**PERANCANGAN DAN SIMULASIPERLINDUNGAN PROPERTI INTELEKTUAL MENGGUNAKAN ALGORITME OBFUSCATION FILTER DIGITAL**

*Design and Simulation of Intellectual Properties using Digital Filter Obfuscation Algorithm*

**1Hanjara Cahya Adhyatma, 2Fairuz Azmi, S.T., M.T., 3Surya Michrandi Nasution S.T., M.T.**

1,2,3Prodi S1 Sistem Komputer, Fakultas Teknik, Universitas Telkom

1mashan@student.telkomuniversity.ac.id, 2wordliner@telkomuniversity.ac.id, 3michrandi@telkomuniversity.ac.id

**Abstrak**

System on a Chip (SoC) adalah sebuah modul embedded system yang memiliki fungsi tertentu dalam sebuah papan chip silicon yang juga bisa disebut dengan Veri Large Scale Integration (VLSI). Pemilik dari desain SoC memiliki hak cipta atas desain sistem yang telah dibuat. Fabless manufacturing merupakan cara pencetakan modul perangkat keras yang desainer Integrated Circuit (IC) adalah Outsourching dari luar pabrik percetakan.

Fabless manufacturing dari desain IC memiliki celah pencurian desain ketika desain akan dicetak atau ketika proyek membutuhkan mutiple module dengan berbagai fungsi dari berbagai desainer. Oleh karena itu setiap modul VLSI dari desainer chip ini membutuhkan bukti ownership dari perancang atau perusahaan produksi. Dalam penelitian ini dibuat verifikasi ownership dengan 2 kunci khusus verifikasi yaitu Polygate sebagai kunci utama yang akan mengaktifkan kunci kedua, dan kunci kedua akan aktif yang prosesnya menggunakan algoritme filter digital.

**Kata kunci : VLSI, Intelectual Property Protection, Digital Signal Processing, Polygate Watermark.**

**Abstract**

System on a Chip (SoC) is an embedded system module Has a certain functionality in a silicon chip board that can also be called With Veri Large Scale Integration (VLSI). The owner of the SoC design has Copyright over the system design that has been created. Fabless manufacturing is How to mold a hardware module that is designer Integrated Circuit (IC) Is 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 From this chip designer re- quires proof of ownership from the designer or Production company. In this study writer make a verification of ownership design with 2 dedicated verification keys ie Polygate as the primary key going Activate the second key, and the second key will be active which process Using a digital filter algorithm.

**Keywords: VLSI, Intellectual Property Protection, Digital Signal Processing, Poly- gate Watermark.**

**1. Pendahuluan**

Integrated Circuit (IC) merupakan modul teknologi dasar dari perangkat elek- tronika tertanam modern. Dengan berkembangnya teknologi IC yang menguta- makan ukuran kecil, dan performa yang tinggi serta dengan harga yang murah mem- buat teknologi IC semakin diminati [1].

Dengan ukuran modul yang sangat kecil dan banyaknya komponen pemban- gun, kerja sama antara desainer dilakukan untuk membangun sebuah modul VLSI sehingga setiap desainer dapat fokus mendesain salah satu fungsi yang terdapat dalam modul tersebut. Kerja sama dilakukan untuk mempermudah pembuatan de- sain VLSI yang memiliki tingkat kerumitan yang tinggi. Desainer juga dapat mem- percepat waktu mendesain dengan menggunakan kode sumber yang sudah ada atau bekerja sama secara paralel membuat masing-masing modul yang nantinya akan digabung menjadi sebuah modul utama VLSI.

Setelah modul selesai dibuat maka modul siap untuk di-produksi. Dalam proses produksi modul perusahaan tempat desainer bekerja tidak perlu memiliki pabrik produksi modul sendiri, perusahaan dapat bekerja sama dengan mitra percetakan yang akan memproduksi modul buatan perusahaan modul tersebut. Cara kerja sama seperti ini disebut dengan Fabless Manufacturing [2].. Ketika akan memproduksi IC, perusahaan harus menyerahkan blueprint modul VLSI ke percetakan, namun blueprint tersebut tidak terjamin kerahasiaan nya serta memungkinkan plagiarisme desain oleh oknum perusahaan atau pihak ketiga yang tertarik menggunakan desain VLSI yang telah diserahkan untuk di-produksi.

