Chapter 1
Introduction

Human society relies heavily on computer systems. They enhance our quality of life by delivering performance, bringing accuracy, and providing security. Applications ranging from nuclear plant controls and jet engines to home appliances like dishwashers and microwaves benefit from computer systems. The dependability of a computer system determines its accountability. The dependability of a system is based on the compliance of delivered services by the system with its functional specifications. The function of the system is described by functional specifications in terms of functionality and performance. The service delivered by the system, on the other hand, is its behavior as it is perceived by its user(s). A broad concept, dependability encompasses availability, reliability, safety, integrity, and maintainability attributes as described in Table 1.1 [2].

Security is more specific, focusing on availability, integrity, and confidentiality. System security demands availability for only authorized actions, integrity with improper meaning unauthorized, and confidentiality. Trust is the dependency of a system (system A) to another system (system B), through which the dependability of system A is affected by the dependability of system B. Trustworthiness in a system is the assurance that the system will perform as expected [2].

A modern society utterly depends on integrated circuits (ICs), or chips, which are the virtual brains for all electronics. In the interest of economic matters, most companies nowadays mostly outsource and fabricate ICs overseas, rendering them increasingly vulnerable to malicious activities such as design modifications created to sabotaging a mission or counterfeiting integrated circuits.

1.1 Hardware Security and Trust

A computer system development, as shown in Fig. 1.1, consists of several steps which are not necessarily performed all in the same design house. The first step is to determine system specifications based on the customer's needs. A complex

M. Tehranipoor et al., *Integrated Circuit Authentication: Hardware Trojans and Counterfeit Detection*, DOI 10.1007/978-3-319-00816-5_1,

Table 1.1 Dependability attributes

Attribute	Definition
Availability	Readiness for correct service
Reliability	Continuity of correct service
Safety	Absence of catastrophic consequences on the users and the environment
Integrity	Absence of improper system alteration
Maintainability	Ability to undergo modification and repairs
Confidentiality	The absence of unauthorized disclosure of information

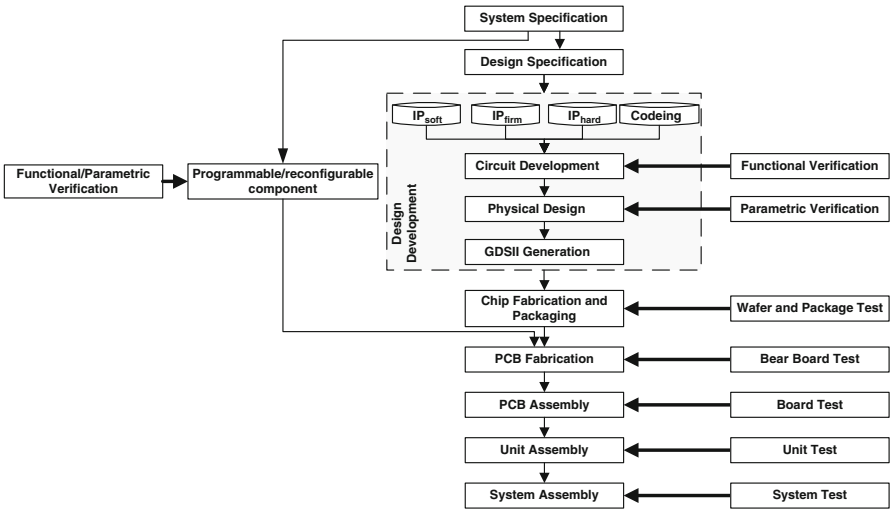

Fig. 1.1 System integration and test process

system may require a variety of components like memories and chips with different applications and functionalities.

After providing the system specifications and choosing the structure of system and its required components, design development requires different tools. Each component demands specific attention to meet all the system specifications. To expedite system development and to reduce the final cost, outsourced alternatives have gradually replaced in-house processes. Third-party intellectual property (IP) cores have displaced the in-house libraries of logic cells for synthesis. Commercial software has supplanted homegrown Computer Aided Design (CAD) tool software. In the next step, designed chips are signed-off for fabrication. Nowadays, most companies are fabless, outsourcing mask production and fabrication. Beside custom designs, companies can reduce total cost and accelerate system development by using commercial-off-the-shelfs (COTSs), reprogrammable modules, like micro-controllers, reconfigurable components, or field programmable gate arrays (FPGAs). Afterwards, they manufacture printed circuit boards (PCBs) and assemble

system components on them. Finally, the PCBs are put together to develop units; the entire system is the integration of these units.

In each step, different verifications or tests are performed to ensure its correctness, as shown in Fig. 1.1. Functional and parametric verifications ascertain the correctness of design implementation in terms of service and associated requirements, like power and performance. Wafer and package tests after the fabrication of custom designs separate defective parts and guarantee delivered chips. The PCB fabrication is a photolithographic process and susceptible to defects; therefore, a PCB should be tested before placing devices on it. After the PCB assembly, the PCB is again tested to verify that the components are properly mounted and have not been damaged during the PCB assembly process. The tested PCBs create units and finally the system, which is also tested before shipping for field operation [12].

Each step of system development is susceptible to security breaches. An adversary may change system specifications to make a system vulnerable to malicious activities or susceptible to functional failures. As external resources, like third party IPs and COTSs, are widely used in design process and system integration, adversaries may hide extra circuit(s) in them to undermine the system at a specific time or to gain control over it. The untrusted foundry issue is rooted in the outsourcing of design fabrication. Establishing a chip fabrication factory is extremely expensive and most semiconductor companies have become fabless in recent years. They ask foundries to fabricate their designs to reduce the overall cost. The third party, however, may change the designs by adding extra circuits, like back doors to receive confidential information from the chip, or altering circuit parameters, like wire thickness to cause a reliability problem in the field. The PCB assembly is even susceptible, as it is possible to mount extra components on interfaces between genuine components. In short, cooperative system development process creates opportunities for malicious parties to take control of the system and to run vicious activities. Therefore, as a part of the system development process, security features should be installed to facilitate trustworthiness, validation, and to unveil any deviation from genuine specifications.

