DESIGN AND SIMULATION OF INTELLECTUAL PROPERTIES PROTECTION USING MIXED MODUL LEVEL AND SIGNAL OBFUSCATION

[1]HANJARA CAHYA ADHYATMA, [2]FAIRUZ AZMI, [3]SURYA MICHRANDI NASUTION
[123]School of Electrical Engineering, Telkom University, Bandung, Indonesia
E-mail: [1]mashan@student.telkomuniversity.ac.id, [2]worldliner@telkomuniversity.ac.id,
[3]michrandi@telkomuniversity.ac.id

ABSTRACT

System on a Chip (SoC) is an embedded system module that has functionality in a silicon chip board that can also be called Veri Large Scale Integration (VLSI). The owner of the SoC design owns the copyright on the design of the system that has been created. Fabless manufacturing is a way of printing hardware modules that Integrated Circuit (IC) designers are Outsourching from outside the printing factory. Fabless manufacturing from IC design has gap design theft When the design will be printed or when the project requires mutiple module With various functions from various designers. Therefore every module is VLSI Of this chip designer requires proof of ownership of the designer or Production companies. In this study plans to make the verification of ownership design with 2 specific key verification that is Polygate as the main key that will activate the second key, and the second key will be active which process using digital filter algorithm.

Keywords: VLSI, Intellectual Property Protection, Digital Signal Processing, Polygate Watermark.

1 Introduction

Providing a series of watermarks as a safeguard to a printed VLSI blueprint that indicates ownership of the designer or module manufacturer will protect against cheating others who will steal the design. So the possibility of theft or plagiarism that causes losses to the company or designer because of its design is stolen or plagiarism reduced. [1]

Broadly speaking the technique of Intellectual Property Protection (IPP) watermarking can be classified into 2 classes namely Dynamic Watermarking and Static Watermarking. Dynamic Watermarking is a watermark that can not be detected except by running a watermarked IP to detect the resulting signal, such as digital signal processing (DSP), or finite state mechine (FSM) watermarking. Static Watermarking is a watermark that refers to the properties of a design, and can only be detected in different static ways, such as paths and watermarking placements. [2] One of the other safeguards is to convert the simulated file from a file. The RTL source code that enables is not easy to be reverse-engineered by third parties, so the model can not be changed and reused with other purposes by third parties and irresponsible users. However, this way only protects from the softwere side that protects the IP from being misused by third party users. [3] For IP security used in project sharing and reusable projects can be used with the security of Digital Signal Processing cell that allows integration in the system.

In this research will perform a combination of polymorph gate IP protection with digital filter algorithm. Using a combination of these two techniques will provide additional security to IP protection that is likely to over write a smaller watermark. Therefore in this study proposed a combination of existing methods to improve security capabilities in an existing VLSI module. Combine polygate as a combination key to enable the digital filter module to be used as a watermark.

2 LSI Development Flow

Transistor is the most important component in the development of modern computer technology. Before the invention of the transistor. The Engineer must use a vacuum tube. Vacuum tubes can work as an electronic switch. However, vacuum tubes require power and large space, expensive, and slow execution capabilities make vacuum tubes replaced by transistors.

With the discovery of transistors whose size and power requirements are small but still effective, Electronic Engineers in the 1950s saw many possibilities for their implementation in more advanced electronic circuits. With the increasing complexity in electronic circuits new problems arise.

One of them is the size of the circuit. A complex circuit like a computer depends heavily on speed. If the number of components on the computer is too much then the connection between the components is also more and more long, causing the transfer of electrical signal speed becomes reduced which causes the process on the computer to be slow.

In 1958 this problem could be solved by the idea of Jack S Kilby whose idea was to assemble electronic components in a silicon block (Monolithic Idea). The idea not only reduces the size of the circuit but also reduces the need for cable connections between circuits and their manufacturing can be automated. But the idea still has many other problems. Nevertheless, the idea was awarded a nobel prize in 2000.

Half a year after Kilby sparked his idea of the Monolithic series. Robert Noyce has the answer to some problems on Kilby's idea. Namely interconnection between circuits. It adds a metal layer to the last layer and removes some layers so that the connection between components can be formed.

Possibility type of attack is changing over time. It is caused based of how bussiness flow in VLSI Design are olso changed. In the early day of VLSI development, a system from designing a module until design is delivered to custommer is done by solo manufacturrer industries.

