Multi-Incentive Delay-based (MID) PUF

Zhengran Zhang[1], Chongyan Gu[2], Yijun Cui[1], Chuan Zhang[3], Maire O'Neill[2], Weiqiang Liu[1*]
[1]*College of Electronic and Information Engineering, Nanjing University of Aeronautics and Astronautics, Nanjing, China*
[2]*Centre for Secure Information Technologies, Queen's University Belfast, Belfast, UK*
[3]*National Mobile Communications Research Laboratory, Southeast University, Nanjing, China*
E-mails: {zhengranzhang, yijun.cui, liuweiqiang}@nuaa.edu.cn, {c.gu, m.oneill}@ecit.qub.ac.uk, chzhang@seu.edu.cn

***Abstract*—This paper proposes a new PUF, namely Multi-incentive Delay-based PUF (MID PUF), which utilizes the fast carry logic (FCL) of Field Programmable Gate Arrays (FPGAs). The proposed MID PUF is completely and efficiently implemented in XOR gates of FCLs. Compared to other single signal excited PUF designs, *e.g.* Arbiter PUF, multiple excitations are applied on the same delay line to produce multiple outputs. To the authors' best knowledge, this is the first strong PUF based on only FCLs. The proposed MID PUF is implemented on Xilinx Spartan-6 XC6SLX9 FPGAs and a reliability experiment is carried out under the operating temperature in a range of 0°C∼70°C. The experimental results show that the proposed MID PUF has a high uniqueness and reliability performance, as well as low hardware consumption. Due to its advantages in both hardware efficiency and PUF metrics, the proposed MID PUF is promising for low-cost security applications on FPGAs.**

***Index Terms*—PUF, multi-incentive, uniqueness, reliability, low-cost**

I. Introduction

With the development of edge computing, the security of ubiquitous distributed terminal nodes has become more and more important as these nodes are sensitive and vulnerable to multiple attacks. It is important to ensure their security during communication and data processing. However, the traditional security methods are impractical to be implemented on the low-cost edge devices that have limited hardware resources. Moreover, the traditional methods always need to store secret keys in non-volatile memory (NVM), which is vulnerable to side channel attacks (SCAs).

A physical unclonable function (PUF) is a circuit design which utilizes the process variations which occur during manufacturing in order to generate a unique intrinsic identifier for an electronic device, *e.g.* a digital fingerprint. This type of circuit has a number of desirable features from a security aspect, such as the ability to provide low-cost identification of an integrated circuit (IC) or to provide a variability aware circuit that returns a device specific response to an input challenge, even though the circuit itself is the same. Hence, PUF is a promising security primitive to secure low-cost IoT devices.

Since the introduction of the PUF concept, a number of PUF designs targeting FPGAs have been proposed. The Ring Oscillator (RO) PUF [1] [2] uses identical ring oscillators to exploits the frequency difference which is determined by path delay. CRO PUF [3], RRO PUF [4] and XCRO PUF [5] are variants with reconfigurable features. Look-Up-Tables (LUTs) are commonly used to implement ROs for these RO based PUF designs to extract the difference between LUTs. The PUF in [6] was proposed to use Multiplexers (MUXs) in FCL block as shown in Fig. 1 to extract frequencies of different LUTs (configure LUTs as shift registers), other than the physical differences of FCL circuits. Hence, it still extracts the differences between LUTs. FPGA has a large number of FCL resources, rarely utilized by previous PUF designs. The Arbiter PUF [7] generates a 1-bit output by comparing two signal propagation delay lines through two symmetrical signal transmission paths. A large number of switch components (MUXs) is needed to achieve high randomness. However, single excitation utilized decides only one 1-bit response per n-bit challenge. To improve the utilization of PUF circuit, multiple excitation can be employed. The principle of multiple excitation is that the step signals are sent multiple times in a short period of time. When the multiple excitation is loaded into the transmission paths, the transmission circuits can produce multiple responses simultaneously. Specifically, the main scientific contributions of this paper are as follows:

- A novel FCL-based reconfigurable PUF (MID PUF) is proposed to explore the characteristics of FCLs. It is the first time to design a PUF completely using FCL logic units according to the authors' best knowledge.
- Multiple excitation strategy is designed to transmit signals in the delay lines to improve the efficiency of hardware circuit design.
- The proposed MID PUF design is implemented on Xilinx Spartan-6 XC6SLX9 FPGAs and a reliability experiment is carried out under the operating temperature in a range of 0°C∼70°C. The experimental results show that the proposed MID PUF design has a high uniqueness and reliability, as well as low hardware consumption.

