unclonable functions and weak physical unclonable functions. For authentication purpose, strong physical unclonable functions are used. In storage purpose, weak physical unclonable function works efficiently. Focus of physical unclonable function is to decide c in $f(c)$, where x is parameter in which function is dependent and that parameter lies on manufacturing variability. Basic difference between strong and weak physical unclonable functions lies on domain of $f(c)$. For strong physical unclonable functions, domain is large, while for weak physical unclonable functions, domain is small.

Consider c as challenge for function; then response given by function is r, $r = f(c)$; physical unclonable functions ensures unpredictability: An adversary cannot predict its response until it recognizes intrinsic properties; robustness: Response of physical unclonable functions is steady over time; uncolorability: An adversary cannot mimic the behavior of weak physical unclonable functions on another device. Since weak physical unclonable functions have less numbers of challenge response pairs, these pairs stored secretly. Mostly weak physical unclonable functions are used for secret key derivation. Physical unclonable functions provide secured storage that is why physical unclonable function response is never exposed. So, response can be used as secret key to encrypt or decrypt data. While in strong physical unclonable functions authenticated directly without using cryptographic hardware, responses are stable to environment, attackers cannot expect response. Weak physical unclonable functions also able to provide authentication with the use of HMAC. Models of weak physical unclonable functions a.

Both weak and strong physical unclonable functions rely on analog physical properties of the fabricated circuit. Example of strong physical unclonable function architectures: Optical physical unclonable function: It was first implementation of a strong physical unclonable function.

Another example of strong physical unclonable function is Arbiter physical unclonable function: There are some limitations due to macroscopic approach of optical physical unclonable function. Silicon implementations were used for strong physical unclonable function, manufacturing variability works as challenge, and that is input for unclonable randomness. In case of Arbiter physical unclonable function, manufacturing variability in the gate delay of each multiplexer produces an edge at the latch and that latch behaves like Arbiter [1]. There are large numbers of concepts for physical unclonable function that are emerging. It is also shown that rate of new physical unclonable function is increasing. It is also observed that concept behind it is randomness. There are several physical unclonable function concepts

for electronic application, so are many options of physical unclonable function, by comparing merits and demerits best suitable option, can be chosen. Choice depends on application.

Examples of weak physical unclonable function are static RAM and ring oscillator physical unclonable function.

In low-cost authentication physical unclonable functions: A strong physical unclonable function can be replacement for secured memory and cryptographic hardware on an embedded system. Strong physical unclonable functions do not demand for anti-tamper circuit structure, any cryptographic hardware, or any additional thing. Strong physical unclonable functions demand less power, area. Conceptually a planned, steady broad evaluation is mandatory to regulate the optimal physical unclonable functions concept and explicit modification for any given purpose should outstanding for all.

2 Literature Survey

Recently, number of concepts related to physical unclonable functions increased, and concepts utilize explicit source of randomness, concerning distinctive material and skills in field of physical unclonable functions and using new materials and technologies in the field of physical unclonable function [2].

Hammouri et al. [3] presented tamper proof lightweight challenge response authentication scheme that varies according to noisy-level physical unclonable functions. Compared to earlier projected structure, this scheme does not require cryptographic hash function which is more expensive for ultra-low power applications. The security against passive attacks is claimed considering that no polynomial time algorithm presents for enquiring threshold of almost half cases.

Reza et al. [4] described application scenario where all previous physical unclonable function-based authentication schemes failed and then used converse physical unclonable function-based authentication scheme.

Wang et al. [5] proposed strong physical unclonable functions that are secured against machine learning attacks on conventional and quantum computers. Lattice physical unclonable functions built through weak physical unclonable functions. Lattice physical unclonable functions are lightweight, digital uses concept of pseudo-random number generator. Delvaux [6] explained physical unclonable function which is a circuit whose input–output conduct is dependent on manufacturing random variations and investigated significance of 21 physical unclonable function-based protocols. Work out proficient predictive model of Arbiter physical unclonable functions.