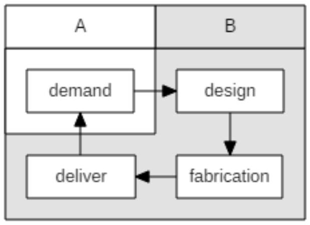


Fig. 1. Old Bussiness

As the shown image above, generally there is 2 type of interaction. There are interaction between custommer and developer (A to B) and interaction between developer and customer (B to A). In this scheme the gap of distribution of design is between A and B side. In this early day security is not much worries.

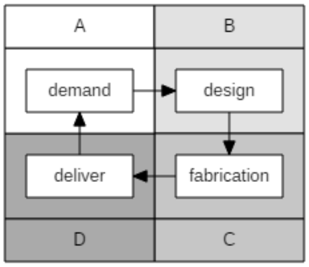


Fig. 2. new Business

But after advancing in the manufacturing of VLSI and increasing demmand of the design. Design become more complicated and cost to manufacturing from scratch to delivering design are expensive in this day. So the solution to do manufacturing of VLSI design is using Fabless manufacturing. As shown in the figure above, there are generally 4 side element for manufacturing a single or combination design module of VLSI. In this method designer and manufacturer are diferent company. In this technique have great advantage because the cost for designing a Design is distributed to each side, and design is more flexible because on the "B" side company, they can make design without have a their own Fabrication Building (Fabless).

3 Attack Possibility

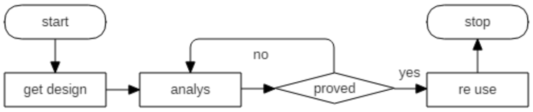


Fig. 3. Clonning

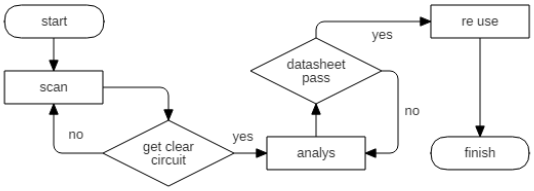


Fig. 4. Reverse Enginerring

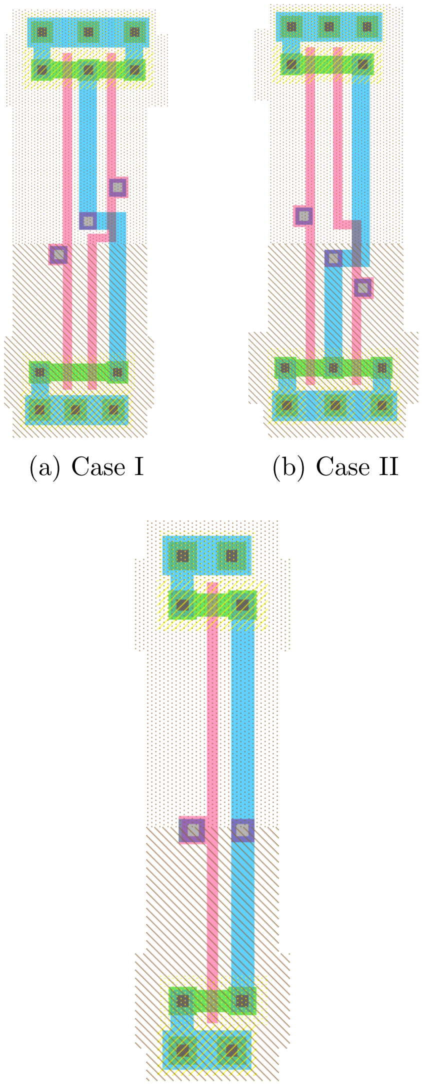
There is multiple possibilities of Intellectual Properties being stolen while in production or development prosses. For example, clonning type of attack and reverse engineering type of attack.

Clonning can be done by directly copy of blue print from leaked distribution design and Reverse engineering are can be done by re analysis an already distributed design.

4 Multi Obfuscation

4.1 Layouting

Gate for layout use CMOS technology. The protection use simple basic CMOS gate for mixed implemented for hard removal from reverse engineering, there are:



(a) Case I

(b) Case II

(c) Case III

Fig. 5. Simulation results for the network.

