FPGA oriented design method of Adjustable Arbiter Physical Unclonable circuit

Jinren Zhou

University of California Irvine

Email: 1219660919@qq.com, TEL: 18955169474

Abstract: In this paper, the design principle of the Arbiter Physical Unclonable Function (APUF) based on the arbiter is studied, the existing problems are analyzed, and the problem of its delay asymmetry is studied. An adjustable APUF structure for FPGA platform is proposed, which includes three modules. To adjust the delay deviation of the two paths of traditional Apuf flexibly, it is implemented and verified on the actual FPGA, which proves its feasibility and superiority.

1. Introduction

As the human society continuously develops, various high and new technologies emerge at the historic moment. As a new technology in the 1960s, the integrated circuit (IC) has experienced an unprecedented development, and its applications have involved in every aspect of our daily life, for example, communication satellites, mobile phones, various medical devices, cars, televisions and so on, so it is obvious that integrated circuit has become part of our daily life.

However, as the IC is applied more deeply, the attention has been gradually paid to its security. The people have more requirements on security as they further the application of IC. For example, the smart cards are widely used in financial services, and their security will directly affect the security of users' properties. Moreover, the security risks in smart phones can lead to the disclosure of personal privacy and information. Furthermore, the hidden safety risks in the auxiliary driving equipment of the car will directly impact personal safety. Therefore, the hardware security problems have caused great concern to chip designers.

Since people recognize this problem, a variety of theories and encryption algorithms have been proposed on how to ensure the security of electronic devices.

The Physical Unclonable Function (PUF) provides a new way to store the secret keys safely.

The PUF is a "digital fingerprint" used as the sole identity of semiconductor devices (for example, microprocessors). Based on various unpredictable random differences (such as threshold voltage, channel length) in the manufacturing process of integrated circuit, PUF can generate a unique ID for each chip. PUF is deemed as an ideal method to solve the problem of integrated circuit security, and it has become an important base of hardware security protection.

PUF is characterized by the uniqueness of its physical microstructure which depends on the random physical factors introduced in the manufacturing process. These factors are unpredictable and uncontrollable, which makes it almost impossible to copy or clone the structure, so that it becomes the security development direction for new generation of integrated circuit.

The concept, characteristics and classification of PUF are introduced in Section 2, the advantages and problems of arbiter-based PUF are analyzed in Section 3, and the design focus and implementation process of this project are proposed in Section 4.

2. PUF overview

2.1 PUF concept and characteristics

"In 2001, Srini Devadas (MIT CSAIL) proposed an IC in which a physically nonclonable function (PUF) was used to generate a secret key. PUF is a system based on device and process deviation. [1] It takes advantage of the inevitable minor differences and changes in the chip manufacturing process to achieve encryption at the physical level. PUF is characterized by the uniqueness of its physical microstructure which depends on the random physical factors introduced in the manufacturing process. These factors are unpredictable and uncontrollable, which makes it almost impossible to copy or clone the structure. PUF has the following three characteristics:

- Random
- Unique
- Non-copyable

These three characteristics can ensure the security and practicability of the chip.

2.2 PUF classification and research direction

According to the implementation methods, the PUF can be divided into non-electronic PUF, analog circuit PUF and digital circuit PUF. We can see its research and development direction from Figure 1

