Middle-East Journal of Scientific Research 22 (8): 1165-1175, 2014
ISSN 1990-9233
© IDOSI Publications, 2014
DOI: 10.5829/idosi.mejsr.2014.22.08.21987

Securing Logic Circuits Using Run-Time Programmable Interconnection Network

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

[1]Research Scholar, Anna University, Chennai, Tamil Nadu, India
[2]Electronics & Communication, SAINTGITS College of Engineering, Kottayam, Kerala, India

Abstract: Security of digital hardware against various possible attacks is a major issue in today's world. Various researchers all over the world had proposed several FPGA threat models and proposed several solutions and methodologies to fight against these threat models. Cryptographic techniques are commonly used to keep digital systems secure and robust against various types of attacks. Cryptography increases system security as well as complexity and cost of the system as well. This paper proposes a new system without using cryptography to secure digital systems against possible threat models by using 8 input 8 output Secured Programmable Interconnection Network (SPIN8X8). This network defines an interconnection pattern between two logic blocks in a digital system and the interconnection pattern is based on the interconnection pattern code applied by the user at run-time. Finally a SPIN array is explained which is based on SPIN8X8 network, which can be used to interconnect different blocks of a system.

Key words: Interconnection Network · Programmable Interconnection · Secured Devices · Programmable Circuits · SPIN

INTRODUCTION

Digital devices and circuits particularly systems based on FPGA are prone to various types of attacks as estimated by various researchers from different parts of the world. Among these, most widely found threat models are bit-stream cloning, altering the FPGA bit-stream and unauthorized usage of the FPGA based system. Researchers had proposed various cryptographic techniques to fight against these FPGA threat models. These techniques increase system security as well as cost and complexity of the system. Due to this reason, cryptographic techniques are not preferred for low cost, less complex digital systems. Cryptography based systems also increases cost as well as size of the digital system. This paper proposes a new technique to enhance security of a logic system by simply dividing the circuits into two sub-circuits and connect these circuits using a Secured Programmable Interconnection Network (SPIN). For the proposed system, as there are 8 inputs and 8 outputs this circuit is called as SPIN8X8. An array of the proposed circuits, called as SPIN array, can be used to increase the degree of security of a system. The interconnection pattern for two blocks defined by the SPIN is dependant on the interconnection pattern code (IPC) of that SPIN. Two blocks are connected using the SPIN network in the proper manner, if and only if proposer IPC is applied to the SPIN. In other words, for each interconnection code defined, blocks are interconnected in a particular pattern which is defined by the SPIN designer.

Present day digital systems rely on cryptographic systems to protect the bit-steams of the FPGA from various types of attacks proposed by various researchers. These are not suitable for small less complex systems, as more resources will be used by the cryptographic blocks and fewer blocks will be used by the actual logic system. Even with cryptography, logic systems with less number of inputs are not secure, as a modern computer can find the relationship between outputs and inputs of the system. For an intruder it is not so difficult to develop the bit-steam with the aid of a computer with good configuration. A Secured Programmable Interconnection Network (SPIN) can be used to secure different logic circuits by not defining an interconnection between different parts of the digital system. A trespasser who is trying to trespass into the system will enter various interconnection

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

patterns and the proposed system provides an interconnection between various blocks for each pattern applied. Even by trial and error method, an intruder cannot find the actual interconnection as for every pattern code applied, there is an interconnection pattern defined for the SPIN network.

Rest of the paper is organized as follows; literature survey is discussed in Section 2. Architecture of 8-input, 8-output programmable interconnection network (SPIN8X8) and a SPIN array for secured logic circuits is explained in Section 3. A motivational example using proposed system is explained in section 4 and Section 5 explains how this system enhances security of a system. Section 6 discusses experimental results of the proposed system and conclusive remarks and future work is explained in Section 7.

Literature Survey: The evolution of secured devices had started long back since the evolution of re-programmable devices like FPGAs. Researchers had proposed several techniques to protect the design of a digital circuit from intruders. Mathew and Zacharia [1] in their studies had proposed an interconnection network which adapts the input-output relationship based on the keyword applied to the interconnection network. Integrated circuits are susceptible to different types of attacks including Side Channel Attacks (SCA). A study conducted by Tiri and Verbauwhede in [2] proposes an efficient method to diminish the problem of SCA in integrated circuits. Authors in [3] had proposed a new logic family which is resistant to Differential Power Analysis (DPA) attack. W. H. Collins [4] had proposed in his studies a new architecture of a System on a Programmable chip which provides a secured computing environment which can be re-configured by the user. In [5], Zahur and Evans had projected a technique to improve effectiveness of security and privacy tools. Moats and drawbridges had been proposed by Huffmire[6] et al. to enhance security of reconfigurable hardware. Authors of [7] had proposed a solution to detect malicious logic in hardware designs before fabrication. If any undesirable logic is detected, then the design can be fixed before it is sent to the end-user. Authors of [8] in their work had explained new threats to security of integrated circuits including Trojan attack and denial of service attack and its possible solution. Goertzel and Hamilton [9] had proposed hardware assurance counter measures to guard the integrated circuit from various threat models. Author of [10], had reported that use of reconfigurable logic barrier can enhance the security of integrated circuits making it robust against different types of attacks. A barrier is introduced between input lines and various blocks of the logic circuit when a wrong key is applied. Ishai *et al.* [11] had reported that even cryptosystems are prone to side channel attacks (SCA) and proposed that incorporating private circuits will enhance security of logic circuits against side channel attacks. Authors of [12] had reported a fast and secure chaos based encryption system using digital logic system which is much more efficient and superior than the existing system. In his work, Chaves [13] had reported that use of a secure computing module will enhance the security of conventional cryptographic systems by 5 times. In [14] Jensen *et al.* had proposed a secure reconfigurable computing architecture for multi-user environment. A survey of possible approaches for implementing reconfigurable gate arrays into secure circuits is discussed by its authors in [15]. Zheng and Potkonjak in [16] had proposed a technique to secure net-list level FPGA design through process variation and degradation. Rajendran et al[17]. had proposed a new technique called camouflaging that can be used to increase security of integrated circuits, which prevents reverse engineering of integrated circuit design. In [18], researchers had reported a new approach to build hardware framework which is resistant to side channel attacks. Studies conducted by authors in [19] stated about the risk of hardware attack on FPGA based systems and proposed architecture of a controller which is self reconfigurable which works on partial reconfiguration technique. Studies conducted by Hu *et al.* in [20] had reported that the usage of information flow tracking called Gate Level Information Flow Tracking (GLIFT) can be used as an effective tool to check flow of information through unreliable channels.

