*Journal of New Media*
DOI:10.32604/jnm.2020.014309
***Article***

Tech Science Press

# An Authentication Mechanism for Autonomous Vehicle ECU Utilizing a Novel Slice-Based PUF Design

**Jihai Yang[1], Zongtao Duan[1], Muyao Wang[2], Jabar Mahmood[1], Yuanyuan Xiao[1] and Yun Yang[1,*]**

[1]School of Information and Engineering, Chang'an University, Xi'an, 710064, China
[2]School of Telecommunications Engineering, Xidian University, Xi'an, 710071, China
[*]Corresponding Author: Yun Yang. Email: yangyun@chd.edu.cn

Received: 12 September 2020; Accepted: 14 September 2020

**Abstract:** Modern autonomous vehicles are getting progressively popular and increasingly getting closer to the core of future development in transportation field. However, there is no reliable authentication mechanism for the unmanned vehicle communication system, this phenomenon draws attention about the security of autonomous vehicles of people in all aspects. Physical Unclonable Function (PUF) circuits is light-weight, and it can product unique and unpredictable digital signature utilizing the manufacturing variations occur in each die and these exact silicon features cannot be recreated theoretically. Considering security issues of communication between Electronic Control Units (ECUs) in vehicles, we propose a novel delay-based PUF circuit using all the available logical components in every two-slice within Configurable Logic Blocks (CLBs) in Field Programmable Gate Array (FPGA) chips, which is significantly suitable for circuit authentication in ECUs of autonomous vehicles and is a significant improvement over the usual arbiter PUF in resource occupation in FPGA chips, that is to say it can get stronger resistance to security risks with less logic resource overhead. Our PUF design is resource efficient so that it can exactly be applied to the source-constrained devices such as in-vehicle ECUs. It effectively reduce the risk of the messages delivered between ECUs being tampered and then vehicle be illegally controlled by adversary. We simulated the proposed PUF circuit in simulator and implemented it on Xilinx boards under different conditions to obtain experimental results, the analyzed result proves that the proposed PUF satisfies the properties of Uniqueness and Stability. Finally, the ECUs authentication mechanism utilizing our PUF circuit is introduced.

**Keywords:** Novel PUF; slice; Autonomous Vehicles Authorization

## 1 Introduction

In-vehicle Electronic Control Unit (ECU) is control device for implementing functions of analyzing data, processing data, and transmitting data, through which the behavior of vehicle can be conveniently taken control. For electronic control units in autonomous vehicles, identity authentication for different ECUs is of first importance because ECUs with execution units must determine that the received control message is sent by a trusted ECU. Therefore, a complete unmanned vehicle control system must contain a reliable authentication mechanism for every ECU unit. However, among the technologies we know so far, there is basic no ECU certification for unmanned vehicles. In addition, we note that ECU is resource-limited device, that is to say it cannot offer enough memory space for heavyweight security devices.

Comparing to traditional encryption mechanism that stores cryptographic keys in Non-Volatile Memory (NVM), Physical Unclonable Function (PUF) tends to provide higher level security for hardware devices as it does not take the risk of being invaded by side-channel invasive attacks, and it is lightweight for external memory and battery is not required [1]. PUFs will produce unique response that is determined not only by the challenge input but the manufacturing variations occur in physical chips at very small regions. The manufacturing variability refers to changes of physical features exist within chips, of which gate delays, threshold voltages, doping concentrations, line widths and power-on state of SRAM are always be utilized to derive the response of certain circuits. It is extremely difficult to get the manufacturing variations of millimeter and nanoscale in physical media like silicon completely control, therefore random physical differences have natural properties that are difficult to clone and counterfeit. PUF is an input-output mapping in the form $r{:}\{0,1\}^{\wedge n} \rightarrow \{0,1\}^{\wedge m}$ where the input is n-bit binary vector and output is m-bit binary vector. A PUF circuit can receive $2^{\wedge n}$ different possible n-bit challenge vectors, each of which produces an m-bit output. Silicon PUFs can generate unique Challenge-Response Pairs (CRPs) for different integrated circuit instances.