Calhoun [7] enlightened physical unclonable function-based e-cash protocol and analyzed arithmetical features of the produced authentication bit strings and specified that physical unclonable function cash is robust, scalable and can be implemented in commercially hardware.

Mukhopadhyay et al. [8] illustrated Internet of Things (IoT) which is network of large number of exclusive distinguishable intercommunicating smart devices. Lightweight authentication protocol for these smart devices should be protected against physical attacks. Explored design tasks, operating principles and defense approaches.

Kong and Koushanfar [9] illustrated strong physical unclonable function which is a circuit structure that abstracts large number of unique chip signs and described information for process variation (process variation produces inherent randomness in silicon structure and disturbs threshold voltage consequential power consumption and delay around silicon chip), circuit aging technique (circuit aging is process in which efficiency of circuit is degraded by its usage) and delay model.

Yin and Qu [10] explained silicon-based physical unclonable function that operates the differences through silicon manufacturing process to abstract information that is exclusive for each chip. Many research shows that physical unclonable function can be used in security of applications.

Bin chen [11] described problem of secret key generation over noisy and biased physical unclonable function to resolve this problem. Polar code-based syndrome structure is applied to break the concept of polarization to cooperation of secret key's randomness and decodability so it will be able to minimize the effect of bias on secret key theft.

Guo et al. [12] explained that physical unclonable function provides challenge–response sets for authentication of devices, but many conventional strong physical unclonable function designs represented by the Arbiter physical unclonable function are hard to implement on FPGA and then suggested new lightweight strong physical unclonable function that can enthusiastically reconstruct while maintaining high entropy and large CRP space.

Rostami [13] illustrated and analyzed two lightweight and secured protocols based on substring matching of physical unclonable function response strings to accomplish authentication and session key exchange; simultaneously, this protocol ensures robustness against noise in the physical unclonable function response string.

Chatterjee et al. [14] developed a secure physical unclonable function-based authentication mechanism and identity without certificate identity protocol. Asymmetric behavior of protocol resolved problems are due to challenge–response pair-based physical unclonable function authentication scheme; it is advantageous over security susceptibility of low hardware.

Kumar et al. [15] explored that ensuring data security in smart devices from external attacks is a tedious job. Generally, traditional cryptographic techniques preserved keys in nonvolatile memory that is susceptible to physical attacks. Physical unclonable functions have capability to save smart devices from physical attacks as keys are not stored in nonvolatile memory and tough to regenerate. In new generation of electronic devices, usage of semiconductor material, for example, carbon nanotubes or 2D materials are preferred reason, is better electrical, optical, mechanical, and thermal properties.

Gu et al. [16] proposed TCR physical unclonable function design dependent on tristate inverter matrix. This design has feature of ultra-lightweight and reconfigurable as compared to RO physical unclonable function design. MOS simulation and FPGA implementation showed and verified the better, consistent, and unique behavior of TCR physical unclonable functions.

Venkata et al. [17] illustrated issues regarding Internet of Medical Things. Adding extra security features to existing electronic devices must not enhance power consumption and diminish battery life. Proposed design of physical unclonable function was advantageous for authentication techniques that is power optimized hybrid oscillator Arbiter physical unclonable function. This physical unclonable function design was verified through 32 nm FinFET and Dpoingless junctionless FETs.

Das et al. [18] discussed new physically secure lightweight anonymous user authentication protocol for Internet of Things applying physical unclonable function; this work is carried out through the tough analysis of ROR model and verified formal security through AVISPA tool and informal security. Real-world implementation of this scheme is analyzed using NS3 simulation tool.

Byun [19] presented novel authentication technique for two parties containing two authentication factors (1. Own physical unclonable function embedded device and 2. long-term secret.) willing to authenticate each other through mutually decided session key over a distributed network. A novel concept DEVICE ORACLE is discovered and presented distinct physical unclonable function embedded AKE ensuring verified security.

