IOSR Journal of VLSI and Signal Processing (IOSR-JVSP)
Volume 4, Issue 1, Ver. I (Jan. 2014), PP 16-21
e-ISSN: 2319 – 4200, p-ISSN No. : 2319 – 4197
www.iosrjournals.org

VLSI Design of Low Cost (PUF) Physical Unclonable Function Using FPGA and Highly Secured Clock Network

Muthumeenakshi.N[1], Hari Prasath Sharma.S[2], Farjanaaameera.M[3], Rajaprabha.R[4]

[1,3](ME-VLSI Design, Sri Shakthi Institute of Engineering and Technology, Coimbatore, India)
[2.](M.Tech-VLSI Design, Bharath University-Chennai, Tamilnadu, India)
[4.](Assistant Professor, Sri Shakthi Institute of Engineering and Technology, Coimbatore, India)

Abstract : *With the ever increasing growth in microelectronic devices and applications, there is an equally pressing more demand for ensuring product authenticity, security and reliability of the electronic system. The security requirements for most of the applications are crucial and evolving. In addition more sophisticated attacks are being developed every day. These attacks often have much higher impact and essentially no way to compensate for them with additional software counter measure. Hence we introduce PUF (Physical Unclonable Function) system based on clock networks for security purpose. On chip Physical Unclonable Functions (PUFs) are emerging as a powerful security primitive that can potentially solve several security problems. In this paper we proposed a PUF system based on clock network for resolving security issues in the circuits. The main aim is to create an unclonable circuit with the help of clock network, return path and multiplexer (Mux) block. The clock network has number of sink to split the input data. Return path used to pass the signal from clock network to mux network. Mux network has multiplexer, delay buffer and SR latch. The response of the PUF circuit is unclonable bit. PUF is an external device which can be placed in a circuit to avoid cloning of the circuit. A PUF needs to be robust against reversible as well as irreversible temporal changes in circuits. PUF functions promise cheap, efficient and secure identification and authentication of devices. It is impossible to copy the protected circuit by others in an exact manner and cannot get the same functionality of the device. Thus we can protect the device from cloning.*

Keywords: *Arbiter, Clock network, Sink, Return path, unclonable bit generation*

I. INTRODUCTION

There is a demand for product authentication, security, and reliability of the electronic system. In 2012, IHS supply ranked counterfeited electronic devices as, analog ICs (25.2%), microprocessors (13.4%), memory ICs (13.1%), PLDs (8.3%). Now a days most of the systems like ATM, Smart card, RFID tag using Printed serial numbers for identification. With ever increasing the growth, the counterfeit also get increased due to that the process of using printed serial numbers system for identification in most of the systems.

The most of the companies and industries are affected as directly. The person who has more hope from the organization, they do this counterfeiting. That most believable person theft the secrets and confidential data, and sell that to the other company or any organization. Due to that, they can easily copy and clone that product. It may be work on good manner. But the product designers get affected as physically and mentally. To avoid these counterfeiting problems, here the PUF (Physical Unclonable Function) system introduced.

The main objective of this paper is to produce more secured system at low cost authentication and device must not be copied and cloned. The products are secured highly but in cheapest way and can be used for high level security. Goal is avoid the counterfeiting occur in an electronic device. PUF technology provides a secure method for storing a key withstanding today attacks and even protecting against future potential attacks.

PUF is defined as a function based on physical characteristics. It is unique for each chip, difficult to predict, easy to evaluate, easy to make, and reliable. It is practically impossible to duplicate. This is used for secure chip authentication. It is one-way function. It has unique and unpredictable way of mapping challenges and response. PUF has more environmental variations like temperature variation, power supply voltage, Electromagnetic interference. PUF can serve a root of trust and provide a key which cannot be easily reverse engineered. It is used for prominent and secure applications.

