Circuit Camouflage Integration for Hardware IP Protection

Ronald P. Cocchi, James P. Baukus, Lap Wai Chow, Bryan J. Wang
SypherMedia International, Inc
5455 Garden Grove Blvd, Suite 300
Westminster, CA 92683
{rpcocchi, jbaukus, lchow, bjwang}@smi.tv

ABSTRACT

Circuit camouflage technologies can be integrated into standard logic cell developments using traditional CAD tools. Camouflaged logic cells are integrated into a typical design flow using standard front end and back end models. Camouflaged logic cells obfuscate a circuit's function by introducing subtle cell design changes at the GDS level. The logic function of a camouflaged logic cell is extremely difficult to determine through silicon imaging analysis preventing netlist extraction, clones and counterfeits. The application of circuit camouflage as part of a customer's design flow can protect hardware IP from reverse engineering. Camouflage fill techniques further inhibit Trojan circuit insertion by completely filling the design with realistic circuitry that does not affect the primary design function. All unused silicon appears to be functional circuitry, so an attacker cannot find space to insert a Trojan circuit. The integration of circuit camouflage techniques is compatible with standard chip design flows and EDA tools, and ICs using such techniques have been successfully employed in high-attack commercial and government segments. Protected under issued and pending patents.

General Terms

Security, Design.

Keywords

Security, Design, Camouflage, Obfuscation, Reverse Engineering, Anti-Cloning, Anti-Counterfeit, Anti-Tamper, Anti-Trojan.

1. INTRODUCTION

The problem of Reverse Engineering (RE) attacks and production of counterfeit integrated circuits are of increasing concern among chip makers [1]. A circuit whose function was extracted through RE can be cloned and counterfeited. Conventional integrated circuits are completely open to analysis, making them more vulnerable to a myriad of attacks. Unprotected ASIC designs are relatively straightforward to reverse engineer [2]. RE can be automated and done cheaply using open-source and commercially available tools [3]. Because RE attacks are so prevalent, protective countermeasures are an important security consideration.

Trojan circuit insertion is another problem faced by both chip vendors and consumers. A malicious entity at a fab or maskmaker can inject unwanted functionality into a "secure" design without the chip vendor's knowledge by modifying the design's mask data prior to fabrication. Resistance to Trojan circuit insertion is an important aspect of Anti-Tamper (AT) protection.

This paper describes integration and tool flow techniques to protect hardware IP from RE attacks and Trojan circuit insertion using a type of hardware obfuscation called circuit camouflage. Circuit camouflage is a set of cell design, circuit design, and layout techniques that obfuscate the real logic function of a circuit from imaging analysis. Circuit camouflage allows chip designers to keep sensitive aspects of custom designs secret from reverse engineers. Several different circuit camouflage techniques are presented with an analysis of their security as well as their practicality of implementation. Three different styles of digital camouflaged logic cells are presented, each of which is a novel way to disguise the function of a hardware circuit. Also, a camouflaged smart fill methodology designed for circuit obfuscation is presented. Camouflaged logic cell and camouflaged smart fill technologies can be used separately or together to provide strong RE resistance and AT protection.

DAC 2014, June 1–5, 2014, San Francisco, CA, USA.

http://dx.doi.org/10.1145/2593069.2602554

2. BACKGROUND

The goal of circuit camouflage technology is to render RE and Trojan circuit insertion infeasible. It is helpful to have a basic understanding of RE techniques prior to examining countermeasures. RE is a rich subject for study, but for the purposes of this paper, it is enough to understand that when analyzing a digital circuit, RE utilizes image recognition to identify cell functions. These images can be obtained from silicon devices through destructive de-layering or non-destructive imaging. For a digital application-specific integrated circuit (ASIC), this process is highly automated. After obtaining scanning electron microscope (SEM) images of active, poly, contact, metal, and via layers, automated software programs assist the RE task by building an image database of gate layouts, and extracting a full netlist using image recognition software. Gate-array designs require only metal, contact, and via layers to completely reverse engineer [4]. Often, only Metal-1 imaging is required to uniquely identify a cell's function [3].

