Lv YQ, Zhou Q, Cai YC *et al.* Trusted integrated circuits: The problem and challenges. JOURNAL OF COMPUTER SCIENCE AND TECHNOLOGY 29(5): 918–928 Sept. 2014. DOI 10.1007/s11390-014-1479-9

Trusted Integrated Circuits: The Problem and Challenges

Yong-Qiang Lv[1] (吕勇强), *Member*, *CCF*, *ACM*, *IEEE*
Qiang Zhou[1,2] (周　强), *Senior Member*, *CCF*, *ACM*, *IEEE*
Yi-Ci Cai[1,2] (蔡懿慈), *Senior Member*, *CCF*, *ACM*, *IEEE*, and Gang Qu[3] (屈　钢), *Senior Member*, *IEEE*

[1] *Tsinghua National Laboratory for Information Science and Technology, Research Institute of Information Technology Tsinghua University, Beijing 100084, China*

[2] *Department of Computer Science and Technology, Tsinghua University, Beijing 100084, China*

[3] *Department of Electrical and Computer Engineering, University of Maryland, College Park, MD 20742, U.S.A.*

E-mail: {luyq, zhouqiang, caiyc}@tsinghua.edu.cn; gangqu@umd.edu

Received April 10, 2014; revised May 19, 2014.

Abstract Hardware security has become more and more important in current information security architecture. Recently collected reports have shown that there may have been considerable hardware attacks prepared for possible military usage from all over the world. Due to the intrinsic difference from software security, hardware security has some special features and challenges. In order to guarantee hardware security, academia has proposed the concept of trusted integrated circuits, which aims at a secure circulation of IC design, manufacture and chip using. This paper reviews the main problems of trusted integrated circuits, and concludes four key domains of the trusted IC, namely the trusted IC design, trusted manufacture, trusted IP protection, and trusted chip authentication. The main challenges in those domains are also analyzed based on the current known techniques. Finally, the main limitations of the current techniques and possible future trends are discussed.

Keywords hardware security, trusted integrated circuit, hardware Trojan, IC authentication, IP protection

1 Introduction

IEEE Spectrum reported a notable incident of hardware security[1] that an Israeli Air Force attack on a suspected Syrian nuclear reactor did not receive any response from the Syrian air defense system in the year of 2007. The military and technology experts concluded that the commercial off-the-shelf microprocessors in the Syrian radar might have been purposely embedded with a hidden "backdoor" inside[1], which could disrupt the radar's function by a preprogrammed code sent by the attackers. This was also called as cyberwar, in which there are much more than what we have seen to be used to attack the hardware/chips and all sides in this battle are arming themselves to create Trojan and hide them deeply in computer and consumer electronics to facilitate the military attacks[2].

In January of 2014, the New York Times exposed that the American National Security Agency (NSA) has the ability to gather secret information from the unconnected computers even though they turn off the WiFi and any other known wireless and wired communication connections①. This is a part of the Quantum program of NSA, which is believed to have achieved much secret data from all over the world. What the Quantum program and the exposed ability of NSA shock people most is that the traditional *physical isolation* is already not secure. The hardware Trojans and backdoors are embedded into the chips, and people cannot trust the traditionally reliable chips any more. Those malicious pieces of circuits can bypass the software security facilities and spy the users, and the users cannot recognize them. The Trojans and backdoors are normally added to or revised from the original circuits in the design stage or in the manufacturing process of the chips. The traditional formal verification and testing tools cannot detect them yet, and the current design flow cannot guarantee such security either.

The hardware Trojans and backdoors can make the chip fault, fail, leak secrets, and lose control. In addition to these internal threats, the external attacks to the chips are also vital to the hardware security, such as the electro-magnetic attacks[3-4], scan-chain attacks[5-6], fault attacks[7-8]. They can cause the chip func-

Regular Paper

The work is supported by the National Natural Science Foundation of China under Grant No. 61228204 and the National Science and Technology Major Project of China under Grant No. 2013ZX01039001-002-003.

①The Quantum Program of NSA, http://www.nytimes.com/2014/01/15/us/nsa-effort-pries-open-computers-not-connected-to-internet.html, May 2014.

tions to be disturbed, failing, or faulty. Meanwhile, the piracy attacks to the intellectual property of the chips, such as reverse engineering, cracking, counterfeiting, and overbuilding[9], are also very critical for the chip owners, which may cause remarkable economical loss or security damage. The hardware security forms the very base of the whole information security and such threats have therefore become very urgent to solve.

2 Trust Model

All above issues can be classified into the category of the trusted integrated circuits (IC), which focus on the trustworthiness of chips in particular. The "trustworthiness" comes from the human being's word "trust", which means secure and reliable. There are three key points in this domain. Firstly, it requires the functions of the circuits are neither more nor less (no more and no less). The *less* can be examined in traditional verification and testing tools with regard to the design specification and the behavior description. However, the *more* is not easy to find out by the traditional methodology due to the absence of the corresponding techniques and tools. The Trojans and backdoors mentioned earlier are just the case of the *more*. Secondly, the intellectual property of the IC is also very important to protect and the trusted IP protection is therefore a crucial part of the trustworthiness of the IC. Thirdly, the chips will finally circulate in the market and be used by the end users, thus the trustworthiness for the end users to investigate from the chips is very important. The users should take the trusted authentication on the chips that they will use to guarantee their security. Readers can also refer to another review paper focusing on a subset of topics of this paper including the threat models, metrics, and the defense techniques[10].

In general, the model of the trustworthiness of the IC circulation can be concluded as shown in Fig.1. There are mainly five key participators in the circulation of the IC, namely 1) the chip vendor who invests to create the IC, 2) the IP vendor who offers the intellectual property cores for the chip vendor to integrate, 3) the third-party design team who is contracted to finish the design of the IC, 4) the foundry who is contracted to fabricate the IC, and 5) the end user who will use the chips.

Some chip vendors, such as TI, Qualcomm, have their own in-house design teams. However, the third-party design teams or the design service providers are often employed in modern complicated IC design, e.g., some EDA (Electronic Design Automation) tool providers often take such responsibilities. Furthermore, few chip vendors can have their own foundries. Nowadays, most chips are outsourced to third-party foundries to speed up the time-to-market and lower the cost. Therefore, from the perspectives of the chip/IP vendor and the end user, there are apparent trust issues introduced by such a multi-participant IC circulation.

