JOURNAL OF INSTITUTE OF SMART STRUCTURES AND SYSTEMS (ISSS)

JISSS, 4(1), pp. 18–37, March–September 2015.

INVITED PAPER

Integrated circuit security: an overview

Ange Marie P. Fievre[a,*], Al-Aakhir A. Rogers[b], Shekhar Bhansali[a]

[a]Dept. of Electrical and Computer Engineering, Florida International University, Miami, FL

[b]Dept. of Electrical Engineering, University of South Florida, Tampa, FL

*Corresponding author: pfiev001@fiu.edu

Keywords

Integrated circuits
Security and protection
Anti tamper
Authentication
Electronics packaging

Received: 11-04-2015

Abstract

Integrated circuits security is surveyed. After the necessity of IC protection, different security classification systems are presented: degree of invasion, IBM levels, and FIPS 104-2 standards. A new classification is proposed, based on protection location (chip itself or package) and on protection aspect: anti-tamper or authentication. The main feature of each protection method is explained, advantages, drawbacks and current research challenges are discussed. It is concluded that security techniques should aim at satisfying the requirements of emerging technologies such as 3D Heterogeneous Systems on a Chip and wearable devices: compactness, anti-tamper and authentication.

1 Introduction: the necessity of IC security

The conception and manufacture of complex integrated circuits (ICs) and semiconductor devices entails a considerable amount of time as well as sophisticated engineering skills, which makes creating such devices an expensive activity. Additionally, ICs can contain software encoded in memories or they can be employed for purposes necessitating encryption in order to maintain the secrecy of valuable information. These ICs impact numerous sectors of the semiconductor industry, ranging from medical, to automotive, to aeronautics, to communications and to defense, which is why their tampering (interfering with them so as to misuse, alter, or corrupt them [Dictionary, 2015]) and counterfeiting (their fraudulent imitation or forgery [Dictionary, 2015]) represent a serious problem [Martin *et al.* 2010]. The global investment on semiconductor research and development (R&D) increased by 7% from $48.7 billion in 2011 to $53.0 billion in 2012 [Yancey, 2013]. Therefore, one can foresee an increase in tampering and counterfeiting activities resulting from insufficient security for the related intellectual property.

Indeed, IHS (formerly Information Handling Services), a market research firm, revealed in an April 2012 publication that the five most commonly counterfeited types of semiconductors represent $169 billion in potential annual risk for the international electronics industry [Lineback, 2012]. The International Chamber of Commerce (ICC) stated that fake and pirated manufactured goods will reach a total value of up to $1,770 billion in 2015 [Frontier, 2011]. With technology and data positioned in combat zones, and original critical military hardware replaced by counterfeits, the danger to security and safety is as a major concern by the United States Senate Armed Services Committee [Committee on Armed Services, 2012]. Another wake-up call was the capture in December 2011 of the US RQ-170 Sentinel surveillance drone fallen in Iran, with the Iranian government claiming to have extracted secret information from the aircraft [Springer, 2013]. Aviation in general and medical devices

ISSS International Conference on Smart Materials, Structures and Systems held on July 08-11, 2014 at IISc Bangalore

both are high-risk targets because of the potential threat to human life.

The challenges posed by counterfeits are twofold. The first challenge is how to protect an IC chip against piracy (unauthorized copy), so that neither its physical structure, logical operation, or informational content can be discovered and replicated by a non-authorized entity. The second challenge is to verify chip integrity versus replicas.

1.1 *Comparison with existing surveys and organization*

Many surveys have been written on the subject of IC security. An early prominent publication, [Anderson & Kuhn, 1996] provides with a taxonomy of attackers, gives examples of non-invasive and physical attacks, and goes over governmental and commercial protection techniques available at the time and their weaknesses. Later, [Skorobogatov, 2005; 2012] add a brief description of the security levels as defined by IBM (International Business Machine) and FIPS (Federal Information Processing Standard), place attacks in non-invasive, invasive and semi-invasive categories and also describe several defense technologies against these types of attacks. Subsequently, [Koushanfar *et al.* 2012] presents anti-counterfeiting approaches and initiatives, discusses general research challenges in that field, and describes several anti-counterfeiting methods. More recently [Rostami *et al.* 2013; 2014] give threat models, state-of-the-art defenses and the defenses metrics for different types of attacks, while [Guin *et al.* 2013; 2014] classify components and counterfeit types, expose supply chain vulnerabilities, identify avoidance and detection measures and review the associated challenges.

This review investigates answers to the two challenges mentioned earlier: protecting chips against piracy and verifying their integrity. This review will identify different types of piracy methods used against ICs, the information obtained through tampering, and different classifications of security techniques. However, a different classification is introduced, in which the location of the protection measure, on the chip itself or in the package, is taken in consideration. On-chip security techniques are generally applicable only to new chips because of modifications in the design or fabrication steps. On the other hand, package-level solutions are independent from the device and can be added to old as well as new chips. In each category, the security goal (anti-tamper or authentication) adds further subdivision. Additionally, this paper presents security techniques that have been proposed over the years, following the new classification, and a summary of the research in IC security is given. The review is concluded with the current active areas of research in IC security that address the requirements for popular emerging system-on-chip and wearable technologies.

2 Types of attacks

There are multiple approaches for counterfeiting a chip or accessing its sensitive data. As previously mentioned [Guin *et al.* 2014], counterfeit integrated circuits can be old ICs that are recycled, or new ICs that are overproduced, given false specifications or sold although defective; a counterfeit can also be a clone (copy).

When layouts or masks are not readily available for duplication purposes, or when critical information is located inside the device, some kind of probing becomes necessary. Historically those means have often involved damage to at least part of the chip; hence, they are commonly termed “attacks.” The types of attacks aimed at discovering the workings of a device or accessing information are classified as invasive, noninvasive, or semi-invasive by [Skorobogatov & Anderson, 2003].

In an invasive attack, the packaging is removed in order to get immediate access to internal components. The IC can then be studied either by microprobing or reverse engineering. Microprobing involves placing a chip under a long-working-distance optical microscope, whereas test signals are received and monitored by a computer. Using a laser, the passivation layer (the inert layer preventing corrosion) is ablated or removed, which allows probe access to the internal signal lines [Anderson & Kuhn, 1996; Skorobogatov, 2012]. A focused ion beam (FIB) can be used to etch/mill through multiple layers to access conductive lines. After locating the conductive line, the FIB deposits a metal, such as platinum, to connect the signal to the surface, making it more easily accessible to larger probes [Tsang, 2011].

In reverse engineering, the different layers of an IC are imaged using a high resolution reflected-light microscope with camera to create a three-dimensional map of the structure. As a result of this destructive invasion method, the IC is often rendered unusable. However, if layers of an IC can be taken off without notably altering trapped charges, the stored information or software contained in the IC can be revealed, and reproduced or modified [Anderson & Kuhn, 1996; 1998].

With the continuing shrinkage of IC components, invasive attacks are becoming more difficult, extremely time-consuming, and require sophisticated instruments and skills. Conversely, noninvasive attacks constitute a lower-cost option for the attacker, as minimal equipment is required for that type of tampering. A noninvasive attack is the study of the IC by indirect means, also called side channels. This method generally consists of tapping the device wires for signal or radiations, or connecting the IC to an external test circuit. Analysis of the signals coming through side-channels has been successfully demonstrated to obtain secret keys from secure devices easier, faster, and at lower cost than destructive attacks. Noninvasive observations can reveal the logical functions of circuit modules [Skorobogatov, 2005] and obtain stored information that is crucial for circuit functionality [Standaert, 2010]. Additionally, there are no signs of tampering, illustrating the danger associated with this type of attack. Common noninvasive methods include:

(1) Collecting timing information from operations associated with security: the time consumed by every input-output pair is recorded, whether it is a single operation or an entire function [Kocher, 1996; Dhem *et al.* 2000].

(2) Looking at current or power consumption during changes of states [Mangard *et al.* 2007; Kocher *et al.* 1999]. Amongst these methods, differential power analysis (DPA), extracts secret information from an integrated circuit as this IC performs the same predictable operations, by applying statistical correlation and error correction methods to data-dependent power traces collected at the supply pins [Kocher *et al.* 1999].

(3) Exploiting electromagnetic radiations that leak information on different components of a device. For one component these emanations are of various types, depend on the operation being performed by the device, and are a result of the characteristics of the component combined with its coupling with other neighboring components. With sensors judiciously chosen and positioned, it is possible to obtain multiple views of operations [Gandolfi *et al.* 2001]. This multidimensionality makes electromagnetic side channels even more effective than power analysis, which is only cumulative [Quisquater & Samyde, 2001].

A semi-invasive attack is between noninvasive and invasive attacks. It can provide an enormous amount of information on a circuit without the cost or the time required by a full invasive attack. It is invasive to the device packaging only, with no damage to the passivation layer. Physical contact is not made with the internal lines and the IC remains functional. For instance, exposure to ultraviolet light rendered security fuses on early erasable memory and microcontrollers inoperative [Skorobogatov, 2005]. Other examples of semi-invasive methods have used infrared light to provide a view through the back surface of a chip [Wagner, 1999], or thermal imaging to locate active areas [Soden, 1997], or a pico-second imaging circuit analysis (PICA) technique to detect optical emissions from the chip [Tsang, 2000]. Other illustrations of semi-invasive methods are optical-beam-induced current (OBIC) [Richards & Footner, 1992] or light-induced voltage alteration (LIVA) [Ajluni, 1995]; both of them utilize laser scanning to detect the location and logic state of transistors. An outstanding semi-invasive attack is fault injection, in which atypical environmental conditions are instigated during cryptographic operation in order to uncover the internal states, and which can breach a circuit faster than noninvasive attacks [Mangard *et al.* 2007; Anderson *et al.* 2008; Boneh *et al.* 1997; Kim & Quisquater, 2007]. Fault injection employs power tampering, short clock signals, large temperature variations, external electromagnetic fields, and light attacks such as pulsed lasers or ultraviolet lamps [Schmidt *et al.* 2009; van Woudenberg *et al.* 2011;

Dehbaoui *et al*. 2012; Balasch *et al*. 2011; Bar-El *et al*. 2006; Endo *et al*. 2011] to alter the state of chosen transistors in the IC, allowing a pirate to figure out the operation of the IC and ways to bypass its security features.

Invasive, noninvasive and semi-invasive attacks are conducted on devices that have been already built. Another threat exists due to the worldwide distribution of IC production currently, and the involvement of often untrusted contractors. This makes it possible for a malicious party to modify or insert stealth components in a circuit during any step of the supply chain. These rogue components will either disable the IC, cause it to behave differently or allow stealing information under specific conditions that will not happen during standard simulations and post-manufacturing tests. This type of attack is termed hardware Trojan [Anderson *et al*. 2008; Abramovici & Bradley, 2009; Adee, 2008; Agarwal *et al*. 2007; Bhunia *et al*. 2013; 2014; Chakraborty *et al*. 2009; Karri *et al*. 2010; Skorobogatov & Woods, 2012; Tehranipoor & Koushanfar, 2010].

