TELKOMNIKA Indonesian Journal of Electrical Engineering
Vol. 14, No. 2, May 2015, pp. 270 ~ 279
DOI: 10.11591/telkomnika.v14i2.7485

QCA and CMOS Nanotechnology Based Design and Development of Nanoelectronic Security Devices with Encryption Schemes

S. Devendra K. Verma*[1], P. K. Barhai[2], V. Nath[3]
Birla Institute of Technology (A Deemed University), Mesra– 835 215, Ranchi, Jharkhand, India
*Corresponding author, e-mail: SDKV@hotmail.com, pkbarhai@bitmesra.ac.in, vnath@bitmesra.ac.in

Abstract

In WiMAX/WiFi Wireless Environment the Transfer of Data/Information is vulnerable to external attacks as it takes place through an open-air medium. The Data/Information is vulnerable to Jamming, Detection, Interception, Network Injection, Interruption, Modification, Packet Scrambling, Fabrication, Unauthorised forwarding and Denial-of-Service (DoS). Our Research Work focuses on 'QCA & CMOS Nanotechnology based Design & Development of Nanoelectronic Security Devices with Encryption Schemes to provide/enhance Security and Privacy for WiMAX/WiFi/Satellite Wireless Communication Systems. The Schemes are based on Dynamic Channel Hopping, Random Channel Selection, Cryptography and Encryption of Information/Data/Control Codes.

Keywords: *nanotechnology, CMOS, QCA, WiMAX, WiFi, cryptography, encryption code*

1. Introduction

WiMAX (Worldwide Interoperability for Microwave Access) supports a variety of Wireless Broadband Connections, such as WirelessMAN, WirelessWAN, Cellular Base Stations & WiFi Internet, IPTV over WiMAX, etc. It provides high-data-rate communications for Fixed-Station (FS) Subscribers to a distance of 30 miles from a Base-Station (BS) and for Mobile-Station (MS) Subscribers to 10 miles from a BS.

In our Research Work, the Security Principles used in WiMAX (IEEE 802.16e) and WiFi (IEEE 802.11i) are analyzed and it is found that many sophisticated Techniques are embedded into WiMAX and WiFi for Authentication and Encryption, but it still exposes to various Security Attacks. There are Security Vulnerabilities in both PHY and MAC Layers of WiMAX. It exposes to various classes of Wireless Attacks, such as Jamming, Interception, Modification, Fabrication, Replay, etc. Similarly WiFi is also exposed to such Wireless Attacks.

WiMAX Programmable Transceiver is a Device, which transmits and receives radio signals simultaneously. It increases its capacity and usability in real-time applying FDD (Frequency Division Duplexing), which provides simultaneous Radio Transmission Channels for the Subscriber and the BS. In Channel/Frequency Hopping a number of Channels are allocated. At the XMTR-End, for a fixed interval the Transmitter transmits in one channel at a time and the RCVR-End, the Receiver synchronizes with the Transmitter by hopping between the Channels and the Message is reconfigured accordingly.

In our Research Work, a Programmable Security Device (PSD) is designed/ developed/ simulated for WiMAX/WiFi/Satellite Wireless Communication Systems. The CMOS Model is developed using CADENCE Software Tool to the scale of 45 nanometer & 1.0v, and the QCA Model using QCADesigner Tool with Cell size <20 nanometer & powered with Clock Signals only. The Model is simulated with four Buses/Carriers/Channels, transmitting Messages from four Sources/Users to four Destinations hopping among four Channels and the Receiver synchronizes with the Transmitter and the Messages are reconfigured accordingly for four Destinations. The PSD System is based on Network, incorporating Dynamic Channel Hopping, Random Channel Selection and Encryption of Messages and Control Codes to provide Security & Privacy in WiMAX/WiFi Wireless Communication Networks.

Received February 9, 2015; Revised April 20, 2015; Accepted May 1, 2015

2. Security Threats in WiMAX & WiFi

The WiMAX and WiFi Protocols are examined to evaluate the Security Measures provided. The Security Architecture for WiMAX is based on two major concepts: Requirements, applicable to the Network Elements and Systems, constituting the end to-end network, are addressed by the Security Layers. For Data Encryption, there are two Schemes – a) AES (Advanced Encryption Standard and b) 3DES (Triple Data Encryption Standard). For the WiFi Protocol, the WEP (Wired Equivalency Privacy) Encryption Scheme was first introduced and later it was modified and the WPA (WiFi Protected Access) Scheme was adopted. A PSK (Pre-Shared Key) is created to authorize contact. WPA is further enhanced and WPA2 Scheme is introduced [1-3].

The Security Architecture and Principles used in the WiMAX (802.16e Protocol) and WiFi (802.11i) are analysed and found that it is not sufficient to prevent/protect from Jamming, Interception and Data Traffic Modification. Application of Channel/Frequency Hopping Technique with Encryption Key and Control Codes is more suitable to deal with Jamming and Interception and provide the required prevention and protection. This kind of Security Management is a Network-based Defence (NBD) Scheme. Its capability is enhanced with application of Control Code and Key Code [4-7].

