Middle-East Journal of Scientific Research 21 (11): 2108-2114, 2014
ISSN 1990-9233

DOI: 10.5829/idosi.mejsr.2014.21.11.21803

A Novel Technique to Enhance Security of Logic Circuits Using a Modified Programmable Secured Logic Module

[1]Binu K. Mathew[1] and [2]K.P. Zacharia

[1]Research Scholar, Anna University, Tamil Nadu, India
[2]SAINTGITS College of Engineering, Pathamuttom, Kottayam, Kerala, India

Abstract: Field Programmable Gate Arrays (FPGAs) are devices used in many VLSI applications, which are programmable in nature. Researchers had proposed various threat models like bit stream copying, unauthorized usage of FPGA systems etc. The problem of bit-stream copying can be avoided by incorporating cryptographic techniques. This not only increases FPGA system security, but increases complexity and cost of the system. For this reason, use of FPGA is not viable for low cost, less complex systems as cryptographic techniques increases cost and complexity of the system. This paper proposes a new technique which enhances security of digital systems and design of a programmable logic module for secured systems which works on the principle of the new technique. The idea is to load the logic module with a default functionality which is changed at run time. FPGAs consist of an array of Look-Up Tables (LUTs) as the programmable element with a routing network which consumes majority of resources in FPGAs. Multiplexer Input lines forms the control word of the LUT and select inputs of the multiplexer can be used as input lines of the LUT. Width of the control word of a LUT with N inputs is 2N bit and total number of elements in the set of possible control words is 2M where M=2N.

Key words: FPGA · Secured devices · Re-configurable devices · Cryptography · Encryption · Decryption

INTRODUCTION

Field Programmable Gate Arrays or FPGAs consist of Look-Up Tables or LUTs as programmable elements and a programmable routing network which consumes a major portion of the FPGA system. FPGAs play an important role in various domains like financial services, military, medical and other similar applications. These systems are used in different areas like financial and military services are prone to various types of attacks. Researchers had proposed several threat models during the last decade. FPGA based systems are intellectual property of its designer, who has invested lot of time and money for its development. Some of the threat models proposed are bit-stream cloning or copying of FPGA bit-streams, altering or modifying the functionality, unauthorized usage etc. The most commonly found FPGA threat models are copying of the bit-stream and unauthorized usage of FPGA based system. Researchers had proposed several techniques to combat these two threat models. Cryptography is a popular technique to check the problem of bit-stream copying and setting password is a widely used technique to avoid unauthorized usage of FPGA based systems. Even though cryptographic techniques reduce the effort of bit-stream cloning, it increases cost, complexity and area of the system. This paper proposes a technique to enhance the security of a digital system by using a logic module with a default functionality which can be changed by a user at run time by applying a control word. Architecture of the proposed modified programmable secured logic module address both threat models-copying of bit-streams and unauthorized usage of systems by an intruder.

Previous Works: A technique to implement various digital circuits using 3-input LUT is discussed by Mathew and Zacharia in [1, 2]. Architecture of a multi-functional device which increases security of reconfigurable circuits is discussed by the authors in [3]. Architecture of a programmable secured logic module which is run time reconfigurable which can implement functions with five variables is explained in [4]. Researcher had studied about various threat models for FPGA based system like bit-stream copying, Trojan attacks, side channel attacks

Corresponding Author: Binu K. Mathew Research Scholar, Anna University, Tamil Nadu, India.