In order to ensure the function of the autonomous vehicle ECUs is complete and the control information system cannot be maliciously attacked, it is necessary to build a authentication mechanism for receiver to identify the sender that want to deliver message is trustworthy before execute corresponding commands. Physical Unclonable Function as a promising class of hardware primitives [2] can deliver secure messages between various controllers and monitors, we propose a novel slice-based arbiter PUF design that uses most of the logic blocks in single slice to produce unique digital signature for every ECU and introduce the authentication mechanism before the process of receiving and processing the data from sender. Because this PUF makes most use of every slice resource, it is extremely source-efficient and adoptable for ECU devices.

**Our Contribution:** Inspired by issue that cryptographic key-based security mechanism are heavyweight by demanding resource more than most resource-constraint devices can provide and autonomous vehicles ECU without authentication mechanism takes terrible risks, we propose a novel lightweight PUF circuit that utilizes unclonable manufacturing variation to produce unique response. Then we implement proposed PUF circuit on Xilinx board and the results prove that the PUF circuit satisfies the property that to evaluate PUF design. Using the proposed PUF circuit, we are the first to introduce authentication mechanism for autonomous vehicles ECU to identify whether the other ECU is trustworthy or not before communicating with it.

**Paper Outline:** The remaining of this paper is arranged as follows. Session 2 gives the background. Session 3 introduces the construction of the proposed PUF design. The experiment and its results are presented in Session 4. Session 5 describes how the proposed authentication mechanism works on in-vehicles ECU devices. Finally, Session 6 concludes the paper and discuss the future work of this paper.

## 2 Related Work

Since PUF was firstly introduced by Pappu et al. using mesoscopic optical systems [3] in 2002, more and more scholars and scientists are involved in research from then on. Different architectures and different types of implementation methods emerge one after another according to different silicon features, among which (1) Ring Oscillator (RO)-based PUF is proposed by SUH et al. [4] aiming to enhance the stability of PUF circuit, it connects several inverters into a loop to produce a stable oscillating signal. The oscillating frequency value is determined by the internal delay of the inverter and the delay of the connection line also affected by the difference in manufacturing process, resulting in the frequency value certainly with randomness and unpredictability. (2) delay-based arbiter PUFs has an arbiter circuit to judge two signals race against each other in two parallel routes and produce the digital signature according to certain input challenges. In arbiter PUF circuit, it requires the symmetrical parallel transistors paths have same circuit structures, and for symmetrical Look-Up Table (LUT) in same stage in two paths receive same challenge signals, which determines the signal in circuit travels through to next stage via cross route or via direct route. In the whole propagation process, because of the variables in the manufacturing process and noise, the two paths accumulate different delay time, according to the difference in delay time then arbiter generates the PUF responses. (3) SRAM PUF is fabricated using the random coupling of the cross-coupled inverter at the moment of power-on. Due to process manufacturing variations, the driving capabilities of different drivers are different, and the difference in internal parameters of the transistor and the small voltage change caused by ambient noise cause a transition of the state to a steady state of logic-0 or logic-1. Anderson [5] proposed a rst PUF that makes use of underlying FPGA architecture and can be naturally embedded into devices and consumes very little area. Aseeri et al. [6] evaluates XOR PUFs' vulnerability utilizing machine-learning method and Machida et al. [7] introduced Double arbiter PUF that especially enhances the unpredictability on FPGA comparing to N-XOR Arbiter PUF.

## 3 Architecture of Proposed PUF

In this section, we introduce the proposed lightweight delay-based PUF that is implemented by slices and with challenge-response pair that of 20 challenge-bit and one corresponding unique response. Delay-based PUF utilizes the time-delay from signal propagation in two symmetric paths where signals race against each other simultaneously through a sequence of same number of stages, each consists of numbers of multiplexers. In essence, the difference is caused by naturally occurred variation in metal wires in very small scale and the structure of two paths are absolutely same to each other. The arbiter decide the digital signature refer to the sum of delay-time of separate blocks. As our proposed PUF occupies all the four LUT resources in a single sliceL, it can be exactly embedded into vehicles ECU system to safeguard security certification. To our best knowledge now, there is rarely authentication and authorization mechanism for vehicles electronic control system while it is of extreme importance in protecting vehicles from being attacked by malicious adversaries. To address this issue, we design a lightweight PUF circuit and then establish an authentication mechanism using the PUF circuit.