Architecture of the Proposed System: This paper proposes architecture of 8 input 8 output secured programmable interconnection network (SPIN8X8) which can be used to enhance system security against various attacks like bit-stream cloning, unauthorized use of logic systems etc. The principle of operation of the proposed system is to interconnect two blocks of a system using proposed SPIN8X8 network with an undefined interconnection pattern by default. A user will define the interconnection pattern at run-time by entering the interconnection pattern code (IPC) so that blocks of the logic system connected to the SPIN8X8 is inter-connected based on the interconnection pattern code entered.

Table 1: Truth Table of the Proposed 8 Input 8Output SPIN (SPIN8X8) with A, B, C, D, E, F, G and H as the inputs

Sr. No	Interconnection Code	Output Pattern (P Q R S T U V W)	Sr. No	Interconnection Code	Output Pattern (P Q R S T U V W)
1	0 0 0 0 0 0	0 0 0 0 0 0 0 0	21	0 1 0 1 0 0	D E F G H A B C
2	0 0 0 0 0 1	A B C E D F H G	22	0 1 0 1 0 1	E F G H A B C D
3	0 0 0 0 1 0	E H F G A B C D	23	0 1 0 1 1 0	F G H A B C D E
4	0 0 0 0 1 1	C D A B G H E F	24	0 1 0 1 1 1	G H A B C D E F
5	0 0 0 1 0 0	F G E H C D A B	25	0 1 1 0 0 0	A C B D E F G H
6	0 0 0 1 0 1	B C A D F G E H	26	0 1 1 0 0 1	C D A B G H E F
7	0 0 0 1 1 0	A D B C E H F G	27	0 1 1 0 1 0	D E B C H A F G
8	0 0 0 1 1 1	F G E H B C A D	28	0 1 1 0 1 1	E F C D A B G H
9	0 0 1 0 0 0	E H F G A D B C	29	0 1 1 1 0 0	F G D E B C H A
10	0 0 1 0 0 1	A B C D E F G H	30	0 1 1 1 0 1	G H E F C D A B
11	0 0 1 0 1 0	C D A B G H E F	31	0 1 1 1 1 0	H A F G D E B C
12	0 0 1 0 1 1	E F G H A B C D	32	0 1 1 1 1 1	A B G H E F C D
13	0 0 1 1 0 0	G H E F C D A B	33	1 0 0 0 0 0	B A C D F E G H
14	0 0 1 1 0 1	B D A C E G F H	34	1 0 0 0 0 1	C A B D E F G H
15	0 0 1 1 1 0	E G F H B D A C	35	1 0 0 0 1 0	D A B C E F G H
16	0 0 1 1 1 1	A C B D F H E G	36	1 0 0 0 1 1	E F G H A D B C
17	0 1 0 0 0 0	F H E G A C B D	37	1 0 0 1 0 0	F G H E A B C D
18	0 1 0 0 0 1	A B C D E F H G	38	1 0 0 1 0 1	G H E F A B C D
19	0 1 0 0 1 0	B C D E F G H A	39	1 0 0 1 1 0	H A B C D E F G
20	0 1 0 0 1 1	C D E F G H A B	40	1 0 0 1 1 1	A D B C E F G H

An intruder will try various interconnection patterns by entering different interconnection pattern codes, but probability of entering correct code is only 1/N where 'N' is the total number of possible interconnection patterns defined for an interconnection network.

Truth table of the proposed 8 input 8 output Secured Programmable Interconnection Network (SPIN8X8) is shown in Table 1 which is not complete due to space limitation. There are more than 200 possible interconnection patterns from "ABCDEFGH" to "HGFEDCBA", but it is limited to 2^N where 'N' is the width of the IPC bus. In the proposed system, N is selected as 6, total number of possible output combinations is 2^6=64, which means that eight input lines can be shuffled in 64 different ways and Table 1 shows only 40 combinations out of 64 possible combinations. An attacker who is trying all possible combinations of the IPCs, probability of applying the correct code is 1/N, where N=64 for the proposed system. Green coloured cell in Table1 shows the correct interconnection pattern with binary value "001001".

The proposed technique can be used to secure a logic circuit, by dividing the digital circuit to be secured into two parts and interconnect these two using the proposed system. An intruder who is trying to use the logic system has to apply correct IPC to interconnect these blocks to form the original circuit. An intruder cannot find whether he/she had applied the correct interconnection pattern code to connect the two blocks to reconstruct the original circuit. The level of security can be enhanced by increasing the number of bits in the IPC bus of the proposed system. For example, if the number of bits in the IPC is selected as 8, total number of possible interconnections between inputs and outputs becomes 2^8 = 256, which makes the system more resistant against any type of attack.

et us consider a simple logic circuit with sixteen different logic blocks as shown in Fig. 1. Let functionality of these logic blocks are defined as F1 to F8 acting as input blocks for blocks F9 to F16 with output of F1 connected to F14, output of F2 is connected to F10 etc. as shown in Fig. 1. An intruder or trespasser can use the logic system at any time as the system is not secured against various FPGA threat models proposed by various researchers, like copying the bit-stream, modification of bit-stream, unauthorized usage of FPGA bit-stream etc. Let us enhance the security of the above logic system by modifying the design by incorporating 8 input 8 output Secured Programmable Interconnection Network (SPIN8X8). The system under consideration is divided into two parts and they are interconnected using the proposed network. The modified diagram is shown in Fig. 2.

By incorporating a SPIN network between various blocks of the logic circuit, its security can be enhanced as shown in the above figure. The blocks are randomly arranged and input ports of the SPIN8X8 network is defined as 'A', 'B', 'C', 'D', 'E', 'F', 'G' and 'H' while output ports are defined as 'P', 'Q', 'R', 'S', 'T', 'U', 'V' and 'W'. The truth table of SPIN8X8 is shown in Table 1.