etc. These FPGA threat models explain the way in which FPGA based systems are affected by the attack. Different security concerns associated with SRAM based volatile FPGA is discussed by S. Drimmer in [5]. Different methods for authentication of bit-streams are explained by the same author in [6], which gives an insight to securing a design of FPGA based system which eliminates the possibility of copying of the bit-streams. In [7], Huffmire *et al*. discuss the security related problems in FPGA based systems for various applications, various possible attacks and solutions to these problems. This also addresses issues like trusted hardware, design theft, physical attacks and system security. Designing of secure system on reconfigurable devices is explained by the authors in [8]. This also suggest a separation technique to make sure that reference monitor is tamper proof and cannot be bypassed. A low cost self protective security mechanism to provide on chip security is discussed and explained in [9]. Anderson *et al*. [10] had proposed different types of cryptographic processors and its applications along with various possible threats like power analysis, logical attack etc. The approach of Digital Rights Management combined with NBTI aging and delay logic is analyzed by the authors Zheng and Potkonjak in [11]. Different evolving pre-fabricated FPGA architecture including asynchronous and nano-technology approaches are discussed by Kuon *et al*. in [12]. In [13], Collins had proposed the architecture of a secured reconfigurable system on programmable chip and implementation of a computer system using SoPC. Design and implementation of a unique chip ID for polymorphic circuit which are reconfigurable in nature is discussed in [14]. Apart from the conventional threat models, [15] had stated new threats for security of integrated circuit and its solution. Architecture of Physically Unclonable Functions (PUF) based on a clock network that can solve security related problems is addressed by in [16]. In [17], the authors had stated various possible threat models that may occur during the IC fabrication process and architecture of a reconfigurable logic barrier which can be used to enhance security of logic devices. A technique to alleviate side channel attack where information leakage depends on a limited number of physical wires is proposed by Ishai *et al*. in [18]. Authors in [19] had proposed different techniques which includes techniques like encapsulation, dongle, manufacturer defined key etc. Several novel reconfigurable physical unclonable functions and their use in secure reconfigurable systems are analyzed and explained by the authors in [20, 21]. Author proposes a secure and strong computing module based on encryption algorithm like AES algorithm which provides data security and protection against malicious attack is proposed in [22].

Proposed System: Major components in FPGAs are LUTs as programmable elements and routing network or interconnection network. Most of resources in a FPGA are used by routing network and only a very small portion of the area is allotted to LUTs which are the programmable elements. This paper proposes a new technique –logic module is loaded with 8-bit binary value called as System Identification Number (SIN), which is stored in a permanent memory like ROM which acts as a control word to implement a three variable function which can be altered by the user at run-time. A user who is authorized to use this logic module can load the Control Word Register (CWR) of the proposed system to implement a function of his choice. The System Identification Number (SIN) can be used to categorize the Programmable Logic Module based on the Manufacturer or application of the proposed system. As length of the SIN is 8-bit, total number of permissible SIN is 2^8=256. A unique SIN can be assigned to each manufacturer and total number of manufacturer who can be licensed to use the proposed logic module is 256. Based on the unique number SIN, system manufacturer can be easily identified. Only an authorized user who knows the manufacturer of the logic module can implement some function using the proposed logic module.

Programmable Secured Logic Module (PSLM): Architecture of a Programmable Secured Logic Module is shown in Figure 1. This architecture proposed by Mathew and Zacharia in [4] is capable of implementing any 5 variable functions. This consists of four 3 input LUTs, an address decoder, six 8-bit register arrays to store the control words, a Bit Flipping Logic (BFL), an output block and three 2 channel multiplexers. In this architecture, by default all registers are loaded with logic ‘0’ and so no functionality is implemented, i.e., when the PSLM is powered on, content of all register locations are logic ‘0’. An authorized user enters the control word of the functionality to be implemented through Data bus in groups of 8-bits. As the register array is filled with logic ‘0’ by default, an intruder cannot copy or change the bit-streams. So this logic module is called as Programmable Secured Logic Module. As number of variables is 5, total number of bits in the control word is 2^5=32 and total number of various possibilities of the control word is $2^{32.}$ As the number of possible is very