Those trust issues can be classified and hence solved in the following four domains. 1) The trusted design, means that the designer implements the design specification with no more and no less. 2) The trusted manufacture, means that the foundry fabricates the chip without modifying the design. 3) The trusted chip/IP supply, means that the chip/IP vendor offers trusted chips/IPs with guaranteed reliability and without ma-

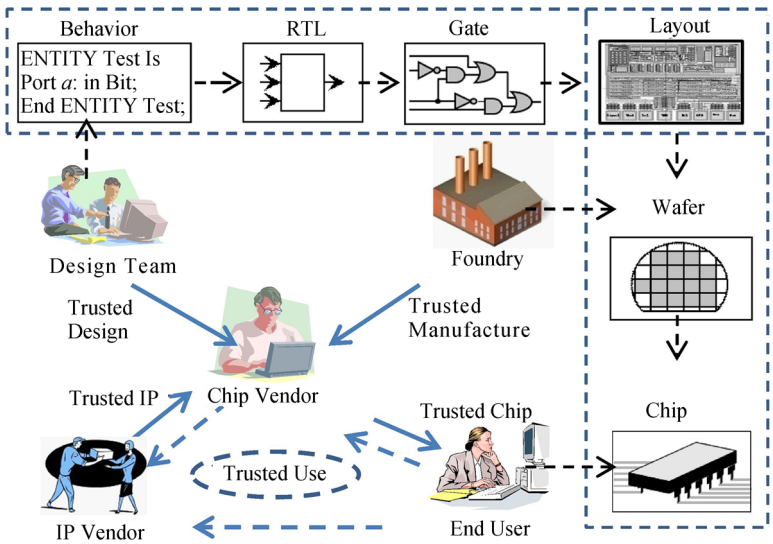

Fig.1. Model of the IC trustworthiness. The main participators of the IC circulation include the chip vendor, IP vendor, third-party design team, foundry, and end user. Some chip vendors may have their own in-house design teams.

licious circuits sneaked. 4) The trusted use, means the intellectual property contained in the chips or IPs is properly protected in using. The trusted IC design reflects the *trust* between the chip vendor and the IC designer. The trusted manufacture reflects the *trust* between the chip vendor and the foundry. The trusted IC/IP supply reflects the *trust* when the chip vendor sells the chip to the end user and the trusted use reflects the *trust* when the end user uses the chip bought from the chip vendor and when the SoC integrator uses the IP cores bought from the IP vendor. This is a sociological problem, but needs technical solutions. However, there are still severe challenges to solve. In those domains, the key challenges and current available techniques are analyzed respectively as follows.

3 Trusted IC Design and Trusted Manufacture

3.1 Challenges

The trust issues in the IC design process and the IC manufacture process are similar. Considering a general case of creating a chip, the chip vendor defines the design specification, i.e., the functional and nonfunctional requirements of the expected chip, and contracts the design task to a third-party design team. The design flow is often a very long process including multiple design stages and unpredictable changing orders and iterations in order for the convergence. The flow at least covers the logic design, layout design, testing and verification, which may be iterated for several loops. A standard design flow is shown in Fig.2, which often contains more pending design steps including the logic optimization, technology mapping, design planning, placement, routing, physical optimization, optical proximity correction (OPC), mask data preparation and so on. After the layout is formatted into the geometrics, e.g., OASIS or GDS-II, the design can then enter the foundry for tape-out.

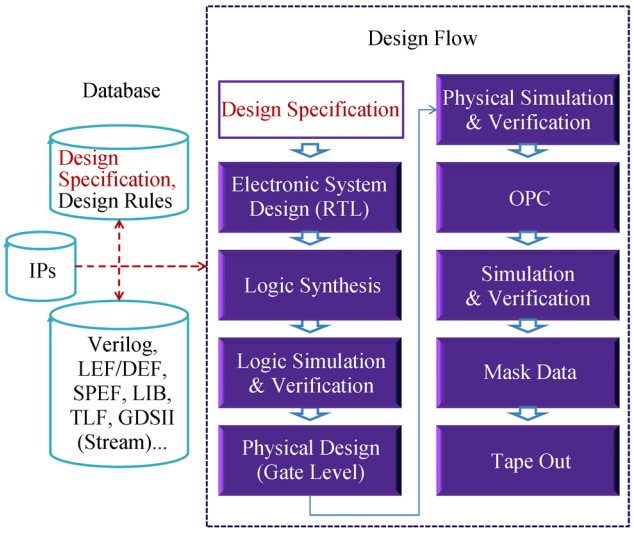

Fig.2. Design flow of ICs. The design steps may iterate rather than flow as the shown one-pass hierarchy.

Actually, there are often more third parties involved in this flow when designing complicated ICs even though the chip vendor has in-house design teams and they can have sufficient EDA tools too. The first reason is the widely used third-party IPs (3PIP) for fast time-to-market. In addition, the design-supporting teams from the EDA tool vendors, the fast design service providers aiming at some special design issues such as clock networks or timing closure and so on, are also often needed. Both the intended designing Trojans and the malicious IPs are the main threats to the trusted design flow[10].

In the foundry, there are still several key procedures to carry on, including layout examination, mask creation, wafer creation, photolithography, testing, packaging and so on. The foundry gives the packaged chips to the chip vendor for acceptance testing.

We can see that there are many opportunities for the advisories to inject the malicious circuits into the original design when they obtain the authorized access to the design data, e.g., the third-party optimization service to add malicious circuits in physical synthesis, or the mask creation to add extra masks of malicious circuits in the foundry. Traditional testing and verification tools cannot handle the "no more" but can handle the "no less" which guarantees the functions are correct. When there are hardware Trojan horses sneaked in the design, those tools cannot be aware. The key challenges to the trusted design and manufacture processes lie in: 1) the flow guarantee, such as the access control, flow adjustment, and security constraints, 2) the design techniques, such as anti-Trojan design techniques and secure IO design techniques, 3) testing and verification for security, such as Trojan detection, security verification and testing for IP cores or IC designs. The possible solutions corresponding to those challenges could be the research topics in the domain of trusted IC.

However, any security measure must have its own starting assumption. There could not be absolutely secure techniques free of any constraints. The detailed effectiveness analysis of the trusted design and manufacture methods is shown in Table 1. The trustworthiness guaranteeing techniques can be classified into four categories, namely design flow and techniques, manufacture techniques, testing, and verification. Each kind of methods has its own limitation of effectiveness.

