Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 5, 2021, Pages. 1934 - 1939
Received 15 April 2021; Accepted 05 May 2021.

Hardware Security based Quantum Dot Cellular Automata Circuit Design – Review and Outlook

M. Amutha[1], K.R. Kavitha[2]

[1]Department of ECE, Sona College of Technology, Salem, India. E-mail: amutha@sonatech.ac.in

[2]Department of ECE, Sona College of Technology, Salem, India. E-mail: kavithakr@sonatech.ac.in

ABSTRACT

In recent scenario, CMOS technology plays a very important role in VLSI based IC technology which is a integration of logic models. The chips operations have shown an outstanding development in the decades. This increment of chips has relied on shrinking the transistor. In CMOS technology, the scaling process has led to severe challenges of power consumption, physical dimensions, and current leakages. Among the probable solutions, Quantum Cellular Automata (QCA) is known as the top promising technologies due to its potential applications in computational designs with appealing features like low power consumption, high speed operation and high device density. The QCA offers a better solutions for some circuit namely adders, multipliers, memories, cryptographic processors and nano communication devices etc. The results of physical hardware attacks are severer and recovery is difficult which the paper is interested to focus on hardware security. This paper discusses the several security challenges like Reverse engineering, gate level net list overbuilding and some of the attacks and their countermeasures based on circuits. Some of the secret key-based cryptographic methods challenges are secret key distribution, generation and more importantly securing these secret keys from physical attacks is the major problems. The Physically Unclonable Functions (PUFs) are freshly used as a hopeful hardware security solution for identification and authentication of circuits. Hardware security has emerged with the several issues like piracy, counterfeiting, and side channel attacks. This paper gives the various methods that are presented by many researchers to secure the innovated design from the third party in CMOS technology. The paper is concluded with a need for research in security in QCA based circuit for hardware security in IC/IP.

KEYWORDS

Quantum Cellular Automata, Physically Unclonable Function, Reverse Engineering, PhysicalAttacks, Counterfeiting.

Introduction

An information security has grown which is mainly focusing on the data storing secrecy and in-transit that including trust, anonymity, and remote ground trothing Since the mid-1970s. The applications of security in the technologies have advanced from protecting physical principles with mainframe systems. This system contains a securing less weight, minimum rate and low-power mobiles, tablets and sensors. Along with this innovation, many new security issues are also emerged in the system namely physical resiliency and side channel attacks respectively.

Some of the security problems in traditional computers which was an untrusted function are involved on the IC manufacturing method such as reverse engineer, insert Trojans or overproduce of ICs model by a fabless design. Evidently, the capability to lessen this problem is done within the ICs production which is significant to the IP protection and also for the untrusted prevention of malicious elements in serious computer systems.

The utilization of key circuits give a mainstream approach to decrease the issues in particular IC piracy and counterfeiting. The Physical Unclonable Functions (PUFs) are the equipment for secure key process that has the operation which maps test reactions for privacy. Therefore the novel reactions are utilized in a few different methods to authorize safety. Additionally the IC technology is scaled for the achievement of nanometer system. In this way, nano electronic gadgets and circuits give a chance to create opportunity equipment security primitives like PUFs.

For many times, nano electronic security parameters are possibly powerful than traditional CMOS security process. It serves the reason for verifiable security in a data hypothetical logic as the multifaceted nature of nanoelectronic security attacking that are proportional to the serious issue to solve a huge arrangement of nonlinear conditions. At last, developing nanoelectronics can possibly yield miniscale structure factors, quick calculation times and ultralow force utilization comparative with current semiconductor innovations.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 5, 2021, Pages. 1934 - 1939
Received 15 April 2021; Accepted 05 May 2021.

The QCA innovation is the ultralow power technology which has the requirements of non-critical designs of power utilization. In any case, attacks of Side Channel Analysis (SCA) caused critical issues to CMOS cryptographic circuits in the previous decade which is dependent on evaluations of energy. The cryptographic code data dropped by the physical usages are misused by these attacks and the Side Channel data is used to break the code in small partitions. A power analysis attack is the most remarkable procedures in SCA. In the electronic security gadget, this attack can isolated the private secret key by evaluating the power utilization of cryptographic circuits. This circuit performed inside the gadget which extremely depends on the information. In the QCA technology, it comprises the electron situation by the variation of cells where the usage of power is ultralow. Likewise, this survey verifies that QCA cryptographic circuits are capable for controlling the power analysis attack.