**2. Dasar Teori**

## Very Large Scale Integrated-circuit

Very Large Scale Integration atau disingkat LSI merupakan proses pembuatan sebuah IC dengan mengkombinasikan ribuan transistor ke dalam sebuah chip. VLSI ada sejak tahun 1970-an ketika semikonduktor kompleks dan teknologi komunikasi sedang berkembang. Mikroprosesor merupakan salah satu peraangkat VLSI. Se- belum adanya teknologi VLSI kebanyakan IC memiliki set fungsi yang terbatas yang dapat di jalankan. Sebuah perangkat chip elektronik dahulu hanya fokus pada sebuah fungsi seperti CPU, ROM, RAM dan rangkaian logika lainnya. De- ngan adanya VLSI memungkinkan disainer IC untuk menambahkan berbagai fungsi kedalam sebuah chip IC. [2]

* 1. **Arus Pengembangan LSI**

Integrated Circuit (IC) merupakan teknologi sirkuit elektronika yang lebih maju. Sebuah rangkaian elektronika dibuat dari berbagai komponen elektronika yang berbeda beda seperti transistor, resistor, kapasitor dan dioda yang saling tersam- bung satu sama lain. [3]

Transistor merupakan komponen terpenting pada pengembangan teknologi komputer moderen. Sebelum ditemukannya transistor. Para Engineer harus meng- gunakan tabung vakum. Tabung vakum dapat bekerja sebagai saklar elektronik. Namun tabung vakum membutuhkan daya dan ruang yang besar, mahal, serta ke- mampuan eksekusi yang lambat membuat tabung vakum tergantikan oleh transistor.

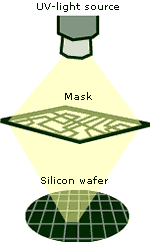
Dengan ditemukannya transistor yang ukuran dan kebutuhan dayanya yang kecil namun tetap efektif, Para Engineer elektronik di tahun 1950an melihat banyak sekali kemungkinan untuk implementasinya pada rangkaian elektronik yang lebih maju. Dengan semakin meningkatnya kompleksitas pada rangkaian elektronik munculah masalah-masalah baru.

Salah satunya adalah ukuran rangkaian. Sebuah rangkaian kompleks seperti komputer sangat bergantung pada kecepatan. Apabila jumlah komponen pada kom- puter terlalu banyak maka sambungan antar komponen juga semakin banyak dan semakin panjang, sehingga menyebabkan kecepatan transfer sinyal listrik menjadi berkurang yang menyebabkan proses pada komputer menjadi lambat.

Tahun 1958 masalah ini dapat dipecahkan oleh ide Jack S Kilby yang idenya adalah merangkai komponen elektronika dalam sebuah blok silikon (Monolithic Idea). Idenya tersebut tidak hanya mengurangi ukuran rangkaian namun juga men- gurangi kebutuhan kabel sambungan antar rangkaian serta manufakturingnya da- pat diautomasi. Akan tetapi idenya tersebut masih memiliki banyak masalah lain. Walaupun begitu, idenya tersebut mendapatkan penghargaan nobel di tahun 2000.

Setengah tahun setelah Kilby mencetuskan idenya tentang rangkaian Mono- lithic. Robert Noyce memiliki jawaban untuk beberapa permasalahan pada ide Kilby. Yaitu interkoneksi antar rangkaian. Yaitu menambahkan lapisan metal pada lapisan terakhir dan menghilangkan sebagian lapisannya sehingga sambungan antar komponen dapat terbentuk.

Dilihat dari proses developing, terdapat 2 cara untuk mendapatkan sebuah de- sain untuk di kloning. Pertama dengan mengambil langsung data mentah desain atau ”blueprint” dan Reverse Engineering saat barang telah dipublikasi di pasaran.