II. The Proposed MID PUF

The overall block diagram of the proposed MID PUF, including core MID units, challenge & response generation modules and signal control unit, is shown in Fig. 2. Signal generator or chip clock signal multiplied by PLLs block is utilized as a clock source for the MID unit. The signal control module generates a clock signal into the delay chain and an enable signal (EN) at an appropriate time to control the signal

This work has been supported by NSFC (No. 61771239, 61871216 and 61871115), Six Talent Peaks Project in Jiangsu Province (2018-XYDXX-009) and Jiangsu Provincial NSF (BK20180059).

978-1-7281-0397-6/19/$31.00 ©2019 IEEE

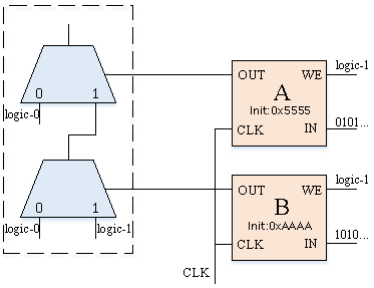


Fig. 1. A FPGA based PUF using FCL block [6].

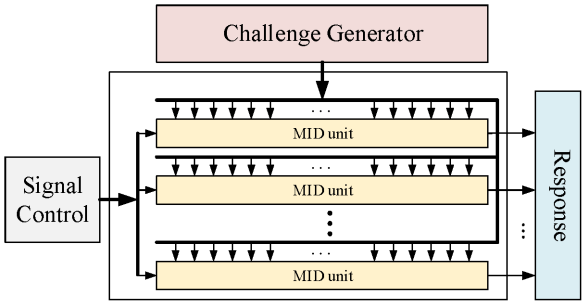


Fig. 2. Overall block diagram of the proposed MID PUF.

transmitted at the MID delay paths. The MID units are the core delay elements utilizing manufacturing process variations to produce unique responses. Multiple MID units can be employed in the proposed MID PUF to provide additional entropy for responses. The challenge generation modules are designed to generate challenges of the proposed MID PUF design.

The main objective of delay-based PUFs is to extract the delay difference of FPGA or ASIC circuit. Normally, basic components such as buffer gates or inverters are utilized to build delay lines. The proposed MID PUF also uses these components, but adopts FCL to extract delay differences between two identical delay lines. Fig. 3 shows a single MID unit design for the proposed MID PUF. The MID unit consists a reconfigurable FCL block chain. Although the same input signal propagates on two parallel delay lines, the underlying gate and net delay variations result in a subtle delay difference between them. The edge sensitive registers are used to acquire and store the signal on the delay lines and XOR gates are used to discriminate the same or different levels of signals transmitted in the delay lines. The EN signal is used as the enable signal of the register and the CLK signal can be used as Multiple excitation signal due to its periodicity and stabilization. The clock signal transmitted on a delay path and the enable signal is precisely controlled. Thus, the rising and falling edges of the clock signal for the delay paths are relatively fixed. Compared with the conventional arbiter PUF, the MID PUF can produce more response bits due to its additional incentive scheme of transmission paths.

