International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 03 Issue 14
October 2016

Design and Analysis of Mux-Founded Bodily-Unclonable Features

[1] SANKARLAL PAL, [2] Y.NARESH, [3]B.BALA KRISHNA, [4] Dr.B.S.R.MURTHY

[1] M.Tech Student,DEPT OF ELECTRONICS & COMMUNICATION ENGINEERING. GANDHI ACADEMY OF TECHNICAL EDUCATION, Ramapuram (Katamommu Gudem), Chilkur(M), Kodad, Telangana 508206

[2] M.TECH,Assistant Professor, DEPT OF ELECTRONICS & COMMUNICATION ENGINEERING. GANDHI ACADEMY OF TECHNICAL EDUCATION, Ramapuram (Katamommu Gudem), Chilkur(M), Kodad, Telangana 508206

[3] M.TECH,Assistant Professor, HOD,DEPT OF ELECTRONICS & COMMUNICATION ENGINEERING. GANDHI ACADEMY OF TECHNICAL EDUCATION, Ramapuram (Katamommu Gudem), Chilkur(M), Kodad, Telangana 508206

[4]Phd, Professor, & Principal. GANDHI ACADEMY OF TECHNICAL EDUCATION, Ramapuram (Katamommu Gudem), Chilkur(M), Kodad, Telangana 508206

ABSTRACT:

Silicon bodily unclonable functions (PUF) make use of the variant for the duration of silicon fabrication method to extract knowledge so as to be distinct for each and every chip. There have been many up to date tactics to how PUF can be used to make stronger security associated applications. Nevertheless, it is recognized that the fabrication variant has very powerful spatial correlation and this has been mentioned as a security threat to silicon PUF. Physical unclonable features (PUFs) can store secret keys in built-in circuits (ICs) through exploiting the uncontrollable randomness because of manufacturing approach variants. These PUFs can be used for authentication of instruments and for key iteration in protection applications. This paper presents a rigorous statistical analysis of quite a lot of types of multiplexer-centered (MUXbased) PUFs including the customary MUX PUF, the feed ahead MUX PUFs, the modified feed-forward MUX PUFs, and multiplexer demultiplexer (MUX/DeMUX) PUF. The modified feed-forward MUX PUF structure is a new structure that's presented on this paper. Three varieties of feed-ahead PUFs are analyzed on this paper. These include feed-ahead overlap, feed ahead cascade and feed-ahead separate. The performance evaluation quantifies inter chip and intra chip variants as a operate of the quantity of stages, the procedure variant variance, the environmental noise variance, and the arbiter skew for one of a kind PUFs. Three different metrics of performance are also presented and analyzed on this paper, which comprise reliability, uniqueness, and randomness. A PUF is extra nontoxic if it

has less intra chip variant. A PUF is more designated if the inter chip variant is towards 50%. A PUF is extra random if its response bit is zero or 1 with equal likelihood. Our statistical evaluation shows that the intra chip

variation is less elegant on the quantity of stages, N, if N is higher than ten. However, the inter chip version is elegant on N if N is less than a hundred. It is proven that the feed ahead PUFs have larger intra chip version than MUX PUFs; however, the modified feed-forward PUFs have drastically lower intra chip version than the feed-forward PUFs. It's shown that the modified feed-forward cascade MUX PUF has the best area of expertise and randomness, even as the usual MUX PUF has the best reliability. The evaluation provided in this paper can be used via the designer to select an appropriate PUF established on the appliance's requirement. This eliminates the need for fabrication and testing of many PUFs for selecting an correct PUF.

