Anti-Counterfeit Techniques: From Design to Resign

Ujjwal Guin, Domenic Forte, and Mohammad Tehranipoor
CHASE Center, University of Connecticut
{ujjwal, forte, tehrani}@engr.uconn.edu

***Abstract*—The emerging threat of counterfeit electronic components has become a major challenge over the past decade. To address this growing concern, a suite of tests for the detection of such parts has been created. However, due to the large test time and cost, it is fairly difficult to implement them. Moreover, the presence of different types of counterfeits in the supply chain – recycled, remarked, overproduced, out-of-spec/defective, cloned, forged documentation, and tampered – makes the detection even more challenging. In this paper, we present a detailed taxonomy of counterfeit types to analyze the vulnerabilities in the electronic component supply chain. We then present the state of knowledge on anti-counterfeit technologies to help prevent counterfeit components from ever entering into the supply chain and to provide capabilities for easy detection.**

I. Counterfeit ICs: The Problem

Counterfeiting of integrated circuits has become a major challenge due to deficiencies in the existing test solutions and lack of low-cost and effective avoidance mechanisms in place. Over the past couple of years, numerous reports [1] have pointed to the counterfeiting issues in the US electronics component supply chain. A Senate Armed Services public hearing on this issue and the later report clearly identified this as a major issue to address because of its significant impact on system reliability and security [2], [3]. As the complexity of the electronic systems and integrated circuits increased significantly over the past few decades, they are mostly fabricated and assembled globally to reduce the production cost. For example, large foundries located offshore can offer lower prices to the design house. This globalization has led to an illicit market willing to undercut the competition with counterfeit and fake parts. If these parts end up in critical applications such as defense, aerospace, or medical, the results could be catastrophic [4].

The identification of counterfeit components in the electronic component supply chain, are broadly classified into two categories – detection tests and avoidance measures. The detection tests use state-of-the-art equipment (X-ray, SEM, SAM, etc.) to detect such parts already in the supply chain whereas the avoidance measures add extra hardware in the circuit to detect counterfeit parts without applying detection tests. The detection tests, recommended by [5] [6] have several challenges including excessive test time and cost. In [7], path-delay fingerprinting was proposed for detecting recycled ICs based on prior usage in the field as their path delay distribution changes. In [8], a statistical approach was presented to distinguish recycled counterfeit ICs by using a one-class support vector machine. Both these techniques require large number of genuine samples to train the model that may not be practical for the components, already in market. In this paper, our focus is to discuss the effectiveness of such measures for counterfeit avoidance for the entire spectrum of counterfeit types and supply chain vulnerabilities.

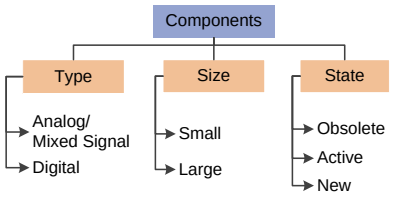

Figure 1. Taxonomy of component types.

Different types of components (shown in Figure 1) can significantly impact the implementation of avoidance measures in the circuit. Components can be classified by their type, size and "state". The descriptions for the type and size are self-explanatory. We categorize state into three distinct types – obsolete, active, and new. Obsolete refers to components which are no longer manufactured by original component manufacturers (OCM) as they may switch to newer designs to improve performance, reliability, and/or manufacturing cost. These components are only be available through OCM authorized or independent distributors of electronic components. Active components are still being manufactured by OCMs, but their designs cannot be changed because of – (i) the extra cost of developing new masks and (ii) performance and reliability concerns. New components are very flexible in implementing avoidance measures as they are still in the design phase where the OCM can – (i) validate the performance and reliability parameters and (ii) modify masks.

The avoidance of counterfeit components is very challenging, partly because there is such a wide variety of counterfeit types, component types, and supply chain vulnerabilities. In this paper, we will highlight the following:

(i) Taxonomy for counterfeit types: The development of taxonomy for the counterfeit components is one of the major contributions of this paper. It is utmost importance to understand various types of counterfeits impacting supply chain in order to develop appropriate avoidance measures.

(ii) Supply chain vulnerabilities: The analysis of electronic supply chain vulnerabilities reveals how different counterfeit components enter into it. By identifying proper measures at different stages, it would be much easier to develop anti-counterfeit measures.