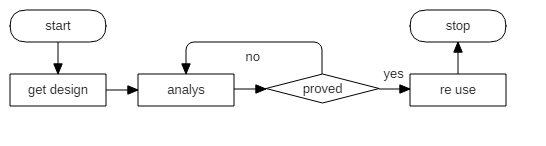


**Gambar 2.1: Produksi Chip Moderen**

Chip pada zaman sekarang berbasis pada photolithography. Pada teknik ini di- gunakan radiasi sinar Ultra Violet yang melewati sebuah mask menuju lembaran silikon yang di lapisi filem photosensitive untuk membentuk suatu rangkaian.

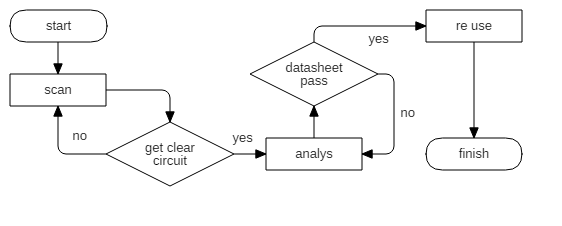
* 1. **Kemungkinan Serangan Desain LSI**

Dilihat dari proses developing, terdapat 2 cara untuk mendapatkan sebuah de- sain untuk di kloning. Pertama dengan mengambil langsung data mentah desain atau ”blueprint” dan Reverse Engineering saat barang telah dipublikasi di pasaran.



**Gambar 2.2: Clonning/Sumber Tidak Terpercaya**

Dalam segi ini serangan dilakukan dengan cara mencuri langsung desain yang sudah siap di fabrikasi serta uji coba kebenaran. Bila pencuri mendapatkan desain yang telah di uji coba, maka pencuri tinggal langsung memperbanyak desain yang telah di curi.



**Gambar 2.3: RE (Reverse Engineering)**

Untuk serangan jenis ini, pencuri sudah pendapatkan produk dari pasar yang telah teruji, pencuri tinggal melakukan scan rangkaian kemudian mengujinya de- ngan datasheet. Apabila hasil scan desain produk di dapati rangkaian yang konkrit/- jelas dan rangkaian tersebut telah teruji sesuai datasheet. Maka pencuri tinggal melakukan fabrikasi.

* 1. **Digital Signal Processing Filter**

Digital Signal Prosesing (DSP) merupakan pengolahan sinyal digital, seperti di- gunakan pada komputer hingga untuk melakukan berbagai operasi proses sinyal. Sinyal yang diproses merupakan kumbulan bilangan sekuensial yang merepresen- tasikan sampel dari variabel sinyal kontinyu pada suatu domain seperti domain waktu, ruang atau frekuensi.

Pada pengolahan sinyal, sebuah filter adalah sebuah alat atau proses yang menghilangkan beberapa komponen atau fitur yang tidak di inginkan dari suatu sinyal. Filtering merupakan kelas proses sinyal.