In WiMAX/WiFi Wireless/Mobile Communication, there are different types of Security Threats, such as: Jamming/ Interception of the Communication Link, Interception/ Modification/ Fabrication/ Forwarding of the Message, Cloning/ Security Code Violation, etc. The Security Services are classified as: Confidentiality, Nonrepudiation, Authentication, Integrity, Availability, Prevention of Security Violation, Security Detection, Recovery, etc. The Techniques (Schemes) used to protect Security and Privacy are: Channel/Frequency Hopping, Encryption of Message, Source/Destination Codes, Authentication, etc [8-11].

The Security Devices & Schemes are based on Channel/Frequency Hopping, a Technique in which a number of Channels are allocated and the Transmitter transmits in one channel at a time for a fixed interval. During that interval some number of bits (data) is transmitted using some encoding scheme. A Receiver, hopping between Channels/Frequencies synchronizes with the Transmitter and the message is reconfigured accordingly. There are two basic types of Frequency Hopping, identified as: a) S-FH (Slow-Frequency Hopping), where several Symbols/Multiple Bits are transmitted on each Frequency Hop, and b) F-FH (Fast-Frequency Hopping). It enables the Carrier Frequency during the Transmission of one Symbol/Bit to change/hop several times.

In this Research Work a PSD (Programmable Security Device) is designed, based on Channel/Frequency Hopping Technique along with Encryption of Messages and Control Codes for providing Security and Privacy in WiMAX/WiFi Wireless Communication.

3. CMOS & QCA Technology

CMOS (Complementary Metal-oxide Semiconductor) Logic is a combination of PMOS and NMOS Logic. The CMOS Logic Functions are designed using both P-Type and N-Type Transistors. The Power Dissipation in CMOS takes place only when Circuit switches and it consumes very little power. It supports fabrication of VLSI Circuits with many more CMOS Gates on an IC having much better performance.

QCA represents an emerging Technology, which was first introduced by Lent et al in 1993. QCA Logic States are represented with Quantum Wells having 4 Quantum-Dots and 2 mobile Electrons. In the QCA Cell, the Electron Tunnelling facilitates the movement of the Electrons to different Quantum-Dots positioning diagonally, based on the Columbic Force. There are two possible Polarizations: +1 (Binary 1) and -1 (Binary 0), depending on the Electrons' positions. In QCA a Logic Signal Transmission Channel is known as Binary Wire. The Cells transmit information in Coded form (0 or 1) from one Cell to another in the Binary Wire without any current flow. Each Cell's Polarization depends upon its previous neighboring Cell's Polarization. In the case of Inverter Chain, the transmission of Code takes place with inversion of the Code of the previous neighboring Cell.

Majority Gate is used to implement QCA. It consists of one Center (Device), three Input and one Output Cells. If A, B, C are Inputs then Output (the majority of A,B,C) = M(A,B,C) = AB+BC+CA. The AND logical operation is performed if the input polarization of Control Input is fixed to -1 (logic 0) and the OR logical operation is performed in the case of +1 (logic 1). When the Cells are placed diagonally, the NOT logical operation is performed. The Majority AND, OR and NOT Gates are shown in Figure 1.

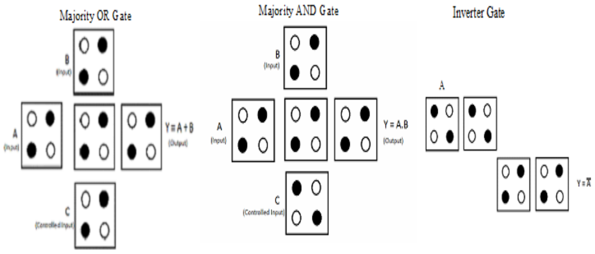


Figure 1. Majority Gates

A Multizone Clock Mechanism is required for Data Propagation in the QCA Circuit. It has four Clock Signals with 90 degree relative phase difference with each other. Zone 0, Zone 1, Zone 2 and Zone 3 are identified as four Clocking Zones, and Switch, Hold, Release and Relax States are identified as four Clock Phase/States. Each Cell is connected to one of four Phases of the QCA Clock in a Clocking Zone. Depending on the polarization of the neighboring Cell, the Switch and Hold States determine the QCA Cell's Polarization while the Release and Relax States are unpolarized. With the changing of the Clock Signal each Cell is latched and unlatched. The QCA Clock and QCA Clock Zones are shown in Figure 2 [12-17].

