ISSN 23499842(Online), Volume 2, issue 1 March 2017
International Journal of Innovative Trends and Emerging Technologies

A HIGH LEVEL KEY-DRIVEN TRANSFORMATIONS FOR HARDWARE SECURITY USING QR CODING

A. KALYANI[1], G. MOHAN RAJ[2]
[1]*PG Scholar, VLSI Design, Department of ECE, Mahabarathi Engineering College, India*
[2]*Assistant professor, Department of ECE, Mahabarathi Engineering College, India*

Abstract
The hardware is protected by various techniques. It involves modification in the layout diagram by adding any dummy connections. Obfuscation is one of the security techniques to protect the hardware. By this method, any gate structure is replaced by xor and an inverter component. It adds additional complexity. Thus reducing the complexity of a device, a high level key driven transformation is used. It includes meaningful and non-meaningful operations. For meaningful operations, each input produces different outputs for every time. And also QR code is used to store the key value. The speed of the process depends on the number of key size and QR code is used to increase claiming rate. Thus the hardware is highly secured by this method.

Index terms: QR code

1. Introduction
A critical challenge for nano electronic systems is to achieve yield and reliability. As VLSI technology scales into the nanometer scale, devices and interconnects are subject to increasingly prevalent defects and significant parametric variations. Based on photolithography, we are making layout features of smaller dimensions than the wavelength of the light, which requires increasingly complex OPC and other DFM techniques at increasing layout area cost. Future nanoelectronic systems are expected to be based on self-assembly manufacture of a regular physical structure, and achieve functionality by reconfiguration. Reconfiguration is further critical for nanoelectronic systems to achieve yield and reliability by bypassing defective or degraded devices and interconnects, which occurrence cannot be avoided or reduced below a certain level as is determined by the uncertainly principle of quantum physics. Here present that reconfigurable computing is further a critical technology to achieve hardware security in the presence of supply chain adversaries.

Hardware is the foundation and the root of trust of any security system. In recent years, a growing number of software based security solutions have been migrated to hardware-based security solutions for much enhanced resistance to software based security threats. Such systems range from smartcards to specialized secure co-processing boxes, wherein hardware provides the source of security and trust for a number of security primitives. However, in recent years, it has been brought into light that hardware is also subject to a number of security threats. An adversary may extract cryptographic keys and confidential information from a system by testing, reverse engineering, or side-channel analysis. More critical threats come from the supply chain and compromise hardware integrity. In today's global IC industry, a supply chain adversary, such as an IP provider, an IC design house, a CAD company, or a foundry may have access to the source code of the design, and may easily tamper a hardware system by planting time bombs which compromise hardware computation integrity, or creating back doors which enable information leak, bypassing access control mechanisms at higher (e.g., OS and application) levels. . In this proposes to achieve VLSI design obfuscation by reconfigurable implementation of a given logic function, which is determined by the end user and unknown to any party in the supply chain. The recently-released Comprehensive National Cyber Security Initiative has identified this supply chain risk management problem as a top national priority. A supply chain adversary's capability is rooted in his knowledge on the hardware design. Successful hardware design obfuscation would severely limit a supply chain adversary's capability if not preventing all supply chain attacks. However, not all designs are obfuscatable in traditional technologies. Here propose to achieve moving target defense in VLSI design by reconfiguration for different logic functions. Moving target defense has been proposed against software based attacks. Obfuscated implementation of a moving target defense scheme further prevents a supply chain adversary or a hardware Trojan from tampering or gaining knowledge on the scheme and launching an attack without being detected. The further propose reconfigurable reversible computing (RRC) - based cryptography and present a generic reconfiguration-based supply chain risk management methodology. This is to design obfuscated circuits by applying high-level transformations during the design phase. The key idea of the proposed work is to generate meaningful design variations by exploiting high-level transformations.

2. Related Work
In this remote activation of ICS for piracy prevention and digital right management by Y. Alkabani, F. Koushanfar and M. Potkonjak [1] provide an overview of Physical Unclonable Functions and explain why they are a very valuable technology to protect a company's IP and hence at the same time its brand. Physical Unclonable Functions are unclonable physical structures that map challenges to responses. They inherit their unclonability from the (deep sub-micron) process variations during manufacturing. They can be turned into a useful tool to generate very secure secret keys in ICs and to provide keys to protect valuable IP of fabless IC companies, IP Vendors and design houses but they provide high overhead.