(iii) Taxonomy for existing counterfeit avoidance measures: Such as taxonomy helps us to understand our current capabilities for avoiding counterfeit parts.

(iv) Challenges of counterfeit avoidance measures: The limitations and implementation challenges for counterfeit avoidance are presented. We clearly identify gaps that must be addressed in the near future.

The rest of the paper is organized as follows. In Section II, we will describe different types of counterfeits, their impact, and how they enter the supply chain. The existing counterfeit avoidance techniques will be presented in Section III. In Section IV, we will then discuss challenges and limitations of current counterfeit avoidance technologies. We will conclude the paper in Section V.

II. Electronic Component Supply Chain Vulnerabilities

A. Counterfeit Types

A counterfeit component (i) is an unauthorized copy; (ii) does not conform to original OCM design, model, and/or performance standards; (iii) is not produced by the OCM or is produced by unauthorized contractors; (iv) is an off-specification, defective, or used OCM product sold as "new" or working; or (v) has incorrect or false markings and/or documentation [9]. Based on the definition above and analyzing supply chain vulnerabilities, we classify the counterfeit types into seven distinct categories shown in Figure 2.

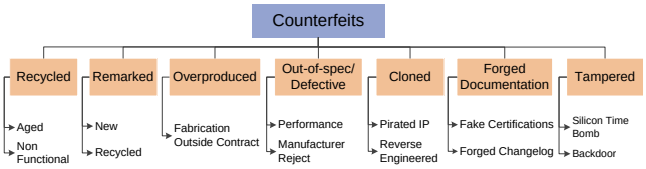

Figure 2. Taxonomy of counterfeit types.

• **Recycled**: It refers to an electronic component that is reclaimed/recovered from a system and then modified to be misrepresented as a new component of an OCM. Recycled parts may exhibit lower performance and shorter lifetime due to aging phenomena from their prior usage. Further, the reclaiming process (removal under a very high temperature, aggressive physical removal from boards, washing, sanding, repackaging, etc.) could damage the part(s), introduce latent defects, or make them completely non-functional due to exposure to extreme conditions in an uncontrolled environment. Such parts will be unreliable and render the systems that incorporate them also unreliable.

• **Remarked**: Most legitimate components contain markings on their packages that indicate manufacturer, trademark, part number, grade, lot code, etc. The remarking is accomplished by either chemically or physically removing the original marking, blacktopping (resurfacing) the surface to hide any scratches or imperfections that have been created, and then remarking the new surface. The primary incentive for remarking is to drive up a component's price on the open market or to make a dissimilar lot fraudulently appear homogeneous. For example, industrial or defense grade components are more valuable than commercial grade because of their superior durability and performance. However, remarked commercial grade components sold as military grade will not be able to withstand the harsh conditions of their more durable counterparts.

• **Overproduced**: Due to globalization, design houses outsource their designs for fabrication and packaging to companies all around the world, mainly to reduce the manufacturing cost. Overproduction occurs when foundries and packaging companies sell components outside of contract with the design house (component's intellectual property (IP) owner). Aside from the loss in profits for the IP owner overproduced ICs may pose serious reliability threats since they are often not subjected to the same rigorous testing as authentic parts and may not meet the manufacturer's standard flow requirements.

• **Out-of-Spec/Defective**: A part is considered defective if it produces an incorrect response to post-manufacturing tests. These parts should be destroyed, downgraded, or otherwise properly disposed of. However, if they instead are sold on the open markets, either knowingly by an untrusted entity or by a third party who has stolen them, there will be an unknown increase in risk of failure.

• **Cloned**: Cloning is widely used by a range of adversaries/counterfeiters (from small entities to large organizations) to copy a design in order to eliminate the large development cost of a part. Cloning can be done in two ways by reverse engineering, and, by obtaining intellectual property (IP) illegally (also called IP theft). Cloning can also occur with unauthorized knowledge transfer from a person with access to the part design.

• **Forged Documentation**: The documentation shipped with a component contains information regarding specification, testing, Certificates of Conformance, Statement of Work, etc. By modifying or forging these documents, a component can be misrepresented and sold even if it is nonconforming or defective. It is often difficult to verify the authenticity of such documents because the archived information for older designs and older parts may not be available at the OCM. Legitimate documentation can also be copied and associated with parts from a lot not corresponding with the legitimate documentation.

