ISSN 2278-3091
Volume 8, No.1.3, 2019
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse0881.32019.pdf
https://doi.org/10.30534/ijatcse/2019/0881.32019

Hardware Obfuscation Driven by QR Pattern using High Level Transformations

Dr. D.R.V.A.Sharath Kumar[1], P.A. Lovina[2]
Professor, Department of Electronics and Communication Engineering, Samskruti College of Engineering and Technology, Hyderabad, India
Assistant Professor, Department of Electronics and Communication Engineering, St. Martins Engineering College, Hyderabad, India
E-Mail:acharyasharath79@ gmail.com[1], loviece@gmail.com[2]

ABSTRACT

This paper presents QR pattern enabled key driven approach for mitigating piracy problem over any digital design, hardware security and reverse engineering (RE) by obfuscation process. However, these techniques can able to achieve the protection with high resource utilization and power consumptions overheads and moreover structural changes alone cannot provide sufficient IP protection for the gate-level net list cores or the IC components. In order to narrow these gaps FSM based structural and functional obfuscation is proposed and key handling is solved using color QR code pattern driven random key extraction and elaborately analyzes confusion metric levels. The experimental evaluation is carried out for proving the logic obfuscation method using FIR DSP digital design. And finally the prevention of the adversary from any reverse engineers process in both the gate- level and the RTL level geometry of IP from piracy and overbuilding. Experimental evaluations demonstrate the low area, power, and trade off the performance over security level of the proposed obfuscation technique.

Key words- Finite state machine (FSM), Register transfer level (RTL), intellectual property (IP) etc.

1. INTRODUCTION

The problem of IP security is a major concern in digital design world and many works have been investigated on hardware prevention of piracy and intellectual property (IP) [1] and they are classified as follows: 1) authentication-based approach, or 2) obfuscation-based approach. Hardware protection has been investigated in many previous works using various contexts. The watermarking techniques [2] are widely used as security measures, which can only be used to prove the ownership not for the protecting the piracy from happening. On the other side Physical Unclonable Functions (PUFs) were used [3] to counterfeiting the digital devices and ICs. Recently, a number of obfuscation techniques are emerged [4] to modify the circuit content using finite-state machine (FSM). In this paper a new hardware obfuscation technique is proposed that can transform the functionally at higher level with significant computation changes which is difficult for reverse engineer to crack. In most existing hardware protection methods [5], [6] obfuscation is achieved by simply altering the code, or by encrypting the source code using some cryptographic algorithm techniques [7]. Though numerous hardware protection schemes exist based on finite-state machine (FSM) to obfuscate the ICs no high level obfuscation based IP protection approach is proposed for any digital circuits in the literature [8], [9]. In this work, for the first time, we presents color QR pattern to obfuscate the DSP circuits via FSM state transformations which are harder to reverse engineer. With QR patterns we embed large amount information's and several keys can be extracted dynamically to control the FSM states that led the DSP circuit more secure and harder for the any adversary to discover its functionality.

In other words, a high level of confusion metrics is achieved using dynamic key extraction and FSM with large number of states to obfuscate the circuits. To generate considerable design variations using abstract level transformations is the critical challenge in any digital systems to yield reliability since VLSI technology is in the nanometer scale, cause vulnerable defects and parametric variations.

In this paper, we present that hierarchical method of reconfigurable hardware structure to achieve hardware security. To mitigate the key handling issues in hardware-based security enhanced digital key extraction method is proposed which can act pseudo randomly to prevent any security threats wherein FSM states provides the source of security and confusion metrics primitives.

2. HIGH LEVEL TRANSFORMATION

Fig. 1 shows the functional block diagram of FSM based functional obfuscation. Here, a key- controlled FSM machine is introduced into a digital design which guides to operate in various distinct modes. They are obfuscated

mode and normal mode. Obfuscated mode consists of meaningful and random permuted events where the circuit behaviors are significantly changes from its original functionality, and the normal mode circuit operates in its behaviors (desired functionality). Once the circuit is reset it is in the obfuscated mode, which we prefer to use QR code patterns based key sequence and the FSM state goes through several state transitions that bring the confusion metrics to hide actual functionality. These state transitions affect the logic functions at selected time intervals, preventing the design to perform its original functionality. The FSM states also contain few empty state transitions where the design will not produce any significant results or retain the previous results to make it difficult for an adversary to identify the state elements inside FSM machine through structural analysis.