Barbareschi et al. [20] extended existing protocol PHEMAP which ensures mutual hardware authentication based on physical unclonable function for one-to-many scenario to CE-dependent Internet of Things scenario, mainly emphasized on complete mutual authentication scheme dependent on PHEMAP whose significance to achieve requirements and restrictions of three-tier Internet of Things (Table 1).

3 Classification of Physical Unclonable Functions

3.1 Classification Dependent on Used Physical Employment

Physical unclonable functions used till now can be roughly categorized into four major groups based on the technology role in physical engagement: optical physical unclonable function, silicon physical unclonable function, coating physical unclonable function, and acoustic physical unclonable function (PUF).

Optical physical unclonable function (OPUF):
It first proposed physical unclonable function, though initially projected as the physical characterization of a particular one-way function used for cryptography. Principal constituent of the optical physical unclonable function shows clear token using arbitrarily fixed smattering elements. After radiation through the laser, a multifaceted image using sunny and shadowy adverts ascends, known as “speckle pattern”. A

Table 1 Physical unclonable functions' evolution

Advancement in physical unclonable functions
Integrated Circuit identification using device mismatch in year 2000
Physical One-way function in year 2001
Physical Random Function in year 2002
Arbiter physical unclonable function and Feed Forward Arbiter in 2004
Coating physical unclonable function in 2006
Latch physical unclonable function, XOR-Arbiter physical unclonable function, Ring Oscillator physical unclonable function and Static RAM physical unclonable function. in 2007
Butterfly physical unclonable function, D Flip-Flop physical unclonable function, Tristate Buffer physical unclonable function, Lightweight Secure physical unclonable functions in 2008
Power Grid physical unclonable function in 2009
Glitch physical unclonable function, SHIC (Super High Information Content) physical unclonable functions in 2010
Mecca physical unclonable function, Bistable Ring physical unclonable function, Ultra-low Power Current-Based physical unclonable function, Current Starved Inverter Chain physical unclonable function and Logically Reconfigurable physical unclonable function in 2011
Converse Physical function in 2012
Light weight authentication protocol 2014
Robustness against noise in the physical unclonable function 2015
TCR physical unclonable function in 2017
optimized hybrid oscillator arbiter physical unclonable function in 2018
Distinct physical unclonable function embedded AKE in 2019

Gabor filter fits in this scenario as a worthy feature extractor specially for these types of configurations; then filter production is the rejoinder of such type of optical physical unclonable function, though the physical factors of the laser (location, wavelength, and orientation) set up the challenge. Composite environment of the communication of laser light through sprinkling particles, the reactions are extremely arbitrary and exclusive. The great requirement of the response arranged the precise microscopic physical particulars of the optical token reasons two similarly formed tokens to display different reactions to the identical challenge, then escapes a specific token and they can be duplicated through great accuracy.

Silicon physical unclonable function:
It exploits strong CMOS manufacturing discrepancies that is the outcome provided inescapable inadequacies in recent integrated circuit manufacturing methods. Manufacturing discrepancy of factors like dopant absorptions and line breadths are obvious like differences in terms of timing performance among cases of the identical integrated circuits. Such time differences dignified for an appropriate circuit system, if required then encoded. Preferably, a silicon physical unclonable function should not involve a nonconformity from the normal CMOS treating steps and implementable with the help of EDA design flows. It is noticed that such type of physical unclonable

functions is inclined toward temperature deviations that finally reward schemes to work the system appropriately.

Coating physical unclonable function:
It is a physical unclonable function in which a defensive coating for integrated circuits is the basis of unpredictability. The dense coating substance is fixed in di-electric elements, which have arbitrary specifications regarding location, shape, and dimension. Underneath the coating layer, an arrangement of sensors for metal wires is applied to scope the capacitance for coating. Calculated values are arbitrary just cause of the arbitrariness is there in the coating, generates the responses to their challenges, all are specific to the voltage of a definite amplitude and frequency, practical to a section of the sensor array. As there are implicit randomness, di-electric constituents and these values are tough to generate two values as all sensors generate similar values. Although there are some disadvantages to use coating physical unclonable function is that it allows restricted number of challenge–response pairs. While the advantage of coating physical unclonable function is less price of their fabrication, an advantage of coating physical unclonable function is that adaptable to identifying some physical changes.

