Counterfeit IC Countermeasure with 4T Cell Based Authentication Circuit

Authors: Pallavi Ebenezer, Degang Chen, and Randall Geiger
Authors Affiliation: Iowa State University
Authors Contact Information: Randall Geiger rlgeiger@iastate.edu 515-294-7745

***Abstract*— A simple and compact authentication circuit based on a 4T bit cell is proposed for counterfeit detection and avoidance. The PUF-based authentication circuit has been designed to reduce or eliminate the reluctance of COTs manufacturers to include on-chip fingerprints by not requiring additional die area, I/O pins, or read-out circuits and by using a deep-sleep mode during normal circuit operation so that it does not interfere with operation of the main IC.**

Keywords— PUF circuit; counterfeit countermeasure; 4T cells; trusted electronics; hardware security

I. INTRODUCTION

The semiconductor industry with its cutting edge technology serves a wide range of consumers which support electrical power grids, communication systems, the healthcare and medical industries, the automotive field, as well as military and aerospace applications. A growing and critical challenge is maintaining legitimate semiconductor products throughout the supply chain. Counterfeit semiconductor parts are now routinely slipped into the supply chain surreptitiously replacing legitimate components produced by authorized sources [1]. These counterfeit ICs pose a major threat to many end users where reliability and performance are critical. Invariably most of the compromised parts are illegitimate and unsafe and have properties and characteristics that are much different than those of the original part even though they may pass basic incoming functional and parametric tests.

In contrast to adversaries whose goal is to introduce Trojans that deliver a disruptive payloads, the motivation of the counterfeiters is almost entirely driven by financial incentives. Counterfeit parts are particularly prevalent in the marketing of discontinued and/or obsolete semiconductors which are essential for maintaining legacy products and many military systems that have a very long service life [6].

The identification of counterfeit ICs is challenging since counterfeiters have become experts at making counterfeit parts look and perform much like that of the original part through the use of sophisticated tools and techniques that are available for legitimate use throughout the semiconductor industry. In recent years, several techniques have been used to detect and thwart the counterfeit ICs which are circulating in the supply chain but in spite of these initiatives, the "counterfeit IC industry" is still prospering. Most ICs produced by the semiconductor industry are lacking of any counterfeit protection provisions and as long as these parts are being used in active electronic systems, they will continue to be ready targets for counterfeiters. Anti-counterfeit measures are needed now for new components and even existing devices that are still in production so that they can be trusted throughout their complete life cycle. One particularly effective method of counterfeit detection and prevention is to establish a process flow whereby parts are authenticated by means of an identifier or tag or an additional fingerprint circuit. Several efficient and effective IC authentication techniques have been available for almost 20 years [2],[3],[5],[6] but widespread adoption of these techniques by the major semiconductor companies has not occurred. This lack of adoption is primarily due to what have been viewed as unfavorable economic tradeoffs by most major players in the semiconductor industry.

This paper focuses on Hardware Intrinsic Security (HIS) where the authentication and security for the component is determined by the inherent unique physical properties of the devices which can be attributable to random process variations that naturally occur during the manufacture of an integrated circuit. It is well known that unique fingerprints can be designed that are physically unclonable by using circuits that are generally classified as physically unclonable functions (PUFs) though for some approaches, "spoofing" of the fingerprint is possible. The major drawback of existing PUF-based authentication approaches is the additional cost (area, power, pins, …) and time required for reading PUF codes and maintaining a PUF-code database. The effectiveness of PUF-based authentication is, in part, reflected in the ChipDNA PUF™ security technology recently introduced by Maxim Integrated where they claim this technology [7] "provides an exponential increase in protection against the invasive and reverse engineering attacks" but the additional cost is reflected, in part, in the observation that this security technology is currently marketed (e.g. DS28E50) in a separate 6-pin IC package.

The proposed IC authentication technique that is used as a counterfeit countermeasure overcomes these limitations of time, area and cost. It is built using a small and simple 4T cell to create a random bit and combining a number of these 4T cells to form a unique code sequence. The random bit-generator block also serves as a shift register that can be used to read out the random PUF code. This makes the layout of the authentication circuit very compact and small enough to be put under a bonding pad, an area that is often not utilized for other

purposes, thus overcoming the concerns of an increase in die area. The authentication circuit is designed to operate when the normal supply voltage is around half of the normal supply voltage ($V_{dd}/2$) but it disconnects itself from the main circuit when a normal supply voltage of V_{dd} is applied. Thus the fingerprint circuit is isolated from the main circuit and does not interfere with the operation of the main IC. The authentication circuit shares the input, output, and ground pins with the main IC so does not require any additional pins thereby reducing a second major concern of the manufacturer.