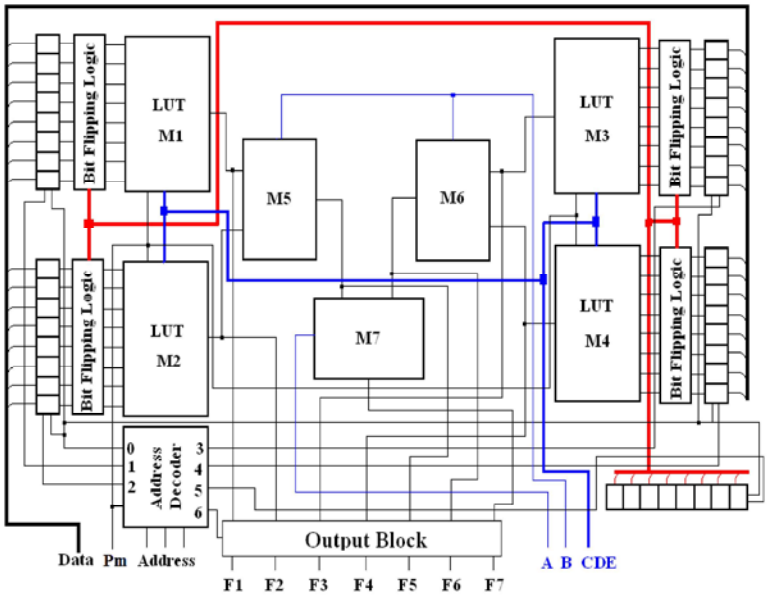

Fig. 1: Block diagram of a 5-variable Programmable Secured Logic Module

large, an intruder cannot find whether he/she had implemented the actual functionality by trial and error method. Architecture of PSLM can be modified so that a 3 variable function implemented on this system even if it is not powered on.

Modified Programmable Secured Logic Module (MPSLM): For PSLM proposed in [4], there is no functionality when it is not powered as all bits of the Control Word Register are set as logic '0'. This architecture is modified to define default functionality for the logic module. The default functionality can be overridden by applying a control word at the data bus of the system. For an intruder this seems like a logic module with a defined functionality and as he/she is not aware of the architecture of the logic module he/she may not be able to override the defined functionality. Even if the intruder is aware of the architecture, as number of bits in the control word is 32, total number of possible functions are 2^{32} five variable functions. An 8-bit ROM is inserted so as to hold the SIN. Output block is used to enable certain outputs and disable remaining outputs of the PSLM. Configuration bits of the output selection block are latched in the Output Enable Latch and number of outputs enabled is based on the contents of the latch. For the proposed system, there are five input variables and seven outputs. These outputs are four 3-variable LUT outputs, two 4-variable LUT outputs and one 5-variable LUT output.

How Proposed Module Is Secure Against Bit Stream Copying?: The security aspects of the proposed system are discussed in the following section. In existing systems, FPGAs which are basically an interconnection of several LUTs, plays a vital role. Functionality or behavior of a LUT depends on its configuration bit-stream or control word. This control word is loaded into memory when a FPGA is programmed, usually by the developer of the FPGA based system. So FPGA bit-stream is not secure and it is prone to various types of attacks like bit-stream copying, unauthorized usage of FPGA based system etc. There are several techniques presently available which not only enhance security of FPGA based system but also enhance the system complexity and cost. Let us consider a combinational circuit with three variables implemented on a 3-input LUT. Length of the control word of the LUT is 2^3=8 and possible number of control words is 2^8=256. The LUT is configured with the intended functionality if and only if the proper control word is loaded into the Control Word Registers. Functionality of the proposed MPSLM is dependent on the control word loaded from the ROM array to input of the Bit Flipping Logic.

All registers in the control word register of the MPSLM is loaded with logic '0' and the SIN memory of the MPSLM is loaded with 8-bit binary number by default. All four 3-input LUT is loaded with same control word and LUTs implements a functionality based on the control word. The intended functionality is injected into the logic module by the user at run time by loading corresponding control word XORed with 8 bit System Identification

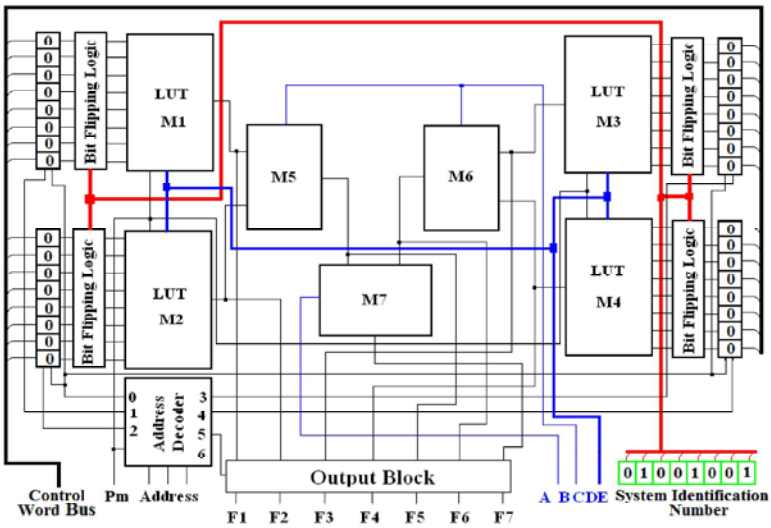

Fig. 2: Block diagram of a 5-variable Modified PSLM (MPSLM) where 'R' indicates a ROM cell.