* 1. **Verilog HDL**

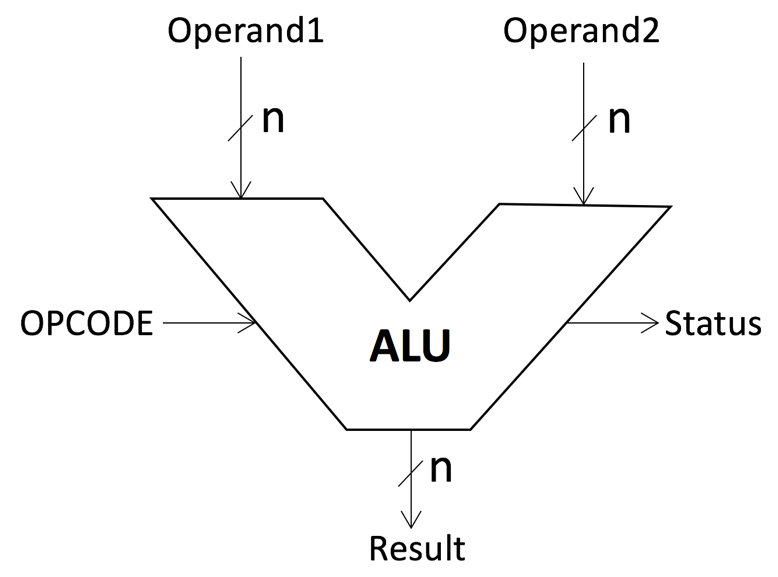
Verilog HDL merupakan bahasa pendeskripsi hardware yang digunakan untuk mendesain dan dokumentasi sistem elektronika. Verilog HDL memungkinkan per- ancang mendesain pada berbagai tingkatan abstraksi. Verilog HDL berasal dari Automated Integrated Design System (yang kemu- dian berubah nama menjadi Gateway Design Automation) pada tahun 1985. Saat itu perusahaan tersebut dipegang oleh Dr. Prabhu Goel, pendiri PODEM test gener- ation algorithm. Verilog HDL di desain oleh Phil Moorby, yang kemudian menjadi chief Designer untuk Verilog-XL dan perusahaan rekan pertama di Cadance Design System. Awalnya Verilog dibuat sebagai bahasa simulasi. Kemudian setelah berkem- bang tidak hanya digunakan untuk simulasi namun juga untuk sintesis. (source www.verilog.com)

* 1. **FPGA**

FPGA merupakan kepanjangan dari Field Programmable Gate Array adalah perangkat keras yang biasa digunakan dalam proses manufakturing IC. FPGA di- gunakan untuk mensimulasikan draft rancangan IC yang siap untuk di test yang apabila telah lolos test akan di lanjutkan ke tahap layout. FPGA hanya digunakan apabila rancangan membutuhkan input dari perangkat lain atau program kernel.

* 1. **ALU**

Aritmatik Logic Unit (ALU) adalah kombinasi rangkaian elektronik digital yang melakukan fungsi aritmatika dan operasi bitwise pada bilangan integer binari. Ini sangat kontras dengan Floating Point Unit (FPU), yang melakukan operasi bilan- gan floating point. Sebuah ALU pada dasarnya bagian dari berbagai macam blok rangkaian komputasi, termasuk Central Prosesing Unit (CPU). Sebuah CPU, FPU, atau GPU mungkin memiliki banyak ALU di dalamnya.

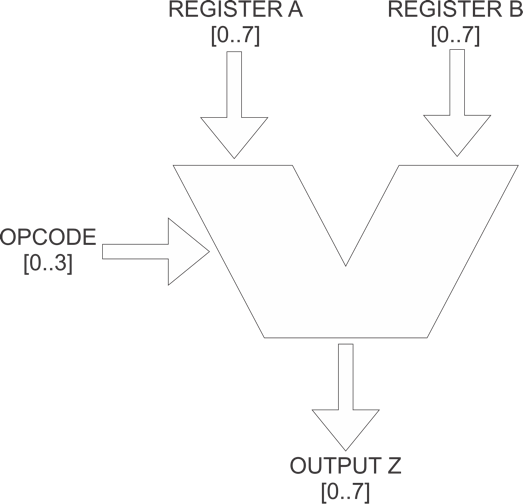


**Gambar 2.10: ALU**

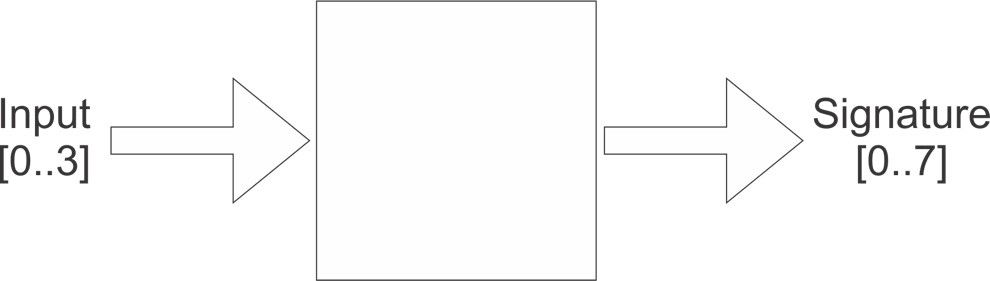
π

**3. Pembahasan**

1. **Gambaran Umum Desain**

Perancangan serta langkah-langkah di perlukan untuk menyelesaikan penelitian ini. Berikut ini akan di jelaskan gambaran serta tahapan dari perancangan system yang di teliti serta skenario simulasi dari hasil desain yang telah dirancang. Desain utama adalah desain modul alu. Pada penelitian kali ini digunakan modul ALU dengan 2 register masing-masing 8 bit input, 4 bit opcode dan 8 bit output seperti ditunjukan pada diagram dibawah ini.

