06/2023

8

Reversible Logic based Cryptography Design Algorithm using Random Keys

S. Rithiga[1], T. Venish Kumar[2], M. Idhayachandran[3], S. Prathap[4]

[1]Student, [2]Associate Professor, [3,4]Assistant Professor

[1,2,3,4] Dept. of Electronics and Communication Engineering, Nadar Saraswathi College of Engineering and Technology, Theni, India.

E-mail: rithigasivakumar@gmail.com[1], venishkumarnscet@gmail.com[2], mchandraan@gmail.com[3],prthpraja@gmail.com[4]

Abstract

Reversible computations, besides quantum computing, have various applications in digital signal processing, nanotechnology and bioinformatics. They are particularly useful in designing low-power devices and improving computational efficiency. Cryptography is vital for protecting sensitive information in fields such as bioinformatics and digital signal processing where private data is frequently exchanged. However, cryptographic algorithms can consume significant power and require large areas, particularly when implemented in hardware. Reversible logic gates offer a potential solution by being more power-efficient and potentially reducing implementation area. Using random numbers as keys for both encryption and decryption in a reversible logic gate-based cryptographic algorithm can enhance security. LSB watermarking is a technique to embed additional metadata into digital media, improving data security. To evaluate the performance of the Field Programmable Gate Array for the Reversible Logic Gate Cryptography Design architecture, comparing it to the other state-of-the-art approach is necessary.

Keywords: Reversible Logic Gate Cryptography Design (RLGCD), Random keys, Field Programmable Gate Array (FPGA), Watermarking

1. INTRODUCTION

Cryptography is the science of securing communications and shielding information from unauthorized access or disclosure [1]. It involves using mathematical algorithms to transform the original data (referred to as plaintext) into an unreadable format (referred to as ciphertext) to maintain confidentiality [2][3]. The process of encryption and decryption is fundamental to cryptographic systems. Encryption is the process of converting plaintext into ciphertext using

DOI: https://doi.org/10.36548/jei.2023.2.004
Received: 02.04.2023, received in revised form: 02.05.2023, accepted: 17.05.2023, published: 27.05.2023

© 2023 Inventive Research Organization. This is an open access article under the Creative Commons Attribution-NonCommercial International (CC BY-NC 4.0) License

NADAR SARASWATHI COLLEGE OF ENGINEERING & TECHNOLOGY
THENI
625 531

Dr. C. MATHALAI SUNDARAM, M.E.,M.B.A.,Ph.D.,
Principal
Nadar Saraswathi College of
Engineering and Technology
Vadapudupatti, Theni-625 531.