Designing Chips that Protect Themselves

Farinaz Koushnafar[1], Igor Markov[2]

[1] *Electrical and Computer Engineering Dept., Rice University, Houston, TX, USA*

[2] *Electrical Engineering and Computer Science Dept., University of Michigan, Ann Arbor, MI, USA*

ARTICLE: Trusted ICs

Designing Chips that Protect Themselves

Farinaz Koushanfar[1] and Igor Markov[2]

[1] *Electrical and Computer Engineering Department, Rice University, Houston, TX, USA*
[2] *Electrical Engineering and Computer Science Department, University of Michigan, Ann Arbor, MI, USA*

Abstract— Leading-edge integrated circuits can cost more than their weight in gold and often control electronic systems of far greater value. However, few mechanisms are currently available to protect investments made by individuals, commercial entities and institutions in electronic products and related intellectual property (IP). Hardware piracy has reached an unprecedented scale and fuels serious threats of subversion by malicious insertions (Trojans). These threats have been articulated by business and military strategists, and confirmed by forensic security experts analyzing recent incidents. In particular, software and network systems running on subverted chips are vulnerable to concerted, remotely-activated, untraceable break-ins. Responding to these challenges in a scalable and cost-effective way requires chips and entire systems that protect themselves from a wide range of attacks, as well as new EDA tools and methodologies for design, verification and test of such chips. These tools integrate recently developed techniques for hardware security and novel design primitives into conventional EDA flows, while preventing or detecting side channels, backdoors, and malicious alterations in functionality. In this article we outline key challenges, introduce recent ideas and ongoing efforts, formulate an agenda for research in IC security, and suggest how EDA techniques can be employed in this context.

Index Terms— IP integration issues, integrated-circuit security, IP protection, Trojan detection

I. INTRODUCTION

While preparing this article, we found dozens of recent media reports on cybersecurity issues, such as the breaking of encryption used in the Sony PlayStation 3, successful attacks on the Trusted Platform Module (TPM) used in modern PCs and on widely-used RSA chips, as well as the circumvention of application locks on Apple iPhones. The FBI has arrested electronics brokers who sold $3.5M worth of fake network equipment to the U.S. government, and U.S. Air Force wings have been tasked with “information operations” and “network warfare”.

From the business perspective, a major concern is the rise of fake or mislabeled hardware, and microelectronics IP theft. Revenue lost to IP infringement reaches into the billions of dollars, but the value of systems that can be compromised by subsequent breaches in chip/networking security is much larger. For example, hardware-based security is a necessary element of fledgling automotive electronics, especially systems for remote tracking, activation and lock-up such as LoJack and OnStar. *Hardware vulnerabilities could open the doors to higher-level attacks on software, content and networks*. Modern distributed power grids, controlled through computer networks, are often cited as a critical infrastructure vulnerable to remote exploits. To this end, a spectrum of hardware-based security methods has recently been developed, but not adopted widely enough to make an impact.

Cybersecurity challenges have become significant enough to merit responses by major corporations whose products have been pirated, and by oil conglomerates suffering from network espionage. Government officials, including the U.S. Secretary of State, have been involved in related international disputes and treaty negotiations. In 2005, the Defense Science Board pointed out the perils of a contaminated chip supply [5] and articulated the growing significance of hardware security in the next decade. Motivated by these trends, in this article we review specific threats to chip supply, outline a research agenda in hardware security, introduce recent ideas and ongoing efforts, and suggest research and business opportunities.

Glossary of Terms

Malicious insertions: Trojans and backdoors	Added components or features hidden in the IC. Backdoors enable remote control of the IC. Trojans implement secret, initially-dormant features.
Side channel	Unintended information channel (usually based on physical observations) exposing IC’s internal states
Trusted Platform Module (TPM)	A secure crypto-processor (spec or implementation) with storage for crypto keys to protect data
Counterfeit (fake) ICs	ICs that are copied, designed, or labeled to mimic another IC, but produced at a smaller cost and/or without authorization.
IC metering: passive and active	Ways to ascertain ownership of design IP, and keep track of manufactured and/or deployed ICs. Passive metering (e.g., watermarking) employs read-only analysis of individual chips. Active metering locks the functionality of the IC so as to require chip activation.
IP watermark	A unique mark (signature) for the IP (design)
Unique chip ID (IC fingerprint)	A unique mark (signature) for the IC (chip)
Physical unclonable function (PUF)	A unique mapping between the IC’s input and output (often depends on unclonable parameter variations)