Implicit in this work is the assumption that a database be created that keeps track of the fingerprint of circuits manufactured with the authentication circuit. Details about how that database is created, who has access to data in the database, how that database is financed, and what is included in the database is beyond the scope of this work. But with widespread cloud access and with the ability to reliably manage large databases, it is envisioned that the per-IC cost for access to this database will be small and the reliability of using this for the purpose of authentication will be very high.

II. BACKGROUND AND PRIOR ART

The concept of using fingerprint circuits for device authentication has been a topic of interest from the beginning of the twenty first century. In 2000, Lofstrom et al. [2] proposed a method to extract unique and random code based on the random mismatch variations in the threshold voltages in an array of MOSFETs using an auto-zeroing comparator. The concept of a PUF which started out with physical one-way functions and then physical random functions [3],[4] followed shortly thereafter. In most of these works, the PUFs possess multiple challenge-response (CRP) pairs. Over the last few years considerable research efforts have been focused on authentication and hardware security resulting in the introduction of a large number of different PUFs. The CRPs of the PUFs are essentially all based upon inherent random variations in the physical properties of simple devices that cause corresponding random variations in electrical characteristics of simple circuits. These include random variations in the delay of a gates, the threshold voltage of transistors, the resistance in segments of the power grid of a chip [8], the capacitance of separate segments in the top metal layer of an IC, the relative delay of two nominally identical paths in a circuit, and the oscillation frequency of a ring oscillator.

Random variations in threshold voltage and gate delays also give rise to intrinsic PUFs associated with the inherent binary output of memory elements, such as SRAMs, latches, and flip-flops that express a random output when forced to a nominally metastable state. Su et al. proposed a structure with an array of bit cells comprised of cross-coupled NOR logic gate latches [9] which produce a random high/low bit based dominantly on the threshold voltage (V_{th}) mismatch of the latch transistors. This technique requires additional decoder circuitry, a readout circuit, pins, and pad drivers. The concept of Fingerprint Extraction and Random Numbers (FERNS) depends primarily on the random mismatch in the V_{th} in the bit cells of the SRAM arrays [10]. Existing SRAM arrays are forced to a nominally metastable state on power up and this results in the generation of a random code in the bit cells. This approach requires minimal additional circuitry. However, additional logical circuits are required for bitshift and bitwise logical operations.

III. TRANSISTOR REUSE FOR AREA REDUCTION

The proposed circuit is similar to the prior art in that it extracts the random code from the mismatch device characteristics in a 4T bit cell. The 4T bit cell is based upon the standard two-inverter loop. The random output code is dominantly determined by the random variations in the threshold voltage. But there are key differences between the existing works and that proposed here. In this work, the fingerprint circuit uses a dedicated minimum-sized 4T bit cell to generate a random binary code but uses the same transistors to form a shift register that is used as a serial readout circuit. The use of minimum-sized transistors in the bit cells enhances the required mismatch between the transistors and also helps reduce the overall die area for the authentication circuit. This circuit is entirely dedicated to random bit generation and is functional only when the main supply voltage is set at approximately half of the nominal value V_{dd} value. Under normal operation of the main IC, the authentication circuit disconnects itself from the circuit so that it doesn't interfere with the operation of the main IC. The authentication circuit reuses the supply, ground and output pins of the main IC thereby eliminating the need for additional pins and pad drivers. The array of 4T cells, when configured as a shift register, is connected in a circular loop thereby continually streaming the random binary sequence to the output when the supply voltage is set at approximately half of the nominal V_{dd} value.

In addition to reusing the transistors in the 4T bit cells to form a shift register, by pairing each the inverters in a bit cell with inverters in adjacent bit cells, another set of 4T bit cells can be created and this set of 4T bit cells can be used to create another random binary sequence. This reuse of the inverters effectively doubles the number of the random Boolean variables provided by the 4T bit cells. With this inverter reuse, each of the 4T bit cells effectively provides two random Boolean outputs.

By using minimum-sized transistors in the 4T bit cells, by reconfiguring the bit cells to form a recirculating shift register for readout, and by doubling the number of effective bits per bit cell, the area required for the authentication circuit can become very small. Even in rather large feature processes, the area required with this approach to generate enough random bits for

use in chip authentication is sufficiently small that the authentication circuit can be placed under a bonding pad. Details about the implementation are discussed in the following section.