Four inverters of the delay lines as shown in Fig. 3 can be implemented by FCL as shown in Fig. 4b. The XOR gates in the FCL block can be configured as inverters or buffer gates due to the logical characteristics of XOR gate. As shown in Fig. 4a, the two inputs of the XOR gate can be denoted as A and B, and the output be Q. When configuring the pin A level, the relation of output of the XOR gate (Q) and input (B) is given as follows: (1) When A = "0", Q = B, the XOR gate acts as a buffer gates. (2) When A = "1", Q = $\overline{B}$ and the XOR gate operates as an inverter. If the input port of a FCL block (DI(3:0), CYINIT, CI) is set to high to assert upper input port of the XOR gate high, the four XOR gates in the FCL block are configured as four inverters. If the output and selection of the FCL module are linked in an orderly way, the module will be configured as four inverters connected end to end. For instance, if O(0) output port is connected to S(1), the signal propagated through the solid path (red) from the input pin S(0), then passes through the connection outside the module and transfers to the next stage path marked with the solid line (yellow).

As shown in Fig. 3, the signal of each inverter at the clock edge will be sampled to generate a valid data. The invalid data collected in the registers are usually zero as shown in Fig. 5. Although the invalid data has no influence to the valid data, it results in a significant increase in the proportion of zeros in the response. Moreover, the randomness and uniqueness of a response can be significantly decreased due to the high proportion of zeros. The response generation of Fig. 3 can be used to remove the invalid data. The XOR layer in the response generation can also be used to remove the offset of zero in the response due to the logical characteristics of an XOR gate. The response generation module also resists to clock jitter and

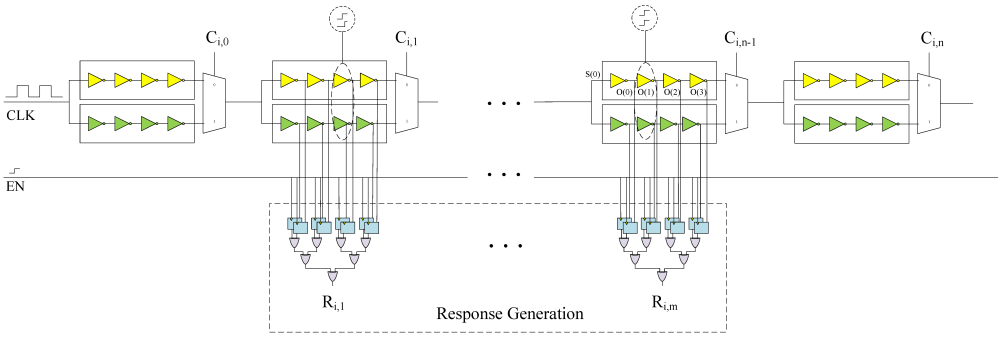
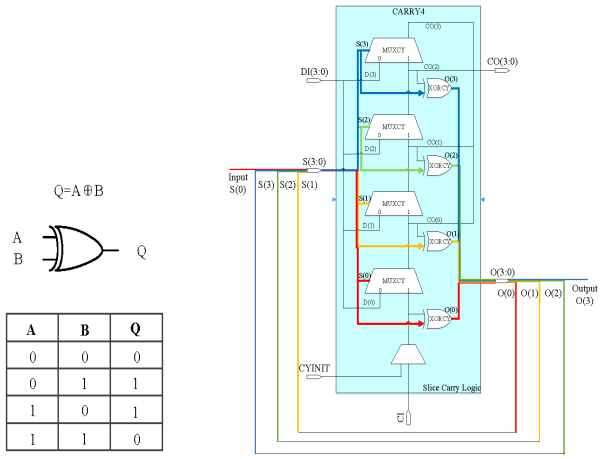


Fig. 3. The schematic of MID PUF.



A	B	Q
0	0	0
0	1	1
1	0	1
1	1	0

(a) (b)

Fig. 4. (a) The truth table of an XOR gate. (b) Four OR gates configured by FCL block.

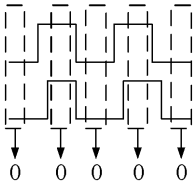


Fig. 5. Invalid data that are not sampled at the clock edge.

clock offset to some extent, thus ensuring the stability of the response data.