Table 1. Limitation of the Effectiveness of Trusted Design and Manufacture Methods

Category	Limitation
Design techniques	Assume designers trusted and others not trusted
Manufacture techniques	Assume manufacturers trusted and others not trusted
Testing methods	Assume anyone not trusted
Verification	Assume anyone not trusted

3.2 Techniques Available

The malicious circuits, i.e., the hardware Trojan horses, may have many forms. Wang and his colleagues decomposed the taxonomy of the hardware Trojans through three categories[11], i.e., 1) the physical characteristics, 2) activation characteristics, and 3) action characteristics. Readers may refer to a further detailed taxonomy of the Trojans[12-13], which is very useful for better understanding the existing and potential threats.

In design and manufacture stages, the testing and the verification are ideal ways to guarantee the trustworthiness. However, it is a severe challenge to detect and locate the malicious circuits in the original design for them. For example, traditional testing and verification methods employ the satisfiability (SAT) model[14] to solve the functional tests to guarantee "no less", but the model cannot help on finding Trojan horses and backdoors. Some proactive techniques directed towards preventing insertion of Trojans[15] were proposed in last decades, including the dead space filling[11], obfuscation[16], the triggering silencing[17], and information hiding[18]. Dead space filling means that the designer fills the empty placement spaces where the possible redundant malicious circuits might be placed since any piece of circuit must have physical space to hold. The obfuscation against the Trojan insertion mainly means the logical obfuscation that makes it harder for the adversaries to understand and add malicious circuits properly. The designers can also employ the built-in-self-test logics (BIST) to defense the Trojans actively by signature examination in transparency mode[19] or on-chip inspection architecture[20-21]. However, those methods cannot guarantee the provable security and have apparent design overhead.

In design stages, the Trojan detection techniques can also be used. For example the detection heuristics based on the circuit features include the unused circuit identification (UCI) based Trojan-checking method[22] and unused input identification[23]. Those methods aim to find out the redundant unused circuits which may be malicious. The unused input identification improves the identification through investigating the chip input signals. It is based on the understanding that the Trojans must be triggered by certain inputs and those unused are mostly suspicious. The statistical optimal test vector generation[24] and the Automatic Test Pattern Generation (ATPG) methods based on design tricks (flip-flop insertion[25] and region partition[26]) were also proposed to improve the activation of Trojans. This category of methods cannot guarantee the detection precision and heavily relies on the vector generation.

In manufacture stage, the layout versus schematic (LVS) based verification may be used for detecting the Trojans inserted in the manufacturing stage. The netlist can be compared to its counterpart from the design stage after being extracted from the manufacture data of the chip. Furthermore, the chip owner can also employ the detecting techniques available for the design stage mentioned above to find out the Trojans based on the extracted suspicious netlist. After the manufacture, the Trojans sometimes are only embedded into some manufactured chips of a given design rather than all of them. The chip owners can use the gate-level characterization (GLC)[27] based post-manufacture Trojan detection methods, which aim to locate Trojans precisely through recovering the characteristics such as path delay[27], leakage current[28-29] of the gates on the target chip under test (CUT) with its circuit design known. The main challenges of this technique are to determine the process variation (PV) factors to build up the equations obtained from the circuit design and solve them to calculate the real delay or leakage current of the gates after they are manufactured, which affects much the detection precision. Meanwhile, the chip owners can also use the side channel based Trojan detection methods[30-32], but the effectiveness of such methods is subject to the noise and the measurement accuracy of equipments. The Trojans with small footprints may survive. Furthermore, the side channel based methods need the golden chip free of any Trojans to compare with, while the GLC-based methods do not need it. Post-manufacture methods focus on detecting Trojans to authenticate the trustworthiness of the chips, some of which also need design tricks to assist. Those methods are thus classified into the techniques for the trusted chips in this paper which are stated further in Section 5. Furthermore, Tehranipoor *et al.* also concluded in detail the design for Trojan prevention and Trojan detection in post-manufacture stages[13,33], which have supplemented technical details and are useful for readers to understand the methods further.

3.3 Key Issues to Solve

In summary, the current techniques mitigate the trustworthiness challenges in design and manufacture

stages. The main goal is to prevent or detect Trojans in a design. However, there are still several key issues to solve in the future.

- The flow-level trusted control is absent.
- The defense techniques do not have provable security although they have claimed promising usability with specific scenarios.
- The untrustworthy designers are not yet well handled in current techniques.

There is still an urgent requirement for the trusted design tools to realize the proposed security techniques from academia.

4 Trusted IP Protection for Trusted Use

4.1 Challenges

Intellectual property (IP) of the chip, meaning the valuable circuit designs, is the core of the IC industry. It means notable benefits of the owner. There are also various IP core providers offering well-designed functional blocks for the IC integrators (chip vendor) to integrate to speed up their chip designs. Providing IP cores is already an outstanding business in IC industry. The owners want their IP cores or chips secure against any infringement such as unauthorized copying, counterfeiting, overbuilding, and using. The academia and the industry have been devoting much effort to the IP protection, and there are even various strict governmental "embargo" laws in the military IC industry. However, the current protection to the intellectual property of the ICs is not secure enough yet, and the IP infringement results in a loss of 250 billion US dollars and 750 000 working positions per year all over the world②. Implicitly, the IP infringement can also cause inestimable damage to the innovation of the IC industry.

There are various types of IP infringement behaviours, including cracking license, piracy, overbuilding, counterfeiting, etc. The chip vendors often use licensing strategies to lock and protect the IP cores or the chips from unauthorized use. The adversaries can copy the authorized licenses directly or side-channel the secret licensing keys[34] to crack such locking. In comparison with the attack to the licensing, the others aim at the design content contained in the chips. Piracy[34-35] activities try to copy or tamper the original designs of the IP cores or chips and reproduce them. Overbuilding[36-37] happens when the untrustworthy manufactures fabricate more chips than what the chip owners expect, or the untrustworthy IC integrators (chip owners) produce and sell more chips with the IP cores than what the IP owners expect. Counterfeiting[38] is to make faked IC. The adversaries forge or imitate the original chips, make up these low-quality faked chips like the genuine ones and sell them to profit.