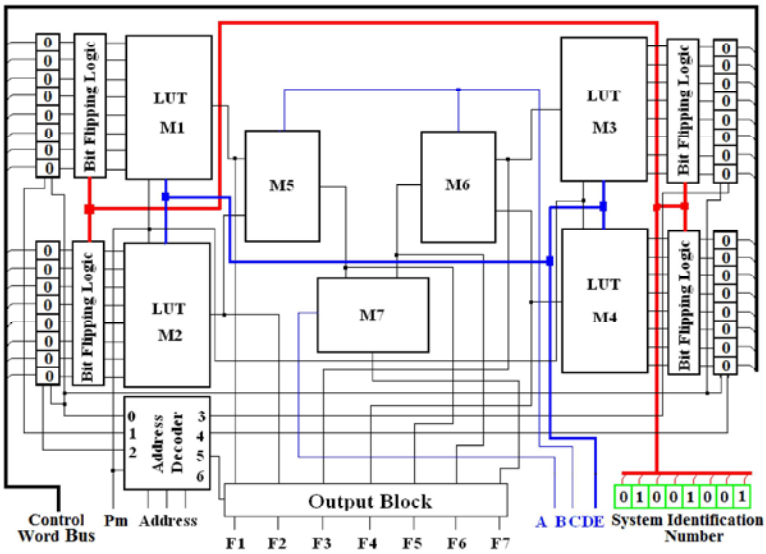

Fig. 3: All bits of the Control Word Register is loaded with logic '0' by default which is changed at runtime by loading appropriate control word

Number. Unlike cryptographic systems where an intruder can correlate present values and past values in the data stream, an intruder can no way find whether he/she had loaded the correct control word into the control word register of the proposed system. Also set of various combinations of control words for a LUT with N input variables is 2^M, where $M=2^N$, for reasonable values of N, is very large, an intruder cannot try all possible combinations to find the actual control word. Even if the intruder tries all control word, one by one, he cannot find whether the system is loaded with a right control word or wrong control word. For the proposed system which is basically a 5 input LUT, total bits in the control word is $2^5=32$ and total number of control words in the set of possible control words is $2^{32}=4294967296$. Probability of selecting a control word from the set of $2^{32}=4294967296$ control words is only 1/4294967296 which is very small.

When the system is initialized, based on the System Identification Number or SIN, the MPSLM is loaded with a functionality, which can be changed by the user at run-time. The SIN stored in on chip ROM memory which is unique for a manufacturer or application, acts as a default control word for the MPSLM. An authorized user who posses the control word of a function to be implemented will load the Control Word Register with this control word to implement a function. If a wrong control word is loaded into the Control Word Register, a wrong functionality is

implemented on the MPSLM. For a 32-bit wide control word, total number of functions that can be implemented is very large and an intruder cannot find whether he/she had loaded MPSLM with actual control word or not. Control word of same function varies for MPSLMs loaded with different System Identification Number. For example, let us consider two MPSLMs, with System Identification Number "00010011" and "10000001". The control word to implement a full adder will be different for these MPSLMs. In other words, control word to implement a function on one MPSLM will implement a different function on another MPSLM. In this way, Modified Programmable Secured Logic Module provides better security compared to Programmable Secured Logic Module, as control word of same function will differ for different MPSLMs as the System Identification Number can be different for different MPSLMs. Thus MPSLM provides more security for logic systems compared to PSLMs.

