Journal of Science and Technology
ISSN: 2456-5660 Volume 5, Issue 5, Sep-October 2020
www.jst.org.in DOI: *https://doi.org/10.46243/jst.2020.v5.i5.pp246-252*

Design of (PUF) Physical Unclonable Function Using FPGA and Secured Clock Network (SCN)

G.Usha Rani1, J.Sneha Latha 2
1(Assistant Professor, Department Of Electronics and Communication Engineering , MGIT, Hyderabad, India)
2(Assistant Professor, Department Of Electronics and Communication Engineering , MGIT, Hyderabad, India)
1Corresponding Author: sneha.jaladi@gmail.com

To Cite this Article
G.Usha Rani, J.Sneha Latha *"**Design of (PUF) Physical Unclonable Function Using FPGA and Secured Clock Network (SCN)**", Journal of Science and Technology, Vol. 05, Issue 05, Sep-Oct 2020, pp.:246-252.*

Article Info
Received: 15-10-2020 Revised: 20-10-2020 Accepted: 23-10-2020 Published: 25-10-2020

Abstract:

A constant growth in the number of microelectronic devices and applications is accompanied by a constant rise in the need for goods that are genuine and secure, as well as for electronic systems that are trustworthy. The security requirements for the vast majority of applications are quite stringent and continually evolving, as is the case with most technologies. On top of that, new and more intricate assaults are being developed on a regular basis. These assaults typically have a significantly higher impact than regular attacks, and there is nothing that can be done to compensate for them other than to deploy more software countermeasures to protect against them. The outcome is the development of a PUF (Physical Unclonable Function) system based on clock networks with the goal of improving security. In the rapidly developing field of on-chip Physical Unclonable Functions (PUFs), a powerful security primitive with the capability of addressing a wide range of security challenges is emerging as a viable option. Specific to electrical circuits, we demonstrated a PUF system based on a clock network that may be used to overcome the security difficulties associated with such circuits. An unclonable circuit is created by merging the clock network, return path, and multiplexer (Mux) blocks together. This is a circuit that cannot be reproduced. Sinks are included in the clock network, and they are used to split the data received as input. When a signal is transferred from the clock network to the mux network, the return path is used to transmit the information. Mux networks are made up of three components: a multiplexer, a delay buffer, and an SR latch (synchronous response latch). When the PUF circuit responds, it returns a single bit that cannot be replicated. In a circuit, a PUF is an external device that may be used to prevent cloning of the circuit from taking place. An effective power supply unit (PUF) must have the ability to endure changes in circuit timing that are both reversible and irreversible in nature. For a wide range of applications, PUF functions provide low-cost, high-efficiency, and secure identification and authentication of devices using a number of methods. Anyone attempting to replicate the protected circuit in its same form will find it difficult, and as a result, they will not be able to achieve the same functionality as the device. As a consequence, we will be able to prevent the gadget from being replicated in the future.

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

I. INTRODUCTION

Product identification, security, and the reliability of the electronic system in general are becoming increasingly important. When it comes to electrical products, according to IHS Supply, analogue integrated circuits (25.2%), microprocessors (13.4%), memory integrated circuits (13.1%), and printed circuit boards (PLDs) were the most commonly counterfeited in 2012. (8.3 percent). Nowadays, printed serial numbers are utilised for identification in the vast majority of systems, including ATMs, smart cards, and RFID tags, among other devices. Counterfeiting is expanding at an even quicker rate than the economy as a whole, owing to the widespread use of printed serial numbers for identification in the majority of systems, which makes counterfeiting even more difficult to detect.

Our has a direct influence on the vast majority of enterprises and industries in this country. This fraud is carried out by the individual who has the greatest amount of faith in the company. He or she takes secrets and confidential data from the other corporation or any other organisation and sells it on the black market to another corporation or any other organisation. Because of this, users will be able to swiftly copy and clone the product in a controlled environment. A competent approach in which to do the work is not impossible. Product designers, on the other hand, are physically and emotionally influenced by their work environment. This technology, known as PUF (Physical Unclonable Function), was developed and applied in order to address the counterfeiting difficulties.

