

A review on quantum utility for secure authentication protocol towards cryptographic standard in quantum dot cellular automata

Suparba Tapna *

*Department of Electronics & Communication Engineering
Brainware University
Barasat 700125
West Bengal
India*

Kisalaya Chakrabarti [†]

*Department of Electronics & Communication Engineering
Haldia Institute of Technology
Haldia 721657
West Bengal
India*

Debarka Mukhopadhyay [®]

*Department of Computer Science and Engineering
CHRIST (Deemed to be University)
Bengaluru 560029
Karnataka
India*

Abstract

QCA, which stands for Quantum Dot-Cellular Automata, is a nanotechnology model that offers an alternative solution to the widely used CMOS technology. Unlike CMOS, QCA is a semiconductor-less technology that transmits information based on the charge of electrons and the electrostatic repulsion between them. This technology provides several advantages over CMOS, including higher device density, faster switching speed, and lower power consumption. When it comes to cryptographic applications, QCA circuits can be extremely useful. Both encryption and decryption processes can be implemented using

This article has been corrected with minor changes. These changes do not impact the academic content of the article.

* E-mail: suparba7@gmail.com (Corresponding Author)

[†] E-mail: kisalayac@gmail.com

[®] E-mail: debarka.mukhopadhyay@gmail.com

logic circuits based on QCA. The research paper describes a basic method for generating ciphertext in QCA, which is useful in secure nano communication based on QCA. The paper discusses how to achieve secure authentication in encrypted communication using QCA. To evaluate the performance and test the proposed method, the researchers used the QCA Designer-2.0.3 tool. This is a software tool specifically designed for designing and simulating QCA circuits. It enables researchers to model and analyze the behavior of QCA-based systems, allowing them to evaluate the effectiveness and feasibility of their proposed encryption technique. Overall, the research paper aims to present a secure encryption method using QCA and demonstrates its implementation and testing using the QCA Designer-2.0.3 tool. By leveraging the unique properties of QCA, such as high device density and low power consumption, the researchers aim to provide a novel approach for secure nano communication and cryptographic applications.

Subject Classification: 35K57, 58D19.

Keywords: Cipher, Quantum dot cellular automata (QCA), Clocking scheme, Mux and De-Mux, Parity, Majority gate, PRBS, Schrodinger, Quantum enhancement security level to optimized entanglement states, n value.

1. Introduction

QCA is an alternative to the semiconductor-based CMOS system, which offers higher device density, faster timing frequency, and lower power consumption compared to CMOS. The references cited provide further information supporting the claims about the limitations of CMOS and the advantages of QCA. QCA provides the opportunity to transmit electron charges through Quantum Dots, independent of electrical energy or clock pulses. Cryptography plays a significant role in securing and transforming real data into encrypted, non-discernible form[1]. The article describes a simple method for generating ciphertext using QCA. The manuscript follows a structured outline including an overview of QCA technology, discussing the clocking mechanism in QCA circuits, exploring the application of QCA in secure nano communication, introducing PRBS and its relevance, addressing the topic of reducing bit error rate in channel coding [2], presenting the results obtained from simulations, and concluding the research work. The references cited provide further details and related research on the specific topics discussed in the article.

2. QCA Overview

The text discusses using Quantum Dot Cellular Automata (QCA) to construct a nanotechnological paradigm suitable for a proposed approach. Figure 1(a) shows a QCA cell with four dots [3, 4] connected by burrowing

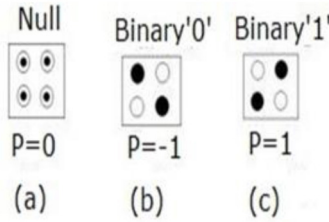


Figure 1

Cell Polarization of different QCA

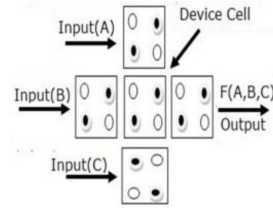


Figure 2

Realization of Majority Gate for Predicted O/P

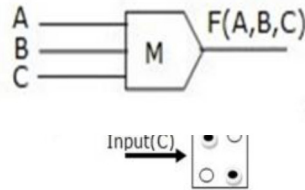


Figure 3

Realization of Majority Gate for Predicted O/P

wires. Two free electrons in antipodal conditions result in two QCA cell polarizations: $P=+1$ and $P=-1$, representing binary logic of '1' and '0'. $P=0$ indicates a null cell with no data. A three-input majority gate is a fundamental logic gate used in Quantum-dot Cellular Automata (QCA), which operates based on the majority gate of the input data. Figure 1 provide details regarding cell polarization of different QCA and Figure 2 and 3 provide information regarding realization of predicted output respectively.