4.2 Layout Verification

For simple see through layout with just verification without mixed gate placement, here is total gate if the gate collected as one cell:

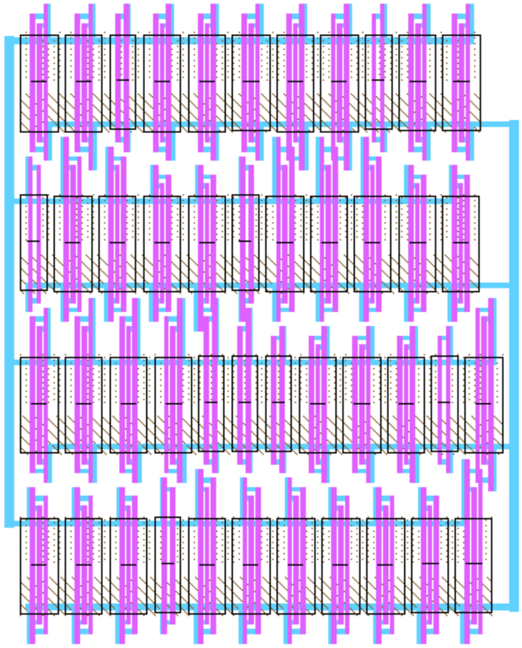


Fig. 6. Simulation results for the network.

In general technique when engineer will manufacturing IC is make hierarchy of cells so it will easy to routing and tracing circuit problem. But if the watermark circuit is manufactured with that technique it will easy to expose watermark circuit inside the IC. So it will lead to hard removal and reverse engineered the IC. To prevent that happening the watermark cell will generate without hierarchy and placed with random routing algorithm. So it will not be so obvious that watermarks circuit is implemented within the main IC core circuit.

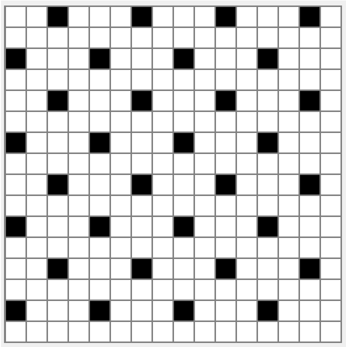


Fig. 7. Obfuscation Mixed Placement Between 2 Module

In this research is using multiple obfuscation that mixed together. First obfuscation is using mixed ciscuit betwen protection module and core module. In this obfuscation core module function are mixed with protection function module.

This technique is made for sole purpose to avoid original core module being extracted by reverse engineering or clonning. If the design are clonned, design have possibility to claim it back by calling protection function that already mixed with original core.

4.3 Digital Filter

Digital Signal Processing in this research is used for extracting encripted signature of original design that mixed with protection function. To activate betwen design the protected IC is activated throught polimorph gate as a key to open signal door to Origianl design core or protection function core that protect original.

4.4 Polimorph Gate

In this research is using combination between polimorph-gate and Digital Signal Processing. This combination will be determined and enabled by polygate as a key to activating a combination of digital filters. After the digital filter is active then the data combination will pass through a combination of filters enabled from the polygate combination.[8], [9] Then the result data combination of these processes will form a special pattern that becomes the watermark data of the designer that characterizes the identity of the designer.

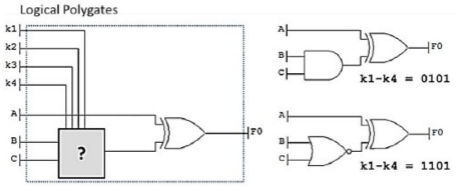


Fig. 8. Simulation results for the network.

Polymorph gate is gate that will change the property of gate such while the key selector key is change. Example is from AND function will active while key is 0101 and it will change to NOR function while key change to 1101.

F = A XOR (A **AND** B)

F = A XOR (A **NOR** B)

4.5 Watermark Flow

Watermark is a circuit that should not stand alone in its implementation although in its development can be done independently. In this research the Module to be in watermark is ALU module.

4.6 Aritmatic Logic Unit (ALU)

Arithmetic Logic Unit (ALU) is a combination of digital electronic circuits that perform arithmetic functions and bitwise operations on integer binary numbers. This is in stark contrast to the Floating Point Unit (FPU), which performs floating point number operations. An ALU is essentially part of a wide range of computing circuit blocks, including the Central Processing Unit (CPU). A CPU, FPU, or GPU may have many ALUs in it.