### *3.1 Property of PUF*

At present, the evaluation method based on FPGA PUF mainly considers its uniqueness as well as stability, also its power and resource consumption are of importance. For the same excitation signal input into PUF circuit under same condition, we evaluate the uniqueness by comparing the degree of similarity between the PUF output responses, when the generated two response signals are the same or very similar, the PUF structure is determined to be non-unique. This comparison result can be indicated by intra-chip Hamming Distances (HD), it represents the number of different bits corresponding two same length words or bit strings, for example the HD value of string "1001" and string "1010" is 2 because the third and fourth bit of the two strings are different. Stability demonstrates whether the PUF can maintain same outputs in repeated tests under different environment factors such as temperature and voltage, etc., it can also be demonstrated by intra-chip HD. We have to mention that for PUF with one-bit response it makes no sense to evaluate its Randomness.

### *3.2 Headings Property of PUF*

Level Xilinx 7 series FPGA includes four families that are all designed for lowest power to enable a common design to scale across families for optimal power, performance and cost. As shown in Fig. 1, the LUTs in 7 series FPGA can be configured as either a 6-input (A1-A6) LUT with one output (O6) or as two 5-input LUT with two separate outputs (O5 and O6), it is same as the previous structure of slice in virtix-5 and virtix-6.

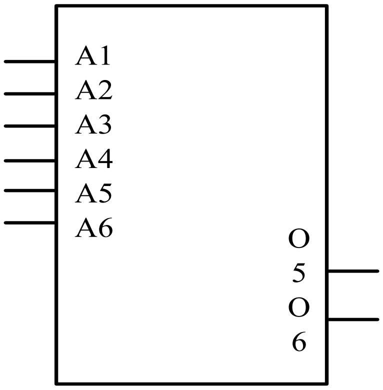

**Figure 1:** Architecture of LUT

There are two types of slice in CLB of FPGA board, both sliceM and sliceL contains four such 6-input LUTs and 8 flip-flops as well as 2-1 multiplexer and arithmetic logic chain, they are arranged in a column within slice and two slices form a CLB, see Fig. 2. The typical difference between sliceM and sliceL is that sliceM has additional function of storing data using distributed RAM and shifting data with 32-bit registers. We deploy all the four 6-input LUTs (LUTA, LUTB, LUTC and LUTD) in single sliceL as four parallel 4-1 multiplexer, and then cascade them in row to form a PUF design and the four 4-1 multiplexer in a sliceL has same address bits, which are challenge bit of PUF to decide the propagation route of data bit in a single LUT.

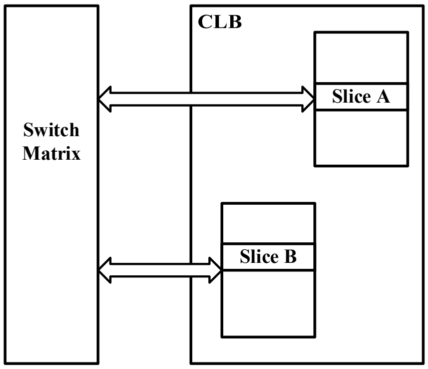

**Figure 2:** Placement of slice within CLB

The time-delay difference between a pair of single LUT or two parallel multiplexers is so small that cannot be precisely judged by arbiter block, therefore we place an array of such 4-1 multiplexer successively and get them connected to form an entire PUF. The upper slice-A and lower slice-B is fixed in every CLB, thus we deploy the two slices in a couple of parallel paths to produce a delay difference which can be judged by arbiter block and then labeled with unique digital signature. Fig. 3 shows the architecture of the upper path of our PUF. We utilize 5 CLBs cascaded together to form a 5-stage of PUF that with 20 bits of challenge-bit in total to be the address bits to decide the route that signal to propagate through. The signal in two slice within a CLB races against each other. We have to point out that our design is based on sliceLs and we constrain our sliceLs in appropriate position using range constraints provided to the Xilinx synthesis tool, because we must ensure the two paths in which signal races against each other have symmetrical structures. We design our PUF circuit with 20 challenge-bit and in first four stages, four LUT in every sliceL has same challenge bit and in the fifth stage only one LUT in sliceL is utilized to judge the upper four paths. We denote sliceL block whose all four LUTs are used by SLICEL-4, similarly the sliceL block in the fifth CLB is denoted by SLICEL-1. This kind of structure maximizes the internal sources of single slice selected to implement such four 4-1 multiplexer and a 2-bit challenge is required in this single multiplexer (inner a slice). In our design, the data-bit is logic-1 for every 4-1 multiplexer and the output of the first stage successively connected to the second stage as the data-bit of the second stage, it is similar in every next stage. Once the data races into LUTs (4-1 multiplexers), then which route it propagate through depend on the challenges bits (address bits) as the output of multiplexer is determined by the address bits. Meanwhile, the different routes will accumulate different time-delay that are exact the process where the uniqueness of the PUF comes from.

