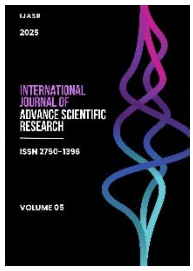
International Journal of Advance Scientific Research
(ISSN – 2750-1396)
VOLUME 05 ISSUE 06 Pages: 36-40
OCLC – 1368736135



Journal Website: http://sciencebring.com/index.php/ijasr

Research Article

Power Analysis Attacks And Cryptographic Circuit Design In Quantum-Dot Technology

Submission Date: May 12, 2025, **Accepted Date:** May 30, 2025,
Published Date: June 19, 2025
Crossref doi: https://doi.org/10.37547/ijasr-05-06-05

Nuriddin Safoev
Tashkent University of Information Technologies named after Muhammad al-Khwarizmi, Tashkent, Uzbekistan

Sirojiddin Salimov
Tashkent University of Information Technologies named after Muhammad al-Khwarizmi, Tashkent, Uzbekistan

Abstract

Quantum-dot Cellular Automata (QCA) has emerged as a promising nanotechnology for ultra-low-power and high-speed cryptographic circuit design. However, its vulnerability to power analysis attacks (PAA) remains a critical concern. This paper reviews existing QCA-based cryptographic implementations, including the Serpent cipher, A5/1 stream cipher, and True Random Number Generators (TRNGs), analyzing their resistance to side-channel attacks. We evaluate power consumption models, security trade-offs, and novel design methodologies for secure nanocommunication.

Keywords

Power analysis attack, Random number generation, pseudo-random number generation, entropy, cryptography, simulations.

Introduction

As digital systems continue to scale down to the nanoscale level, the demand for secure and energy-efficient cryptographic hardware has intensified. Traditional CMOS (Complementary Metal-Oxide Semiconductor) technology, despite its widespread adoption, faces critical limitations in terms of power leakage, heat dissipation, and scalability. In response to these challenges,

International Journal of Advance Scientific Research
(ISSN – 2750-1396)
VOLUME 05 ISSUE 06 Pages: 36-40
OCLC – 1368736135

ISSN-2750-1396

Quantum-dot Cellular Automata (QCA) has emerged as a promising post-CMOS nanotechnology, offering near-zero static power dissipation, ultra-dense circuitry, and high clocking frequencies. These characteristics make QCA particularly attractive for implementing cryptographic systems in secure nano- and quantum communication environments [1].

However, the benefits of QCA do not inherently guarantee immunity against all forms of cyber threats. Among the most insidious are side-channel attacks, especially Power Analysis Attacks (PAA), which exploit variations in power consumption to deduce secret cryptographic keys. While conventional CMOS-based systems have been extensively studied under these attack models, the susceptibility of QCA circuits remains an underexplored but pressing concern.

This paper investigates the vulnerability of various QCA-based cryptographic implementations to power analysis attacks. We place a particular emphasis on the Serpent block cipher, known for its robust mathematical structure and 32-round security-enhanced architecture, as well as the A5/1 stream cipher and True Random Number Generators (TRNGs) designed using QCA logic. The study further explores reversible logic implementations, such as authentication circuits based on Fredkin gates, highlighting their impact on reducing power signatures and enhancing fault tolerance [2].

By analyzing power models, logic designs, and architectural trade-offs, this work aims to provide a comprehensive understanding of the security landscape for QCA-based cryptographic circuits. Our goal is to assess whether QCA technology can truly serve as a secure foundation for next-generation cryptographic systems, or whether novel countermeasures must be integrated to withstand the evolving threats of side-channel attacks.

2. Power Analysis Attacks on QCA Cryptographic Circuits

2.1 Upper Bound Power Model in QCA

To evaluate the vulnerability of QCA-based circuits against power analysis attacks (PAA), [3] proposed an upper bound power model. This model estimates the worst-case dynamic power consumption in QCA circuits, accounting for polarization switching activities that occur during signal propagation. In their investigation, a 4-bit × 4-bit sub-module of the Serpent cipher was implemented in QCA to observe how even minimal power variations can be exploited. The results revealed that correlation-based attacks (CPA) were capable of identifying the correct cryptographic key, indicating that the intrinsic low-power advantage of QCA does not inherently guarantee resistance to side-channel threats.

