Sabbatical Leave Taken
Fall 2015

Quantum-dot Cellular Automata (QCA) Nano Circuits

Dr. Mohammed Niamat
Professor of EECS
College of Engineering
Sabbatical Report

Period: Fall 2015

Submitted by: Mohammed Niamat, Professor, Dept. of Electrical Engineering and Computer Science, University of Toledo.

The sabbatical was used to perform research in the area of QCA circuits, testing, and hardware oriented security. Some time was also spent to meet several professors and graduate students at the Dept. of Electrical Engineering at the Z. H. College of Engineering and Technology in Aligarh, India, to explore research areas of mutual interest in the area of QCA circuits related to cybersecurity and testing.

The outcomes outlined in the sabbatical application were successfully met and can be judged by the publication of the following papers as a result of the work done during the sabbatical period (fall 2015):

- "Hardware-Oriented Authentication for Advanced Metering Infrastructure", IEEE Transactions on Smart Grids, under second revision

Abstract: This paper introduces a novel authentication scheme for Advanced Metering Infrastructure (AMI) of Smart Grid using Physically Unclonable Functions (PUFs). The scope of the design covers the communication between the utility company (UC) and the smart meter (SM) network. The scheme is based on hardware-oriented security and can be connected to existing smart meters. Authentication keys of 64 bits are used for security level 1 (L1). The size of keys can increase up to 1024 bits for level 5 (L5). Though the length of the key is short, it does not compromise the security. The PUF used in this scheme is
extremely difficult to model by adversaries as each authentication key is used only once. The authentication key is generated from the response using hamming code. The design of the scheme ensures fault tolerance as Ring Oscillator (RO) comparison pairs with high frequency differences are selected to prevent bit flips and only 10% discrepancy is tolerated. The proposed scheme has high efficiency in terms of latency and data storage. As a proof of concept, two different machine learning algorithms, Support Vector Machine (SVM) and Multigene Genetic Programming (MGGP), are used to show that the PUF cannot be modeled by adversaries.


Abstract - Silicon Physically Unclonable Functions (SPUFs) are delay based PUFs that exploit stochastic manufacturing process variations of Integrated Circuits (ICs) on silicon chips to construct unclonable cryptographic secret keys which are unique for each chip. One variant of SPUFs, named Ring Oscillator (RO) PUFs, is typically used for the authentication of silicon technology devices including FPGA chips. Prior research on the area of ROPUF shows that RO frequencies are affected by spatial systematic process variations and hence the generated responses are not statistically random. In addition to the negative effects of systematic variations on overall ROPUF performance, reduced randomness in the generated responses can lead to major hardware security threats. In this paper, Logarithmic and Absolute Diverseness Technique (LDT), a novel security technique based on base-10 logarithm and square root of RO deviations from the global RO mean, is proposed to nullify the effects of spatial systematic variation on the response bits of a unique reconfigurable ROPUF design (r-ROPUF) and improve the reliability of the structure. The proposed technique is implemented on the data obtained from 30 Spartan 3E FPGA chips. IBM-SPSS statistical software is used to demonstrate the transformation of RO frequencies to statistically normal frequencies with high reliability through the implementation of the proposed technique. Additionally, it is shown via MATLAB simulation that the technique nullifies the effects of spatial systematic variation on the average RO frequencies extracted from four different r-ROPUF structures. Finally, the response bits generated from each r-ROPUF structure successfully passed the entire National Institute of Standards and Technology (NIST) statistical tests for randomness and exhibited true randomness and higher reliability compared to earlier techniques.

• "A Dynamic Area-Efficient Technique to Enhance the Security of ROPUFs against Modeling Attacks," The 15th International Conference on Security and Management (SAM'16), Las Vegas, July 25-28, 2016, under review

