Authentication Circuit with Low Incorporation Barrier for COTs Manufacturers

Pallavi Ebenezer, Degang Chen, and Randall Geiger
Iowa State University
rlgeiger@iastate.edu

***Abstract*— A simple PUF-based authentication circuit is proposed that will lower the entry barrier for counterfeit countermeasures by COTs manufacturers of integrated circuits. The on-chip fingerprint circuit does not require additional die area, I/O pins, or a separate read-out circuit. This approach to assuring integrity in the semiconductor supply chain will result in negative financial incentives for counterfeiters. An 80 bit authentication circuit which includes a 16 bit frame header has been designed in a UMC 65nm process with an area estimate of 0.01 mm^2.**

***Keywords*— PUF, fingerprint, counterfeit IC, counterfeit IC countermeasure, authentication**

I. Introduction

Counterfeit electronic components and systems in the global supply chain have become an insidious problem in the semiconductor industry for the past several years [1]. The presence of counterfeit parts throughout the electronics industry is now a reality with counterfeit parts surfacing in industrial control systems, personal electronics, computer and communication systems, transportation and automobiles, avionics, military systems, financial systems, and medical devices. Aside from the legal issues surrounding counterfeiting, the performance and reliability of counterfeit devices is unpredictable. Failure of critical systems in areas such as medicine, military, and transportation can have dramatic and fatal consequences. Illicit parts are seen in various segments of the supply chain from simple low-level passive components to high-tech microprocessors. The counterfeit parts could be entirely fakes, relabeled inferior devices, or heavily used components that are removed from discarded used systems. These parts are often difficult to detect by visual inspection and often have measured electrical properties and characteristics that are not much different than those of legitimate parts making it difficult to detect them from standard non-destructive electrical testing.

The precise magnitude of the counterfeit problem is not well known, at least in part, because it is not easy to spot counterfeit components in the supply chain. Some sources report that annual global revenue loss from reputable semiconductor manufacturers due to counterfeit sales is about $100 billion whereas other source suggest that it is around 1% of total semiconductor sales [1], [2]. Regardless of exactly how big the grey semiconductor market is, it is flourishing, it is reported to be growing, and is a threat to both producers and consumers.

Counterfeit parts are particularly prevalent in the segment of the supply chain that provides discontinued and/or obsolete semiconductors which are essential for maintaining legacy products and systems. Legacy systems in the military, in public transportation and infrastructure systems, and in some medical systems are widely used since these systems tend to have a very long service life [2].

For the past several years, numerous approaches have been proposed [2], [4]–[8] to protect new components from being jeopardized in the supply chain and to detect illegitimate semiconductor devices that have already been introduced into the supply chain. These approaches include hardware obfuscation and advanced Circuit and Intellectual Property (IP) authentication[3] strategies such as adding unique fingerprints, RFIDs, or cryptographic blocks. These types of solutions can solve the technical aspects of the counterfeit problem and can provide highly reliable and robust security against counterfeiting. Unfortunately, these solutions invariably come with the downside of additional circuitry, die area, bonding pads, development time, cost for testing and validation, and the expenses associated with developing and maintaining a planet-wide data authentication infrastructure. The major semiconductor manufacturers that feed the bulk of the semiconductor supply chain with Commercial Off The Shelf (COTs) parts have been slow to adopt these approaches to a significant level thereby allowing the illicit grey-market semiconductor components to pass through the supply chain into critical electronic systems. Whereas the semiconductor counterfeiters are motivated almost entirely by financial incentives, the lack of action by the COTs manufacturers to address the counterfeit IC problem is driven almost entirely by the belief that there is a financial counterincentive to address the problem. This delicate balance between incentives for the counterfeiters and the financial counterincentives for COTs manufacturers creates a fertile gap for low-reliability components to fill sockets in some of society's most critical systems. Closing this gap calls for clever solutions to combat this Hardware Intrinsic Security (HIS)[3] challenge.