A. Baumgarten, A. Tyagi and J. Zambreno presented a provably secure method called preventing IC piracy using reconfigurable logic barriers for embedding multiple watermarks in sequential designs [2]. A number of different watermarks signed with the IP owner's secret key from a public key cryptography system are generated. The owner's watermarks are then dissembled into the states and transitions

of the original sequential design. Analysis of watermark properties and the attack resiliency of the new multiple watermarking constructions were presented. Experimental evaluations on benchmark circuits demonstrate practicality and low overhead of the new provably secure multiple watermarks construction method. The main limitation of this method is that it involves more transitions.

As semiconductor manufacturing requires greater capital investments, the use of contract foundries has grown dramatically, increasing exposure to mask theft and unauthorized excess production. While only recently studied, IC piracy has now become a major challenge for the electronics and defense industries. S. Bhunia and R.S. Chakraborty [3] proposed a novel comprehensive technique called harpoon: an obfuscation-based soc design methodology for hardware protection to end piracy of integrated circuits (EPIC). EPIC [6] is based on (i) automatically-generated chip IDs, (ii) a novel combinational locking algorithm, and (iii) innovative use of public-key cryptography. The overhead of EPIC on circuit delay and power is negligible, and the standard flows for verification and test do not require change in the evaluation. In fact, major required components have already been integrated into several chips in production. A comprehensive protocol analysis concludes that EPIC is surprisingly resistant to various piracy attempts. It requires that every chip be activated with an external key, which can only be generated by the holder of IP rights, and cannot be duplicated.

Recent trends of hardware intellectual property (IP) piracy and reverse engineering pose major business and security concerns to an IP-based system-on-chip (SoC) design flow. D. James and R.Torrance proposed a Register Transfer Level (RTL) hardware IP protection technique based on low-overhead key-based obfuscation of control and data flow called the state of the art in semiconductor reverse engineering [4]. The basic idea is to transform the RTL core into control and data flow graph (CDFG) and then integrate a well obfuscated finite state machine (FSM) of special structure, referred as “Mode-Control FSM”, into the CDFG in a manner that normal functional behavior is enabled only after application of a specific input sequence. However the implemented have little overhead in the process of obfuscation.

3. Proposed Method

High-level transformations have been known for a long time and have been used in a wide range of applications, such as pipelining and have been used in synthesis of DSP systems. An adversary knows which inputs are functional inputs and which inputs are lock inputs. He can then identify the lock gates connected to the lock inputs. Structural obfuscation and functional obfuscation are defined as follows: Piracy protection is achieved by structural modification, which is realized by altering the structure of a DSP circuit by using high-level transformations. This is a so-called ”passive” technique, which does not directly affect the functionality of the DSP circuit. Obfuscation is used to hide the functionality from others. Achieved by functional modification, which is realized by encrypting the normal functionality of a DSP circuit with a key. The DSP circuit cannot function correctly without the key. This is an ”active” technique, which directly alters the functionality. High-level transformations alter the structure of a DSP circuit, while maintaining the original functionality.

A novel DSP hardware protection methodology through obfuscation by hiding functionality via high-level transformations is proposed. The Figure 1 shows that it helps the designer to protect the DSP design against piracy by controlling the circuit configuration among the generated variation modes F G SR clk reconfigurator reset state MUX select signal connection 1 connection 2 connection k Obfuscating configuration FSM key (switch instances) and then the ring counter is used to give the control signal to the multiplexer.

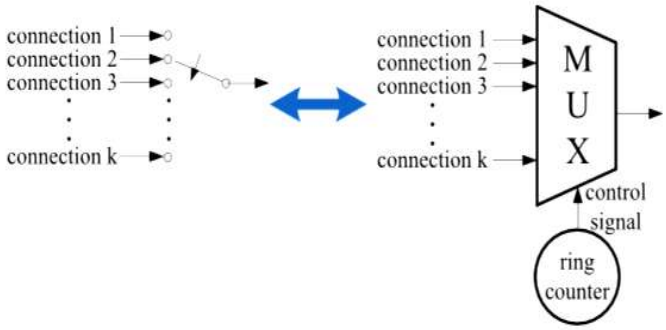

Figure 1: Proposed Secure Switch Design of the Original Design

The detailed design flow is described below

Step 1: DSP algorithm. This step generates the DSP algorithm based on the DSP application.