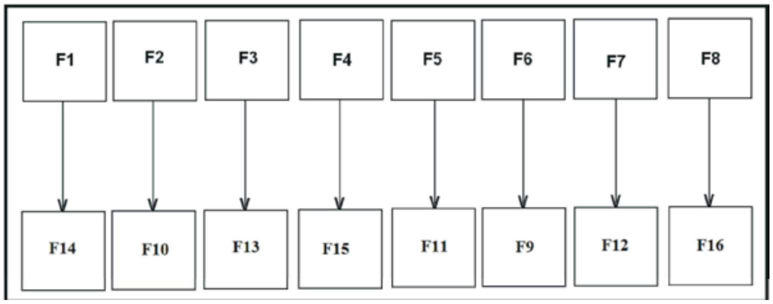


Fig. 1: A logic circuit with 16 blocks with one-to-one interconnection

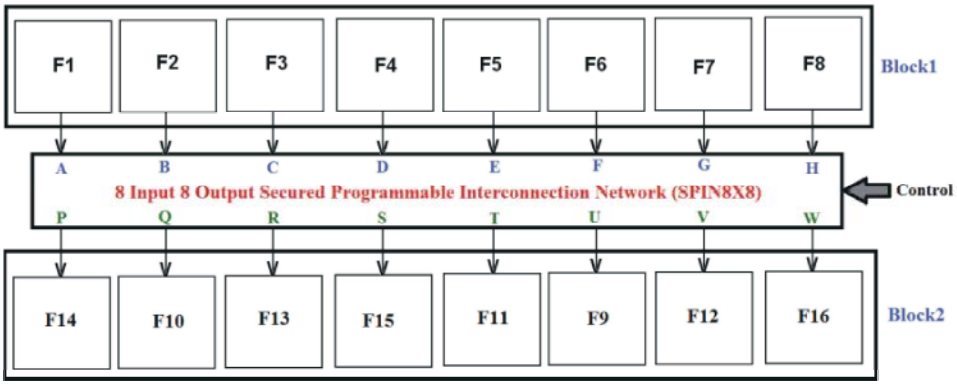


Fig. 2: Logic circuit divided into two blocks with 8 pair of logic blocks interconnected through the proposed SPIN network

The relationship between inputs and outputs of the SPIN network depends on the interconnection pattern code or "Control" input as shown in Fig. 2. When binary value of the "Control" input is set as "0000000", all output of the SPIN8X8 becomes logic '0', irrespective of the logic values at A, B, C, D, E, F, G and H inputs of the SPIN8X8 network. This is highlighted in Table 1 in Red colour. A user must apply a binary value other than "000000" as the interconnection pattern code to establish connection between various inputs and outputs of the proposed system.

When binary value at the "Control" input is "001001", then P = A, Q = B, R = C, S = D, T = E, U = F, V = G and W = H. In Table 1, this output combination is shown in green colour. This means that, when interconnection pattern code or "Control" input is "001001", output of F1 is connected to input of F14, output of F2 is connected to input of F10, output of block F3 is connected to input of F13 and so on as shown in Fig. 1. When Control value is changed to "0111111", output of t he SPIN8X8 network is P = A, Q = B, R=G, S = H, T = E, U= F, V= C and W = D. This is shown in Table 1 in blue colour. This means that output of block F1 is applied to input of block F14 through SPIN network, output of block F2 is F10, output of F7 is connected to F13 and so on. In this way relationship between input and output can be varied by varying the logic value at the "Control" input of the SPIN8X8 network.

Let us consider a scenario when an intruder trying to use the logic system which should be secure against unauthorized usage. The intruder is not aware of the control word to implement a particular function. The intruder will try various values randomly. Let the binary value at the "Control" be "011011". The SPIN network connects A (output of block F1) to T (input of block F11), B (output of block F2) is connected to U (input of block F9), C (output of block F3) is connected to R (input of block F13), D (output of block F4) is connected to S (input of block F15), E (output of F5) is connected to P(input of F14), F is connected to Q, G is connected to V and H is connected to W. Fig. 3 shows the diagram of various blocks of a system interconnected using SPIN8X8 network with "Control" set as "011011". The resulting logic function being implemented is shown in Fig. 4. It can be seen that logic values at the output of F1, F2, F5 and F6 are routed to wrong logic blocks on the other side of the SPIN, output of F1 to input of F11, output of F2 to input of F9, output of F5 to input of F14 and output of F6 to input of F10. In the actual logic diagram various blocks are connected as shown in Fig. 1.

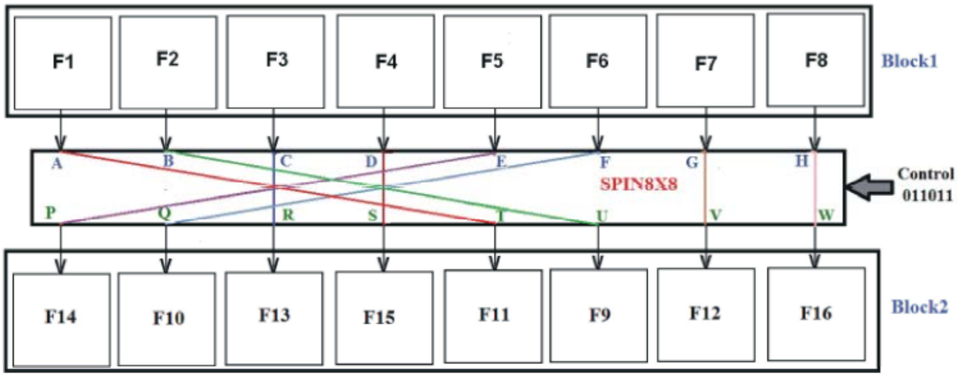


Fig. 3: Control input of SPIN4X4 network is set as “01101”

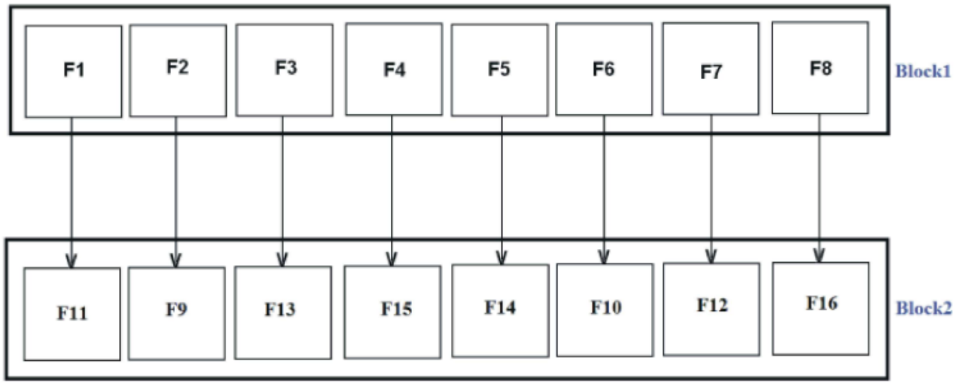


Fig. 4: Actual functionality being implemented when “Control” = “011011”

Motivational Example: Let us consider a motivational example to explain the working of proposed system. For explanation point of view, let us consider a 4 bit ALU, a benchmark circuit to explain “How the proposed system does enhance security against various threat models of a logic system? Fig. 5 shows the diagram of a 4bit ALU. This circuit is not secured against any of the threat models like copying the bit streams, modifying the bit-stream, unauthorized usage of the logic system etc.