INTRODUCTION:

Since the number of networked smart objects, programs, and data is constantly increasing,there is an equally growing demand to ensure the security and reliability of these units. Since they are pervasive in our daily lives, this issue has become a significant societal challenge. One central task lies in realizing secure and reliable identification, authentication, and integrity checking of these systems .Integrated circuits have become an integral part of the world we live in. The era of ubiquitous computing is upon on us as we are surrounded by a host of electronic devices that facilitate different sectors such as banking, healthcare and transportation. Smart card applications such as credit cards, transportation payment systems, RFID tags and wireless sensor networks are becoming increasingly widespread. The field of hardware security assumes greater significance in the context of these applications. Smart cards should be capable of performing reliable authentication, store sensitive data such as ATM passwords and perform secure communication between devices. These requirements motivate the need to have secure cryptographic primitives in hardware. "Security engineers face the seemingly contradictory challenge of providing lightweight cryptographic algorithms for strong authentication, encryption and other cryptographic services that can perform on a speck of dust." The integrity of authentication schemes and encryption algorithms lies in a unique ID or a secret key. Hence it is imperative that

these secret keys aregenerated and stored in a secure manner, protecting them from malicious attackers. Conventional approaches rely on storing the secret key in non volatile storage on chip,either in fuses or EEPROMs. However, these are susceptible to invasive attacks as the secret isstored permanently in digital form. Reverse engineering attacks using a combination of chemical and optical methods allow an attacker to read out the entire digital content stored in memory. Preventing invasiveattacks becomes an expensive proposition as it involves providing tamper resistant hardware. Non invasive attacks such as side channel attacks pose a new threat to achieving secure hardware protocols. Side channel attacks prove to be very powerful as they bypass the theoretic and mathematical security of the cryptographic algorithms and extract the information presented due to implementation weaknesses. Side channel attacks leverage the fact that the electrical characteristics of a chip such as power and timing are data dependent. Successful attacks using differential power analysis and EM analysis has been carried out to leak the secret key used during encryption. Hence, any hardware mechanism aiming to be robust should be resistant to invasive and non invasive attacks. In addition to these concerns, ultra low power applications such as wireless sensor networks and RFID tags impose additional constraints. Passive RFID tags are powered by RFID readers through inductive coupling, limiting the power that can be consumed by digital circuitry. The energy per operation becomes a concern in battery powered devices such as Active RFID tags. In the near future, wireless sensor nodes may depend on energy harvesting from ambient energy sources such as solar energy for their power requirements. This would impose tighter constraints on the power consumption of an integrated circuit. Further, smartcards are implemented with small form factors aimed at reducing the cost of each device. RFID tags limit the number of gates to be used by security primitives to 2000 [6]. Hence, a good cryptographic Primitive should be lightweight, occupy little area on silicon and should have very low power Consumption. As electronic devices become ubiquitous and interconnected, people are increasingly relying on integrated circuits (ICs) for performing security sensitive tasks as well as handling sensitive information. For example, an RFID is often used as a key card to controlaccess to buildings, smart cards carry out financial transactions, and

mobile phones often contain sensitive data such as confidential documents, personal emails, etc. Therefore, it is critical for ICs to be able to perform operations such as authentication of devices, protection of confidential information, and secure communication in an inexpensive yet highly secure way. A common ingredient that is required to enable the above security operations is a secret on each IC, which an adversary cannot obtain or duplicate. The current best practice is to place a secret key in non-volatile memory such as fuses and EEPROM, and use cryptographic primitives such as digital signature and encryption to authenticate a device and protect confidential information. Two important metrics that are typically applied to categorize the uniqueness and robustness of PUF responses and UNO fingerprints are inter-device and intra-device distances. Inter-device distance is often quantified as the average Hamming distance between the responses to the same challenge obtained from two different PUFs/UNOs, or the average distance between the fingerprints of two unique objects measured in the same conditions. Intra-device distance is the average Hamming distance between the responses to the same challenge applied at different times and environmental conditions to the same PUF/UNO, or the average distance between the repeatedly measured fingerprint(s) of a unique object. Ideal PUFs and UNOs should lead to large inter-device and small intra-device distances. Another key requirement for PUFs and unique objects is the entropy of the resulting responses or fingerprints. The entropy quantifies the number of independent IDs that can be generated by the same device architecture.