3. CAMOUFLAGED LOGIC CELLS

Camouflaged logic cells are gates whose logic function cannot practically be determined using traditional RE techniques including image recognition and voltage contrast. Camouflaged logic cell layouts employ the concept of a camouflaged connection. A camouflaged connection is either an apparent connection between two or more nodes that actually performs no connection (connected nodes appear to be isolated), or a connection between two or more nodes that is designed to be undetected (isolated nodes appear to be connected). There are a large number of physical implementations available to create camouflaged connections [5,6,7]. Although a detailed discussion is outside this paper's scope, commercial products show camouflaged connections are extremely difficult to detect using modern RE techniques [12]. Most connection implementations can be fabricated at virtually any process node; others may be restricted.

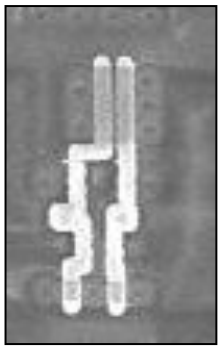

Figure 1. Conventional 2-input NOR gate poly layer

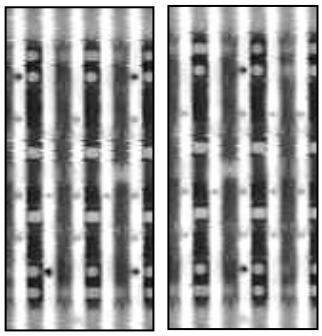

Figure 2. Camouflaged 2-input NAND (left) and NOR (right) gates, metal layer

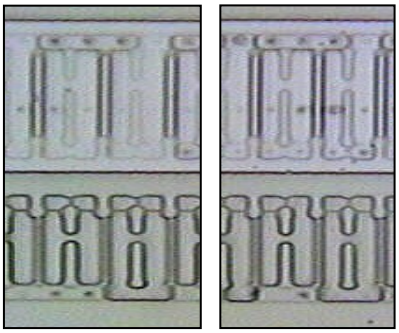

Figure 3. Camouflaged 2-input NAND (left) and NOR (right) gates, active layer

A set of SEM images was taken from two fielded silicon devices to compare a camouflaged logic cell, designed with camouflaged connections, against a standard logic cell. A foundry's conventional 2-input NOR gate, taken from a conventional fielded silicon device, is shown in Figure 1. Camouflaged 2-input NAND and NOR gates, taken from a camouflaged silicon device, are shown in Figures 2 and 3. The standard logic cell shown in Figure 1 is immediately recognizable to a reverse engineer or pattern recognition software program because of its distinctive visual signatures.

The camouflaged cells shown side-by-side in Figures 2 and 3 do not contain recognizable visible signatures that would aid in pattern recognition. Cell functions are differentiated through use of camouflaged connections, which are difficult to detect. The vertical traces in the centers of the cells of Figure 2 are the metal layers of two camouflaged gates, a 2-input NAND gate on the left and a 2-input NOR gate on the right. The active layers of the same gates are shown in Figure 3. Since these camouflaged gates were custom-designed such that all transistors are of equal size and spacing, cell boundaries between abutted cells are hidden, which further complicates RE and circuit extraction [8].

Three styles of camouflaged logic cells are presented below. The camouflaged cells do not require any fabrication process changes, and camouflaged cells can co-exist with non-camouflaged cells on a single chip. One style of camouflaged cells is typically chosen for a design, although nothing precludes using multiple styles of camouflaged logic cells on a single design.

3.1 Foundry Standard Cell

In the Foundry Standard Cell approach, a camouflaged cell library resembling the ASIC's target foundry's standard cell library is created to supplement and add security features to the foundry's original cell library. The secure ASIC is comprised primarily of foundry cells, but also contains enough camouflaged cells to thwart the reverse engineer.