In the most previous proposed PUF structures, reconfigurable components such as MUX and XOR gates are used to build reconfigurable PUF structures, thus increasing the entropy of response. Delay lines in the MID PUF can also be reconfigured by adding MUXs. As shown in Fig. 6, each delay line can be reconfigured by using a MUX to select one of two parallel FCL blocks connected to the MUX. An $n-$bit challenge is applied to the selection port of MUXs. It can change two pathways at the same time to utilize different FCL blocks. This improvement can provide a larger number of independent response and make MID PUF a strong PUF.

III. The Implementation of MID PUF on FPGA

To validate the proposed MID PUF design on FPGA, we implement it on four Xilinx Spartan-6 XC6SLX9 FPGAs. The configurable logic blocks (CLBs) are the main logic resources to implement sequential and combinatorial circuits on FPGAs. A CLB element contains a pair of slices which has no direct physical interconnection on Xilinx Spartan-6. There are three type of slices, SLICEX, SLICEL and SLICEM, on FPGA.

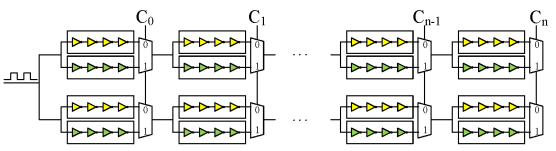


Fig. 6. FCL block chains.

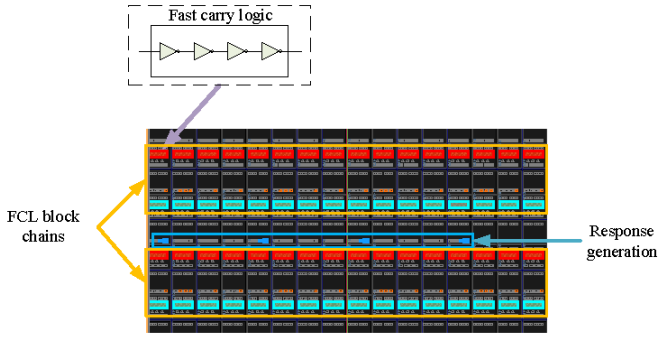


Fig. 7. FPGA implementation of the MID unit.

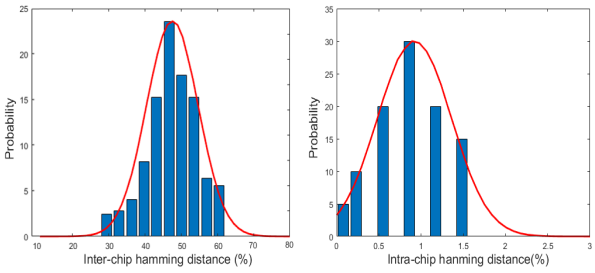
SLICEX, the basic slice, does not contain FCL structure and Wide Multiplexers. SLICELs and SLICEMs are the superset of SLICEX. Xilinx Spartan-6 XC6SLX9 FPGA has one FCL block in the SLICEL and SLICEM. Fig. 7 shows the hardware implementation of one MID unit for the proposed MID PUF design on FPGA. The components in light blue and red colors represent the upper and lower delay lines implemented by FCL blocks, respectively. The components in red color represent the FCL blocks implemented on SLICELs and the ones in blue color represent the FCL blocks implemented on SLICEMs. The XOR gates in the response generation module are synthesized by look up tables (LUTs) as shown in blue color in Fig. 7. The FCL blocks are placed in parallel to ensure the same wire delay for both paths. The response is only affected by the physical characteristics of the fundamental electronic element.

IV. Experimental Results

The proposed MID PUF design is implemented in 4 Xilinx Spartan-6 XC6SLX9 FPGAs and evaluated under the operating temperature in a range of 0°C∼70°C. In this section, two most important PUF metrics, uniqueness and reliability for the proposed MID PUF design are analyzed. The hardware resource consumption on FPGA is investigated and compared with previous RO PUF designs. In the experiment, four identical proposed MID PUFs are implemented in different areas on one FPGA. Hence, 16 proposed MID PUFs are provided for the experiment. 16 instances of FCL block chains are instantiated in the chain module to generate a 64-bit response. The number of CRPs used to evaluate the uniqueness and reliability for the proposed MID PUF design is 5,000.