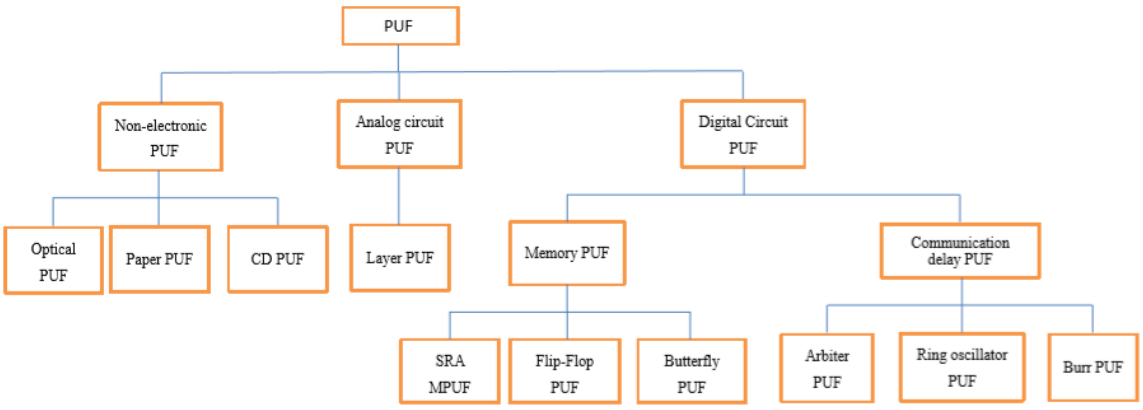

Figure 1. PUF Classification

Although initially proposed in 2001, PUF has developed rapidly. During the relevant research in this field, such as the smart cards, the relatively well-developed cryptography applications, the verification application in hardware security field and the algorithm protocol in secret key generation of software, PUF plays an irreplaceable role due to its good properties such as non-cloning, tamper-proofing and lightweight. However, there still are a lot of research momentum and improvement room in many aspects for this new technology, such as theoretical exploration and application practice. Especially in 2002, Gassend [2] et al. proposed the concept of silicon PUF, which can generate exponential excitation phase to respond CPR(Challenge Response Pair, CRP), so it has a good security performance, but it is susceptible to temperature, voltage and other external factors. The arbiter-based PUF [3], ring oscillator (RO)-based PUF [4] and Glitch PUF [5] all fall into the range of silicon PUF, and most researches are on the arbiter-based PUF and the RO-based PUF.

3. Arbiter PUF design with adjustable time delay for FPGA platform

3.1 Advantage

In 2005, Lim et al. [3] proposed arbiter-based PUF (hereinafter referred to as APUF), which properly solved the problem that silicon PUF was susceptible to external factors such as temperature and voltage. The arbiter-based PUF does not test the absolute delay of a circuit, but it obtains the response output by comparing the delays between two independent paths. Its design model is shown in Figure 2.

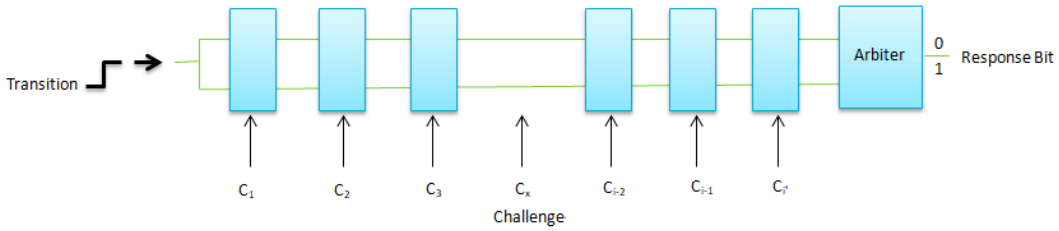

Figure 2. APUF Design Model [3]

As compared with other PUFs, the APUF has the following advantages:
(1) It is compatible with the design process in traditional IC products;
(2) The hardware cost of this PUF is lower;
(3) The hardware power consumption of this PUF is lower;
(4) It can be further implemented in FPGA

3.2 Deficiencies

Figure 3 shows a specific circuit structure of APUF. It is composed of two units (Multiplexer) containing n signal communication paths. They have the same input end (Transition), and the output end is connected to the signal input end of arbiter D flip-flop and the input end of clock. The input of excitation signal Ci (Challenge) can choose the parallel access or cross access to change the time delay of path.

