Hardware-Based Anti-Counterfeiting Techniques for Safeguarding Supply Chain Integrity

Md Tanvir Arafin
ECE Department,
University of Maryland
College Park, Maryland USA
marafin@umd.edu

Andrew Stanley
CISO,
Philips
Andover, Massachusetts, USA
andrew.stanley@philips.com

Praveen Sharma
CISO,
Philips
Andover, Massachusetts, USA
praveen.sharma@philips.com

***Abstract*— Counterfeit integrated circuits (ICs) and systems have emerged as a menace to the supply chain of electronic goods and products. Simple physical inspection for counterfeit detection and basic intellectual property (IP) laws and protection measures are becoming ineffective against advanced reverse engineering and counterfeiting practices. As a result, hardware security based techniques have emerged as promising solutions for combating against counterfeiting, reverse engineering and IP theft. However, these solutions have their own merits and shortcomings and these options need to be carefully studied and compared before implementing in a design. Therefore, in this work, we present a comparative overview of available hardware security solutions to fight against IC counterfeiting. We provide a detailed contrast of the techniques in terms of integration effort, deployability and security matrices that would assist a system designer to adopt any one of these security measures for safeguarding the supply chain of his product against counterfeiting and IP theft.**

Keywords—IC counterfeiting; IP protection; Hardware Metering; Circuit Obfuscation; PUF; Supply Chain Management.

I. INTRODUCTION

In recent years, hardware counterfeiting of enterprise products is increasingly becoming one of the fastest growing criminal ventures [1]. The electronic design and manufacturing industries are vulnerable to these counterfeiting attacks. Product counterfeiting ranges from simple relabeling attacks to extensive reverse engineering and fabrication ventures. Not only the products fall victim of such criminal activities, but also that product subcomponents—major system components and critical integrated circuits (ICs)—in the system are reverse engineered and counterfeited. As a result, IC counterfeiting is becoming a serious concern for supply-chain integrity, a menace for the security of a business entity and a threat to public health, safety, and national security. In response to these threats, active research is being pursued designing and advancing current electronic manufacturing and distribution process for preventing IC counterfeiting and reverse engineering efforts.

Counterfeit ICs have the potential to become pervasive in critical electronic devices. They have found their ways in medical devices such as Automated External Defibrillator (AEDs) and intravenous drip machines, critical infrastructures such as braking systems in high-speed trains and power supply in airport landing lights, and even in radiation detectors and nuclear submarines [2]. Progress in an integrated circuit (IC) design and fabrication technology has reduced the cost of manufacturing and reverse engineering tremendously. As a result, a lucrative business model of IC counterfeiting emerges. This results in a billion dollar electronic circuit-counterfeiting business around the globe.

A few areas of impact of illegally manufactured and distributed ICs are as following:

a. *Loss in revenue, intellectual property, and brand recognition*: Counterfeited ICs usually replace a known and trusted manufacturer, which can result in a tremendous loss in revenues for the legitimate manufacturer. Furthermore, counterfeiting is an attack on the brand recognition and reputation of the business, and therefore, it can affect the brand in the market competition in the long run. In 2011, Semiconductor Industry association (SIA) estimated that $7.5 billion dollar cost incurred per year to the electronic industries due to IC counterfeiting [2].

b. *Loss of reliabilities in a critical system's functional capability*: Counterfeit components can find their way into the critical system such as military equipment, financial infrastructure, electronic grid, transportation systems, healthcare products *etc*. This has the potential to create reliability and security issues for such systems. Therefore, for components in such systems, runtime detection of authenticity should be in practiced.

c. *Malware injection*: One of the common by-products of counterfeit electronic goods is the proliferation of malware in the system containing such electronic products. For example, malicious executables are commonly reported in forged memory components [2].

d. *Hardware Trojan insertion*: Since illegal manufacturers can reverse engineer or alter partial/complete hardware components, they can easily insert hardware Trojans. Such malicious alteration can create targeted attacks on a system at some future time or could leak critical information and cryptographic keys to an adversary [5].