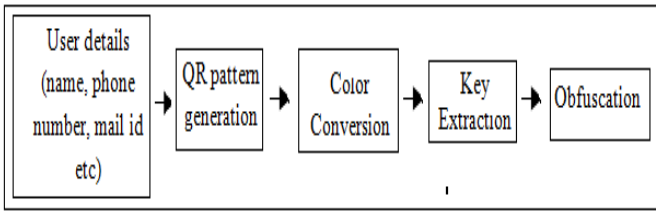

Figure 1: Functional Block Diagram

3. HIERARCHICAL OBFUSCATION APPROACH

Here novel IP protection methodology through FSM machine by changing its functionality via abstract level QR key generation is presented. This approach helps the designer to embed wide range information through pattern and protect against piracy using random key selection among the generated pixel sequence from digital QR pattern. Finally reconfiguration is assigned for each state of FSM machine and MUX selects desired connection for obfuscation as shown in figure 2.

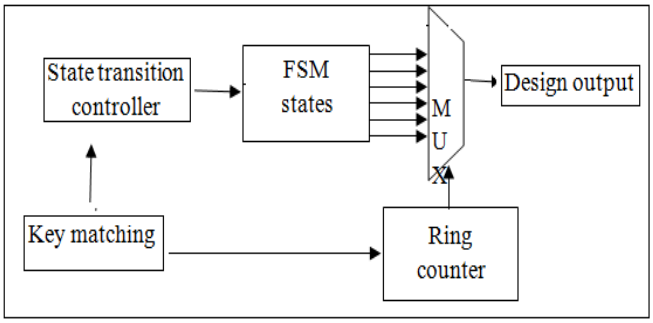

Figure 2: FSM based confusion metrics architecture

3.1 Color QR code generation

QUICK response (QR) codes have rapidly emerged as most widely used identification techniques in many real time applications like transport, retail industries. Every QR Code symbol includes an encoding region, alignment and function patterns. Depends on the encoding capacity it is available with several versions from 1 to 40.

The step by step procedure of color QR code generations is shown Fig 3. Initially input user information is encoded using alpha numeric encoder to form the compressed bit stream. The bit streams are divided into group of blocks.

Parity blocks are added for error correction metrics to generate final bit patterns.

Transform user information's into a bit stream B of codes;

Convert bits sequence B into blocks of eight bits and signifies them by a binary pattern block, resulting QR pattern image;

Convert the QR pattern into color patterns as follows; QR1-> Cyan: QR2-> Magenta: QR3-> Yellow.

Concatenate the primary QR patterns to generate RGB color pattern as shown in Fig 4.

Figure 3: Color QR code generations

Figure 4: Color QR code

4. OBFUSCATION STEPS INVOLVED

Design: It is the primary step which creates the net list based on DSP algorithm.

Abstract level transformation: For every individual application based on the performance requirement it is necessary to choose suitable high-level transformation (type1 or type2).

Further the above selected transformations have to apply simultaneously with obfuscation where variation modes and various configurations of the switch instances are designed.

Secure switch design: It is designed based on the variations of high-level transformations. It is to be noted that, different configure data could be mapped into the same mode and it only involves simple combinational logic synthesis.

QR key driven FSM state transition controller: To obfuscating the design functionally using FSM machines ring counters are incorporated which is controlled by hierarchical key matching process. Various configuration modes are used for structural obfuscations simultaneously at this level.

5. EXPERIMENTAL RESULTS

QR code pattern driven abstract level transformations allows designing hierarchical key matching using same data path but different behavioral changes in the circuits. Here data path is implement a 15th-order digital FIR filters. For meaning obfuscation, number of taps is

changes and for non meaningful state arithmetic operations are changes both of these correspond to different modes. Though these outputs which were generated by different modes are functionally incorrect, it appears as correct outputs under different state transitions as per FSM states as shown in Fig.5, since the probabilistic behaviors of design output is meaningful from a designer point of view. The initialization keys are extracted dynamically from input color QR patterns and the configuration known for the circuit is working appropriately as shown in Fig 6.

5.1 Trade off Performance over Confusion Metrics

The obfuscation level is dependent on the number of FSM states used state transitions (Ts), the re- configuration stages after functional transformations (S), and the key sizes used in each stage of hierarchical matching steps. To estimate the obfuscation level against performance measure for two categories of parameters as shown in Table 1 performance metrics are evaluated as shown in Table 2.

Table 1: Obfuscation degree variation modes.

Type 1:	
Key size	8
Obfuscating FSM states	256
Reconfiguration stages	256
Type 2:	
Key size	12
Obfuscating FSM states	4096
Reconfiguration stages	16

Table 2: Trade off analyzes of number states Vs performance report using CYCLONE II FPGA family (EP2C35F672C6).