1.1.1 Hardware Trojans

The practice of outsourcing design and fabrication in the interest of economy, has raised serious national security concerns, since an adversary can subvert a design by adding extra circuits, called hardware Trojans [1]. In general, a hardware Trojan is defined as any intentional alteration to a design in order to alter its characteristics. A hardware Trojan has a stealthy nature and can alter design functionality under rare conditions. It can serve as a time bomb and disable a system at a specific time, or it can leak secret information through side channel signals.

A Trojan may affect circuit AC parameters such as delay and power; it also can cause malfunction under rare conditions. Shown in Fig. 1.2, a hardware Trojan consists of Trojan payload and Trojan trigger [16]. A functional Trojan takes inputs

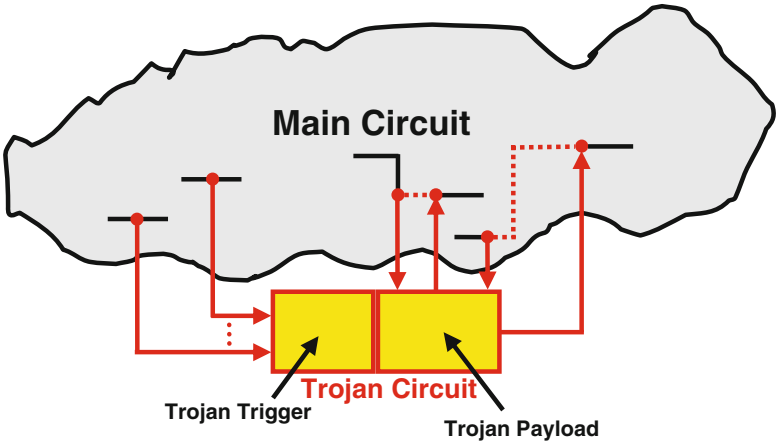

Fig. 1.2 Functional Trojan implementation

from some internal nets of the main circuit to the Trojan payload and restitches some other nets of the main circuit through Trojan payload to modify design functionality. The Trojan trigger determines the activation condition(s) under which the Trojan payload can propagate erroneous values into the main circuit.

Wang, Tehranipoor, and Plusquellic developed the first detailed taxonomy for hardware Trojans [7, 8]. This comprehensive taxonomy lets researchers examine their methods against different Trojan types. Currently, the industry lacks metrics to evaluate the effectiveness of methods in detecting Trojans. Such metrics could foster a comprehensive taxonomy to help analyze Trojan detection techniques. Because malicious alterations to a chip's structure and function can take many forms, Wang and colleagues decomposed the Trojan taxonomy into three main categories (see Fig. 1.3) according to their physical, activation, and action characteristics. Although Trojans could be hybrids of this classification (for instance, they could have more than one activation characteristic), this taxonomy captures the elemental characteristics of Trojans and is useful for defining and evaluating the capabilities of various detection strategies.

The physical characteristics category describes the various hardware manifestations of Trojans. The type category partitions Trojans into functional and parametric classes. The functional class includes Trojans that are physically realized through the addition or deletion of transistors or gates, whereas the parametric class refers to Trojans that are realized through modifications of existing wires and logic. The size category accounts for the number of components in the chip that have been added, deleted, or compromised. The distribution category describes the location of the Trojan in the chip's physical layout. The structure category refers to the case when an adversary is forced to regenerate the layout to insert a Trojan, which could then cause the chip's physical form factor to change. Such changes could result in different placement for some or all design components. Any malicious changes in physical layout that could change the chip's delay and power characteristics would

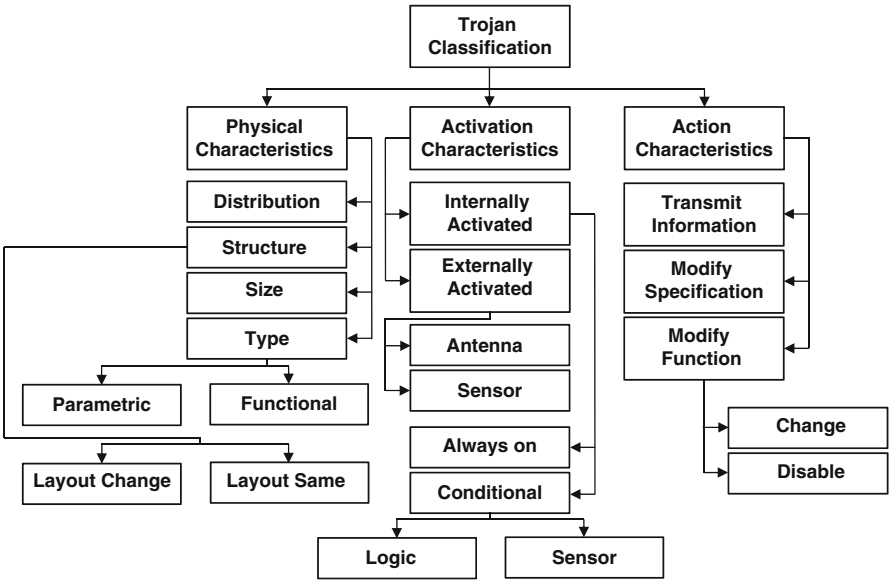

Fig. 1.3 Hardware Trojan Taxonomy

facilitate Trojan detection. Wang and colleagues identified current adversaries' capabilities for minimizing the probability of detection.