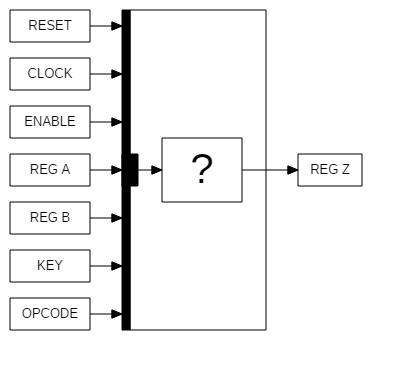
**Gambar 3.1: Desain ALU yang akan dilindungi**

Selain menggunakan desain ALU penulis juga merancang desain perlindungan dengan input 4 bit dan output 8 bit seperti yang ditunjukan diagram dibawah ini. modul inilah yang nantinya akan diselipkan pada modul ALU.

**Gambar 3.2: Desain rangkaian pelindung**

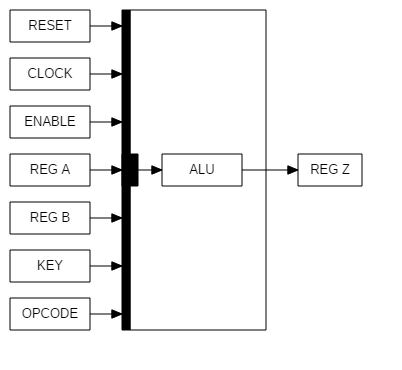
1. **Skema Perlindungan**

Skema perlindungan ini dilakukan teknik Pengolahan Sinyal Digital untuk ek- straksi data signature dan obfuscation dengan polymorph gate untuk menyem- bunyikan keberadaan signature. Dibawah berikut merupakan spesifikasi I/O pada modul yang akan dilindngi.



**Gambar 3.3: Desain rangkaian Top modul yang terdapat rangkaian lain**

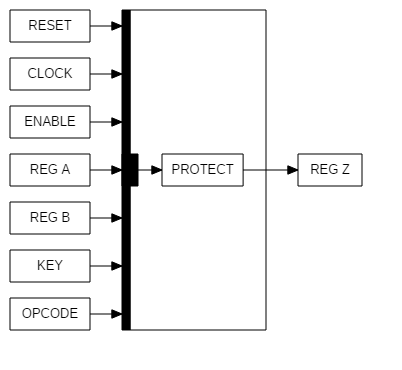
Untuk teknik obfuscation dengan polymorph dilakukan desain yang bertujuan menyelipkan suatu modul lain pada modul utama tanpa diketahui pengguna. Teknik ini seperti memberikan program Trojan kedalam suatu program utama. Namun sub- program ini bukan untuk merusak namun untuk melindungi. Seperti ilustrasi di atas menunjukan suatu modul besar namun ada sesuatu lain di dalam modul tersebut.



**Gambar 3.4: Desain rangkaian ALU pada top modul**

Pertama penulis menggunakan rangkaian ALU sebagai modul besar (utama) dengan spesifikasi I/O chip yang telah ditentukan sebelumnya. Lalu fungsional ALU ditest dengan spesifikasi yang telah dibuat.

Skema perlindungan ini dilakukan teknik Pengolahan Sinyal Digital untuk ek- straksi data signature dan obfuscation dengan polymorph gate untuk menyem- bunyikan keberadaan signature. Dibawah berikut merupakan spesifikasi I/O pada modul yang akan dilindngi.