The fundamental purpose of this effort is to produce a more secure system at a more affordable cost than currently available. The key objectives of this study are to ensure that the device cannot be replicated or cloned and that it cannot be copied. The products are extremely safe, but they are also reasonably priced, and they may be used for high-level security applications. The goal is to prevent the occurrence of counterfeiting in an electronic device from occurring. In the present day, it is feasible to keep a key safely utilising PUF technology, while simultaneously protecting it against potential attacks that may be conducted in the future.

It is defined as a function that has as its foundation physical characteristics. Because this technology is unique to each chip, it is difficult to predict, but it is simple to assess, simple to create, and reliable. In the majority of circumstances, it would be almost hard to duplicate. A chip authentication system that is both secure and quick is implemented using this method. It is only capable of transmitting information in one direction. It employs a unique and startling approach of mapping barriers and responding to them, which is described below. It is more vulnerable to environmental changes such as temperature variations, power supply voltage variations, and electromagnetic interference variations than other types of semiconductor. The usage of PUF as a root of trust and as a key that cannot be easily reverse engineered has the potential to be extremely beneficial. It is used for applications that need to be both visible and secure at the same time.

With this project, we hope to build FPGA-based cryptography that will be capable of encrypting and decrypting data as it is sent from one computer to another. As described in this article, the encryption / decryption mechanism is created and written into the FPGA, which is then responsible for managing data transfer between the two computers.

II. Related Works

For the purpose of constructing PUF, the most generally used methods are either based on fluctuations in logic gate / wire delays or leakage currents [5, 6], or they make use of a bi-stable circuit element, such as SRAM arrays [1, 4]. The PUF described in [5] made use of the difference in delay between pairs of parallel timing channels that had the same nominal delay in order to achieve their performance. These routes were connected to an arbiter, which generated PUF bits, which were subsequently transmitted to the relevant paths. Challenge bits were used to multiply CRPs by segmenting and multiplexing the paths, resulting in an increase in the number of CRPs. It has been demonstrated that an ASIC can be implemented with 180nm CMOS technology [2]. The United States government and the semiconductor industry have identified potential system vulnerabilities arising from the contract foundry model, such as hardware intellectual property theft and integrated circuit theft, as well as counterfeiting [7, 8]. These vulnerabilities include counterfeiting, hardware intellectual property theft, and integrated circuit theft. The following papers [3, 9, 10] include more information on the design, performance, and security aspects of PUFs that are important to our work.

III. SECRET COMMUNICATION

3.1 CRYPTOGRAPHY

In cryptology, cryptography refers to the branch of study that is concerned with the development of methods for encryption and decryption, all with the objective of maintaining the secrecy of messages. While the plain text refers to the original communication, the secret message refers to the coded form of the same communication, and the two are not synonymous (chipper text). It is referred to as enciphering or encryption in cryptography, whereas the act of recovering plain text from cypher text is referred to as deciphering or decryption in the field of information technology. Cryptography is a discipline of research that investigates the many technologies that are used for encrypting and decrypting communications. In this case, the term "cryptography" refers to an approach that uses encryption.

In cryptanalysis, techniques are studied that can be utilised to decode a communication without having prior knowledge of the material that is encrypted. When expressed in layman's terms, the cryptographic technique is referred to as "contravention of the code." Cryptology is a word that refers to the sciences of cryptography and cryptanalysis when they are considered as a whole.

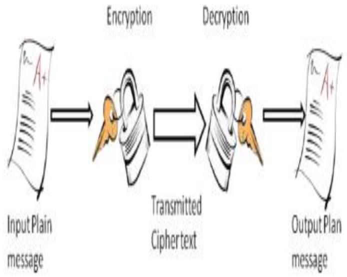

Fig.1 Simplified model of conventional encryption

3.2 DESTROYING THE DESTROYING THE ENCRYPTION

The algorithm's input is the original intelligible message or data that was submitted to the algorithm as a starting point. The plain text is subjected to a number of substitutions and modifications as a result of the encryption process. Aside from that, the secret key is supplied as an input to the encryption algorithm as well. The key is a numeric value that is not dependent on the plain content of the message. A number of various outputs are generated depending on whatever key is being pressed at any particular point in time by the software. The exact substitutions and changes carried out by the algorithm are dependent on the key that was used to carry them out. Currently, the cypher text seems to be an apparently random stream of information that has no apparent value.