$$F(A,B,C) = AB+BC+CA \quad (1)$$

If we fixed its contribution estimation to logic values '0' as well as '1', at that point rationale AND- gate or potentially entryway may be formulated individually[4] composed as:

$$F(A,B,0) = A.B \quad (2)$$

$$F(A,B,1) = A+B \quad (3)$$

Table 1 provide details of Truth Table of Majority Voter Gate. QCA wires transmit data within a QCA circuit through electrostatic

Table 1
Truth Table of Majority Voter Gate

A	B	C	F(A, B, C)
0	0	0	0
0	0	1	0
0	1	0	0
0	1	1	1
1	1	0	1
1	0	1	1
1	1	0	1
1	1	1	1

communication among QCA cells. There are two types of QCA wires: 90° QCA wire and 45° QCA wire. In 90° QCA wire, the polarization remains the same throughout the entire QCA exhibit, while in 45° QCA wire, the polarization changes in each consecutive cell in the cluster. A QCA inverter can be formed by placing QCA cells at a 45° angle. QCA timing has four stages, each with a delay of $\pi/2$, providing a new way to design nano-circuits different from CMOS circuits. The switch stage increases the boundary between QCA cell dots, energizing the QCA cell through electron tunneling. The hold stage maintains the cell's current status. The release stage lowers the resistance between dots, allowing the electron to tunnel through the dots and unexciting the QCA cell. The relax stage maintains the lowered resistance, and the cell remains unexcited.

3. Literature Survey

The transmission of data involves issues of security. In the article "Cryptographic Models of Nano communication Network Using Quantum Dot Cellular Automata", the authors Bikash Debnath, Jadav Chandra Das, and Debashis De [4] explain that the devices that perform the encoding and decoding are known as the encoder and decoder. However, there are challenges to developing such devices, including circuit complexity and power distribution at the nanoscale level. To address these challenges, reversible logic with Quantum Dot Cellular Automata (QCA) is proposed as a promising alternative to traditional semiconductor-based devices. QCA has high protection against side-channel attacks, particularly from power analysis attacks. Researchers have explored several QCA-based cryptographic models for secure data transmission, examining the current QCA-based circuits for cryptographic engineering in terms of circuit

complexity, device area, and operating speeds. The article “Cryptography in Quantum Cellular Automata” by Mohammad Amin Amiri, Sattar Mirzakuchaki, and Mojdeh Mahdavi discusses the use of QCA technology for implementing logic circuits. QCA cells have quantum dots in which the position of electrons determines the binary degrees of 0 and 1. This is a significant feature of QCA against traditional logic in which logical states are stored through voltage levels. The article “Design and Analysis of QCA Cryptographic Circuits” by Mansi Rana and Mr. Ajay Dagar describes a model in which the total capacity of QCA circuits is divided into two main parts, leakage power and switch power. In recent studies, many more efficient QCA designs have been developed, including QCA devices logic circuits using select or gateways switch gates and various alternative QCA wiring approaches, as well as the design of the memory cell as an important component in QCA devices. The article “Hardware Security based Quantum Dot Cellular Automata Circuit Design” by M. Amutha and K.R. Kavitha discusses the potential of Quantum Cell Automata (QCA) as a promising alternative to traditional VLSI-based IC technology, which is a combination of logic models. While the design of each of these circuits has been outlined separately, the overall design still needs improvement.

4. Motivation

In the field of nanotechnology, the main aspect to consider for secure nano-communication is the different observation for standard implication using Quantum Dot Cellular Automata(QCA). The thermodynamic effect for adjacent QCA cell is the most important factor and a significant achievement through the implementation of security enhancement protocol in quantum-inspired phenomenon.