The rest of the paper is organized as the background of QCA technology is explained in section2. The section 3 comprises the hardware attacks with the different types and the section 4 includes the hardware security methods. The section 5 described the related papers to the QCA work and finally the survey is concluded with the section 6 and references.

Background

A.QCA Basics

QCA is an emerging nano-technology that can be promised to quantum based on columbic interaction process. The polarizations of electrons are the well-known logic state than voltage level as in QCA CMOS innovation. This technology has four quantum dots that are situated at four corners of the cell. Each cell has two free electrons which is the cell's limitation. This electrons has logical values with the placement of dots where the assign the two consistent electrons polarization of P = +1.00 and P = −1.00 i.e., rationale '1' and rationale '0' of a QCA cell individually (Fig. 1).

The quantum cells are operated with the polarization Inverse because of columbic repulsion between two adjacent corner cells. The basic elements of QCA are the QCA wire, Majority Voter (MV) and Inverter. The MV is modeled using five QCA cells. The middle cell is surrounded by three input cell and one output cell where the middle one is influenced by the majority of inputs that is shown in Fig. 2.

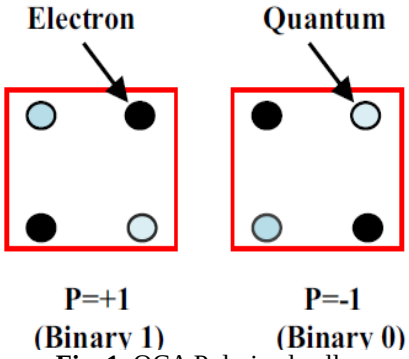

Fig. 1. QCA Polarized cell

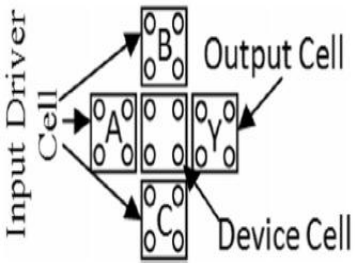

Fig.2. QCA majority voter (MV)

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 5, 2021, Pages. 1934 - 1939
Received 15 April 2021; Accepted 05 May 2021.

Hardware Attacks

A. Physical Attacks

This attack is defined as physicality of the attack done with hardware tools which also distinguishes the hardware from the software. Unlike the software attacks that is done by just injecting a vulnerability tool on the web for the attacks. But the hardware attacks can be only performed with an extensive knowledge of circuit model then the attack is occurred.

B. Side-Channel Attack

In PC security, a side-channel attack is an attack that supports data picked up from the execution of a processing framework, rather than shortcomings inside the developed methods itself (for example cryptanalysis and programming bugs). Timing data, power utilization, electromagnetic leaks or perhaps sound can give an extra wellspring of information, which might be abused.

C. Power Analysis

It is a type of side channel attack that the aggressor considers the power utilization of a cryptographic equipment gadget. These attacks accept essential physical properties of the gadget: semiconductor gadgets are administered by the laws of physics that direct the adjustments in voltages inside the gadget require little developments of electrical charges (flows). By estimating those flows, it is conceivable to get familiar with a limited quantity of data about the information being controlled.

Hardware Security Methods

A. Hardware Security Module

An hardware security module (HSM) might be a physical PC that shields and oversees computerized keys for robust validation and gives crypto processing. These modules generally are accessible the state of a module card or an outside gadget that joins on to a PC or organization server.

B. IC Camouflaging

Integrated circuit (IC) camouflaging is layout level logic locking technique against third party attack by IC extraction. In camouflaging, possible to implement all logic functions but increases power dissipation of IC's.

C. Logic Obfuscation

Logic obfuscation is a simple gate inserting or embedding technique to prevent attacker from IC stealing. The original operations of IC obtained or booted only when the correct key given by user. By increasing the count of key gate the security level of the circuit get increased

Related Work

A. System –Level Analysis

Randy Torrance et al. [1] examines the strategies utilized for system level examination, commonly equipment and programming; practice investigation, taking a gander at the materials and processes used to assemble the chip; and circuit extraction, bringing the chip down to the semiconductor level, and working back up through the interconnects to produce schematics.