Activation characteristics refer to the criteria that cause a Trojan to become active and carry out its disruptive function. Trojan activation characteristics fall into two categories: externally activated (e.g., by an antenna or a sensor that can interact with the outside world) and internally activated (which are further classified as always on and condition based), as Fig. 1.3 shows. "Always on" means the Trojan is always active and can disrupt the chip's function at any time. This subclass covers Trojans that are implemented by modifying the chip's geometries such that certain nodes or paths have a higher susceptibility to failure. The adversary can insert the Trojans at nodes or paths that are rarely exercised. The condition-based subclass includes Trojans that are inactive until a specific condition is met. The activation condition could be based on the output of a sensor that monitors temperature, voltage, or any type of external environmental condition (such as electromagnetic interference, humidity, altitude, or temperature). Alternatively, this condition could be based on an internal logic state, a particular input pattern, or an internal counter value. The Trojan in these cases is implemented by adding logic gates and/or flipflops to the chip, and hence is represented as a combinational or sequential circuit.

Action characteristics identify the types of disruptive behavior introduced by the Trojan. The classification scheme shown in Fig. 1.3 partitions Trojan actions into three categories: modify function, modify specification, and transmit information. The modify-function class refers to Trojans that change the chip's function by adding logic or by removing or bypassing existing logic. The modify-specification

class refers to Trojans that focus their attack on changing the chip's parametric properties, such as delay when an adversary modifies existing wire and transistor geometries. Finally, the transmit-information class includes Trojans that transmit key information to an adversary.

Trojan circuits are sly, triggering only under rare conditions. Trojans are designed to be silent most of their lifetime, to have a very small size relative to their host designs, and to make only limited contributions to circuit characteristics. Analyzing the vulnerabilities of IC development process requires the knowledge of design, fabrication, and test processes. To ensure a client's IC is authentic, the entire design and fabrication process must be made trustworthy or manufactured ICs should be verified by clients for trustworthiness. Having a separate and secure IC supply chain is desirable but economically prohibitive. Today, only Intel and few other companies still design and manufacture all their own chips in their own fabrication plants. Other chip designers have gone fabless, outsourcing their manufacturing to offshore facilities. In doing so, they avoid the huge expense of building a state-of-the-art fab, which, in 2007, cost as much as 2–4 billion in US dollars [1]. For example, the Petagon reports it now manufactures only 2 % of the more than $3.5 billion of integrated systems bought for military gears in secure facilities run by American companies [10]. These facts demand effective methods and techniques for Trojan prevention and detection.

1.1.1.1 Trojan Detection Methodologies

Several Trojan detection methodologies have been developed over the past few years. Without loss of generality, the methods are categorized as either side-channel analysis or Trojan activation, which are mainly chip-level solutions and architectural-level Trojan detection solutions.

Trojan Detection Using Side-Channel Signal Analysis

Side-channel signals, including timing and power, can be used for Trojan detection. Trojans typically change a design's parametric characteristics for example, by degrading performance, changing power characteristics, or introducing reliability problems in the chip. This influences power and/or delay characteristics of wires and gates in the affected circuit. Power-based side-channel signals provide visibility of the internal structure and activities within the IC, enabling detection of Trojans without fully activating them. Timing-based side channels can detect a Trojan's presence if the chip is tested using efficient delay tests that are sensitive to small changes in the circuit delay along the affected paths and that can effectively differentiate Trojans from process variations.

Power-Based Hardware Trojan Detection: In power-based techniques, the power consumption of IC under authentication (IUA) is compared with that of Trojan-free

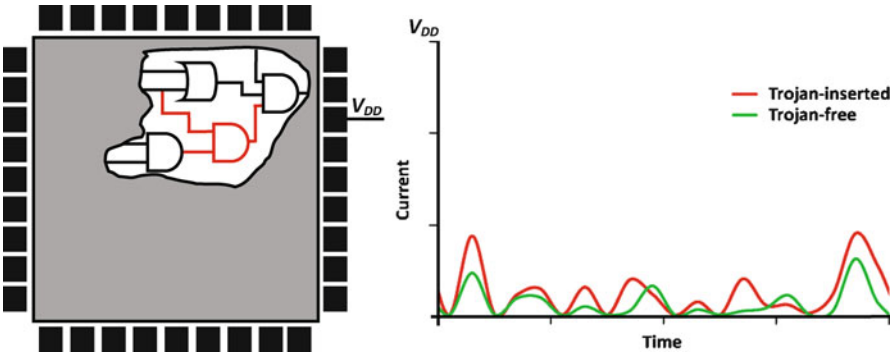

Fig. 1.4 Hardware Trojan detection based on power analysis

(golden) circuits. Figure 1.4 shows the measured current from VDD pin in Trojan-free and Trojan-inserted circuits over a specific time interval. Each current measurement consists of several elements, including (1) the main circuit current consumption which is the same for all chips, (2) measurement noise which can be eliminated by averaging several measurements, (3) process variations which are random and cannot be canceled, and, lastly, (4) Trojan contributions if they exist. Any measurable difference beyond process variations can be an indication of Trojan existence.

Agrawal et al. were the first to use side-channel information to detect Trojan contributions to circuit power consumption [3]. To obtain the power signature of Trojan-free (i.e., genuine) ICs, random patterns are applied and power measurement is performed. After patterns are applied, a limited number of ICs are reverse engineered to ensure they are Trojan free. Once the reference signature is obtained, the same random patterns are applied to the IC under authentication (IUA). If the IUA's power signature differs from the reference signature, the IUA is considered suspicious and it might contain a Trojan. Trojans of different sizes under different process variations are detected by applying random patterns and observing the signatures. If the Trojan is comparable in size with the circuit, its impact on the circuit-transient current will be significant and could be measured easily. However, process variations will mask the impact of very small Trojans on circuit power consumption.