An intruder can easily intrude into the system by applying a set of logic values. The above circuit is not at all secure against any of the threat models and is vulnerable to any type of attack by an intruder. Level or degree of security of the circuit shown above can be enhanced by including 8 Input 8 Output Secured Programmable Interconnection Network (SPIN8X8). Even though the proposed system does not prevent modification of bit-stream of the design, it is robust enough to prevent two commonly found threat models – Bit-stream cloning and unauthorized usage of FPGA based system. The proposed SPIN network acts as an interconnection network between various logic blocks. Secured version of the 4 bit ALU after incorporating 8 input 8output SPIN network is shown in Fig. 6.

The interconnections between 8 inputs and 8outputs purely depends only on the binary value at the IPC input of the system and Table1 shows an incomplete truth table of the SPIN8X8 network which defines the relationship between 8 inputs and 8 outputs for various values of IPC. Relationship between inputs and outputs can be varied by varying the binary value of IPC as shown in Table 1. Number of possible interconnections between inputs and outputs of the SPIN8X8 network depends on width of the IPC input of the SPIN8X8 network. In the proposed SPIN8X8 network, width of the IPC is 6 and total number of interconnections defined for the proposed system is 64 and probability of applying an interconnection pattern is only 1/64. In general, probability of selecting an interconnection pattern is $1/2^N$, where N is the width of the IPC bus. The degree of security provided by the SPIN network can be enhanced by increasing the width of IPC bus. If width of IPC bus is increased by one bit, total number of possible interconnections gets doubled and thus probability of occurrence of an interconnection pattern by trial and error method can be halved. For example, when IPC width is increased from 6 to 7, total number of possible interconnections becomes 128 and probability of application of an IPC becomes 1/128.

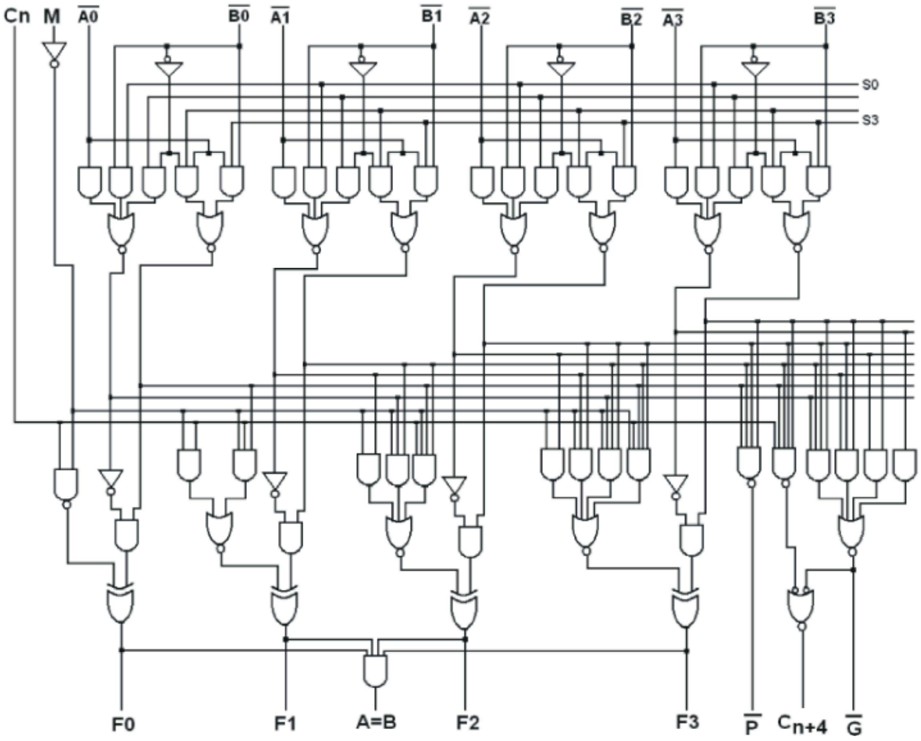


Fig. 5: Unsecured implementation of a 4 bit ALU considered in the example

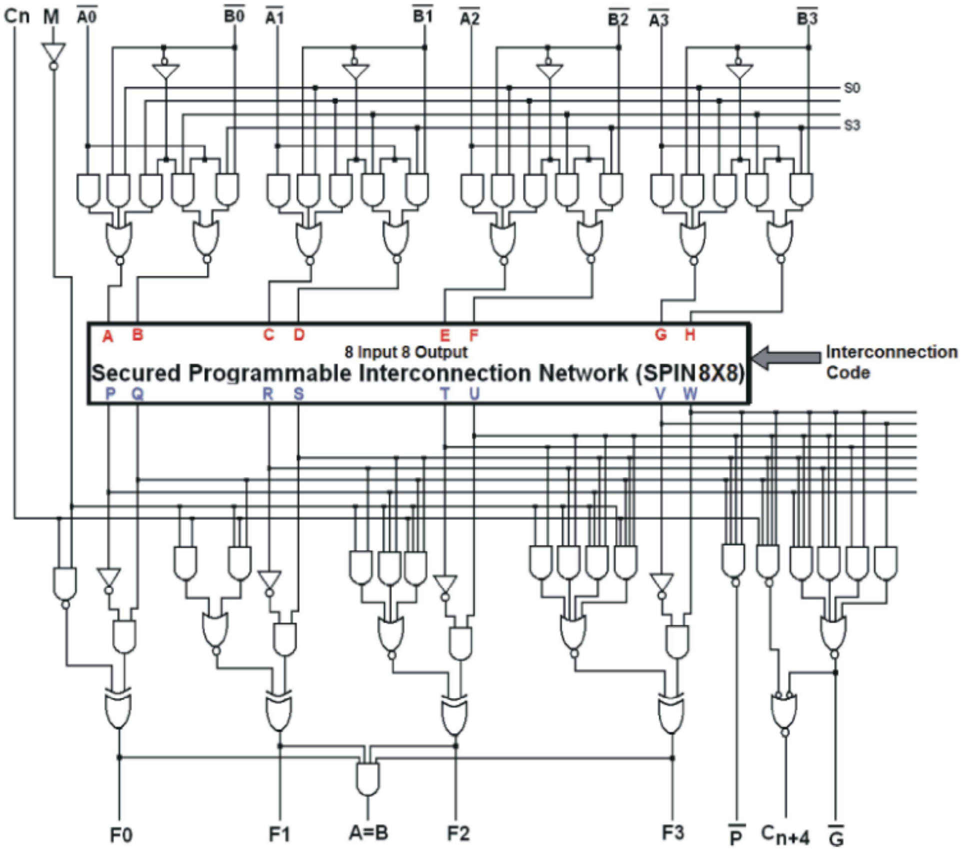


Fig. 6: Security of a 4 Bit ALU can be enhanced by incorporating a SPIN8X8 network