Different from the software attacks, the chips are not easy to trace from inside the gates and netlists of the layout due to the very deep submicron technologies. Nevertheless, there are still some powerful attacking techniques available for accessing the internal secrets and contained designs of the chips, for example, the side channel[39], scan chain attacks[40], and reverse engineering[41]. Side channel and scan chain attacks exploit the internal information of the chip, e.g., the key, by collecting and analyzing the leaked information. Side channel attacks use electromagnetic information, such as power, current, delay, heat, and light. Scan chain attacks use the scan chains of the testing infrastructure. Side channel has broken all major hardware cryptographic algorithms[10,42]. Reverse engineering can infer the chip functions, identify the manufacture technologies, and even extract the gate-level circuit designs by IO testing, micro-probing, laser or X-ray scanning and imaging, and so on. Both side channel and reverse engineering are just techniques. They do not mean illegal and can be used in legal ways.

The chip and IP core owners want a trusted method to protect their IP from infringement so that they do not need to worry about the adversary users. Unless the protecting method is provably secure, it cannot be regarded as trusted from the technical perspective. However, it is a very severe challenge to setup such a secure IP protection methodology or a series of methods to form the trusted base. There is still much space to improve.

4.2 Techniques Available

Current IP-protecting techniques can be classified into two categories. The first category is the passive protections. Designers can embed the watermarks into the design, which can be inherited and manufactured[43-45]. The watermarks can be extracted from the chips to verify as long as the chips are suspicious of piracy or counterfeiting. In order to realize the verification on every single piece of chip, the hardware fingerprinting was applied[46-48]. The hardware fingerprints utilize the process variation in IC manufacturing and have the capacity to be calculated and examined for each chip. Directly embedding and checking the watermarks or fingerprints cannot prevent the IP infringement. Therefore, the proactive protecting techniques were invented and account for the mainstream of the IP protecting techniques.

② Advancing Intellectual Property Protection, http://www.agmaglobal.org/, May 2014.

Encryption methods based on securely stored keys[49] can protect the hardware IPs from piracy, unauthorized use via licensing. However, the key storage is not always secure against side channel and reverse engineering. In order to implement the licensing of pay-per-use and pay-per-device, the software-hardware binding protection techniques were also proposed[50-51] based on PUF or stored-keys. The PUF (or physical fingerprinting) based licensing strategy is secure against piracy, overbuilding, and counterfeiting, but the replay attacks and reverse engineering are still the most outstanding threats to such licensing strategies.

IC metering methods[52-53] can prevent the IC design from overbuilding. They use the physical fingerprinting and lock the combinational logic or sequential logic functions of the chip so that only the right authorized licenses from the owner can unlock the design. The basic idea is that they create a physical unclonable identifier (ID) for the chip and use it to control the correct transitions of the finite state machines (FSM) of the circuit. The circuit behaves correctly only on the authorized chips with right physical unclonable IDs. Any overbuilt copies cannot have the same IDs with any of the authorized ones due to the uncontrolled physical variations in manufacturing and therefore cannot work. Although Koushanfar proposed a secure FSM construction method against the reverse engineering[53], the current IC metering is still not secure against the reverse engineering and side channel attacks to the physical unclonable identifiers and the data paths to access to the IDs.

Counterfeiting has brought severe performance degradation and posed real security threats for ICs because the counterfeiters may sell mislabelled, used/old/recycled ICs to customers and those fake ICs may have been inserted hardware Trojans or spywares. Mislabelled chips can be detected by visual inspection, depackaging, or X-ray photography of the packages[54]. Used/old/recycled ICs can also be recognized by detecting their aging or reliability heuristically[55]. The physical fingerprint based IP protecting and IC metering techniques may be used in preventing counterfeiting via proper licensing schemes. However, the licensing updating and the method to prevent replay attacks (downgrading attacks especially for FPGA products) are the issues to solve. Take the replay attack as an example: the adversaries may use the licenses from the older versions to the updated products, which may make the system still work without paying for the new licenses.

Reverse engineering is a technique to identify IC's structure, design, and functionality. Reverse engineering has been widely used to legally collect competitive intelligence, and check for commercial piracy and patent infringements. It can invasively extract the gate-level netlist through package removing, delayering, imaging, annotation, schematic read-back, and functional analysis. Unfortunately, reverse engineering is also widely used to crack, pirate, and counterfeit the chip/design. To prevent the reverse engineering, the logic obfuscation techniques based on redundant finite state machines[16] and gate insertion[36,43] were invented to obfuscate partial combinational and sequential logic function of design, which can make it confusing and hard to interpret. Authors of [44] proposed a memory-based obfuscation method that hides the key parts of the design by storing the true tables into a memory. Camouflaging[45] is a layout-level obfuscating technique designing the logic blocks as the same physical layouts to resist image processing based extraction of a gate-level netlist from a chip. However, those techniques cannot prevent cloning, counterfeiting, and overbuilding. Their security against reverse engineering is also not theoretically proved or convincing. The side channel attacks, logic testing, and micro probing may still threaten their security.

4.3 Key Issues to Solve

In summary, the current techniques for IP protection have mostly covered the important aspects in this domain. The IP infringement behaviours, including the licensing crack, piracy, overbuilding, and counterfeiting, often employ various attack techniques, such as copy, cloning, side channel, and reverse engineering. There are many passive and proactive IP-protecting techniques proposed to prevent the IP infringement behaviours. However, there are still several key issues to solve in the future.

• There is still no technique able to prevent all the main IP infringement behaviours in one framework.

• Reverse engineering can still dramatically threaten the IP security.

• A trusted IP protection methodology and its infrastructures are still absent.

There are no usable tools available in this domain yet, and the current academic methods still have severe usability issues.

5 Trusted Chip/IP Authentication for Users

5.1 Challenges

In the view of the end users (the chip vendors are considered as the end users of the third-party IP providers), they care about their chips/IPs purchased from the vendors, hope them free of any Trojan horses, backdoors, and are reliable against the external vari-

ance. This is a requirement of trust when a customer buys a product. In fact, however, it can hardly be met. As mentioned earlier, various sources of reports have shown that some of the chips currently circulating are definitely not clean. The Prism plan and the Quantum plan of NSA have made people's information environment extremely untrustworthy. The political and military competition among countries may make the chips evil in today's highly international industry.