Rad et al. proposed a region-based transient power signal analysis method to reduce the impact of increasing process variation levels and leakage currents [11]. A region is a portion of the layout that receives the majority of its power from surrounding power ports or C4 bumps. Measurements are made through each power port individually by applying patterns. The transient-current detection algorithm is based on a statistical analysis of the I_{DDT} waveform areas generated at each power ports as a test sequence is simulated on the design. For each orthogonal pairing of power ports, a scatter plot is constructed. The authors used several different process models for Trojan-free and Trojan-inserted designs. A prediction ellipse

derived from a Trojan-free design with different process models can help distinguish between Trojan-inserted and Trojan-free designs. The dispersion in the Trojan-free data points is a result of uncalibrated process and test environment (PE) variations. However, regional analysis alone is not sufficient for dealing with the adverse effects of PE variations on detection resolution. Signal calibration techniques are necessary to attenuate and remove PE signal variation effects, to fully leverage the resolution enhancements available in a region-based approach. Calibration is performed on each power port and for each chip separately, and it measures the response of each power port to an impulse. After each test pattern is applied, the response is calibrated using the calibration matrix. The results presented by Rad et al. show that calibration can increase the distance between Trojan-free and Trojan-inserted designs under different process parameters.

Alkabani and Koushanfar proposed several approaches for gate-level timing and power characterization via nondestructive measurements [13]. Each measurement forms one equation. After a linear number of measurements are taken, a system of equations for mapping the measured characteristics to the gate level is formed. Potkonjak et al. exploited the formulation of gate-level characterization using linear programming and singular-value decomposition to detect Trojans [14]. They used both timing and static-power measurements. Trojan detection is performed via constraint (equation) manipulation. This method attempts to find the measurement matrix with the highest rank, and derives several heuristics for detecting gates that have inconsistent characteristics compared to their original specified characteristics. Learn, test, and resubstitution statistical validation techniques are used to estimate the bounds for normal (non-malicious) characteristics. The experiments considered errors in noninvasive measurements, but not process variations. The evaluation results are promising because gate-level characterization with high accuracy is possible. The gate-level characterization methods can find the characteristics of controllable gates. This controllability is known to be high for static power measurements and I_{DDQ} testing. Alkabani and Koushanfar used statistical convergence of gate-level estimation and signal integrity for Trojan detection [13]. They found efficient robust approximations for gate power consumptions and identified malicious insertions using multiple consistency checking.

Delay-Based Hardware Trojan Detection: There are also techniques that analyze the impact of Trojans on design performance. Any additional gates or wiring introduces extra capacitances, and then any rising or falling on Trojan-inserted paths creates extra time for transition. Figure 1.5 shows that the Output_Tx signal in a Trojan-free circuit changes sooner compared with a Trojan-inserted circuit. The signal over the highlighted path passes through extra wiring and an additional gate and experiences additional delay due to the resistance and capacitance of the extra wiring and transport delay of the Trojan gate.

In [6] a path delay fingerprint is proposed which is basically similar to [3] but based on analyzing circuit delay. A Trojan, even one small in size compared to the size of the main circuit, can have impact on at least one path. A circuit has many paths, each representing one part of the entire circuit characteristic.

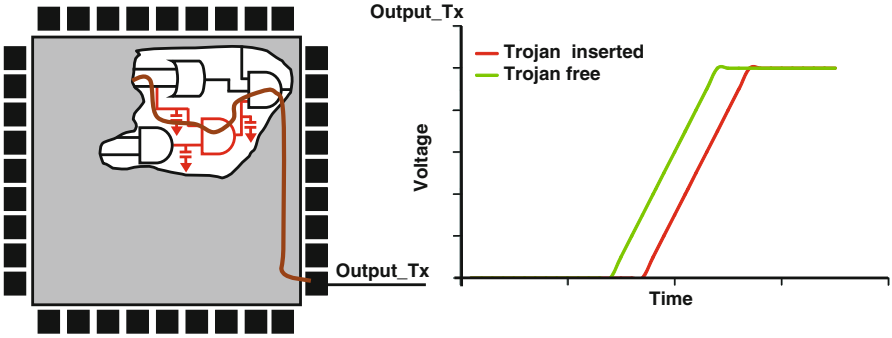

Fig. 1.5 Hardware Trojan detection based on delay analysis

The technique measures the delay of several nominated paths on several chips to bring process variations into account. Afterwards, the chips are reversed engineered to ensure they are genuine, and their measurements are used as a signature. The same measurements are performed on other chips and compared with the signature. Any difference can be an indication of Trojan insertion.

As another delay-based approach, a specific delay measurement circuit based on shadow registers is provided to measure the delay of a candidate path in [9]. The technique is mainly used for IC characterization and it can be utilized for hardware Trojan detection, as well. The delay of a nominated path between two registers (source and destination registers) is characterized by a shadow register which has a clock (clk2) with the same frequency as the clock applied to the registers (clk1), but with a negative phase shift (i.e. negative skew). To characterize the path, clk2 is applied with different skew till the captured data in the shadow register and destination register become different, and then clk2, along with the pattern applied to the path under test, is stored. Two measurements are performed at the design time and test time. The design-time measurement is performed on nominated paths with different process variations to develop a statistical data for each path. At the test time the same measurement is performed on each path and compared with the stored statistical data. Any significant difference between stored clk2 at design time and obtained clk2 at test time indicates Trojan existence.

Trojan Activation Methods

Trojan activation strategies can accelerate the Trojan detection process, and in some cases have been combined with power analysis during implementation. If a portion of the Trojan circuitry is activated, the Trojan circuit will consume more dynamic power, which will further help differentiate the power traces of Trojan-inserted and Trojan-free circuits. The existing Trojan activation schemes can be categorized as follows.

Region-Free Trojan Activation: These methods do not rely on the region but depend on accidental or systematic activation of Trojans. For example, Jha and Jha presented a randomization-based probabilistic approach to detect Trojans [15]. They showed that it's possible to construct a unique probabilistic signature of a circuit on the basis of a specific probability for patterns applied to its inputs. They apply input patterns based on the specific probability to IUA and compare its outputs with the original circuit. If there are differences in the outputs, a Trojan is present. For Trojan detection in a manufactured IC, patterns can be applied only on the basis of such probability to obtain a confidence level regarding whether the original design and the fabricated chip are the same. Wolff et al. analyzed rare-net combinations in designs [16]. These rarely activated nets are used as Trojan triggers. At the same time, nets with low observability are used as payloads. Wolff et al. generated a set of vectors to activate such nets and suggested combining them with traditional ATPG test vectors to activate a Trojan and to propagate its impact if the Trojan was connected to these nets.