II. CONTAMINATED CHIPS

Challenges in IC security involve threats directed at chips themselves, design data, embedded systems, and even the software that runs on these chips. Unlike purely software-based exploits, IC subversion has a higher barrier to entry in terms of cost, required design expertise and distribution channels. Therefore, infrastructure and cost considerations play a significant role in our discussion.

Problem 1. Counterfeit or malicious chips can be designed, manufactured or marketed by stand-alone entities, such as the fake NEC Corp. that was dismantled in China several years ago after the real NEC Corp. received unexpected customer-support requests [4]. However, infiltrating a typical IC design and fabrication flow (shown in Figure 1) requires a much smaller capital investment and entails smaller risks. The flow often starts from the functional specification and goes through the stages of design, fabrication, testing, packaging and integration in consumer electronics. Multiple entities are involved in this flow. For example, design houses often send their chips to offshore facilities for fabrication. The red exclamation marks in Figure 1 indicate potential vulnerabilities, including transfers of design data and specific steps of the flow. Vulnerabilities may be introduced by (a) unauthorized remote access to design data, (b) disgruntled, malicious or intimidated IC engineers, (c) physical access to design offices, and even (d) corrupted software tools [15].

Problem 2. IC Trojan horses, side channels and backdoors. Perhaps the most obvious threat vector is third-party Intellectual Property (IP) included during the design stage. While such IP blocks can be specified at different levels of abstraction, they may contain dormant malicious features that can be activated remotely – a basic example of an *IC Trojan horse* [1][5][16]. Third-party IP blocks may implement *side channels* and *hidden monitors* that can be activated by statistically-improbable secret commands. Such an unauthorized control mechanism is termed a *backdoor* or a *hardware Trojan* [17][9]. Once backdoors are embedded into a sufficient number of units, or into mission-critical units, hidden features can be activated in concert, leading to *denial of service*, *disclosure of confidential information*, and other adversarial benefits. Identifying the perpetrators can be difficult – a backdoor can be secretly embedded into otherwise legitimate electronic systems, or designed as a feature, but then used by someone else. The latter scenario is exemplified by the well-publicized case in which cellular phones of 100 top Greek officials were bugged for two years (2004-2005) [11]. Replacing compromised ICs can be costly, and their interactions with software are difficult to study.

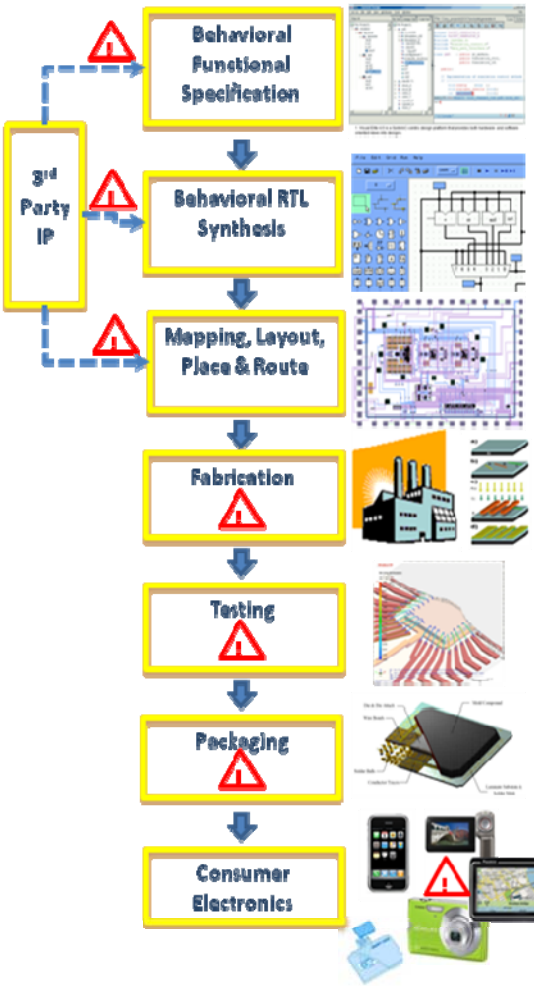

Figure 1 – A typical IC design flow and its vulnerabilities

Problem 3. **Need for IC metering.** Fabless IP providers, on the other hand, must meter the use of IP blocks sold, so as to protect their revenue stream. Indeed, once an authorized batch of ICs is produced, the incremental cost of doubling production is small. Such excess production, sometimes

caused by mistake, gives rise to pirated chips which can be indistinguishable from authorized chips, but sold at half-price, undermining the market for legitimate chips. A spectrum of *watermarking* techniques at different levels of abstraction has been developed for uniquely identifying the IP [7][12]. In addition to unique identification of design IP by watermarking, techniques for unique IC identification, known as *IC metering*, have been known and used for 30-40 years, usually in the form of passive IC metering by fingerprinting the IC. Techniques developed recently offer stronger enforcement by requiring every chip to be activated with a unique code (active IC metering) [2][14]. Without such protections, perpetrators can introduce small, subversive changes into unauthorized chips that are undetectable by conventional testing procedures [1][5][10][16]. Such *design Trojans* jeopardize the functionality of an IC, its network communications, as well as its vendor's reputation. While visual inspection of chip internals has been effective until recently, further miniaturization of process technology to deep-subwavelength feature sizes makes this increasingly difficult.

Problem 4. **Protecting lightweight applications**, such as smartcards and RFIDs [8]. Due to their physical availability to attackers and limited complexity, such devices can be reverse-engineered, with the purpose of altering their intended behavior. Attackers may refill electronic-cash systems with "free money", fake electronic passports, or fool a supermarket checkout system into scanning a new television set as a toothbrush. In such embedded systems, the considerations of power, size and cost limit the inclusion of reliable security cores [13]. While generally more secure, larger embedded systems may be vulnerable to component replacement and the IC threats discussed earlier.

III. AGENDA FOR RESEARCH IN HARDWARE SECURITY

Until recently, efforts in electronic system security have mostly focused on network and operating-systems aspects, as well as biometrics – but have paid less attention to unauthorized physical access and malicious changes in IC designs. However, recent fast-paced developments in cybersecurity, as well as their monetary impact, suggest that broader IC-centric research efforts are necessary. Several ongoing initiatives pursue contest-like settings where teams of researchers act as attackers and defenders, so as to explore leading-edge techniques for IC subversion, along with protection mechanisms. DARPA is running one such program, called TRUST, with industrial participants. Polytechnic University in Brooklyn has been organizing annual student competitions along these lines for the last several years. *Key challenges in hardware security involve high-level chip defenses (activation and locking protocols, multichip systems, interactions with software) and necessary IC infrastructure (unique chip IDs, verification and test, physical integrity, and suppression of side channels).*

Challenge 1. Effective measures to prevent IC cloning through unauthorized manufacturing can significantly boost the marketplace. Other forms of design IP (e.g., soft and hard cores) also lack established protection mechanisms. Despite the breadth of business contexts and technical circumstances, the adoption of such measures is typically obstructed by their overhead in cost, power, and performance. While preventive measures such as fingerprinting or watermarking could be useful in court cases [7][12], they are not cost-effective for detection of potential abuse. By contrast, *active metering of ICs/IPs* monitors and queries the devices during activation or normal use [2][14].

Challenge 2. To differentiate individual ICs and prevent digital cloning, researchers have proposed the idea of Physical Unclonable Functions (PUFs) and other forms of unclonable identification. A PUF is a function embodied in the physical structure of the device that is easy to evaluate but hard to capture in its entirety within typical time/memory constraints [10] [3][16][20]. Such unclonable identifiers are especially important for Field Programmable Gate Arrays (FPGA), where secure non-volatile memory for key storage is not readily available [18]. The current challenges and

active research topics in this area include the development of methods for ensuring PUF stability under different ambient conditions, and ensuring PUF robustness to sophisticated attacks.