Fig. 6 shows diagram of a modified 4 bit ALU secured by incorporating 8 input 8 output Secured Programmable Interconnection Network (SPIN8X8). Eight inputs of the SPIN network is defined as A, B, C, D, E, F, G and H, while eight outputs are defined as P, Q, R, S, T, U, V and W. Interconnection between these 8 inputs and 8 outputs of the proposed system depends on the Interconnection pattern Code (IPC) or simply interconnection code. As the width of the IPC bus is 6 bit, total number of possible interconnections between input and output bus are 2^6=64. As mentioned previously, Table 1 shows relationship between input bus and output bus of a SPIN8X8 network which is incomplete and can be expanded up to 64 different input-output relations.

Let us discuss the scenario when an unauthorized person tries to intrude into the system by applying a random interconnection pattern code to the SPIN8X8 network. Let the binary value at the IPC input is set as "00111". When interconnection code is set as "001111", the interconnection pattern of the SPIN8X8 network becomes, P = A, Q = C, R = B, S = D, T = F, U = H, V = E and W = G. When interconnection pattern code is "001111" signals at the input side of the SPIN8X8 network is routed to wrong logic gates at the output side of the SPIN8X8 network. Similar is the case when any binary value other than "001001" is applied. If IPC is selected as "011111" then the interconnection pattern selected by the SPIN8X8 network is ABGHEFCD, i.e.; P = A, Q = B, R = G, S = H, T = E, U = F, V = C and W = D. For any IPC other than "001001", outputs of logic gates at the input side of the SPIN network is routed to input of wrong logic gates and the circuit realized is different from the actual one shown in Fig. 5, producing wrong outputs for various input combinations when compared to actual 4 bit ALU.

An authentic user will select "001001" as the interconnection pattern code, for which output of the SPIN8X8 network will be P = A, Q = B, R = C, S = D, T = E, U = F, V = G and W = H. For this IPC output of logic blocks in the input side of the SPIN8X8 network is routed to input of actual/right logic gates in the output side of the SPIN8X8 network and thus realizing the actual logic circuit as shown in Fig. 5 realizing the truth table of a 4 bit ALU. In short operation of the circuit shown in Fig. 6 can be briefed as a logic circuit which realizes a 4 bit ALU when interconnection pattern code is "001001" and a circuit which behaves in a different manner when IPC is different from "001001". Thus by incorporating the proposed SPIN network with 8 inputs and 8 outputs, security of the logic circuits can be enhanced. Fig. 7(a) and Fig. 7(b) shows the behavior of the 4 bit ALU when IPC is "001111" and "001001" respectively.

A logic system with several numbers of 8-bit buses can be made secure by using a system which is the extension of proposed system, which consists of an array of SPIN network called SPIN array. SPIN array consists of an array of SPIN network, a 6-bit D latch for each SPIN network and an N:2^N decoder to generate latch enable signals for the latches connected to each SPIN network. The D latch connected to each SPIN network is used to hold the interconnection pattern code for that SPIN network and as mentioned earlier, interconnection between input and output buses of the SPIN network depends on the interconnection pattern code. Decoder with 2 inputs and 4 outputs generate latch enable (LE) signals for the D flip-flop array as latch. Fig. 8 shows the block diagram of a SPIN array with four SPIN networks.

Fig. 8 shows the block diagram of a SPIN array with four 8bit-buses and four 8bit output buses which consists of four SPIN8X8, four 6-bit D latches to hold the interconnection pattern code for each SPIN8X8 network and a 2:4 address decoder which generates LE signals for the four 6-bit D latches. The input and output lines of the SPIN8X8 network are denoted as "I_Bus" and "O_Bus" respectively. To re-order the input lines of a SPIN8X8 network, first step is to assert the "Ed" input of the SPIN array as logic '1' to enable the decoder which generates LE signal. The interconnection pattern code for a SPIN8X8 network is placed on the "IPC" input and address of the corresponding SPIN network is placed on the address lines A1 and A0. Based on the binary values at the address lines A1 and A0, one of the four outputs of the address decoder changes which latches the interconnection pattern code into the D-latch, defining a relationship between I_Bus and O_Bus of the SPIN network connected to that D-latch. Interconnection-pattern code is placed on IPC input of the SPIN array and decoder is enabled by asserting "Ed" signal as logic '1'. The decoder input is set as A1=A0=logic '0'which set the latch enable signal of D-latch D0 connected to first SPIN8X8 marked as S0, loading the interconnection pattern code placed at IPC into that D-latch which defines interconnection pattern between I_Bus0 and O_Bus0. Let the required interconnection pattern for first SPIN8X8 is I_Bus0(0) = O_Bus0(0), I_bus0(1) = O_Bus0(1), ……I_Bus0(7) = O_Bus0(7), the binary value required to be placed on IPC bus is "001001". The interconnection pattern code is placed on the IPC bus and logic values at Ed, A1 and A0 are asserted as logic'1', logic'0' and logic'0' respectively. Latch enable signal LE signal of D latch D0 goes high, latching the contents placed on IPC bus.