To summarize, the main features of the four types of attacks described above are compared in Table 1. Ideally, an anti-tampering device would not only be impervious to all four, but it would indicate if any attack were attempted against it. A desired feature that would allow a legitimate examiner to confidently ascertain that an IC is not a counterfeit would be continued improvement in device integrity. However, in a nonideal world, ideas for a completely tamper-proof and authenticatable IC are often well ahead of the technological means available to create such device, which is why security methods are classified according to the type of protection they offer.

3 Classification of security solutions

The number of patents filed on IC security is proof that it is a constant preoccupation. However, there are fewer IC security techniques released to the point of implementation in an experimental setting or for commercial or governmental purposes, and this is evidence of the complexity of the task at hand. With the various types and evolution of attacks, different classification approaches have been offered, in regards to the first challenge posed by counterfeits, i.e. tamper resistance.

One system simply follows the attack classification and considers which type of attack is being counteracted [Skorobogatov & Anderson, 2003], based on the fact that most anti-tampering techniques offer a countermeasure against either invasive/semi-invasive or semi-invasive/noninvasive attacks; resistance against all three types of attacks usually comes from an integration of different solutions, each solution tackling one type of attack.

Large companies are highly targeted, and as a result put high-level solutions in place for protection. For example IBM, a leader in secure systems, lists six security levels for electronic systems in general, according to the amount of expertise, time, and the equipment cost necessary to break these levels of defense [Abraham *et al*. 1991]:

(1) Level ZERO: no security features; no time, no cost;

(2) Level LOW: little security; inexpensive and easy attack;

(3) Level MODL: security against low-cost attacks; some expertise, cost up to $5,000;

(4) Level MOD: moderate security; some expertise, time, cost up to $50,000;

(5) Level MODH: advanced security; much expertise and time, cost over $50,000;

(6) Level HIGH: security against all known attacks.

The US government, in the more specific framework of cryptographic modules for sensitive

Table 1. Comparison of the main four types of integrated circuit attacks.

	Depackaging	Physical contact with internal circuitry	Fast	Expensive	Tamper-evident
Invasive	Yes	Yes	No	Yes	Yes
Semi-invasive	Yes	No	Yes	No	Yes
Noninvasive	No	No	Yes	No	No
Hardware trojan	No	No	Yes	No	No

information, imposes the FIPS (Federal Information Processing Standard) 140-2 standard, established by the National Institute of Standards and Technology (NIST). This standard describes in increasing order four levels of security, as well as the active or passive nature of the protection [NIST, 2001], and any system performing cryptographic operations and used by the government or military must abide to it:

(1) Level 1, the lowest level of security, requires typical passivation methods, for example a seal (protective) layer to counter environmental or other physical damage;

(2) Level 2 enhances the physical security of Level 1 by making tamper evidence of the seal mandatory;

(3) Level 3 intends to stop an unauthorized party from obtaining access to key security parameters stored inside the module, for example, by placing the module in a solid, opaque, hermetic enclosure to discourage access to the contents or ensuring that tampering will destroy the module;

(4) Level 4 offers the highest level of security. It calls for active anti-tampering technologies or a combination of passive and active tamper-resistant layers. With active anti-tampering, a targeted IC will take some action when subjected to any suspicious activity. This event can be environmental conditions or variations outside of the normal working ranges of the module, such as voltage, photon detection, acceleration, strain, temperature, chemical reactions, or proximity. Typical reactions are erasure or destruction. Level 4 mechanisms are particularly helpful in physically unguarded settings.

Another system of classification is proposed in Figure 1. In a first division, it considers the location of the countermeasures. This organization stems from the fact that protection can be implemented in the device packaging or, more intimately, added to the chip. In order to integrate both challenges posed by counterfeits, authentication is included in addition to tamper resistance, and the security solutions are further partitioned according to which challenge they address. The following examination of IC security techniques uses this classification approach.

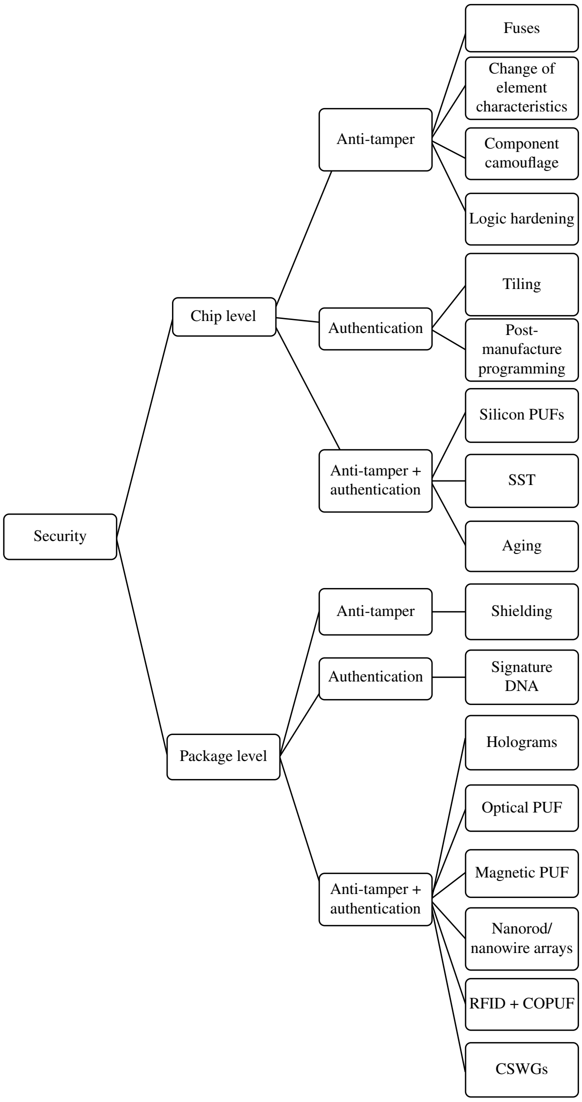


Figure 1. Security classification based on location and goal of the protection.

4 IC security techniques

4.1 *Chip-level security*

4.1.1 Anti-tamper. One of the first security issues tackled by IC manufacturers was attacks against erasable programmable read-only memories (EPROM). To prevent unauthorized access, they placed security fuses shielded by a metal cover opaque to ultraviolet light. The objective was to make the fuses hard to find and if found, difficult to manipulate by a pirate. In electrically erasable programmable read-only memories (EEPROM), inverted memory cells were made more resistant to UV light. Furthermore, to counter well-equipped and highly skilled entities that could resort to laser cutting or FIB machines to take away the protective metal, multiple fuses would be placed at different locations. This would affect the data contained in the memory and make it useless [Skorobogatov, 2012].

Some researchers have proposed changing the characteristics of the circuit elements. For example, FIB implants could reduce the switching speed of chosen logic gates, making the usual low speed test methods useless in establishing their correct logic functions [Walden, 1993; 1994]. Also largely suggested has been camouflage. One example would make analog components look like digital components and hide the former amongst a digital IC [Ciccone & Yup, 2001]. Another illustration would be to configure false interconnection contacts in read-only memory (ROM) devices or in flash memory cells [Vajana & Patelmo, 2003; Vajana & Patelmo, 2003]. In other instances, a lightly doped density (LDD) region called "channel block" would be placed between the active areas, where the dopant type of the channel block would determine if there is connection or not. However, the density would be so small that usual reverse engineering methods would not discover the presence or polarity of the implants [Baukus *et al.* 2000; Chow *et al.* 2009; Clark *et al.* 2012]. These connections would not be made of metal wires, but instead they would be buried, making surface etch necessary [Baukus *et al.* 1999; 2001; 2005; Clark *et al.* 2007]. Also, fake apparent metal connections and nonworking transistors looking like real ones would mislead a reverse engineer [Baukus *et al.* 2012; Chow *et al.* 2004; 2007; 2008; 2011; 2012; Cocchi *et al.* 2013]. Another example uses fake features isolated by invisible etch stop films [Hsu *et al.* 2013]. These methods do make reverse engineering harder by forcing the attacker into brute force, but at the cost of power, area and delay overheads [Rajendran *et al.* 2013].

Security fuses, FIB implants and camouflage seek mostly to protect against invasive attacks. On the other hand, various protection methods termed logic hardening have been proposed at the circuit level specifically against noninvasive and semi-invasive attacks.

A method against timing attack is to make all operations take the same amount of time [Kocher, 1996; Bhunia *et al.* 2013], but this is clearly at the cost of efficiency. Another technique with less negative impact on performance and also used against electromagnetic leakage is to blind, i.e. to modify the way a computation is conducted so that it is uncorrelated to timing or electromagnetic radiations [Kocher, 1996]. Other timing countermeasures eliminate cache or modify the way data is cached [Skorobogatov & Woods, 2012; Tehranipoor & Koushanfar, 2010; Page, 2003; Cohen & Aviv, 2005].

One way to counter DPA is to make power consumption constant. This can be achieved by using gates that consume power independently of their input values, i.e. dual-rail logic, where the logic is replicated using complement wires and gates [Ambrose *et al.* 2011; Bucci *et al.* 2011; Hoang & Fujino, 2014; Morrison & Ranganathan, 2014; Saputra *et al.* 2003; Tiri & Verbauwhede, 2004]. An on-chip signal suppression circuit can be added without alterations to the encryption circuitry to prevent information escaping through the current supply pin side-channel to be acquired by differential power analysis. The total current drawn from the supply is maintained at a defined level. Since DPA receives information resulting from variations in the supply current, when these variations are reduced, a pirate needs more power samples to differentiate information from noise. The number of necessary power traces can be made excessively large, rendering the attack very long and expensive for the attacker [Ratanpal *et al.* 2004]. These countermeasures are accomplished at the price of higher power expenditure and larger circuit area.

Circuit-level solutions such as randomization or update of keys during computation are used as well against timing attacks, power analysis or electromagnetic leakage. Signal strength reduction can also be effective against both electromagnetic and power analysis attacks [Agrawal *et al.* 2003].

A great deal of research is also aimed at counteracting fault attacks. Input parameters are commonly protected using cyclic redundancy checks; processing parts by redundant computation, checks on algorithm-specific properties, or blinding of exponentiation algorithms; and program flow by a signature. In these cases the security requirements have to be balanced with hardware or time overhead. Inherent countermeasures, such as the choice of parameters, can also be used.