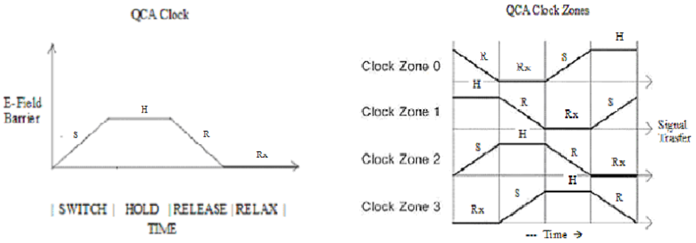


Figure 2. QCA Clock Signal

4. Methodology

Our approach will be to design, develop, qualify and optimize PSD-CMOS Model to the Scale of 45 nanometers and Voltage = 1.0V, using CADENCE Software Tool. Also simulate, layout and verify PSD-QCA Model with QCA-Cell size < 20 nanometer, using QCADesigner Tool. The 'Molecular Nanoelectronics' Technology and the 'Top-down' approach is more suitable for obtaining Nanostructure within the size of < 50 nm scale and Cell size < 20nm. PSD will be a new Device to provide/enhance Security and Privacy for WiMAX/WiFi/Satellite Wireless Communication Systems. [18-20].

5. Simulation Tools & Setup

Two Simulation Tools are used to design, develop, model and qualify PSDs (Programmable Security Devices). Cadence Software Tool is used to model PSD-CMOS and QCADesigner Tool is used to model PSD-QCA Devices.

5.1. CADENCE Software Tool

The Cadence Software Tool is an Electronic Design Automation Software, used for CMOS Circuits Simulation. It is known as Cadence Analog and Digital System Design Tools (GPDK46nm). The Process Geometries include the length and width of a Transistor to the scales of 45nm and 65nm respectively.

5.2. QCADesigner

The QCADesigner Tool is used for QCA Circuits Simulation, constructed with QCA Cells (each cell size = 20nm). The Tool having CAD capabilities, helps to layout and simulate QCA Circuits. To facilitate rapid and accurate simulation, QCADesigner has three Simulation Engines: a) DLSE (Digital Logic Simulation Engine), which determines Cells to be either null or fully polarized; b) NASE (Nonlinear Approximation Simulation Engine), which determines the stable state of the Cells, depending on the nonlinear cell-to-cell response function; and c) TSSE (Two-State Simulation Engine), which forms an approximation of the full quantum mechanical model. In QCA Circuits, the control of the flow of information is performed using four Clock Signals: Clock Zone 0, Clock Zone 1, Clock Zone 2 and Clock Zone 3.

6. Simulation Model

A PSD (Programmable Security Device) is designed with Switches/Transmission Gates (TG) for XMTR-End and RCVR-End. The Simulation Model (defined for communication), comprises of four Bus Carriers/Channels (as B0, B1, B2, B3), four Source/User Communication Links (as S0, S1, S2, S3), four Destination Links (as D0, D1, D2, D3), and four Control Links (as C0, C1, C2, C3). There are four Frequencies assigned (as f0, f1, f2, f3) for Bus Carriers/Channels (as B0, B1, B2, B3). The Control Link is used to select a Bus Carrier for each User/Source Link in this configuration for transmitting Message/Data. Similarly, for receiving Data, the Control Link is used to synchronize the transmitter and select Bus Carrier for each Destination Link. The PSD (Programmable Security Device) is shown in Figure 3. The CMOS Transmission Gate Circuit and the Transmission Gate Circuit Analysis are shown in Figure 4 & Figure 5.

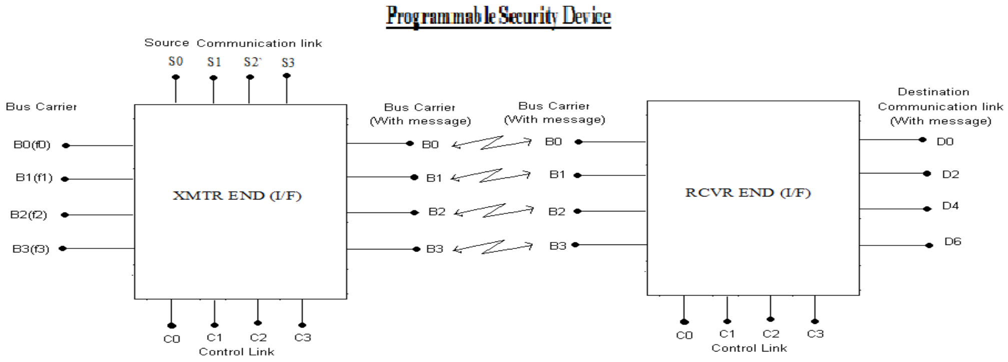
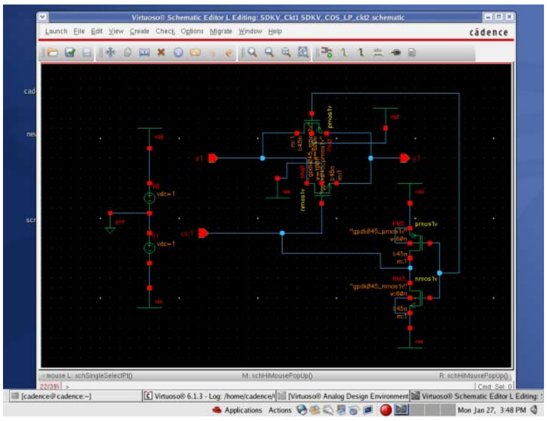