Additional custom cells that visually mimic logic gates from the ASIC's target foundry standard cell library but possess differing logical functions are used sporadically in the ASIC. Through use of camouflaged connections, the camouflaged cells' functions would differ from what their layouts suggest. When attempting a circuit extraction, RE analysis would mistakenly interpret the camouflaged "look-alike" gates as foundry standard cell gates, resulting in an incorrect netlist. The concept of camouflaged connections is used to construct these look-alike camouflaged cells.

The target foundry library cell's layouts impose some restrictions on the logic function of look-alike camouflaged cells. Typically the function of the camouflage cell must be of equal or lesser complexity than the original foundry standard cell. For example, it would be possible to utilize camouflaged connections to make a functional camouflaged inverter that appears to be a buffer, but it would not be possible to design a functional camouflaged 3-input NAND gate that looks like a 2-input NAND gate.

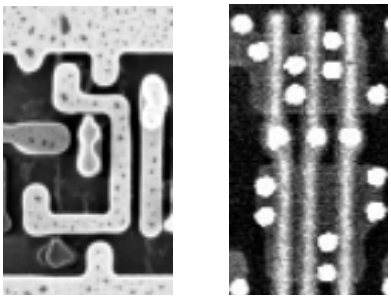

Figure 4. Conventional 2-input AND gate

SEM images of the Metal 1 (left) and Poly (right) layers of a foundry's library AND2 gate are shown in Figure 4. The same layers of a camouflaged standard cell gate, designed to resemble the foundry's library gate while performing a different function, are shown in Figure 5. Because the foundry cell appears identical to the camouflaged cell, a reverse engineer following standard

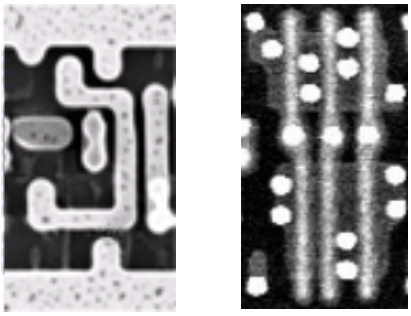

Figure 5. Camouflaged 2-input AND gate with alternate function

procedures would interpret both cells as AND2 gates. Since the camouflaged gate performs a different function than AND2, the resulting netlist extracted from silicon would not function correctly.

A higher number of unique camouflaged cell designs results in a stronger implementation of the foundry standard cell camouflage approach. Multiple layouts based on the same foundry library cell can add uncertainty to the RE process.

3.2 Custom Cell

The custom cell approach features a custom-designed, functionally complete camouflaged cell library. A circuit, or an entire ASIC, would be comprised solely of these custom cell camouflage cells. Since the camouflaged library is custom-designed, the cells can be optimized for a number of design goals such as reducing area, improving timing, or low switching power, or low leakage. Custom cell camouflage libraries perform similarly to other standard cell library at the same technology node.

The primary feature of a strong custom cell camouflage library is that every cell appears identical to every other cell in the library at every mask layer, which prevents automated cell recognition. Different logic functions are realized through use of camouflaged connections. Groups of cells are designed such that physical layouts of cell substructures utilize only transistors of identical size and spacing with those of other cells in the group. Because all transistors have the same size and spacing, the cell boundaries disappear when cells are abutted to each other, making RE much more difficult. Following standard RE techniques, it would not be possible to differentiate the 2-input NAND from the 2-input NOR gate in Figures 2 and 3.

The strength of the custom cell library increases with more unique cell designs. Multiple layouts of the same cell function can add uncertainty to the RE process.

3.3 Elementary Block

An Elementary Block library is another style of custom-designed, functionally complete camouflaged cell library. Similar to custom cell, an elementary block camouflaged circuit consists of apparently-identical structures replicated throughout the entire ASIC. However, instead of all transistors being identical in size and spacing, elementary block camouflage libraries are derived from one logic gate layout. Different logic functions are realized through camouflaged connections. An entire ASIC or block is comprised of cells derived from the same library cell layout [9].