Experimental Result: The proposed Modified Programmable Secured Logic Module (MPSLM) is implemented in VHDL and the same is synthesized using Xilinx ISE 8.1i. The MPSLM is loaded with different control words and various inputs were applied to check the functionality of the proposed system. The design is implemented on a XILINX SPARTAN 3E FPGA and target device selected was XC3S100E. For the proposed MPLM, there are two modes of operation-program mode and functional mode. When Pm input is logic '1' then the MPSLM is in program mode and when Pm =logic '0' the proposed system is in function mode. During program mode the system can be loaded with various control words to realize various functions. In this state MPSLM will implement a logic function based on the SIN and is ready to be loaded with various control words. Control words are loaded into the various locations in the control word register array in the logic module by placing the address of the register location on the address bus. Output block can be explicitly configured by loading appropriate control word into the OCwR register of the register array. During function mode, the logic module realizes different functions based on the control word stored in the control word registers. MPSLM realizes seven different functions – four 3-variable functions, two 4-variable functions and one 5-variable function. As the logic module behaves on the basis of control word loaded into the control word register, application of a wrong control word results in a functionality which is different from the actual one. Table 1 shows the comparison of device utilization of the proposed system for SPARTAN 3E.

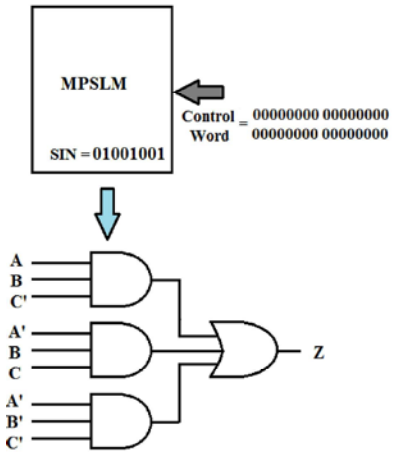

Fig. 4: All bits of the Control Word Register is loaded with logic '0' MPSLM is loaded with the function ABC' + A'BC + A'B'C'

Table 1: Comparison of device utilization details of the proposed chip A, B - Not used, C=P, D=Q, E=R

Standard Function	No. of Slices used	No. of 4 input LUTS used	Reconfigurable
PQ'R	1	1	No
P'QR+P'Q'R	1	1	No
P'QR+PQ'R'	1	1	No
P'Q+QR'	1	1	No
PQ'+P'QR	1	1	No
P'QR+PQR'+P'Q'R'	1	1	No
P'Q+QR+PQ'R'	1	1	No
PQR+P'Q'R'+P'QR	1	1	No
Proposed System	40	58	Yes

Figure 4 shows the proposed MPSLM with a System Identification Number "01001001" and system is loaded with logic function Z=ABC' + A'BC + A'B'C' and default control word of the proposed system is "00000000 00000000 00000000 00000000". To implement a 3 variable function on the MPSLM, the first three bytes of the control word must be logic '0' and last byte of the control word must be replaced with appropriate value, based on the logic function to be implemented. If the System Identification Number is "00101000" then default function implemented on the PSLM is Z = AB'C + A'BC. As the System Identification Number is 8-bit wide, 256 different functions can be implemented on a PSLM. This means that, if allotment of System Identification Number is done on manufacturer basis, 256 different manufacturers can be assigned with System Identification Number which is a reasonable number. In future, if required the width of the System Identification Number can be increased to accommodate more manufacturers if required.

CONCLUSION

This paper proposes a Modified Programmable Secured Logic Module (MPSLM) which enhances security of digital systems without using bit-stream encryption. Conventional FPGA based systems which use cryptographic techniques to avoid bit-stream copying and other similar attacks, are not run time re-configurable. This new technique not only makes a system runtime reconfigurable, but also enhances the system security. Bit stream encryption is mainly employed to avoid copying of bit streams when they are loaded into the FPGAs. In the proposed system, as the design is partially or fully incomplete, the intruder should load the MPSLM with proper control word before proceeding further. By default, the MPSLM module is loaded with a System Identification Number and functionality of the proposed system is based on the SIN. An authorized user, by loading appropriate control word can program the proposed system with intended functionality and so this system is more secure compared to other FPGA based systems..

The advantages of Modified Programmable Secured Logic Module can be summarized as:

- Provides security against bit-stream copying and less complex compared to systems with bit stream encryption.
- Run time reconfigurable by loading the system with a new control word.
- Behaviour of the proposed system can be changed very easily by changing the control word – this feature can be used for digital rights management.

The proposed architecture with five inputs or variables can be extended to have more variables, so that a small digital system can be fully developed using the modified version of the proposed architecture. This can be used as a run time partially reconfigurable logic module which can be used for DSP applications.

