20 Years of Research on Intellectual Property Protection

Miodrag Potkonjak[1], Gang Qu[2], Farinaz Koushanfar[3], and Chip-Hong Chang[4]

[1]Computer Science Department, University of California, Los Angeles, CA, USA.
[2] Electrical and Computer Engineering Department, University of Maryland, College Park, MD, USA
[3] Electrical and Computer Engineering, University of California, San Diego, CA, USA.
[4] School of Electrical and Electronic Engineering, Nanyan Technological University, Singapore.
Contact author: gangqu@umd.edu

***Abstract*—VLSI intellectual property (IP) reuse based design methodology was adopted by the semiconductor industry in the early 1990's and how to protect design IPs from piracy and misuse has since been a challenging problem. 2017 marks the 20th anniversary of the IP protection development and working group was founded and the first series of IP watermarking papers were published. In this paper, we survey the efforts from industry, government, and academia on securing the design IPs in the past 20 years with focus on development from academia side.**

Keywords—intellectual property, reverse engineering, IP protection, digital watermarking, digital fingerprinting, IP metering, circuit obfuscation, hardware security..

I. A Quick History

Accordingly to the International Technology Roadmap for Semiconductors (ITRS), in 1990 with RTL design, an average hardware engineer's productivity is 4K gates per year. In the following five years, in-house placement and route and tall-thin engineer have helped to improve this to 9K gates per year, a pace much slower than the famous Moore's law. This created the so-called design productivity gap: engineers cannot design all the transistors available on a single die. To close this gap, industry moved to the era of IP reuse based design and IPs have quickly become the most valuable assets for design companies.

Perhaps one of the earliest efforts on circuit IP protection is the treaty on "layout-designs (topography)" established by the World Intellectual Property Organization (WIPO) in 1989, where it requires "each contracting party" to "secure adequate measures to ensure the prevention of acts considered unlawful" and "appropriate legal remedies where such acts have been committed" [1]. The listed unlawful acts include "reproducing a protected layout-design in its entirety or any part" and "importing, selling or otherwise distributing for commercial purposes a protected layout-design" or an IC that incorporates a protected layout-design.

In 1996, the Virtual Socket Interface Alliance (VSIA) was founded to dramatically enhance semiconductor industry's design productivity by establishing standards for the adoption of IPs (which VSIA also referred to as virtual components). VSIA attracted more than 200 members at its peak and was dissolved in 2008 after accomplishing the above mission. VSIA identified six challenges and built development and working groups (DWG) for each of them. Among them, IP protection was one of the most technically challenging. The IPP DWG was created in 1997 with goals to 1) enable IP providers to protect their VCs against unauthorized use, 2) protect all types of design data used to produce and deliver VCs, 3) detect use of VCs, and 4) trace use of VCs [2].

Over the years, circuit IPs have quickly evolved from layout-designs to any stand-alone component of a SoC design and more generally, any innovation and technology that makes design better. These include hard IPs (such as GDSII files and custom physical layout), firm IPs (such as placed RTL blocks), and soft IPs (such as synthesizable HDL source codes). Meanwhile, the goal of IP protection is extended with the various emerging types of IP infringements including overbuilding and counterfeiting. Reverse engineering, the enabling tools for most IP piracy, becomes more and more powerful. New nano materials, design and fabrication technologies are proposed to countermeasure these IP piracy. We will not and cannot give a complete coverage of the available IP protection mechanisms and research advances with sufficient technical depth. Instead, our intention is to reflect the history and pay the tribute to those who have contributed in the past 20 years.

II. Industrial Standards by the VSIA IPP DWG

In the first document published by the IPP DWG in 2000, three approaches to secure a VC were identified: "using the deterrent approach, the VC owner may deter the infringer from contemplating the theft of the VC by using proper legal means. With the protection approach, the owner tries to prevent unauthorized use of the VC. And, using the detection approach, the owner detects and traces both legal and illegal use of the VC, so a proper course of action can be taken" [2].

Commonly used deterrents include patents, copyrights, contracts, trademarks, and trade secrets. They do not directly prevent IP piracy or provide physical protection of the IP, but rather discourage the misuse of IPs because the infringer, once being caught, may face lawsuits and severe penalty to recover the financial loss of the IP owner. However, all of these except trade secrets are affirmative rights, which means that it is the IP owner's responsibility to identify IP infringement and catch the IP infringer.