Challenge 3. *Verification* of third-party design IP, and *test* of off-the-shelf IC components for security and integrity, are essential to effective countermeasures against many types of attacks [15][17]. However, easy silver bullets are unlikely, as these techniques may have to subsume traditional design verification and circuit test. Rather than detecting and localizing accidental bugs during a prolonged effort, it is becoming necessary to identify intentionally-placed backdoors and side-channels through quick inspection. Such techniques must span all levels of abstraction employed in IC design: from logic-level search for sequentially-deep states (a hallmark of a backdoor) and Boolean outputs that do not match the prototype (likely side-channel), to unexpected patterns of power consumption (Trojan added) or unexpected sensitivity to process variations (likely alteration). Some ICs now actively resist malicious alterations through built-in redundancy and self-checking [8].

Challenge 4. Efforts toward improved physical integrity of electronic systems must include better understanding of relevant attacks [22] and corresponding protections (e.g., side-channel attacks are well-studied now, but fault-injection and chip-replacement attacks are not). RFIDs, smartcards, e-passports and mission-critical industrial systems drive related efforts. The portable nature and small form factors of these devices hamper the integration of costly and processing-intensive security mechanisms [13].

Challenge 5. The impact of corrupted chips on software needs to be studied in great detail, with the goal of devising effective countermeasures [21]. Such countermeasures may be preventive, detective and/or reactive, including fallback scenarios and *safe* modes. Both software-based and IC-based techniques in this category are of great interest.

IV. RECENT INDUSTRY AND STANDARDS-SETTING EFFORTS

A number of companies, large and small, as well as government institutions hold stakes in various hardware aspects of cybersecurity. In the semiconductor industry, such companies are represented by the participants of the DARPA TRUST program [1] that focuses on the implantation of Trojan horses (by “red teams”) and their detection (by “blue teams”). In the U.S., NIST is the primary standards-setting body for solutions in secure hardware, software and communications protocols. In addition to well-known milestones, such as AES, NIST is developing new standards for cryptographic hash functions (earlier functions are no longer considered cryptographically secure). A major initiative in the PC industry, known as the Trusted Platform Module (TPM), primarily focuses on software security (viruses, Trojans) [19]. Supported by Microsoft Windows and Linux, TPM is implemented as a separate chip with secure memory for software keys. TPM checks the integrity of the hardware configuration and halts the operating system if significant changes are detected. However, TPM does not track *subtle* changes in ICs such as design Trojans.

In the automotive industry, several European and U.S. projects are working toward new standards for vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication, including security solutions. A small embedded security company, escrypt, is responsible for the design, implementation, and testing of security hardware and software components in some of these projects (see http://www.escrypt.com for more details). Its security platform esBOX V2X for secure vehicle communication is currently undergoing field-operational tests. The esBOX implements the DSRC IEEE 1609.2 draft security standard and offers fast signature generation and verification (400sig/s), broadcast of certificates, as well as encryption

and decryption services. Additionally, esBOX supports IEEE 1609.11 compliant applications, such as secure tolling and electronic payment schemes. It is compatible with Ethernet, Wi-Fi, Bluetooth, cellular and satellite communications. The hardware includes an Open Multimedia Application Platform board (TI OMAP with a 720 MHz ARM Cortex A8) connected to an FPGA (Xilinx Virtex-4 FX12) that accelerates cryptographic primitives and offers further reconfigurability. esBOX protects itself using countermeasures against spoofed, relayed and replayed messages.

V. THE ROLE OF EDA RESEARCH AND DEVELOPMENT

Improving hardware security requires modifications to how chips are designed and optimized, verified and tested. However, these *changes must be compatible with existing practice, prevailing IC design infrastructure, embedded software, and semiconductor manufacturing equipment, while requiring only minimal additional design resources, especially the time of IC engineers. Most of the additional work must be delegated to EDA tools by enriching existing EDA tool-chains with hardware-security features. Therefore, progress in hardware security is unthinkable without concerted efforts of the EDA industry and the research community*. A number of research and business opportunities exist in hardware security for EDA researchers and EDA vendors. Some of them directly address challenges articulated above, and some offer necessary design-flow infrastructure.