These solutions are reviewed in more detail by [Karaklajic *et al*. 2013; Marzouqi *et al*. 2014; Verbauwhede *et al*. 2011].

Garbled circuits promise a general solution to all noninvasive and semi-invasive attacks, with circuit area comparable to existing countermeasures [Goldwasser *et al*. 2008; Huang *et al*. 2011; 2012; Järvinen *et al*. 2010; Yao *et al*. 1986; Bellare *et al*. 2012].

4.1.2 Authentication. The other challenge is authenticating a chip, in other words determining whether the chip is an original or not. For that the IC has to be marked by a key that is impossible or too costly to reproduce. Chip authentication data have traditionally been stored on nonvolatile memory located on the chip itself. The basic measures to prevent unauthorized access to this information are encryption of the data and/or permanent disconnection of the fuses leading to the section of the memory where it is written. However, with the plurality of types of attacks available, those precautions are no deterrent to a skilled and determined pirate, thus prompting more sophisticated methods to encode the origin and identity markers of ICs.

One authentication method has been the adaptation of watermarking to hardware, which means embedding authentication information in the circuitry in a manner invisible to the user. Researchers at UCLA utilized unused portions of FPGA blocks to mark their circuits [Lach *et al*. 1998]. The circuit was divided in tiles, each tile having several possible instances. Two instances of the same tile had the same functionality and were interchangeable, but with different layouts with marking differently located. One circuit instance was thus made up of a set of instances of diverse tiles. In this fingerprinting technique, although timing properties might vary from one tile instance to another, there was no effect on global performance, timing, or power consumption. However, the technique cannot be employed for application specific designs (ASICs), which use a single mask. A method suitable for ASICs was the assignment of a unique ID to each chip by appending a small section to the control path that could be programmed after manufacture [Koushanfar *et al*. 2001]. Besides incorporating the unique ID into the functionality of the IC, this technique was the first that would allow assessment of the number of counterfeits in the event that piracy would be discovered. However, new solutions were needed that would not be limited to meter counterfeits, but would instead prevent their creation and circulation. Methods allying anti-tamper and authentication at the chip level are reviewed next.

4.1.3 Anti-tamper with authentication. An innovative method to give a unique ID to each IC was the Integrated Circuit Identification Device (ICID). That technique required no unusual processing steps, and no post-manufacture encoding was necessary. Identical transistors, forming an array, drove each a resistive load. Fabrication variations caused the current passing through this load to be random, and the corresponding voltage was converted to a bit string [Lofstrom *et al*. 2000].

ICID was the first example of a Physically Unclonable Function (PUF), before the name was coined. This authentication method has been gaining in popularity for the past decade and takes advantage of unique characteristics that are inherent to each IC. Two identically functional instances of the same chip will have distinctive features that are due to uncontrollable random imperfections created during fabrication [Gassend *et al*. 2002]. This unique pattern is the key that identifies the chip, and cannot be duplicated. The key unlocks a secret set of challenge (applied physical stimulus) and response (unpredictable but repeatable device reaction), coming from an exponentially large pool of possibilities, for authentication. In addition, any probing attempt alters the PUF's behavior, ruining the PUF and providing tamper evidence of invasive attack.

Other examples of integrated circuit-based PUFs are silicon PUFs. The first PUFs of this type were arbiter-based PUFs where a latch determines which of two racing signals going through a sequence of MUX stages arrived first [Gassend *et al*. 2002; 2004]. Implemented for circuit authentication, they make use of delay information as parameters. To achieve reliability of those PUFs in environmental variations, relative delay comparisons are taken into account [Lee *et al*. 2004]. Security is further enforced by the fact that the key is volatile and is only generated when the device is powered. However, arbiter-based PUFs display weakness in front of model-building and emulation attacks [Lim *et al*. 2005; Majzoobi *et al*. 2008; Rührmair *et al*. 2010], and have low entropy, which limits their unpredictability [Katzenbeisser *et al*. 2012]. Reliability problems, like the effects of aging, also need to be resolved.

More reliability and simplicity were brought in a modification of the arbiter PUFs, applicable to both Application-Specific Integrated Circuits (ASICs) and Field-Programmable Gate Arrays (FPGAs) [Suh & Devadas, 2007]. They use delay loops to generate Ring Oscillator Physical Unclonable Functions (ROPUFs), simple circuits that oscillate with a frequency affected by fabrication variations and hence would not be predictable, but could still easily be established by a counter. ROPUFs have become one of the most widespread physical unclonable functions, seeking more security and smaller area [Bin *et al.* 2011; Chen *et al.* 2011; Kumar *et al.* 2012; Maiti & Schaumont, 2011; Maiti *et al.* 2012; Mansouri & Dubrova, 2012; Merli *et al.* 2010; Qu & Yin, 2009; Vivekraja & Nazhandali, 2011; Yin, 2012], although the most recently proposed implementation [Guin *et al.* 2014] is not universal and its structure must be adapted to the type (analog, digital, or mixed) and size of the chip. Nonetheless, it seems that the security goal is still at a distance of being achieved, as a complete characterization of arbiter PUFs was demonstrated in [Tajik *et al.* 2014] using backside photonic emission analysis, with the claim that this method is applicable to all delay-based PUFs.

Several publications treat of SRAM-based Physical Unclonable Functions [Boehm & Hofer, 2009; Bohm *et al.* 2011; Cortez *et al.* 2012; Guajardo *et al.* 2007; 2008; Holcomb *et al.* 2007; 2009; Kim *et al.* 2010; 2011; Koeberl *et al.* 2012; Maes *et al.* 2009; Saxena & Voris, 2011; Schrijen & van der Leest, 2012; Selimis *et al.* 2011; van der Leest *et al.* 2012]. This compact security method takes advantage of existing static random access memory cells (cells that hold data as long as power is supplied) that take consistently at power-up one of two arbitrary stable states, 0 and 1. One particular memory cell arrives at a state, always the same, determined by the manufacture process. A challenge is a subset of these memory cells; the response is their respective power-up state. Not all FPGAs offer uninitialized SRAM memory, and the idea is adapted with Butterfly Physical Unclonable Functions (BPUFs) that use cross-coupled latches, do not require any power-up for assessment, and are appropriate for all sorts of FPGAs [Kumar *et al.* 2008]. However latch-based PUFs are less robust to temperature variations than SRAM PUFs [Katzenbeisser *et al.* 2012].

In any case, settling-state-based PUFs such as SRAM and BPUFs lack the level of security expected from a PUF, as SRAM PUFs have been characterized by FIB circuit edit and laser stimulation, and cloned [Helfmeier *et al.* 2013; Nedospasov *et al.* 2013].

More recent popular PUF developments at the chip level include the following:

(1) Glitch PUFs relying on delays, use glitches in combinatorial logic circuits [Anderson, 2010; Suzuki & Shimizu, 2010; Shimizu *et al.* 2012; Yamamoto *et al.* 2012].

(2) Secret Model PUFs associated with physical PUFs, mimic the PUF challenge-response activities, lessening the required amount of storage for challenge-response pairs [Devadas, 2014; Kong *et al.* 2014; Majzoobi *et al.* 2009; Majzoobi & Koushanfar, 2011].

(3) Public PUFs or PPUFs, defined as "multiple-input–multiple-output systems that are much faster to execute than they are to simulate, and whose security no longer relies on the secrecy of their physical parameters as PUFs do" [Potkonjak & Goudar, 2014], can be modeled, but the model evaluation requires much more work and time than the evaluation of the PUF itself [Majzoobi *et al.* 2009; Potkonjak & Goudar, 2014; Beckmann & Potkonjak, 2009; Meguerdichian & Potkonjak, 2011; Rajendran *et al.* 2012; Wendt & Potkonjak, 2011]. The same idea appears in SIMPL systems (Simulation Possible but Laborious systems) [Rührmair, 2009; Rührmair *et al.* 2010; Rührmair, 2011; 2012].

A concept completely different from PUFs, the Secure Split-Test (SST) [Contreras *et al.* 2013] proposes to place two blocks, a functional-locking block to guarantee that only ICs unlocked by the intellectual property (IP) owner have correct functionality and a scan-locking block to ensure that functional results cannot be scanned out and subsequently allow tampering with the protection hardware. In addition to the area overhead created by the additional blocks, the multiple exchanges between the IP owner and the foundry will add to the SST cost.

In the particular case of recycled ICs, i.e. components that are defective or used originals sold as new and working out of specification, the natural course of action is to find a way to compare them to non-defective, unused chips. The absence of functional defect is ascertained through extensive testing. Once established that an IC is fully functional, the other parameter is its “length of service.” The circuit aging concept, first used for reliability assessment, has been recently applied to combat IC recovery by a research group in Connecticut. First, they proposed a comparison between two ring oscillators, the first a reference free of stress and the second a stressed ring aging rapidly [Zhang *et al.* 2012]: the larger the difference between the rings frequency, the older the chip. The effects of temperature and inter-chip process variations are filtered out by data analysis. The two rings create minimal overhead and because they are bound to each other their relative frequency cannot be tampered with. Next, using instead the delay distribution of paths, the same researchers completely eliminate the area overhead [Zhang *et al.* 2012; Tuzzio *et al.* 2012]. Indeed, the delay distribution being within a certain range, a larger delay indicates an older IC. This implementation is also applicable to legacy ICs and is completely tamper-proof, since it uses inherent properties of the circuit. However, with large process variations sufficient accuracy can be difficult to attain. A third embodiment uses counters to record usage time and an embedded antifuse memory block to store the recorded values [Zhang & Tehranipoor, 2014]. The memory block cannot be reprogrammed, which makes it tamper-evident.

Another group compares the aging between similar parts of one circuit to create a signature [Zheng *et al.* 2014], a method also applicable to legacy chips.

In the next subsection, we will consider package-specific security solutions.

4.2 *Package-level security*

4.2.1 Anti-tamper. Protection has been often envisioned to be added as one or several supplementary layers, including extra circuitry for a response to tampering. For example, plates connected together and having serpentine or meandering conductor paths on them could be used as protective shielding against invasive or side-channel attacks [Cohen & Aviv, 2005; Farooq *et al.* 2007; Kleijne, 1986; Richards *et al.* 2013]. In other models, top and metal layers could be made more difficult and slower to etch than the passivation layer and the active circuitry [Byrne, 1994], bonded substrates could support memory detectors on their external face [Mori, 1994], or an adhesive layer covered with porous material could send an electrical signal when torn [Chan *et al.* 2010]. Other examples would modify the packaging using a molding compound in which a change in capacitance or impedance would be detected by some circuitry [Cole & Yakura, 1999; Thornley *et al.* 2011], add magnetic components to produce a magnetic response in elements situated on the target IC [Knudsen, 2010], or place reservoirs containing fluid chemicals that would destroy a circuit under reverse engineering attack [Das *et al.* 2012; Katti *et al.* 2014]. In another solution, a conductor is tightly wound around the protected IC and a detection circuit, all packaged together in a solid epoxy rendering the wires invisible from the outside; the winding of two devices is not exactly the same, even though they come from the same fabrication process [Weingart, 1987]. However, this type of housing has the drawback of being complicated to build and consequently expensive to produce.