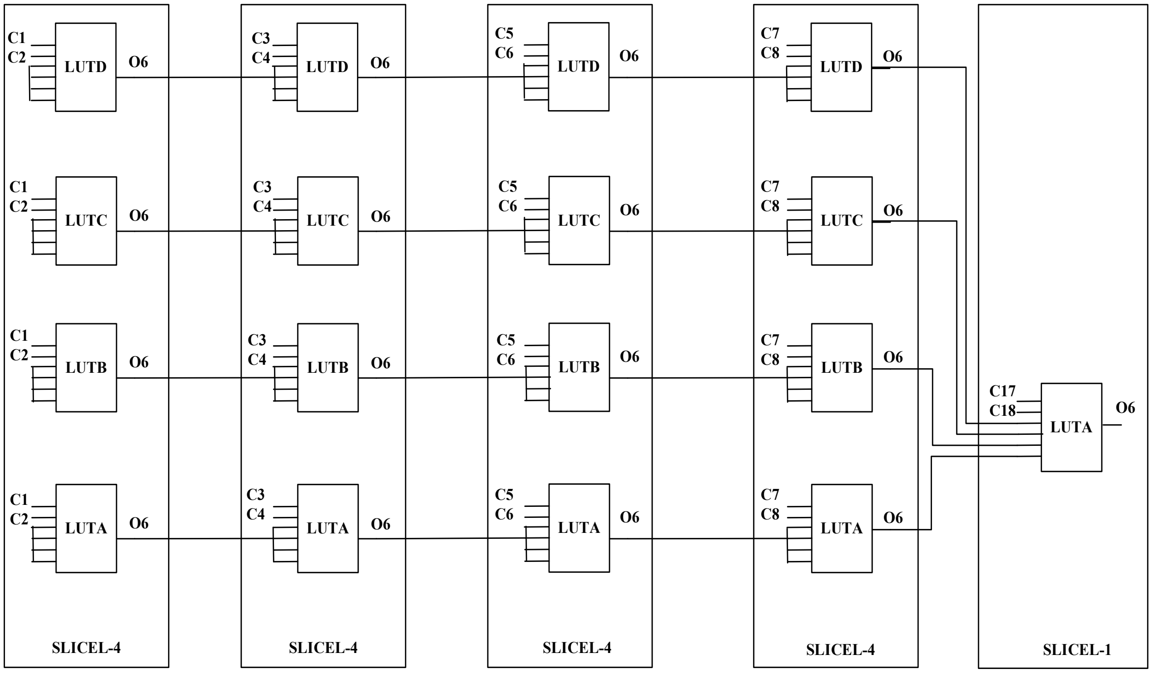

**Figure 3:** Structure of signal route in a single path

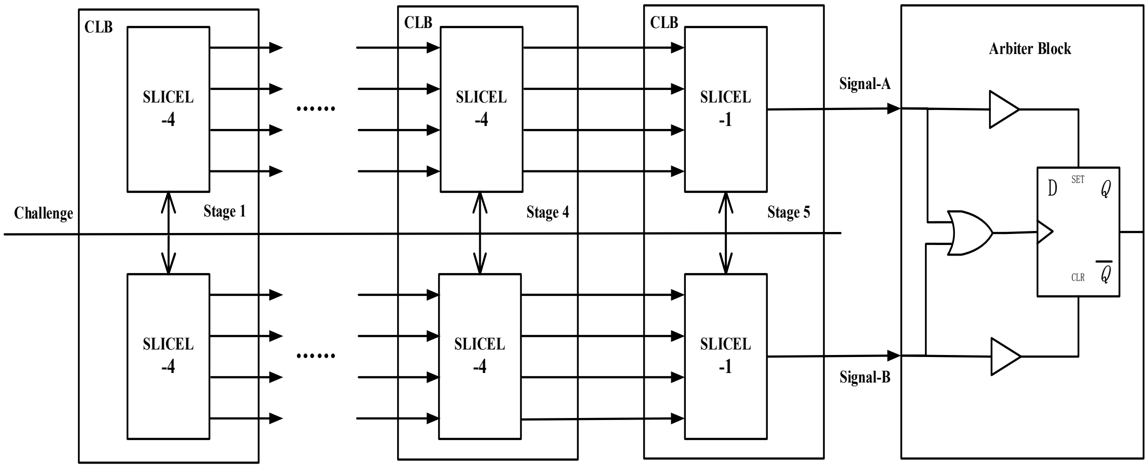

**Figure 4:** Architecture of the proposed PUF

### *3.3 Arbiter of PUF*

In previous part we introduced the structure of proposed lightweight PUF, signals propagate through symmetric paths get delay-time difference in small scale of metal wire and the difference between two paths gradually get accumulated in LUTs and metal wires while through the sequent 5 stages slices, when signals get to arbiter block it can be told out by D-flip-flop. As it shown in Arbiter Block in Fig. 4, when signal-A(it is logic-1) arrives earlier than signal-B(also is logic-1)，in this case, the upper input of the or-logic cell is logic-1 and the lower input is logic-0, then the or-logic cell will be triggered and its output signal as the enable signal to trigger the D-flip-flop to output the digital logic-1, in the opposite case when signal-B arrives at or-logic block less total time-delay, the D-flip-flop correspondingly outputs logic-0 as the digital signature. This structure of arbiter is much stabler as the or-logic block can naturally eliminate the abnormal shake comparing to single D-flip-flop. Note that the SLICEL-4 block in Figure.3 is equivalent substitute of SLICEL-4 in Fig. 4.

## 4 Experiment and Result

### *4.1 Experiment Setup*

We implemented our PUF circuit on 2 Xilinx 7 series FPGA boards, the specific model is virtix-7 ek-v7-vc707, we denote them as vc707-1 and vc707-2 and both two boards incorporate 28-nm technology. In order to analyze the stability we placed our PUF circuit in same region on same board under different temperature, here we adjusted the temperature using a hair dryer and Xilinx ChipScope tool is used to detect temperature, namely 33℃, 39℃, 45℃ and 51℃ respectively, and obtained responses corresponding to every level of temperature, there are 8 groups of data collected totally. For uniqueness we placed the PUF design in different regions on same board and set the environment temperature maintain in 33℃, 3 groups of