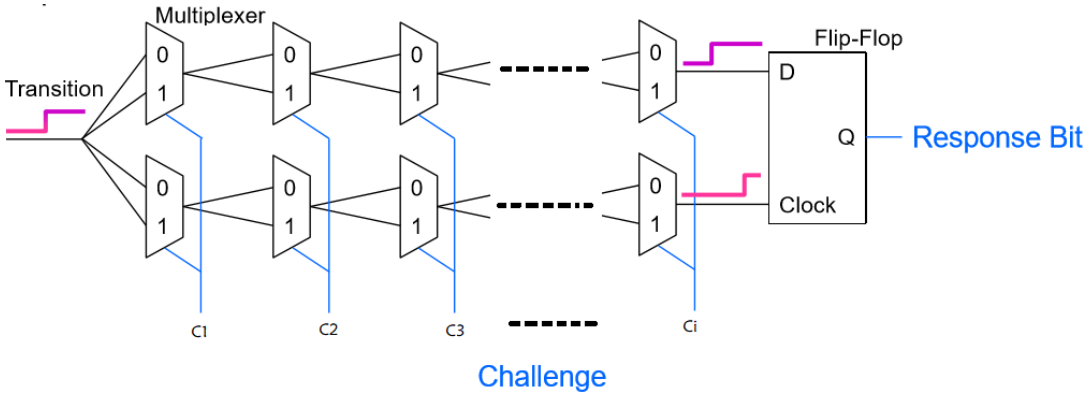

Figure 3. APUF Circuit Structure

According to the APUF circuit structure, the APUF design is composed of several alternative logic gates, and the input of each alternative logic gate is from the output of the previous logic gate. Every two alternative logic gates share an excitation signal (challenge bit). The specific input-output relationship is: when the input end (Transition) generates a rising edge signal, if such signal reaches the input end D first, then the output terminal (q), i.e. response bit, is 1.

If such a signal reaches the clock signal end (Clock) first, then the output terminal (Q), i.e. response bit, is 0.The path length of the upper and lower paths depends on the input of the excitation signal. Due to process deviation in chip manufacturing, even the excitation signal input and the number of logic gates of the upper and lower paths are the same, the time for signals of upper and lower paths to

arrive at trigger will be different, which will lead to an unstable output result. This output instability limits the application of arbiter PUF

According to the above, we learn that the arbiter PUF generates responses according to the delay of two paths. The basic principle of arbiter PUF design is to make the two paths have the same delay, which requires a completely symmetrical layout and wiring in the two paths of arbiter PUF.

However, in the FPGA design environment, it is very difficult to design a symmetrical APUF due to the limitations of FPGA on layout and wiring, and its uniqueness has great differences. Even the carefully designed APUF may have large delay deviation

Therefore, arbiter-based PUF has the following disadvantages:

(1) Poor randomness and uniqueness: the traditional APUF has a very high demand for the symmetry of the upper and lower delay paths, but it is difficult to carry out reasonable layout and wiring constraints on the FPGA platform to meet the absolute symmetry requirements, which leads to poor randomness and uniqueness.

(2) Overlong test time: in order to obtain a stable CRP, the test time is overlong. "According to statistics, 105 times are required for each CRP" [6].

(3) More hardware cost is required on Error Correction Code ECC [7]: since the constant Error Correction Code is required in PUF design to obtain a Secret Key, the hardware cost on ECC is higher.

4. Adjustable Arbiter PUF

4.1 Design principle

According to literature [8], the randomness of 50 arbiter PUFs is evaluated to obtain the probability density distribution function of randomness in the chip, as shown in Figure 4. In figure 4, the abscissa is the probability that a PUF responds to 1 under 1,000 excitations, that is, the randomness in the chip, and the ordinate is the percentage of PUF with specific randomness in the chip. In Figure 4, the average value and standard deviation of randomness in chip of arbiter PUF are 50% and 3.4%, respectively. However, in order to ensure the security performance of PUF, the output probability of both 0 and 1 shall be around 50%. According to Figure 4, the randomness in chip in the traditional APUF is hardly close to the ideal value 50%, and there is certain deviation. The reason is that the system deviation (for example, process deviation) causes the time delay of some paths to be generally higher than that of other paths. In addition to the unbalanced time delay of the two paths, the randomness problems may also be caused by the metastability and minor time delay failure of D flip-flop. Therefore, it is necessary to effectively improve the randomness of PUF.