From a supply-chain perspective, counterfeit ICs can enter into the chain at different points as shown in Figure 01. Therefore, a rigorous supply chain management is required for combating against fake electronic circuits. One of the simplest solutions to this problem is incorporating certification of authenticity (CoA) measures with the product and the electronic components. However, maintaining rigorous supply-

chain management effort can be impossible due to the human factor. Since we are dealing with hardware counterfeiting, software-based authentication is somewhat inadequate If the counterfeit product is capable of executing similar systems as the original one, then it is difficult to differentiate two of them using software-based solutions such as functional testing. Therefore, in this work we have examined hardware security solutions for anti-counterfeiting techniques.

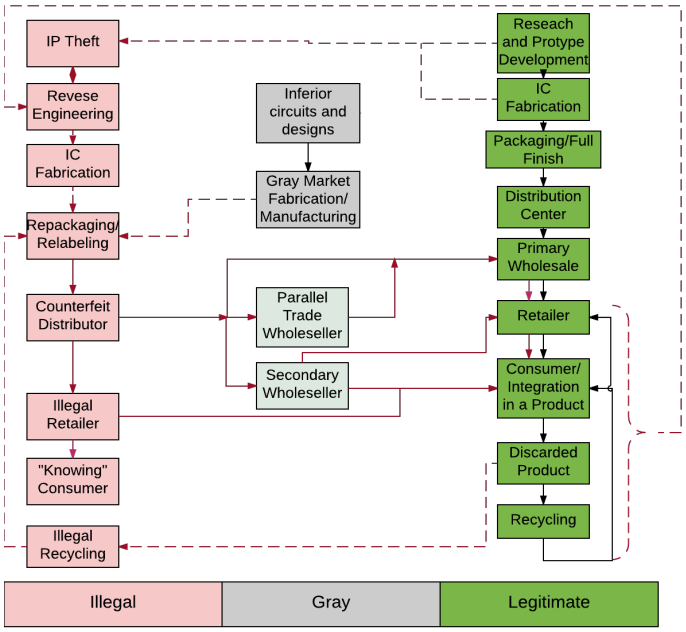


Figure 01: How counterfeit ICs enter into the IC supply chain. The green boxes represent legitimate steps in the life-cycle of an IC, the grayish boxes represent the gray market players that affect the supply chain and the red boxes represent the life-cycle of a counterfeit IC. The solid red lines present the paths that an illegal design uses to infiltrate the supply chain and the dashed lines provide ways that a legitimate design and supply process helps sustaining an illegal counterfeiting enterprise. Similar designs can be found in [4].

II. Counterfeiting Techniques

The prevailing belief about counterfeiting is that it is usually done by adversaries with limited manufacturing capacity and their business model is notional. This general notion can explain most of the common practices in counterfeiting such as - repackaging and reselling an inferior product as its superior counterpart or recycling an older chip and relabeling it as a new one. Such techniques obviously do not require advanced manufacturing capabilities. However, this model relies on the supply of cheaper alternatives of a given product in the market for sustaining a profit margin. This exposes a gray market, which constitutes the supplier of these substandard products and the counterfeiters. The manufacturers of these low-grade electronic products actually have a decent capacity of reverse engineering and manufacturing a given design. From a security perspective, this creates a more serious concern because such manufacturers can insert hardware or software Trojans in the design, which can find its way inside a secure system. Therefore, we can categorize the IC counterfeiting techniques into three common categories:

A. Relabeling and repackaging

This is the simplest attack on the supply chain of a given electronic product. Inferior, defective or overproduced ICs are relabeled and repacked for monetary gain. For example, in recent years there have been an increased number of relabeling attacks on memory components: such as flash drives and SD cards used in the commodity electronics. There are two ways these attacks are being performed. Firstly, a lower capacity memory component is relabeled as a higher capacity one. In such cases, there are reports of malicious software and hardware controllers, which misrepresent the capacity of the component to the system and erases data automatically to give the illusion of larger capacity. The second type of counterfeiting involves using low-grade component repackaged as some higher grade one. For example, an SD card without ECC is repackaged as the one with ECC.

B. Reverse engineering and illegal manufacturing

To maintain a supply of low-grade parts and ICs, manufacturing is essential. Such manufacturing involves stealing intellectual properties by reverse engineering a given electronic product. With the advancement of probing and testing technologies, reverse engineering has become more accessible than before. Furthermore, the manufacturing cost for electronic components is getting cheaper. As a result, reverse engineering simpler IC-designs and components and manufacturing them for gaining a market share is becoming a lucrative business model for counterfeiters and gray market entrepreneurs.