4.2.2 Authentication. Active research has been conducted for the past few years to tag ICs with biological deoxyribonucleic acid (DNA). According to its proponents, the DNA signature is practically impossible to replicate, is inexpensive, requires only minimal change in the fabrication process, and is extremely accurate, the probability of a false positive authentication being one in a trillion [Hayward & Meraglia, 2011]. It consists in an ink containing shuffled plant DNA to produce a quaternary sequence unique to each IC chip and kept in a database. This ink also fluoresces under certain light frequencies. The product derived from this research, SigNature® DNA, is marketed by Applied DNA Science and has been used on microchips by the Department of Defense [Defense Logistics Agency, 2012; Applied DNA Sciences, 2013]. However, DNA is known for its sensitivity to harsh conditions [Lindahl, 1993], and the Semiconductor Industry Association (SIA) has shown reluctance to accept this technology as a general IC marking solution. The SIA does not believe SigNature DNA to be as reliable as presented, as it has not been independently evaluated or tested on a wide variety of products of different origins [SIA, 2012].

4.2.3 Anti-tamper with authentication. Other package security methods are armed with protection devices offering both tamper evidence and authentication capability.

The most widely known electromagnetic protection is probably the hologram [Reynolds *et al.* 1989], a type of diffractive optically variable image device (DOVID), often seen on smart cards. A hologram is a 3D picture showing different perspectives depending on its position with respect to the viewer, in an effect called parallax. Hidden and apparent authentication mechanisms can cohabit on a hologram. When positioned at the seal point of a package, a hologram also acts as a tamper-evidence device. However, available instruments are able to resolve conventional holograms in a matter of days [Gale, 1997; McGrew, 1990] and more sophisticated added nanoscale features, for example those operating in the near-field regime [Naruse *et al.* 2012] will probably be at the reach of state-of-the-art cloning apparatus as well.

PUFs, intrinsically tamper-resistant, are also used for authentication at the package level.

An optical PUF was suggested by Pappu, made of a transparent material, in which light scattering particles were inserted at random in the course of fabrication. When hit by a laser beam, the device would produce a speckle pattern, and minor variations in the location of just a few particles from one device to another would noticeably modify their whole interference patterns. In this implementation, the challenge set would be the position, angle amplitude and wavelength of the laser, and the response would be the speckle pattern [Pappu *et al.* 2002]. Although fabrication of the light scattering token itself is a low-cost process, the depicted PUF involved pricey and sizeable equipment comprising a laser and a precise mechanical positioning system. The relative position of the laser, token and image sensor should be exactly the same every time the speckle pattern is recorded. Other authors [Gassend, 2003]; [Tuyls & Škorić, 2006; Tuyls & Škorić, 2007; Rührmair *et al.* 2013] suggested an integrated version of the optical PUF where the incidence angle parameter would be replaced by the number of lasers that would be turned on or by switchable display pixels in a second embodiment. However in all cases, the smallest change in the token due to normal usage or environmental variations would change the speckle pattern and result in a false alert.

A magnetic PUF has been applied for card authentication, taking advantage of the noise-like permanent characteristics of magnetic stripes. The magnetic particles forming the stripes are of different sizes and shapes, randomly assembled, and emit an unchanging and unique background signal [Hart *et al.* 2013; Indeck & Muller, 1997; MagTek; Morley *et al.* 2007]. Card readers must be adapted for the use of this magnetic PUF, which affects its cost.

Another type of PUF for package authentication might be created using an array of nanorods. During the development of an assembling method to form gold nanorods on a nanostructured surface, it was noted that although the same array pattern could be repeated, the individual nanorods varied slightly in length, orientation and separation with the previous nanorod in the array. This translated into a shift in color and intensity in their far-field imaging [Slaughter *et al.* 2010; Kuemin *et al.* 2012]. Silver nanowires exhibit polarization-dependent surface-enhanced Raman scattering, that offers covert authentication because encrypted in the nanostructure [Zhang & Tehranipoor, 2014].

Radio-Frequency Identification (RFID) labels [Tuyls & Batina, 2006] allow–as opposed to a conventional bar code–automatic identification of a tag from a distance with no line-of-sight necessary with the reader [Want, 2006; Shepard, 2005; Roberts, 2006]. The tag is an antenna/microchip assembly and the reader is a second antenna emitting radio-frequency waves and receiving a response signal with information from the tag. However, by itself the tag is subject to easy cloning, which is why it is being associated with Coating Physical Unclonable Functions (COPUFs) or delay-based PUFs [Tuyls & Batina, 2006; Bolotnyy & Robins, 2007; Devadas *et al.* 2008; Jin *et al.* 2012; Kulseng *et al.* 2010; Ranasinghe *et al.* 2004] to form an "unclonable" tamper-evident RFID tag. COPUFs [Tuyls *et al.* 2006; Skoric *et al.* 2006; 2007], which use a protection layer shielding an IC, are attractive because of their low manufacturing cost. The coating film contains dielectric particles that are random as to their dimensions, shape, and location. Metal line sensors arranged underneath the protective layer like a comb are employed to determine the local capacitance of the coating. These capacitances are random because of the random properties of the particles in the coating, and constitute the responses to voltage challenges, each of different frequency and amplitude. Coating PUFs allow the detection of physical tampering, as a result of changes in the local responses, as well as device authentication. An insulating layer between the COPUF aluminum lines and the IC underneath, acts as a barrier against crosstalk between sensors and protected circuit. However, these additional metal and insulation layers create a sizeable packaging overhead; and because the sensors have to be constantly active, power consumption is significantly increased.

A method suggested by Fievre *et al*. uses coupled subwavelength gratings (CSWGs) [Rogers *et al*. 2009; 2011] in which engineering defects are exploited to create "fingerprints" for device chips, and allow verification of identity in addition to tamper evidence [Fievre *et al*. 2014]. A slight variation of one of the grating patterns in the pair of coupled gratings differentiates this specific set of gratings from another one, while the general output of each system remains essentially the same. This feature translates into variations in the intensity pattern of transmitted waves, distinguishing one device from another. Although reminiscent of the optical PUF in [Pappu *et al*. 2002], this new optical implementation circumvents the misalignment challenges that would necessitate bulky positioning equipment. This is accomplished by the use of an optical fiber as delivery medium. This solution also provides tamper evidence in addition to authentication, which is a step forward from the currently used DNA taggant [Hayward & Meraglia, 2011]. The tamper evidence aspect is ensured by the fact that the slightest intrusion attempt will either break the original near-field coupling between the gratings or modify the far-field intensity map.

Table 2 provides a summary of the security solutions examined in this survey.

5 Conclusion

Compiling the contribution of numerous researchers in the area of integrated circuit security, this paper explains the challenges with IC protection. One may encounter different types of attacks:

Table 2. Summary of security solutions.

Security solution	Protection
Fuses	Counter advanced invasive attacks such as laser cutting or FIB
Change of element characteristics and camouflage	Make usual invasive test methods useless
Logic hardening	Hardens circuit against noninvasive and semi-invasive attacks
Tiling	Authenticates without effect on performance, timing or power of FPGA
Post-manufacture programming	Allows metering when counterfeiting is discovered
Silicon PUFs	Authenticate thanks to a unique volatile pattern that cannot be duplicated (or take too long to simulate in the case of PPUF), are destroyed by physical tampering
Secure Split-Test (SST)	Guarantees that only ICs unlocked by IP owner have correct functionality and prevents tampering with the protection hardware
Aging	Allows identification of recovered ICs, is tamper evident
Shielding	Protects the IC with a tamper-proof enclosure
SigNature DNA	Offers unique sequences for authentication
Holograms	Offer covert or overt authentication, are tamper-evident when placed at seal point of package
Magnetic PUF	Offers a unique fingerprint for authentication, is tamper evident
Optical PUF	Offers a unique pattern for authentication with complex output and hard modeling, is tamper evident
Nanorod/nanowire arrays	Translate into a possibly covert, unique shift in color and intensity in their far-field imaging for authentication, are tamper evident
RFID + COPUF	Allows identification from a distance, no line-of-sight necessary, is tamper evident
CSWGs	Provides tamper evidence and authentication without the need to open a package

invasive, noninvasive, semi-invasive, or Trojan. This distinction in attack type constitutes one basis for an anti-tamper classification system, but others exist, and amongst them are the IBM security levels and the FIPS 104-2 standards. For this review, a new classification system is presented, based on the location of the protection, which can be on the chip itself or on the package, and also on the aspect of protection: anti-tamper or authentication. IC security techniques for anti-tamper or authentication at chip level and at package level are discussed and summarized.

One's outlook should consider the increased focus this past decade on 3D Heterogeneous Systems on a Chip (3D-HSoC) [Bhansali *et al.* 2004; Lewis & Lee, 2007; Jain *et al.* 2005; Chapman *et al.* 2004; Lewis *et al.* 2009; Chapman *et al.* 2005; Jain & Chapman, 2006; 2010; Bhansali *et al.* 2005; Jain & Chapman, 2011; Jiang *et al.* 2009; Marinissen *et al.* 2010; Wu *et al.* 2010; Jiang *et al.* 2009] and the explosion of wearable devices that carry a lot of personal information [Jovanov *et al.* 2005; Milenković *et al.* 2006; Li *et al.* 2010; Ng *et al.* 2006; Al Ameen *et al.* 2012; Cao *et al.* 2009; Patel & Wang, 2010; Huang *et al.* 2009; Lim *et al.* 2010; Chen *et al.* 2011; Latré *et al.* 2011; Hall & Hao, 2006; Ullah *et al.* 2012]. These chips are custom-produced in small quantities and hence carefully controlled. A usual way of inspecting them is to open the package, study individual chips, and then repackage the device for reintegration into the supply chain. Nevertheless, with the security and privacy issues entailed with these systems, there has been a growing recognition of the need to burry passive covert tamper-evident solutions in packages to provide clues in the instance the initial technologies would be compromised. The prospect of generalized use of Systems on a Chip (SOCs) and wearable devices makes it useful to examine the research directions applicable to the security of these types of ICs. A mandatory attribute for SOCs and wearable devices is compactness. However, the most critical aspects of these chips being sensitive information protection and reliability, it is paramount to ally anti-tampering with device authentication. A single solution offering both security features would be preferable to respect the compactness requirement. Additionally, it would be very convenient if one did not need to access the IC itself to check if it has been tampered with or to authenticate it, the packaging giving all this information. With the stealth nature of the security desired, the newer optical means such as nanowire arrays or CSWGs might be of choice.

