The Journal of Supercomputing (2023) 79:3024–3054
https://doi.org/10.1007/s11227-022-04779-8

Logic Realization of Galois Field for AES SBOX using Quantum Dot Cellular Automata

P. Rajasekar[1] · H. Mangalam[2] · C. S. Subash Kumar[3]

Accepted: 10 August 2022 / Published online: 29 August 2022

Abstract

With the growing technological trends in VLSI domain, quantum dot cellular automata (QCA) technology is slowly replacing CMOS technology due to its smaller feature size, high operating frequency and reduced power consumption. In the initial research phase, QCA has been used to implement various combinatorial and sequential circuits models, which are the fundamental blocks in various applications. Nowadays, researchers focus on the implementation of application-based designs using QCA. This motivated to implement the Galois field (GF) functions for SBox module in the most secure cryptography encryption standard AES with QCA. In AES, SBOX is the predominant power consumption modules. Hence, a research has been carried out to implement a compact QCA-based AES-SBOX with GF. This paper describes the implementation of our proposed QCA-based AES-SBOX with Galois field and analysis of various GF functional modules in terms of area, performance, energy and QCA cells used. The functional verification is performed using the simulated waveforms.

Keywords QCA · Galois Field (GF) · AES SBOX · Cryptography Algorithm · QCA Designer

H. Mangalam and C. S. Subash Kumar authors contributed equally to this work.

✉ P. Rajasekar
rajasekarkpr@gmail.com

H. Mangalam
hmangalam2@gmail.com

C. S. Subash Kumar
subashkumarcs@gmail.com

[1] ECE, Narayana Engineering College, Gudur, SPSR Nellore 524101, Andhrapradesh, India

[2] ECE, Sri Ramakrishna Engineering College, Coimbatore 641022, Tamilnadu, India

[3] EEE, PSG Institute of Technology and Applied Research, Coimbatore 641062, Tamilnadu, India