• **Tampered**: Components that are tampered can have dangerous consequences for the systems that incorporate them. For example, tampered chips can act as silicon time bombs where their functionality is unexpectedly "killed" at a critical moment [10]. Tampered chips may also contain backdoors that give access to critical system functionality or leak secret information to an adversary. A detailed taxonomy for tampering with a device at the die level (i.e., hardware Trojan) can be found in [10].

B. Supply Chain Vulnerability

Typically an electronic component will go through a process as shown in Figure 3. This process includes design, fabrication, assembly, distribution, usage in the system, and finally end of life. The vulnerabilities associated with each step are discussed in more detail below.

• **Design**: The design implementation of large complex integrated circuits has evolved to a stage where it is extremely challenging to complete the entire design in-house. The flow

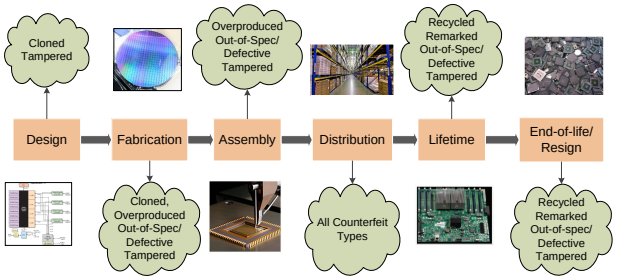

Figure 3. Electronic components supply chain vulnerabilities.

from RTL to GDSII is performed in many different places (even in different countries) mainly to reduce the development cost and design-to-market time. Design reuse has also become an integral part of SoC design. Hard IPs (layout level designs), firm IPs (designers can optimize codes with parameterized constraints), and soft IPs (synthesizable register-transfer level (RTL) designs) can be used for this purpose. Attacks on the design stage can be performed in the two following ways: (i) the counterfeiter can steal these IPs to create cloned components, (ii) the counterfeiter can tamper with codes to modify the functionality, create backdoors, etc.

• **Fabrication**: Today's integrated circuits are manufactured in fabrication facilities (fabs) located all around the world primarily to reduce the manufacturing cost. The design house contracts a foundry to fabricate their designs, discloses the details of their IPs, and also pays for mask-building costs based on their designs. The contract agreement between the foundry and design house is protected by IP rights [11]. However, this contract foundry business model (namely horizontal business model) creates a trust issue between the design house and foundry. The design house must trust foundry not to overproduce ICs or pirate IPs. An untrusted foundry can potentially (i) make extra/overproduced ICs, by hiding their yield, and selling those extra ICs in the open market, (ii) clone the design, and (iii) source defective and out-of-specification wafers to packaging companies to make finished parts.

• **Assembly**: After fabrication, the foundry send tested wafers to assembly to cut the wafers into dies, package the dies, and perform final tests before being shipped to the market. An untrusted assembly can (i) build overproduced ICs by hiding the yield information, (ii) sell the defective/out-of-specification ICs, and (iii) remark, forge, or upgrade a component's marking.

• **Distribution**: The tested ICs are sent either to the distributors or system integrators. The distributors sell those ICs in the market. There are two types of distributors – authorized and unauthorized – existing in the supply chain. The threat lies mostly from unauthorized distributors. There are several reports pointing to phony distributors potentially sourcing all seven types of counterfeit components in the supply chain.

• **System Integration/ Lifetime**: System integration is the process of assembling together all the components and subsystems into one complete system. An untrusted system integrator can potentially use all types of counterfeit components in their system. They can maximize the profit by using the cheap or tampered counterfeit components.

• **End-of-life/ Resign**: When electronics age or become outdated, they are typically retired/resigned and subsequently replaced. Proper disposal techniques are highly advised to extract precious metals and to prevent hazardous materials (lead, chromium, mercury, etc.) from harming the environment [12]. Yet, these techniques are largely ignored, resulting in a large amount of electronic waste or e-waste. For instance, in the United States, only 25% of electronic waste was properly recycled in 2009 [13]. That percentage might be lower for many other countries. A profitable business has grown out of reclaiming used components from this e-waste, remarking them, and then, re-inserting them into the supply chain as new components. According to current reports, these recycled and remarked components account for over 80% of the reported counterfeit parts in the supply chain [14] and represent a growing threat [15]. Also, in this stage the counterfeiter can potentially tamper used components for sabotage or malfunction.