Abstract - Physical Unclonable Functions (PUFs) are the state-of-art topic of hardware oriented security and trust. Ring Oscillator PUFs (ROPUFs) are promising primitives for the security of silicon technology chips including ASICs and FPGAs. Despite the prevalence of numerous techniques for fabrication of ROPUFs, to the best of our knowledge, a well-
established dynamic technique that can provide updated secret keys to improve ROPUF security against modeling attacks does not exist. In this paper, an area-efficient technique that exploits an appropriate reconfiguration mechanism and utilizes dedicated FPGA resources to build a dynamic multi-stage ROPUF (d-ROPUF) structures is introduced. To determine the correlation between each structure and its performance, the normality of the generated RO frequencies is studied. Experimental results show that a structure with fewer stages has higher performance in terms of variability and diverseness. Statistical characteristics of the response bits are studied at normal and varying temperature and voltage variations in order to validate the performance of the proposed technique in terms of uniqueness, uniformity, bit-aliasing, and reliability. Our results show that the d-ROPUF exhibited excellent uniqueness, uniformity, bit-aliasing, and reliability at varying operating conditions.


Abstract- Silicon Physical Unclonable Functions (SPUFs) are security primitives that are embodied in a chip and exploit the manufacturing process variations of the Integrated Circuits (ICs) to extract unique secrets for chip authentication and cryptographic key generations. Due to their simple implementation and high performance, Ring Oscillator PUFs (ROPUFs) are one of the most suitable security solutions for silicon technology devices including ASICs and FPGAs. As far as our knowledge goes, there is no comprehensive research that assesses the impact of varying environmental conditions on the performance of controlled-inverter Configurable ROPUFs (c-ROPUF). In this paper, we use our previously proposed c-ROPUF design to analyze RO sample frequencies that are extracted from five Spartan 3E FPGAs (90 nm) at five different temperatures & voltages. The experimental results show that RO frequencies follow a fixed pattern which shows that environmental variation effects are uniformly distributed on the individual ROs throughout the FPGA chips. However, RO frequencies are exposed to high bit flips percentage due to voltage variations compared to temperature variations.

"Physical Unclonable Functions for Hardware Oriented Security and Trust," The 7th Annual Midwest Graduate Research Symposium (MGRS), Toledo, OH, April 9th, 2016, presented by graduate student

The next step would be to convert the techniques presented in these papers to the QCA equivalent circuits. The material will also form the groundwork for submitting a research grant in the area of cybersecurity to the CISE Directorate of NSF. Also, the work done in the area of cybersecurity for smart meters is currently being submitted to the NSF I-Corps program for possible commercialization of the product.
The International Technology Roadmap for Semiconductors (ITRS) predicts the size limit for CMOS technology to reach 5 nm to 10 nm by 2017. This trend of down scaling in transistor size has long obeyed Moore's law, which states that the number of transistors integrated on a chip of unit area will double approximately every 18 months. To handle this exponential growth curve of device density and increased processing power, there has been a pressing need for rapid improvements in all aspects of integrated circuit (IC) fabrication. At gate lengths below 0.1 mm, FETs will begin to encounter fundamental problems where the quantum effects begin to dominate the device performance that make further scaling difficult due to the following major reasons:

- As the channel length decreases, the thickness of the oxide layer decreases which results in an increase in the gate leakage current caused due to electron tunneling. This quantum mechanical phenomenon causes an increase in the power consumption as the channel length scales down.

- As spacing between interconnects decreases, capacitive coupling increases. This causes an increase in delay for the signal to traverse through interconnects which degrades the system performance.

Thus, there is need for new technologies that can overcome these limitations. Researchers are investigating for alternatives to CMOS technology at nano scale like carbon nanotube field effect transistors, nanowires, single electron transistors, quantum cellular automata and spin transistors. Amongst the alternatives being considered, quantum-dot cellular automata (QCA) technology has emerged as one promising transistor-less technology which may
replace CMOS circuits in the future. QCA circuits, comprising of quantum cells, transfer information from one cell to the other due to the coulombic interactions between the electrons. Since there is no actual cmTent flow, QCA architectures can achieve low power dissipation of 100W/cm² with greater device density (10¹² devices/cm²) at Terra Hz operating speed. The advantage of QCA lies in its extremely high packing density possible due to the small size of the dots, simplified interconnections, and extremely low power consumption.

Research Objectives

FPGAs present an attractive application of QCA as they are well suited for fabrication due to their homogenous structure. Standard QCA cells are used to model the configurable logic block (CLB) of the FPGA. The CLB has more than one look-up table (LUT). A 5-input LUT is designed which emulates a Viiix-5 Xilinx FPGA architecture. The CLB of Virtex-5 architecture has two slices each containing four LUTs.