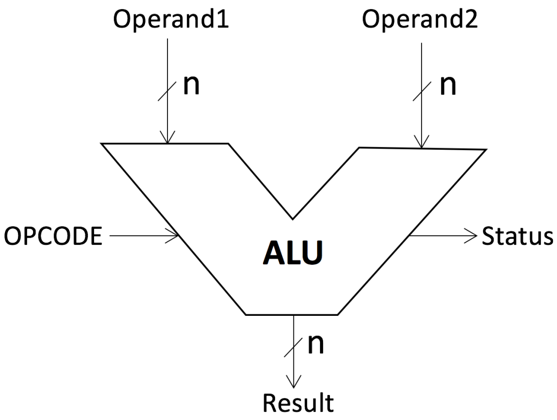


Fig. 9. ALU

4.7 Flow Diagram

Filter is 3 bit data filter that will clip maximal value or minimal value that has set before. So the data that will go through system is accepted data from clipping filter.

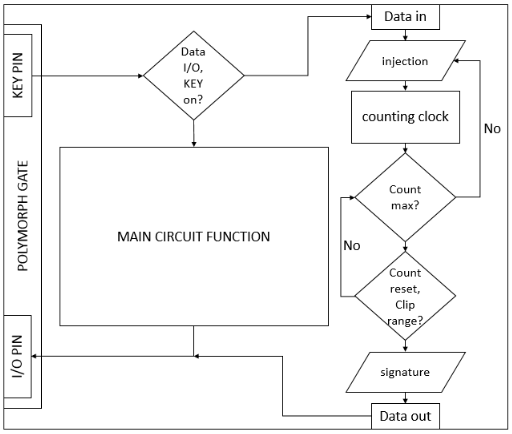


Fig. 10. Simulation results for the network.

In this illustration showed how IC is watermarked with given technique. With polymorph gate as bridge between watermark and main circuit function and key pin as gate to access between main function and watermark. To access watermark, developer will activated combined code to given key pin in the printed IC, and after the key activated it will open bridge in the polymorph to watermark circuit. After watermark circuit is opened, developer will inject secret encoded data to circuit and it will decode the given data as signature on the output pin. Data injected as bit stream so it need time to inject and waiting for de-coded output stream.

To extract signature from injected data it will counting how many data will be slice and clip it until given tolerate count. After that data will be checked if the data is inside tolerated range, if yes data will be transferred to polymorph I/O as extracted signature data.

5 Digital Filter Obfuscation Mixed Algorithm

Design is made to make confusion. A single Hardwere Intellectual Properties have a core, but original electrical design are unknowen to the public. For example we have ALU for main core, but what kind of proccess and how the designare unknowen, just I/O and the I/O function are knowen to the public.

Below is an example of program listing in the illustration above. So there are 1 Top module and 3 sub modules on chip design which have given protective circuit

```
// Main Modul IC Watermark
module alu( RST, CLK, ENA, RGA, RGB, RGZ
    , KEY, OPT);
    // Deklarasi I/O
    input  RST, CLK, ENA;
    input  [3:0]OPT;
    input  [7:0]RGA,RGB;
    input  [1:0]KEY;
    output [7:0]RGZ;
    wire   [7:0]A,B,RGZ;
    // Core Inti
    alu_min aluj(RST, CLK, ENA, RGA, RGB
        , A, KEY, OPT);
    // Protektor
    protection prot(RST, CLK, ENA, RGA,
        RGB, B, KEY);
    // Bridge antara core dan protektor
    bridge jembatan(A, B, RGZ);
endmodule
```

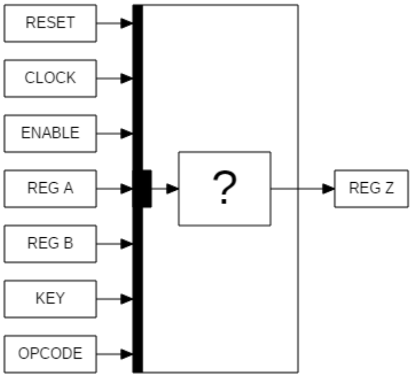


Fig. 11. Obfuscation

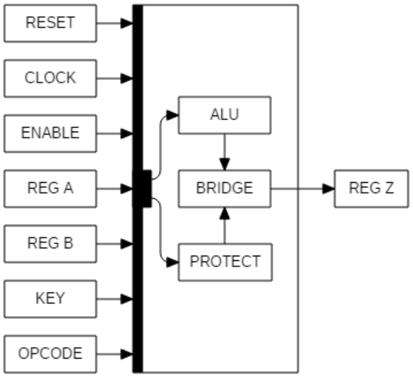


Fig. 12. Internal System Obfuscation

But actually design have two core, main core function(ALU) and Protection funtion core. The active Function are main Core, but protection core are sleeping and mixed inside.