This work focuses on reducing or eliminating the financial counterincentives faced by most major COTs manufacturers in the semiconductor industry. One particularly effective method of counterfeit mitigation for new parts is to associate each component with a unique ID or fingerprint as part of the manufacturing process and to track this fingerprint from the manufacturer to end user with a secure planet-wide database. One of the simplest and most cost effective solutions for creating this fingerprint is to use the random process variations [6] that naturally occur during the manufacture of electronic devices to create a unique fingerprint. Fingerprints (sometimes referred to as keys) based upon the natural random variations are often termed physically unclonable functions (PUFs) which, as their name applies, are physically unclonable [9]. A large number of different PUFs have been reported in the literature.

A major limitation of most existing PUFs is the additional resources required to implement these PUFs such as additional die area, additional pins, additional circuitry for reading out the fingerprint, and additional resources needed for maintaining a database for managing the key. An example of a PUF based authentication solution available in industry that is highly reliable is the ChipDNA PUF™ security technology recently introduced by Maxim Integrated [8]. This part claims to "provide an exponential increase in protection against the invasive and reverse engineering attacks" but requires a separate 6-pin IC package. Many existing PUFs are designed to be "strong PUFs" with many Challenge Response Pairs (CRP) that are extremely difficult to spoof but even most "weak PUFs" provide a much higher level of protection than is needed for thwarting counterfeiters.

The proposed PUF-based authentication used as a counterfeit countermeasure focuses on reducing area overhead, eliminating pin overhead, and reducing cost by integrating the PUF into the readout circuit itself. A standard approach for generating a single random bit in a PUF code is based upon a bit cell comprised of two inverters connected back to back to form a four-transistor (4T) memory cell. When power is applied, this memory cell will settle into one of two states. An array of n such cells will provide an n-bit PUF code which appears to be randomly generated from one integrated circuit to another but in which most bits for each individual integrated circuit will provide the same output each time power is applied. In addition to the four transistors needed for the two inverters, one or two additional transistors are typically needed to access the PUF code stored in these cells. Some additional readout circuitry may be needed as well if the PUF circuit is not a part of an existing SRAM block.

In this work, one unique random code per inverter rather than one unique random code per inverter pair is generated. This is achieved by reconfiguring the back to back inverters using a second inverter pairing approach thereby doubling the effective number of cells. The reconfiguration is done with the transistors that are used to access the cells during readout. This reduces the area for a given number of random bits by about a factor of 2. A number of these unit blocks are connected as a recirculating dynamic shift register to serially read out the random PUF code. The same transistors that are used to access the PUF code are used to form the shift register. This feature helps to further reduce the area of a PUF since the readout is embedded in the PUF array. The PUF code is serially directed to the output making it particularly easy to read the PUF output code. With this approach, a compact layout which is small enough to be put under a bonding pad can be used to generate a PUF code that is long enough for authentication in counterfeit protection applications. In layouts where no functional circuitry is placed under the bonding pads, there is no area overhead for the authentication circuit if the area under the bonding pad is used for the PUF circuit.

The proposed circuit is designed to operate at a supply voltage at about half the nominal supply voltage ($V_{DD,n}/2$) and is isolated from the main IC when operated at V_{DD}. Thus the PUF circuit doesn't interfere with the normal operation of the main IC. Since the supply voltage for the proposed circuit is the supply voltage of the main IC itself, there is no need for additional supply pins. The ground and output pins are also shared with the main IC, since they operate at different supply voltage values, thus completely overcoming the need for additional pins.

Implicit in this work is the assumption that a database is 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. Some have proposed using a blockchain approach for building this database.

II. Related Work

Since the beginning of the twenty first century, there has been significant interest in the concept of using the manufacturing variability attributable to inherent random process variations and the associated device mismatch characteristics of nominally identical structures to build practical fingerprint circuits for device authentication. This variability can be used to produce random variations in electrical characteristics of simple circuits such as random variations in the gate delays, random trip points of logic gates, random variations in the resistance of segments in the power grid of a chip [6], random variations in the capacitance of separate segments of interconnects in an IC, and random variations in the oscillation frequency of ring oscillators. This fingerprint proposed in this work is based dominantly on the combined effects of random variations in device model parameters such as threshold voltage and mobility, and to a smaller extent based upon random variations in device dimensions.