2.2 Serpent Cipher in QCA

The Serpent cipher, characterized by its 32-round substitution-permutation network (SPN) architecture, offers enhanced cryptographic strength compared to AES (Rijndael), particularly due to its increased round count and conservative design principles. Despite its theoretical robustness, QCA-based implementations of

International Journal of Advance Scientific Research
(ISSN – 2750-1396)
VOLUME 05 ISSUE 06 Pages: 36-40
OCLC – 1368736135

Serpent remain susceptible to PAAs, as attackers can exploit the key-dependent internal operations of the cipher [4]. This vulnerability allows for the sequential recovery of subkeys by analyzing power consumption patterns during encryption.

In a study conducted by authors[5], a detailed QCA-based realization of the Serpent cipher was developed, featuring:

A 128-bit input block size and full 32-round SPN architecture.

Key mixing operations implemented using AND and NOT gate logic, along with linear transformations using AND/OR gates.

A highly compact 16:1 multiplexer-based S-Box design, composed of approximately 4,800 QCA cells, requiring 10 clock cycles to produce each S-Box output.

These design characteristics demonstrate the feasibility of implementing complex ciphers in QCA, but also underscore the pressing need for side-channel countermeasures, given that attackers can still leverage subtle power differences to mount effective PAAs.

3. QCA-Based Cryptographic Architectures

3.1 Encryption and Decryption in QCA

Authors [9] proposed a Quantum-dot Cellular Automata (QCA)-based encoder-decoder architecture tailored for secure nanocommunication. The core encryption and decryption operations follow a bitwise XOR mechanism:

$$B_i = E_{K_i}(A_i) = A_i + K_i \; mod \; 2$$
$$A_i = D_{K_i}(B_i) = B_i + K_i \; mod \; 2$$

Here, A_i denotes the plaintext bit, K_i the key bit, and B_i the corresponding ciphertext bit. The addition modulo 2 effectively implements a logical XOR operation.

The proposed QCA circuit occupies an area of approximately 36,000 nm^2, comprising 42 cells, including three majority gates and two inverters. Notably, the design is scalable and can accommodate arbitrary key lengths, making it well-suited for nano-level cryptographic applications.

3.2 A5/1 Stream Cipher Implementation

Authors[6] realized the A5/1 stream cipher—originally used in GSM communication—within the QCA framework. The implementation leverages majority gates to control the behavior of shift registers, which form the backbone of the ciphering mechanism. A dedicated memory block is designed to retain data when the ENABLE signal is high and to update the stored values when the signal is low. This functional behavior highlights the potential of QCA technology in supporting real-time stream cipher architectures, with efficient control and minimal area overhead.

3.3 Reversible Authentication Circuits

In [7], Fredkin gates—well-known reversible logic primitives—were employed to develop an energy-efficient reversible authentication circuit. The design achieves a low quantum cost of 0.041 and

International Journal of Advance Scientific Research
(ISSN – 2750-1396)
VOLUME 05 ISSUE 06 Pages: 36-40
OCLC – 1368736135

demonstrates reduced power dissipation by eliminating information loss. Additionally, the circuit's robustness against thermal noise was evaluated using Hamming distance analysis (see Fig. 28), underscoring its suitability for low-power, thermally-stable QCA implementations in authentication protocols.

4. Secure Nanocommunication and TRNGs

4.1 Cryptographic Nano-Routers

A secure nanocommunication architecture was introduced in [8], incorporating XOR-based encoder and decoder circuits for data encryption and decryption. The communication flow is managed by a QCA-based nano-router utilizing a 4:1 multiplexer (MUX) and a 1:4 demultiplexer (DEMUX) to securely route encrypted data between nodes. This design highlights the potential of QCA for integrating compact, secure routing mechanisms within nanoscale networks, ensuring confidentiality and controlled data flow at the physical layer. Ref. [8] proposed a nano-communication architecture with:

Encoder/Decoder: XOR-based circuits.

Nano-router: 4:1 MUX and 1:4 DEMUX for encrypted data routing.