Acoustic physical unclonable function:
This physical unclonable function is constructed based on properties belongs to acoustical wave propagation. Any oscillating voltage of electrical signal is converted into mechanical vibration through a transducer. These vibrations transmitted as a sound wave in a specific solid medium and disseminates on the arbitrarily distributed inconsistencies of the solid medium. The reflections of these sound waves are dignified by another transducer which changes these vibrations again in the form of electric signal. It shows that the reflections of each token are exclusive.

3.2 Classification Based on Response Collection Mechanism

Intrinsic physical unclonable function-
Intrinsic physical unclonable function is embedded inside the hardware system, it preserves without any modification done to produce randomness, and obviously any opponent cannot read it exactly due to this feature that a reader will not disturb its output value. The measurement settings are inbuilt in the physical unclonable function and is integrated on chip. Such type of physical unclonable functions (like Silicon physical unclonable functions) are comparatively easy to build and control because these PUFs usually do not required any preprocessing and post-processing, although some error correction for noise is required, but these PUFs are prone to security susceptibilities.

Controlled-physical unclonable function-
Controlled-physical unclonable function relates to an algorithm in a very special way and that algorithm controls these types of PUFs. Any changes in the algorithm

are reflected in the controlled-physical unclonable function. This algorithm discourages the reader to directly challenge the physical unclonable function and limits the information about responses that is seen by the outside world. A controlled physical unclonable function makes enumerating physical unclonable function responses harder and stops man-in-the-middle attacks. In addition, some physical unclonable functions require external or extra logic to explicitly introduce randomness (such as the optical and coating physical unclonable function) can also be considered under this category.

4 Authentication Scheme

We discuss a scheme that defines working of authentication protocol. A network corresponding several nodes (named as node1, node2, node3, noden) acts as sources and receiver of information. Network consists of some server nodes (named as SN1, SN2,…SNi) put upon to manage the communication of each node in its range and forward the data to a router (named as router1, router2…, routerj). The router therefore forwarded the information to the cloud through and through the network gateway. The data nodes have limited computational resources, while the server nodes and advanced nodes are comparatively resourceful. It is pretended that the server nodes and the data nodes are dispersed in the way that each data node is always inside the read range of one server node. Every data node, server node and router need to be authenticated so mount a physical unclonable function instance on them. Written account that in the given architecture, there is no definite key storage available for the nodes. We depicted our protocol for data nodes and server nodes. The protocol grows through the following steps:

Firstly, enrollment phase is performed, formerly each data node is assigned to a particular server node. Through this, a CRP database created for the physical unclonable functions contained in each node in the server node corresponding to the data node. In next phase if two nodes want to communicate under same server, their server node authenticates those nodes, then generation of their public/private key pairs occurred, and then share secure key pair. In last phase, secure communication executed, the two nodes send and receive the message securely over the network using the keys, without any intervention of the server. If a node1 wants to communicate to node2, then server1 needs to authenticate both of these nodes before key generation and communication between these two nodes. Similarly, if server1 wants to communicate with server2, then router1 needs to authenticate both these servers before key generation and communication. In the same way if a router1 wants to communicate with router2, then network gateway needs to authenticate these two routers, before key generation and communication between these two routers. If a node wants to move from one server to another server, then all things will come through by server2 now onward as mentioned in Fig. 1.

In enrollment phase, server sends random challenge to the mobile data node; then node employs challenge c to its physical unclonable function and produces response