An elementary block camouflaged library also supports cells that can be programmed after manufacture. Use of one-time-programmable (OTP) technology enables post-production programmability of some gates in the design, which has a number of possible applications. By performing the final programming step in a secure facility, critical design secrets can be protected from theft by a malicious fab. Furthermore, programmable gates can be strategically used in a functional implementation such that different functions can be realized with the same circuit after post-production programming.

4. CAMOUFLAGED SMART FILL

Camouflaged smart fill, also referred to as Post Place & Route (PP&R) processing techniques, consist of overlaying active cell and metal geometries that resemble real logic cells and interconnect. The fill layers also include contacts and vias, connected in a realistic fashion to create a dense routing network. Active signals may be included in this fill process, which grants additional resistance to voltage contrast tools used by reverse engineers. The added network of cells and interconnect dramatically increases the RE workload and error rate.

The addition of camouflage smart fill provides protection for the designer's ASIC against Trojan circuit insertion by consuming all unused silicon area in the processed layers. An attacker cannot insert any logic gates or create any additional routing traces without removing existing circuitry. To increase the complexity of the PP&R camouflage smart fill process, portions of the filled network can be connected back into the ASIC. It is difficult for an attacker to know which traces are functional or extraneous.

Camouflaged smart fill can be applied alone or in conjunction with camouflaged logic cells. It is also possible to employ camouflaged logic cells without employing camouflaged smart fill. When possible, the best RE protection utilizes both obfuscation techniques. Camouflaged smart fill may be selectively applied to sections of an ASIC, with design considerations discussed in Section 5. Note that resistance to Trojan circuit insertion will be reduced in an incompletely filled design.

4.1 Filling Metal Layers

After an ASIC design has passed logic and physical verification, PP&R processing techniques can be applied to the design's mask data on a layer-by-layer basis without affecting the function of the ASIC. Realistic logic cell patterns on Metal-1 with metal and via interconnect can be employed to consume all available cell area and routing channels on the die. The visual effect of this fill differs greatly from traditional types of fill that are used for yield improvement and meeting metal density rules. Figure 6 illustrates a design before and after its metal layers have been filled with camouflaged smart fill. In addition to increasing the volume of data to process, the PP&R camouflage smart fill also increases uncertainty of the RE task since it becomes difficult to determine which traces are real and which are extraneous. Additional metal traces can be tied to power, ground, an active switching signal, or can be floating. A variety of signal types reduces the effectiveness of reverse engineering techniques such as voltage contrast.

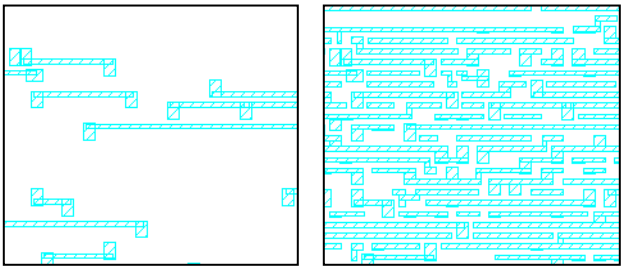

Figure 6. Before and after camouflage smart fill of poly, contact, and active layers

4.2 Filling Active Device Layers

In addition to filling metal layers, active device layers can be filled with realistic filler cells without affecting the function of the ASIC [10]. As with metal fill, filling the active device layers increases the reverse engineer's workload and uncertainty. The devices are connected to the metal fill network described in

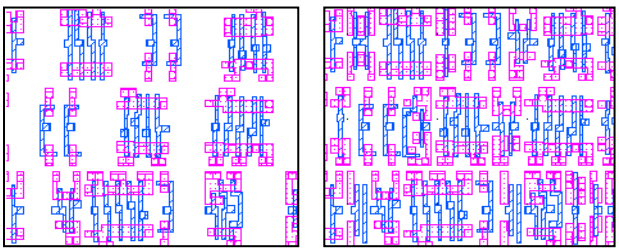

Figure 7. Before and after camouflage smart fill of poly, contact, and active layers

Section 4.1. Figure 7 illustrates a design before and after Poly, Contact, and Active layers have been filled.

