Microprocessors and Microsystems 45 (2016) 32–44

Contents lists available at ScienceDirect

Microprocessors and Microsystems

journal homepage: www.elsevier.com/locate/micpro

A novel pseudo random number generator based cryptographic architecture using quantum-dot cellular automata

Tamoghna Purkayastha[a], Debashis De[a,b,*], Kunal Das[c]

[a] Department of Computer Science and Engineering, West Bengal University of Technology, BF-142, Sector I, Salt Lake City, Kolkata, 700064, India
[b] School of Physics, The University of Western Australia, 35 Stirling Highway, Crawley, Perth, Western Australia 6009
[c] Department of Computer Science and Engineering, National Institute of Technology, District Papum Pare, Yupia, Arunachal Pradesh, India 791112

ARTICLE INFO

Article history:
Received 14 October 2015
Revised 21 January 2016
Accepted 1 March 2016
Available online 17 March 2016

Keywords:
PRNG
QCA
QCA-tile
Majority voter
Hardware cryptography

ABSTRACT

Pseudo random number generator (PRNG) based hardware cryptographic architecture is presented in quantum-dot cellular automata (QCA) technology. Major achievement is the production of cipher texts using random number generator instead of fixed keys. The random ciphers thus generated reduce the detection probability. A novel algorithm for cipher text design has been provided in this paper. In a bottom-up approach, we have designed all the architectural components which include QCA based XOR block, 4-bit Counter, 4 to 16 Decoder, Memory Elements and two PRNG blocks. Finally a synchronized integration of the individual components led to the generation of a novel cryptographic architecture. This design has achieved two layers of security. First layer is ensured by the encryption scheme, which has been achieved by the PRNGs and XOR block and the second layer is achieved by a Permutation Block at the transmission end. An effective and innovative cryptographic scheme compared to the existing works is proposed here.

1. Introduction

Quantum-dot cellular automata (QCA) is turning out to be a strong alternative of CMOS based technology. Since its inception by C.S. Lent and co-workers in [1–2] a number of architectural logics have been implemented in QCA [3–10]. Apart from all the benefits that QCA possess, i.e. low power consumption, high speed of operation up to tera hertz frequency, QCA continued to suffer from a serious issue. Particularly, the room temperature fabrication of QCA cell. But very recently Dilabio et al. [11] fabricated QCA cell which is operable in and above 293 Kelvin. This invention acts as a big motivation for future implementation of QCA based circuits.

In the past decade, side channel analysis (SCA) attack based on power analysis have become a significant threat to CMOS based cryptographic circuits [12,13]. In case of power analysis attack, the attackers can reveal the secret key from the measurements of the power consumption of the circuit during its encryption and decryption process. QCA could be of significant benefit in cryptography as there is no current flow in QCA circuits. Liu et al. [14] provided an interesting insight in this issue. The authors in [14] have performed both worst-case and best-case scenario of SCA attack prevention using QCA based cryptographic circuits and concluded that QCA could be an attractive alternative to combat power analysis attack in the future computing. Several QCA based cryptographic circuits have been designed so far [14–18]. The existing works primarily focus on designing QCA based serpent blocks and QCA based cryptographic processor with fixed keys. Having fixed keys or lesser combination of keys will not be beneficial as the keys can be easily cracked by the attackers. It is necessary to produce random sequences to achieve less vulnerable ciphers because of its dynamic nature. It would be less predictable to any intruder as the key pattern is not fixed for the entire communication and varies in different instances of time. Random Sequence Generators are thus a valuable part of cryptographic architectures.

The basic advantages of using random number based cryptography are as follows:

1 Generation of unpredictable random number key for secure communication [19–22].
2 Pseudo-random numbers are important in practice for their speed in number generation and their reproducibility, and they are thus central in applications such as simulations, e.g., of physical systems with the Monte Carlo method, in cryptography, and in procedural generation.
3 Cryptographic applications require the output to be unpredictable which is obtained by using this PRNG. One such

* Corresponding author. Tel.: +91-9830363215.
E-mail address: dr.debashis.de@gmail.com (D. De).

http://dx.doi.org/10.1016/j.micpro.2016.03.001
0141-9331/

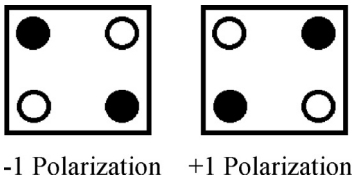

Fig. 1. QCA cell polarizations.

example includes Vernam cipher [20] where a truly random cipher can be generated.