Dealing with third-party IP. Since interfacing to external and third-party IP is a source of vulnerability, new methods and tools for verifying interfaces and checking the integrity of the third-party IPs are needed. Another potential research direction is *compartmentalization* and *firewalling* of design blocks, such that a malicious core cannot jeopardize valuable design resources.

Infrastructure for unique chip IDs. A common theme in recent literature on hardware security is the application of PUFs to chip fingerprinting, hardware-based authentication, and key generation for public-key cryptography [3][14][16][20]. Such applications of PUFs motivate new physical-design techniques for stabilization of PUF responses in the presence of environmental fluctuations and process variations [20]. To integrate this research into EDA flows, new CAD tools and techniques will have to be introduced to automatically embed the unclonable keys in IC designs and layouts and ensure resiliency against removal attacks.

Verification techniques, such as unbounded model-checking, may be instrumental in IP inspection, e.g., to detect hidden features that are triggered by statistically unlikely input combinations. To achieve scalability, functional simulation may first identify circuit modules that remain dormant under normal execution, while more time-consuming formal methods can focus on such modules. Deeper analysis may detect sequentially deep states that can only be reached under certain conditions and may be used by design Trojans to evade detection by traditional techniques for design verification and circuit test.

IC Inspection and Testing. A potential avenue to explore for Trojan detection is accelerated inspection of ICs that would guard against malicious alterations by matching masks or chips against correct templates of a golden functionality. Such inspection tools must be cheaper than those currently offered by semiconductor equipment vendors, and must also be easily accessible so as to be employed throughout the supply chain by third parties, but without facilitating extensive reverse-engineering. Formulating a proper (golden) error-free model is a challenge on its own. Further, the verification/test protocol should be mindful of disclosing intellectual property. To this end, it is possible that zero-knowledge proofs developed by theoretical computer scientists may find new uses in this application. On the other hand, modern and upcoming optical and X-ray metrology tools have not been used to their full potential because adequate methods for automated characterization and test are poorly understood. The development of new methods and tools for hardware security will also be

driven by the emergence of nano-scale devices and atomic-scale effects, with subsequent changes to manufacturing processes and chip testing.

Physical design support. Past work in this domain includes comprehensive techniques for watermarking IC layouts [7], classified today as passive hardware metering. However, mask-level watermarking still appears an interesting research problem. Passive hardware metering suffers known limitations as it helps *confirm rather than discover* malfeasance. While active metering techniques are available today, they do not address several types of known attacks. To this end, there is demand for layout techniques to resist incremental layout modifications that affect functionality or insert side-channels. Such specialized techniques may need to the counter common objective of increasing flexibility to enable late design changes, or can be applied as post-processing to final designs.

Conceptual challenges in IC security deal with (1) data representations that can faithfully capture design functionality at each level of abstraction, as well as chip layout, (2) algorithms to compare both functionalities and layouts, with particular efficiency for nearly identical comparands, (3) methodologies for challenge-response tests that combine coverage guarantees of existing EDA tools with cryptography protocols to ensure resistance to attacks, and (4) effective optimization to decrease the overhead of hardware security. It is particularly interesting to explore the amount of flexibility present in highly optimized designs, and potential means to enable or disable such flexibility.

In summary, we feel that by addressing key needs in IC hardware security, the EDA community can add significant value to existing methods and tools. While we have touched upon several open problems, many more interesting and useful challenges can be identified and pursued, leading to chips that can protect themselves from various attacks.