Figure 3. Programmable Security Device


Virtuoso® Schematic Editor L Editing: SDKV_Ckt1 SDKV_COS_LP_ckt2 schematic
Launch File Edit View Create Check Options Migrate Window Help
cādence
vdc=1
vdc=1
gpdk045_pmos1v
gpdk045_nmos1v
pmos1v
nmos1v

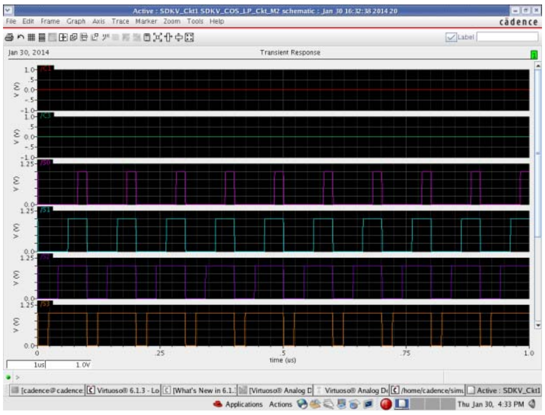

Active : SDKV_Ckt1 SDKV_COS_LP_Ckt_M2 schematic
File Edit Frame Graph Axis Trace Marker Zoom Tools Help
cādence
Jan 30, 2014
Transient Response
V (V)
1.0
.5
0.0
-.5
-1.0
1.25
0.0
0
.25
.5
.75
1.0
time (us)

Figure 4. CMOS Transmission Gate Circuit

Figure 5. CMOS Transmission Gate Analysis

There are two Models: PSD-CMOS Model and PSD-QCA Model, designed, developed, simulated and analysed, having a set of 4 Bus Carriers (Channels), Source/User Communication Links and Control Links and it can be expanded to a set of 8, 12 or 16 Channels.

6.1. PSD-CMOS Model

The PSD-CMOS Model is designed and developed using CADENCE Software Tool to the scale of 45 nm and 1.0V. CMOS Switches/Transmission Gates (TG) Matrix is used to design PSD for XMTR-End and RCVR-End. The PSD Switch Matrix is needed at both Transmitting and Receiving Ends for configuring different Patterns. The same Pattern is used by both the XMTR and RCVR for transmitting and receiving the Data/Message. A set of four Switches/Transmission Gates are connected to each Contrl Link. One Control Link is selected at a time and each Switch connects one User/Source Link to one Bus Link at the Transmitting End and similarly one Destination Link to one Bus Link at the Receiving End.

In this Model, for four Control Links (as C0, C1, C2, C3), a set of four Control Codes (as CC1, CC2, CC3, CC4) are defined having different values as follows:

CONTROL LINK	**CONTROL CODE**
C0	CC1 = 11000001
C1	CC2 = 11000010
C2	CC3 = 11000011
C3	CC4 = 11000100

For each Channel/Frequency Hopping, the Control Code is selected randomly, and the associated Control Link is activated accordingly for allocating Bus Carriers (Channels) to the User/Source Links at the Transmitting End, and similarly allocating the Bus Carriers (Channels) to the Destination Links at the Receiving End. During each Channel/Frequency Hopping, Message/Data is transmitted from the User/Source Links to the corresponding Destination Links. Again for the next Channel/Frequency Hopping, a new Control Code is selected randomly, the associated Control Link is activated, Channels are allocated and transaction of Message/Data takes place as mentioned above. For encrypting the Control Code and transmitting to the Receiving End, an Encryption Key is defined.

A set of Transmission Gates (TG) are used for Switch Matrix. Using CADENCE Software Tool, a PSD-CMOS Model is simulated (for 1.0V and 45 nm scale). The PSD-CMOS Model and the PSD-CMOS Model Analysis are shown in Figure 6 & Figure 7 respectively.

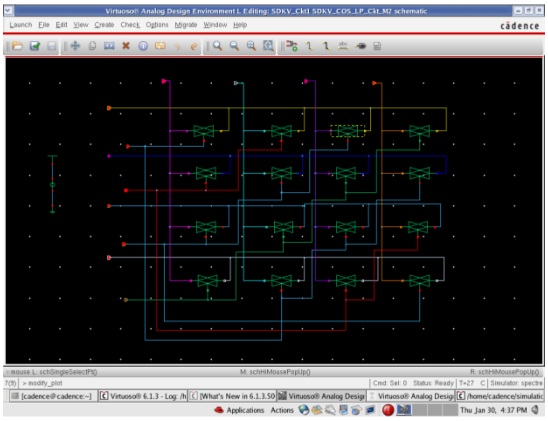

Virtuoso® Analog Design Environment L Editing: SDKV_Ckt1 SDKV_COS_LP_Ckt_M2 schematic
Launch File Edit View Create Check Options Migrate Window Help
cādence