**Gambar 3.5: Desain rangkaian pelindung pada top modul**

Setelah itu ganti rangkaian modul ALU dengan modul perlindungan seba- gai modul utama kemudian dilakukan tes fungsional kembali untuk mengetahui apakah rangkaian perlindungan dapat bekerja diatas arsitektur serta spesifikasi modul utama.

Setelah didapat kedua modul dapat berjalan sesuai dengan semestinya maka langkah selanjutnya menggabungkan kedua modul tersebut bada modul utama. pada penggabungan kali ini digunakan teknik obfucation polymorph untuk memilih antara modul mana yang harus berjalan pada modul utama.

Setelah itu ganti rangkaian modul ALU dengan modul perlindungan seba- gai modul utama kemudian dilakukan tes fungsional kembali untuk mengetahui apakah rangkaian perlindungan dapat bekerja diatas arsitektur serta spesifikasi modul utama.

Setelah didapat kedua modul dapat berjalan sesuai dengan semestinya maka langkah selanjutnya menggabungkan kedua modul tersebut bada modul utama. pada penggabungan kali ini digunakan teknik obfucation polymorph untuk memilih antara modul mana yang harus berjalan pada modul utama.

**4. Implementasi dan Pengujian Sistem**

## Pengujian

Setelah desain selesai di rancang, kemudian dilakukan pengujian untuk menge- tahui apakah desain yang telah dirancang dapat bekerja dengan baik serta menge- tahui bagaimana performasi alat yang di rancang.

## Sekenario Pengujian

Untuk pengujian yang dilakukan adalah pengujian funsional algoritma (behav- ioral) serta pengujian performansi waktu operasi dan daya yang dibutuhkan alat yang telah dirancang. Pada pengujian fungsional dilakukan pengujian mengguankan simulasi diagram waktu. Pada diagram waktu dapat dilihat proses input output satu demi satu dalam satuan waktu tertentu. Pengujian satu persatu dilakukan untuk mengetahui secara detail fungsional IC yang telah dirancang.

Apabila uji fungsional tidak ditemukan anomali, maka dilanjutkan pengujian se- lanjutnya yaitu pengujian daya serta performansi. Hal ini untuk mengetahui apakah terjadi perubahan yang signifikan pada perangkat yang diberi perlindungan dengan yang tidak diberi perlindungan.

**5. Kesimpulan dan Saran**

## Kesimpulan

Meninjau hasil analisis yang di lakukan dari pengujian yang telah dilakukan, di dapat kesimpulan sebagai berikut.

1. Masih memungkinkan menyisipkan suatu rangkaian pelindung ke dalam rangkaian utama tanpa mengganggu fungsi utama rangkaian.

2. Terjadi penurunan kecepatan proses serta peningkatan kebutuhan daya pada hasil analisis simulasi di fpga.

3. Dari hasil kompilasi gerbang, komponen komponen yang digunakan untuk fungsi rangkaian utama dan fungsi rangkaian pelindung menyatu, sehingga bisa digunakan sebagai pengecoh agar rangkaian sulit ditiru.

## Saran

Agar Teknologi pengamanan Intelektual Properti lebih maju serta memperbaiki permasalahan yang masih ada pada penelitian ini, berikut beberapa saran dari untuk pengembangan dan penelitian selanjutnya:

1. Penelitian ini dilakukan pada layer software, untuk meningkatkan kecepatan akses dan mengurangi konsumsi daya dari hasil analisis level behavioral pada fpga, dibutuhkan analisis lebih lanjut pada syntesis level gate (netlist) dan level phisical (layout).

2. Saat ini teknologi serta teknik perlindungan properti intelektual perangkat keras masih terbilang baru, bidang keamanan pada IC masih minim resource serta proses manufakturing IC sendiri begitu kompleks dan luas serta spesi- fikasi desain setiap produk sangat rahasia. Dibutuhkan kajian khusus kea- manan pada Level fabrikasi seperti RTL Level, Gate Level dan Layout Level.

**Daftar Pustaka**

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

[3] 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.

[4] *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.*

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

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

[7] *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.*

[8] *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.*

[9] *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.*

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

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

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

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