Protection mechanisms use means such as encryption, licensing agreements, dedicated hardware, or chemicals to prevent unauthorized access to the IP. Standard encryption can

978-1-4673-6853-7/17/$31.00 ©2017 IEEE

be applied to protect design IPs despite the rather expensive decryption process. For example, Xilinx has a decryption unit on its FPGA board since the Virtex-II family. Its design tool allows user to select multiple plaintext messages and uses them as the key to encrypt the FPGA configuration bitstream file. The decryption unit will decrypt it before configuring the FPGA board. Chemicals have long been integrated in chips for passive protection, mainly for military devices. When the surface of the die is scratched and exposed to the atmosphere, it will damage the exposed silicon and thus prevent reverse engineering.

Perhaps another notable contribution of the IPP DWG is the establishment of two IP protection standards, the physical tagging standard for hard IPs and another one for soft IPs. These standards, when adopted by the industry, will provide a convenient way to track the IPs and to detect the use of IPs (the last two goals of IP protection). However, these standards are recommended for honest designers and are vulnerable against even some simple attacks such as removing or modifying the tags. In the rest of this paper, we will focus on the detection approaches that have been developed in the past 20 years.

III. Constraint Based Digital Watermarking and Fingerprinting

The initial "imaginary" IP infringers are dishonest IP users who might misuse the IP with or without the help of reverse engineering. The above deterrent approaches and protection mechanisms are general concepts that have been used to protect the likes of data and software. Their effectiveness is questionable (as they rely on IP owners to identify and prove infringement) and they may create obstacles for design reuse.

It is worth mentioning that at the same time (early and mid-1990s), the advance of one technology known as "the Internet" made it effortless to share and redistribute digitized multimedia artifact and software. The multimedia signal processing community has responded with protection mechanisms of digital watermarking, fingerprinting, and forensics. Software society has also introduced software watermarking and obfuscation. It is not surprising that hardware design community wanted to use the same concepts and terminologies. Although creating, embedding, and detecting digital watermark in multimedia and software are relatively simple, it remained a big challenge on how to do the same for hardware design IPs.

The breakthrough came from the research group in UCLA led by Professor Potkonjak, where they developed the first hardware watermarking and fingerprinting techniques in 1997 and reported in early 1998 on DSP [3] and FPGA [4] designs. Since then, the same concept has been applied to almost every phase of IC design to protect all sorts of design IPs from physical layout to Verilog codes, and in the forms of combinational circuits and sequential logic as well as abstract computational models such as finite state machine and graph models. Most of the early efforts were included in the book [5] published in 2003, where the authors have formally built the constraint-based IP protection paradigm. More recent work can be found in a book chapter published in 2016 [6].

In the heart of this paradigm is adding extra constraints during various design phases to embed signatures of IP owner (known as watermark) and legal IP user (known as fingerprint). These constraints will not impact the functionality of the IP, but will result in "unnecessary" and "random" structures and properties in the implementation of the IP. The existence of these structures and properties will be used to "probabilistically" establish the IP ownership or identify IP users. The specific methods of creating, embedding, and extracting these additional constraints are design specific. The fundamental assumption is that the design space is sufficiently large to accommodate the watermark and fingerprint.

There are many requirements for a watermarking or fingerprinting method to be effective. In short, the watermarked/fingerprinted IP has to (1) perform the **desired functionality**, (2) maintain IP's quality or incur **low overhead**, (3) provide **high credibility** of the proof of IP owner and legal user, (4) allow **easy detection** of the embedded watermark/fingerprint, (5) remain **robust and resilient** against fabrication variations and potential attacks, (6) be **transparent** to the design process and tools by not requiring major changes to the process and tools; (7) offer the capability of **part protection** to any portion of the IP; and (8) be **fair** to all the IP owners and users in terms of quality of the IP, the watermark and the fingerprint.