4.2 True Random Number Generation

In [9], a QCA-based True Random Number Generator (TRNG) was proposed, leveraging a self-starved feedback-based SRAM cell to produce non-deterministic output bits. A floating clock mechanism is introduced to enhance entropy and ensure higher randomness levels in the generated bitstream. Such TRNGs play a crucial role in cryptographic systems, particularly for generating unpredictable keys, initialization vectors, and nonces, which are foundational to the overall security of encryption schemes in QCA-based systems.

5. Fault-Tolerant Designs

A fault-tolerant D-type flip-flop design was presented in [10] for use in QCA-based shift registers. The architecture is scalable to n-bit configurations, offering enhanced reliability for sequential logic applications. Power dissipation analysis conducted using the QCAPro simulation tool demonstrated that the proposed design achieves lower energy consumption compared to conventional implementations. This advancement supports the development of robust and energy-efficient QCA circuits for cryptographic and communication systems where fault tolerance is critical.

Conclusions

Quantum-dot Cellular Automata (QCA) presents a promising paradigm for energy-efficient and high-speed cryptographic circuit design, offering significant benefits over traditional CMOS technologies. However, as this study has highlighted, the threat of power analysis attacks (PAA) persists even in QCA-based systems due to exploitable power consumption patterns. Addressing these vulnerabilities is essential for the secure deployment of QCA in practical applications.

International Journal of Advance Scientific Research
(ISSN – 2750-1396)
VOLUME 05 ISSUE 06 Pages: 36-40
OCLC – 1368736135

ISSN-2750-1396

Future research should prioritize the development of refined power models that enhance leakage resilience, the design of robust and correlation-resistant S-Box architectures, and the creation of scalable True Random Number Generators (TRNGs) to ensure high entropy in cryptographic key generation. While QCA-based cryptographic architectures hold substantial potential to transform secure nanocommunication, overcoming side-channel attack vectors remains a critical research challenge. Continued innovation in secure QCA design will be vital to realizing its full potential in next-generation cryptographic systems.

REFERENCES

1. Chan, W. K. (2009). Random Number Generation in Simulation.
2. Gutterman, Z., Pinkas, B., & Reinman, T. (2006). Analysis of the Linux Random Number Generator.
3. Haahr, M. (2011). Introduction to Randomness and Random Numbers.
4. Marsaglia, G. (2005). Random Number Generators.
5. Schneier, B. (2007). Dual_EC_DRBG: A Case Study in Backdoors.
6. Sunar, B., Martin, W., & Stinson, D. (2006). A Provably Secure True Random Number Generator.
7. Eastlake, D., Schiller, J., & Crocker, S. (2005). Randomness Requirements for Security. RFC 4086. https://www.rfc-editor.org/rfc/rfc4086
8. Gutterman, Z., Pinkas, B., & Reinman, T. (2006). Analysis of the Linux Random Number Generator. IEEE Symposium on Security and Privacy. https://doi.org/10.1109/SP.2006.26
9. Dorrendorf, L., Gutterman, Z., & Pinkas, B. (2007). Cryptanalysis of the Random Number Generator of the Windows Operating System. ACM CCS. https://doi.org/10.1145/1315245.1315274
10. Lacharme, P. (2012). Security flaws in Linux's /dev/random. https://eprint.iacr.org/2012/251
11. Kelsey, J., Schneier, B., Ferguson, N. (1999). Yarrow-160: Notes on the Design and Analysis of the Yarrow Cryptographic Pseudorandom Number Generator. https://www.schneier.com/paper-yarrow.pdf
12. Dodis, Y., et al. (2013). Security Analysis of Pseudorandom Number Generators with Input: /dev/random is not Robust. ACM CCS. https://doi.org/10.1145/2508859.2516661
13. National Institute of Standards and Technology. (2012). A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. NIST SP 800-22 Rev. 1a. https://doi.org/10.6028/NIST.SP.800-22r1a
14. Müller, T. (2013). Security of the OpenSSL PRNG. International Journal of Information Security, 12(4), 251–265. https://doi.org/10.1007/s10207-013-0213-7