Figure 6. PSD-CMOS Model

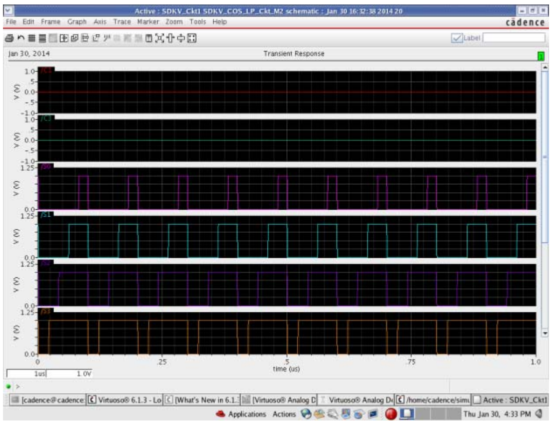

Active : SDKV_Ckt1 SDKV_COS_LP_Ckt_M2 schematic : Jan 30 16:32:38 2014 20
File Edit Frame Graph Axis Trace Marker Zoom Tools Help
cādence
Label
Jan 30, 2014
Transient Response
V (V)
time (us)

Figure 7. PSD-CMOS Model Analysis

6.1.1. Simulation Results & Analysis

A PSD-Channel/Frequency Hopping Pattern is simulated in which for each Channel/Frequency Hopping Time Slots (as t0, t1, t2, t3), the Control Codes are selected randomly in the sequence of CC2, CC4, CC1 and CC3. For each Channel Hopping Time Slots, the Source/User Links are allocated to the Bus Carriers (Channels) where the S0 is linked to B1, B3, B0 and B2 in sequence corresponding to the Channel/Frequency Hopping Time Slots t0, t1, t2 and t3 as shown below. The PSD-Channel Hopping Pattern is shown in Figure 8.

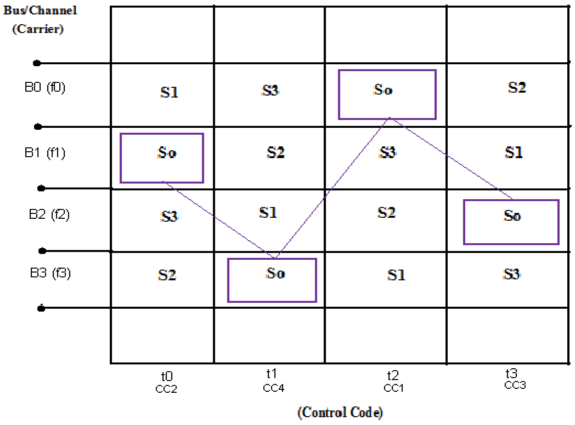


Figure 8. PSD-Channel Hopping Pattern

BUS CARRIER		**HOPPING TIME SLOT**			
(Linked to Source)		**t0**	**t1**	**t2**	**t3**
B0	→	S1	S3	**S0**	S2
B1	→	**S0**	S2	S3	S1
B2	→	S3	S1	S2	**S0**
B3	→	S2	**S0**	S1	S3

The Simulation Model using CADENCE (for 1V and 45 nm scale) is analysed and it is found that the performance of the Circuit Model for Switch Matrix is verified and qualified functionally.

6.2. PSD-QCA MODEL

The PSD_QCA Model is designed and developed using the QCADesigner Tool with QCA Cell size < 20nm, and its performance is analysed and qualified. The PSD-QCA Model and PSD-QCA Model Analysis are shown in Figure 9 & Figure 10.

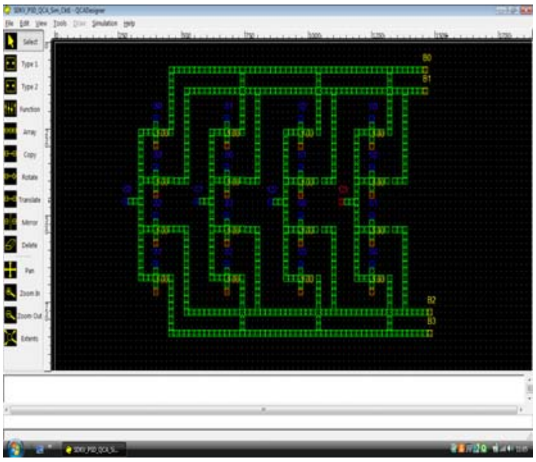


Figure 9. PSD-QCA Model

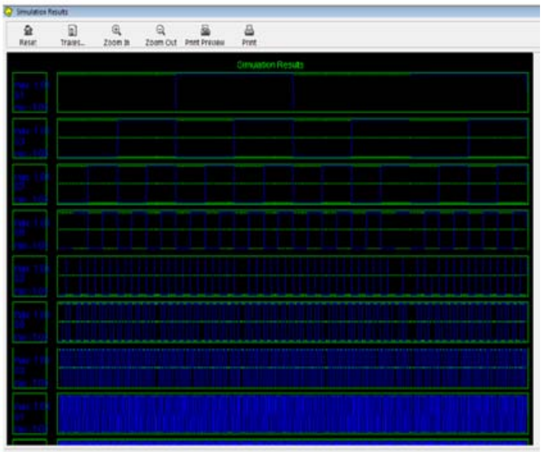


Figure 10. PSD-QCA Model Analysis

The PSD-QCA Logic is defined as follows:
Case 1: C0 Control Link is selected:
QCA AND Logic 0: B0 = m(C0,S0,0) = m(1,S0,0) = S0
QCA AND Logic 1: B1 = m(C0,S3,0) = m(1,S3,0) = S3
QCA AND Logic 2: B2 = m(C0,S2,0) = m(1,S2,0) = S2
QCA AND Logic 3: B3 = m(C0,S1,0) = m(1,S1,0) = S1