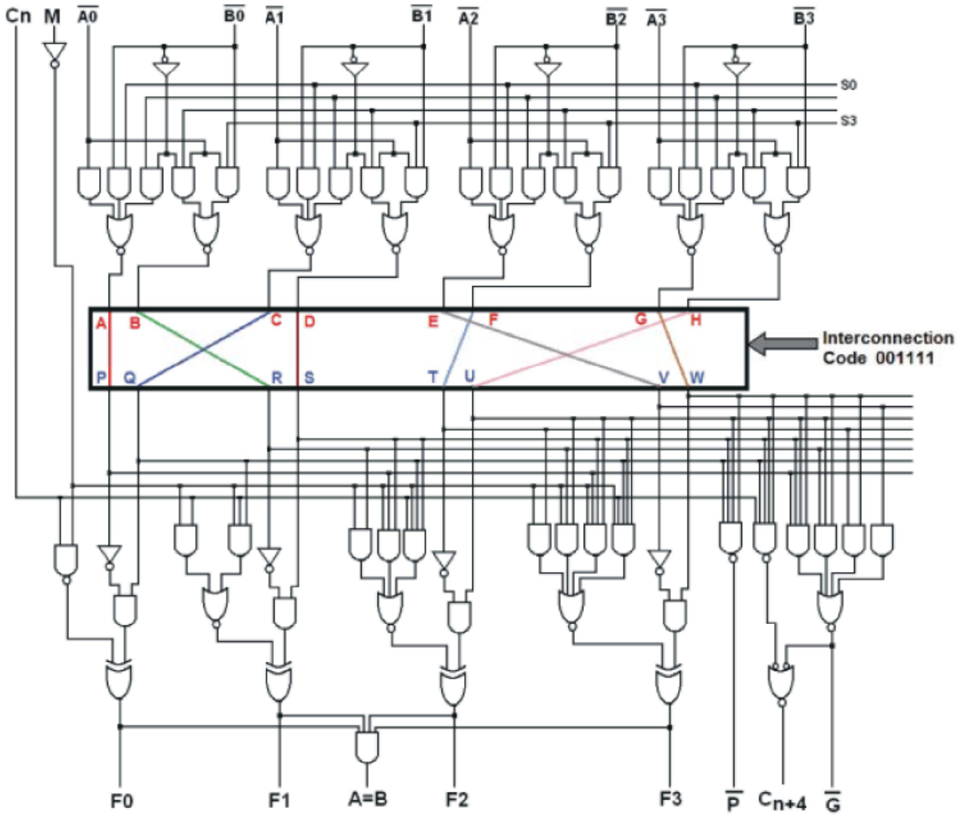


Fig. 7(a): 4bit ALU with SPIN8X8 network with IPC set as “001111”

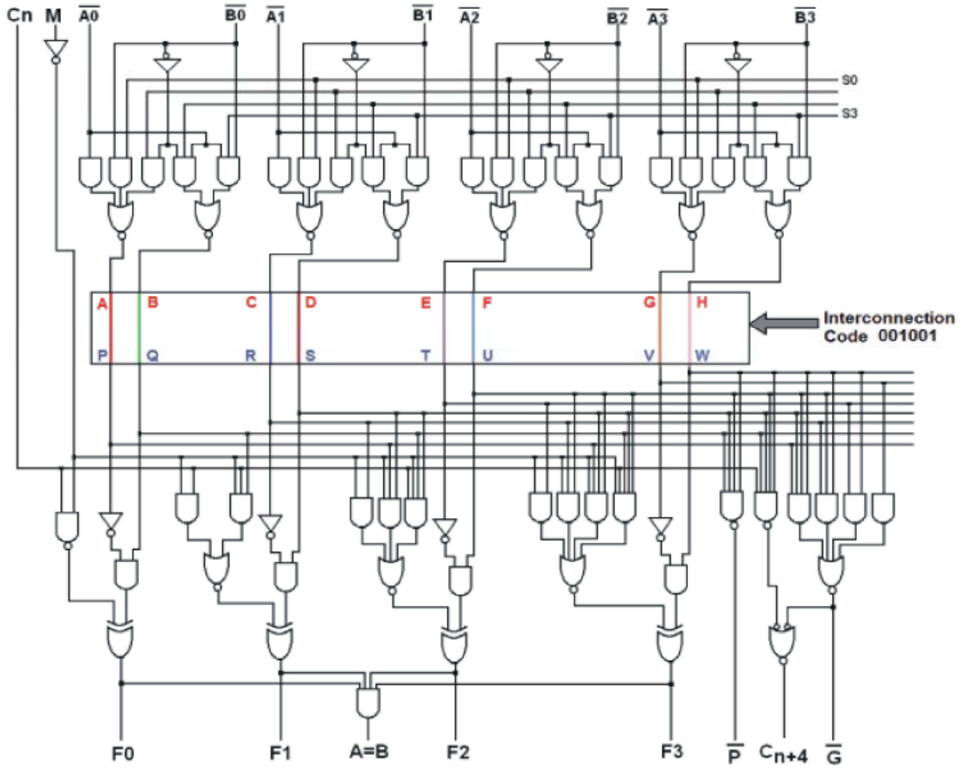


Fig. 7(b): 4bit ALU with SPIN8X8 network with IPC set as “001001”

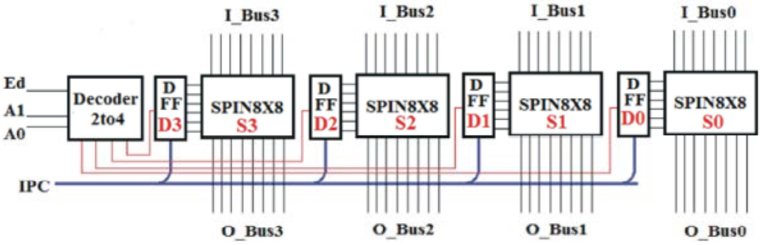


Fig. 8: Block diagram of a SPIN array which consists of four SPIN networks which can re-order four 8 bit buses

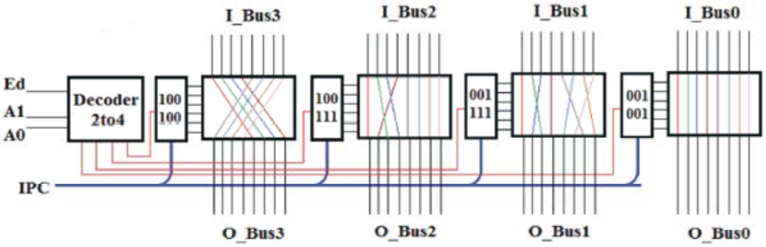


Fig. 9: SPIN array loaded with four different IPC which defines four different interconnection patterns for four SPIN8X8 networks