II. LITERATURE SURVEY: A. Silicon MUX PUF: There are several subtypes of PUFs, each with its own applications and security features. A major type is the so-called silicon PUFs, which exploit the delay variations of circuit components to generate a unique signature for each IC. Silicon PUFs can be integrated into chips very conveniently, since these are implemented with standard digital logic and do not require any special fabrication. The examples of Silicon PUFs include: 1) MUX PUF 2) ring oscillator PUF 3) SRAM PUF and 4) butterfly PUF A MUX PUF is an example of a Strong PUF that is unclonable due to manufacturing process variations, and can accommodate many possible challenge-response pairs (CRPs). As illustrated in Fig. 1, in a MUX PUF, each challenge creates two paths through the circuit that are excited

simultaneously. The output is generated according to the delay difference between the two paths. A MUX PUF consists of N stages of MUXs and one arbiter which connects the last stage of the two paths. MUXs in each stage act as a switch to either cross or straight propagate the rising edge signals, based on the corresponding challenge bit. Each MUX should be designed equivalently, while variations will be introduced during manufacturing process. Finally, the arbiter translates the analog timing difference into a digital value. For instance, if the rising edge signal arrives at the top input of the arbiter earlier than the signal arriving at the bottom input, the output will be one; otherwise, if it reaches the bottom path first, the output will be zero. The output response depends on the applied challenge bits and will be permanent for each IC after fabrication or only vary in a small range due to environmental variations. For transistors, manufacturing randomness exists due to variations in transistor length, width, gate oxide thickness, doping concentration density, body bias, metal width, metal thickness, and interlevel dielectric (ILD) thickness, and so on . These manufacturing variations lead to a significant amount of variability for the MUX-based PUFs, which are sufficient to generate unique challenge-response pairs for each IC by comparing the delays of two paths

Definition of PUF Performance By simulating The quality of a PUF is determined by three important metrics namely uniqueness, Reliability and security. In addition to these metrics, the design cost of the PUF in terms of area and power consumption also plays a key role in choosing the PUF for different applications. The three main metrics of a PUF circuit are discussed below. Uniqueness Uniqueness is the most important property of a PUF as it indicates the ability to distinguish between different ICs. Uniqueness is determined by applying different inputs for the same system the output must be different. The identification capability of a PUF is directly related to the amount of process variation, specifically inter-chip variation present. Large process variation results in a larger value of uniqueness. Reliability A robust PUF circuit should be capable of reproducing CRPs in presence of noise and environmental variations. Supply voltage variations and temperature variations impact the delay and power consumption of a circuit and it may affect different parts of the circuit differently. This can result in different responses for the same challenge

from a given PUF instance. Most PUF circuits use relative comparison to generate CRPs achieving a high degree of reliability. In spite of relative comparisons, some erroneous responses can occur. This is measured by looking at the total number of bit errors in responses obtained by subjecting the PUF to different voltage and temperature conditions. Security The security metric in PUFs indicates a PUF's susceptibility to different types of modeling attacks. The key notion in PUFs is that it is impossible to construct an exact replica of a PUF instance even with complete knowledge of the design. This is an extremely useful property as it prevents untrusted foundries from producing counterfeit chips. However it is possible to mimic the challenge response behavior of a PUF through software modeling techniques. In Linear PUFs, stages delays are additive in nature and this gives rise to modeling attacks through Support Vector Machines (SVM). High prediction accuracies greater than 90%can be achieved through SVM attacks on linear PUFs such as Arbiter PUFs. To counter these attacks, non linearity's have been introduced to create feed forward and arbiter PUFs. However a recently proposed machine learning method is capable of breaking all current PUF constructions. The three feed-forward MUX PUF structures with the same parameter variations and environmental conditions, we were able to conclude in [19], [20] that the FFO structure is the most reliable among the three feed-forward structures. In this paper, we focus on analyzing the quantitative performance of various MUX-based PUFs through statistical modeling of the delay variations and environmental variations. Performance indicators ranging from zero to one with one representing the best performance are generated through a theoretical analysis. Randomness A MUX-PUF is expected ideally to produce unbiased 0's and 1's. Randomness represents the ability of the PUF to output 0 and 1 response with equal probability. Therefore, a randomness of one indicates unbiased PUF responses.