A. Uniqueness

The response should be distinguishable from each other generated by different PUF instances when the same challenge is applied. The inter Hamming distance (HD), described in [11], is normally utilized to estimate the uniqueness of a PUF design. The ideal value of uniqueness should be 50%, indicating that there is no correlation between the outputs of different PUFs in different devices. The uniqueness result for the proposed MID PUF design is shown in Fig. 8a, where the average value of inter-chip variation is 47.2%, close to the ideal value.



(a) (b)

Fig. 8. Uniqueness and reliability of proposed MID PUF.

TABLE I
UNIQUENESS AND RELIABILITY OF FPGA-BASED PUFS

Types	Uniqueness	Reliability
RO PUF [1]	46.1%	0.48%
CRO PUF [3]	47.31%	0.86%
RRO PUF [4]	49.97%	2.60%
XCRO PUF [5]	48.85%	2.28%
Proposed PUF	47.2%	0.73%

B. Reliability

Similarly, the response of a PUF design should remain the same under different operating conditions. However, it is sensitive to the external environment, *e.g.* supply voltage and environmental temperature. To investigate the reliability of the proposed MID PUF design, a commonly used intra-HD method is applied. The definition of reliability is provided in [11]. The reliability result for the proposed MID PUF design is shown in Fig. 8b, the average value of intra-chip variation is 0.73%, which is small compared to other RO PUF design as shwon in Table I.

C. Metrics Comparison

The average uniqueness and reliability of several representative RO PUF designs are presented in Table I. It shows that the proposed MID PUF has better uniqueness result than the conventional RO PUF design but not as good as the CRO PUF, RRO PUF and XCRO PUF designs. However, the proposed MID PUF achieves higher reliability result than the CRO PUF, RRO PUF and XCRO PUF designs but the conventional RO PUF design. Hence, it is a tradeoff between uniqueness and reliability for the proposed MID PUF design in a practical application.

D. Hardware Resource Consumption

In this paper, we use the same metric which called Unit Response Cost (URC) as shown in (1), introduced in [12], to evaluate cost efficiency for a PUF design implemented on FPGA. The CLB is the basic resources of FPGAs and URC denotes the number of CLBs required for per bit response.

$$URC = \frac{N_{CLB}}{R_{BIT}} \tag{1}$$

where R_{BIT} is the number of response bits, while N_{CLB} denotes the number of required CLBs to generate R_{BIT} bit response. Thus the lower the URC, the higher the hardware efficiency of the design. The URC of RO, CRO, RRO, XCRO PUF are provided in [12]:

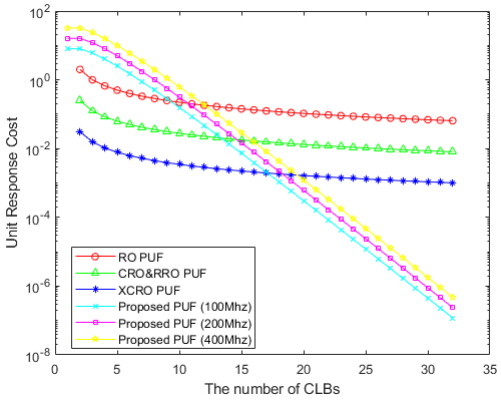


Fig. 9. URCs of RO, CRO, RRO, XCRO and the proposed MID PUFs.

When the frequency of clock source is 100MHz, using 16 CLBs, which include 16 FCL blocks, the MID PUF can generate 2 possible bits by configuring different paths. The ouput layer can be implemented in the same CLBs with the FCL blocks. The URC of the proposed MID PUF is calculated as (2).

$$URC = \frac{16n}{2^n}. \tag{2}$$

Fig. 9 shows that the hardware resource consumption of the proposed MID PUF design is significantly improved. When the number of CLBs for the proposed MID PUF designs is greater than 20, the URC of MID PUF is exponentially lower than the other PUF designs, including RO PUF, CRO PUF, RRO PUF and XCRO PUF designs. Furthermore, it also demonstrates that hardware efficiency of the proposed MID PUF increases significantly when increasing its clock frequency. The higher the frequency, the more the clock edge and the larger the number of valid data. Hence, the proposed MID PUF design achieves a significant lightweight performance than the other PUF designs.