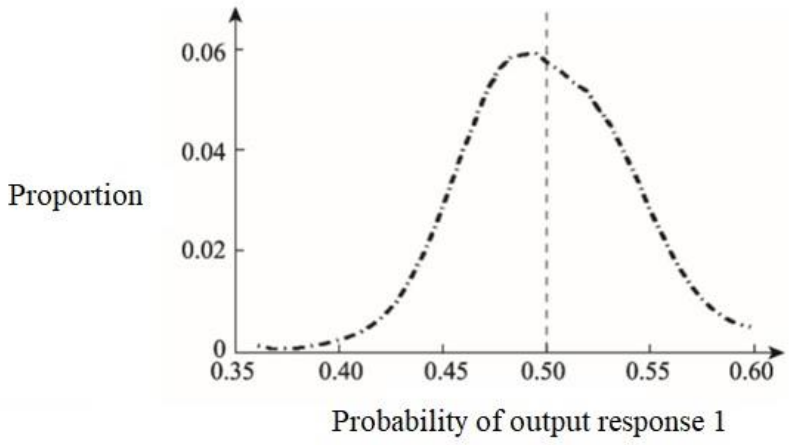

Figure 4. Probability Density Distribution of Randomness in Chip [8]

In order to address the above problems, the "Adjustable Arbiter Physical Unclonable Function" (Adjustable Arbiter PUF) is proposed in this paper, as shown in Figure 5.

According to Figure 5, the whole adjustable A-APUF is composed of three structures: excitation module, adjustable module and correction module. We mainly introduce the adjustable module here.

Similar to the traditional APUF, the time delay of the path is still used in adjustable module to generate excitation response, and just the adjustment circuit Buffer of time delay is added to the traditional APUF, as shown in Figure 5 "Path Segments for Adjusting the Response Distributions" area. In the adjustable module, all upper and lower logic gates are controlled by different excitation signal (challenge), so when a challenge signal is 1, its time delay is inevitable to increase due to the additional buffer in that path.

The working principle is as follows: according to the output results, we can invert whether signal arrives at port D or CLOCK first. If signal arrives at port D first, it means that the time delay in path-D of port D is less than that in path -C of Clock. In this case, it can be adjusted in two manners:

(1) The excitation signal input of Adjustable Buffers in path-D of port D is added to increase the tine delay in path-D of port D, so that the stability of time delay in path-D and path-C is achieved;

(2) The excitation signal input of Adjustable Buffers in path-C of Clock is decreased to lower the tine delay in path-C of Clock, so that the stability of time delay in path-D and path-C is achieved;

When the signal arrives at the Clock first, it is adjusted in the same way.

By adding a reasonable number of buffers, the delay of the upper and lower paths can be adjusted to achieve the goal that the distribution of 0 and 1 is within 50%, to improve the stability.

In this way, we can adjust the delay of the upper and lower paths, to improve the randomness and uniqueness of CRP. At the same time, we can evaluate the stability of CRP by judging the delay difference between the two paths.