The proposed research is divided into the following two phases:

I. Design, modeling, implementation and simulation of various FPGA components in QCA technology.

The CLB components that were designed, modeled and simulated in QCA are:

- Decoder
- Memory Array
- Multiplexer
- Flip Flop
The first three components listed above are integrated to form a LUT. The LUTs are integrated with Flip Flops (FF) to form a complete slice of CLB of an FPGA. Standard QCA cells are used for generating the physical layouts of the components. All the physical layouts of the components are simulated using the QCA Designer tool. The CLBs are tested by implementing boolean equations and verifying the simulations with their expected outputs. A detailed analysis of the proposed architecture has been discussed.

2. Design, modeling, implementation and simulation of testing strategies and fault analysis in QCA.

A built-in self test (BIST) model is designed, modeled and implemented at the quantum level. The components of the BIST model are:

- Test Pattern Generator
- Output Response Analyzer

The simulations of the components are verified with the expected outputs. The designed BIST model is incorporated in the CLB tested for various faults.

QCA represents a new technology at the nanotechnology level. It was first introduced by Lent et al. which offered a new potential paradigm shift in computing. Unlike conventional technologies which use voltage or current to represent the binary values, QCA uses the position of the electrons in a cell to represent binary values. QCA technology has inherent features like high device density \(10^{12} \text{ devices/cm}^2\), higher operating speed (high clock frequency, usually in the range of Tera Hz) and lower power consumption \(100 \text{ W/cm}^2\).
The standard QCA cells have four quantum dots and two electrons. There are various kinds of QCA cells proposed which include a six-dot QCA cell and an eight-dot QCA cell. The six-dot and eight-dot are still in their developing stages therefore, the standard four-dot QCA cells are used for generating physical layouts throughout this research. The figure on next page illustrates the standard QCA cell with four dots and two electrons. The two electrons in each cell are free to tunnel within the cell but they are bounded by the cell boundary. The two electrons in the cell repel each other to occupy diagonal cells.

QCA is an array of nano-electronic device cells where the information transmission and processing is purely due to the coulombic mechanism unlike other conventional technologies where information is transferred by electric current. Figure below shows the cell geometry and it also indicates the tunneling energy between the ground state and any one of the stable state designated by 't'.

Quantum dots are small semi-conductors or metal islands with a diameter small enough to make their charging energy greater than 'kB T' (where 'kB' is Boltzmann's...
constant and 'T' is the operating temperature). Exactly two mobile electrons are loaded in the cell which can move to different diagonal quantum dots within the QCA cell by means of electron tunneling. Electron tunneling is assumed to be controlled by potential barriers (that would exist underneath the cell) that can be raised and lowered between adjacent QCA cells by means of capacitive plates. Apart from the two states discussed above, there is another 'unpolarized' state in which the cell has little or no polarization. In such a state, the inter-dot potential barriers are lowered which reduces the confinement of electrons in the quantum dots.

Thus QCA cells perform the computation by coulombic interactions with its neighboring cells to influence each other's polarization. The following section reviews the clocking scheme in QCA before proceeding to some simple, yet essential, QCA logic devices: QCA wires, majority gate and inverters.

Clocking in QCA

Timing, in general, is controlled through a reference signal (i.e., a clock) and is mostly required for sequential circuits. Timing in QCA is accomplished by clocking in four distinct and periodic phases that are needed for both combinational and sequential circuits. Clocking not only provides the control for information flow but also controls the true power gain in QCA. The signal energy lost to the environment is also restored by the clock. 'Clocking' is a very important parameter in QCA design.

Abrupt switching and adiabatic switching are the two types of switching methods in the operation of QCA:
• **Abrupt Switching:** When the inputs to the QCA circuit change suddenly, the circuit would be in some randomly excited state which is unpredictable. Therefore, the QCA circuit has to be relaxed to ground state by dissipating energy. This inelastic relaxation is uncontrolled and the QCA circuit might enter a meta-stable state that may be determined by a ground state.

• **Adiabatic Switching:** In this kind of switching, the system is always kept in its instantaneous ground state. A clock signal is introduced to ensure adiabatic switching. This is the preferred method of switching.