For sleeping protection core, can be called by activated polimorph gate and inject specific signal stream to the protection circuit. The signal like teeth in the ”padlock key” and protection circuit is the padlock.

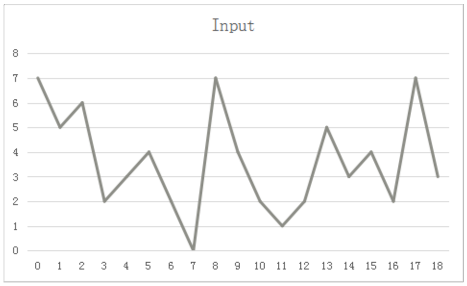


Fig. 13. Input Signal

TABLE 1
FPGA Speed Analysis

Unprotected	Minimum	Maximum
Period	2.692ns	371.471MHz (freq)
Input arrival time before clock	10.075ns	-
Output required time after clock	-	5.558ns
Protected	Minimum	Maximum
Period	4.023ns	248.571MHz (freq)
Input arrival time before clock	8.667ns	-
Output required time after clock	-	6.962ns

After protection circuit inserted by input signal stream, circuit will generate an signature as identity of the original design. This feature serve as ”watermark of the design”.

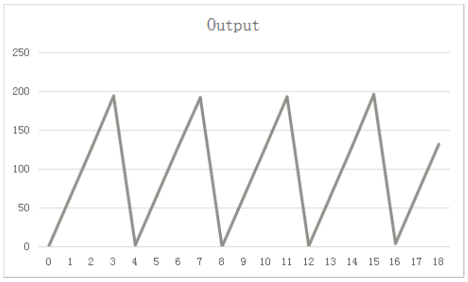


Fig. 14. Output Signal

The output shape of signature may look like similar, but it is different, judging by upper signal and period each signal it will determine whos signature belonge.

6 Analisys

First the device performance analysis before it is protected, then protect the main core with the protective circuit and analyze its performance and compare the result of the analysis before, with the result of post-protected analysis. TABLE 5 are recap data analysis results before and after given a protective circuit. there are soft-estimation clock speed on FPGA architecture XILINX.

This design already implemented in softcore software sim and FPGA. For the key as given bellow used 3bit combination key for 20 shape and 3bit extracted signature for 5 shape.

Data in data out is example how filter is going in and let the verification data through system generated and will procced so data will change to specific bit array. By injected long bit stream data to IC with purpose to deceive the attacker. And the output is just specific short bit stream data. The purpose given long input and short output is to avoid watermarks is detected by forced data injection. And here is example with streaming bit data with clipping on the 5/1 injection data. With 20 data stream and 4 data output as zero is ignored. Inputted data will be procced with given algorithm before to extract signature data.

TABLE 2
Input Array

H	111
F	101
G	110
C	010
D	011
E	100
C	010
A	000
H	111
E	100
C	010
B	001
C	010
F	101
D	011
E	100
C	010
H	111
D	011
INPUT	HFGCDECAHECBCFDECHD
OUTPUT	CABE

TABLE 3
On-Chip Power Summary

Unprotected	Power (mW)
Clock	1.12
Static Power	10.42
Total	11.54
Protected	Power (mW)
Clock	1.37
Static Power	10.42
Total	11.79

From the analysis result there is a decrease of maximum process speed on FPGA from 371.471 Mhz to 248.571 Mhz or about 33%. In the soft-simulation results indicate that there will be a decrease in the speed of the module being developed.