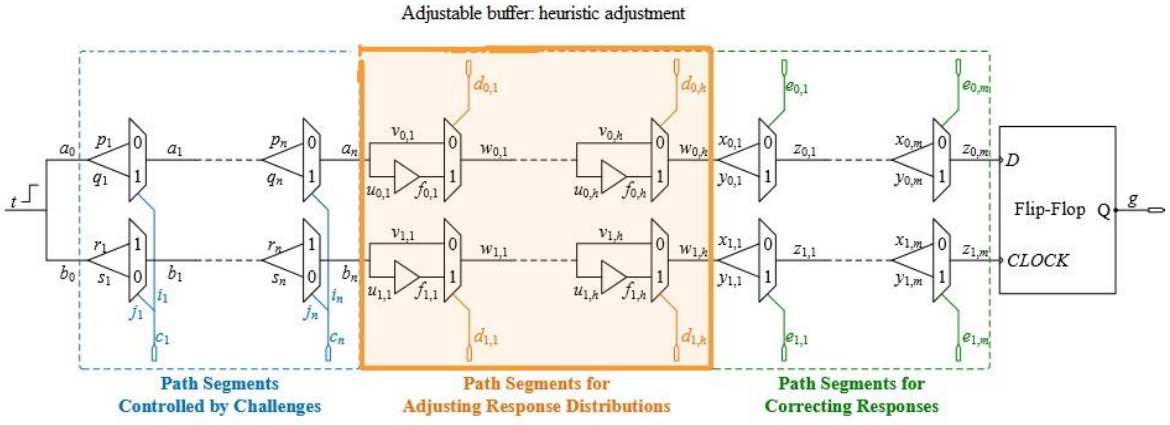

Figure 5. A-APUF Circuit Structure

Therefore, when the time delay in a path is larger than that of another path due to system deviation (for example, process deviation), the appropriate number of buffers can be inserted into the path whose time delay is often smaller so as to balance the time delay size of these two paths, ensuring that the probability of response to both 0 and 1 is similar, namely improving the randomness in chip.

4.2 Design platform FPGA

The FPGA (Field Programmable Gate Array) is the product of the further development of PAL, GAL and other programmable devices. As a semi-customized circuit in ASIC (Application-Specific Integrated Circuit) field, it not only solves the inadequacy of customized circuit, but also overcomes the limitation on the number of gate circuits in the original programmable device.

4.3 Design language and software

Hardware Description Language (HDL) is a language used to design digital logic systems and describe digital circuits, and the commonly used languages include VHDL, Verilog HDL, System Verilog and System C.

The Vivado design kit is an integrated design environment released by FPGA manufacturer Xilinx in 2012. It includes a highly integrated design environment and a new generation of tools from the system to the IC level, and they are established on a shared extensible data model and a common debugging environment.

The Verilog HDL simulation under vivado2019.1 environment is adopted in this project. This project also has the following features in design:

(1) Timing closure is added

In the program design, the timing closure is added to increase design working frequency, and the timing analysis report after layout and wiring is obtained through timing analysis tools.

(2) The TCL scripting language is used to improve work efficiency

TCL (Tool Command Language) is a general-purpose scripting language which can be interpreted to run on almost all platforms, and TCL command lines are also available in VIVADO.

In A-APUF, the TCL language is used to create a new project. Because TCL language is powerful and easy to understand, it can automatically add the constraint conditions into the program so as to avoid the error of manual input.