Region-Aware Trojan Activation: Banga and Hsiao developed a two-stage test generation technique that targets magnifying the difference between the IUA and the genuine design power waveforms [4]. In the first stage (circuit partitioning), a region-aware pattern helps identify the potential Trojan insertion regions. To detect a Trojan circuit, the activity within a portion of the circuit is increased while the activity for the rest of the circuit is simultaneously minimized. The flip-flops in a circuit are classified into different groups, depending on structural connectivity. In the next stage (activity magnification), new test patterns concentrating on the identified regions are applied to magnify the disparity between the original and Trojan-inserted circuits. Regions (a set of flip-flops) exhibiting increased relative activity are identified by using the vector sequence generated in the first stage to compare the relative differences between the power profiles of the genuine and Trojan circuits. In this stage, more vectors for the specific regions, marked as possible Trojan regions, are generated using the same test generation approach as in the circuit-partitioning stage. Banga and Hsiao discussed magnifying Trojan contributions by minimizing circuit activity [5]. This involves keeping input pins unchanged for several clock cycles. Thus, circuit activity comes from the state elements of the design. Overall switching activity is therefore reduced, and can be limited to those specific portions of the design that help Trojan localization. Different portions of the design can be explored by changing input vectors to localize a Trojan. At the same time, each gate is equipped with two counters: TrojanCount and NonTrojanCount. With each vector, if the number of transitions at a gate's output exceeds a specific threshold, its TrojanCount would increase, and vice versa. The TrojanCount/NonTrojanCount ratio, called the gate weight, indicates a gate's activity. A high gate-weight ratio means the gate is considerably impacted by a Trojan, because there is a relatively high power difference corresponding to that gate's activation. Because the test engineer does not know the Trojan type or size, both region-free and region-aware methods are necessary. If a Trojan circuit's inputs come from the part of the circuit where they are functionally dependent (i.e., part

of the same logic cone), the region-aware method can be effective. However, if the Trojan inputs are randomly selected from various parts of the circuit, region-free methods could increase the probability of detection.

Architecture-Level Trojan Detection

Verbauwhede and Schaumont explored trust issues at different levels of design abstraction (protocols, software, microarchitecture, and circuits) [17]. At the most abstract level, the adversary can access the interpreter and perform software tempering, scan-chain readout, or a fault attack. Side-channel information can be used at the software-architecture level. At the hardware microarchitecture and circuit levels, the attacker takes into account power energy consumption or electromagnetic energy. Hence, the authors proposed a systematic countermeasure to protect the root of trust at different design abstractions.

Tamper-proof techniques such as placing security parts into special casing with light, temperature, tampering, or motion sensors can provide protection at the physical level. Side-channel information such as power consumption should be separated from processing data or execution time to provide circuit-level protection. To deal with power fluctuation, different technologies such as full-custom dynamic and differential logic styles should be used. In experiments conducted by the authors, advanced encryption standards employing wave dynamic and differential logic remained safely after 1.5 million power-differential attack measurements, whereas standard CMOS technology disclosed the key only after 2,000 attack measurements.

To deal with side-channel attacks at the microarchitecture level, Verbauwhede and Schaumont suggested balancing if-and-else instructions to use the same amount of time and power during execution. The structure of microprocessors providing potential sources of side-channel information should be considered seriously. The authors also suggested using secure algorithm techniques, such as key and exponent blinding, to disable side-channel attacks at lower levels.

Suh, Deng, and Chan proposed authenticating the hardware by directly checking its implementation details at a low level [18]. The microarchitecture features of a high-end secure microprocessor are complex and unique for each model. A secure processor is authenticated by a checksum response to a challenge within a time limit. The unique checksum is based on the cycle-to-cycle activities of the processor's specific internal microarchitectural mechanism. Privacy is not breached, because the checksum depends on the processor-manufactured model and not the specific processor. The authors showed that small differences in the crypto-architecture result in significant deviations in the checksum. Their work relied on the speed advantages of the actual processor rather than simulations that attempt to impersonate the processor. The time limit on the authentication ensures resiliency against simulation models attempting to compute the checksum.

Bloom, Narahari, and Simha introduced a runtime Trojan activity detection mechanism using a hardware guard circuit and operating-system support [19].

Trojan attacks can either be internally or externally activated, and they can cause denial of service, privilege escalation, or leakage of sensitive information. Trojans can be detected by failure analysis and hardware verification, ATPG, or side-channel analysis. Bloom, Narahari, and Simha's work concentrated on denial-of-service (DoS) and privilege escalation attacks [19]. They used a hardware guard circuit to efficiently perform the testing, while the operating system generated the checks. Their hardware circuit included a timer, a scratch RAM, a simple processor, and an optional content-addressable memory (CAM).

Two tests were proposed: liveness checks and memory protection checks. Liveness checks are pseudo-random noncached-memory accesses that prevent simple prediction, delay, and replay attacks. Two solutions were provided for memory protection: a naive solution and a solution using a real-time operating system (RTOS). The naive solution periodically schedules a process that continuously tries to read the kernel memory. However, the process is time-consuming. RTOS support is needed to control the time of the checking process, which is created as a real-time task that is frequently required and consumes less time. The proposed solutions are evaluated on SPECit 2006 benchmarks. The overhead for using RTOS supportis approximately 2.2 %.

McIntyre et al. used hardware multicore systems, which permit simultaneous execution of the same functionality combined with verification [20]. Multicore systems are inherently redundant. Thus, as trust detection among the multiple cores is discovered, distributed software scheduling could be exploited to avoid low-trust cores. The distributed multicore task scheduler determines, over time and in the field, each core's hardware trust level.