For QCA, the clock signals are generated through an electric field, which is applied to the cells to either raise or lower the tunneling barrier between dots within a QCA cell. This electric field can be supplied by CMOS wires, or CNTs buried under the QCA circuitry. Depending upon the strength of the electric field applied to a QCA cell, the QCA cell has two distinct polarizations. One of the methods for clocking was proposed by K. Hennessy et. al. where conducting wires were used below the plane of the QCA molecules to generate a suitable electric field. The schematic representation of this idea is shown in the figure. The QCA cells are spread across the XY plane and the Y plane consists of a series of conducting wires just below the plane of the QCA cells. The conducting wires are excited to produce electric fields by applying suitable voltage. A conductor placed above the QCA cells is grounded so that it draws the electric field in the Z direction. The state of the QCA cell is affected only by the component of the electric field. The component does not affect the state of the QCA cell and the component is zero due to symmetry. Time varying voltages are applied to the conducting wires in such a way that two adjacent wires have a phase shift of \( \pi/
2 radians between them. This configuration ensures that every fourth wire will have the same applied signal. When the barrier is low, the cells are in a non-polarized state; when the barrier is high, the cells are not allowed to change state. Adiabatic switching is achieved by initially lowering the barrier, removing the previous input, applying the current input and then raising the barrier. If transitions are gradual, the QCA system will remain close to the ground state.

Modified Schematic Model to Represent Clocked QCA Array

In a QCA circuit, information is transferred and processed in a pipelined fashion and a multi-bit information transfer for QCA is allowed through signal latching. All cells within the same zone are allowed to switch simultaneously, while cells in different zones are isolated. This pipelined information transfer is illustrated in the figure. QCA has four different clocks and each clock is represented in a different color shown in the figure below. Clock 0, 1, 2 and 3 are indicated by the colors green, pink, blue and white, respectively. The
assignment of clock should be in the same order i.e. clock 0, clock 1, clock 2 and clock 3.

When the clock is applied to the QCA circuit, all the cells in that particular clock zone attains a stable state depending on the driver and all the remaining QCA cells in other clock zones are in a ground state. This is indicated in the figure, where the electrons in stable state are highlighted and the ground state is indicated by the presence of dots only.

Information Transfer in a Clocked QCA Binary Wire

QCA clock has four phases (switch, hold, release, and relax) and each phase acts as a potential that modules the inter-dot barriers of all the cells in that phase. For effective information flow, array of QCA cells can be divided into sub-arrays of different clock phases. The next figure illustrates the polarizations in the QCA cell during the four phases of the clock. During the 'switch' phase of the clock, the unpolarized QCA cells polarize in
accordance with the driver cell, the cells maintain their polarization for the duration of the 'hold' phase. The 'release' phase of the clock releases the inter-dot barriers and the cells tend to gradually lose their polarization, and continue to stay in an unpolarized state in the 'relax' phase.

Phases of a QCA Clock.

QCA Logic Devices

A driver of a QCA cell could be an input device such as a nanotube, a very thin wire or a tip of a scanning tunneling microscope (STM). In semiconductor QCA, a standard technique called "plunger electrode" has been used to alter the electron occupancy of the input cell. Reading the output state of a QCA cell is difficult, because the required measurement process should not alter the charge of the output cell. Electrometers made from ballistic point-contacts, the STM method, and SET electrometer have been used to read the output. There are two configurations of fabricating the QCA cells: Standard QCA cells and 45° Rotated QCA cells. As the information in QCA is transferred due to coulombic interactions between the two corresponding QCA cells, the state of one cell influences the state of the other corresponding cell. The various kinds of QCA logic devices are:
• Binary Wires

• Majority Voter

• Inverter.

Binary Wires

The QCA cells tend to align to the polarization of its neighbors. Therefore, a linear arrangement of cells can be used as a wire to transmit information. An example of QCA wire is shown in the figure below, and its simulation is shown in the next figure. It can be observed that the binary wire is divided into various clock zones. This is done to ensure that the signal strength carried by the wire is not degraded, as the signal strength tends to deteriorate with a long chain of QCA cells in the same clock zone.