Alex Baumgarten et al. [2] manages the need to add reconfigurable-logic obstructions to the data stream. The author presented these impediments can be intensely executed, and furthermore proposes the best situations for them,

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 5, 2021, Pages. 1934 - 1939
Received 15 April 2021; Accepted 05 May 2021.

thinking about their effectiveness and overhead. This paper gives an obstruction implementation analysis, incorporating similitudes with different methodologies, and furthermore assesses the flexibility of this way to deal with attacks.

B. Multiplexer based Approaches

Yu-Wei Lee et al. [3] presentedlogic obfuscation technique by using MUX.By using MUX as selecting boolean logic, the original output are corrupted until the correct key given by the user. The result show the Mux based approach has higher resilient to brute force attack than other methods.

Stephen M. Plaza et al. [4] introduced a multiplexor-based locking approach that conserves test response permitting IC testing by a third party before activation. In this literature, it preventing the counter straight attacks and lower the coverage of wide open circuits to the foundry.

C. Obfuscation Using Keys

Jeyavijayanrajendran et al. [5] have analyzed a insertion of logic gates in circuit as an exponential function and identified best location for placing key gates.

Jeyavijayan Rajendran et al. [6] developed a method for privacy ICs from these attack which is to encrypt the overall circuits by inserting an extra gates. For instance, the exact outputs are changed and it provide original only when selected inputs are used for these gates. In recent logic encryption, the insertion of gates at random into the circuit but does not fundamentally make certain that wrong keys curved the outputs. This method ensures that incorrect keys twisted the outputs. This method activates a designer to controllably corrupt the outputs.

Jarrod A. Roy et al. [7] proposed a End Piracy of Integrated Circuits (EPIC) method. It is the process of that each chip be triggered with an outer key that can only be produced by the owner which cannot be spared. This method is based on robotically-generated chip IDs, inventive use of public-key cryptography and a combinational locking algorithm. In this method, the circuit delay and power is insignificant and the customary flows for confirmation and test do not need change.

D. Logic Locking Methods

Yang Xie et al. [8] have suggested an new logic locking technique by using delay gates. The delay gate used to change the overall circuit delay and power consumption to confuse an attacker.

M Yasin et al [9] presented a lightweight countermeasure that aims at steadily pruning the key. This proposed logic locking method known SARLock, that has merits of the number of distinctive input patterns to recover the secret key. The SARLock stops the SAT attack by representation the attacker effort in the amount of the secret key, while its operating cost grows only linearly.

M Rostami et al. [10] illustrated the modern categorization of threat models, valuation metrics and high-tech defenses for vital hardware-based attacks.

E. Power Consumption Techniques

A.P.Chandrakasan et al. [11] proposed for power consumption technique for digital systems in CMOS. This method engages an optimization at all stages of the model. This technique includes the hardware used to put into practice the digital circuits. The model are implemented the circuits from the uppermost level the techniques are developed.

Issam S. Abu-Khater et al. [12] proposed a CMOS low-power high-presentation multiplier model. In this paper, a new full adder circuits were simulated and fabricated using 0.8- pm CMOS (in BiCMOS) technology. This circuit is compared to the conventional CMOS full adder. Therefore, CPL implementation of the Booth encoder offered more power savings at speed improvement in comparison.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 5, 2021, Pages. 1934 - 1939
Received 15 April 2021; Accepted 05 May 2021.

Kazuo Yano et al. [13] have proposed a Pass-Transistorsbased logic locking approach to prevent a IC from attack.This type of locking increases security at the same time reduces hardware overhead also.

F. Obfuscated Circuits Design Techniques

Yingjie Lao et al. [14] have presentedprotection methodsto secure adigital signal processing (DSP)basedcircuits.It uses finite-state machine (FSM states as key to lock a DSP circuits.The correct state of signal flow used to unlock a original functionality of the circuits.The implementation results show that higher level security than standard locking methods.

Rajat Subhra Chakraborty et al. [15] recommended a fresh design tactics for hardware IP security using netlist-level obfuscation. The projected methodology can be incorporated in the SoC design and industrialized flow to all together obfuscate and validate the design.