Verifying the trustworthiness of manufactured ICs requires a post-manufacturing step to validate the conformance of the fabricated ICs to the original functional and performance specifications. Current design methodologies provide an adversary with multiple opportunities to insert Trojans that can go undetected. It is important to develop design-for-hardware-trust (DFHT) strategies (i) to prevent Trojan insertion into a design and (ii) to detect the Trojan if inserted. In other words, ICs must be designed in such a way that undetected changes to a circuit are near impossible.

1.1.2 Counterfeit ICs

Counterfeiting and piracy are longstanding problems which are growing in scope and magnitude. They are of great concern to governments because of (i) the negative impact they can have on innovation, (ii) the threat they pose to the welfare of consumers and (iii) the substantial resources that they channel to criminal networks, organized crime and other groups that disrupt and corrupt society. They are of concern to business because of the negative impact that they can have on (i) sales and licensing, (ii) brand value and firm reputation, and (iii) the ability of firms to benefit from the breakthroughs they make in developing new products [21].

Innovation in the business sector has always been the main driver of economic growth through the development and implementation of ideas for new products and processes. These inventions are usually protected via patents, copyrights, and trademarks. However, without adequate protection of these intellectual property (IP) rights, the incentives to develop these new ideas and products would be considerably reduced, thereby weakening the innovation process and critical thinking [21]. These risks are seen as particularly high for those industries in which the research and development (R&D) costs associated with the development of new products are very high compared to the cost of producing the resulting products. In the world of electronics, the R&D costs for the semiconductor industry are indeed extremely high, and protection of their IP rights is of utmost importance.

Without a doubt, counterfeiting of integrated circuits has become a major challenge due to the deficiencies in the existing test solutions. In the past couple of years, numerous reports (to be found in [22]) have pointed out to the counterfeiting issues in US electronic component supply chain. Senate Armed Services public hearing on this issue and the later report have clearly identified this as a major twenty-first century issue for US to address because of its significant implications on taxpayer money as well as the loss of lives that can be associated with deploying counterfeit parts in DOD critical applications [23, 24]. The report also indicated the lack of sufficient investment in this domain and that there are major shortcomings in detecting such counterfeit parts and the need to address them immediately.

In today's global economy, electronics components travel around the world before they make it into a system, such as, cell phone, computer, or security system. This global market has greatly reduced the cost of electronics, as large foundries can offer lower and lower prices. However, there is another illicit market willing to undercut the competition with equally illicit parts. If one of these ends up in consumer products, it will likely go undetected. The part may fail prematurely or unexpectedly, and the manufacturer will simply label the product as a defective unit and likely replace the product under warranty. However, if these parts end up in critical applications such as defense, aerospace, or medical, the results could be catastrophic. This is the market of counterfeits and it is stirring up serious problems in some sectors—including the United States Department of Defense [25].

Just how big the market is remains a mystery still. A study conducted from 2005–2007 [26] reveals that 50 % of original component manufacturers (OCM) and 55 % of distributors (authorized and unauthorized) have encountered counterfeit parts. The Electronic Resellers Association International [27] monitors, investigates, and reports issues that are affecting the global supply chain of electronics. ERAI, in combination with Information Handling Services Inc. [28], have been monitoring and reporting counterfeit component statistics dating back to 2001. The most recent data (Fig. 1.6) provided by IHS shows that reports of counterfeit parts have quadrupled since 2009.

Along with the increase of counterfeit incidents, it is also very important to analyze the vulnerabilities of the electronic components. Table 1.2 shows the five

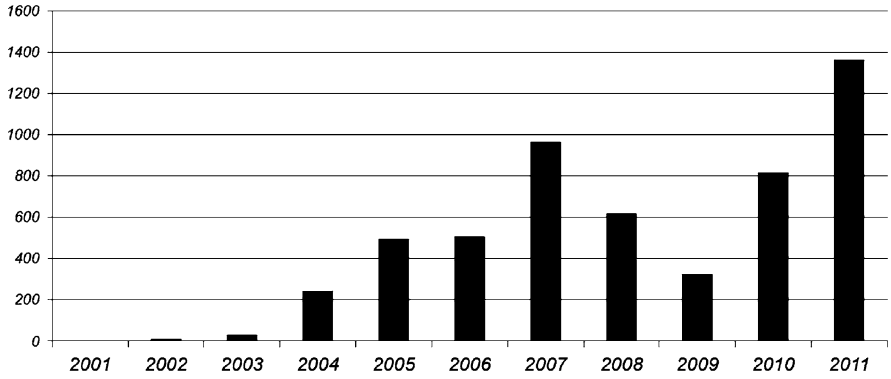

Fig. 1.6 Counterfeit incidents reported by IHS [29]

Table 1.2 Top-5 most counterfeited semiconductors in 2011 (Percentage of counterfeit part reports)

Rank	Commodity type	% of reported incidents (%)
#1	Analog IC	25.2
#2	Microprocessor IC	13.4
#3	Memory IC	13.1
#4	Programmable logic IC	8.3
#5	Transistor	7.6

Source: IHS Parts Management 2012 [30]

most commonly counterfeited components according to the percent of reported counterfeit incidents. They are as follows: analog ICs, microprocessor ICs, memory ICs, programmable logic ICs and transistors. Together, these five component groups contribute around 68 %, slightly more than two-thirds, of all counterfeit incidents reported in 2011. In this chapter, parts and components are used interchangeably to refer electronic devices.

This steady increase of reported incidents reflects the need for effective methods of testing parts and maintaining proper records as parts travel through the supply chain. There are a handful of available standards that seek to do just this, with more being written and revised constantly. The committee responsible for many of these standards is the G-19 Counterfeit Electronic Parts Committee, set forth by SAE International [31]. Their standards target three different sectors of the industry: distributors, users, and test service providers (i.e., test laboratories). A collection of the standards that they have written or are currently working on is as follows.