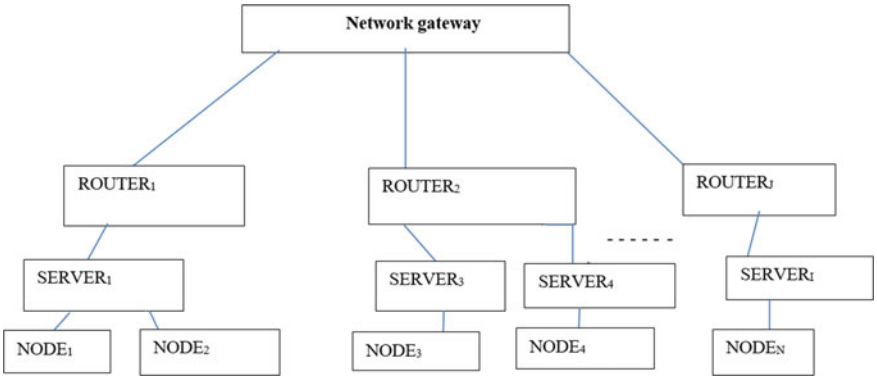

Fig. 1 Communication architecture of different types of nodes

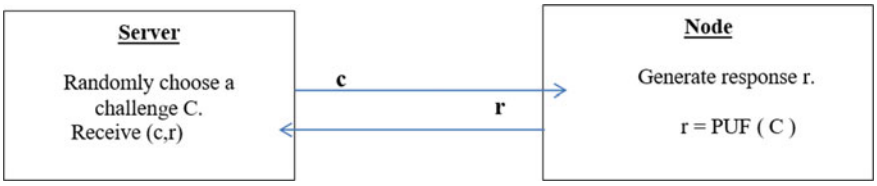

Fig. 2 Enrollment phase

r and send back to its server, then server update its database by (c, r) pair as shown in Fig. 2. These types of many challenge response pairs are stored in database according to the memory of server. This database is secured.

Second phase Authentication Phase: with the help of challenges $c1$, $c2$ for node1 and $c3$, $c4$ for node 2 and corresponding responses $r1$, $r2$ for node1 and $r3$, $r4$ for node2 applied hash function on them calculated $\Delta 1$ and $\Delta 2$ for any particular timestamp.

$$Q1 = \text{Hash function } (\text{puf1}(c1) \,||\text{puf1}(c2) \,||ts)$$
$$Q2 = \text{Hash function } (c1 \oplus c2)$$
$$\text{Private key} = t.Q1$$
$$\text{Public key} = t.Q2$$

Similarly, we will calculate for node2.

Last phase communication phase: In this phase, node1 sends message to node2. This communication is secured against CPA, CCA, repudiation attack [21].

5 Security of Physical Unclonable Function

New technologies do not bring only new facilities but also bring some weakness and unpredicted problems. We will discuss diverse physical unclonable function particularized attack.

These are some of the attacks:

Fault attacks on physical unclonable functions and fuzzy extractors:

Fault attacks initiate a suspected performance in that device when using over intense situation or compel it to function in a manner to enclose fault into it, provoking to work at immoderate temperature that will significantly change physical unclonable function random noise conduct on the far side of error correction potentiality of the circuit [18, 20, 22].

Side channel attacks on physical unclonable functions: Side channel attacks are hardware-dependent attack those wants to analyze hardware and interpret cryptographic key. As data processed in hardware are interrelated to each other, after analysis of hardware behavior attackers can go through analysis of data also. Attackers discover characteristics of section for example power consumption while analyzing secret information to be extracted [23].

3. Modeling attacks on delay-based physical unclonable functions: Goal of these types of attack is to figure out mathematics approximation for definite set of challenge response pair.

So that afterward approximation can help in forecasting of responses for unknown challenges with comparatively higher accuracy. Delay-supported physical unclonable function for example arbiter physical unclonable function and its variance is sensitized to these types of modeling attacks imputable to linear delay circuits [8].

6 Secured Physical Unclonable Functions Dependency

Physical unclonable functions have two important security parameters: unpredictability and unclonable property. Unclonable property is very much required characteristic that is not attained using traditional cryptographic methods. It can be divided into two forms again: mathematically unclonable and physically unclonable. A physical unclonable function is physically unclonable if the manufacturer cannot create a physical duplicate of the physical unclonable function with alike challenge–response pair. It is termed as existential unclonable. Generally, all silicon-based physical unclonable functions hold this property. Physical unclonable function is mathematically unclonable.