References

Abraham, D.G., *et al.* (1991) "Transaction security system." *IBM Systems Journal*. **30**, 206–229.

Abramovici, M. and Bradley, P. "Integrated circuit security: new threats and solutions," in *Proceedings of the 5th Annual Workshop on Cyber Security and Information Intelligence Research: Cyber Security and Information Intelligence Challenges and Strategies*, 2009, p. 55.

Adee, S. (2008) "The hunt for the kill switch." *Spectrum IEEE*. **45**, 34–39.

Agrawal, D., *et al.* (2003) "The EM side—channel (s)," in *Cryptographic Hardware and Embedded Systems-CHES 2002*, ed: Springer, pp. 29–45.

Agrawal, D., *et al.* (2007) "Trojan detection using IC fingerprinting," in *Security and Privacy, 2007. SP'07. IEEE Symposium on*, pp. 296–310.

Ajluni, C. (1995) "2 New imaging techniques promise to improve IC defect identification." *Electronic Design*. **43**, 37–38.

Al Ameen, M., *et al.* (2012) "Security and privacy issues in wireless sensor networks for healthcare applications." *Journal of Medical Systems*. **36**, 93–101.

Ambrose, J.A., *et al.* (2011) "Multiprocessor information concealment architecture to prevent power analysis-based side channel attacks." *IET computers & digital techniques*. **5**, 1–15.

Anderson, J.H. "A PUF design for secure FPGA-based embedded systems," in *Proceedings of the 2010 Asia and South Pacific Design Automation Conference*, 2010, pp. 1–6.

Anderson, M.S., *et al.* (2008) "Towards Countering the Rise of the Silicon Trojan," Defence Science and Technology, Edinburgh (Australia).

Anderson, R. and Kuhn, M. "Tamper resistance-a cautionary note," in *Proceedings of the second Usenix workshop on electronic commerce*, 1996, pp. 1–11.

Anderson, R. and Kuhn, M. (1998) "Low cost attacks on tamper resistant devices," in *Security Protocols*, 1998, pp. 125–136.

Applied DNA Sciences, "Applied DNA Sciences Successfully Marks Mission-Critical Microchips for the Department of Defense," ed: applieddnasciences, 2013.

Balasch, J., *et al.* "An In-depth and Black-box Characterization of the Effects of Clock Glitches on 8-bit MCUs," in *Fault Diagnosis and Tolerance in*

Cryptography (FDTC), 2011 Workshop on, 2011, pp. 105–114.

Bar-El, H., *et al.* (2006) "The sorcerer's apprentice guide to fault attacks." *Proceedings of the IEEE*. **94**, 370–382.

Baukus, J.P., *et al.* "Camouflaged circuit structure with step implants," 5,973,375, 1999.

Baukus, J.P., *et al.* "Digital circuit with transistor geometry and channel stops providing camouflage against reverse engineering," US 6,064,110 A, 2000.

Baukus, J.P., *et al.* "Secure integrated circuit," US 6,294,816 B1, 2001.

Baukus, J.P., *et al.* "Programmable connector/isolator and double polysilicon layer CMOS process with buried contact using the same," US 6,893,916 B2, 2005.

Baukus, J.P., *et al.* "Camouflaging a standard cell based integrated circuit," US 81,512,35 B2, 2012.

Beckmann, N. and Potkonjak, M. "Hardware-based public-key cryptography with public physically unclonable functions," in *Information Hiding*, 2009, pp. 206–220.

Bellare, M., *et al.* "Foundations of garbled circuits," in *Proceedings of the 2012 ACM conference on Computer and communications security*, 2012, pp. 784–796.

Belva Martin, A.-M.F., *et al.* (2010) "Mitigating the Risk of Counterfeit Parts." *Journal of the IEST*. **53**, 5–17.

Bhansali, S., *et al.* "3D heterogeneous sensor system on a chip for defense and security applications," in *Defense and Security*, 2004, pp. 413–424.

Bhansali, S., *et al.* "Inter-layer vias and TESH interconnection network for 3-D heterogeneous sensor system on a chip," in *Proc. of SPIE Vol*, 2005, p. 307.

Bhunia, S., *et al.* (2013) "Protection Against Hardware Trojan Attacks: Towards a Comprehensive Solution." *IEEE Design & Test*. **30**, 6–17.

Bhunia, S., *et al.* (2014) "Hardware Trojan Attacks: Threat Analysis and Countermeasures." *Proceedings of the IEEE*. **102**, 1229–1247.

Bin, H., *et al.* "A Multiple Bits Output Ring-Oscillator Physical Unclonable Function," in *Intelligent Signal Processing and Communications Systems (ISPACS), 2011 International Symposium on*, 2011, pp. 1–5.

Boehm, C. and Hofer, M. "Using srams as physical unclonable functions," in *Proceedings of the 17th Austrian Workshop on Microelectronics-Austrochip*, 2009, pp. 117–122.

Bohm, C., *et al.* "A microcontroller sram-puf," in *Network and System Security (NSS), 2011 5th International Conference on*, 2011, pp. 269–273.

Bolotnyy, L. and Robins, G. "Physically unclonable function-based security and privacy in RFID systems," in *Pervasive Computing and Communications, 2007. PerCom'07. Fifth Annual IEEE International Conference on*, 2007, pp. 211–220.

Boneh, D., *et al.* "On the importance of checking cryptographic protocols for faults," in *Advances in Cryptology—EUROCRYPT'97*, 1997, pp. 37–51.

Bucci, M., *et al.* (2011) "Delay-based dual-rail precharge logic." *Very Large Scale Integration (VLSI) Systems, IEEE Transactions on*. **19**, 1147–1153.

Byrne, R.C. "Tamper resistant integrated circuit structure," 5,369,299, 1994.

Cao, H., *et al.* (2009) "Enabling technologies for wireless body area networks: A survey and outlook." *Communications Magazine, IEEE*. **47**, 84–93.

Chakraborty, R.S., *et al.* "Hardware Trojan: Threats and emerging solutions," in *High Level Design Validation and Test Workshop, 2009. HLDVT 2009. IEEE International*, 2009, pp. 166–171.

Chan, K., *et al.* "Tamper respondent system," US 7,787,256 B2, 2010.

Chapman, G.H., *et al.* "Defect avoidance in a 3-D heterogeneous sensor [acoustic/seismic/active pixel/IR imaging sensor array]," in *Defect and Fault Tolerance in VLSI Systems, 2004. DFT 2004. Proceedings. 19th IEEE International Symposium on*, 2004, pp. 67–75.

Chapman, G.H., *et al.* "Inter-plane via defect detection using the sensor plane in 3D heterogeneous sensor systems," in *Defect and Fault Tolerance in VLSI Systems, 2005. DFT 2005. 20th IEEE International Symposium on*, 2005, pp. 158–166.

Chen, M., *et al.* (2011) "Body area networks: A survey." *Mobile Networks and Applications*. **16**, 171–193.

Chen, Q., *et al.* "The bistable ring puf: A new architecture for strong physical unclonable functions," in *Hardware-Oriented Security and Trust (HOST), 2011 IEEE International Symposium on*, 2011, pp. 134–141.

Chow, L.-W., *et al.* "Integrated circuits protected against reverse engineering and method for fabricating the same using vias without metal terminations," US 6,791,191 B2, 2004.

Chow, L.-W., *et al.* "Integrated circuits protected against reverse engineering and method for fabricating the same using an apparent metal contact line terminating on field oxide," US 7,294,935 B2, 2007.

Chow, L.-W., *et al.* "Use of silicon block process step to camouflage a false transistor," US 7,344,932 B2, 2008.

Chow, L.-W., *et al.* "Covert transformation of transistor properties as a circuit protection method," US 7,541,266 B2, 2009.

Chow, L.-W., *et al.* "Symmetric non-intrusive and covert technique to render a transistor permanently non-operable," US 8,049,281 B1, 2011.

Chow, L.-W., *et al.* "Conductive channel pseudo block process and circuit to inhibit reverse engineering," US Patent 8,258,583, 2012.

Ciccone, J.C. and Yup, B.L. "Standard cell power-on-reset circuit," US 6,173,436 B1, 2001.

Clark, W.M. Jr., *et al.* "Implanted hidden interconnections in a semiconductor device for preventing reverse engineering," US 7,166,515 B2, 2007.

Clark, W.M. Jr., *et al.* "Programmable connection and isolation of active regions in an integrated circuit using ambiguous features to confuse a reverse engineer," US 8,168,487 B2, 2012.

Cocchi, R.P., *et al.* "Method and apparatus for camouflaging a standard cell based integrated circuit with micro circuits and post processing," US 8,510,700 B2, 2013.

Cohen, Y. and Aviv, A. "Anti-tampering enclosure for electronic circuitry," USA Patent US 6,853,093 B2, 2005.

Cole, R.K. and Yakura, J.P. "Method and apparatus for protecting functions imbedded within an integrated circuit from reverse engineering," 5,861,652, 1999.

Committee on Armed Services, "Inquiry into Counterfeit Electronic Parts in the Department of Defense Supply Chain," United States Senate, Washington, DC2012.

Contreras, G.K., *et al.* "Secure split-test for preventing ic piracy by untrusted foundry and assembly," in *Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT), 2013 IEEE International Symposium on*, 2013, pp. 196–203.

Cortez, M., *et al.* "Modeling SRAM start-up behavior for Physical Unclonable Functions," in *Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT), 2012 IEEE International Symposium on*, 2012, pp. 1–6.

Das, R.N., *et al.* "Anti-tamper microchip package based on thermal nanofluids or fluids," US8288857 B2, 2012.

Defense Logistics Agency, "Dna authentication marking on items in fsc 5962," D. o. Defense, Ed., ed. Columbus, OH, 2012.

Dehbaoui, A., *et al.* "Electromagnetic transient faults injection on a hardware and a software implementations of aes," in *Fault Diagnosis and Tolerance in Cryptography (FDTC), 2012 Workshop on*, 2012, pp. 7–15.

Devadas, S., *et al.* "Design and Implementation of PUF-Based "Unclonable" RFID ICs for Anti-Counterfeiting and Security Applications," in *RFID, 2008 IEEE International Conference on*, 2008, pp. 58–64.

Devadas, S. "Non-networked RFID-PUF authentication," US8683210 B2, 2014.

Dhem, J.-F., *et al.* "A practical implementation of the timing attack," in *Smart Card Research and Applications*, 2000, pp. 167–182.

Dictionary, O.E. "'tamper, v.1' II.5," in *Oxford English Dictionary*, ed: Oxford University Press, 2015.