Case 2: C1 Control Link is selected:
QCA AND Logic 0: B0 = m(C1,S1,0) = m(1,S1,0) = S1
QCA AND Logic 1: B1 = m(C1,S0,0) = m(1,S0,0) = S0
QCA AND Logic 2: B2 = m(C1,S3,0) = m(1,S3,0) = S3
QCA AND Logic 3: B3 = m(C1,S2,0) = m(1,S2,0) = S2
Case 3: C2 Control Link is selected:
QCA AND Logic 0: B0 = m(C2,S2,0) = m(1,S2,0) = S2
QCA AND Logic 1: B1 = m(C2,S1,0) = m(1,S1,0) = S1
QCA AND Logic 2: B2 = m(C2,S0,0) = m(1,S0,0) = S0
QCA AND Logic 3: B3 = m(C2,S3,0) = m(1,S3,0) = S3

Case 4: C3 Control Link is selected:
QCA AND Logic 0: B0 = m(C3,S3,0) = m(1,S3,0) = S3
QCA AND Logic 1: B1 = m(C3,S2,0) = m(1,S2,0) = S2
QCA AND Logic 2: B2 = m(C3,S1,0) = m(1,S1,0) = S1
QCA AND Logic 3: B3 = m(C3,S0,0) = m(1,S0,0) = S0

7. PSD (Programmable Security Device)–2

There are three types of Encryption-based PSD-2 Models: a) PSD-2 Model-A, b) PSD-2 Model-B and c) PSD-2 Model-C. There are 16 Encryption Codes (ECs) defined and identified with Code No. (Cn). One Code No. is selected randomly and the corresponding Encryption Code (EC) is identified and used for Encryption Schemes. A Table with Code No. (Cn) and Encryption Codes (ECs) is defined as follows:

CODE NO. (Cn):	ENCRYPTION CODE (EC):
C0:	11111111
C1:	10101010
C2:	01010101
C3:	11001100
C4:	00110011
C5:	11110000
C6:	00001111
C7:	11000011
C8:	11100111
C9:	00011000
C10:	11000011
C11:	00111100
C12:	10000001
C13:	01111110
C14:	11001111
C15:	11110011

7.1. PSD-2 Model-A

In this model, at the XMTR-End, one Code No. (Cn) is selected randomly and the corresponding 8-bit Encryption Code (EC) is identified, and 8-bit Data (D) to be transmitted is XOR with it and transmitted along with the Encryption Code (EC). At the RCVR-End, the received Encrypted Data is XOR with the Encryption Code (EC) and the transmitted Data (D) is retrieved. A PSD-2 Model-A is shown in Figure 11.

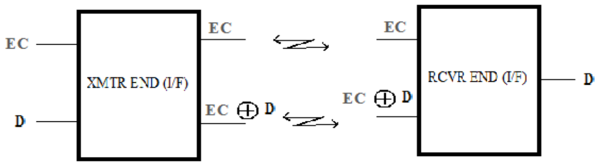


Figure 11. PSD-2 Model-A

7.2. PSD-2 Model-B

In this model, at the XMTR-End, one Code No. (Cn) is selected randomly and the corresponding 8-bit Encryption Code (EC) is identified, 8-bit Data (D) to be transmitted is XOR with it. The XOR Data and the Encryption Code (EC) both are further inverted or XOR with '11111111' separately and transmitted. At the RCVR-End, the Encrypted Data and Encryption Code are first inverted or XOR with '11111111' separately and then they are XOR together and the transmitted Data (D) is retrieved. A PSD-2 Model-B is shown in Figure 12.

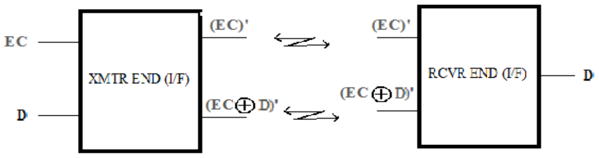


Figure 12. PSD-2 Model-B

7.3. PSD-2 Model-C

In this model, the Table with Code No. (Cn) and Encryption Codes (EC) is available at both XMTR-End and RCVR-End. At the XMTR-End, a Code No. (Cn) is selected randomly and the corresponding 8-bit Encryption Code (EC) is selected and the 8-bit Data (D) to be transmitted is XOR with it and transmitted along with the Code No. (Cn). At the RCVR-End, the received Encrypted Data is XOR with the Encryption Code (EC) corresponding to the Code No. (Cn) received, and the transmitted Data (D) is retrieved. A PSD-2 Model is shown in Figure 13.