data collected. We obtained 65536 signatures in every single implementation in total. In previous Section 3, we have introduced the concept of intra-chip HD and inter-chip HD that can indicate the uniqueness and stability of PUF circuit. Further in detail, intra-chip HD is the number of bits that differ in two bitstrings obtained from same chip but tested under different environment conditions. The intra-chip HD are typically converted into percentages by dividing each of them by the length of the bitstrings.

### *4.2 Property Analysis*

The stability demonstrates the PUF's performance in repeated tests under different environment, of which temperature is a key factor that influence its performance. We evaluate the stability by computing the intra-chip HD of every two group of responses of implementation that is in the temperature of 33℃, 39℃, 45℃ and 51℃ respectively, we get the result from region X0 on both vc707-1 and vc707-2 boards and following table.1 shows the details. We can see in Tab. 1, intra-chip HD of both the two boards is very small and the mean value of VC707-2 is 0.22794% and mean value is also smaller than 1%, it proves that our PUF design satisfies the stability.

**Table 1:** Relative intra-chip HD of implementation under different temperature

| Tem1 (℃) | Tem2 (℃) | VC707-1 (%) | VC707-2 (%) |
|---|---|---|---|
| 33 | 39 | 1.12153 | 0.21302 |
| 33 | 45 | 1.34421 | 0.25450 |
| 33 | 51 | 1.41168 | 0.28928 |
| 39 | 45 | 0.71081 | 0.20066 |
| 39 | 51 | 0.72601 | 0.22514 |
| 45 | 51 | 0.24697 | 0.18505 |
| Mean | | 0.92687 | 0.22794 |

We evaluate the uniqueness by comparing the distance between the responses collected from region X0, X4 and X194 in vc707-1 chip, every two groups of data are compared to each other and the distance can be indicated by relative intra-chip HD. We get 65536 1-bit responses in single implementation and compared the corresponding bit to judge whether they are same or not. We show the result in Tab. 2 as follow, from the table we could see the mean relative hamming distance is 43.53725% it is close to the idle value of 50%.