C. Illegal Recycling

Another simple method of counterfeiting is recycling the older chips. This weakness comes from the consumer side of the supply chain. Usually, at the end of a product lifecycle, consumers discard the product with most of the components functioning. Unregulated disposal of aged products has led to the business of recycling older ICs and selling them as a newer one. Since the IC primarily originates from a trusted source, recycling can retain system security, however, this practice creates serious reliability concern for a given system.

III. Hardware Security Measures For Safeguarding Supply Chain

As discussed in the previous sections, human factors can weaken the integrity of the supply chain of a given chip design. Law enforcement and subsequent legal actions can address IC counterfeiting problems; however, legal actions are inherently an after-the-fact measure. Therefore, necessary prevention techniques must be adopted to stop the proliferation of the counterfeited IC before or during it attacks the supply chain.

Physical inspection can be a simple solution for counterfeit detection. However, with the increased capabilities and cheaper printing and packaging techniques, it will become increasingly difficult to detect a counterfeit IC. Therefore, in this work we compare hardware security based technique that provides better solution against counterfeiting.

Hardware security measures can provide two key benefits: It can

1. Provide dynamic detection of counterfeited ICs and prevent further damages in the system

2. Help the legal authorities to find the details on the supply-chain of the illegal goods and provides a way of legally pursue an IP infringement case.

However, introducing theses security measures incurs the cost and therefore, a designer must weigh the options carefully to better suit the target product and the nature of counterfeiting.

In this work, we have measured different existing hardware based anti-counterfeiting solutions in terms of three different parameters:

A. Integration Effort

E1. Design overhead (Power/Area/Cost)