4.4 Implementation of A-APUF on FPGA

The following are the various results of A-APUF in the Vivado implementation

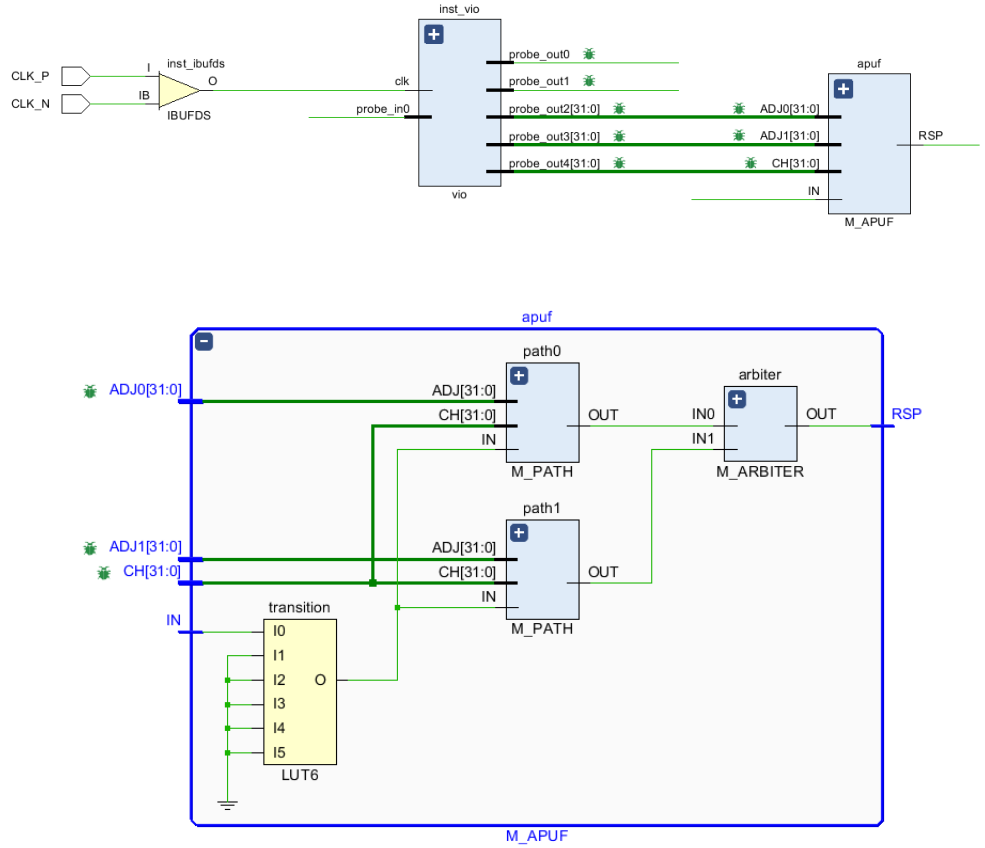

Figure 6. A-APUF Elaborated Design

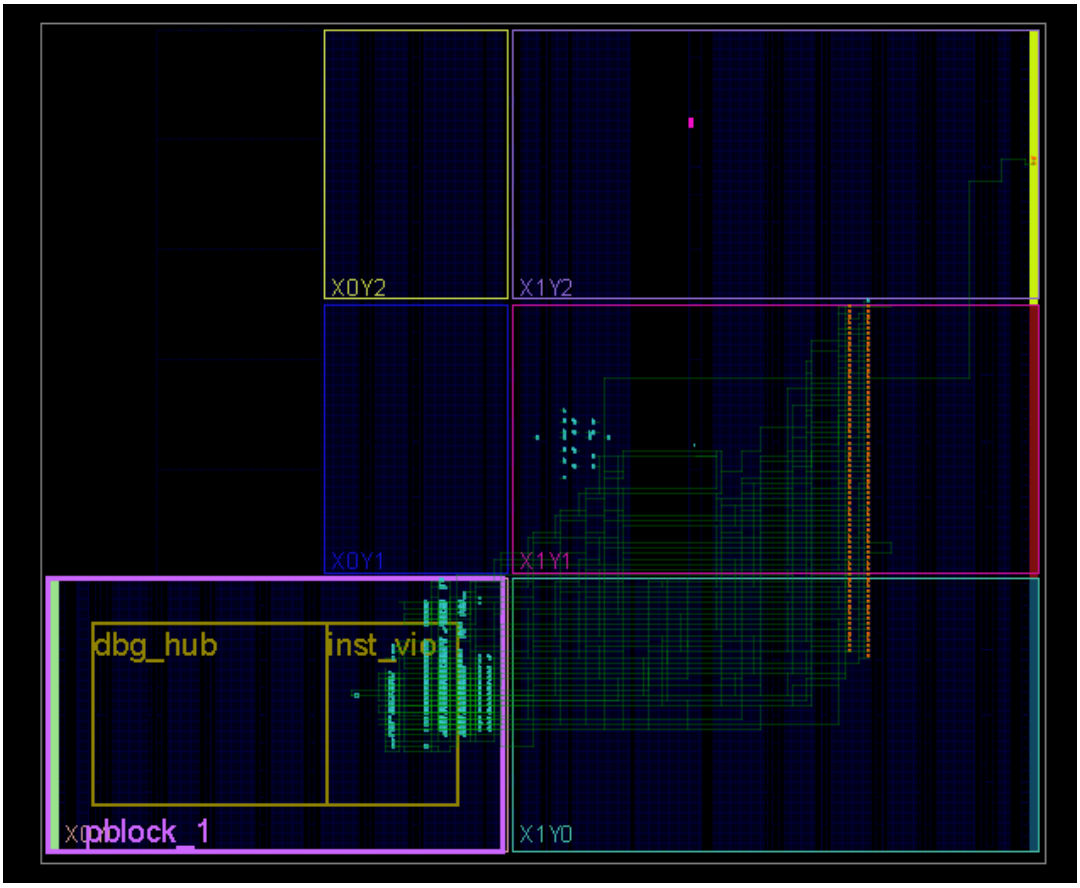

Figure 7. Implemented Design

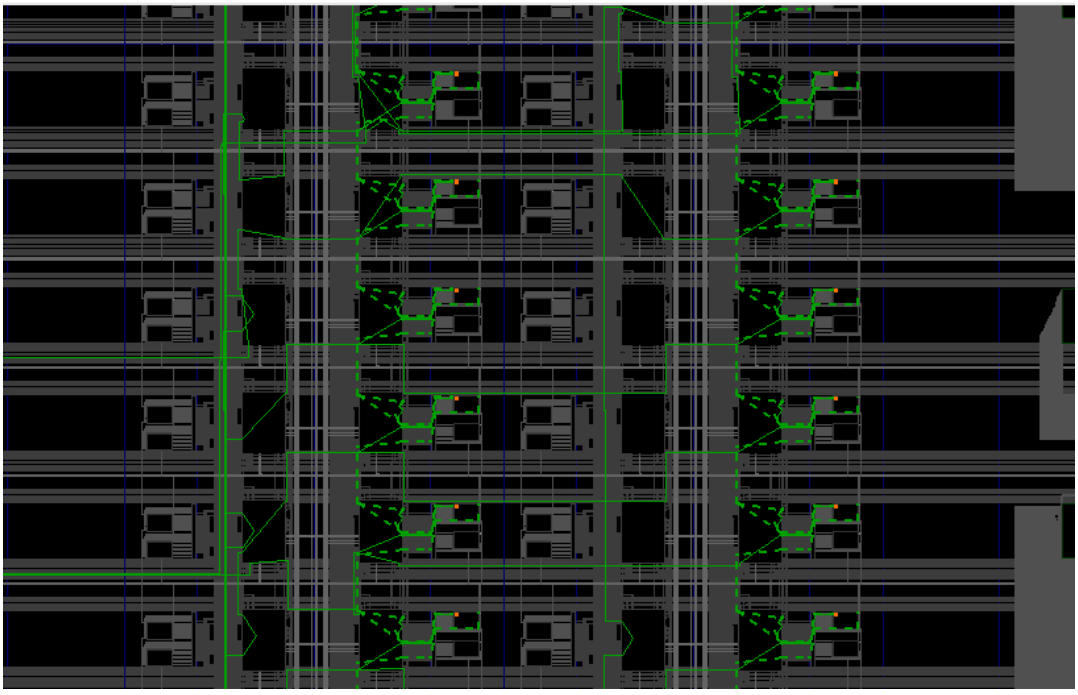

Figure 8. Core Layout and Wiring Constraint Graph

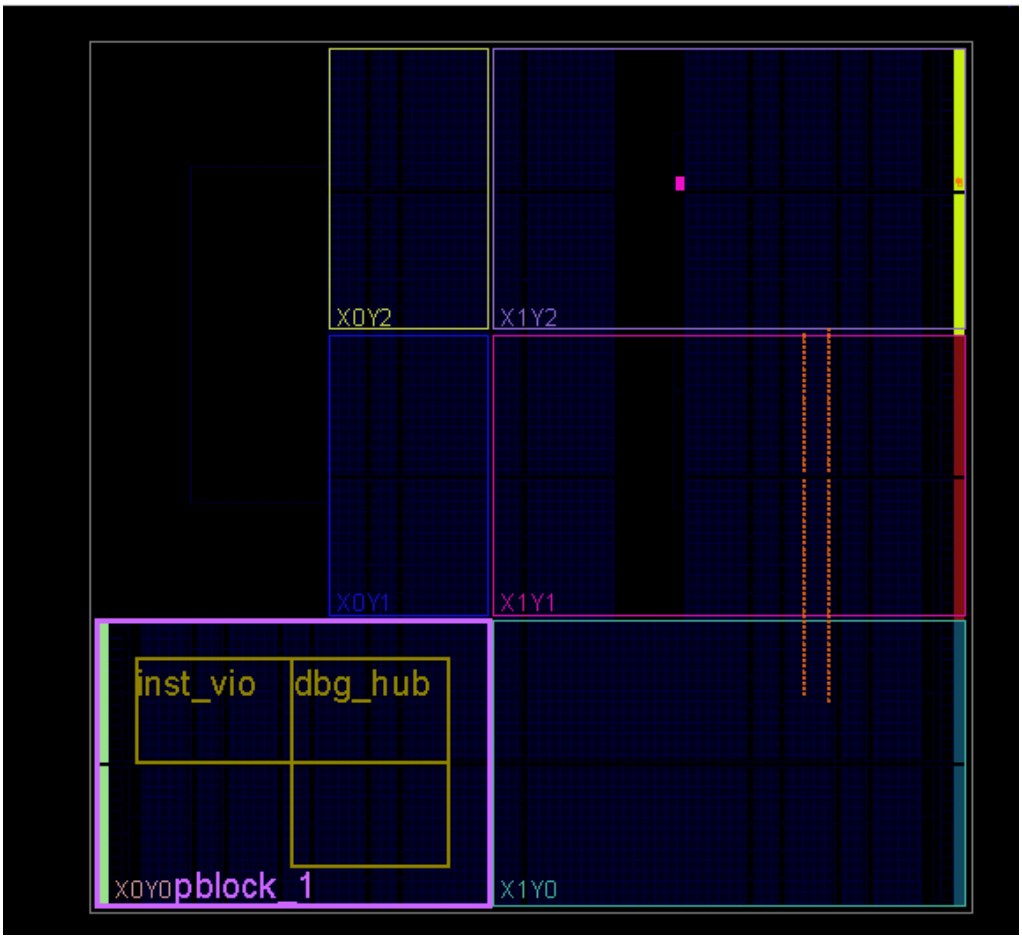

Figure 9. Synthesized Design

5. Summary

PUF is a promising and new security technology that can provide a low-cost, high security key storage and generation mechanism in both ASIC and FPGA. However, there are also some problems, such as delay asymmetry in APUF. To solve these problems, the traditional APUF model was researched and the causes of the response deviation were obtained. Then a design