Step 2: High-level transformation selection. Based on the specific application, appropriate high-level transformation should be chosen according to the performance requirement (e.g., area, speed, power or energy).

Step 3: Two-level FSM generation. The reconfigurator and the obfuscating FSM are incorporated into the DSP design. The configuration key is generated at this step.

Step 4: Design specification. This step includes the HDL and netlist generation and synthesis of the DSP system. The proposed design methodology does not require significant changes to established verification and testing flows. In fact, the obfuscated DSP circuit with the correct key behaves just like the original circuit.

Here we use that the DSP circuits can be obfuscated via high-level transformations [7] by appropriately designing the switches in a secure manner. The switches generated by high-level transformations are periodic N-to-1 switches. These switches can be implemented as multiplexers, whose control signals are obtained from ring counters. Thus, the security of the switch relies upon design of the ring counters such that the outputs of the ring counters can be obfuscated. A ring counter is often modeled as an FSM. An FSM is usually defined by a 6-tuple (I, O, S, S_0, F,G), where S is a finite set of internal states, I and O represent the inputs and outputs of the FSM, respectively, F is the next-state function, G is the output function, and S_0 is the initial state. However, unlike general FSMs, the FSM of a ring counter is input independent, such that it always transits to the next state based on the current

state. As a result, the control signal of the switches (i.e., output of the FSM) will be periodic. In Obfuscation via high-level transformation, selected high-level transformations are applied simultaneously.

In existing works, they have demonstrated that functional obfuscation can be achieved by embedding well-hidden FSM (i.e., obfuscating FSM) in the circuit to control the functionality based on a key. In order to achieve design obfuscation by using high-level transformations, we propose a reconfigurable switch design. The detailed implementation is shown here where SR represents the state registers that store the information of the current state. The complete system of the proposed obfuscated DSP circuit is described in detail. The DSP circuits are obfuscated by introducing a FSM whose state is controlled by a key. The FSM enables a reconfigurator that configures the functionality mode of the DSP circuit. High-level transformations lead to many equivalent circuits and all these create ambiguity in the structural level. High-level transformations also allow design of circuits using same datapath but different control circuits. For example, a datapath may implement a 3rd-order or a 6thorder digital filter, or in general an order filter, where l is a positive integer.

These correspond to different modes. While these modes generate outputs that are functionally incorrect, these may represent correct outputs under different situations, since the output is meaningful from a signal processing point of view. Finally, other modes lead to non-meaningful outputs. The initialization key and the configure data must be known for the circuit to work properly. Consequently, the circuit behaves as an obfuscated circuit.

Programs can be written where:

- Filter weighting functions (coefficients) can be calculated on the fly, reducing memory requirements.

- Algorithms can be dynamically modified as a function of signal input.

4. Structural Degree Obfuscation

Structural Obfuscation Degree: Manual attacks can be performed by visual inspection and structural analysis. In these types of manual attacks, the adversary has to analyze the RTL or gate-level structure as well as the layouts. This is a weak attack, as the adversary has very little chance of figuring out the obfuscation scheme for large DSP circuits. The obfuscation degree of the structural obfuscation is dependent on the number of independent switches (Ns), the period of switch instances after high-level transformations (P), and the number of connections for each independent switch (Cm). The main objective is to protect DSP circuits against reverse engineering. The obfuscated DSP circuits will only operate in the desired mode with a negligible probability that others would be able to find. Thus, the correct functionality is hidden to the adversary even when the adversary can access the DSP circuits. In addition, the proposed obfuscating scheme also satisfies a set of following properties to ensure security and resiliency against attacks.

The obfuscation is invisible to the functional DSP circuits. Its presence would not interfere with regular operation of the design. The probability of finding the correct key for a DSP circuit is low by employing our proposed obfuscation scheme. The chance for an adversary to enter a DSP circuit into the correct mode by random guessing is 1/2L+K, which will be negligible when the bit-length of the key is long. Therefore, the correct key is a strong proof of ownership.

Since the obfuscation modes are generated along with the high-level transformation design phase [5], all the stages after this phase in the high-level synthesis flow would contain the obfuscation. The proposed obfuscating methodology can be used for all common DSP designs. It has only described a few examples of high level transformations for hardware obfuscation. Finite State Machine is used to control the output signals. Initial four bit keys are given to the encoder where the four bit keys are converted into sixteen bit keys. In this first eight bit keys are taken and it is converted into three states. This output is used as configuration key to the reconfiguration. This key is again stored into the QR code.

5. Experimental Results

The figure 2 shows that the key value is changed mean that the different pulse value is obtained. It depends upon the clock and reset signals. The combination of positive and negative pulse is given as clock signal. For each key value, each output is obtained. Suppose when the correct key value is given means than their corresponding output is obtained. Thus the key value is directly depends on their output.

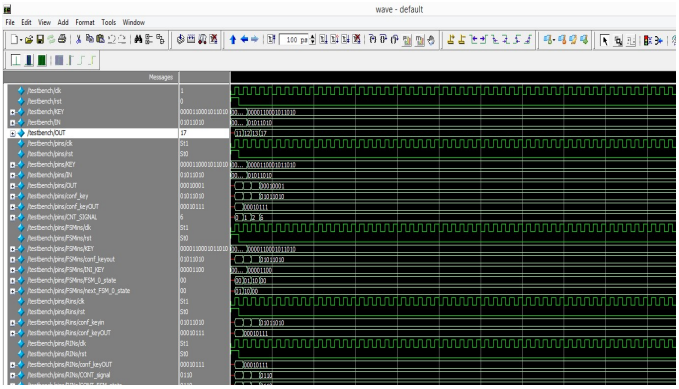

Figure 2: Key values changed and the corresponding output

A. SYNTHESIS REPORT

The figure 3 shows that the four bit keys, reset and clock signals are given to the obfuscating pins and this output is given to the reconfigurator where the four bit keys are converted into eight bit keys. And then in the ring counter this key is again reduced to four bits. Thus this output value is put as key to the reconfigurator.

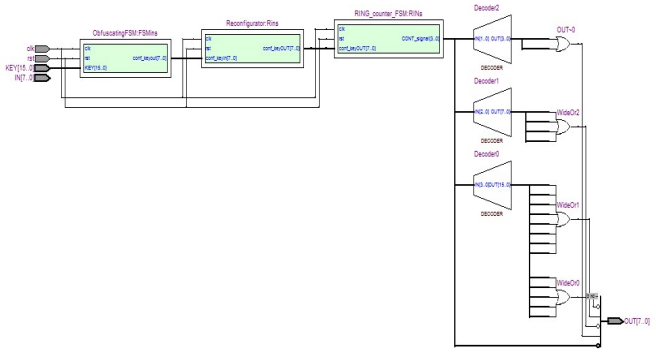

Figure 3: RTL Schematic Report

B. MAP VIEWER

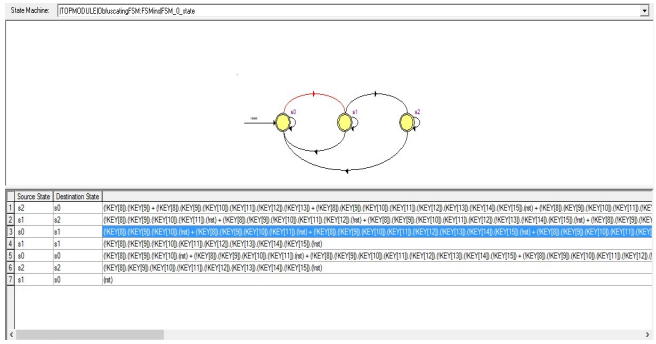

Figure 4: Technology Map Viewer

This technology map viewer figure 4 shows that the key values are divided into different states such as state0, state1 and state2. Each source state is defined as s0, s1 and s2. Map viewer is similar to the signal state diagram. This graph shows the plot of different states. For confusing the piraters the key values are given into different states at different format.