The main aim of this project is to design FPGA based cryptography which encrypts / decrypts the data from the PC to PC. In this paper the encryption / decryption algorithm is designed and programmed in to the FPGA and data transfer between the PCs is controlled by the FPGA

II. RELATED WORKS

The most dominant approaches for implementing PUF either leverage the bi-stable circuit element such as SRAM arrays [1, 4], or are based on variations in logic gate / wire delays or leakage currents [5, 6]. The PUF in [5] utilized delay difference between pairs of parallel timing paths with equal nominal delay. PUF bits were generated by a delay arbiter connected to these paths. To increase the number of CRPs, the paths were segmented and multiplexed by challenge bits. An ASIC implementation was demonstrated in 180nm CMOS [2]. The US government and semiconductor companies point out potential system susceptible to danger resulting from the contract foundry model, hardware intellectual property and IC theft, as well as counterfeiting [7, 8]. Further aspects of PUF design, performance and security foundations applicable to our work can be found in [3, 9, 10].

III. SECRET COMMUNICATION

3.1 CRYPTOGRAPHY

The branch of cryptology dealing with the design of algorithms for encryption and decryption, intended to guarantee the secrecy of messages. An original message is known as the plain text, while the coded message is called the secret message (chipper text). The method of converting the original text to cipher text is known as enciphering or encryption; restoring the plain text from the cipher text is deciphering or decryption. The many schemes used for enciphering comprise the area of study known as cryptography. Such a scheme is known as cipher.

Techniques used for decrypting a message without any knowledge of the encrypting details fall into the area of cryptanalysis. The cryptography technique is what the lay person's calls "contravention the code". The areas of cryptography and cryptanalysis together are called cryptology.

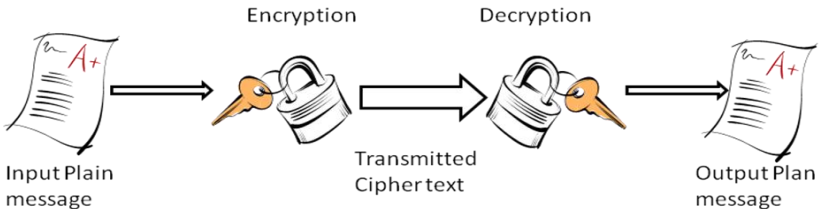

Fig.1 Simplified model of conventional encryption

3.2 ENCRYPTION

The original intelligible message or data that is fed into the algorithm is the input. Encryption algorithm performs varies substitutions and transformations on the plain text. Secret key is also given as input to encryption algorithm. The key is a value independent of the plain text. The algorithm reproduces the different output depending on the specific key being used at the time. The exact substitutions and transformation performed by the algorithm depend on the key. The cipher text is an apparently random stream of data, as it stands, is meaningless.

3.3 DECRYPTION

This is essentially the encryption algorithm run in reverse process. It takes the cipher text and produces the original plain text.

IV. PROPOSED SYSTEM

The aim of this project is to communicate the data secretly using Low Cost PUF using Highly Secured Clock Network i.e. we first send the data (plain text) to the encryption process .The output of this process will be cipher text. This cipher text is fed into the decryption process and then the data (plain text) is got as output. The main aim is that since we shuffle the data it is very hard for the unknown person to find out the original data. Since for each data will be a change in the cipher text and so the person has to know the process in order to find out the original data.

In this process the Input plain text is converted to binary format and transferred to the FPGA kit through the serial port. The internal buffer collects the data and according to the function like (encryption / decryption) block will be selected. The encryption and decryption algorithm used in our design in based on Low Cost PUF using Secured Clock Network. The output of the encryption block is called cipher text or cryptogram will be transferred in order to decrypt the data. The outputs of these blocks are stored in the output buffer