- AS6081—Counterfeit Electronic Parts Avoidance, **Distributors**
- ARP6178—Counterfeit Electronic Parts; Tool for Risk Assessment of Distributors, **Distributors & Users**
- AS5553—Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition, **Users**
- AS6171—Test Methods Standard; Counterfeit Electronic Parts, **Test Providers**

While SAE is the most prominent figure when it comes to standards and counterfeits, there are a couple of programs that are designed to help independent distributors gain trust from customers. Components Technology Institute, Inc. [32] is a multi-discipline company providing engineering and consulting services, training courses, and component conferences. They have created the Counterfeit Components Avoidance Program [33] (CCAP-101). Independent distributors can be certified as CCAP-101 compliant, which is done by means of a yearly audit. Another program with similar goals has been developed by the Independent Distributors of Electronics Association [34]. There is a comparison of the SAE's AS5553, CTI's CCAP-101, and IDEA's STD-1010 available in [35].

Note that these standards only deal with the detection of parts that are already in the market. There is another side to the anti-counterfeiting effort that takes on the prevention approach for parts that are currently being (will be) fabricated. Silicon physical unclonable functions (PUFs) have received much attention from the hardware security and cryptography communities as a new approach for IC identification, authentication and on-chip key generation [36–40]. 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 [41, 42]. The variations can help generate a unique signature for each IC in a challenge-response form, which allows later identification of genuine ICs.

Due to the globalization of the semiconductor industry and the prohibitively high cost to create 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. The existing research on avoidance attempts to allow an IC designer to control the number of ICs produced. As an example, 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 [37, 39, 43–46]. Active metering approaches, however, lock each IC until it is unlocked by the IP holder [42, 47–51]. This locking is done in a variety of ways including: (i) initializing ICs to a locked state on power-up [42], (ii) combinational locking by, for instance, scattering XOR gates randomly throughout the design [49–51], and (iii) adding a finite-state machine (FSM) which is initially locked and can be unlocked only with the correct sequence of primary inputs [48, 52].

Studying the vulnerabilities of electronic supply chain to counterfeiting is necessary to effectively address the problem. A comprehensive taxonomy of potential counterfeit component types reveals counterfeiters capability in forging. These shall shed light on challenges and foster efforts towards counterfeit detection and prevention.

References

1. S. Adee, "The Hunt for the Kill Switch," http://www.spectrum.ieee.org/print/6171.
2. A. Avizienis, J. Laprie, B. Randell, and C. Landwehr, "Basic Concepts and Taxonomy of Dependable and Secure Computing," IEEE Transactions on Dependable and Secure Computing, Vol. 1, No. 1, 2004, pp. 11–33.
3. D. Agrawal, S. Baktir, D. Karakoyunlu, P. Rohatgi and B. Sunar, "Trojan Detection using IC Fingerprinting," in Proc. of the *Symposium on Security and Privacy*, pp. 296–310, 2007.
4. M. Banga and M. S. Hsiao, "A Region based Approach for the Identification of Hardware Trojans," in Proc. of the *IEEE International Workshop on Hardware-Oriented Security and Trust (HOST2008)*, pp. 40–47, 2008.
5. M. Banga and M. S. Hsiao, "A Novel Sustained Vector Technique for the Detection of Hardware Trojans," in Proc. of the *International Conference on VLSI Design*, pp. 327–332, 2009.
6. Y. Jin and Y. Makris, "Hardware Trojan Detection using Path Delay Fingerprint," in Proc. of the *IEEE International Workshop on Hardware-Oriented Security and Trust (HOST 2008)*, pp. 51–57, 2008.
7. M. Tehranipoor and F. Koushanfar, "A Survey of Hardware Trojan Taxonomy and Detection," in *the IEEE Design & Test of Computers,* vol.27, no.1, pp. 10–25, 2010.
8. X. Wang, M. Tehranipoor, and J. Plusquellic, "Detecting Malicious Inclusions in Secure Hardware: Challenges and Solutions," in Proc. of the *IEEE International Workshop on Hardware-Oriented Security and Trust (HOST2008)*, pp. 15–19, 2008.
9. J. Li and J. Lach, "At-speed Delay Characterization for IC Authentication and Trojan Horse Detection," in Proc. of the *IEEE International Workshop on Hardware-Oriented Security and Trust (HOST08)*, pp. 8–14, 2008.
10. J. Markoff, "Old Trick Threatens the Newest Weapons," http://www.nytimes.com/2009/10/27/science/27trojan.html?_r=3&emc=etal
11. R. Rad, X. Wang, J. Plusquellic and M. Tehranipoor, "Power Supply Signal Calibration Techniques for Improving Detection Resolution to Hardware Trojans," in Proc. of the *International Conference on Computer-Aided Design (ICCAD08)*, pp. 632–639, 2008.
12. L. Wang, C. Wu, and N. Touba, "VLSI Test Principles and Architectures: Design for Testability," Morgan Kaufmann Publishers.
13. Y. Alkabani and F. Koushanfar, "Consistency-Based Characterization for IC Trojan Detection," in Proc. of the *International Conference on Computer-Aided Design (ICCAD09)*, pp. 123–127, 2009.
14. M. Potkonjak, A. Nahapetian, M. Nelson, and T. Massey, "Hardware Trojan Horse Detection Using Gate-Level Characterization," in Proc. of the *ACM/IEEE Design Automation Conference (DAC09)*, pp. 688–693, 2009.
15. S. Jha and S.K. Jha, "Randomization Based Probabilistic Approach to Detect Trojan Circuits," in Proc. of the *High Assurance Systems Engineering Symposium (HASE08)*, pp. 117–124, 2008.
16. F. Wolff, C. Papachristou, S. Bhunia, R.S. Chakraborty, "Towards Trojan Free Trusted ICs: Problem Analysis and Detection Scheme," in Proc. of the *Design, Automation and Test in Europe (DATE08)*, pp. 1362–1365, 2008.
17. I. Verbauwhede and P. Schaumont, "Design Methods for Security and Trust," in Proc. of the *Design, Automation and Test in Europe (DATE07)*, pp. 672–677, 2007.
18. G.E. Suh, D. Deng, and A. Chan, "Hardware Authentication Leveraging Performance Limits in Detailed Simulations and Emulations," in Proc. of the *ACM/IEEE Design Automation Conference (DAC09)*, pp. 682–687, 2009.
19. G. Bloom, B. Narahari, and R. Simha, "OS Support for Detecting Trojan Circuit Attacks," in Proc. of the *IEEE International Workshop on Hardware-Oriented Security and Trust (HOST09)*, pp. 100–103, 2009.