Obfuscation type	Area(LE's used)	Fmax report
Type 1	513	317.16MHz
Type 2	512	59.66MHz

6. STATE OF THE ART COMPARISON

As this paper is the first attempt to generate color QR pattern to obfuscate any digital circuits with high-abstraction level transformations, it is very tough to compare with the existing methodologies which are using generic keys. Therefore, we have evaluated some key metrics to analyze the performance of proposed technique. However, the use of FSM based level transformations using unique patterns from a security perspective has not been investigated in any of the existing obfuscation techniques.

In addition other techniques only attain protection either structural or functional while our work provides both the protection. The key merits of the proposed methodology is the generation of QR pattern from a meaningful information's from a copyright point of view, such that it is hard to get the desired functionality from any other iterative modes of operations. Other existing method [10] not ensures the moderation from a protection point of view. Finally, In terms of protection and design performance are concerned, the proposed methodology is far superior to all other state-of- the-art comparisons. While the proposed work alters the functionality based on QR key driven FSM state transitions, but existing methods are based on explicit Key modifications [11].

7. CONCLUSION

Here the efficiency of QR patterns for both structural and functional obfuscation of DSP design is proved and its abstract level transformation using FSM machines with state transition controller is also proved. Hardware complexity is considerably reduced as compared to existing reconfigurable structural obfuscation methods. Compared with all other existing methods key handling issues in our proposed methodology is solved with the generation of color QR pattern followed by digital key extraction using pseudo random pattern generation module and gives both high confusion metrics and modular variations in key matching process. Finally we analyze the hardware complexity trade-off between security level retention through FSM states over performance degradation. Here without compromising any performance reduction high level obfuscation methodology is incorporated and its efficiency is proved through FPGA hardware synthesis.

REFERENCES

1. E. Castillo, et al. IPP@HDL: efficient intellectual property protection scheme for IP cores. IEEE Trans. on VLSI, 15(5):578-590, 2007. https://doi.org/10.1109/TVLSI.2007.896914
2. L. Yuan and G. Qu, "Information hiding in finite state machine," in Information Hiding Workshop, 2004, pp. 340–354 https://doi.org/10.1007/978-3-540-30114-1_24
3. B. Gassend, D. Clarke, M. van Dijk, and S. Devadas, "Controlled Physical Random Functions," in ACSAC '02: Proceedings of the 18th Annual Computer Security Applications Conference. Washington, DC, USA: IEEE Computer Society, 2002, p. 149
4. R. S. Chakraborty and S. Bhunia, "Hardware protection and authentication through netlist level obfuscation," in Proc. Int. Conf. Comput.-Aided Design, Nov. 2008, pp. 674–677 https://doi.org/10.1109/ICCAD.2008.4681649
5. R. S. Chakraborty and S. Bhunia, "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, Oct. 2009.

https://doi.org/10.1109/TCAD.2009.2028166

6. Y. Lao and K. K. Parhi, "Protecting DSP circuits through obfuscation," in Proc. IEEE Int. Symp. Circuits Syst., Jun. 2014.
   https://doi.org/10.1109/ISCAS.2014.6865256
7. N. Ferguson and B. Schneier. Practical Cryptography. John Wiley and Sons, 2003.
8. R. S. Chakraborty and S. Bhunia, "Hardware protection and authentication through netlist level obfuscation," in Proc. Int. Conf. Comput.-Aided Design, Nov. 2008, pp. 674–677 .
   https://doi.org/10.1109/ICCAD.2008.4681649
9. W. P. Griffin, A. Raghunathan, and K. Roy, "CLIP: Circuit level IC protection through direct injection of process variations," IEEE Trans. Very Large Scale Integr. (VLSI) Syst., vol. 20, no. 5, pp. 791–803, May 2012.
   https://doi.org/10.1109/TVLSI.2011.2135868
10. D G Sankar Rao, N.M.Ramalingeshwar, D.Vijendra Kumar, Simhadri Kollu," Analysis of static and dynamic CMOS low power high speed NP Domino logic", International Journal of Advanced Trends in Computer Science and Engineering, Volume 7, No.6, November - December 2018
    https://doi.org/10.30534/ijatcse/2018/05762018
11. F. Koushanfar and Y. Alkabani, "Provably secure obfuscation of diverse watermarks for sequential circuits," in Proc. Int. Symp. Hardw.- Oriented Security Trust, Jun. 2010, pp. 42–47.
    https://doi.org/10.1109/HST.2010.5513115
12. R. S. Chakraborty and S. Bhunia, "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, Oct. 2009
    https://doi.org/10.1109/TCAD.2009.2028166