Also it is not probable to generate a mathematical approximation which exhibits the original Physical unclonable function conduct nearby previous one. There is no known silicon physical unclonable function that is mathematically unclonable. This mathematical unpredictability states that opponent cannot forecast same challenge response pair from already existing set of challenge–response pairs. Typically, *fn* (the

random function) is dignified through these security experiments which consist of an important knowledge as well as a challenge phase. In the learning phase, the opponent examines the behavior of the random function *fn* for particular input challenges × 1, × 2, …, *xn* (it can be specified by opponent). Finally, in the challenge stage, the opponent provides values in the set of (*x*, *fn* (*x*)) for some *x* × 1, × 2, …, *xn* surely. Normally, unpredictability is evaluated through of entropy or can specified as average min-entropy of physical unclonable function distribution [24].

7 Current Trend for Authentication Protocol

7.1 Ultra-Lightweight Authentication Protocol

Rather than to design an authentication protocol by using ultra-lightweight weight operations, it can be difficult when employs it from scrape. It is better to design ultra-lightweight authentication protocol using traditional challenge–response pair authentication protocol using cryptographic primitive for ultra-lightweight construction [13]. Ultra-lightweight primitives were not applicable to DES (data encryption standard it is a symmetric key algorithm), AES (advanced encryption standard is also known as Rijndael algorithm), and IDEA (International Data Encryption Algorithm is also known as improved Proposed Encryption Standard), though ultra-lightweight primitives are applicable to low-cost primitives designed for this purpose [25, 26].

7.2 Human-Dependent Authentication Protocol

This human-dependent authentication protocol needs lightweight evaluation dependent on learning parity with noise. Although human-dependent authentication protocol has many specific features, this protocol requires additional protective environment, when any third-party adversary involved in between message communication and tries to modify the message [17]. Then there were lot of works done to avoid man-in-middle attack in human-dependent authentication protocol with different versions like random-human-dependent authentication protocol, trusted-human-dependent authentication protocol, bilinear-human-dependent authentication protocol, and tree-human-dependent authentication protocol [10, 22].

8 Conclusion

We studied various research papers related to physical unclonable functions and their different models; illustrated their variations based on applications, devices, materials,

and attacks; and covered comparative analysis of physical unclonable functions with traditional techniques in many aspects.

We undergo through metrics of physical unclonable functions for any application and discussed authentication scheme of data nodes if they want to communicate each other considering all the conditions whether data nodes are under the same server, router, network gateway, or in different constraints. Current study on physical unclonable functions primarily concentrated on apprehension of the capabilities and limitations of physical unclonable function by detailed study of possible attacks on physical unclonable functions. This paper covers applications of physical unclonable functions in IoT environment as well as current trends of authentication protocol in scope of ultra-lightweight authentication protocol and human-dependent authentication protocol.