The end users should be partitioned at least into two categories, i.e., professional and nonprofessional users. The professional means those having the access to the professional examination and detection platforms, tools, and techniques for ICs; the unprofessional means those without such access. They need some measures to help authenticate the trustworthiness of the chips, which, however, is not realistic yet. There are neither professional tools nor general methods for both categories of users to authenticate the chips.

Similar to human society, the most general and convenient method to authenticate a chip is to examine its unique identification. Traditional methods eligible for such a goal include the nonvolatile memory-stored identifier[49], watermark[56], physical fingerprint[46] including physical unclonable functions (PUF)[57-58], etc. The memory-stored identifier is not secure against piracy. The watermark and some physical fingerprints (e.g., the leakage current based fingerprint) are not perfectly readable or checkable after packaging. The PUF utilizes the uncontrollable process variations during the production of IC to generate a unique signature for each IC. It is a very promising secure primitive for hardware security. However, the stability and security of PUF is still an issue to solve in identifying a trusted chip. A perfect fusion with the readability, stability, and security of the identification method is the main challenge in this domain.

Identification-based methods are not suitable for authenticating third-party IPs (3PIP) due to the following two reasons. 1) There are often many IP cores integrated to a single design, which may cause high cost to have the identifiers. 2) The IPs may be provided in either soft cores (RTL codes) or hard cores (library macros), which results in the difficulty to find proper identifying methods.

The identification-based methods are not yet sufficient for authenticating a trusted chip. More professional tools and techniques should be developed in examining the trustworthiness of an IC-under-authentication (IUA). The end user cannot access any internal design details except for the packaged IOs after obtaining the chips. Using noninvasive technologies to explore the sneaked malicious circuits and potential security weakness may be a low-cost and efficient choice for the professional users in comparison with extracting the layout via reverse engineering invasively. Side channel and scan chain scanning are known methods available in this domain. The Trojans can be detected via monitoring and analyzing the leaked physical information, such as power[30], delay[31], or by scanning the scan chains[59] via the testing entries of the chips. However, the effects of such methods may heavily depend on the measurement accuracy of the side channels, the golden version of the chip, and the precision of the calculation models or the design tricks. The precision and the resolution of finding the Trojans are often hard to meet.

It becomes much more complex when the SoC integrator wants to authenticate or verify the third-party IP cores due to the absence of the golden version. For the soft cores, the trusted design verification techniques stated earlier are available. However, for the hard cores, only the methods without needing the golden version are eligible.

Regarded as an end user's tool, it needs a good balance between the cost and the security for trusted chip authentication in adapting to the requirements of the professional and the unprofessional users. A trusted third-party may be required in the chip identification based chip authentication. Provably secure methods will be the candidate choices for the professional users, which is a severe challenge yet to solve. The design examination methods employed in trusted IC design, e.g., the layout verification, may also be considered when the reverse engineering is available.

5.2 Techniques Available

The IC identification and examination methods can be used to authenticate the trustworthiness of a chip. There are four kinds of techniques available for IC identification. The first is the direct nonvolatile memory-stored identifier[49], which has been widely used in computer hardware (e.g., MAC address), FPGAs. However, this technique is easy to be cloned, micro-probed or side channel[35]. Another technique is watermark[56]. The designer embeds some hiding information (watermark) into the circuit, which can be extracted after manufacture. However, the watermark is statically embedded into the circuit and it cannot differentiate a specific chip uniquely (every chip has the same watermark), and all the produced chips have the same watermark. Fingerprinting[46] is a physical technique which can extract the unique identifier from each manufacture chip due to the process variations. The delay, power, and leakage current can be utilized to calculate the physical fingerprint of a chip. More specifically, the physical un-

clonable function (PUF) is a piece of well-designed circuit embedded into the original circuit design, which can give the unique and unclonable outputs regarded as a physical fingerprint of the chip after manufacture. Due to its outstanding security and good usability (readable, stable, and unique), PUF has been a well-known promising security primitive. Using those techniques to make identifiers of the chips, users can trace their originations and obtain an authentication supported by a trusted third party.

As mentioned earlier, the identification-based methods are not suitable for third-party IP core (3PIP) authentication due to the cost and implementation difficulty. The trustworthiness verification techniques stated in the section of the trusted design techniques are the possible candidates for the soft IP core authentication. Tehranipoor *et al.* proposed a theoretical overview on the possible techniques for the trustworthiness verification of the soft 3PIP cores[33], including the formal verification, code coverage analysis for redundant circuits and testing. For the hard IPs provided in the form of layout macros (as a library), it is more difficult to detect the Trojans since there are no golden versions present for the IPs. Among the Trojan-detecting methods stated in the following paragraph, the possible candidates to verify the trustworthiness of the hard 3PIPs may be those without needing the golden version of the chip, which is actually not perfectly solved yet.

For the users with more technological capacities, the invasive and noninvasive chip authentication methods may be employed to verify if there are Trojans or backdoors sneaked in the chip. The noninvasive methods mainly include the side channel, testing, and mathematical model based methods. Invasive methods mainly refer to the reverse engineering methods. Agrawal *et al.* proposed a side channel based power analysis method to detect Trojans embedded in a chip[30]. The basic idea is to capture the power profile signatures by comparing the golden chip and the infected chips. As long as the Trojans work, they consume extra power compared with the clean chips. Later, many other side channel methods were developed, including the delay analysis[31-32], power supply analysis[60], and comprehensive methods[61]. They have the same motivation and similar methodology as the power side channel. The effectiveness of such methods is subject to the noise and the measurement accuracy of equipments, and the Trojans with small footprints may survive. They also need a purely clean (golden) chip free of Trojans to compare with. In order to improve the effectiveness, some design tricks (Design for Trust)[13,33] were employed in design stages to improve the Trojan activities in either test-time or run-time testing[14], e.g., the flip-flop insertion[25], region partition[26], and sensor manipulation[62]. In order to give better Trojan resolution without golden chips, authors of [27] proposed the gate-level characterization (GLC) based post-manufacture Trojan detection methods, which aimed to locate Trojans precisely through recovering the characteristics such as path delay[27], leakage current[28-29] of the gates on the target chip under test (CUT) with its circuit design known. The linear and nonlinear equations with measured delay or leakage current values from the measuring points of CUT are built. The statistical analysis after certain number of simulations on the CUT validates the Trojans detection. One of the main challenges of this technique is to determine the process variation (PV) factors to build up the equations obtained from the circuit design and solve them to calculate the real delay or leakage current of the gates after they are manufactured. Another problem of this technique is its difficulty in practice due to 1) the selecting of the candidate parts of the circuit to calculate and 2) the heuristics used affecting the precision of the detection. The authors of [62] proposed a comprehensive method to combine the design techniques (adding temperature sensors), post-manufacture techniques (side channels), and test-time and run-time techniques together to improve the precision of post-manufacture Trojan detection with known clean circuit design and without the golden chip.