C. COMPARISON TABLE

A hardware system is reconfigurable if a user can direct the system to perform different computations by writing to the memory of the system. In a broad sense, a general-purpose computer is reconfigurable in that an user can direct the system to perform different computations by writing to the instruction memory. While for reconfigurable computing most people today refer to programmable logic devices (PLD) such as field programmable. LUT-based reconfigurable logic as in FPGA gate arrays (FPGA), where a configuration memory directs an array of configuration multiplexers for different interconnect structures and logic functions.Cyclone III is used as a family in the Quartus II tool. The total number of registers used in this method is thirteen for measuring the area. The total logic elements used in the Quartus II tool is thirty three and the total number of pins in this method is thirty four. No additional memory is used by this method. The total phase locked loop is zero. Thus the total area is reduced by this method.

Typical technology of today for a reconfigurable logic function is based on a lookup table, including a 2 n -to-1 multiplexer and 2 n configuration memory cells for an n-input logic function, while alternative reconfigurable computing fabrics have been proposed for emerging technologies.The Table 1 shows the maximum speed of the slow corner in the obfuscation method. Speed is defined as how fast the device or hardware runs. The maximum speed of the slow corner is 487.33MHz.

From the Table 1, the experimental evaluations shows that the total thermal power dissipation in the existing system is 113.49mW and in the proposed system the total power dissipation is reduced to 57.84mW. The dynamic power dissipation is zero and the static and thermal power dissipation is reduced than the existing method. On comparing both the existing and proposed system the overall power dissipation is reduced.

Table 1: Trade Off Analyzes Of Number States Vs Performance Report with QUARTUS II Hardware Synthesis Using CYCLONE II Family (EP2C35F672C6)

TYPE	AREA	SPEED	PPOWER DISSIPATION
TYPE trade off design (maximum FSM states)	513	317.16MHz	57.84mW
TYPE volume key input (optimal FSM states)	512	59.66MHz	98.6mW
Existing method	654	49.56MHz	113.49mW

6. Conclusion

This project proved the efficiency of structural and functional obfuscation by utilizing high-level transformation techniques with variation in modes. Here construct the secure reconfigurable switch design which will increases hardware complexity slightly as the as compared to existing method. Compared with all other existing obfuscation methods, in the proposed methodology, key input will give non-meaningful variation modes in levels. Here analyze the complexity trade-off between numbers of states in FSM over complexity. Finally in order to reduce the hardware complexity without compromising security optimal FSM states were used and its efficiency is proved through hardware synthesis.

References

[1] Alkabani Y. Koushanfar F. and Potkonjak M. (2007), 'Remote activation of ICs for piracy prevention and digital right management', in Proc. IEEE/ACM Int. Conf. Comput.-Aided Design, pp. 674-677.
[2] Baumgarten A. Tyagi A. and Zambreno J. (2010), 'Preventing IC piracy using reconfigurable logic barriers', IEEE Des. Test Comput., vol. 27, no. 1, pp. 66-75.
[3] Bhunia S. and Chakraborty R.S. (2009), 'HARPOON: An obfuscation-based SoC design methodology for hardware protection', IEEE Trans. Comput.-Aided Design Integr. Circuits Syst., vol. 28, no. 10, pp. 1493-1502.
[4] James D. and Torrance R. (2011), 'The state-of-the-art in semiconductor reverse engineering', in Proc. 48th ACM/EDAC/IEEE Design Autom. Conf. (DAC), pp. 333-338.
[5] Karri R. Pino Y. Rajendran J. and Sinanoglu O. (2012), 'Security analysis of logic obfuscation ', in Proc. 49th ACM/EDAC/IEEE Design Autom. Conf., pp. 83-89.
[6] Koushanfar F. Markov I.L. and Roy J.A. (2008), 'EPIC: Ending piracy of integrated circuits', in Proc. Design, Autom. Test Eur., pp. 1069-1074.
[7] Lao Y. and Parhi K.K. (2015), 'Obfuscating DSP circuits via high-level transformations', IEEE Trans. Very Large Scale Integr. (VLSI) Syst., vol. 23, no. 5, pp. 819-830.
.