III. Low entry barrier authentication circuit

A. Overview

The basic bit cell of the proposed PUF-based fingerprint circuit is shown in Fig. 1. When the switches with even index k are closed and odd index k are open, inverters with even index k are paired together with inverters with odd index k-1 to form 4T memory cells. When power is applied to the inverters, a random bit is generated at the output of the inverters with even index INL_k. This will be designated as Mode 1 operation. And when switches with odd index k are closed and those with even index k are open, inverters with even index k are paired together with inverters with odd index k+1 to form 4T memory cells. When power is applied to the inverters, a random bit is generated at the output of the inverters with even index of INL_k. This will be designated as Mode 2 operation.

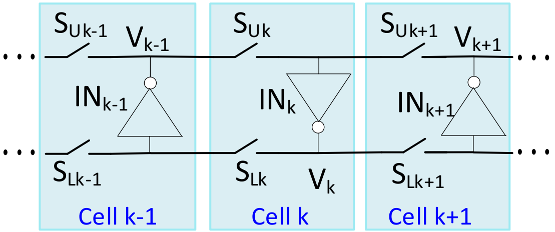

Fig. 1 Basic Bit Cell of Proposed PUF

Minimum sized transistors are used in the inverters of the bit cells to enhance the mismatch characteristics thereby reducing the number of "soft" bits, bits that may not always express the same value when power is applied to the inverters due to noise, temperature variations, or aging. The switches can also be made with single transistors. In either Mode 1 or Mode 2, after the inverter outputs are loaded with the random bit codes, the circuit is configured as a dynamic circulating shift register by alternately clocking all upper switches that have an even index and all lower switches that have an odd index.

The operation of the PUF circuit in Mode 1 and Mode 2 is depicted in Fig. 2 for the first six inverters where the switches have been suppressed in the figure. This shows the switches configured with solid lines to acquire the random codes and the shift-path when configured as a dynamic shift register. Note that the acquire mode is often termed the "static hold" mode in a dynamic shift register.

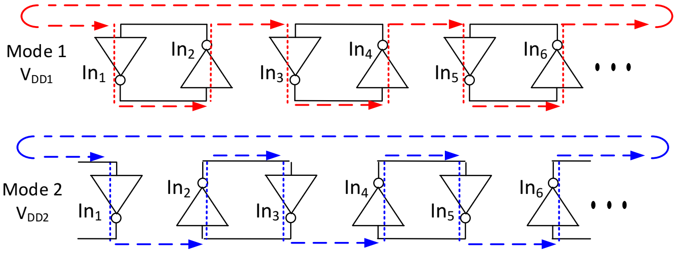

Fig. 2. PUF/Dynamic Shift Register

Even in rather large feature processes, the area required with this approach to generate enough random bits for use in chip authentication circuit can be ssufficiently small that the authentication circuit can be placed under a bonding pad [11-13]. Additional details about the implementation are discussed in the following section.

B. *Proposed PUF Circuit*

The block diagram of the proposed PUF circuit is shown in Fig. 3. Four pins V_{DD1}, V_{DD2}, Gnd, and Output are common between the main IC and the PUF circuit. Mode 1 and Mode 2 are controlled by the supply pins V_{DD1} and V_{DD2} respectively and the corresponding clocking sequence of the dynamic shift registers. To avoid interference with the operation of the main circuit, the PUF circuit is designed so that the devices in the PUF circuit operate in the weak inversion region and so that the PUF circuit disconnects itself from the supply pins when the normal operating voltages of the main circuit are applied to the supply pins. When the supply voltage V_{DD1} is set at approximately half of the nominal supply voltage and V_{DD2}=0V, the PUF circuit will be operating in Mode 1 and the output can be obtained by simply connecting one pin of the circulating shift register to an output pin thus presenting the fingerprint code serially at the output pin. Similarly, when V_{DD2} is set at approximately half of the nominal supply voltage and V_{DD1}=0V, the PUF circuit operates in Mode 2. And, as in Mode 1, the output can be read at the same output node when the dynamic shift register is clocked. The random outputs in Mode 1 are distinct from the random output in Mode 2.