REFERENCES

1. Mathew Binu, K. and Dr. K.P Zacharia, 2012. New techniques to enhance FPGA based system security, International Journal of Advanced Research in Computer Engineering & Technology, 1(5): 533-543.
2. Binu K. Mathew and Dr. K.P Zacharia, 2012. New Logic Module for secured FPGA based system, International Journal of Electronics and Communication Engineering, 1(5): 91-94.
3. Binu K. Mathew and Dr. K.P. Zacharia, 2014. Novel technique to enhance security of reconfigurable circuits, Journal of Theoretical and Applied Information Theory, In Press.
4. Binu K. Mathew and Dr. K.P. Zacharia, 2014. Architecture of a multi-Functional programmable secured logic module, Australian Journal of Basic and Applied Science, in press.
5. Drimer, S., 2008. Volatile FPGA design security – a survey, Computer Lab, University of Cambridge.
6. Drimer, S., 2007. Authentication of FPGA bit-streams: why and how. In Applied Reconfigurable Computing, volume 4419 of LNCS, 73-84.
7. Huffmire, T., S. Prasad, T. Sherwood and R. Kastner, 2008. Threats and Challenges in reconfigurable hardware security.
8. Huffmire, T., S. Prasad, T. Sherwood and R. Kastner, 2008. Designing Secure Systems on reconfigurable Hardware.
9. Huffmire, T., S. Prasad, T. Sherwood and R. Kastner, 2008. Managing Security in FPGA-based embedded systems,
10. Anderson, R.J., M. Bond, J. Clulow and S.P. Skorobogatov, 2005. Cryptographic processors -a survey. Technical Report 641, University of Cambridge, Computer Laboratory.
11. Zheng, J.X. and M. Potkonjak, 2012. Securing netlist level FPGA design through exploiting process variation and degradation, www.dl.acm.org/ citation.cfm?id=2145716
12. Kuon, I., R. Tessier and J. Rose, 2007. FPGA Architecture: Survey and Challenges, Foundations and Trends in Electronics Design Automation, 2: 135-253.
13. Collins, W.H., 2013. A Secure Reconfigurable System-On-Programmable Chip Computer system, M.S. Thesis, Graduate School, University of Tennessee.
14. Sekanina, L., R. Ruzicka, Z. Vasicek, V. Simek and P. Hanacek, 2013. Implementing a unique chip ID on a Reconfigurable Polymorphic Circuit, Information Technology and Control, 42: 1.
15. Abramovici, M. and P. Bradley, 2009. Integrated Circuit Security - New Threats and Solutions, http://www.cisr.ornl.gov/csiirw/09/CSIIRW09-Proceedings/Abstracts/Abramovici-abstract.pdf

16. Muthumeenakshi, N. and R. Rajaprabha, 2014. Low cost Physical Unclonable Function using secured clock network, *IJIRCCE*, Special, 1: 2.
17. Baumgarten, A.C., 2009. Preventing integrated circuit piracy using reconfigurable logic barriers, M.S. Thesis, Graduate School of Computer Science, Iowa State University.
18. Ishai, Y., A. Sahai and D. Wagner, 2004. Private Circuits: Securing Hardware against Probing Attacks, http://www.cs.berkeley.edu/~daw/papers/privcirc-crypto03.pdf
19. Valette, N., L. Torres, G. Sassatelli and F. Bancel, 2006. Securing embedded programmable gate arrays in secure circuits, http:// www.cecs.uci.edu/ ~papers/ ipdps06/ pdfs/74-RAW-paper-1.pdf
20. Lao, Y. and K. Parhi, 2011. Novel Reconfigurable Silicon Physical Unclonable Functions, https:// www.truststc.org/ conferences/ 11/ CPSWeek/ papers/ FDSCPS-11_4.pdf.
21. Maes, R., P. Tuyls and I. Verbauwhede, 2008. Intrinsic PUFs from flip-flops on reconfigurable devices, https:// www.cosic.esat.kuleuven.be/ publications/ article-1173.pdf
22. Chaves, R., 2007. Secure computing on reconfigurable systems, PhD Thesis, Technical University of Lisbon, Lisbon.