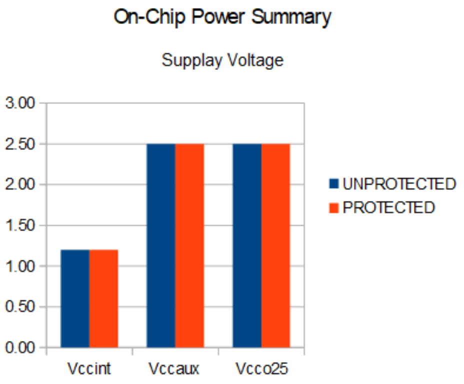


Fig. 15. Suplay Voltages

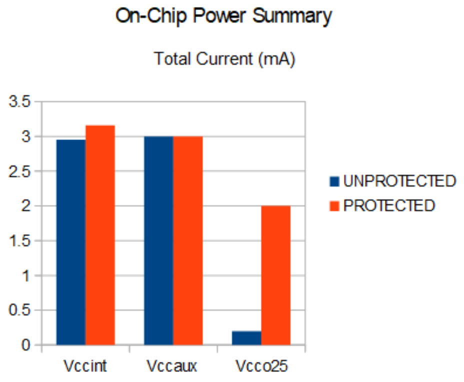


Fig. 16. Total Current

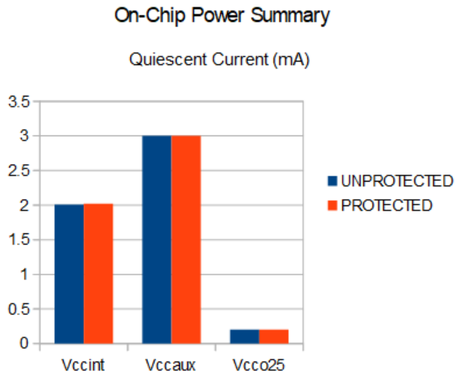


Fig. 17. Quiescent Current

The compilation using the standard library of mosis found the number of gates used before the protected circuit is 5234 and increased to 5324 after the circuit is given a shield. Increasing the amount of gate used increases about 1.69%. This means that if done generate from netlist to layout increase the layout is not very significant.

TABLE 4
Gate after compilation to netlist

Gate Synthesys	Gates
Unprotected	5234
Protected	5324

7 Conclusion

Using multiple protection in a signle design is possible to protect the design from multiple possibility attack. And this design also have zero-io-overhead that maintain size of original design. In the future research using development of this technique we hope there are design that totally secure from every possibility attack of Intellectual Properties Violation (Clonning and Reverse Engineering).

TABLE 5
Data time verification 20 to 4 clock

Time	in 0	in 1	in 2
0	1	1	1
1	1	0	1
2	1	1	0
3	0	1	0
4	0	1	1
5	1	0	0
6	0	1	0
7	0	0	0
8	1	1	1
9	1	0	0
10	0	1	0
11	0	0	1
12	0	1	0
13	1	0	1
14	0	1	1
15	1	0	0
16	0	1	0
17	1	1	1
18	0	1	1
19	0	0	0

Time	out 0	out 1	out 2
0	0	0	0
1	0	1	0
2	0	0	0
3	0	0	1
4	0	1	1

TABLE 6
Power Supply Currents

Unprotected				
Supply Source	Supply Voltage	Total Current (mA)	Dynamic Current (mA)	Quiescent Current (mA)
Vccint	1.20	2.95	0.94	2.01
Vccaux	2.50	3.00	0.00	3.00
Vcco25	2.50	0.20	0.00	0.20
Protected				
Supply Source	Supply Voltage	Total Current (mA)	Dynamic Current (mA)	Quiescent Current (mA)
Vccint	1.20	3.16	1.14	2.02
Vccaux	2.50	3.00	0.00	3.00
Vcco25	2.50	2.00	0.00	0.20

References

[1] ”The History of the Integrated Circuit”. Nobelprize.org. Nobel Media AB 2014. Web. 25 Aug 2017. http://www.nobelprize.org/educational/physics/integrated_circuit/history/

[2] R. Chapman and T. S. Durrani, IP Protection of DSP Algorithms for System on Chip Implementation, vol. 48, no. 3, pp. 854861, 2000.

[3] Watermarking Techniques for Electronic Circuit Design, no. 1, pp. 117.

[4] Leonid Azriel, Student Member, Ran Ginosar, Senior Member, and Shay Gueron. Using Scan Side Channel to Detect IP Theft. pages 1–13, 2017.

[5] Abhishek Basak, Swarup Bhunia, Senior Member, Thomas Tkacik, Sandip Ray, and Senior Member. Security Assurance for System-on-Chip Designs With Untrusted IPs. 12(7):1515–1528, 2017.

[6] Mohammad-mahdi Bidmeshki, Xiaolong Guo, Raj Gautam Dutta, Yier Jin, and Yiorgos Makris. Tracking in Proof-Carrying Hardware IP Part II :. 12(10):2430–2443, 2017.

[7] Xi Chen, Gang Qui, Aijiao Cui, and Carson Dunbar. Scan Chain based IP Fingerprint and Identification. 2017.