III. Counterfeit Avoidance Measures

Different types of components, namely obsolete, active, and new impact differently for implementing counterfeit avoidance measures. New mechanisms can be put in place during the design of new chips that could help to prevent counterfeiting. As obsolete parts are no longer being manufactured, and active parts are being fabricated based on a previous design and developed masks, the focus should be on the implementation of avoidance measures at the package level. In the following, we will briefly discuss various counterfeit avoidance measures that can be implemented for new, active, and obsolete components. Figure 4 shows the taxonomy for such counterfeit avoidance measures. It is broadly classified into two major categories – chip ID and package ID.

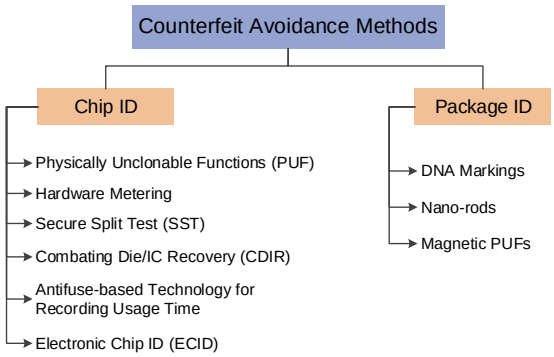

Figure 4. A taxonomy of counterfeit avoidance techniques.

A. Chip ID

Techniques to generate chip IDs are based on extracting unique features and parameters from a circuit to help uniquely identify each chip or embedding a unique ID into the chip during or after fabrication and test. The various available techniques are described below:

• **Physically Unclonable Functions**: PUFs [16] have received much attention from the hardware security and cryptography communities as a new approach for IC identification, authentication, and on-chip key generation. Silicon PUFs exploit inherent physical variations (process variations) that exist in modern integrated circuits. These variations are uncontrollable

and unpredictable, making PUFs suitable for IC identification and authentication. These variations can help generate a unique signature for each IC in a challenge-response form, which allows later identification of genuine ICs. In recent years various PUF architectures have been proposed. These include the arbiter PUF, the ring oscillator PUF, the SRAM PUF, and so on. PUFs can be used to detect cloned ICs as they generate unique IDs which result from randomness in the IC manufacturing process that cannot be controlled or cloned. These unique IDs of genuine ICs can be stored in a secured database for future comparison. Overproduced ICs can also be detected through this method, by searching the chip IDs under authentication in these secured databases. If no match is found, there is a high probability that the IC is not registered and is a member of an overproduced type.

• **Hardware Metering**: Hardware metering is a set of security protocols that enable the design house to achieve the post-fabrication control of the produced ICs to prevent overproduction. The design house can distinguish different ICs produced with the same masks, as hardware metering provides a unique way to tag each chip and/or its functionality [17] [18]. Hardware metering approaches can be either passive or active. Passive approaches uniquely identify each IC and register the IC using challenge-response pairs. Later, suspect ICs taken from the market are checked for proper registration. Active metering approaches, however, lock each IC until it is unlocked by the IP holder. This locking is done in a variety of ways, including: *(i)* initializing ICs to a locked state on power-up, *(ii)* combinational locking by, for instance, scattering XOR gates randomly throughout the design, and *(iii)* adding a finite-state machine (FSM) which is initially locked and can be unlocked only with the correct sequence of primary inputs.

• **Secure Split Test**: Due to the globalization of the semiconductor industry and the prohibitively high cost of creating foundries and assembly companies for packaging, test, and burn-in processes, foundries now often fabricate the wafers/dies, test them, and ship them to the assembly. The assembly then packages the dies, tests them, and ships the ICs to the market. The foundry/assembly, however, can ship defective, out-of-spec, or even overproduced chips to the black market, as described in Section II-A. Secure Split-Test (SST) secures the manufacturing test process to prevent counterfeits, allowing intellectual property (IP) owners to protect and meter their IPs [19]. SST introduces hardware components for cryptography and will block the correct functionality of an IC until it is activated by the IP owner. SST is designed to be resilient against different types of attacks to prevent the IC from being activated without IP owner's key. SST introduces the IP owner back into the manufacturing test process. SST is designed to prevent different types of counterfeited ICs such as cloned, overproduced, defective/ out-of-spec ICs.