Filling active decice layers also increases a reverse engineer's uncertainty regarding cell boundaries. When this technique is combined with a custom cell camouflaged library, where all transistors are of equal size and spacing, the problem of identifying which cells are part of the real design becomes exceptionally difficult.

5. DESIGN CONSIDERATIONS

The technologies described in this paper introduce new security features to an ASIC design that can be integrated into a standard design flow. Circuit camouflage is a set of novel cell and ASIC layout techniques that provide strong resistance to RE without affecting the device's logical function. Circuit camouflage features are 100% CMOS compatible, requiring no foundry process changes [8]. However, designers must plan on possible impacts to a circuit's area, timing, and power consumption. Not surprisingly, the impact to area, timing, and power depends primarily on the set of circuit camouflage features to be chosen.

Foundry standard cell camouflage logic cells generally have a miniscule impact on design area and power, depending on the number of cells used. A small number of extra cells, on the order of a few percent of the design area to be camouflaged, is very effective in preventing reverse engineering. Overall timing impacts can be effectively nullified by avoiding touching the ASIC's critical timing paths.

An ASIC design that is synthesized to a custom cell camouflage logic cell library does not inherently incur any area, timing, or power penalties when compared to a typical standard cell library at the same technology node. A custom cell camouflage library can be designed to meet area, timing, or power criteria with similar constraints as a traditional standard cell library.

An ASIC design that is synthesized to an elementary block camouflaged library will incur some area when compared to a typical standard cell library at the same technology node. It is expected that this penalty is on the order of 10%, although this number varies by library implementation and is also highly design-dependent. Timing and power consumption penalty is expected to be significantly less than the area penalty. An elementary block camouflage library can be designed to meet area, timing, or power criteria, although with less efficiency than a custom cell camouflage library. The programmable elementary block cells mentioned in Section 3.3 incur a further area penalty because of additional circuitry required to support programming.

Camouflage smart fill introduces additional traces to a design. Due to the increased parasitic capacitance of these traces, a design employing this fill will incur an average interconnect timing penalty on the order of 5-10% for the 90nm technology node. This figure will vary based on technology and routing density. Camouflage smart fill can be applied selectively to portions of an ASIC, such as specifically targeting the security core of a larger system-on-a-chip. To mitigate the additional parasitic capacitance, designers may choose to avoid applying camouflage fill certain high-frequency sections of the chip. Placing camouflaged smart fill traces adjacent to clock nets is generally avoided, as this can introduce unwanted delay and skew into a clock tree.

6. RELIABILITY AND EFFECTIVENESS

Circuit camouflage technology has been utilized to protect proprietary algorithms and other IP, to secure smart card secrets, and to prevent counterfeit devices in commercial and government sectors for over 20 years. This circuit camouflage technology also provides anti-tamper protection and inhibits the insertion of Trojan circuits during the manufacturing process. A leading vendor of circuit camouflage technology claims over 200 million devices employing their circuit camouflage cell libraries and camouflage smart fill are deployed in the field, with no known in-field failures or security compromises [8].

7. CAMO TOOL FLOW INTEGRATION

A Camouflage library is developed for a specific feature size and fabrication process. To an ASIC designer, Camouflaged logic cells are merely another type of standard cell to be used in the ASIC design. The fabrication process design rules and DRC+LVS run decks are used for camouflage library design and verification. All phases of design and verification utilize industry standard tools and models. For the initial camouflage library development of a Foundry Standard Cell Camouflage library, the Camouflage library designer receives frontend (Verilog and .lib) and backend (GDS, LEF, and CDL) files for the foundry standard library. The fabrication house makes this data available to the Camouflage library developer. It is important that the same version of the foundry standard cell library, design rules and run deck be used in the Camouflage library design and in the integrated circuit design by the ASIC designer when developing their product.