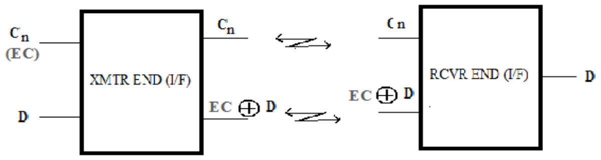


Figure 13. PSD-2 Model-C

8. PSD-2 Logic Circuit Model

A PSD-2 Logic Circuit for both XMTR-END and RCVR-END is designed as shown in Figure 14.

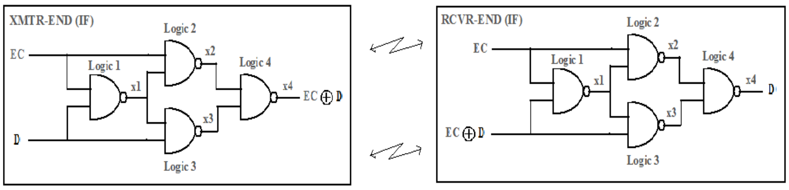


Figure 14. PSD-2 Logic Circuit

8.1. PSD-2 CMOS Model

The PSD-2 XOR-CMOS Model and the PSD-2 XOR-CMOS Model Analysis are shown in Figure 15 and Figure 16.

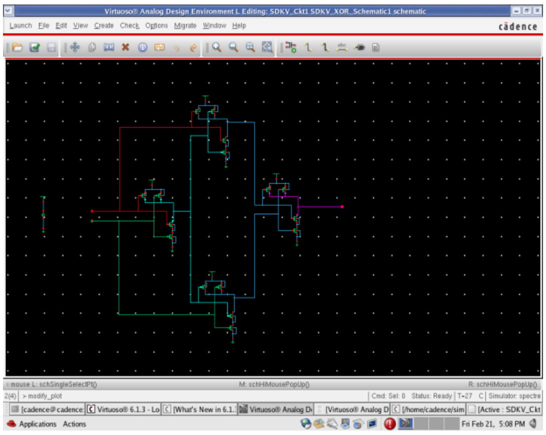

Virtuoso® Analog Design Environment L Editing: SDKV_Ckt1 SDKV_XOR_Schematic1 schematic
cadence
Applications Actions

Figure 15. PSD-2 CMOS Model

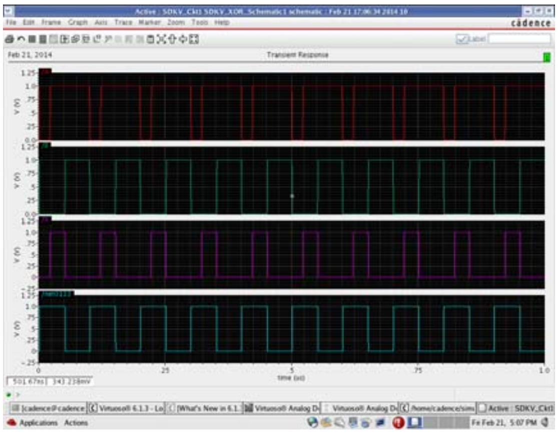


Figure 16. PSD2 CMOS Model Analysis

8.2. PSD-2 QCA Model

The PSD-2 QCA Model is designed and developed and its performance is analysed and qualified. The PSD-2 QCA Model and the PSD-2 QCA Model Analysis are shown in Figure I7 & Figure 18.

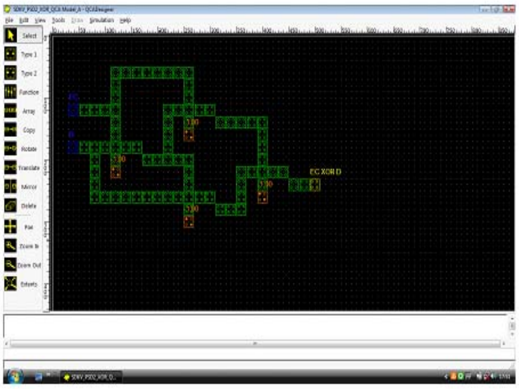


Figure 17. PSD-2 QCA Model

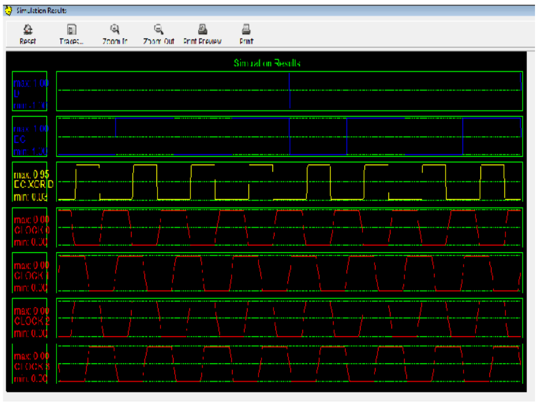


Figure 18. PSD-2 QCA Model Analysis

The PSD-2 QCA Logic is defined as follows:
QCA NAND Logic 1: x1 = (m(EC,D,0))’
QCA NAND Logic 2: x2 = (m(EC,x1,0))’
QCA NAND Logic 3: x3 = (m(x1,D,0))’
QCA NAND Logic 4: x4 = (m(x2,x3,0))’