method of Adjustable Arbiter PUF for FPGA platform was proposed to effectively improve the delay deviation problem in traditional APUF. Finally, the FPGA verification was conducted through experiment, which proved the outstanding performance of the proposed method.

References

[1] Li Lei, FPGA Implementation of PUF based on RO Circuit Change, the 5th issue of electronic technology application, 2018
[2] Gassend B, Clarke D, M, Van Dijk, et al. Silicon physical random functions [J]. ACM Conference on Computer and Communications Security–CCS, 2002, 2: 148-160.
[3] Lim D, Lee W J, Gassend B, et al. Extracting secret keys from integrated circuits [J]. IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 2005, 13: 1200-1205.
[4] Yu H, Leong P, Kinkelmann H, et al. Towards a unique FPGA-based identification circuit using process variations [J]. In IEEE Int'l Conf. on Field Programmable Logic and Applications, 2009, 9: 397-402.
[5] Daisuke Suzuki, Koichi Shimizu. The Glitch PUF: A new delay-puf architecture exploiting glitch shapes [J]. Cryptographic Hardware and Embedded Systems – CHES, 2010, 6225: 366-382.

[6] C. Zhou, et.al., "Secure and Reliable XOR Arbiter PUF Design: An Experimental Study based on 1 Trillion Challenge Response Pair Measurements," DAC, 2017
[7] Q. Guo, et.al., "PUFPass: A Password Management Mechanism Based on Software/Hardware Codesign," Integration, VLSI journal, 2018.
[8] Majzoobi M, Koushanfar F, Potkonjak M. Testing techniques for hardware security[C] //Proceedings of IEEE International Test Conference. Los Alamitos: IEEE Computer Society Press, 2008: 1-10