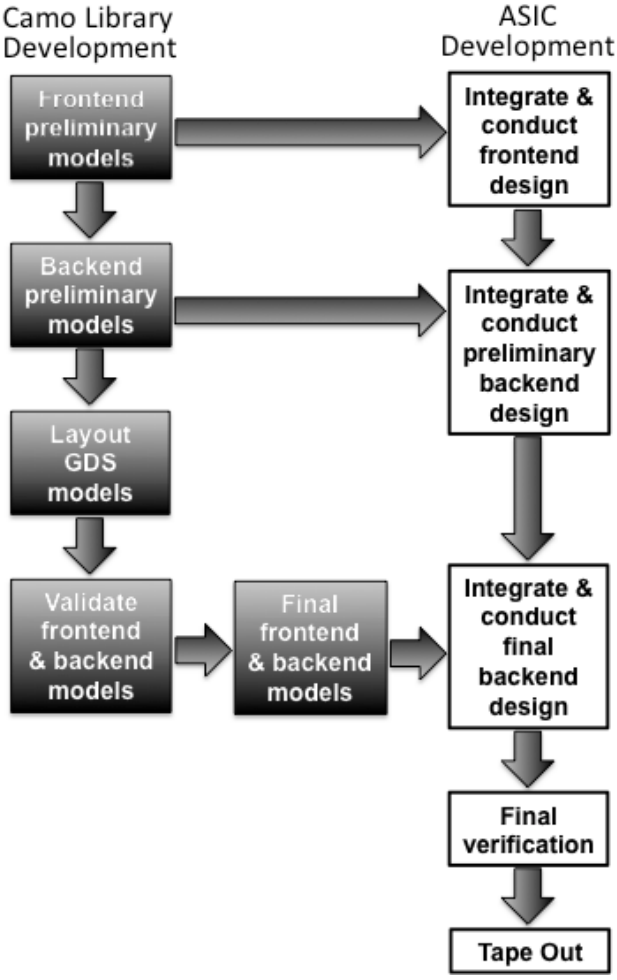

Figure 8. Camo Library Development integration with a typical ASIC design flow

Figure 8 depicts a Camouflage Cell Library development integrated into a typical ASIC development. Preliminary frontend models of the Camouflage library can be generated almost immediately using a script-based generation process based on the foundry standard cell library's Verilog and .lib models. This can be done before the Camouflage logic cells layouts are designed, allowing Camouflage library cell design to proceed in parallel with the overall ASIC design. The ASIC designer can begin designing their product and can perform frontend tool flow trials while production backend Camouflage library models are being developed. Once the Camouflage library cell layouts are ready, production frontend models can be created by the Camouflage library designer with industry standard library model generating tools.

A layout editor is used to design backend GDS layouts for the logic cells. This process typically takes several months, depending on the number of Camouflage logic cells in the library. Design rules are extensively studied and consulted during the cell layout process. Hundreds of polygons are used to construct cells. DRC and LVS tools are used to validate the design of each cell. Camouflage cells are abutted against other logic cells to ensure that all design rules are met. LEF models, used for automated place-and-route, can be generated using industry standard tools such as Cadence Virtuoso. CDL models, used for LVS verification, are created using standard backend design tools.

After the Camouflage library backend models are complete, the ASIC designer performs a final verification of the models and integrates the production Camouflage library models into their flow. The ASIC designer will then conduct end-to-end tool flow trials. The ASIC designer performs a trial run to ensure that all frontend and backend models are present and that they adhere to the foundry design rules and run deck. ASIC design proceeds by following all design and verification steps as appropriate for their typical flow (such as DRC/OPC/LVS/Antennae). After this process has been completed, the ASIC with integrated Camouflage library cells has passed all verification rules and is ready for tape out.