It has been demonstrated, both in theory and practice, that watermarking and fingerprinting techniques satisfying the above properties can be developed in many design stages [5,6]. The two most challenging requirements are low overhead and easy detection (in remote and nondestructive fashion), which are both closely related to the practicality of the watermark or fingerprint. This is particularly true for fingerprinting because all the fingerprinted copies must be distinct which poses a unique challenge for chip fabrication. A couple of recently proposed methods generate fingerprints in two phases to solve this problem. First, flexibilities in circuit implementation are identified or created in the chip. Then in the post-silicon stage such as the chip testing phase these flexibilities are configured to reflect fingerprints [7].

IV. Hardware Metering

The reuse based design methodology and the expensive cost of in-house chip fabrication facility have turned most design houses to be fabless, where they have to outsource their design to foundries elsewhere. This gives the foundries access to the details of the chips and the possibility to overbuild them without the authorization from the design house. So IP owner's next "imaginary" infringer is such untrusted foundries.

Digital watermarking cannot solve this problem because the overbuilt chips carry the authentic watermark of the design house. Although fingerprint can identify each chip, the overbuilt chips will simply make the user who has the same fingerprint the source of overbuilt chips. So new methods are needed to defend against this kind of IP infringement and the solution is integrated circuit (IC) metering, which is an effective protocol that enables design houses to have post-fabrication control over their ICs.

The basic concepts behind IC metering is to embed a unique tag to each IC and make sure that the tag is under the control of the design house instead of the foundry. Many different types of tags have been proposed and used for hardware metering. They can be categorized based on various criteria [8]:

Passive metering has tags that can only be used for chip identification, while tags in **active** metering can also enable, disable, or control the chip. Based on whether such control is part of the design or not, active metering can be further divided into **internal controlled** or **external controlled. Intrinsic** metering does not need the help from additional components or the modification of the design, while **extrinsic** metering methods do. Depending whether the tag interacts with the chip's functionality or not, we have **non-functional** metering and **functional** metering. Finally, we have **reproducible** and **unclonable** tags based on whether the tags can be reproduced or not. Next we show a couple of example tags.

Serial number is perhaps the most popular and one of the earliest way for device tagging. A serial number can be physically indented on the device or stored permanently in the memory. These tags are passive, extrinsic, non-functional, and reproducible. The fact that such tags can be reproduced makes it unsuitable to countermeasure foundry overbuilding.

Now considering the following scheme: during the design phase, add control signals and logic (such as XOR gates) to non-critical paths; each fabricated IC will be locked unless all control signals to the inserted logic have correct values, which are controlled by the design house and will be released to each IC buyer (for example, by some asymmetric cryptographic primitives such as PKI). This approach is apparently active, external controlled, extrinsic, unclonable, and functional.

V. Design Obfuscation

While the above digital IP watermarking, fingerprinting, and metering techniques can deter IP piracy, they do not actively prevent IP piracy from happening or make it harder. Remember that most IP piracy starts with reverse engineering (RE), it makes sense to increase the complexity of RE by design obfuscation, another term that has been used in the literature of software protection. In this section, we highlight two recently developed hardware obfuscation methods: logic locking [9] and IC camouflaging [10].

The common feature of both approaches is that the design and fabrication of the circuit will be modified such that RE attackers will not be able to obtain a working gate level netlist to continue IP piracy with traditional RE tools. In logic locking, additional gates such as XOR are inserted in non-critical wires. The added input to such gates are control signals known as keys. The circuit will function correctly only when correct key values are provided. It is assumed that the RE attackers will not be able to access the key values, which can be stored in secure memory. With such keys, the IP owners can control the chips with the support of public-key infrastructure (PKI) [9]. In that sense, this method is also known as logic encryption. It will be effective to defend both malicious IP users and untrusted foundries.

Circuit camouflaging, on the other hand, is based on the fact that RE technology is normally 2-3 generations behind the latest design technology. For example, RE tools will not be able to detect the dummy and true contacts between certain adjacent metal layers. By taking advantage of such limitations, the circuit can be fabricated in a certain way that some cells with difference functionalities (such as NAND, NOR, and XOR) will appear identical to RE attackers. To extract the true functionality of the IP, the attacker need to pay extra efforts [10]. Other IC camouflaging approaches use the always-on and always-off MOS transistors, or configure the camouflaged cells by information stored in SRAM, or utilized special characteristics of the emerging devices.