Dictionary, O.E. "'counterfeit, v.' 1.b.," in *Oxford English Dictionary*, ed: Oxford University Press, 2015.

Endo, S., *et al.* (2011) "An on-chip glitchy-clock generator for testing fault injection attacks." *Journal of Cryptographic Engineering*. **1**, 265–270.

Farooq, M.G., *et al.* "Method and structure for implementing secure multichip modules for encryption applications," USA Patent US7281667 B2, 2007.

Fievre, A.M.P., *et al.* (2014) "Effect of beam size, finite number of lines, and rotational misalignment on coupled subwavelength gratings." *JOSA A*, **31**, 2603–2609.

Frontier, "Estimating the global economic and social impacts of counterfeiting and piracy," Report Commissioned by Business Action to Stop Counterfeiting and Piracy (BASCAP) 2011.

Gale, M.T. (1997) "Replication techniques for diffractive optical elements." *Microelectronic Engineering*. **34**, 321–339.

Gandolfi, K., *et al.* "Electromagnetic analysis: Concrete results," in *Cryptographic Hardware and Embedded Systems—CHES 2001*, 2001, pp. 251–261.

Gassend, B., *et al.* "Silicon physical random functions," in *Proceedings of the 9th ACM conference on Computer and communications security*, 2002, pp. 148–160.

Gassend, B., *et al.* (2004) "Identification and authentication of integrated circuits." *Concurrency and Computation: Practice and Experience*. **16**, 1077–1098.

Gassend, B.L. "Physical random functions," Massachusetts Institute of Technology, 2003.

Goldwasser, S., *et al.* "One-time programs," in *Advances in Cryptology–CRYPTO 2008*, ed: Springer, 2008, pp. 39–56.

Guajardo, J., *et al.* "FPGA intrinsic PUFs and their use for IP protection," in *Cryptographic Hardware and Embedded Systems-CHES 2007*, ed: Springer, 2007, pp. 63–80.

Guajardo, J., *et al.* "Brand and IP protection with physical unclonable functions," in *Circuits and Systems, 2008. ISCAS 2008. IEEE International Symposium on*, 2008, pp. 3186–3189.

Guin, U., *et al.* "Anti-Counterfeit techniques: from design to resign," *Microprocessor test and verification (MTV)*, 2013.

Guin, U., *et al.* (2014) "Counterfeit Integrated Circuits: A Rising Threat in the Global Semiconductor Supply Chain." *Proceedings of the IEEE*. **102**, 1207–1228.

Guin, U., *et al.* "Low-cost On-Chip Structures for Combating Die and IC Recycling," in *Proceedings of the The 51st Annual Design Automation Conference on Design Automation Conference*, 2014, pp. 1–6.

Hall, P.S. and Hao, Y. "Antennas and propagation for body centric communications," in *Antennas and Propagation, 2006. EuCAP 2006. First European Conference on*, 2006, pp. 1–7.

Hart, A.D., *et al.* "Card authentication system," US8447991 B2, 2013.

Hayward, J.A. and Meraglia, J. "DNA to Safeguard Electrical Components and Protect Against Counterfeiting and Diversion," in *ISTFA 2011: Conference Proceedings from the 37th International Symposium for Testing and Failure Analysis*, *November 13017*, *2011*, *San Jose Convention Center*, *San Jose*, *California*, *USA*, 2011, pp. 238–241.

Helfmeier, C., *et al.* "Cloning physically unclonable functions," in *Hardware-Oriented Security and Trust (HOST)*, *2013 IEEE International Symposium on*, 2013, pp. 1–6.

Hoang, A.-T. and Fujino, T. (2014) "Intra-Masking Dual-Rail Memory on LUT Implementation for SCA-Resistant AES on FPGA." *ACM Transactions on Reconfigurable Technology and Systems (TRETS)*. **7**, 10:1–19.

Holcomb, D.E., *et al.* "Initial SRAM state as a fingerprint and source of true random numbers for RFID tags," in *Proceedings of the Conference on RFID Security*, 2007.

Holcomb, D.E., *et al.* (2009) "Power-up SRAM state as an identifying fingerprint and source of true random numbers." *Computers*, *IEEE Transactions on*. **58**, 1198–1210.

Hsu, L.L., *et al.* "Techniques for Impeding Reverse Engineering," US Patent 20,130,052,822, 2013.

Huang, Y., *et al.* "Faster Secure Two-Party Computation Using Garbled Circuits," in *USENIX Security Symposium*, 2011.

Huang, Y., *et al.* "Private set intersection: Are garbled circuits better than custom protocols?," in *19th Network and Distributed Security Symposium*, San Diego, 2012.

Huang, Y.-M., *et al.* (2009) "Pervasive, secure access to a hierarchical sensor-based healthcare monitoring architecture in wireless heterogeneous networks." *Selected Areas in Communications*, *IEEE Journal on*. **27**, 400–411.

Indeck, R.S. and Muller, M.W. "Method and apparatus for secure data storage and manipulation using magnetic media," US5625689 A, 1997.

Jain, V. and Chapman, G.H. "Defect tolerant and energy economized DSP plane of a 3-D heterogeneous SoC," in *Defect and Fault Tolerance in VLSI Systems*, *2006. DFT'06. 21st IEEE International Symposium on*, 2006, pp. 157–165.

Jain, V.K., *et al.* "A highly reconfigurable computing array: DSP plane of a 3D heterogeneous SoC," in *SOC Conference*, *2005. Proceedings. IEEE International*, 2005, pp. 243–246.

Jain, V.K. and Chapman, G.H. "Massively deployable intelligent sensors for the smart power grid," in *Defect and Fault Tolerance in VLSI Systems (DFT)*, *2010 IEEE 25th International Symposium on*, 2010, pp. 319–327.

Jain, V.K. and Chapman, G.H. "Enhanced Defect Tolerance Through Matrixed Deployment of Intelligent Sensors for the Smart Power Grid," in *Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT)*, *2011 IEEE International Symposium on*, 2011, pp. 235–242.

Järvinen, K., *et al.* "Garbled circuits for leakage-resilience: Hardware implementation and evaluation of one-time programs," in *Cryptographic Hardware and Embedded Systems*, *CHES 2010*, ed: Springer, 2010, pp. 383–397.

Jiang, L., *et al.* "Layout-driven test-architecture design and optimization for 3D SoCs under pre-bond test-pin-count constraint," in *Proceedings of the 2009 International Conference on Computer-Aided Design*, 2009, pp. 191–196.

Jiang, L., *et al.* "Test architecture design and optimization for three-dimensional SoCs," in *Proceedings of the Conference on Design*, *Automation and Test in Europe*, 2009, pp. 220–225.

Jin, Y., *et al.* "PUF-Based RFID authentication protocol against secret key leakage," in *Web Technologies and Applications*, ed: Springer, 2012, pp. 318–329.

Jovanov, E., *et al.* (2005) "A wireless body area network of intelligent motion sensors for computer assisted physical rehabilitation." *Journal of NeuroEngineering and rehabilitation*. **2**, 6.

Karaklajic, D., *et al.* (2013) "Hardware Designer's Guide to Fault Attacks." *Very Large Scale Integration (VLSI) Systems*, *IEEE Transactions on*. **21**, 2295–2306.

Karri, R., *et al.* (2010) "Trustworthy hardware: Identifying and classifying hardware trojans," *Computer*. 39–46.

Katti, R.R., *et al.* "Tamper-resistant MRAM utilizing chemical alteration," US8730715 B2, 2014.

Katzenbeisser, S., *et al.* "PUFs: Myth, fact or busted? A security evaluation of physically unclonable functions (PUFs) cast in silicon," in *Cryptographic Hardware and Embedded Systems–CHES 2012*, ed: Springer, 2012, pp. 283–301.

Kim, C.H. and Quisquater, J.-J. (2007) "Faults, injection methods, and fault attacks." *Design & Test of Computers*, *IEEE*. **24**, 544–545.

Kim, J., *et al.* "Toward reliable SRAM-based device identification," in *Computer Design (ICCD)*, *2010 IEEE International Conference on*, 2010, pp. 313–320.

Kim, J., *et al.* "System accuracy estimation of SRAM-based device authentication," in *Design Automation Conference (ASP-DAC)*, *2011 16th Asia and South Pacific*, 2011, pp. 37–42.

Kleijne, T.A. "Security device for the secure storage of sensitive data," 4,593,384, 1986.

Knudsen, C.J. "Tamper-resistant packaging and approach using magnetically-set data," US 7,685,438 B2, 2010.

Kocher, P., *et al.* "Differential power analysis," in *Advances in Cryptology—CRYPTO'99*, 1999, pp. 388–397.

Kocher, P.C. "Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems," in *Advances in Cryptology—CRYPTO'96*, 1996, pp. 104–113.

Koeberl, P., *et al.* (2012) "A practical device authentication scheme using SRAM PUFs." *Journal of Cryptographic Engineering*. **2**, 255–269.

Kong, J., *et al.* "PUFatt: Embedded Platform Attestation Based on Novel Processor-Based PUFs," in *Proceedings of the The 51st Annual Design Automation Conference on Design Automation Conference*, 2014, pp. 1–6.

Koushanfar, F., *et al.* (2001) "Intellectual property metering," in *Information Hiding*. 81–95.

Koushanfar, F., *et al.* "Can EDA combat the rise of electronic counterfeiting?," in *Proceedings of the 49th Annual Design Automation Conference*, 2012, pp. 133–138.

Kuemin, C., *et al.* (2012) "Oriented Assembly of Gold Nanorods on the Single-Particle Level." *Advanced Functional Materials.* **22**, 702–708.

Kulseng, L., *et al.* "Lightweight mutual authentication and ownership transfer for RFID systems," in *INFOCOM, 2010 Proceedings IEEE*, 2010, pp. 1–5.

Kumar, R., *et al.* "On Design of Temperature Invariant Physically Unclonable Functions Based on Ring Oscillators," in *VLSI (ISVLSI), 2012 IEEE Computer Society Annual Symposium on*, 2012, pp. 165–170.

Kumar, S.S., *et al.* "The butterfly PUF protecting IP on every FPGA," in *Hardware-Oriented Security and Trust, 2008. HOST 2008. IEEE International Workshop on*, 2008, pp. 67–70.

Lach, J., *et al.* (1998) "Fingerprinting digital circuits on programmable hardware," in *Information Hiding*. 16–31.

Latré, B., *et al.* (2011) "A survey on wireless body area networks." *Wireless Networks*. **17**, 1–18.

Lee, J.W., *et al.* "A technique to build a secret key in integrated circuits for identification and authentication applications," in *VLSI Circuits, 2004. Digest of Technical Papers. 2004 Symposium on*, 2004, pp. 176–179.