4.1 UNCLONABLE SECRET KEY GENERATION
4.1.1 BLOCK DIAGRAM

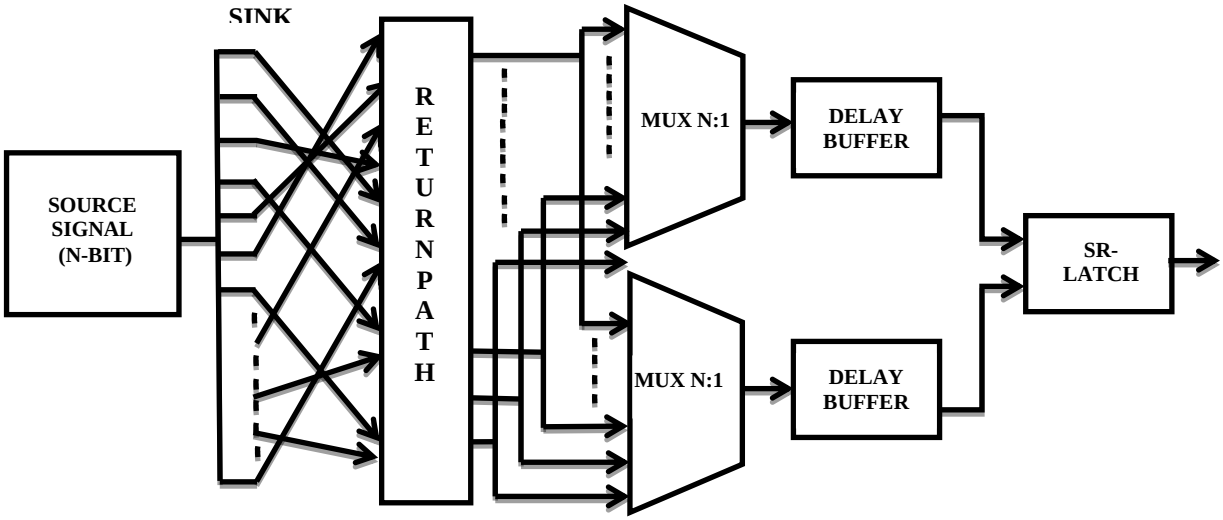

Fig.2. Block diagram for Unclonable Secret key Generation

4.1.2 BLOCK DIAGRAM DESCRIPTION

Here we introduce our proposed PUF architecture. For introducing PUF we need clock network. A clock PUF compares the arrival time of the clock signal and generates the stable but unclonable bits. A figure shows the flow of the clock PUF. The major components of our paper are explained below.

- The source signal is given to the clock network. Source signal is in the form of binary digits. That signal is branched out and inserted to the sink without affecting the clock network.
- The return path catches the signal from the sink and passes it to the mux network. The return path has even number of inverters. Here return paths are buffered and accumulate the process variation from different region of the chip.
- The multiplexer network is selecting two clock signals and compares it. The clock signal is distributed with the pair of adjacent multiplexors or using distributed multiplexors.
- A pair of externally controlled delay buffers with matched delays to maximize the variation.
- The result from the buffer is given to the SR-latch to determine which of two signal transitions first.

In this clock PUF the sink is selected then connected to the return path as carefully, to get equal propagation delay and matched length. There is not necessary to connect the sink result as directly to the return path we can connect the result of the sink to any node of return path for increasing the security level. The mux arbiter compares pairs of clock transition and producing a bit at a time. It pass through the delay buffer which can compensate for unintentional systematic delay encountered on the way. At the end of the architecture a latch is connected.

4.2 DEVICE DESCRIPTIONS

The following devices are present in the clock PUF architecture. They are explained detail manner in following sessions. The devices are

- Source of clock network (input)
- Sinks
- AND gate
- Multiplexer
- Tunable Delay buffer
- SR Latch

- **Source of Clock Network:** Source is the input of the clock network. An input is given like a binary bit. It can be split in number of levels depends on input. This process will continue up to get single bit separation. This separated bit is given to the input of sink. Sink has flip-flop & AND gate combination network.
- **Sink:** It is the combination of flip-flop & AND gate network. Each bit which is split from the clock source given to the input of the sink. Number of sink network used here depends on the clock source. Because each split bits require a sink network. The output of the sink network is given to the input of the return path. Sink network is given in fig.3.

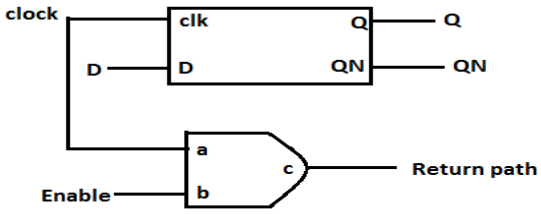

Fig.3 Sink circuit

- **Return Path:** Return path of the clock PUF architecture is used to pass the input value to the output as without change in input value. But can connect any output of the sink to any input of the return path. Due to that the data changes and correction can be conducted by designer only, others don't get idea about the internal connection. So security can be increased depends on the connection.