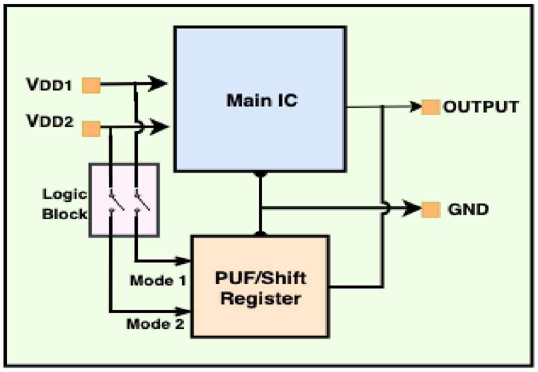

Fig. 3. Block diagram of the proposed PUF

In both modes, after applying the appropriate supply voltages and after the outputs which comprise the fingerprints have stabilized, the shift register is clocked causing the fingerprint code to circulate in the shift register. The merging of the PUF generator with the shift register to eliminate the need for more circuit complexity should be apparent from the schematic shown in Fig. 2.

A frame header or comma string is used to frame the random PUF code generated in the shift register. The comma string is generated by intentionally skewing the size of the devices in the appropriate 4T bit cells to force the bit-code to a predetermined value. These 4T frame header cells are also incorporated into the same shift register that is used to generate the random fingerprint bits. Skewing is achieved by using either a strong PMOS or a strong NMOS transistor in the appropriate inverter to intentionally produce a '1' and '0' respectively as shown in Fig. 4.

Though the two circulating outputs can be identified using the comma bits, without a synchronization signal at the output it will be difficult to determine where to sample the output. A standard external Clock and Data Recovery (CDR) circuit will be used to read the serial output string and to identify the header.

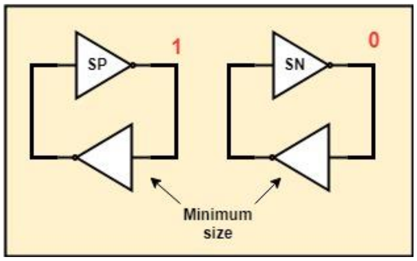

Fig. 4. Skewed inverter for Comma bit generation

IV. Results and Discussion

An 80-bit PUF circuit was designed in a UMC 65nm process. The circuit generates a 64-bit random code along with a 16 bit comma sequence. The estimated area of this circuit is 0.01mm^2 which is comparable to the area of a bonding pad.

Three samples from the Monte Carlo simulations of the PUF cells for Mode 1 and Mode 2 are shown in Fig. 5 and Fig. 6 respectively. For illustrative purposes, the results are shown for 20 bits of the code (10 bits in each mode) with 2 comma bits for Mode 1 and 3 comma bits for Mode 2. Since this is in a circular shift register, the codes keep repeating every 10 clock cycles in each mode. Fig. 5 shows the simulation result for the 10 bits in Mode 1 when V_{DD1} is set at 0.6V. The comma bits for Mode 1 are at PUF cell locations 2 and 7 with codes '1' and '1' respectively. Fig. 6 shows the simulation result for the 10 bits for Mode 2 when V_{DD2} is at 0.6V. The comma bits for mode 2 are located at PUF cell positions 1, 2 and 6 with codes '1', '0' and '0' respectively. Hence in this example, Mode 1 generates 8 random PUF code bits and Mode 2 generates 7 random PUF code bits respectively. The randomness of these codes for the 64 random bits in the 80-bit PUF circuit has been validated with Monte Carlo simulations.