IV. OPERATION AND IMPLEMENTATION

A. *Anti-counterfeit Circuit*

A block diagram of the proposed anti-counterfeit circuit is shown in the Figure 1. In this circuit, four pins (V_{DD1}, V_{DD2}, Gnd, Out) are common between the main IC and the authentication circuit.

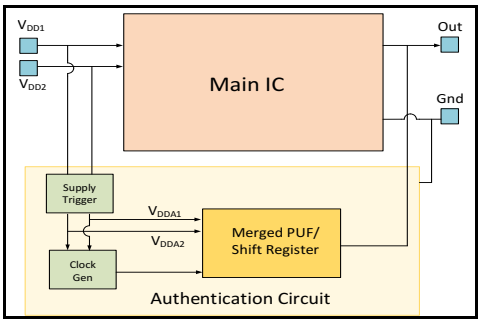

Fig. 1. Block diagram of anti-counterfeit circuit

The Supply Trigger circuit produces supply voltages V_{DDA1} and V_{DDA2} to power the Authentication Circuit when the voltages on V_{DD1} and V_{DD2} are at or below approximately half of the nominal supply voltages for the Main IC. The Supply Trigger disconnects the Authentication Circuit when normal operating voltages are applied to the main circuit.

The fingerprint of the circuit is generated in the Merged PUF/Shift Register (MPSR). The MPSR is a bi-directional circulating dynamic shift register. 4T bit cells are formed by the pair-wise coupling of adjacent inverters in the shift register in what is generally termed the static-hold mode of operation. When powered up in the static-hold mode, a Boolean code which represents the fingerprint is captured in the output of the 4T bit cells. After the fingerprint is captured, the MPSR is clocked and one node of the Shift Register is connected to the Output pin of the circuit. As long as the clock is active, the fingerprint will be serially present on the Output pin. Since each inverter in a standard dynamic shift register is adjacent to two inverters, there are two natural pairings of the inverters into 4T bit cells and each pairing results in a unique Boolean output when powered-up in a static-hold mode. Though there might be a small correlation between adjacent Boolean outputs, this correlation will be small. Thus the MPSR can provide two serial outputs thereby doubling the effective number of bits in the fingerprint over what would be attainable with fixed 4T bit cells.

As in the earlier work of the authors [11], [12], random variations in device characteristics of small transistors are used to generate the random binary sequences. In this work, the random code is generated in minimum-sized 4T bit cells that, along with shift and transfer switches, comprise the MPSR. As is standard when using 4T bit cells to generate random Boolean codes, the two inverters internal to the 4T bit cells are ideally matched and, upon power-up, are driven to operation in a metastable state. Because of random variations in device characteristics the inverters will leave the metastable state and generate a valid Boolean value at the output. This Boolean value is a random variable at the design stage and, in a well-designed bit cell with a symmetric layout, has an equal probability of being high or low. Since most bit cells will express the same output each time the circuit is powered up, the Boolean output of a MPSR comprised of n bit cells (i.e. 2n inverters) forms an n-bit digital fingerprint and if the bit sequence is sufficiently long, this digital fingerprint will be unique for each chip. In most processes, the random variation in the threshold voltages of the transistors will be the dominant contributor to the randomness of the Boolean output of the bit cell. In most prior works, each 4T bit cell produces one bit in the fingerprint sequence. Since each inverter in the MPSR can be naturally associated with two 4T bit cells, each 4T bit cell effectively produces 2 bits in the fingerprint sequence.

B. *Implementation of Fingerprint Generator*

An implementation of a segment of the MPSR is shown in Figure 2. During Mode 1, the even/odd inverters (e.g. I_{NV2}:I_{NV3}, I_{NV4}:I_{NV5},…) are pairwise connected to form 4T bit cells using the appropriate switches to force the MPSR into the static hold mode at startup. After the outputs which comprise the first fingerprint code have stabilized, the MPSR is clocked and the first fingerprint code will circulate in the shift register. Mode 1 is initiated by setting V_{DDA1} to half the nominal supply voltage of the main IC and setting V_{DDA2} =0.

During Mode 2, the odd/even inverters (e.g. I_{NV3}:I_{NV4}, I_{NV5}:I_{NV6} …) are pairwise connected to form 4T bit cells using the appropriate switches to force the MPSR into the static hold mode at startup. After the outputs which comprise the second fingerprint code have stabilized, the MPSR is clocked and the second fingerprint code will circulate in the shift register. Mode 2 is initiated by setting V_{DDA2} to half the nominal supply voltage of the main IC and setting V_{DDA1} =0.

During readout, in Mode 1, the dynamic shift register shifts from left to right and in Mode 2, the dynamic shift register shifts from right to left. Merging of the PUF generator with the shift register to form the MPSR should be apparent from the schematic shown in Figure 2.