  In return path network, even number of inverters are connected depends on the designer. By connecting the inverters as even manner, can get the output as same as the input otherwise the response get varied. The output of the return path is given to the input of the multiplexer
- **Multiplexer:** The term multiplexer means many to one. Multiplexing is the process of transmitting a large number of information over a single line. A digital multiplexer (MUX) is combinational circuits that select digital information from several sources and transmits the selected information on a output line. A multiplexer is also known as a data selector since it selects one of many inputs and steers the information to the output.

  The multiplexer has several data input lines and single output line. The selection of a input line is controlled by a set of selection lines. The selection line decides the number of input lines of a particular multiplexer. If the number of n input lines is equal to 2m, then m select lines are required to select one of the n input lines.
- **Delay Buffer:** Delay buffer act as a buffer with some delay. It has single input and single output signal. But it gives the output signal with some delay.

- **SR Latch:** In this paper we use SR-Latch. SR latch have two inputs, S and R. S and R is called set and reset respectively. The S input is support to produce HIGH on Q (i.e. store binary 1 in flip-flop). The R input is support to produce LOW on Q (i.e. store binary 0 in flip-flop). Q' is complementary output of Q, so it always holds the opposite value of Q. The output of the S-R latch depends on current as well as previous inputs or state, and its state (value stored) can change as soon as its inputs change.

4.3 IMPLEMENTATION

By using the above unclonable bit we can generate cryptography key. This unclonable bit can control the devices which need more security. The generated unclonable bit given to the input of the devices as externally, and it controls that device as internally. If anyone wants to copy that secured device means they cannot copied as correctly due to that internal variation and cannot be cloned too. Thus that device get most security and can be withstand in their unique character

V. SIMULASION RESULT

For simulate this paper we use ModelSim. From the block diagram we know that each level needs the result of the previous level to respond to the next level. The source signal has n-bit binary value as input. It split into a single bit then passes it to the return path through the sink. Then send it to the mux network for getting result as unclonable bit.

A pair of delay buffers at the inputs of the delay arbiter compensates for the intrinsic delay difference between paths. When nominal delays of two return paths are matched, their comparison generates a random bit. Small biases in such bits can be tolerated by combining multiple bits. The best settings of delay buffers are determined empirically based on a sufficiently large lot of chips. By setting delays to median values, one decreases systematic bias in delay differences and increase variation entropy available for PUF bit generation. To further increase entropy, several settings for delay buffers can be used. Using such settings as a challenge response mechanism repeals attacks based on replaying or analyzing responses to a single setting. Finding good settings of delay buffers and PUF read-out does not require external tools when delay buffers can be programmed via multiplexed input pins.

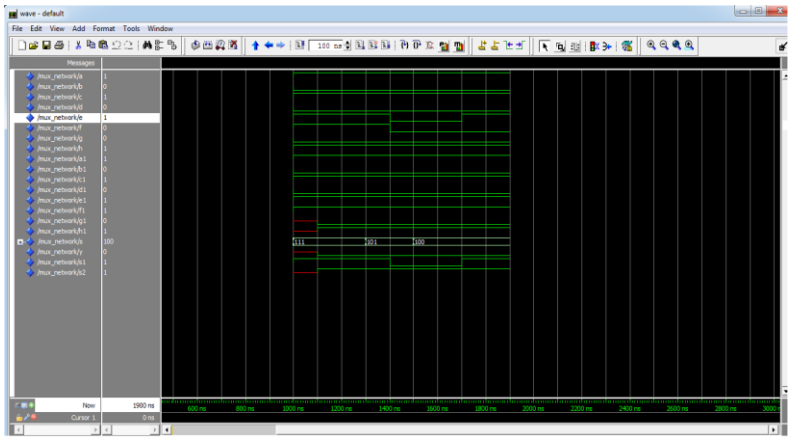

Fig.4 Unclonable bit generation

VI. CONCLUSION

In this project we introduce PUF system based on clock network for security purpose. This PUF system ensures product authenticity, security and reliability of the electronic system. Now a days, lots and lots of companies are emerging and they produce products (circuit devices) for mobile, laps, iPhone etc., but the original product designer not getting the merit for their product due to a major problem called counterfeiting. To avoid that problem we proposed a PUF system using clock network. This circuit produce security key and protect the device from cloning. If the system attempt to be copied by someone, they can't get the exact functionality of the system. Hence the product with PUF cannot be cloned. It is implemented in RFID technology and can be implemented in finger print, smart card system, etc., also. Our government accepts this product for the security purpose. Recently this PUF receive particular attention in the chip market as a promising way to provide security. Hence we implement PUF system to avoid counterfeiting and protect the products in an efficient way.