NOVEL RECONFIGURABLE PUFS In order to add reconfigurable property into general MUX based silicon PUFs, we must make the challenge-response pairs (CRPs) reconfigurable, which can be used to update the database for an authentication system. The methods can be classified into two categories: (a) Make the challenge-response pairs reconfigurable directly, by adding some extra circuits into the structure, but without configuring the main PUF circuit.

This can be achieved by utilizing some techniques to preprocess the challenge before applying to PUF or pre-process the response before using it for authentication. (b) Make the PUF circuit reconfigurable, therefore the challenge response pairs will be reconfigurable as well. We propose several novel non-FPGA reconfigurable PUFs implementations for the above two categories, which would be more suitable for practical use than FPGA-based techniques. Furthermore, we address the reliability and the security of the PUF performance, as some information of the hidden secrets that an adversary can take advantage of may leak out during reconfigurations.

CONCLUSION We have presented a systematic statistical approach to quantitatively evaluate various types of MUX-based PUFs. We defined three performance indicators reliability, uniqueness, and randomness to compare the performances of these MUX-based PUFs. These indicators are also validated by the corresponding simulation results. The experimental results show that the proposed statistical analysis approach effectively reflects the characteristics of various PUF designs. We have also proposed a novel modified feedforward MUX PUF structure, which has better reliability than the standard feed forward MUX PUF.

REFERENCES

[1] R. Pappu, B. Recht, J. Taylor, and N. Gershenfeld, "Physical one-wayfunctions." Science, vol. 297(5589), p. 2026, 2002.

[2] B. Gassend, D. Clarke, M. V. Dijk, and S. Devadas, "Silicon physicalunclonable functions," the 9th ACM Conference on Computer andCommunications Security, p. 160, 2002.

[3] ——, "Controlled physical unclonable functions," in Computer SecurityApplication Conference, 2002, pp. 149–160.

[4] S. Kumar, J. Guajardo, R. Maesyz, G. Schrijen, and P. Tuyls, "Extendedabstract: The butterfly PUF protecting IP on every FPGA," Hardware-OrientedSecurity and Trust (HOST 2008), pp. 67–70, 2008.

[5] R. Maes, P. Tuyls, and I. Verbauwhede, "Intrinsic PUFs from flip-flops onreconfigurable devices," in Benelux Workshop Information and System Security(WISSec 08), 2008.

[6] D. E. Holcomb, W. P. Burleson, and K. Fue, "Initial SRAM state as a fingerprintand source of true random numbers," in Conference on RFID Security, 2007.

[7] U. Ruhrmair, F. Sehnke, J. Solter, G. Dror, S. Devadas, and J. Schmidhuber,"Modeling attacks on physical unclonable functions," in Conference on RFID Security, 2010.

[8] M. Majzoobi, F. Koushanfar, and M. Potkonjak, "Techniques for design and implementation of secure reconfigurable PUFs," ACM Transactions on Reconfigurable Technology and Systems, vol. 2, no. 1, pp. 1– 33, 2009.

[9] D. Lim, J. W. Lee, B. Gassend, G. E. Suh, M. V. Dijk, and S. Devadas, "Extracting secret keys from integrated circuits," IEEE Transaction on Very Large Scale Integration Systems, vol. 13, no. 10, p. 1200, 2005.

[10] H. Chang and S. Sapatnekar, "Statistical timing analysis considering spatial correlation in a pert-like traversal," in IEEE International Conference Computer-Aided Design Integrated Circuits and Systems, 2003, pp. 621–625.