20. D. McIntyre, F. Wolff, C. Papachristou, S. Bhunia, D. Weyer, "Dynamic Evaluation of Hardware Trust," in Proc. of the *IEEE International Workshop on Hardware-Oriented Security and Trust (HOST09)*, pp. 108–111, 2009.
21. OECD (2007) http://www.oecd.org/dataoecd/13/12/38707619.pdf.
22. trust-HUB (2013) http://trust-hub.org/home.
23. U.S. Senate Committee on Armed Services (2012) Inquiry into Counterfeit Electronic Parts in the Department Of Defence Supply Chain http://www.armed-services.senate.gov/Publications/Counterfeit%20Electronic%20Parts.pdf.
24. U.S. Senate Committee on Armed Services (2012) Suspect Counterfeit Electronic Parts Can Be Found on Internet Purchasing Platforms http://www.gao.gov/assets/590/588736.pdf.
25. US Congress (2011) Ike Skelton National Defense Authorization Act for Fiscal Year 2011.
26. U.S. Department Of Commerce (2010) Defense Industrial Base Assessment: Counterfeit Electronics.
27. ERAI (2012) Electronic Resellers Association International (ERAI).
28. IHS (2012) Information Handling Services Inc.
29. IHS (2012) Reports of Counterfeit Parts Quadruple Since 2009, Challenging US Defence Industry and National Security.
30. IHS (2011) Top 5 Most Counterfeited Parts Represent a $169 Billion Potential Challenge for Global Semiconductor Market.
31. SAE (2012) SAE International.
32. CTI (2012) Components Technology Institute, Inc.
33. CTI (2011) Certification for Coutnerfeit Components Avoidance Program.
34. IDEA (2012) Independent Distributors of Electronics Association (IDEA).
35. CTI (2010) Comparison of AS 5553, CTI-CCAP-101B, and IDEA-STD-1010-A.
36. Pappu, R. (2001) Physical one-way functions.
37. Suh, G.E. and Devadas, S. (2007) Physical Unclonable Functions for Device Authentication and Secret Key Generation. Proc. of ACM/IEEE on Design Automation Conference: 9–14.
38. Kursawe, K. and Sadeghi, A.-R. and Schellekens, D. and Skoric, B. and Tuyls, P. (2009) Reconfigurable Physical Unclonable Functions - Enabling technology for tamper-resistant storage. Proc. of IEEE International Workshop on Hardware-Oriented Security and Trust: 22–29.
39. Kumar, S.S. and Guajardo, J. and Maes, R. and Schrijen, G.-J. and Tuyls, P. (2008) Extended abstract: The butterfly PUF protecting IP on every FPGA. Proc. of IEEE International Workshop on Hardware-Oriented Security and Trust: 67–70.
40. Bolotnyy, Leonid and Robins, Gabriel (2007) Physically Unclonable Function-Based Security and Privacy in RFID Systems. Proc. of IEEE International Conference on Pervasive Computing and Communications: 211–220.
41. Xiaoxiao Wang and Tehranipoor, M. (2010) Novel Physical Unclonable Function with process and environmental variations. Design, Automation Test in Europe Conference Exhibition: 1065–1070.
42. Alkabani, Yousra M. and Koushanfar, Farinaz (2007) Active hardware metering for intellectual property protection and security. 16th USENIX Security Symposium on USENIX Security Symposium: 20:1–20:16.
43. Lofstrom, K. and Daasch, W.R. and Taylor, D. (2000) IC identification circuit using device mismatch. Proc. of IEEE International Solid-State Circuits Conference: 372–373.
44. Lee, J.W. and Daihyun Lim and Gassend, B. and Suh, G.E. and van Dijk, M. and Devadas, S. (2004) A technique to build a secret key in integrated circuits for identification and authentication applications. Proc. of Digest of Technical Papers on VLSI Circuits: 176–179.
45. Su, Y. and Holleman, J. and Otis, B. (2007) A 1.6pJ/bit 96 % Stable Chip-ID Generating Circuit using Process Variations. Proc. of IEEE International on Solid-State Circuits Conference: 406–611.
46. Farinaz Koushanfar and Gang Qu and Miodrag Potkonjak (2001) Intellectual property metering. Information Hiding: 81–95.

47. Chakraborty, R.S. and Bhunia, S. (2008) Hardware protection and authentication through netlist level obfuscation. Proc. of IEEE/ACM International Conference on Computer-Aided Design: 674–677.
48. Alkabani, Yousra and Koushanfar, Farinaz and Potkonjak, Miodrag (2007) Remote activation of ICs for piracy prevention and digital right management. Proc. of IEEE/ACM international conference on Computer-aided design: 674–677.
49. Roy, J.A. and Koushanfar, F. and Markov, I.L. (2008) EPIC: Ending Piracy of Integrated Circuits. Proc. on Design, Automation and Test in Europe: 1069–1074.
50. Jiawei Huang and Lach, J. (2008) IC activation and user authentication for security-sensitive systems. Proc. of IEEE International Workshop on Hardware-Oriented Security and Trust: 76–80.
51. Baumgarten, A. and Tyagi, A. and Zambreno, J. (2010) Preventing IC Piracy Using Reconfigurable Logic Barriers. IEEE Design Test of Computers: 66–75.
52. Chakraborty, R.S. and Bhunia, S. (2009) HARPOON: An Obfuscation-Based SoC Design Methodology for Hardware Protection. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems: 1493–1502.