Jiliang Zhang. [16] analyzed these hardware security approaches and suggested a realistic logic obfuscation method with low expenditure to prevent a challenger from RE both the gate-level netlist and the layout-level geometry of IP/IC and safe guard.

Conclusion

In this study, the hardware security research had been presented. The current analysis endeavors were additionally expounded on likewise on the grounds that the future patterns during this rising area. This outline gives a reference to hardware security research and ideally, is a straightforward guide for scientists to hitch this region and drive the limit further. Through this paper, we would like to draw in analysts to present a security in QCA based circuits to settle equipment level dangers and, as the last objective, to guarantee the reliability of the "root-of-trust".

References

[1] R.Torrance et al.: “The State-of the-Art in Semiconductor Reverse Engineering,” *IEEE/ACM Design Automation Conference* (2011) 333 (DOI: 10.11452024724.2024805)

[2] A.Baumgarten et al.: “Preventing IC Piracy Using Reconfigurable Logic Barriers,” *IEEE Des.Test. Computer*(2010) 66 (DOI: 10.1109/MT.2010.24)

[3] Y.W.Lee and N Touba, “Improving Logic Obfuscation via Logic Cone Analysis,” *Proceedings Latin-American Test Symposium,* 2015 (DOI: 11.1109/LATW.2015 7102410)

[4] S.Plaza et al.: Solving the Third-Shift Problem in IC Piracy with Test-Aware Logic Locking,” *IEEE Transactions on CAD of Integrated Circuits and Systems,* 34 (2015) 961. (DOI: 10.1109/TCAD.2015.2404876)

[5] J. Rajendran et al.: “Security Analysis of Logic Obfuscation,” *ACM Design Automation* (2012) 83. (DOI: 10.1145/2228360.2228377)

[6] J.Rajendran et al.: “Fault Analysis-Based Logic Encryption,” *IEEE Transactions on Computers64* (2015)410 (DOI: 10.1109/TC.2013.193)

[7] J.Roy et.al.: “Ending Piracy of Integrated Circuits”, *IEEE Computer* 43 (2010) 30. (DOI: 10.1109/MC.2010.284)

[8] Y.Xie and A.Srivastava, “Delay Locking: Security Enhancement of Logic Locking against IC Counterfeitingand Overproduction,” *IEEE/ACM Design Automation Conference* (2017) 91. (DOI: 10.1145/3061639.3062226)

[9] M.Yasin et al.: “SAR Lock: SAT Attack Resistant Logic Locking”, *IEEE International Symposium on Hardware Oriented Security and Trust* (2016) 236 (DOI: 10.1109HST.2016.7495588)

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 5, 2021, Pages. 1934 - 1939
Received 15 April 2021; Accepted 05 May 2021.

[10] M.Rostami, et al: "A Primer on Hardware Security:Models, Methods, and Metrics," *IEEE*102 (2014) 1283 (DOI: 10.1109/JPROC2014.2335155).

[11] A.P.Chandrakasan and R.W.Brodersen, "Minimizing power consumption in digital CMOS circuits", *Proceedings IEEE* 83 (1995) 498 (DOI: 10.1109/5.371964)

[12] I.S.Abu-khater et.al,"Circuit techniques for CMOS low-power high-performance multipliers," *IEEE Journal Solid-State Circuits,* 31 (1996) 1535 (DOI:10.1109/4.540066)

[13] K.Yano et.al.: "Top-down pass-transistor logic design," *IEEE JournalSolid-State Circuits* 31 (1996) 792 (DOI: 10.1109/4.509865)

[14] Y.Lao et.al.: "Obfuscating DSP circuits via high-level transformations,"*IEEE Trans. Very Large Scale Integration(VLSI) system*23 (2015) 819 (DOI:10.1109/TVLSI.2014.2323976)

[15] R.S.Chakraborty et.al.: "HARPOON: An obfuscation based SoC design methodology for hardware protection," 28 (2009) 1493 (DOI: 10.1109/TCAD.2009.2028166)

[16] J.Zhang, "A practical logic obfuscation technique for hardware security," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*," 24 (2016) 1193 (DOI: 10.1109/TVLSI.2015.2437996)