**Table 2:** Relative Intra-chip HD of Different Regions in VC707-1

| Region 1 | Region 2 | Relative intra-chip HD (%) |
|---|---|---|
| X0 | X4 | 45.36064 |
| X0 | X194 | 35.43507 |
| X4 | X194 | 49.81604 |
| Mean | | 43.53725 |

## 5 Authentication Mechanism

In this section we introduce the process how the proposed PUF circuit works in the authentication mechanism to provide in-vehicle ECUs with security assurance. Messages can be transmitted securely between the two involved ECUs after identities of ECU is confirmed to be trustworthy in authentication mechanism, if the authentication process fails, the receiver (sink ECU) will not accept the information delivered by sender (source ECU). The principle of the PUF authentication is to verify whether the Challenge-Response Pair data stored within source ECU is consistent with the real-time verification response of the PUF circuit in the sink ECU. The authentication process can be described in following steps.

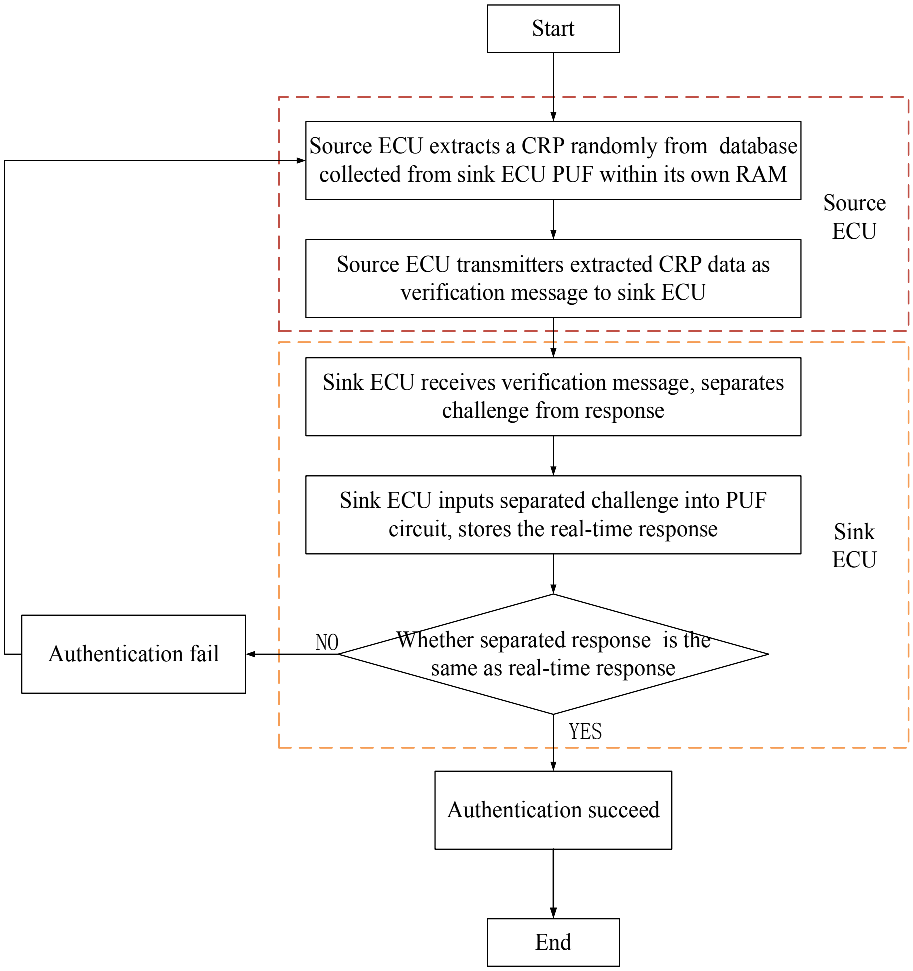
Start
Source ECU extracts a CRP randomly from database collected from sink ECU PUF within its own RAM
Source ECU transmitters extracted CRP data as verification message to sink ECU
Source ECU
Sink ECU receives verification message, separates challenge from response
Sink ECU inputs separated challenge into PUF circuit, stores the real-time response
Sink ECU
Whether separated response is the same as real-time response
NO
Authentication fail
YES
Authentication succeed
End

**Figure 5:** The flow of authentication process

**Hardware integration:** As we described in previous part, authentication mechanism confirms ECU identity by judging the consistency of stored response and real-time response, the stored response and real-time response are corresponding to same 20-bit challenge. To identify the ECU is trustworthy before transmitter messages using our PUF circuit, every ECU unit in the vehicle must be embedded with a Xilinx FPGA chip. Then our PUF design is implemented on the chip and all the Challenge-Response Pairs data be collected and stored in database. Then we collect the database of all the ECU units and store them into every ECU's memory part. During the authentication process, source ECU firstly determine the sink ECU to communicate with then pick out a CRP, which is collected from PUF in sink ECU, randomly in memory part and send it to sink ECU as the verification message.