VI.CONCLUSION

Several key emerging challenges in electronic design can be addressed with a new breed of integrated circuits that cannot be freely cloned or replaced, and resist malicious alterations. New methods for protection of integrated circuits and their contents/communications are being developed and integrated within the traditional design automation flow. Such methods will motivate new EDA products and revisions of existing products, while offering significant value to their users. Several improvements are required and many challenges remain to be addressed by researchers. Contemporary topics in this field include the development of new techniques for IC and IP protection and necessary infrastructure, such as stable and unclonable methods for IC identification and unclonable attack-resilient security key storage, verifying the integrity of third party IP, testing for malicious alterations, and identifying and detecting hardware backdoors (Trojans). Security of multichip systems and the impact of subverted chips on software are very promising topics, as is ensuring the security and protection of lightweight embedded systems. EDA is uniquely positioned to play a key role in providing security and protection for future generations of hardware designs and their applications. A great deal of relevant technical information is available in the publications listed in our references. Recommended reading includes coverage of the following topics: IC metering and piracy protection [2][15], IP watermarking [7][12], Physical Unclonable Functions (PUFs) [16][10], and Trojan insertion/detection [1][17]. Recent technical publications discuss the design of malicious hardware and the addition of hard-to-detect nefarious features [9][15][19], new attacks on key components of hardware infrastructure for cryptography [22], and the design of secure systems from untrusted components [21].

REFERENCES

[1] S. Adee. The hunt for the kill switch. *IEEE Spectrum*, May 2008.

[2] Y. M. Alkabani and F. Koushanfar. Active hardware metering for intellectual property protection and security. *USENIX Security Symposium,* 2007, pp. 291-306.

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

[4] P. Clarke. Fake NEC company found, says report. *EE Times*, May 4, 2006.

[5] Defense Science Board Task Force on High Performance Microchip Supply. Report A365534, 2005.

[6] U. Feige, A. Fiat and A. Shamir. Zero-knowledge proofs of identity. *J. Cryptology*. 1(2) (1988), pp. 77-94.

[7] A. B. Kahng, J. Lach, W. H. Mangione-Smith, S. Mantik, I.L. Markov, M. Potkonjak, P. Tucker, H. Wang and G. Wolfe. Watermarking techniques for intellectual property protection. *Proc. Design Automation Conference*, 1998, pp. 776-781.

[8] O. Kömmerling and M G. Kuhn. Design principles for tamper-resistant smartcard processors. *USENIX Workshop on Smartcard Technology*, 1999.

[9] S. T. King, J. Tucek, A. Cozzie, C. Grier, W. Jiang and Y. Y. Zhou. Designing and implementing malicious hardware. *First USENIX Workshop on Large-Scale Exploits and Emergent Threats* (LEET), April 2008.

[10] M. Majzoobi, F. Koushanfar and M. Potkonjak. Techniques for design and implementation of secure reconfigurable PUFs. *ACM Trans. on Reconfigurable Technology and Systems* 2(1) (2009), pp. 1-33.

[11] V. Prevelakis. The Athens affair. *IEEE Spectrum*, July 2007.

[12] G. Qu and M. Potkonjak. *Intellectual property protection In VLSI design: theory and practice*. Kluwer Academic Publishers, 2003.

[13] S. Ravi, A. Raghunathan, P. Kocher and S. Hattangady. Security in embedded systems: Design challenges. *ACM Trans. on Embedded Computing Systems* 3(3) (2004), pp. 461-491.

[14] J. Roy, F. Koushanfar and I. L. Markov. EPIC: ending piracy of integrated circuits. *Proc. Design, Automation and Test in Europe*, 2008, pp. 1069-1074.

[15] J. Roy, F. Koushanfar and I. L. Markov. Circuit CAD tools as a security threat. *Proc. Intl. Symp. on Hardware-Oriented Security and Trust*, 2008, pp. 65-66.

[16] G. E. Suh and S. Devadas. Physical unclonable functions for device authentication and secret key generation. *Proc. Design Automation Conference*, 2007, pp. 9-14.

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

[18] S. Trimberger. Trusted design in FPGAs. *Proc. Design Automation Conference*, 2007, pp. 5-8.

[19] Trusted Computing Group. http://www.trustedcomputinggroup.org.

[20] M. Yu and S. Devadas. Secure and robust error correction for physical unclonable functions. *IEEE Design and Test of Computers* 27(1) (2010), pp. 48-65.

[21] M. Hicks, M. Finnicum, S. T. King, M. K. Martin and J. M. Smith. Overcoming an untrusted computing base: detecting and removing malicious hardware automatically. *IEEE Security and Privacy*, 2010.

[22] A. Pellegrini, V. Bertacco and T. Austin. Fault-based attack of RSA authentication. *Proc. Design and Test in Europe,* 2010.