• **Combating Die / IC Recovery (CDIR)**: The first CDIR to prevent parts from being recycled has been presented in [20] [21]. The technique in [20] inserts a light-weight sensor in the chip to capture the usage of the chip in the field and provides an easy detection capability. This type of sensor relies on the aging effects of MOSFETs to change a ring oscillator frequency in comparison with the golden one embedded in the chip. As a part used in the field ages because of the wearout mechanisms such as NBTI and HCI, the shift in the frequency of this sensor indicates the level of aging and provides a simple readout of the value.

• **Antifuse-based Technology for Recording Usage Time**: The antifuse-based sensor first proposed for recycled IC detection appeared in [22]. It is composed of counters and an embedded antifuse memory block. The counters are used to record the usage time of ICs while its value is continuously stored in an antifuse memory block. Since the antifuse memory block is one time programmable, counterfeiters can not erase the context during the recycling process. Two different structures of the AF-based sensor have been proposed to measure the usage time of ICs. *CAF-based sensor* records the cycle count of the system clock during chip operation. The usage time of recycled ICs can be reported by this sensor, and the measurement scale and total measurement time could be adjusted according to the application of ICs. On the other hand, *SAF-based sensor* uses circuit activity as trigger (clock) to the counter. A number of signals with low switching probability is selected to calculate the usage time. It generally requires less area overhead than the CAF-based sensor.

• **Electronic Chip ID (ECID)**: To track ICs throughout the supply chain, each IC can be tagged with a unique ID. This ID can be easily read during the chip's lifetime. The conventional approach for writing the unique ID into a non-programmable memory (such as One-Time-Programmable [OTP], ROM, etc.) requires post-fabrication external programming, such as laser fuses [23] or electrical fuses (eFuses) [24]. The eFuse is gaining popularity over laser fuses because of its small area and scalability [24].

B. Package ID

The avoidance measures discussed so far only target new ICs. However, a large portion of the supply chain is populated by active and obsolete components. There is no opportunity for adding any extra hardware to create a chip ID in those designs. For tagging such active and obsolete components, we need to create package IDs that do not require the access to designs. No package modifications should be allowed during the generation of package IDs. These IDs can be used for new components as well. DNA markings, Nanorods, and magnetic PUFs are three viable options for creating package IDs.

• **DNA Markings**: Plant DNA is scrambled to create new and unique genetic sequences, and these new sequences integrated with inks. These inks are then applied on the packages of the ICs at the end of the packaging process. Authentication includes first checking whether the ink fluoresces under specific light, and second sending a sample of the ink to a lab to verify that the DNA is in the database of valid sequences [25]. Recently, DoD mandated [26] the DNA marking be placed on the components in order to track them throughout the supply chain. DNA markings have several limitations that introduce some serious concerns of their applicability in counterfeit avoidance. The fast authentication achieved by observing the fluorescence of the marking under specific light can be imitated by counterfeiters, either by invalid DNA or by other materials. But detailed DNA validation is extremely time-consuming and costly [27].

• **Nanorods**: A microscopic pattern is created by growing an array of nanospheres into nanorods that are less than 100nm long [28]. Each time the process is repeated, the same pattern is created, but the exact angle and length of each individual nanorod varies, so that each set of nanorods is distinct. After the array of nanorods is grown, it is applied to a chip using a specialized printer. The chip can be authenticated by comparing the overall pattern and visual properties of each nanorod to a database.

• **Magnetic PUF**: A magnetic PUF uses inherent characteristics of magnetic stripes for unique identification [29]. Each magnetic stripe, due to the randomness of the creation process, has a noise-like component along with the data that is stored. This noise is unpredictable and difficult to clone, yet is consistent and repeatable, therefore acting as a PUF.

IV. Avoidance Challenges

We believe that research in the avoidance of counterfeit electronic components is still in its infancy. There are major challenges that must be overcome in the development of effective test methods. In this section, we will discuss the counterfeit avoidance challenges, which urgently need to be resolved in the near future. Table I presents a comparative study of all the different counterfeit avoidance technologies. We have assigned each technology a score of high, medium, or low, depending on effectiveness.