3.3 TECHNOLOGY OF DECRYPTIVE KEYS

This is, in essence, the same encryption operation as previously, but with the opposite mechanism being used to do it. It takes the encrypted content and turns it back into the plain text format that it was originally in.

IV. PROPOSED SYSTEM

The goal of this project is to transfer sensitive data in a secure manner utilising Low Cost PUF and a Highly Secured Clock Network, which means that we must first submit the data (in plain text) to the encryption process before sending it back. Cipher text will be produced as a result of this procedure. This encrypted text is sent into the decryption process, and as an output, the data (plain text) is obtained from the procedure. The major goal is that, because we shuffle the data, it will be extremely difficult for an unknown individual to determine the original data. Because each data point will result in a change in the cypher text, the individual must be familiar with the procedure in order to recover the original data.

The input plain text is translated to binary format and transmitted to the FPGA kit through the serial connection during this operation. The data is collected in the internal buffer, and a block will be picked based on the function (encryption / decryption) that is being used. With Secured Clock Network, we were able to create an encryption and decryption method that was low in cost and easy to implement in our design. A cryptogram is a textual representation of the output of an encryption block. It is sent in order to decode data encrypted with it. All of these blocks' outputs are placed in a buffer called the output buffer.

4.1 UNCLONABLE SECRET KEY GENERATION

4.1.1 BLOCK DIAGRAM

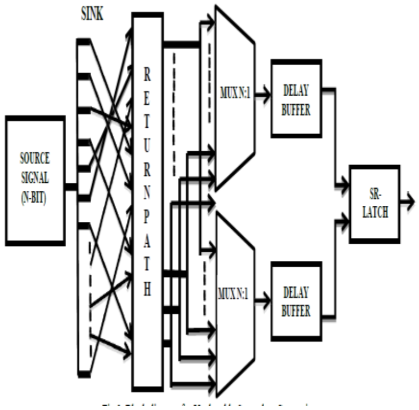

Fig.2. Block diagram for Unclonable Secret key Generation

4.1.2 BLOCK DIAGRAM DESCRIPTION

Detailed information on our suggested PUF architecture may be found in the next section. The establishment of a clock network is required before we can begin implementing PUF. An example of a clock PUF producing stable but unclonable bits as a result of the comparison is when the clock signal is checked for its arrival time on the bus by a clock PUF. By looking at a diagram, it is possible to understand how the clock PUF operates. Please see the section below for further information on the major components of our study.

The source signal is routed to the clock network, where it will be further processed before being returned to the source. The binary integers that make up the source signal are represented as a series of numbers in the source signal representation. This signal is branched off and injected into the sink, where it is received. This is done without interfering with the clock distribution network, which is important.

It is the responsibility of return pathways to collect signals from sinks and transport them to the mux network, where they are utilised for further processing. It is vital to have an even number of inverters on the return path in order to ensure proper operation. As a result of the buffering of the return routes in this place, the process variation from other portions of the chip might be kept in this region.

The multiplexer network selects two clock signals and then performs a comparison between the two clock signals that were picked. A pair of nearby multiplexors or a scattering of multiplexors may be used to spread the clock signal, depending on the architecture of the device.

To increase the amount of variation available, a pair of delay buffers that are controlled from the outside and have matching delays is used.

When the buffer is full, the result of the buffer is transmitted to the SR-latch, which uses it to choose which of two signals will be the first to transition out of the buffer when the buffer is fully loaded.