Acknowledgements

We would like to thank our parents and esteemed Bharath University Research and Development Chennai, Sri Shakthi Institute of Engineering and Technology Coimbatore, TamilNadu. Our parents And our team members.

AUTHER'S PROFILE

N.Muthumeenakshi is doing her Masters of Engineering degree in VLSI Design from Sri Shakthi Institute of Engineering and Technology Coimbatore, Tamil Nadu. She has completed her Bachelors of Engineering in Electronics and Communication Engineering from Anna University Chennai, Tamil Nadu, India.

S.Hari Prasath Sharma He has obtained Bachelors of Engineering Degree in Electronics and Communication Engineering from Anna University Chennai, Tamil Nadu. Who was worked as (R&D Engineer) in **Signals and System India Pvt.Ltd**-Chennai After that he worked as (Sr.Project Engineer) in **Pantech Solutions Pvt.ltd**-Chennai. Now He is the Director at **APPKEE Solutions Pvt.ltd**-Coimbatore, Tamil Nadu and also pursuing M.Tech. (VLSI Design) from **Bharat University**- Chennai, Tamil Nadu, India. His research interest contributes to the development of VLSI-FPGA Design, Implementation and Low power VLSI Design.

M.Farjanaaameera is doing her Masters of Engineering degree in VLSI Design from Sri Shakthi Institute of Engineering and Technology Coimbatore, Tamil Nadu. She has completed her Bachelors of Engineering in Electronics and Communication Engineering from Anna University Chennai, Tamil Nadu, India.

R.Rajaprabha is a Assistant Professor of ECE Department with Sri Shakthi Institute of Engineering and Technology Coimbatore, TamilNadu. She received her Masters of Engineering degree in VLSI Design from **Karpagam University.** She has completed her Bachelors of Engineering in Electronics and Communication Engineering from Anna University Chennai, Tamilnadu. Her current research interest is in the area of CAD of VLSI, Design of Digital, Analog and Mixed Signal VLSI Circuits, Low power VLSI.

REFERENCES

Journal Papers:

[1] D.E. Holcomb, W. Burleson, and K. Fu. Power-up SRAM state as an identifying fingerprint and source of true random numbers. IEEE Trans. Comp., 58(9):1198–1210, September 2009

[2] J.W. Lee, A. Lim, B. Gassend, G.E. Suh, M. van Dijk, and S. Devadas. A technique to build a secret key in integrated circuits for identification and authentication applications. In Symp. VLSI, pages 176–179, 2004

[3] F. Armknecht, R. Maes, A.-R. Sadeghi, F.-X. Standaert, and C. Wachsmann. A formalization of security features of physic functions. *In IEEE Symp.Sec'ty & Privacy*, pages 397–412, 2011.

Chapters in Books:

[4] J. Guajardo, S.S. Kumar, G. Schrijen, and P. Tuyls. FPGA intrinsic PUFs and their use for IP protection. (In Crypto Hardware & Emb Sys (CHES), 2007) 63–80.

[5] B. Gassend, D. Clarke, M. van Dijk, and S. Devadas. Controlled physical random functions.(In ACSAC, 2002) 149–160.

[6] G. Suh and S. Devadas. Physical unclonable functions for device authentication & secret key generation.(In DAC,2007) 9–14.

Theses:

[7] Defense Science Board (DSB) study on High Performance Microchip Supply, 2005

[8] Defense Industrial Base Assessment: Counterfeit Electronics study by U.S. Dept. Of Commerce Bureau of Industry & Security Office Of Tech. Evaluation, 2010.

[9] R. Maes and I. Verbauwhede. Physically Unclonable Functions: a Study on the State of the Art and Future Research Directions. Springer, 2010

[10] U. Ruhrmair, S. Devadas, and F. Koushanfar. Security Based on Phys. Unclonability and Disorder. Springer, 2011