• **Reliability**: A major issue that must be overcome for many of these techniques is reliability. For example, the response of a PUF must be constant for a given challenge over a wide range of environmental variations, ambient noise, and aging effects. Hardware metering also has the same reliability concern as it uses PUFs. There is a serious reliability concern regarding DNA marking, as environmental conditions such as high temperatures can potentially damage the DNA and either make the sequence unreadable or change the sequence. The reliability of nanorods and magnetic PUFs are not yet been verified.

• **Uniqueness**: It is a measure of randomness between two chip IDs. Ideally, two IDs should differ with a probability of 0.5 under the same test conditions. Better uniqueness makes it difficult for counterfeiters to guess new IDs after obtaining a set of IDs. PUFs and magnetic PUFs produce responses nearly equal to the ideal case [30]. Any high-level language (C/C++, Java, Matlab etc.) can generate a true random number, which is generally used as the ECID. In DNA, due to the very large number of base pairs, there are enough sequences to support billions of unique markings. However, in the fast-authentication mode of DNA testing, the observation of a specific "light" can be easily imitated by an adversary. For nanorods, the uniqueness of the marking is based on the number of nanorods in the pattern and the sensitivity of the measuring device to color and intensity of light. Since the exact angle of each individual nanorod is random, it is very unlikely that the same process will produce the same result, and manually cloning the marking at nanoscale is not practical.

• **Tamper resistance**: The difficulty faced by the attacker/counterfeiter when attempting to disable the counterfeit avoidance system is referred to as tamper resistance. It is extremely difficult to physically clone the IDs generated by PUFs and magnetic PUFs. The CDIR sensors also provide high tamper resistance because they employ unavoidable aging. It is easy to clone the ECID as it is static and readable. It is easy for counterfeiters to imitate the color generated by DNA markings during fast-authentication mode. The tamper resistance of nanorods has not yet been verified.

• **Area overhead**: It provides the area required on the die to implement a counterfeit avoidance measure. PUFs, CDIR sensors and ECID require low area overhead whereas hardware metering, SST, and poly fuse-based sensors offer medium area overhead. DNA markings, nanorods, and magnetic PUFs do not require any area overhead on the die.

• **Target counterfeit types**: Different available technologies target different counterfeit types. PUFs and magnetic PUFs can detect remarked, overproduced, and cloned counterfeit types. SST can likely detect overproduced, out-of-spec/defective, and cloned component types. CDIR and poly fuse-based sensors are designed to target recycled and remarked types. ECID can potentially detect remarked type. DNA markings, and nanorods can detect recycled and remarked counterfeit types. Figure 5 shows all currently available technologies to address various counterfeit types.

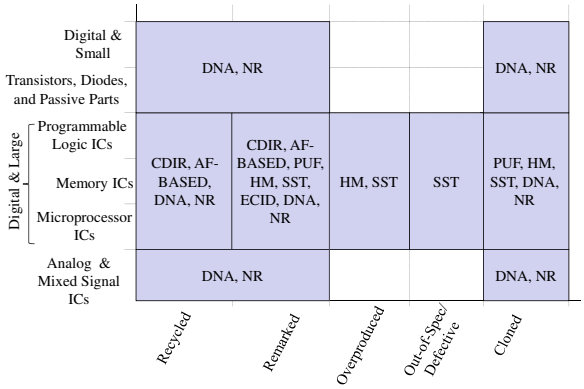

Figure 5. Available technologies for counterfeit avoidance.

• **Target components**: Another challenge to consider is what type of components should be targeted for implementing avoidance measures. DNA markings, nanorods, and magnetic PUFs may be implemented in both analog and digital components whereas the other anti- counterfeit measures can only target the digital components. From Figure 5, it is clear that we have only DNA and NR to address the avoidance of small component types (small digital, entire analog and mixed signal components). However, as we described earlier that the authentication and reliability issues with DNA and NR, these entire spectrum of components need much more attention to the research community. Again, there are no technologies available to us to address the authentication of these components to prevent overproduced and out-of-spec/defective types getting into the supply chain.