9. Conclusion

Our Research Work is focused on Application of CMOS-VLSI and QCA Nanotechnology in WiMAX/WiFi/Satellite and other Wireless Communication Systems. A PSD (Programmable Security Device) is designed, developed modelled and qualified based on CMOS Nanotechnology (to the scale of 45 nm and 1.0v) and QCA Nanotechnology (to the scale of Cell size < 20 nm), applicable to WiMAX/WiFi/Satellite Wireless Communication Systems in Real-time Environment to provide Security and Primacy. This Research Work will lead to Design & Develop of Smart & Small Devices and provide Architectural Innovation, Value Added Services, Full Scale QoS (Quality of Service) and Higher Security & Privacy.

10. Future Work

Our Research Work will address Long term Technical Challenges, and it will focus on Design, Development and Transformation of CMOS-VLSI Circuits/Devices/Systems into QCA Nanotechnology for WiMAX/WiFi/Satellite and other Wireless Communication Systems to achieve Low Power, Low Voltage, Miniaturization, Added Features/Functionalities and Reliability.

References

[1] WiMAX Forum. Mobile WiMAX – Part I: A Technical Overview and Performance Evaluation. 2006.

[2] WiMAX Forum. Mobile WiMAX – Part II: A Comparative Analysis. 2006.

[3] Ghosh, et al. Broadband Wireless Access with WiMAX/802.16: Current Performance Benchmarks and Future Potential. *IEEE Communications Magazine.* 2005: 129-136.

[4] Jacoba Stuart. WiMAX Subscriber and Mobile Station Authentication Challenges. *IEEE Communications Magazine.* 2011: 166-172.

[5] Johnson David, Walker Jesse. Overview of IEEE 802.16 Security. IEEE Computer Society Press. 2004; 2(3): 40-48.

[6] Kim Hyung-Joon. IEEE 802.16/WiMAX Security, WiMAX Security Functions. Dept. of Electrical and Computer Engineering, Stevens Institute of Technology. NJ, USA.

[7] Xu Sen, Mathews Manton, Huang Chin-Tser. Security Issues in Privacy and Key Management Protocols of IEEE 802.16, WiMAX Security Functions. Dept. of CSE, Univ. of South Carolina.

[8] Elmasry George F, Welsh Robert, Jain Manoj, Hoe Ben. Security and Network Operations, Challenges with Cellular Infrastructure in the Tactical Theater. *IEEE Communications Magazine.* 2011: 72-80.

[9] Hegland Anne Marie, Kongsberg Defence & Aerospace, Winjum Eli, Hedenstad Ole-Erik, Norwegian Defence Research Establishment. A Framework for Authentication in NBD Tactical Ad Hoc Networks. *IEEE Communications Magazine.* 2011: 64-71.

[10] Barbeau Michel. *WiMAX/802.16 Threat Analysis*. Proceedings of the ACM Int. Workshop on Quality of Service and Security in Wireless and Mobile Networks, Q2Swinet ’05, ACM Press. 2005: 8-15.

[11] Baldini Gianmarco, JRC-EC, Picchi Ottavio, Luise Marco. The EULER Project: Application of Software Defined Radio in Joint Security Operations. *IEEE Communications Magazine.* 2011: 55-62.

[12] CS Lent, et al. Quantum Cellular Automata. *Nanotechnology.* 1993; 4(1): 49-57.

[13] PD Tougaw, CS Lent. Logical Devices Implemented Using Quantum Cellular Automata. *Journal of Applied Physics.* 1994; 75(3): 1818-1825.

[14] CS Lent, B Isaksen. Clocked Molecular Quantum-Dot Cellular Automata. *IEEE Transaction on Electron Devices.* 2003; 50(9).

[15] A Imre, et al. Majority Logic Gate for Magnetic Quantum-Dot Cellular Automata. *Science.* 2006; 311: 205-209.

[16] I Amlani, et al. Digital logic using Quantum-dot Cellular Automata. *Science*. 1999; 284: 289-291.

[17] JC Ellenbogen. A Brief overview of Nanoelectronic Devices. *MITRE MSR Program*. 1998.

[18] S Devendra, K Verma, PK Barhai. Design & Development of Nanoelectronic AOI & OAI Devices based on CMOS and QCA (Quantum-Dot Cellular Automata) Nanotechnology. *IJAET Journal.* 2013; 6(1).

[19] S Devendra, K Verma, PK Barhai. Design & Development of Nanoelectronic Binary Decision Tree Device based on CMOS and QCA (Quantum-Dot Cellular Automata) Nanotechnology. *IJCA Journal.* 2012; 7(1).

[20] S Devendra, K Verma, PK Barhai. Design & Development of ‘Programmable Security Controller (PSC) (A Nanotechnology Device)’ for WiMAX/WiFi Wireless Communication. *IJMAN Journal.* 2012; 2(1).