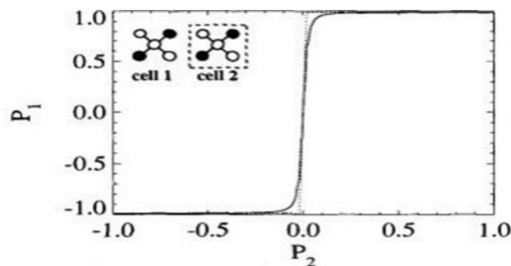


Figure 4

Thermodynamic Behavior of a QCA Cell

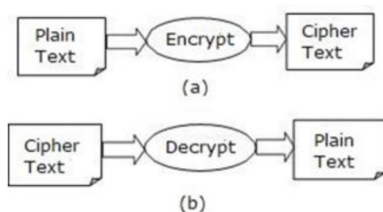
“The QCA worldview relies on the cluster reaching its ground state to achieve the desired outcome. However, at non-zero temperatures, the system may deviate from the ground state and produce a warm average of correct and incorrect outcomes. Due to the absence of power rails to maintain cells away from their thermodynamic equilibrium state, warm effects can be detrimental to the design at high temperatures. Imagine a “standard” QCA cell with the aspects and boundaries described in Ref. [6]. The quantum dots in the cell are separated by 20nm, and the material boundaries are those of GaAs with a dielectric constant of 10. When two adjacent cells with polarization P2 drive the cell, a slightly different response curve than that shown in Figure 4 is generated, resulting in the polarization of the cell, P1. This response capability P1(P2) is advantageous because a line of cells will align with a polarization value given by the appropriate position of repeated cycles of this response curve”[7].

5. Evaluation of Performance Indexes of QCA-based Cryptographic Standard

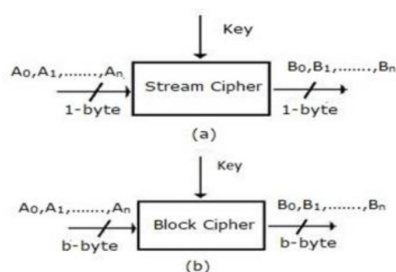
The assessment file for the hybrid energy system is crucial for improving the system’s performance. It mainly affects the results of the development objective capability. There are currently three commonly used records, namely financial, energy, and climate-related files, and their combination. With the increase in the use of renewable energy in the system[8], it is essential to improve the reliability and flexibility of the system, and hence, the associated performance assessment record has gained more attention recently[9].

6. Assumption of dynamic features & uncertainty in optimization technique

The portrayal of a framework has a significant impact on the design improvement model and its development outcomes. However, most of the current design enhancement studies overlook the vulnerability and dynamic qualities of the framework while portraying it. This treatment may not significantly affect the results for cross-breed frameworks that do not contain sustainable power. But, for frameworks with sustainable power sources, ignoring vulnerabilities and dynamic attributes may lead to significant deviations in the system’s design outcomes. This chapter is essentially divided into two aspects: taking into account vulnerability and taking into account dynamic attributes[10,11].

**Figure 5**

Encryption System and Decryption System

**Figure 6**

QCA Stream Cipher and QCA Block Cipher

7. Secure Nanocommunication using QCA and relevant Schrodinger Concept

Ensuring secure communication is crucial for data privacy. Nowadays, it is imperative to consider more authenticated ways of sharing information between senders and receivers. In this proposed technique, channel coding is used in a nano communication network to address the same kind of assumption phenomenon.

Cryptography encodes messages to provide security against unauthorized access. Encryption converts messages into unrecognizable codes, while decryption reverses the process. In symmetric key cryptography, plain text can be encrypted in two ways: stream code and square code. Each byte is encrypted with the key in the Figure 5, and the plain text is encrypted on a block figure in a square of bytes, all with the key shown in Figure 6.

We propose using a 1-bit PRBS generator to secure a nano communication network. The generator produces a pseudorandom binary sequence used as a key in channel coding applications. To reduce the bit error rate, we can decrease transmission capacity. Channel coding can recover from errors during transmission. The BER data is the number of decoded bits still having errors after error correction, divided by the total number of decoded bits. Finally, every electron molecule traveling through the passage carries on the collectively of waves. Figure 7 and 8 shows the Schrodinger 2D wave equation for 1st approach for $n = 3$ and 4 respectively.