• **Implementation cost**: The cost for implementing a PUF would entail storing and maintaining the challenge-response pairs in a secure database, along with its area overhead. For hardware metering and SST, back-and-forth communication between the design house and foundry make it expensive to implement. For CDIR and poly fuse-based structures, the cost comes from the area overhead. To authenticate the ICs, low-

Table I
IMPLEMENTATION CHALLENGES OF COUNTERFEIT AVOIDANCE TECHNIQUES.

Avoidance Techniques	Reliability	Uniqueness	Tamper Resistance	Area overhead	Target Counterfeit Types	Target Component	Implementation Cost
Physically Unclonable Functions (PUF)	Medium	High	High	Low	Remarked, Overproduced, Cloned	Digital ICs	Medium
Hardware metering	Medium	High	Medium	Low/Medium	Overproduced, Cloned	Digital ICs	High
Secure Split Test (SST)	NA	NA	Medium	Medium	Overproduced, Cloned, Out-of-spec/ defective	Digital ICs	High
Combating Die/IC Recovery (CDIR)	Medium	NA	High	Low	Recycled, Remarked	Digital ICs	Low
Poly Fuse-based Technology for Recording Usage Time	Medium	NA	High	Medium	Recycled, Remarked	Digital ICs	Medium
Electronic Chip ID (ECID)	High	High	Low	Low	Remarked	Digital ICs	Low
DNA Markings (DNA)	Medium	Medium	Medium	NA	Recycled, Remarked	All (Digital/Analog/RF/etc.)	High
Nanorods (NR)	Not Verified	Medium	Not Verified	NA	Recycled, Remarked	All (Digital/Analog/RF/etc.)	Not Verified
Magnetic PUF	Not Verified	High	High	NA	Remarked, Overproduced, Cloned	All (Digital/Analog/RF/etc.)	Not Verified

cost equipment is required. We need only a secure database to store the ECID. Thus, the cost from area overhead is negligible. The detailed authentication for identifying the plant DNA applied to the IC is expensive.

V. CONCLUSION

In this paper, we have presented all the counterfeit types currently corrupting the electronic component supply chain. We have analyzed the vulnerabilities in the electronic component supply chain. We have described all current available technology to address counterfeit avoidance. We believe that the current effort to address the counterfeiting problem is clearly not sufficient. More research is needed to implement effective avoidance measures that are adaptable as the counterfeiting process will become more sophisticated over time. Above all, new, low-cost, and robust anti-counterfeit mechanisms must be developed.

REFERENCES

[1] trust-HUB, http://trust-hub.org/home.

[2] U.S. Senate Committee on Armed Services, "Inquiry into Counterfeit Electronic Parts in the Department Of Defence Supply Chain," May 2012.

[3] U.S. Senate Committee on Armed Services, "Suspect Counterfeit Electronic Parts Can Be Found on Internet Purchasing Platforms," February 2012. [Online]. Available: http://www.gao.gov/assets/590/588736.pdf

[4] US Congress, *Ike Skelton National Defense Authorization Act for Fiscal Year 2011*. [Online]. Available: http://www.gpo.gov/fdsys/pkg/BILLS-111hr6523enr/pdf/BILLS-111hr6523enr.pdf

[5] SAE, "Counterfeit electronic parts; avoidance, detection, mitigation, and disposition," 2009, http://standards.sae.org/as5553/.

[6] IDEA, "Acceptability of electronic components distributed in the open market," http://www.idofea.org/products/118-idea-std-1010b.

[7] X. Zhang, K. Xiao, and M. Tehranipoor, "Path-delay fingerprinting for identification of recovered ics," in *Proc. of IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems*, Oct. 2012.

[8] K. Huang, J. Carulli, and Y. Makris, "Parametric counterfeit IC detection via support vector machines," in *IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT)*, 2012, pp. 7–12.

[9] U.S. Department Of Commerce, "Defense Industrial Base Assessment: Counterfeit Electronics," Jan. 2010.

[10] M. Tehranipoor and F. Koushanfar, "A survey of hardware trojan taxonomy and detection," *IEEE Des. Test*, vol. 27, no. 1, pp. 10–25, 2010.

[11] "Defense Science Board (DSB) study on high performance microchip supply (2005)," http://www.acq.osd.mil/dsb/reports/ADA435563.pdf.