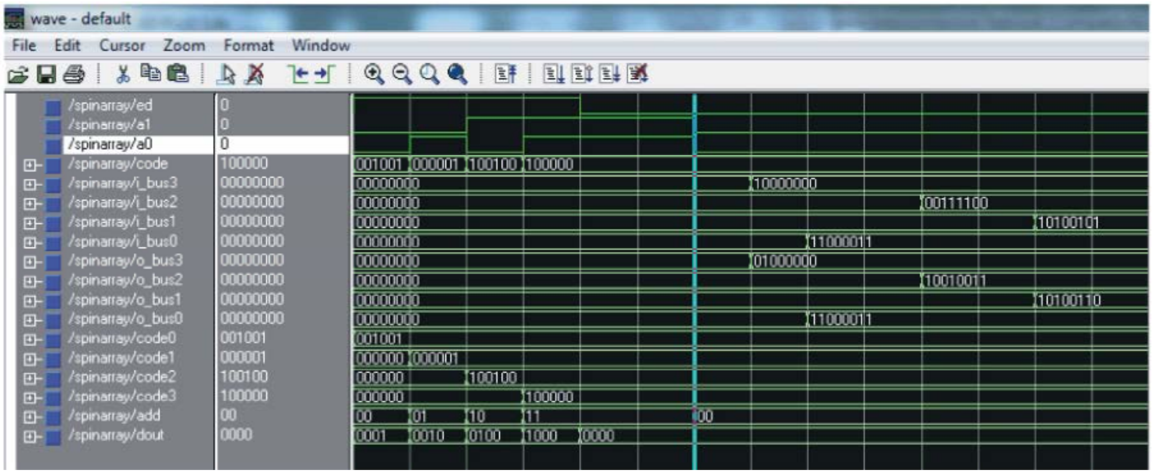
Table 2: Device Utilization Summary for different number of Interconnection Pattern Codes (N)

	Used	Available	% Used	Used	Available	% Used	Used	Available	% Used
Logic Utilization		N = 4			N = 5			N = 6	
No of slices used	33	960	3%	73	960	7%	93	960	9%
No of 4 input LUTs	65	1920	3%	122	1920	6%	162	960	8%
No of bonded IOBs	20	66	31%	21	66	32%	22	66	33%
Probability	1/16			1/32			1/64		

Fig. 9 shows a SPIN array loaded with four different interconnection patterns for the four SPIN8X8 networks. The interconnection pattern code for SPIN8X8 denoted as S0 is “001001” which defines the input-output relation as P=A, Q=B, R=C, S=D, T=E, U=F, V=G and W=H, where A, B, C, D, E, F, G and H are the inputs of a SPIN8X8 network and P, Q, R, S, T, U, V and W are outputs of the SPIN8X8 network. For the SPIN8X8 networks S1, S2 and S3, the interconnection patterns coders are “001111”, “1001111” and “100100” respectively and input-output relation for these SPINS are shown in the above figure. Incorporating a SPIN array in a logic circuit enhances its security as by default no interconnection is defined and at runtime an authentic user can define the correct interconnection pattern by applying appropriate IPC.

Experimental Results: The proposed system with 8 input 8 output is modeled in VHDL and behavioral code is synthesized using Xilinx ISE 8.1i. SPIN8X8 with Interconnection Pattern Codes of different widths was implemented and relationship between input and output of the proposed system was verified for different values of IPC. The target device selected was XC3S100E and device utilization summary is shown in Table 2 below.

Proposed system, SPIN8X8 with different width of IPC, 4bit, 5bit and 6bit was implemented in VHDL language using behavioral style of modeling. The number of interconnection patterns is 16 for 4bit IPC, 32 for 5bit IPC and 64 for 6bit IPC. When 4bit IPC was implemented, only 3% of total number of slices is utilized. Number of 4 bit LUTs used is also 3% while 31% of the bonded Input-Output blocks are used for 8 inputs, 8 outputs and 4 bit IPC. For the implementation of a SPIN8X8 with 5 bit wide IPC, which provides 32 (2^5) interconnection patterns, out of 960 slices only 73 slices are used (7%). Number of 4bit LUTs utilized for the implementation of the SPIN8X8 with 32 interconnection patterns is122 (6%) and number of bonded IOBs is 21 out of 66 (32%). In the case of a SPIN8X8 with 6 bit wide IPC bus, 2^6or 64 interconnection patterns are possible, only 6% of slices are used. Utilization of 4bit LUTs is just 8% from the 960 available 4 bit LUTs. Percentage of utilization of IOBs is almost same compared to SPIN8X8 with 4 bit wide IPC and 5 bit wide IPC. Table 2 shows the device utilization summary for different width of IPC. When resource utilization of various SPIN8X8 networks are compared, there is no significant difference between these three networks for a particular target device, in this case XC3S100E.



```
/spinarray/ed      0
/spinarray/a1      0
/spinarray/a0      0
/spinarray/code    100000    001001 000001 100100 100000
/spinarray/i_bus3  00000000  00000000  10000000
/spinarray/i_bus2  00000000  00000000  00111100
/spinarray/i_bus1  00000000  00000000  10100101
/spinarray/i_bus0  00000000  00000000  11000011
/spinarray/o_bus3  00000000  00000000  01000000
/spinarray/o_bus2  00000000  00000000  10010011
/spinarray/o_bus1  00000000  00000000  10100110
/spinarray/o_bus0  00000000  00000000  11000011
/spinarray/code0   001001    001001
/spinarray/code1   000001    000000 000001
/spinarray/code2   100100    000000 100100
/spinarray/code3   100000    000000 100000
/spinarray/add     00        00 01 10 11 00
/spinarray/dout    0000      0001 0010 0100 1000 0000
```

Fig. 10: Simulation result for SPIN array loaded with four different IPC which defines four different interconnection patterns for four SPIN8X8 networks

Probability of application of an interconnection pattern is 1/16, 1/32 and 1/64 respectively. In general, probability of application of an interconnection pattern for a SPIN8X8 network with 'N' bit wide IPC; the probability of application of an interconnection pattern is 1/N. From Table 2, it is evident that, more the number of interconnection pattern, less the probability of application of an interconnection pattern and more the degree of security.

For big systems with more number of 8bit buses, a SPIN array was designed and implemented. The proposed system consists of four SPIN8X8 networks along with four 6bit D latches and a 2:4 decoder which generates latch enable (LE) signals for the four 6bit latches. There are two modes of operation – Program mode and Function mode. In program mode all IPCs are loaded into the four D latches and in Function mode signal to be re-ordered are applied to the four 8bit input buses. Fig.10 shows the simulation results of a SPIN array implemented using VHDL. Left side of the blue line in the following waveform shows various binary values during Program mode and waveform on the right side of the blue line various values associated with the SPIN array during Function mode. During Program mode, four different IPCs are loaded into the D-latches and during Function mode, 8-bit input buses are loaded with four different binary values which appears re-ordered on the 8-bit output buses.