E2. Design Effort and cost of intellectual property

E3. Effect on yield and lead-time

E4. Maturity of the technique

B. Deployability

D1. Deployment cost per user

D2. Maintenance cost per user

D3. Cost of recycling

D4. Ease of Use/ Efficiency of Use

D5. Ease of testing

D6. Backwards Compatibility

C. Security

S1. Resilient to testing attacks

S2. Resilient to Reverse engineering

S3. Probability of success of exploitation

S4. Ease of counterfeit detection

S5. Ease of recovery from loss

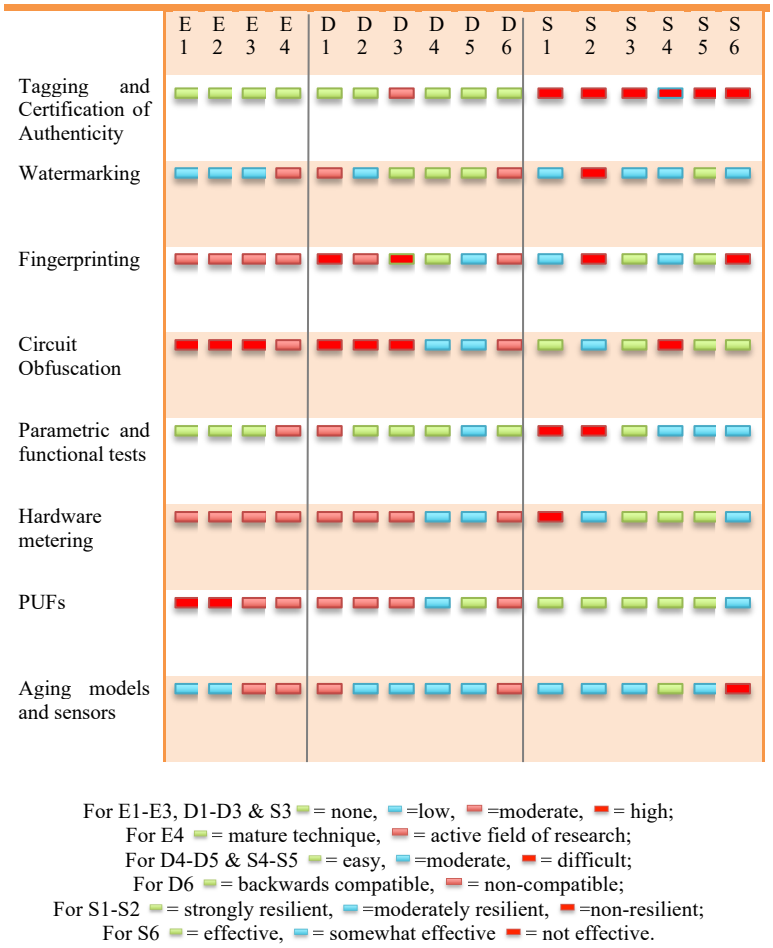
S6. Effectiveness in IP protection

One of the simplest solutions is tagging a serial number on the electronic components and keeps a record for the valid tags. We measure all of the hardware security solutions against this simple measure of counterfeit protection. It should be noted that application of any one of these technologies would depend on the nature and spread of counterfeiting problem and the product. Therefore, we do not rank the technologies by their average merit; instead, we present their effectiveness in different scenarios, which would give a designer a practical overview of which technique to incorporate into her design. A graphical representation of this comparison is given in Table I.

T1. *Tagging and Certification of Authenticity*: The most prevalent form of anti-counterfeiting technique is tagging the packaging of an authentic chip with a unique serial number and keeping a database of all authentic chips. A certificate of authenticity can be provided for all of the chips carrying an authentic serial or identification tag. In terms of implementation, this approach does not require additional design overhead in terms of power or the area budget of the chip. This technique is easily deployable too since the only cost of deployment is in maintaining the database of the authentic product. However, this approach does not provide any security against reverse engineering and IP theft. Furthermore, a counterfeiter can easily to copy the tag and re-label a fake IC. Therefore, this method does not fare well in terms of security.

T2. *Watermarking*: To identify the sources of IP theft, hardware based watermarking techniques can be used. Watermarking adds signatures in the circuit design, which is unique for a given instance of a bulk production. Watermarks are added on a given IP to create multiple version of the IP for distribution for manufacturing at a different time or at different facilities. Hardware watermarks do not change the functionality of the IC, rather it adds some information about the distribution of a given IP [6]. In an event of an IP-theft, the available counterfeited ICs can be examined to reveal the source of the manufacturer from which the IP was stolen. Watermarking is relatively easy to implement and deploy, however, it provides limited assistance in counterfeit detection and safeguarding the supply chain.

TABLE I: COMPARISON OF DIFFERENT ANTI-COUNTERFEITING TECHNIQUES



T3. *Fingerprinting*: While watermarking creates a unique signature for each batch of fabricated device, hardware fingerprints are unique for each device. These fingerprints can be added by incorporating unique keys in each ICs, or

by exploiting the fabrication variation. Hardware fingerprinting techniques are based on the idea that each device is capable of creating unique fingerprints due to the incorporation of fingerprint generators, combinational logic locks [8] or the fabrication variation of micro and nanoelectronic circuitry. Since it is difficult for counterfeited ICs to possess the same fingerprints as an authentic one, this technique is successful in counterfeit detection and hardware Trojan detection [7]. However, adding unique keys, as fingerprints, on each IC during manufacturing can be prohibitively expensive. PUF based fingerprinting provides a better alternative as discussed later.

T4.*Circuit obfuscatio*n: Circuit obfuscation and IC camouflaging techniques such as the ones discussed in [9-11] tries to obfuscate the functional properties of a given IC by adding additional logical blocks in the design. An obfuscated circuit essentially hides the IP and thus protects the key design ideas from being stolen. However, circuit obfuscation techniques usually require a key for proper operation and the security of the key can dictate the success of IP protection.

T5.*Parametric and Functional tests*: Parametric and functional tests provide simple but effective techniques for detecting a counterfeit integrated circuit. Parametric tests constitute a comparison of a suspected chip with a golden chip using different measurement techniques such as leakage current measurement, power consumption measurement, threshold current detection, propagation delay testing, set-up time testing *etc.* [12,13]. Although parametric tests are time efficient, they suffer from the effects of process variation, IC usage and aging. Functional tests verify the functionality of the chip, and therefore, do not perform well if the counterfeit product performs all of the functionality as the original. At a given facility these tests are easy to perform and can effectively support all different generations of a given IC.

T6.*Hardware metering*: Active or passive hardware metering provides a secure way of tracking the usage of a manufactured chip. Passive metering is similar to fingerprinting; however, the use of a specific IC is also is monitored and documented [14]. Active metering can access, lock or unlock a metered IC for restraining its usage [15]. Although hardware metering can be a preferred solution in terms of security, the implementation cost for such design needs to be carefully considered.