[12] H. Levin, "Electronic waste (e-waste) recycling and disposal facts, statistics & solutions," 2011, online. [Online]. Available: http://www.moneycrashers.com/electronic-e-waste-recycling-disposal-facts/

[13] U.S. Environmental Protection Agency, "Electronic waste management in the united states through 2009," May 2011.

[14] L. W. Kessler and T. Sharpe, "Faked parts detection," *Printed Circuit Design & Fab*, vol. 27, no. 6, p. 64, 2010.

[15] J. Villasenor and M. Tehranipoor, "Chop shop electronics," *Spectrum, IEEE*, vol. 50, no. 10, pp. 41–45, 2013.

[16] R. Pappu, "Physical one-way functions," Ph.D. dissertation, Massachusetts Institute of Technology, 2001.

[17] F. Koushanfar, G. Qu, and M. Potkonjak, "Intellectual property metering," in *Inform. Hiding*. Springer-Verlag, 2001, pp. 81–95.

[18] F. Koushanfar and G. Qu, "Hardware metering," in *Proc. Design Automation Conference*, 2001, pp. 490–493.

[19] G. Contreras, T. Rahman, and M. Tehranipoor, "Secure split-test for preventing ic piracy by untrusted foundry and assembly," in *Int. Symposium on Defect and Fault Tolerance in VLSI Systems (DFT)*, 2013.

[20] X. Zhang, N. Tuzzio, and M. Tehranipoor, "Identification of recovered ics using fingerprints from a light-weight on-chip sensor," in *Proc. of IEEE on Design Automation Conference*, June 2012, pp. 703 –708.

[21] J. Villasenor and M. Tehranipoor, "Are you sure its new? the hidden dangers of recycled electronics components," in *IEEE Spectrum*, 2012.

[22] X. Zhang and M. Tehranipoor, "Design of On-chip Light-weight Sensors for Effective Detection of Recycled ICs," *IEEE Transactions on VLSI (TVLSI)*, 2013.

[23] K. Arndt, C. Narayan, A. Brintzinger, W. Guthrie, D. Lachtrupp, J. Mauger, D. Glimmer, S. Lawn, B. Dinkel, and A. Mitwalsky, "Reliability of laser activated metal fuses in drams," in *Proc. of IEEE on Electronics Manufacturing Technology Symposium*, 1999, pp. 389–394.

[24] N. Robson, J. Safran, C. Kothandaraman, A. Cestero, X. Chen, R. Rajeevakumar, A. Leslie, D. Moy, T. Kirihata, and S. Iyer, "Electrically programmable fuse (efuse): From memory redundancy to autonomic chips," in *Proc. of IEEE on Custom Integrated Circuits Conference*, 2007, pp. 799–804.

[25] M. Miller, J. Meraglia, and J. Hayward, "Traceability in the age of globalization: A proposal for a marking protocol to assure authenticity of electronic parts," in *SAE Aerospace Electronics and Avionics Systems Conference*, Oct. 2012.

[26] U.S. Defense Logistics Agency, "DNA AUTHENTICATION MARKING ON ITEMS IN FSC 5962," Aug. 2012. [Online]. Available: https://www.dibbs.bsm.dla.mil/notices/msgdspl.aspx?msgid=685

[27] Semiconductor Industry Association (SIA), "Public Comments - DNA Authentication Marking on Items in FSC5962," Nov. 2012.

[28] C. Kuemin, L. Nowack, L. Bozano, N. D. Spencer, and H. Wolf, "Oriented assembly of gold nanorods on the single-particle level," *Advanced Functional Materials*, vol. 22, no. 4, pp. 702–708, 2012.

[29] R. E. Morley, E. J. Richter, and G. L. Engel, "Method and apparatus for authenticating a magnetic fingerprint signal using an adaptive analog to digital converter," Patent US7 210 627 B2, May 1, 2007. [Online]. Available: https://patentimages.storage.googleapis.com/pdfs/US7210627.pdf

[30] Y. Hori, T. Yoshida, T. Katashita, and A. Satoh, "Quantitative and Statistical Performance Evaluation of Arbiter Physical Unclonable Functions on FPGAs," in *International Conference on Reconfigurable Computing and FPGAs (ReConFig)*, 2010, pp. 298–303.