V. CONCLUSION

In this paper, a novel MID PUF design, which utilizes the FCL of an FPGA, is proposed. It is the first time to design a PUF completely using FCL logic units according to the authors' best knowledge. Multiple excitation strategy is utilized to transmit signals in the FCL delay lines to improve the efficiency of the hardware circuit design. The proposed design has been implemented in Xilinx Spartan-6 XC6SLX9 FPGAs with a fixed location of the delay lines to achieve a balanced routing. The proposed MID PUF design shows good uniqueness and reliability results compared with other delay-based PUFs. Moreover, it uses significantly less hardware resources to produce responses than other designs. Hence, the proposed MID PUF is a promising candidate for lightweight IoT applications.

REFERENCES

[1] G. Suh, and S. Devadas, "Physical unclonable functions for device authentication and secret key generation," in Proc. Annu. Design Autom. Conf. (DAC), pp. 9–14, 2007

[2] W. Liu, Y. Yu, C. Wang, Y. Cui and M. O'Neill, "RO PUF design in FPGAs with new comparison strategies," In Proc. IEEE International Symposium on Circuits and Systems (ISCAS), pp. 77-80, 2015.

[3] A. Maiti and P. Schaumont, "Improved Ring Oscillator PUF: An FPGA-friendly Secure Primitive," Springer-Verlag New York, 2011, pp. 375–397.

[4] Y. Cui, C. Wang, W. Liu, Y. Yu, M. ONeill, and F. Lombardi, "Low-cost configurable ring oscillator PUF with improved uniqueness," In Proc. IEEE International Symposium on Circuits and Systems (ISCAS), pp. 558–561, 2016.

[5] L. Zhang, C. Wang, W. Liu, M. ONeill, and F. Lombardi, "XOR gate based low-cost configurable RO PUF," in Proc. IEEE International Symposium on Circuits and Systems (ISCAS), pp. 1452–1455, May 2017.

[6] J. H. Anderson, "A PUF design for secure FPGA-based embedded systems," in Proc. Annu. Design Automation Conference (DAC), pp. 1–6, 2010.

[7] Jae W. Lee, D. Lim, B. Gassend, M. van Dijk, and S. Devadas, "A technique to build a secret key in ICs for identification and authentication applications," in Proc. Symp. VLSI Circuits, pp. 17–19, 2004.

[8] Y. Su, J. Holleman, and B. P. Otis, "A digital 1.6 pj/bit chip identification circuit using process variations," IEEE J. Solid-State Circuits, vol. 43, no. 1, pp. 69–77, Jan 2008.

[9] S. Kumar, J. Guajardo, R. Maes, G. J. Schrijen, and P. Tuyls, "The butterfly PUF protecting IP on every FPGA," in Proc. IEEE Int. Workshop on Hardware-Oriented Security and Trust (HOST), Anaheim, CA, June 2008, pp. 67–70.

[10] V. der Leest, G. J. Schrijen, H. Handschuh, and P. Tuyls, "Hardware intrinsic security from D flip-flops," in Proc. 5th ACM Workshop on Scalable Trusted Computing, pp. 53–62, Oct. 2010.

[11] M. Roel, Physically Unclonable Functions: Constructions, Properties and Applications, Springer Publishing Company, Incorporated, 2016, pp.16-23.

[12] W. Liu, L. Zhang, Z. Zhang, C. Gu, C. Wang, M. O'Neill, and F. Lombardi, "XOR-Based Low-Cost Reconfigurable PUFs for IoT Security," ACM Transactions on Embedded Computing Systems, DOI: 10.1145/3274666.