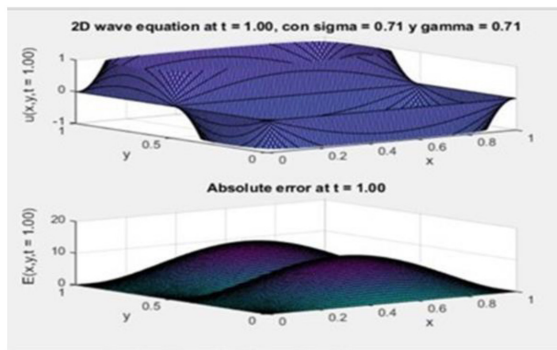


Figure 7

Schrodinger 2D wave equation for 1st approach($n=3$) of Quantum number

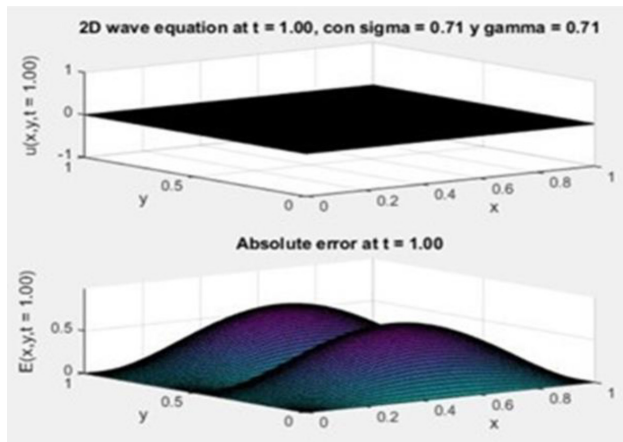


Figure 8

Schrodinger 2D wave equation for 1st approach($n=4$) of Quantum number

8. Discussions and Conclusions

The Bistable QCA Designer2.0.3 game engine was used to execute the circuit, and yield was obtained using the pinboard. The proposed circuit can guide the creation of a secure QCA encryption module due to its low force usage and fast time rates. Encryption and decryption can be performed on any length of the message bit as well as key material. This cryptographic approach can improve authentication and encryption in nano communication networks with Pseudo-Random Binary Sequence (PRBS). In the future, cryptographic calculations for a secure nano-

matching framework based on QCA can be performed using this proposed approach.

References

- [1] M. Niemer, P. Kogge, Problems in designing with qcas: Layout = timing, *Int. J.Circuit Theory Appl* 29, 49–62 (2001).
- [2] S. Umira, R. Qadri, Z. Bangi, M. Banday, G. Bhat, A novel cryptographic design in quantum dot cellular automata, 1–6 (2018).
- [3] Kumar, Ankit, et al. "An improved quantum key distribution protocol for verification." *Journal of Discrete Mathematical Sciences and Cryptography* 22.4 : 491-498 (2019).
- [4] B. Debnath, J. Das, D. De, S. Mondal, A. Aumadian, M. Salimi, M. Ferrara, Security analysis with novel image masking based quantum-dot cellular automata information security model, *IEEE* 8, 117159–117172 (2020).
- [5] K. Navi, S. Sayedsalehi, R. Farazkish, M. R. Azghadi, Five-input majority gate, a new device for quantum-dot cellular automata, *Comput. Theor. Nanoscience* 7, 1546–1553 (2010).
- [6] P. Singh, A. Majumder, B. Chowdhury, R. Singh, N. Mishra, A novel realization of re-versible lfsr for its application in cryptography, 601–606 (2015).
- [7] M. Amiri, M. Mahdavi, S. Chaki, Qca implementation of a5/1 stream cipher, 48–51 (2009).
- [8] Kumar, Ankit, et al. "An enhanced quantum key distribution protocol for security authentication." *Journal of Discrete Mathematical Sciences and Cryptography* 22.4 : 499-507 (2019).
- [9] Quantum cryptography-A modern approach, Salabh Rai, Ayush Kumar Upadhyay, Divyank Sharma, Dharm Raj, Ajay Kumar Gupta, Danish Ather, *Journal of Discrete Mathematical Sciences & Cryptography*, Vol. 26, No. 7, pp. 1991–2006 (2023).
- [10] A. Ciarlo, Exploring the potential of threshold logic for cryptography related operations, *IEEE Transactions on Computer* 60, 452–462 (2011).
- [11] A unified description of cryptosystems: From classical to quantum protocols, Giuseppe De Riso, Marialaura Noce, *Journal of Discrete Mathematical Sciences & Cryptography*, Vol. 26, No. 8, pp. 2285–2299 (2023).