[8] Xiaoming Chen, Qiaoyi Liu, Yu Wang, Qiang Xu, and Huazhong Yang. Low-Overhead Implementation of Logic Encryption Using Gate Replacement Techniques. 2017.

[9] Jeffrey T Dellosa. The Impact of the Innovation and Technology Support Offices (ITSOs) on Innovation , Intellectual Property (IP) Protection and Entrepreneurship in Philippine Engineering Education. (April):762–770, 2017.

[10] Xiaolong Guo, Student Member, Raj Gautam Dutta, Student Member, and Yier Jin. Eliminating the Hardware-Software Boundary : A Proof-Carrying Approach for Trust Evaluation on Computer Systems. 12(2):405–417, 2017.

[11] Yier Jin, Xiaolong Guo, Raj Gautam Dutta, Mohammad-mahdi Bidmeshki, and Yiorgos Makris. Tracking in Proof-Carrying Hardware IP Part I :. 12(10):2416–2429, 2017.

[12] Jian Lin. Analysis of the Key Factors of Intellectual Property Management at Art Institutions. pages 206–208, 2017.

[13] Hardware Matters. Antipiracy-Aware IP Chip Set Design for CE Devices: A Robust Watermarking Approach. (april):118–124, 2017.

[14] Hardware Matters. Hardware Security of CE Devices. (January), 2017.

[15] By Saraju P Mohanty and Rochester Chapters. Information Security and IP Protection Are Increasingly

Critical in the Current Global Context. (June):3–5, 2017.

[16] By Saraju P Mohanty and Rochester Chapters. Information Security and IP Protection Are Increasingly Critical in the Current Global Context. (June):3–5, 2017.

[17] Xuan Thuy Ngo, Jean-luc Danger, Sylvain Guilley, Tarik Graba, Yves Mathieu, Zakaria Najm, and Shivam Bhasin. Cryptographically Secure Shield for Security IPs Protection Threats on Integrated Circuits. 66(2):354–360, 2017.

[18] Xuan Thuy Ngo, Jean-luc Danger, Sylvain Guilley, Tarik Graba, Yves Mathieu, Zakaria Najm, and Shivam Bhasin. Cryptographically Secure Shield for Security IPs Protection Threats on Integrated Circuits. 66(2):354–360, 2017.

[19] Protection Of, Trade Secrets, Under The, T S Directive, and Protection During. The European Union Trade-Secrets Directive: To-Dos for Companies? (april):2016–2017, 2017.

[20] A Sengupta and D Roy. Protecting IP core during architectural synthesis using HLT-based obfuscation. 53(13):1–2, 2017.

[21] A Sengupta and D Roy. Protecting IP core during architectural synthesis using HLT-based obfuscation. 53(13):1–2, 2017.

[22] Anirban Sengupta, Member Ieee, Dipanjan Roy, Student Member Ieee, and Saraju P Mohanty. Triple - Phase Watermarking for Reusable IP Core Protection during Architecture Synthesis. 0070(c), 2017.

[23] Wei-tek Tsai, Libo Feng, and Hui Zhang. Intellectual-Property Blockchain-based Protection Model for Microfilms. pages 174–178, 2017.

[24] Nandeesha Veeranna and Benjamin Carrion Schafer. Efficient Behavioral Intellectual Properties Source Code Obfuscation for High-Level Synthesis. 2017.

[25] Marc Wehlack and Konrad Spang. Motivations for and Barriers to Offshoring Development Projects to China A Case Study of the Automotive Industry. pages 169–173, 2017.

[26] Muhammad Yasin, Student Member, Ozgur Sinanoglu, and Senior Member. Testing the Trustworthiness of IC Testing : An Oracle-Less Attack on IC Camouflaging. 12(11):2668–2682, 2017.

[27] Dongrong Zhang, Miao Tony He, Xiaoxiao Wang, and Mark Tehranipoor. Dynamically Obfuscated Scan for Protecting IPs Against Scan-Based Attacks Throughout Supply Chain. 2017.

[28] Jiliang Zhang and Lele Liu. Publicly Verifiable Watermarking for Intellectual Property Protection in FPGA Design. 25(4):1520–1527, 2017.

[29] Jiliang Zhang and Lele Liu. Publicly Verifiable Watermarking for Intellectual Property Protection in FPGA Design. 25(4):1520–1527, 2017.