Obfuscation is one of the most active topics on IP protection with many proposed potential attacks to de-camouflage the circuits and corresponding countermeasures. Both logic encryption and IC camouflaging can be used to defend RE attacks, only logic encryption may help against untrusted foundries because the IP owners will have control on the keys. IC camouflaging, on the other hand, may not be useful in this case because all details of the camouflaged cells have to be released to the foundry for the correct fabrication unless certain post-silicon procedures are in place to configure the camouflaged cells.

VI. Emerging Technologies and Mechanisms

In this section, we briefly overview other emerging technologies that can be used for IP protection.

Split manufacturing: an effective method to prevent leaking complete design information to "untrusted" foundry is now known as split manufacturing. In a patent granted in 2004, it was proposed to use different manufacturing lines for the fabrication of the front-end-of-line pieces and the back-end-of-line pieces of the chip, and then a joining process will combine these pieces to form a semiconductor die [11]. The recent design trend of 3D integration provides another dimension for split manufacturing. Despite the cost of designing the joining process, testing the correct functionality of the die, and impact on the yield, this approach remains a viable solution when untrusted foundries have to be used. However, split manufacturing will not prevent RE attacks.

Physical Unclonable Function: Silicon Physical Unclonable Function (PUF) is a small piece of circuitry embedded in the design that can extract the intrinsic variation during fabrication process and utilize such variation for various applications [12]. The proposed silicon PUFs over the years are either based on delay or memory, examples include arbiter PUF, ring oscillator PUF, butterfly PUF, flip-flop PUF, buskeeper PUF, SRAM PUF, and bistable PUF. PUF has emerged as a very versatile hardware security primitives and can be used to help in solving many challenges in IP protection. For example, the uniqueness and unpredictability of PUF can be used as an intrinsic tag for IC identification, metering, and anti-counterfeiting; secret keys can be created and stored in terms of PUF; the information extracted from PUF can enhance IC obfuscation and hardware based encryption. The main current unsolved challenges for PUF are on the usability as the underlining fabrication variation can be very sensitive to environment variations such as voltage, temperature, humidity, and circuit aging.

Scan chain and DfT methods: as we have discussed earlier, the usability and practicality of the IP protection techniques are crucial for the industry to adopt them. Many recent investigation has pointed to post-silicon design phase such as testing as the place for IP protection. One particular area that researchers have focused on and enjoyed success in the design of scan chain, where effective methods have been proposed for watermarking, fingerprinting, metering, obfuscation, as well as building PUFs [6,7]. One of the advantages for techniques at this stage is the controllability and observability of the circuit available to the users without depackaging the chip. This makes it possible to detect the embedded watermark and fingerprint and to identify the IC for metering. However, this also introduces security vulnerabilities as it becomes a side channel for attackers to obtain sensitive system state information or a backdoor to access the system for IP infringement.

Emerging devices: As modern chip design moves to heterogeneous integration of traditional CMOS and new emerging nano-materials such as MEMS, phase change memory, tunneling FETs, resistive memory, and spintronics, we are facing many new challenges in the protection of IP integrated in such new devices. Meanwhile, this also provide us opportunities to design interesting hardware security primitives (for, but not only for, IP protection) based on unique physical features of such devices. For example, various memristor based PUF, device identification, data encryption, user authentication and cryptography implementations have been proposed recently [13].

Light weight security for IoT applications: to end this paper, we consider the billions of Internet of Things (IoT) devices that are used in our daily life. Among the many design challenges in IoT devices, IP protection is very important for several reasons. First, the market of IoT applications is tremendous which could motivate IP piracy on various IoT devices. Second, majority of these devices do not demand the highest possible performance and thus are rarely build with the latest technology, which opens the door for RE attacks. Finally, due to the extreme resource constraints on such devices, traditional cryptographic protocols are not implemented, which again makes such devices vulnerable to many known attacks, let alone implementing any IP protection mechanisms. Lightweight cryptography solutions have been proposed where the security strength (such as the length of the keys) is sacrificed for affordable security implementation. IP protection of these devices thus will demand ultra-low resource and should come together with other hardware security primitives such as device authentication [14].