Lewis, D.L. and Lee, H.-H. (2007) "A scanisland based design enabling prebond testability in die-stacked microprocessors," in *Test Conference, 2007. ITC 2007. IEEE International*, pp. 1–8.

Lewis, D.L., *et al.* (2009) "High performance non-blocking switch design in 3D die-stacking technology," in *VLSI, 2009. ISVLSI'09. IEEE Computer Society Annual Symposium on*, pp. 25–30.

Li, M., *et al.* (2010) "Data security and privacy in wireless body area networks." *Wireless Communications, IEEE*. **17**, 51–58.

Lim, D., *et al.* (2005) "Extracting secret keys from integrated circuits." *Very Large Scale Integration (VLSI) Systems. IEEE Transactions on*. **13**, 1200–1205.

Lim, S., *et al.* "Security issues on wireless body area network for remote healthcare monitoring," in *Sensor Networks, Ubiquitous, and Trustworthy Computing (SUTC), 2010 IEEE International Conference on*, 2010, pp. 327–332.

Lindahl, T., (1993) "Instability and decay of the primary structure of DNA." *Nature*. **362**, 709–715.

Lineback, R. (2012) "Semiconductor R&D Spending to Hit Record-High $53.4 Billion in 2012," IC Insights September 4, 2012.

Lofstrom, K., *et al.* "IC identification circuit using device mismatch," in *Solid-State Circuits Conference, 2000. Digest of Technical Papers. ISSCC. 2000 IEEE International*, 2000, pp. 372–373.

Maes, R., *et al.* "Low-overhead implementation of a soft decision helper data algorithm for SRAM PUFs," in *Cryptographic Hardware and Embedded Systems-CHES 2009*, ed: Springer, 2009, pp. 332–347.

MagTek. Available: http://www.magneprint.com/

Maiti, A. and Schaumont, P. (2011) "Improved ring oscillator PUF: an FPGA-friendly secure primitive." *Journal of cryptology*. **24**, 375–397.

Maiti, A., *et al.* (2012) "A robust physical unclonable function with enhanced challenge-response set." *Information Forensics and Security, IEEE Transactions on*. **7**, 333–345.

Majzoobi, M. and Koushanfar, F. (2011) "Time-bounded authentication of FPGAs." *Information Forensics and Security, IEEE Transactions on*. **6**, 1123–1135.

Majzoobi, M., *et al.* (2008) "Testing techniques for hardware security," in *Test Conference, 2008. ITC 2008. IEEE International*, pp. 1–10.

Majzoobi, M., *et al.* (2009) "Techniques for design and implementation of secure reconfigurable PUFs." *ACM Transactions on Reconfigurable Technology and Systems (TRETS)*. **2**, 5:1–33.

Mangard, S., *et al.* *Power analysis attacks: Revealing the secrets of smart cards* Vol. 31: Springer, 2007.

Mansouri, S.S. and Dubrova, E. (2012) "Ring oscillator physical unclonable function with multi level supply voltages," in *Computer Design (ICCD), 2012 IEEE 30th International Conference on*, pp. 520–521.

Marinissen, E.J., *et al.* (2010) "A structured and scalable test access architecture for TSV-based 3D stacked ICs," in *VLSI Test Symposium (VTS), 2010 28th*, pp. 269–274.

Marzouqi, H., *et al.* (2014) "Review of gate-level differential power analysis and fault analysis countermeasures." *Information Security, IET*. **8**, 51–66.

McGrew, S.P. (1990) "Hologram counterfeiting: problems and solutions," in *OE/LASE'90*, Los Angeles, CA, pp. 66–76.

Meguerdichian, S. and Potkonjak, M. "Matched public PUF: ultra low energy security platform," in *Proceedings of the 17th IEEE/ACM international symposium on Low-power electronics and design*, 2011, pp. 45–50.

Merli, D., *et al.* "Improving the quality of ring oscillator PUFs on FPGAs," in *Proceedings of the 5th Workshop on Embedded Systems Security*, 2010.

Milenković, A., *et al.* (2006) "Wireless sensor networks for personal health monitoring: Issues and an implementation." *Computer communications*. **29**, 2521–2533.

Mori, R. "Tamper resistant module with logical elements arranged on a substrate to protect information stored in the same module," 5,309,387, 1994.

Morley, R.E. Jr., *et al.* "Method and apparatus for authenticating a magnetic fingerprint signal using an adaptive analog to digital converter," US7210627 B2, 2007.

Morrison, M. and Ranganathan, N. (2014) "Synthesis of Dual-Rail Adiabatic Logic for Low Power Security Applications." *Computer-Aided Design of Integrated Circuits and Systems*, *IEEE Transactions on*. **33**, 975–988.

Naruse, M., *et al.* (2012) "Optical security based on near-field processes at the nanoscale." *Journal of Optics*. **14**, 094002–94014.

Nedospasov, D., *et al.* (2013) "Invasive PUF analysis," in *Fault Diagnosis and Tolerance in Cryptography (FDTC)*, *2013 Workshop on*, pp. 30–38.

Ng, H., *et al.* (2006) "Security issues of wireless sensor networks in healthcare applications." *BT Technology Journal*. **24**, 138–144.

NIST, "FIPS 140-2: Security requirements for cryptographic modules," in *Information Technology Laboratory*, *National Institute of Standards and Technology*, ed, 2001.

Page, D. (2003) "Defending against cache-based side-channel attacks." *Information Security Technical Report*. **8**, 30–44.

Pappu, R., *et al.* (2002) "Physical one-way functions." *Science*. **297**, 2026–2030.

Patel, M. and Wang, J. (2010) "Applications, challenges, and prospective in emerging body area networking technologies." *Wireless Communications*, *IEEE*. **17**, 80–88.

Potkonjak, M. and Goudar, V. (2014) "Public physical unclonable functions." *Proceedings of the IEEE*. **102**, 1142–1156.

Qu, G. and Yin, C.-E. (2009) "Temperature-aware cooperative ring oscillator PUF," in *Hardware-Oriented Security and Trust*, *2009. HOST'09. IEEE International Workshop on*, pp. 36–42.

Quisquater, J.-J. and Samyde, D. "Electromagnetic analysis (ema): Measures and counter-measures for smart cards," in *Smart Card Programming and Security*, ed: Springer, 2001, pp. 200–210.

Rajendran, J., *et al.* (2012) "Nano-PPUF: A Memristor-based Security Primitive," in *VLSI (ISVLSI)*, *2012 IEEE Computer Society Annual Symposium on*, pp. 84–87.

Rajendran, J., *et al.* (2013) "Security analysis of integrated circuit camouflaging," in *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*, pp. 709–720.

Ranasinghe, D., *et al.* "Security and privacy: Modest proposals for low-cost RFID systems," in *Auto-ID Labs Research Workshop* Zurich, Switzerland, 2004.

Ratanpal, G.B., *et al.* (2004) "An on-chip signal suppression countermeasure to power analysis attacks." *Dependable and Secure Computing*, *IEEE Transactions on*. **1**, 179–189.

Reynolds, G.O., *et al. The new physical optics notebook: Tutorials in Fourier optics* Vol. 61: SPIE Optical Engineering Press New York, 1989.

Richards, B. and Footner, P. *The Role of microscopy in semiconductor failure analysis*: Oxford University Press, 1992.

Richard, H., *et al.* "Point of sale terminal having enhanced security," USA Patent, 2013.

Roberts, C.M. (2006) "Radio frequency identification (RFID)." *Computers & Security*. **25**, 18–26.

Rogers, A.-A., *et al.* (2011) "Verification of evanescent coupling from subwavelength grating pairs." *Applied Physics B*. **105**, 833–837.

Rogers, A.-A.A., *et al.* (2009) "Far-field evanescent wave propagation using coupled subwavelength gratings for a MEMS sensor." *JOSA A*. **26**, 2526–2531.

Rostami, M., *et al.* (2013) "Hardware security: Threat models and metrics," in *Proceedings of the International Conference on Computer-Aided Design*, pp. 819–823.

Rostami, M., *et al.* (2014) "A Primer on Hardware Security: Models, Methods, and Metrics." *Proceedings of the IEEE*. **102**, 1283–1295.

Rührmair, U., *et al.* (2010) "Modeling attacks on physical unclonable functions," in *Proceedings of the 17th ACM conference on Computer and communications security*, pp. 237–249.

Rührmair, U., *et al.* "Towards electrical, integrated implementations of SIMPL systems," in *Information Security Theory and Practices. Security and Privacy of Pervasive Systems and Smart Devices*, ed: Springer, 2010, pp. 277–292.

Rührmair, U., *et al.* "Optical PUFs Reloaded," IACR Cryptology ePrint Archive, Report 2013/2152013.

Rührmair, U. "SIMPL Systems: On a Public Key Variant of Physical Unclonable Functions," *IACR Cryptology ePrint Archive*, 2009, Vol. 2009.

Rührmair, U. "SIMPL systems, or: can we design cryptographic hardware without secret key information?," in *SOFSEM 2011: Theory and Practice of Computer Science*, ed: Springer, 2011, pp. 26–45.

Rührmair, U. "SIMPL systems as a keyless cryptographic and security primitive," in *Cryptography and Security: From Theory to Applications*, ed: Springer, 2012, pp. 329–354.

Saputra, H., *et al.* (2003) "Masking the energy behavior of DES encryption [smart cards]," in *Design, Automation and Test in Europe Conference and Exhibition, 2003*, pp. 84–89.

Saxena, N. and Voris, J. (2011) "Data remanence effects on memory-based entropy collection for RFID systems." *International Journal of Information Security*. **10**, 213–222.

Schmidt, J.-M., *et al.* (2009) "Optical fault attacks on AES: A threat in violet," in *Fault Diagnosis and Tolerance in Cryptography (FDTC), 2009 Workshop on*, pp. 13–22.

Schrijen, G.-J. and van der Leest, V. "Comparative analysis of SRAM memories used as PUF primitives," in *Proceedings of the Conference on Design, Automation and Test in Europe*, 2012, pp. 1319–1324.

Selimis, G., *et al.* "Evaluation of 90 nm 6T-SRAM as Physical Unclonable Function for secure key generation in wireless sensor nodes," in *Circuits and Systems (ISCAS), 2011 IEEE International Symposium on*, 2011, pp. 567–570.

Shepard, S. *RFID: radio frequency identification*: McGraw-Hill New York, 2005.

Shimizu, K., *et al.* (2012) "Glitch PUF: extracting information from usually unwanted glitches." *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*. **95**, 223–233.

SIA, "Public Comments – DNA Authentication Marking on Items in FSC5962," Semiconductor Industry Association, 2012.

Skoric, B., *et al.* (2006) "Information-theoretic analysis of capacitive physical unclonable functions." *Journal of Applied physics*. **100**, 024902.