When constructing this clock PUF, the sink must be carefully chosen and then linked to the return channel with care in order to guarantee that the propagation delay and matching length are equivalent. For the purpose of increasing security, it is not necessary for the sink result to be linked directly to the return path; alternatively, any node of this path may be coupled with the sink result. With the aid of a mux arbiter, it is feasible to compare pairs of clock transitions while also creating a single bit at the same time in one operation. The packet travels through a delay buffer during routing, which is capable of adjusting for any unexpected systematic delays that may occur along the route. In order to tie everything together, a latch is linked at the conclusion of the design.

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 the clock network refers to the point at which a clock network receives its input signal. When providing an input, a binary bit is used as the format. Depending on the input, it may be separated into a number of different levels. Once the single bit separation is achieved, this process will be continued until it is attained. This split bit is given to the sink's input in order for it to function properly. Sink is made out of a hybrid flip-flop and AND gate network, as seen below.

Sink: It is a hybrid of a flip-flop and an AND gate network that is housed in a single package. An individual split bit is defined as a bit that has been isolated from the clock source and fed into the sink's input. In this scenario, the clock source determines the number of sink networks that will be used to do the task. The establishment of a sink network is required for each split bit, therefore resulting in a net gain. The output of the sink network is connected to the input of the return network through this channel. Figure 3 shows a representation of the sink network.

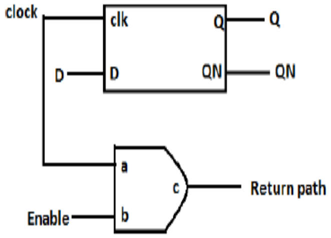

Fig.3 Sink circuit

The return path is the path taken by the clock when it returns to its original location. It is feasible to transmit the value from the input to the output in its original form, with no alteration to the value of the input, while using the PUF architecture. However, any sink output may be linked to any return path input, and the same is true in the opposite direction. Because data updates and repairs are only authorised to be carried out by the designer, the remainder of the team is totally unaware of the interconnections that exist inside the system as a result. It is therefore possible to attain a better level of security depending on the type of connection that is utilised.

Return route networks are created by connecting together a certain number of inverters, which is always an even number, according to the specifications of the designer. When inverters are connected in a uniform manner, the output will be equal to the input; however, when they are not connected in a uniform manner, the response will be variable. After being processed via the return path, the output is sent back into the multiplexer, where it will be further processed.

In computer science, the term "multiplexer" refers to an electrical device that combines multiple signals into a single output signal. Multiplexing is a phrase that refers to the transmission of a high number of bits of information across a single transmission line in one continuous stream. An electrical device called a digital multiplexer (MUX) is a type of device that chooses digital information from a range of sources and sends the information that has been selected via a single data transmission line. A multiplexer is also referred to as a data selector in certain quarters due to the fact that it picks one of many inputs and routes the information to the output as a consequence of the fact that it selects one of numerous inputs.

A total of four data input lines are connected to the multiplexer, but only one output line is connected to the output line, resulting in a total of four data input lines on the multiplexer. The control of the selection of an input line is performed through the employment of a series of selection lines that are sequentially connected. The selection line specifies the maximum number of input lines that a certain multiplexer is capable of processing at any one moment in a given configuration. 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 from a pool of all possible input lines from which to select one of the n input lines from the pool of all potential input lines

Buffer with a short lag time between operations: A delay buffer is a buffer with a short lag time between operations. This gadget just provides one input signal and one output signal, which is sufficient for most applications. This device does provide an output signal that has a little degree of delay, on the other hand.

A device known as the SR-Latch is being utilised in this inquiry. To govern the functioning of the latching mechanism, the S and R inputs of an SR latch are used in conjunction with each other. The letters S and R are used to symbolise the concepts of set and reset, respectively. It is feasible to obtain a high value for Q with the aid of the S input (i.e. store binary 1 in flip-flop). Support for this input is provided in order to achieve a low value on the Q scaling system (i.e. store binary 0 in flip-flop). Given that Q' is the complementary output of Q, it will always have a value that is diametrically opposed to Q. Q' also has a value that is diametrically opposed to Q. S-R latches have an output that is dependent on both the current and prior inputs or states, and the state of the S-R latch (that is to say, the value stored) can change immediately if any of the inputs or states of the S-R latch change.