In addition to the noninvasive methods, the reverse engineering methods can also help analyze and locate the possible malicious circuits after recovering the netlist of the chip. It may improve the efficiency to combine the noninvasive methods with the reverse engineering to analyze the target chips comprehensively especially when there is neither the golden chip nor the design content present.

5.3 Key Issues to Solve

In summary, the current techniques for trusted chip authentication can mainly be concluded into the IC identification and post-manufacture trustworthiness authentication. Physical fingerprinting including the physical unclonable functions (PUF) utilizes the process variation of manufacture and has good security features. The identification-based chip authentication is suitable for the average use. The post-manufacture Trojan detection methods are the known important techniques for authenticating the trustworthiness of the chip for the end users. The GLC-based methods need the design content of the chip, while the side channel based methods need the golden chip. The end users can select based on their actual situation. There are still several key issues to solve in the future.

• Average users cannot have the access to the circuit design of the chip, and it is still a problem to detect Trojans precisely without the golden chip or the design content.

• The precision and usability of the post-manufacture Trojan detection has still much space to improve.

• There is still no general chip authentication methodology or framework available for the IC industry.

In chip authentication, the reverse engineering may be another candidate despite of its high cost. It can help recover the design content and the techniques in design stages can thus be used to help locate the Trojans.

6 Conclusions

Hardware security has played a more and more important role in current information security infrastructure. Known reports and exposed facts have shown that there are severe hardware security problems in general consumer electronics and application-specific ICs. This paper proposed the trust model meant by a trusted IC aiming at the guaranteed security, which contains five key roles (players) and four key trusted issues, namely trusted design, trusted manufacture, trusted IC supply, and trusted IC using. The trust model indicates that the main research work in this domain should concentrate on the techniques and methods in trusted design and manufacture, trusted IP protection, and trusted chip authentication. According to a comprehensive review on the current technologies, we can see that the current key challenges to the trusted IC are mainly presented in the domains of IC design, IC manufacture, IP protection, and the chip authentication.

Although current techniques have been focusing on those issues for couple of years, there are still clear limitations in those key domains, which may become the future trends of the research. The limitations of the current techniques and the possible future research trends include:

1) Trusted IC Design and Manufacture

• The flow-level trusted control is currently absent.

• The current defending techniques do not have provable security although they have claimed promising usability with specific scenarios.

• The untrustworthy designers are not yet well handled in current techniques.

2) Trusted IP Protection

• There is still no technique able to prevent all the main IP infringement behaviours in one framework.

• Reverse engineering can still dramatically threaten the IP security.

• A trusted IP protection methodology and its infrastructures are still absent.

3) Trusted Chip Authentication

• It is hard to be solved to detect Trojans precisely without the golden chip and design knowledge.

• The precision and usability of the post-manufacture Trojan detection has still much space to improve.

• There is still no general chip authentication methodology or framework available for the IC industry.

Furthermore, all the proposed techniques from the academia have limited usability and there is still much space to improve before they become eligible EDA tools.

References

[1] Adee S. The hunt for the kill switch. *IEEE Spectrum*, 2008, 45(5): 34-39. http://spectrum.ieee.org/semiconductors/design/the-hunt-for-the-kill-switch, May 2014.

[2] Markoff J. CYBERWAR: Old trick threatens the newest weapons. The New York Times, Oct. 2009. http://www.nytimes.com/2009/10/27/science/27trojan.html?_ r=2&pagew, Apr. 2014.

[3] De Mulder E, Örs S B, Preneel B *et al.* Differential power and electromagnetic attacks on a FPGA implementation of elliptic curve cryptosystems. *Computers and Electrical Engineering*, 2007, 33(5/6): 367-382.

[4] Dehbaoui A, Lomne V, Maurine P *et al.* Enhancing electromagnetic attacks using spectral coherence based cartography. In *VLSI-SoC: Technologies for Systems Integration*, Becker J, Johann M, Reis R (eds.), Springer Berlin Heidelberg, 2011, pp.135-155.

[5] Da Rolt J, Di Natale G, Flottes M L *et al.* New security threats against chips containing scan chain structures. In *Proc. IEEE International Symposium on Hardware-Oriented Security and Trust* (*HOST*), June 2011, p.110.

[6] Yang B, Wu K, Karri R. Secure scan: A design-for-test architecture for crypto chips. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 2006, 25(10): 2287-2293.

[7] Bar-El H, Choukri H, Naccache D *et al.* The sorcerer's apprentice guide to fault attacks. *Proceedings of the IEEE*, 2006, 94(2): 370-382.

[8] Aumüller C, Bier P, Fischer W *et al.* Fault attacks on RSA with CRT: Concrete results and practical countermeasures. In *Proc. the Cryptographic Hardware and Embedded Systems* (*CHES*), Aug. 2002, pp.260-275.

[9] Yuan L, Qu G, Ghouti L *et al.* VLSI design IP protection: Solutions, new challenges, and opportunities. In *Proc. the 1st IEEE NASA/ESA Conference on Adaptive Hardware and Systems*, June 2006, pp.469-476.

[10] Rostami M, Koushanfar F, Rajendran J, Karri R. Hardware security: Threat models and metrics. In *Proc. International Conference on Computer-Aided Design*, Nov. 2013, pp.819-823.

[11] Wang X, Tehranipoor M, Plusquellic J. Detecting malicious inclusions in secure hardware: Challenges and solutions. In *Proc. IEEE Int. Workshop Hardware-Oriented Security and Trust* (*HOST*), June 2008, pp.15-19.

[12] Karri R, Rajendran J, Rosenfeld K, Tehranipoor M. Trustworthy hardware: Identifying and classifying hardware Trojans. *IEEE Computer*, 2010, 43(10): 39-46.

[13] Tehranipoor M, Koushanfar F. A survey of hardware Trojan taxonomy and detection. *IEEE Design & Test of Computers*, 2010, 27(1): 10-25.