References

1. Herder C, Yu MD, Koushanfar F, Devadas S (2014) Physical unclonable functions and applications: A tutorial. Proc IEEE 102(8):1126–1141
2. McGrath T, Bagci IE, Wang ZM, Roedig U, Young RJ (2019) A PUF taxonomy. Appl Phys Rev 6(1)
3. Hammouri G, Öztürk E, Sunar B (2008) A tamper-proof and lightweight authentication scheme. Pervasive Mob Comput 4(6):807–818
4. Kocabaş Ü, Peter A, Katzenbeisser S, Sadeghi AR (2012) Converse PUF-based authentication. Lect Notes Comput Sci (including Subser. Lect Notes Artif Intell Lect Notes Bioinf) 7344:142–158, LNCS
5. Wang Y, Xi X, Orshansky M (2019) Lattice PUF: a strong physical unclonable function provably secure against machine learning attacks 2019
6. Delvaux J (2019) Machine-learning attacks on PolyPUFs, OB-PUFs, RPUFs, LHS-PUFs, and PUF-FSMs. IEEE Trans Inf Forensics Secur 14(8):2043–2058
7. Calhoun J, Minwalla C, Helmich C, Saqib F, Che W, Plusquellic J (2019) Physical Unclonable function (PUF)-based e-Cash transaction protocol (PUF-Cash). Cryptography 3(3):18
8. Mukhopadhyay D, Chakraborty RS, Nguyen PH, Sahoo DP (2015) Tutorial T7: physically unclonable function: a promising security primitive for Internet of Things, pp 14–15
9. Kong J, Koushanfar F (2014) Processor-based strong physical unclonable functions with aging-based response tuning. IEEE Trans Emerg Top Comput 2(1):16–29
10. Yin CE, Qu G (2014) Obtaining statistically random information from silicon physical unclonable functions. IEEE Trans Emerg Top Comput 2(2):96–106
11. Chen B, Willems FMJ (2019) Secret Key Generation over biased physical unclonable functions with polar codes. IEEE Internet Things J 6(1):435–445
12. Hou S, Guo Y, Li S (2019) A lightweight LFSR-based strong physical unclonable function design on FPGA. IEEE Access 7:64778–64787
13. Rostami M, Majzoobi M, Koushanfar F, Wallach DS, Devadas S (2014) Robust and reverse-engineering resilient PUF authentication and key-exchange by substring matching. IEEE Trans Emerg Top Comput 2(1):37–49
14. Chatterjee U et al (2019) Building PUF based authentication and key exchange protocol for IoT without explicit CRPs in verifier database. IEEE Trans Dependable Secur Comput 16(3):424–437
15. Kumar N, Chen J, Kar M, Sitaraman SK, Mukhopadhyay S, Kumar S (2019) Multigated carbon nanotube field effect transistors-based physically unclonable functions as security keys. IEEE Internet Things J 6(1):325–334

16. Cui Y, Gu C, Wang C, O'Neill M, Liu W (2018) Ultra-lightweight and reconfigurable tristate inverter based physical unclonable function design. IEEE Access 6:28478–28487
17. Yanambaka VP, Mohanty SP, Kougianos E, Puthal D (2019) PMsec: physical unclonable function-based robust and lightweight authentication in the internet of medical things. IEEE Trans Consum Electron 65(3):388–397
18. Banerjee S, Odelu V, Das AK, Chattopadhyay S, Rodrigues JJPC, Park Y (2019) Physically secure lightweight anonymous user authentication protocol for internet of things using physically unclonable functions. IEEE Access 7:85627–85644
19. Byun JW (2019) End-to-end authenticated key exchange based on different physical unclonable functions. IEEE Access 7:102951–102965
20. Barbareschi M, De Benedictis A, La Montagna E, Mazzeo A, Mazzocca N (2019) A PUF-based mutual authentication scheme for cloud-edges IoT systems. Futur Gener Comput Syst 101:246–261
21. Chatterjee U, Chakraborty RS, Mukhopadhyay D (2017) A PUF-based secure communication protocol for IoT. ACM Trans Embed Comput Syst 16(3)
22. Yilmaz Y, Gunn SR, Halak B (2018) Lightweight PUF-based authentication protocol for IoT devices. In: 2018 IEEE 3rd international verification and security workshop, IVSW 2018, pp 38–43
23. Merli D, Stumpf F, Sigl G (2013) Robust authentication using physically unclonable functions. Lect Notes Comput Sci (including Subser Lect Notes Artif Intell Lect Notes Bioinf) 3(1):19–41
24. Oztürk E, Hammouri G, Sunar B (2008) Towards robust low cost authentication for pervasive devices. In: 2008 Sixth annual IEEE international conference on pervasive computing and communications. PerCom 2008, pp 170–178
25. Schoenmakers B (1998) Security aspects of the ecashTM payment system. Lect Notes Comput Sci (including Subser Lect Notes Artif Intell Lect Notes Bioinform) 1528:338–352
26. Van Herrewege A et al. (2012) Reverse fuzzy extractors: enabling lightweight mutual authentication for PUF-enabled RFIDs. Lect Notes Comput Sci (including Subser Lect Notes Artif Intell Lect Notes Bioinform) 7397:374–389, LNCS