Conclusion

Intellectual property (IP) protection has been identified as one of the key enabling technologies for the reuse based design methodology. In the past 20 years, there have been significant progress in the research and development of theoretically sound and practical IP protection mechanisms. This paper provides a balanced discussion of the history, the motivation, the challenges, and the available solutions for this problem. For IP owners, they face potential infringements of their IPs from not only their competitors, but also IP users and foundries. To achieve a full protection, law enforcement deterrent approaches such as copyright and patent are a must whenever possible as that remains the only legal way to get back the revenue lost due to IP piracy. However, to catch IP infringement, various existing IP protection methods will be useful: digital watermark will establish the IP's authorship; fingerprint can trace the IP and IP infringer; IC metering will prevent foundry from overbuilding chips; circuit obfuscation can effectively increase the difficulty of reverse engineering; split manufacturing avoid the leak of design information to untrusted foundries; scan chain design and other post-silicon design and testing techniques will have more practical values than those techniques at other early design levels for most IP protection methods (except perhaps watermarking); application specific design constraints (such as those in IoT devices) and IP infringement models should be considered before the adoption of any IP protection approaches. To summarize, IP protection is a system engineering problem that requires a holistic approach to solve. The lessons we have learned over the 20 years on IP protection will also be valuable for the development of hardware security primitives for emerging applications and emerging devices. .

Acknowledgement. This work was supported in part by AFOSR MURI under award number FA9550-14-1-0351.

References

[1] WIPO. "Treaty on Intellectual Property in Respect of Integrated Circuits", May 26, 1989. http://www.wipo.int/treaties/en/text.jsp?file_id=295136

[2] Virtual Socket Interface Alliance, "Intellectual Property Protection White Paper: Schemes, Alternatives and Discussion" Version 1.1, January 2001.

[3] I. Hong and M. Potkonjak, "Techniques for Intellectual Property Protection of DSP Designs", ICASSP, pp. 3133-3136, 1998.

[4] J. Lach, W.H. Mangione-Smith, and M. Potkonjak, "Fingerprinting Digital Circuits on Programmable Hardware", IHW, pp. 16-31, 1998.

[5] G. Qu and M. Potkonjak, "Intellectual Property Protection in VLSI Design: Theory and Practice", Kluwer Academic Publishers, 2003.

[6] C.-H. Chang, M. Potkonjak, and L. Zhang, "Hardware IP Watermarking and Fingerprinting", in Secure System Design and Trustable Computing, pp 329-368, Springer, ISBN 978-3-319-14970-7, 2016.

[7] G. Qu, C. Dunbar, X. Chen, and A. Cui, "Digital Fingerprint: A Practical Hardware Security Primitive", in "Digital Fingerprinting", pp 89-114, Springer, ISBN 978-1-4939-6601-1, 2016.

[8] F. Koushanfar, "hardware Metering: A Survey", in "Introduction to Hardware Security and Trust", pp. 103-122, Springer, ISBN 78-1-4419-8079-3, 2012.

[9] J. A. Roy, F. Koushanfar, and I. L. Markov, "EPIC: Ending Piracy of Integrated Circuits," in 2008 Design, Automation and Test in Europe, 2008, pp. 1069–1074.

[10] J. Rajendran, M. Sam, O. Sinanoglu, and R. Karri, "Security Analysis of Integrated Circuit Camouflaging," ACM Conference on Computer Communications and Security, 2013.

[11] R. Jarvis and M. McIntrye, "Split manufacturing method for advanced semiconductor circuits", US Patent App. 10/305,670, 2004.

[12] Suh, G. Edward, and Srinivas Devadas. "Physical unclonable functions for device authentication and secret key generation." *Proceedings of the 44th annual Design Automation Conference*. ACM, 2007.

[13] Arafin, M. T., et al. "A survey on memristor modeling and security applications." *Sixteenth International Symposium on Quality Electronic Design*. IEEE, 2015.

[14] G. Qu and L. Yuan. "Design things for the internet of things: an EDA perspective". In Proceedings of the 2014 IEEE/ACM International Conference on Computer-Aided Design (ICCAD '14). IEEE Press, Piscataway, NJ, USA, 411-416. 2014.