**Authentication process:** The authentication process can be shown by flow in Fig. 5. The process consists of following steps. Firstly, source ECU extracts a CRP data randomly from database collected from sink ECU PUF within its own memory then sends it to the sink ECU. Secondly, sink ECU receives the verification message (CRP data) from source ECU and separates 20-bit challenge from 1-bit response, then it inputs the separated 20-bit challenge into the PUF circuit to excites the PUF circuit to produce a real-time response. Thirdly, the CPU of sink ECU verify the consistency of the separated response and real-time response, in the case that they are same, it indicates authentication successes so that the source ECU can be trusted. In the opposite case, the authentication fails and the source ECU is judged to be forged ECU and sink ECU no longer accepts the messages it sends until authentication successes.

## 6 Conclusion and Future Work

We have carefully studied the mechanism that how a complete arbiter Physical Unclonable Function works and then presented the details of designing our novel delay-based PUF circuit in this paper, and introduced the process how the authentication mechanism works. ECUs in vehicles are source-constrained and authentication is of key importance for protecting it from being attacked. The proposed PUF circuit is source-efficient and lightweight so that can be suitably applied to Electronic Control Units (ECUs) authentication of autonomous vehicles as a barrier to the safety of unmanned vehicles. We implemented proposed PUF on a set virtix-7 FPGA boards and analyzed the data, it got proved that the PUF is of proper properties. It is to say the proposed PUF could embedded into ECUs to identify and authorize message senders and receivers before executing certain control function. In the future, we will further to optimize the property and overhead of our PUF design and investigate its performance against machine learning attacks.

**Acknowledgement:** The authors would like to thank anonymous reviewers for their attentions and constructive comments to make this work more complete.

**Funding Statement:** This work was supported by the Key Scientific and Technological Innovation Team of the Shaanxi Province, China, under Grant No. 2017KCT-29, and the Key Research Item for the Industry Shaanxi Province under Grant No. 2018GY-136.

**Conflicts of Interest:** The authors declare that they have no conflicts of interest to report regarding the present study.

## References

[1] V. Immler, J. Obermaier, M. Konig, M. Hiller and G. Sig, "B-TREPID: Batteryless tamper-resistant envelope with a PUF and integrity detection," in *Proc. 2018 IEEE Int. Sym. on Hardware Oriented Security and Trust (HOST)*, Washington, DC, USA, pp. 49–56, 2018.

[2] U. Chatterjee, R. S. Chakraborty, H. Kapoor and D. Mukhopadhyay, "Theory and application of delay constraints in arbiter PUF," *ACM Transactions on Embedded Computing Systems (TECS)*, vol. 15, no. 1, pp. 1–20, 2016.

[3] R. Pappu, B. Recht, J. Taylor and N, "Physical one-way functions," *Science*, vol. 5899, no. 297, pp. 2026–2030, 2002.

[4] G. E. Suh and S. Devadas, “Physical unclonable functions for device authentication and secret key generation,” in *Proc. 2007 44th ACM/IEEE Design Automation Conf.*, Institute of Electrical and Electronics Engineers, San Diego, CA, pp. 9–14, 2007.

[5] J. H. Anderson, “A PUF design for secure FPGA-based embedded systems,” in *Proc. 2010 15th Asia and South Pacific Design Automation Conf. (ASP-DAC)*, Institute of Electrical and Electronics Engineers, Taipei, pp. 1–6, 2010.

[6] A. O. Aseeri, Y. Zhuang and M. S. Alkatheiri, “A machine learning-based security vulnerability study on XOR PUFs for resource-constraint Internet of Things,” in *Proc. 2018 IEEE Int. Cong. on Internet of Things (ICIOT)*, Institute of Electrical and Electronics Engineers, San Francisco, CA, pp. 49–56, 2018.

[7] M. Takanori, Y. Dai, I. Mitsugu and Kazuo, “A New arbiter PUF for enhancing unpredictability on FPGA,” *The Scientific World Journal*, vol. 2015, no. 1, pp. 1–13, 2015.