Skoric, B., *et al.* "Experimental hardware for coating PUFs and optical PUFs," in *Security with Noisy Data*, ed: Springer, 2007, pp. 255–268.

Skorobogatov, S. and Woods, C. (2012) "Breakthrough Silicon Scanning Discovers Backdoor in Military Chip," *Cryptographic Hardware and Embedded Systems–CHES 2012*, pp. 23–40.

Skorobogatov, S. "Physical Attacks and Tamper Resistance," in *Introduction to Hardware Security and Trust*, ed: Springer, 2012, pp. 143–173.

Skorobogatov, S.P. and Anderson, R.J. "Optical fault induction attacks," in *Cryptographic Hardware and Embedded Systems-CHES 2002*, ed: Springer, 2003, pp. 2–12.

Skorobogatov, S.P. "Semi-invasive attacks-a new approach to hardware security analysis," *Technical report, University of Cambridge, Computer Laboratory*, 2005.

Slaughter, L.S., *et al.* (2010) "Effects of symmetry breaking and conductive contact on the plasmon coupling in gold nanorod dimers." *Acs Nano*. **4**, 4657–4666.

Soden, J.M., *et al.* (1997) "IC failure analysis: Magic, mystery, and science." *Design & Test of Computers, IEEE*. **14**, 59–69.

Springer, P.J. *Military robots and drones*: ABC-CLIO, 2013.

Standaert, F.-X. "Introduction to side-channel attacks," in *Secure Integrated Circuits and Systems*, ed: Springer, 2010, pp. 27–42.

Suh, G.E. and Devadas, S. "Physical unclonable functions for device authentication and secret key generation," in *Proceedings of the 44th annual Design Automation Conference*, 2007, pp. 9–14.

Suzuki, D. and Shimizu, K. "The glitch PUF: a new delay-PUF architecture exploiting glitch shapes," in *Cryptographic Hardware and Embedded Systems, CHES 2010*, ed: Springer, 2010, pp. 366–382.

Tajik, S., *et al.* "Physical Characterization of Arbiter PUFs," in *Cryptographic Hardware and Embedded Systems–CHES 2014*, ed: Springer, 2014, pp. 493–509.

Tehranipoor, M. and Koushanfar, F. (2010) "A Survey of Hardware Trojan Taxonomy and Detection." *Design & Test of Computers, IEEE*. **27**, 10–25.

Thornley, R.Q., *et al.* "Intrusion detection using a conductive material," US 8,004,419 B2, 2011.

Tiri, K. and Verbauwhede, I. "A logic level design methodology for a secure DPA resistant ASIC or FPGA implementation," in *Proceedings of the conference on Design, automation and test in Europe-Volume 1*, 2004, pp. 246–251.

Tsang, J.C., *et al.* (2000) "Picosecond imaging circuit analysis." *IBM Journal of Research and Development*. **44**, 583–603.

Tsang, Y.L. "Identification of Extension Implant Defect in Sub-Micron CMOS ICs-Analysis Technique, Model, and Solution," in *ISTFA 2011: Conference Proceedings from the 37th International Symposium for Testing and Failure Analysis, November 13–17, 2011*, San Jose Convention Center, San Jose, California, USA, 2011, pp. 212–217.

Tuyls, P. and Škorić, B. "Physical Unclonable Functions for enhanced security of tokens and tags," in *ISSE 2006—Securing Electronic Busines Processes*, ed: Springer, 2006, pp. 30–37.

Tuyls, P. and Škorić, B. "Strong authentication with physical unclonable functions," in *Security, Privacy, and Trust in Modern Data Management*, ed: Springer, 2007, pp. 133–148.

Tuyls, P. and Batina, L. "RFID-tags for Anti-Counterfeiting," in *Topics in Cryptology–CT-RSA 2006*, ed: Springer, 2006, pp. 115–131.

Tuyls, P., *et al*. “Read-proof hardware from protective coatings,” in *Cryptographic Hardware and Embedded Systems-CHES 2006*, ed: Springer, 2006, pp. 369–383.

Tuzzio, N., *et al*. “A zero-overhead IC identification technique using clock sweeping and path delay analysis,” in *Proceedings of the great lakes symposium on VLSI*, 2012, pp. 95–98.

Ullah, S., *et al*. (2012) “A comprehensive survey of wireless body area networks.” *Journal of medical systems*. **36**, 1065–1094.

Vajana, B. and Patelmo, M. “Anti-deciphering contacts,” US 6,528,885 B2, 2003.

Vajana, B. and Patelmo, M. “Mask programmed ROM inviolable by reverse engineering inspections and method of fabrication,” US 6,614,080 B2, 2003.

van Woudenberg, J.G., *et al*. “Practical optical fault injection on secure microcontrollers,” in *Fault Diagnosis and Tolerance in Cryptography (FDTC), 2011 Workshop on*, 2011, pp. 91–99.

van der Leest, V., *et al*. “Efficient implementation of true random number generator based on sram pufs,” in *Cryptography and Security: From Theory to Applications*, ed: Springer, 2012, pp. 300–318.

Verbauwhede, I., *et al*. “The fault attack jungle-a classification model to guide you,” in *Fault Diagnosis and Tolerance in Cryptography (FDTC), 2011 Workshop on*, 2011, pp. 3–8.

Vivekraja, V. and Nazhandali, L. “Feedback based supply voltage control for temperature variation tolerant pufs,” in *VLSI Design (VLSI Design), 2011 24th International Conference on*, 2011, pp. 214–219.

Wagner, L.C. *Failure analysis of integrated circuits: tools and techniques*: Springer, 1999.

Walden, R.H. “Dynamic circuit disguise for microelectronic integrated digital logic circuits,” 5,202,591, 1993.

Walden, R.H. “Method for disguising a microelectronic integrated digital logic,” 5,336,624, 1994.

Want, R. (2006) “An introduction to RFID technology.” *Pervasive Computing, IEEE*. **5**, 25–33.

Weingart, S.H. (1987) “Physical security for the pABYSS system.” *System*. **1**, 3.

Wendt, J.B. and Potkonjak, M. “Nanotechnology-based trusted remote sensing,” in *Sensors, 2011 IEEE*, 2011, pp. 1213–1216.

Wu, X., *et al*. (2010) “Test-access mechanism optimization for core-based three-dimensional SOCs.” *Microelectronics Journal*. **41**, 601–615.

Yamamoto, D., *et al*. “Performance and security evaluation of AES s-box-based glitch PUFs on FPGAs,” in *Security, Privacy, and Applied Cryptography Engineering*, ed: Springer, 2012, pp. 45–62.

Yancey, T. (2013) Semiconductor R&D Spending Rises 7% Despite Weak Market. *Research Bulletin*.

Yao, A.C.-C. (1986) “How to generate and exchange secrets,” in *Foundations of Computer Science, 1986., 27th Annual Symposium on*, pp. 162–167.

Yin, C.-E. “A Group-Based Ring Oscillator Physical Unclonable Function,” Doctoral Dissertation, Electrical Engineering, University of Maryland, College Park, 2012.

Zhang, X. and Tehranipoor, M. (2014) “Design of on-chip lightweight sensors for effective detection of recycled ICs.” *Very Large Scale Integration (VLSI) Systems, IEEE Transactions on*. **22**, 1016–1029.

Zhang, X., *et al*. “Identification of recovered ICs using fingerprints from a light-weight on-chip sensor,” in *Proceedings of the 49th Annual Design Automation Conference*, 2012, pp. 703–708.

Zhang, X., *et al*. (2012) “Path-delay fingerprinting for identification of recovered ICs,” in *Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT), 2012 IEEE International Symposium on*, pp. 13–18.

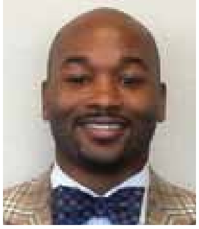
Zheng, Y., *et al*. “CACI: Dynamic Current Analysis Towards Robust Recycled Chip Identification,” in *Proceedings of the The 51st Annual Design Automation Conference on Design Automation Conference*, 2014, pp. 1–6.

Shekhar Bhansali, Ph.D., is Alcatel Lucent Professor and Chair of the Department of Electrical and Computer Engineering at Florida International University. His research interests are in the area of nano-enabled biosensors and impedance based microsystems. Prof. Bhansali has invented numerous room temperature sensors for both biomolecules and gases. He has conceptualized and led numerous interdisciplinary graduate research-training programs, including IGERT, NSF Bridge to Doctorate and Alfred P. Sloan Doctoral Fellowship Programs to increase diversity, retention and graduation rates of doctoral students in STEM. These programs have matriculated over 180 graduate students. He is the recipient of the NSF CAREER Award (2003), Outstanding Researcher award (2004) Alfred P. Sloan Foundation Outstanding Mentor Award (2009), William R jones Outstanding Mentor Award (2004, 2009), FEF Outstanding Mentor Award (2009) and FIU top Scholar Award (2013) He holds 24 patents and has published over 200 peer-reviewed publications.

Ange Marie P. Fievre, Ph.D., received the B.S. degree in electronics engineering from Université d'Etat d'Haïti, Port-au-Prince, Haiti in 2003, and the M.S. degree in computer engineering and the Ph.D. degree in electrical engineering from Florida International University, Miami, respectively in 2006 and 2015.

From 2005 to 2009, she was a Research Assistant with the Nanophotonics Group, Department of Electrical and Computer Engineering (ECE), Florida International University (FIU), Miami. In 2012, she became a Research Assistant with the BioMEMS and Microsystems Group, ECE Department, FIU. Her research interests include dielectric structures for high-power applications, nano-apertures, subwavelength grating structures and optical solutions for hardware security.

Dr. Fievre was a recipient of the two-year Latin American and Caribbean center (LACC) scholarship in 2004, and of the SPIE Educational Scholarship in 2010. She is a member of SPIE, of the National Society of Black Engineers (NSBE), and is a McKnight fellow.



Al-Aakhir A. Rogers, Ph.D., received the B.S. and M.S. degrees in electrical engineering from North Carolina Agricultural and Technical State University, Greensboro, in 2003 and 2005, and the Ph.D. degree in electrical engineering from the University of South Florida, Tampa, in 2011.

Since 2011, he has been a Senior Member of Technical Staff with Draper Laboratory in St. Petersburg, FL. His research interests include nanolithography, subwavelength optical structures, MEMS, and microsystem electronics. He has two U.S. patents.

Dr. Rogers was the recipient of the NSF East Asia Pacific Summer Institute (EAPSI) Fellowship, the NSF Bridge to the Doctorate Fellowship, the Alfred P. Sloan Minority Ph.D. Fellowship, and the FEF McKnight Fellowship. He was recipient of the 2010 Diversity Honor Roll Award and of the 2011 Golden Bull Award, from the University of South Florida.