[14] Biere A, Cimatti A, Clarke E M *et al.* Symbolic model checking using SAT procedures instead of BDDs. In *Proc. the 36th ACM/IEEE conference on Design automation* (*DAC*), June 1999, pp.317-320.

[15] Chakraborty R S, Narasimhan S, Bhunia S. Hardware Trojan: Threats and emerging solutions. *IEEE International High Level Design Validation and Test Workshop*, Nov. 2009, pp.166-171.

[16] Chakraborty R S, Bhunia S. Security against hardware Trojan through a novel application of design obfuscation. In *Proc. IEEE/ACM Int. Conf. Computer-Aided Design* (*ICCAD*), Nov. 2009, pp.113-116.

[17] Waksman A, Sethumadhavan S. Silencing hardware backdoors. In *Proc. IEEE Symposium on Security and Privacy*, May 2011, pp.49-63.

[18] Gu J, Qu G, Zhou Q. Information hiding for trusted system design. In *Proc. the 46th ACM/IEEE Design Automation Conference* (*DAC*), July 2009, pp.698-701.

[19] Chakraborty R S, Paul S, Bhunia S. On-demand transparency for improving hardware Trojan detectability. In *Proc. Hardware-Oriented Security and Trust* (*HOST*), June 2008, pp.48-50.

[20] Kim L W, Villasenor J D, Koc C K. A Trojan-resistant system-on-chip bus architecture. In *Proc. Int. Conf. Military Communication*, Oct. 2009.

[21] Abramovici M, Bradley P. Integrated circuit security: New threats and solutions. In *Proc. the 5th Cyber Security and Information Intelligence Research Workshop*, Apr. 2009, Article No.55.

[22] Hicks M, Finnicum M, King S T *et al.* Overcoming an untrusted computing base: Detecting and removing malicious hardware automatically. In *Proc. IEEE Symposium on Security and Privacy*, May 2010, pp.159-172.

[23] Zhang J, Yuan F, Wei L *et al.* VeriTrust: Verification for hardware trust. In *Proc. the 50th Annual Design Automation Conference*, May 29-June 7, 2013, pp.1-8.

[24] Chakraborty R S, Wolff F, Paul S. MERO: A statistical approach for hardware Trojan detection. In *Proc. the 11th Workshop on Cryptographic Hardware and Embedded Systems* (*CHES*), Sept. 2009, pp.396-410.

[25] Salmani H, Tehranipoor M, Plusquellic J. A novel technique for improving hardware Trojan detection and reducing Trojan activation time. *IEEE Transactions on VLSI*, 2012, 20(1): 112-125.

[26] Banga M, Hsiao M S. A region based approach for the identification of hardware Trojans. In *Proc. IEEE International Workshop on Hardware-Oriented Security and Trust* (*HOST*), June 2008, pp.40-47.

[27] Potkonjak M, Nahapetian A, Nelson M, Massey T. Hardware Trojan horse detection using gate-level characterization. In *Proc. the 46th Design Automation Conference* (*DAC*), July 2009, pp.688-693.

[28] Cha B, Gupta S K. Trojan detection via delay measurements: A new approach to select paths and vectors to maximize effectiveness and minimize cost. In *Proc. Conference on Design, Automation and Test in Europe*, Mar. 2013, pp.1265-1270.

[29] Wei S, Meguerdichian S, Potkonjak M. Malicious circuitry detection using thermal conditioning. *IEEE Transactions on Information Forensics and Security*, 2011, 6(3): 1136-1145.

[30] Agrawal D, Baktir S, Karakoyunlu D *et al.* Trojan detection using IC fingerprinting. In *Proc. IEEE Symposium Security and Privacy*, May 2007, pp.296-310.

[31] Jin Y, Makris Y. Hardware Trojan detection using path delay fingerprint. In *Proc. IEEE International Workshop on Hardware-Oriented Security and Trust* (*HOST*), June 2008, pp.51-57.

[32] Skorobogatov S, Woods C. Breakthrough silicon scanning discovers backdoor in military chip. In *Proc. the 14th Workshop on Cryptographic Hardware and Embedded Systems* (*CHES*), Sept. 2012, pp.23-40.

[33] Tehranipoor M, Salmani H, Zhang X *et al.* Trustworthy hardware: Trojan detection and design-for-trust challenges. *IEEE Computer*, 2011, 44(7): 66-74.

[34] Yang B, Wu K, Karri R. Scan based side channel attack on dedicated hardware implementations of data encryption standard. In *Proc. IEEE International Test Conference*, Oct. 2004, pp.339-344.

[35] Koushanfar F. Hardware metering: A survey. In *Introduction to Hardware Security and Trust*, Tehranipoor M, Wang C (eds.), Springer New York, 2012, pp.103-122.

[36] Roy J, Koushanfar F, Markov I. Ending piracy of integrated circuits. *IEEE Computer*, 2010, 43(10): 30-38.

[37] Chakraborty R S, Bhunia S. HARPOON: An obfuscation-based SoC design methodology for hardware protection. *IEEE Trans. Computer-Aided Design of Integrated Circuits and Systems*, 2009, 28(10): 1493-1502.

[38] Moudgil R, Ganta D, Nazhandali L *et al.* A novel statistical and circuit-based technique for counterfeit detection in existing ICs. In *Proc. the 23rd ACM International Conference on Great Lakes Symposium on VLSI*, May 2013, pp.1-6.

[39] Kocher P, Jaffe J, Jun B. Differential power analysis. In *Proc. the 19th Advances in Cryptology*, May 1999, pp.388-397.

[40] Rolt J D, Natale G D, Flottes M *et al.* A novel differential scan attack on advanced DFT structures. *ACM Transactions on Design Automation of Electronic Systems*, 2013, 18(4): Article No.58.

[41] Torrance R, James D. The state-of-the-art in semiconductor reverse engineering. In *Proc. the 48th IEEE/ACM Design Automation Conference* (*DAC*), June 2011, pp.333-338.

[42] Rohatgi P. Improved techniques for side-channel analysis. In *Cryptographic Engineering*, Koç Ç K (ed.), Springer US, pp.381-406.

[43] Rajendran J, Pino Y, Sinanoglu O, Karri R. Security analysis of logic obfuscation. In *Proc. the 49th IEEE/ACM Design Automation Conference* (*DAC*), June 2012, pp.83-89.