T7.*Physically Unclonable Functions (PUFs)*: PUFs can provide strong challenge-response based authentication mechanisms for authentic ICs. Since the challenge-response pairs are derived from the unique physical fingerprint of a given device, it is physically impossible to replicate the same responses. As a result, PUFs can provide great security benefits against IC counterfeiting; however, PUFs can claim significant implementation and deployment costs,

T8.*Aging models and sensors*: Finally aging models and sensor such as the ones discussed in [17] can be used for detecting recycled counterfeit ICs

IV. CONCLUSIONS

Although there exist several anti-counterfeiting techniques, the implementations of such techniques are not widely practiced yet. The key reasons for this scenario can be associated with inertia in design and development, cost of maintaining an anti-counterfeit program, lack of technological advancement for testing design and system integrity during runtime, cost of recycling and regulated disposal, cost of maintaining the database of failed and replaced parts, compliance with regulations and an overall apathy towards counterfeiting. Finally, we provide the following recommendations to business organizations for addressing the IC-counterfeiting problem:

a. Implement anti-counterfeiting measures which is preferable;

b. Secure sensitive data and hardware first, consider safe and fault tolerant electrical designs for critical systems;

c. Raise awareness about the problems and newer designs should use authentication techniques to reject counterfeited ICs;

d. Legacy hardware and components in critical systems and infrastructure must be maintained, regulated and recycled systematically.

ACKNOWLEDGMENT

This work is supported by Philips Internship Program.

REFERENCES

[1] "2015 Situation Report on Counterfeiting in the European Union", available at https://euipo.europa.eu/ohimportal/documents

[2] "Winning the Battle Against Counterfeit Semiconductor Products", available at http://www.semiconductors.org/clientuploads/Anti-Counterfeiting/SIA%20Anti-Counterfeiting%20Whitepaper.pdf

[3] "Obama to Sign Bill Combating Counterfeit Chips", available at http://www.eetimes.com/document.asp?doc_id=1328931

[4] "Supply Chain Toolkit 2014", available at http://www.ipo.gov.uk/ipctoolkit.pdf.

[5] M. Tehranipoor, and F. Koushanfar. "A survey of hardware Trojan taxonomy and detection." *IEEE Design and Test of Computers* 27.1 (2010): 10-25.

[6] G. Qu and M. Potkonjak, "Intellectual Property Protection in VLSI Design," Kluwer Academic Publisher, 2003.

[7] D. Agrawal, et al. "Trojan detection using IC fingerprinting." *2007 IEEE Symposium on Security and Privacy (SP'07)*. IEEE, 2007.

[8] J. A., Roy, F. Koushanfar, and I. L. Markov. "EPIC: Ending piracy of integrated circuits." *Proceedings of the conference on Design, automation, and test in Europe*. ACM, 2008.

[9] J. Rajendran, et al. "Security analysis of logic obfuscation." *Proceedings of the 49th Annual Design Automation Conference*. ACM, 2012.

[10] J. Rajendran, et al. "Security analysis of integrated circuit camouflaging." *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*. ACM, 2013.

[11] J. Zhang, "A practical logic obfuscation technique for hardware security." *IEEE Transactions on Very Large Scale Integration (VLSI) Systems* 24.3 (2016): 1193-1197.

[12] G.F. Nelson, W. F. Boggs, "Parametric tests meet the challenge of high-density ICs." Electronics 48(5):108–111, 1975

[13] K. Lofstrom, W. R. Daasch, and D. Taylor. "IC identification circuit using device mismatch." *Solid-State Circuits Conference, 2000. Digest of Technical Papers. ISSCC. 2000 IEEE International*. IEEE, 2000.

[14] F. Koushanfar, G. Qu, and M. Potkonjak, "Intellectual property metering," IH, pp. 81–95, 2001.

[15] Y. Alkabani and F. Koushanfar. "Active Hardware Metering for Intellectual Property Protection and Security" USENIX Security, pp. 291–306, 2007.

[16] B. Gassend et al., "Silicon physical random functions," ACM CCS, pp. 148–160, 2002.

[17] K.K. Kim, W. Wang, and K. Choi, "On-chip aging sensor circuits for reliable nanometer MOSFET digital circuits," T-CAS-II, vol.57, no. 10, pp.798–802,2010