Implementation of the principles in the real world is covered in Section 4.3.

With the help of the unclonable bit, which we described before, we can build a cryptography key. If you want to control devices that require a higher degree of security than the default, you can utilise this unclonable bit to do so. An external connection is established between the unclonable bit that has been formed and one of the device's inputs, and the device that is externally connected controls the device that is internal. Anyone attempting to correctly replicate or clone the encrypted device will be prevented from doing so because to the internal variance of the device. As a result, the item receives the highest level of security possible while yet retaining its unique identity.

V. SIMULASION RESULT

ModelSim was used to create an exact replica of the document in question. As we can see from the block diagram, each level is dependent on its predecessor in order to respond to the next level in the sequence. The input signal for the source signal is represented by an n-bit binary value. A single bit of information is divided and transmitted to the return channel through the sink by use of this device. After that, it is routed through the mux network, where it is returned as an unclonable bit as a result.

Inputs to the delay arbiter include a pair of delay buffers, which correct for the inherent delay difference between the paths at the time of their creation. A random bit is generated when the nominal delays of two return paths are identical, and the comparison of the two results in the formation of another random bit. Putting a large number of such bits together allows for the tolerance of minor biases in the bits themselves. Empirical findings are obtained when a sufficiently large number of chips are employed to determine optimal delay buffer settings for each individual chip in the system. Increasing the amount of variable entropy available for PUF bit formation and decreasing the amount of systematic bias in delay differences can both help to minimise the amount of systematic bias in delay differences. There are a variety of delay buffer choices available that may be used to increase entropy even more. In the context of a challenge response method, attacks focused on replaying or analysing replies to a single setting are made useless since the setting is employed as a challenge response method. There are no extra tools required to find the best delay buffer and PUF read-out settings because delay buffers may be programmed using multiplexed input ports.

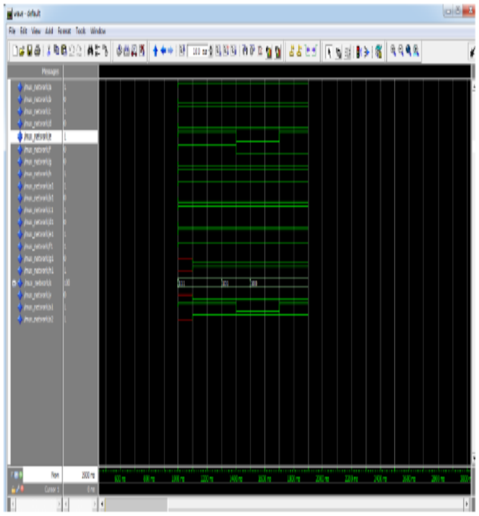

Fig.4 Unclonable bit generation

VI. CONCLUSION

The goal of this project is to provide a PUF system that is based on a clock network for the purpose of providing security. In addition to protecting the legitimacy of the items, this PUF system also safeguards the security and reliability of the electronic system. There are numerous companies today developing and manufacturing products (circuit devices) for mobile phones, laptop computers, iPhones, and other electronic devices; however, the original product designer is not receiving credit for their work as a result of an increasingly widespread problem known as counterfeiting. In order to solve this challenge, we introduced a PUF system that takes use of a clock network as described previously. This circuit creates a security key, which is used to prevent the device from being duplicated by unauthorised individuals. In the case that someone tries to clone the system, they will not be able to gain the exact functionality of the system because of the way the system is designed. As a result, the product containing PUF is no longer available for replication. It is employed in RFID technology and may also be used in other systems such as finger print recognition, smart card systems, and other similar systems, among other things. The use of this product in the interest of national security has been allowed by our government. In recent years, this PUF has attracted a great deal of attention in the semiconductor sector, since it looks to be a realistic alternative for ensuring data security. We have created a product identification number (PUF) system in order to deter counterfeiting and efficiently protect our items from being stolen or lost.

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