The other kind of QCA wire is termed as the "Inverter chain". In the inverter chain, the standard QCA cells are rotated by 45° in vertical or horizontal orientation. The polarizations in such QCA cells tend to align opposite to the corresponding QCA cell. Figure below shows the inverter chain representation and the next figure shows the QCA layout. The simulation is also shown.
Majority Voter

Majority Voter (MV) is one of the logic gates in QCA. The logic function implemented by the MV is \( f(A, B, C) = A \cdot B + B \cdot C + C \cdot A \). The logic of the MV is implemented by the five QCA cells indicated in the figure. The QCA layout is shown in the figure below. The QCA cell present at the centre of the gate is called the decision making cell which tends to polarize to the majority of the inputs. The QCA simulation of the MV is shown in the next figure.
QCA Simulation of Majority Voter

By fixing the value of one of the three inputs to logic 'O' or logic '1', the MV can be programmed as an AND gate or an OR gate, respectively. The logical functions of AND gate and OR gate are shown in Equation 1.1 and Equation 1.2.

\[
\text{MV}(A, B, C) = A \cdot B \text{ when } C = 0 \tag{1.1}
\]

\[
\text{MV}(A, B, C) = A + B \text{ when } C = 1 \tag{1.2}
\]
The figures below show the representation of AND gate and OR gate, respectively. The QCA implementation of AND gate and OR gate are also shown.

(a) AND Gate Representation. (b) QCA Layout of AND Gate

QCA Simulation of AND Gate
Molecular QCA

A simpler representation of QCA logic gates can be implemented using molecular QCA which not only yields greater performance but can also operate at room temperatures. In molecular QCA, cells are structurally homogeneous down to the atomic level. The molecular QCA cells are implemented using a class of compounds called 'mixed – valence compounds' which exhibit a unique property of having multiple redox centers in different oxidation states. Each molecule functions as a QCA cell and the redox centers function as quantum dots where the information is encoded with charge configuration and the tunneling
junction provided by bridging ligands shown in the figure below. The transfer of electronic charge from one molecule to its neighboring molecule is through quadrupole to quadrupole interactions. The coulombic energies should be in the range of 0.2 – 0.5 eV for the model to operate at room temperature].

To find the response functions of a model, the quadrupole moment of a single molecule should be interpolated between the states 'O' and 'I'. The Scrodinger's equation is used to evaluate the value of the output molecule.

Molecular Implementation of a QCA Cell

The logic states can be defined by using the ally! group shown in the figure. The state with a positive dipole moment is represented as logic 'I' and the state with a negative dipole moment is represented as logic 'O'. The alignment for logic 'I' is such that an unpaired electron is on the bottom ally! group and a positive charge is on the top ally! group. On the other hand, the alignment for logic 'O' is such that the bottom ally! group has a positive charge and the top ally! group has an electron.
Molecular QCA devices offer certain advantages over the other implementation models with respect to area, power dissipation and information transfer rates. Implementation of molecular QCA devices reduces the cell size to approximately 1nm x 1nm. Experiments conducted by Lent and Timler have proved that, if clocking is considerably slowed down, the reversible processes can be implemented with ultralow power dissipation. For the information to be transferred without any loss of data, the molecular QCA devices should be able to switch between 'O' and '1' fast enough to cope with the clock. It has been reported that the transfer rates of the mixed valence compounds used in molecular QCA have switching times between 10 s and 13 s.

Molecular QCA presents unique challenges such as bonding of the array surface which requires treating the existent strongly bound, chemically robust and mixed valence complexes in chemistry with the use of complex stereoscopic and electro-chemical techniques.
Mobile chargers are created by chemical oxidation or reduction shown in the figure below. Molecules are suitable for the implementation because they act as natural and uniformly small quantum dots with high density that are suitable for room temperature operations.

Molecular Form of QCA cell

Magnetic QCA

This concept was introduced by Cowburn and Welland, who demonstrated the operations of magnetic QCA (MQCA) using an array of disk shaped particles, with a diameter of 110nm, that exhibit collaborative behavior. In magnetic QCA, magneto static interactions between nano particles ensure that the system is bi-stable. The moments of nanoparticles are either parallel or anti parallel to the axis of the chain. The information is propagated via magnetic interactions as opposed to the electrostatic interactions in metal and molecular interactions.