The tool suite used by the Camouflage library designer does not have to be the same as those used by the ASIC designer. However, the appropriate models and format needs to be established so that the ASIC designer can use what is produced by the Camouflage library designer. All cells and extraneous camouflage circuits are Spice and switch-level simulated to guarantee minimal additional leakage current and correct output polarity. ASIC designers are provided all models and perform the same stringent verifications applied to their own non-Camouflaged designs.

8. CONCLUSIONS

Circuit camouflage technology provides mature and effective methodologies for protecting a circuit against reverse engineering, counterfeiting, and Trojan circuit insertion. Depending on security, design, and schedule requirements, some methodologies may be more appropriate than others. These techniques have been readily adapted suit a standard design flow so that they can be applied to a broad array to target domains.

9. REFERENCES

[1] Guin, U., Tehranipoor, M., DiMase, D., and Megrdician, M. 2013. Counterfeit IC Detection and Challenges Ahead, ACM SIGDA (Mar. 2013).

[2] Torrance, R., and James, D. 2009. The State-of-the-Art in IC Reverse Engineering, *Proceedings of the Cryptographic Hardware and Embedded Systems* (Sep. 6-9 2009).

[3] Nohl, K, Evans, D., Plotz, S., Plotz, H. 2008. Reverse-Engineering a Cryptographic RFID Tag, USENIX Security Symposium (Jul. 31 2008).

[4] Avery, L.R., Crabbe, J. S., Al Sofi, S., Ahmed, H., Cleaver, J. R. A., Weaver, D. J. 2002. Reverse Engineering Complex Application-Specific Integrated Circuits (ASICs), *Proceedings of the Diminishing Manufacturing Sources and Material Shortages Conference* (Mar. 2002).

[5] Baukus, J. P., Clark, Jr., W. M., Chow, L. W., Kramer, A. R. 2001. Secure Integrated Circuit. (Sept. 2001). US Patent No. 6294816, Filed May 29th., 1998, Issued Sept. 25th., 2001.

[6] Baukus, J. P., Chow, L. W., Clark, Jr., W. M. 1999. Digital circuit with transistor geometry and channel stops providing camouflage against reverse engineering. (July 1999). US Patent No. 5930663, Filed May 11th., 1998, Issued July 27th., 1999.

[7] Clark, Jr., W. M., Baukus, J. P., Chow, L. W. 2004. Implanted hidden interconnections in a semiconductor device for preventing reverse engineering. (Nov. 2004) . US Patent No. 6815816, Filed Oct. 25th., 2000, Issued Nov. 9th., 2004.

[8] SypherMedia International, Inc. 2012. Circuit Camouflage Technology. (Mar. 2012) . Retrieved Dec. 2, 2013 from http://smi.tv/SMI_SypherMedia_Library_Intro.pdf

[9] Cocchi, R. P., Baukus, J. P., Wang, B. J., Chow, L. W., Ouyang, P. 2012. Building block for secure CMOS logic cell library. (Feb. 2012). US Patent 8111089, Filed May 24th., 2010, Issued Feb. 7th, 2012.

[10] Chow, L. W., Baukus, J. P., Wang, B. J., Cocchi, R. P. 2012. Camouflaging a standard cell based integrated circuit. (Apr. 2012). US Patent 8151235, Filed Feb. 24th., 2009, Issued Apr. 3rd, 2012.

[11] Sobh, T., Elleithy M. K., and Patel S. 2007. Reverse Engineering of VLSI Chips: A Roadmap, *Journal of Engineering and Applied Sciences*, Vol. 2, No. 2, pp 290-298 (2007).

[12] SypherMedia International, Inc. 2014. Circuit Camouflage Technology. (Feb. 2012) . Retrieved Feb. 28, 2014 from http://smi.tv/solutions.htm#lib