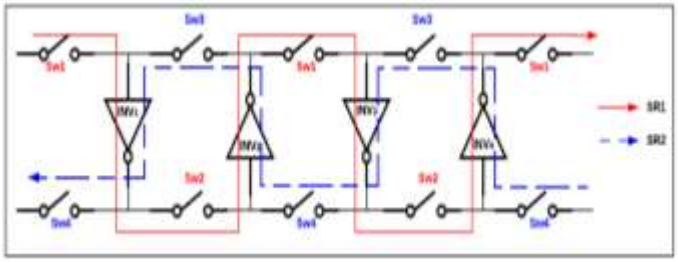

Fig. 2. Merged PUF/Dynamic Shift Register

The two circulating output sequences generated by the MPSR contain the digital fingerprint but without a sychronization signal at the output, it will be difficult to determine where the sequence starts or, equivalently, it will be difficult to associate the serial output with the output that was estabilshed in the 4T bit cells. Though the circulating sequences also represent a fingerprint even if an association between bit-cell location and Boolean output code is not made, in this work we will provide a frame header so that the actual outputs of the 4T bit cells can be read directly from the output sequence. One way do this would be to provide a synchronization signal on another output pin but to minimize the number of output pins that are used to read the output, a header will be embedded in the serial output sequence. This will be achieved by fixing the sizing on a portion of the inverters in the MPSR so that they always provide a predetermined output on the 4T bit cells. This frame header will be used in an external Clock and Data Recovery circuit to frame the data. This approach is widely used in standard serial data transmission. This will require a modest amount of area overhead in the MPSR.

V. SIMULATION RESULTS

An authentication circuit with a 64-bit random PUF code and a 16-bit deterministic frame header has been designed in a 0.13µm CMOS process. The estimated area for this circuit is 0.014mm^2. This is comparable to the area of a bonding pad.

Simulation results of the serial output of the MSPR for two samples obtained from a Monte Carlo simulation are shown in Figure 3 where for illustrative purposes, the deterministic frame header was reduced to 5 bits, [01010] and [10001], for Modes 1 and 2 respectively. The left part of the figure shows the output when operating in Mode 1. The right part of the figure shows operation during Mode 2. In the middle part of the figure, the supply voltages VDD_{A1} and VDD_{A2} are both 0V. From these simulations, the presence of the frame header bits (in the black squares) should be apparent. The first several bits of the PUF sequence are shown following the header bits. Many simulations have been made that show the randomness of the PUF sequences.

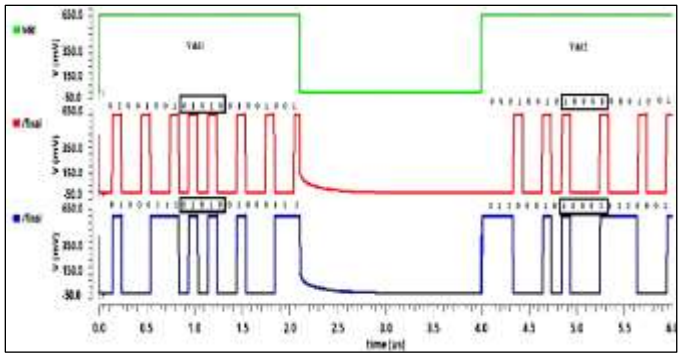

Fig. 3. Simulation Result of the Authentication Circuit

VI. REMOVAL OF FINANCIAL INCENTIVES

The goal of this work is to reduce the counterfeit ICs introduced in the supply chain by reducing or eliminating the financial incentives while requiring no increase in die area and no additional pins in the IC. By reusing the pins of the main IC, by making the area small enough to place the authentication circuit under a bonding pad, and by shutting the authentication circuit off during normal operating of the main IC, the reluctance of semiconductor manufacturers to incorporate authentication circuits on components should be reduced.

In this work, no mention was made of the strength of the PUF or of whether this approach can be "spoofed". Since the "counterfeit IC industry" is strictly driven by financial incentives with essentially no concerns of malice, this work focuses only on removing financial opportunities for counterfeiters. No attempt was made to create a strong PUF and no attempt was made to prevent "spoofing". At the expense of additional area, very strong PUFs could be created and "spoofing" could be made arbitrarily challenging. But since this work is not focusing on hardware security, neither become relevant for reducing the financial incentives for counterfeiters. Further, any overhead to make "spoofing" more challenging will likely come at the expense of increased cost to the semiconductor manufacturers which are currently reluctant to include authentication protocols.