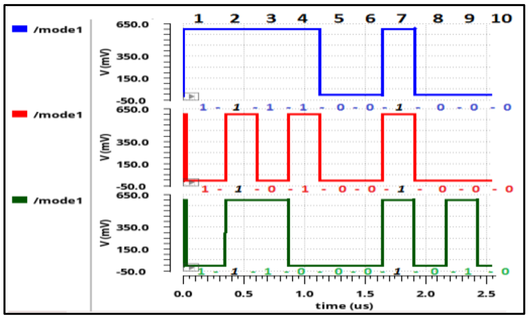

Fig. 5. Monte Carlo simulation result for Mode 1

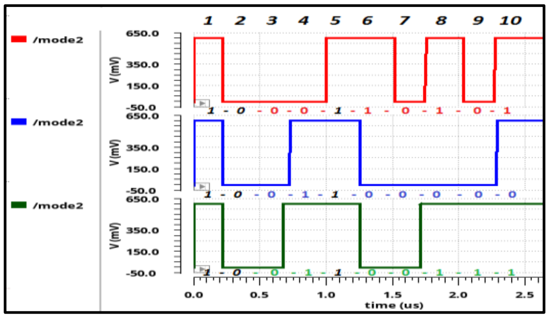

Fig. 6. Monte Carlo simulation result for Mode 2

V. Conclusion

A simple counterfeit countermeasure using a PUF-based fingerprint embedded in a serial readout circuit that reduces some of the major authentication overhead concerns of semiconductor manufacturers has been proposed. It requires minimal area overhead, no pin overhead, and has no impact on the operation of the main integrated circuit. This approach should help reduce the financial incentives for counterfeiters to push counterfeit parts into the semiconductor supply chain and should also help reduce the perceived financial counterincentives of COTs manufacturers to incorporate fingerprint authentication in their products.

Acknowledgment

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 and S. Tiku, "Bogus: electronic manufacturing and consumers confront a rising tide of counterfeit electronics," IEEE Spectrum, vol. 43, no. 5, pp. 37–46, May 2006.

[2] U. Guin, K. Huang, D. DiMase, J. M. Carulli, M. Tehranipoor, and Y. Makris, "Counterfeit Integrated Circuits: A Rising Threat in the Global Semiconductor Supply Chain," Proceedings of the IEEE, vol. 102, no. 8, pp. 1207–1228, Aug. 2014.

[3] Institute of Electrical and Electronics Engineers, Ed., 2013 IEEE International Test Conference (ITC 2013): Anaheim, California, USA, 6 - 13 [i.e. 10 - 12] September 2013 ; [at ITC Test Week 2013 ; test week: September 8 - 13, conference & exhibition: September 10 - 12]. Piscataway, NJ: IEEE, 2013.

[4] K. Lofstrom, W. R. Daasch, and D. Taylor, "IC identification circuit using device mismatch," IEEE International Solid-State Circuits Conference, pp. 372–373, Feb. 2000.

[5] B. Gassend, D. Clarke, M. van Dijk, and S. Devadas, "Silicon Physical Random Functions," 9th ACM Conference on Computer and Communications Security, New York, NY, USA, pp. 148–160, 2002.

[6] J. W. Lee, B. Gassend, G. E. Suh, M. van Dijk, and S. Devadas, "Extracting secret keys from integrated circuits," IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol. 13, no. 10, pp. 1200–1205, Oct. 2005.

[7] D. E. Holcomb, W. P. Burleson, and K. Fu, "Power-Up SRAM State as an Identifying Fingerprint and Source of True Random Numbers," IEEE Transactions on Computers, vol. 58, no. 9, pp. 1198–1210, Sep. 2009.

[8] "ChipDNA Embedded Security PUF Technology - Maxim." [Online]. Available: https://www.maximintegrated.com/en/design/partners-and-technology/design-technology/chipdna-puf-technology.html. [Accessed: 28-Apr-2019].

[9] C. Herder, M.-D. Yu, F. Koushanfar, and S. Devadas, "Physical Unclonable Functions and Applications: A Tutorial," Proc. IEEE, vol. 102, no. 8, pp. 1126–1141, Aug. 2014.

[10] "A 1.6pJ/bit 96% Stable Chip-ID Generating Circuit using Process Variations - IEEE Conference Publication." [Online]. Available:https://ieeexplore.ieee.org/abstract/document/4242437 [Accessed: 28-Apr-2019].

[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.

[13] P. Ebenezer, D. Chen, R. Geiger, "Counterfeit IC Countermeasure with 4T Cell Based Authentication Circuit", Government Microcircuit Applications and Critical Technology Conference, (GOMAC-Tech), 2019.