CONCLUSION

A Secured Programmable Interconnection Network (SPIN) with 8 inputs and 8 outputs also called as SPIN8X8 can be used to amplify the degree of security of digital circuits. Interconnection between input lines and output lines of SPIN8X8 depends on the binary value of the Interconnection Pattern Code (IPC) of the SPIN8X8 network. The default value of the Interconnection Pattern Code is "000000" in the case of a 6 bit wide IPC and default output of the SPIN8X8 is defined as logic'0', i.e., all output lines will be at logic'0' when interconnection code is "000000". For a SPIN8X8 network as number of possible interconnection between output and input depends on the width of the IPC bus, probability of application of right interconnection pattern is less for an IPC with 6 and more bits. When IPC bus is loaded with a wrong binary value, output of a logic block is routed to a wrong logic block where it is not intended to be. In this way by hiding the routing information or by defining a generic routing pattern logic circuits can be made secure.

To secure logic systems with multiple buses, a SPIN array can be used which posses more than one input and output buses. For systems with four 8bit buses, a SPIN array with four 8-bit input and four 8-bit output buses can be used as explained in the later part of this paper. This system enhances the security of the digital system, as an intruder by trial and error method must apply all the four IPC codes correctly in a single step. Probability of this is only $1/2^{24}$ which is almost impossible.

Compared to logic systems based on cryptography which occupy a large amount of FPGA resources, proposed system provides security ensuring that there is not much increment in the complexity and cost of the system. Cryptographic systems are less preferred for less complex system, due to the above mentioned factors of cost and complexity. The degree of security can be enhanced by increasing number of possible interconnection patterns between input and output of the proposed system. For complex systems, security enhancement can be achieved by using a SPIN array with more number of input and output buses. When more number of SPIN8X8 networks is incorporated, number of input and output buses as well as degree of security of the system also increases. For example when a SPIN array with eight 8-bit input and eight 8-bit output buses is used, actual width of the interconnection pattern code increases to 48 and probability of application of an IPC by trial and error method becomes $1/2^{48}$, which means better security compared to a 4 input 4 output SPIN array.

REFERENCES

1. Binu, K. Mathew and K.P. Zacharia, 2014. Programmable interconnection network for secured logic circuits, unpublished.
2. Tiri, K. and I. Verbauwhede, 2006. A digital design flow for secure integrated circuits", IEEE Trans. on Computer Aided Design of Int. Circuits and Systems, 25(7): 1197-1208.
3. Tripathy, A.K., A. Prathiba and V.S. Kanchana Bhaaskaran, 2013. A new improved MCML logic for DPA resistant circuits, Int. Journal of VLSI Design and Communication Systems, 4(5): 63-75.
4. Collins, W.H., 2013. A secure reconfigurable system-on-programmable chip computer system, Master's Thesis, University of Tennessee, Knoxville, Tennessee.
5. Zahur, S. and D. Evans, 2013. Circuit structures for improving efficiency of security and privacy tools", 34th IEEE symposium on security and privacy, San Francisco, pp: 1-15.
6. Huffmire, T., B. Brotherton, N. Callegari, J. Valamehr, R. Kastner, T. Sherwood and J. White, 2008. Designing secure systems on reconfigurable hardware, ACM Trans. On Design Automation of Electronics Systems, 13(3): 44.
7. Waksman, A., M. Suozzo and S. Sethumadhavan, 2013. FANCI: Identification of stealthy malicious logic using Boolean functional analysis, Proceedings of the 2013 ACM SIGSAC Conference on Comp. and Comm. Security, New York, pp: 697-708.
8. Abramovici, M. and P. Bradley, Integrated circuit security- New threats and solutions, Proceedings of the 5th Annual Workshop on Cyber Security and Information Intelligence Research: Cyber Security and Information Intelligence Challenges and Strategies, Article No. 55.
9. Goertzel, K.M. and B.A. Hamilton, 2013. Integrated circuits security threats and hardware assurance countermeasures, Crosstalk.
10. Baumgarten, A.C., 2009. Preventing integrated circuit piracy using reconfigurable logic barriers", Master's Thesis, Iowa State University, Ames, Iowa.
11. Ishai, Y., A. Sahai and D. Wagner, 2003. Private circuits:securing hardware against probing attacks", Proceedings of the annual international cryptology conference, California, pp: 463-481.
12. Khare, A.A., P.B. Shukla and S.C. Silakari, 2014. Secure and fast chaos based encryption system using digital logic circuit, Int. Journal of Computer Network and Information Security, pp: 25-33.
13. Chaves, R., Secure computing on reconfigurable systems, PhD Thesis, Technical University of Lisbon, Portugal.
14. Jensen, D.W., D.A. Greve and M.M. Wilding, 1999. Secure Reconfigurable Computing, Second Annual Military and Aero-space Applications of Programmable Devices and Technologies.
15. Valette, N., L. Torres, G. Sassatelli and F. Bancel, 2006. Securing embedded programmable gate arrays in secure circuits, 20th Int. Parallel and Distributed Processing Symposium.
16. Zheng, J.X. and M. Potkonjak, 2012. Securing netlist level FPGA design through exploiting process variation and degradation, Int. conference FPGA'12, USA, pp: 129-138.
17. Rajendran, J., M. Sam, O. Sinanoglu and R. Karri, 2013. Security analysis of integrated circuit camouflaging", Proceedings of the 2013 ACM SIGSAC Conference on computer and communications security, New York, pp: 709-720.
18. Costan, V. and S. Devadas, 2011. Security challenges and opportunities in adaptive and reconfigurable hardware, IEEE Symposium on Hardware Oriented Security and Trust, pp: 1-5.
19. Kepa, K., F. Morgan, K. Kosciuszkiewicz and T. Surmacz, 2010. SeReCon: A secure reconfigurable controller for self-reconfigurable systems", Int. Journal of Critical Computer Based Systems, 1(1//2/3): 86-103.
20. Hu, W., J. Oberg, A. Irturk, M. Tiwari, T. Sherwood, D. Mu and R. Kastner, 2011. Theoretical fundamentals of gate level information flow tracking, IEEE Trans. on Computer Aided Design of Integrated Circuits and Systems, 30(8): 1128-1140.