The proposed approach is easy to "spoof". One simple spoofing approach would be to read the code of a "legitimate" device, presumably purchased by the counterfeiter, and then deterministically store that code in a separate piece of hardware that is either internal to or adjacent to the die of a counterfeit part. But the cost of producing such a part would likely be dramatically higher than the market value of the corresponding counterfeit IC. And, since presumably an IC with a given fingerprint could only be sold once (assuming the database has entries that keep track of "purchased" parts), the financial opportunity to market a large number of counterfeit ICs following this approach would be non-existent.

The strength of the PUF, the reliability of a PUF, or even the uniqueness of the PUF is also of little concern. For example,

if a small percentage (e.g. 0.01%) of legitimate devices are incorrectly classified as counterfeit because the PUF code is incorrectly read, the end user would simply discard the device without concern of whether the device was really a counterfeit part or not. If the PUF code on a legitimate part were on occasion incorrectly read and overlapped with a valid code of another legitimate but un-purchased part, the consumer would still have a legitimate part and the legitimate un-purchased part would then be condemned since it would then be incorrectly labeled as "purchased". But a subsequent consumer would then discard that part even though the part was legitimate. Without a financial incentive to the counterfeiter, counterfeit parts would simply disappear from the supply chain.

VII. CONCLUSION

A simple authentication circuit has been proposed that requires minimal area overhead, no pin overhead, and that has no impact on the operation of the main integrated circuit. This approach reduces most of the major concerns of semiconductor manufacturers about incorporating authentication protocols in commercial of the shelf components. It is intentionally a simple circuit but should be effective for reducing or eliminating the financial incentives that drive the counterfeit IC supply chain today.

ACKNOWLEDGEMENTS

This work was supported, in part, by the National Science Foundation (NSF), by the Semiconductor Research Corporation (SRC), and by the Texas Analog Center of Excellence (TxACE).

REFERENCES

[1] M. Pecht,"The counterfeit electronic problem", Open Journal of Social Sciences, 1(12), 2013.

[2] K. Lofstrom, W. R. Daasch, and D. Taylor, ''IC identification circuit using device mismatch", IEEE Int. Solid-State Circuits Conf (ISSCC), pp. 372–373, Feb. 2000.

[3] B. Gassend, D. Clarke, M. V. Dijk, and S. Devadas, ''Silicon physical random functions", Comput. Commun. Security Conf., pp. 148–1, 2002.

[4] G. Suh and S. Devadas, ''Physical unclonable functions for device authentication and secret key generation,'' Proc. Design Autom. Conf., pp. 9–14, 2007.

[5] R. Maes amd I. Verbauwhede, " Physically unclonable functions: A study on the state of the art and future research directions", Towards Hardware-Intrinsic Security, Information Security, and Cryptography, pp. 3–37, Springer, Heidelberg , 2010.

[6] U. Guin, K. Huang, D. DiMase, J. Carulli, Jr., M. Tehranipoor, and Y.Makris, "Counterfeit Integrated Circuits: A Rising Threat in the Global Semiconductor Supply Chain", Proceedings of the IEEE, pp.1207-1228, Aug. 2014.

[7] "ChipDNA PUF Security Overview", https://www.maximintegrated.com/en/design/partners-and-technology/design-technology/chipdna-puf-technology.html, Jan 2019.

[8] D. Lim, J.W. Lee, B. Gassend, et al., "Extracting Secret Keys from Integrated Circuits," IEEE Trans. VLSI Systems, vol. 13, no. 10, pp. 1200-1205, Oct., 2005.

[9] Y. Su, J. Holleman, and B. Otis, "A 1.6pJ/bit 96% Stable Chip-ID Generating Cicuit using Process Variations", IEEE International Solid-State Circuits Conference (ISSCC), pp. 15–17, Feb. 2007.

[10] D. Holcomb, W. Burleson, and K. Fu, ''Power-up SRAM state as an identifying fingerprint and source of true random numbers,'' IEEE Trans. Computers, vol. 58, no. 9, pp. 1198–1210, Sep. 2009.

[11] P. Ebenezer, D. Chen, and R. Geiger, "Unauthentic IC Countermeasures for Future Integrity of the Semiconductor Supply Chain", IEEE National Aerospace and Electronics Conference (NAECON), pp.158-164, 2018.

[12] Q. Wang, P. Ebenezer, J. Aymond, D. Chen, R. Geiger, "Counterfeit Countermeasures with Subthreshold Authentication Undercircuits", Government Microcircuit Applications and Critical Technology Conference, (GOMAC-Tech), 2018.