[44] Baumgarten A, Tyagi A, Zambreno J. Preventing IC piracy using reconfigurable logic barriers. *IEEE Design and Test of Computers*, 2010, 27(1): 66-75.

[45] Rajendran J, Sam M, Sinanoglu O, Karri R. Security analysis of integrated circuit camouflaging. In *Proc. ACM SIGSAC Conference on Computer & Communications Security* (*CCS*), Nov. 2013, pp.709-720.

[46] Qu G, Potkonjak M. Fingerprinting intellectual property using constraint-addition. In *Proc. the 37th IEEE/ACM Design Automation Conference* (*DAC*), June 2000, pp.587-592.

[47] Lach J, Mangione-Smith W H, Potkonjak M. Fingerprinting digital circuits on programmable hardware. In *Proc. the 2nd Int. Workshop on Information Hiding*, April 1998, pp.16-31.

[48] Qu G, Potkonjak M. Intellectual Property Protection in VLSI Design. Springer, 2003.

[49] Smerdon M. Security solutions using Spartan-3 generation FPGAs (v1.1). Xilinx White Paper, Apr. 2008, http://www.xilinx.com/support/documentation/white_papers/wp266.pdf, May 2014.

[50] Zhang J, Lin Y, Lyu Y *et al.* FPGA IP protection by binding finite state machine to physical unclonable function. In *Proc. the 23rd Field Programmable Logic and Applications* (*FPL*), Sept. 2013.

[51] Maes R, Schellekens D, Verbauwhede I. A pay-per-use licensing scheme for hardware IP cores in recent SRAM-FPGAs.

IEEE Trans. Information Forensics and Security, 2012, 7(1): 98-108.

[52] Alkabani Y, Koushanfar F, Potkonjak M. Remote activation of ICs for piracy prevention and digital right management. In *Proc. IEEE/ACM International Conference on Computer-Aided Design* (*ICCAD*), Nov. 2007, pp.674-677.

[53] Koushanfar F. Provably secure active IC metering techniques for piracy avoidance and digital rights management. *IEEE Trans. Information Forensics and Security*, 2012, 7(1): 51-63.

[54] Chatterjee K, Das D. Semiconductor manufacturers' efforts to improve trust in the electronic part supply chain. *IEEE Trans. Components and Packaging Technologies*, 2007, 30(3): 547-549.

[55] Huang K, Carulli J, Makris Y. Parametric counterfeit IC detection via support vector machines. In *Proc. IEEE Int. Symp. Defect and Fault Tolerance in VLSI and Nanotechnology Systems*, Oct. 2012, pp.7-12.

[56] Cui A, Chang C, Tahar S *et al.* A robust FSM watermarking scheme for IP protection of sequential circuit design. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 2011, 30(5): 678-690.

[57] Yin C, Qu G. Temperature-aware cooperative ring oscillator PUF. In *Proc. IEEE International Workshop on Hardware-Oriented Security and Trust* (*HOST*), July 2009, pp.36-42.

[58] Zhang J, Wu Q, Lyu Y *et al.* Design and implementation of a delay-based PUF for FPGA IP protection. In *Proc. CAD/CG*, Oct. 2013, pp.1-6.

[59] Salmani H, Tehranipoor M. Layout-aware switching activity localization to enhance hardware Trojan detection. *IEEE Transactions on Information Forensics and Security*, 2012, 7(1): 76-87.

[60] Rad R, Plusquellic J, Tehranipoor M. Sensitivity analysis to hardware Trojans using power supply transient signals. In *Proc. IEEE International Workshop on Hardware-Oriented Security and Trust* (*HOST*), June 2008, pp.3-7.

[61] Bhunia S, Abramovici M, Agrawal D *et al.* Protection against hardware Trojan attacks: Towards a comprehensive solution. *IEEE Design and Test*, 2013, 30(3):6-17.

[62] Forte D, Bao C, Srivastava A. Temperature tracking: An innovative run-time approach for hardware Trojan detection. In *Proc. IEEE/ACM International Conference on Computer-Aided Design* (*ICCAD*), Nov. 2013, pp.532-539.

Yong-Qiang Lv is an assistant professor in the Research Institute of Information Technology at Tsinghua University, Beijing. He received his B.S. degree in computer science from Xidian University, Xi'an, in 2001, M.S. and Ph.D. degrees in computer science from Tsinghua University, in 2003 and 2006 respectively. His research interests include hardware-software fusion architecture and hardware security. He also leads an interdisciplinary team at Tsinghua University working on the innovative cyber-physical architectures and systems from a fusion perspective of computer science, art and medicine.

Qiang Zhou received his B.S. degree in computer science and technology from the University of Science and Technology of China in 1983, M.S. degree in computer science and technology from Tsinghua University in 1986, and Ph.D. degree in control theory and control engineering from Chinese University of Mining and Technology in 2002. His research interests include VLSI layout theory and algorithms.

Yi-Ci Cai is a professor in the Department of Computer Science and Technology, Tsinghua University. She received her B.S. degree in electronic engineering from Tsinghua University in 1983, M.S. degree in computer science and technology from Tsinghua University in 1986, and Ph.D. degree in computer science from the University of Science and Technology of China in 2007. Her research interests include design automation for VLSI integrated circuits algorithms and theory, power/ground distribution network analysis and optimization, high performance clock synthesis, and low power physical design.

Gang Qu received his B.S. and M.S. degrees in mathematics from the University of Science and Technology of China, in 1992 and 1994, respectively, and Ph.D. degree in computer science from the University of California, Los Angeles, in 2000. Upon graduation, he joined the University of Maryland at College Park, where he is currently a professor in the Department of Electrical and Computer Engineering and the Institute for Systems Research. He is also a member of the Maryland Cybersecurity Center and the Maryland Energy Research Center. Dr. Qu is the director of Maryland Embedded Systems and Hardware Security Lab and the Wireless Sensors Laboratory. His primary research interests are in the area of embedded systems and VLSI (Very Large Scale Integration) CAD (Computer Aided Design) with focus on low power system design and hardware related security and trust. He studies optimization and combinatorial problems and applies his theoretical discovery to applications in VLSI CAD, wireless sensor network, bioinformatics, and cyber-security. Dr. Qu has received many awards for his academic achievements, teaching, and service to the research community. He is a senior member of IEEE and serving as associate editor for the IEEE Transactions on Computers, IEEE Embedded Systems Letters and Integration, and the VLSI Journal.