4 Finally the proposed PRNG based cryptography also guarantees the following characteristics:
   - Confidentiality
   - Integrity
   - Non-repudiation
   - Authentication

Keeping this in mind in this paper, we have proposed the concept of hardware cryptography in QCA technology. Following are the contributions of the proposed work:

1 Cipher text generation of 8-bit data streams has been implemented.
2 Two layer of security has been achieved.
3 The 1st layer is the random sequences of key are generated to achieve less vulnerable ciphers because of the dynamic nature. This is achieved by Random Sequence Generators which act as a vital part of the proposed cryptographic architecture. The derived key sequences are used to encode the incoming data stream to create cipher texts. It would be less predictable to any intruder due to random key pattern for the entire communication which varies in different instances of time.
4 The 2nd layer of security is achieved at the transmission end. This extra layer of security has been incorporated at the interfacing of data lines and the selection lines of the Multiplexer through permuting the derived ciphers and keys.

1.1. QCA preliminaries

The basic building block of QCA device is a QCA cell shown in Fig. 1. A QCA cell contains four electron holding sites known as quantum-dots. When two extra electrons are injected within the cell they align themselves diagonally at farthest distance from each other due to columbic repulsion. As a result, two polarizations are formed based on the position of the electrons within the dot, viz. polarization +1 (digital 1) and polarization –1 (digital 0).

In QCA technology, two fundamental gates are used which are QCA Inverters and Majority voters, shown in Fig. 2. When two QCA cells are placed at corners then the polarization of the output cell will be inverse of that of the input cell, giving rise to inverter characteristics. The majority voter on the other hand will provide the majority of the input polarization at the output. The equation of majority voter is given in Eq. (1).

$$Y = AB + BC + CA$$
$$Y = M(ABC) \quad (1)$$

Another important QCA structure that has been used in the proposed design is QCA tile structure [23]. QCA cells when placed in matrix form forms an $n \times n$ tile structure. Various complex logic gates, viz. NNI, AOI, can be designed using QCA tile. The major benefit of QCA tile is that it is area efficient and defect tolerant [23].

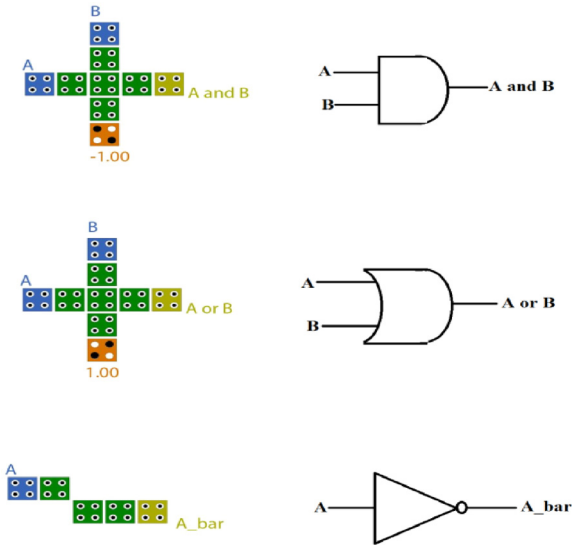

Fig. 2. QCA gates.

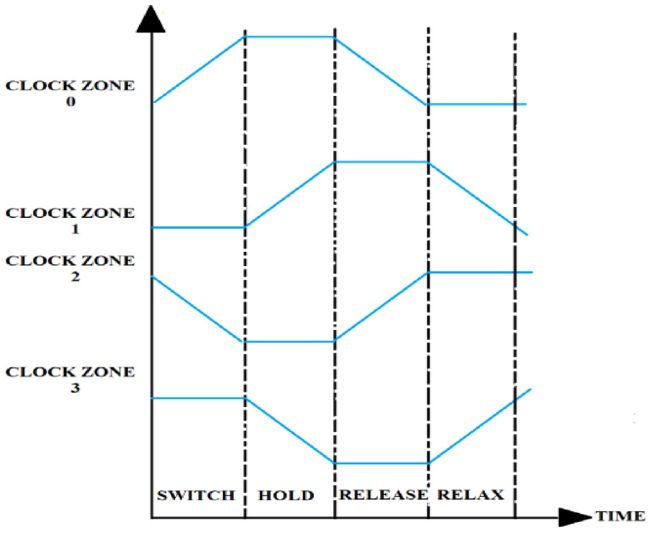

Fig. 3. QCA clocking.

1.2. QCA clocking

The barrier between adjacent quantum-dots in a cell is increased and decreased by clocking. A QCA cell switches between Polarizations –1 and +1 when the inter-dot barrier is low as electrons tunnel between the neighbouring dots in a cell. QCA clocking has four phases, viz. switch, hold, release and relax, as shown in Fig. 3. During switch and hold phases the inter-dot barrier is high and initially unpolarized cells attain the polarization states of the input cells. The polarization state remains fixed in hold phase. During release phase, the inter-dot barriers are gradually lowered which remain low during the relax phase.

2. Working principle of proposed cryptographic circuit

The working principle of the proposed architecture can be summarized in the following algorithm: