بسم الله الرحمن الرحيم

∞∞∞

تم رفع هذه الرسالة بواسطة / سامية زكى يوسف

بقسم التوثيق الإلكتروني بمركز الشبكات وتكنولوجيا المعلومات دون أدنى مسئولية عن محتوى هذه الرسالة.

ملاحظات: لا يوجد

AIN SHAMS UNIVERSITY
FACULTY OF ENGINEERING
CAIRO – EGYPT

FPGA IP Cores Encryption Systems Based On Nonlinear Algorithms

A Thesis

Submitted in partial fulfillment for the requirements of the degree
of Master of Science in Electrical Engineering
Electronics and Communications Engineering Department
Ain Shams University

Submitted by

Eng. Haitham Abdel-Hady Mohamed
Electronics and Communications Department
Faculty of Engineering, Ain Shams University

Supervised By

Prof. Dr. Wagdy Refaat Anis
Electronics and Communication Department
Faculty of Engineering – Ain-Shams University (ASU), Cairo, Egypt

Prof. Dr. Ahmed H. Madian
Nano Electronics Integrated Systems Center (NISC)
Nile University, Cairo, Egypt

Prof. Dr. Ahmed Abdel-Hafez
National Telecommunications Regulatory Authority, Cairo, Egypt

Cairo - 2022

AIN SHAMS UNIVERSITY
FACULT AIN SHAMS UNIVERSITY
FACULTY OF ENGINEERING
CAIRO – EGYPT

Examiners Committee

Name: **Haitham Abdel-Hady Mohamed**

Thesis: **FPGA IP Cores Encryption Systems Based on Nonlinear Algorithms**

Degree: **Master of Science in Electrical Engineering**

Name, Title, and Affiliate	**Signature**
1. Prof. Dr. Mohamed Hassan Abdel_Azeem Electronics and Communication Eng. Department Faculty of Engineering Arab Academy for Science Technology and Maritime Transport, Cairo, Egypt	…………….
2. Prof. Dr. Ismail Mohamed Hafez Electronics and Communication Eng. Department, Faculty of Engineering, Ain Shams University, Cairo, Egypt	……………...
3. Prof. Dr. Wagdy Refaat Anis Electronics and Communication Eng. Department, Faculty of Engineering Ain Shams University, , Cairo, Egypt.	…………….

Date: / / 2022

STATEMENT

This Thesis is submitted to Ain Shams University in partial fulfillment of the degree of Master of Science in Electrical Engineering.

The work included in this thesis was carried by the author in the Department of Electronics and Communications Engineering, Ain Shams University.

No part of this Thesis has been submitted for a degree or a qualification at any other university or institute.

Name **:** Haitham Abdel-hady Mohamed

Signature:

Date : / / 2022

Publications

[1] H.A. Mohamed, A.H. Madian, W. R. Anis and A. A. Abdel Hafez, "Generation of the chaotic keys on the fly for AES encryption system", 2021 3rd Novel Intelligent and Leading Emerging Sciences Conference (NILES), pp. 1-5, Cairo, Nov 2021.
DOI: 10.1109/NILES53778.2021.9600560.

Acknowledgment

First and foremost, I would like to express my gratitude to ALLAH, the Ever-Living and the Sustainer of all existence, the One who neither begets nor is born, nor is there any comparable to Him.

I am thrilled to express my heartfelt gratitude and appreciation to my superiors:

Prof. Dr. Wagdy Anis (ASU)

Prof. Dr. Ahmed H. Madian (NU)

Prof. Dr. Ahmed Abdel-Hafez (NTRA)

Throughout my research, I am grateful for their supervision, direction, generous suggestions, criticism, and constant support.

My heartfelt gratitude goes to Prof. Ahmed H. Madian for his advice, open-door policy, and numerous helpful feedbacks during the dissertation writing process. I believe that your guidance has helped me develop as a researcher.

Finally, I'd like to express my gratitude to my family, to whom I owe so much. To **mother**, **wife**, and **my daughter**, as well as **my brothers.**

I sincerely apologize to **my wife** and **my daughter** for all of the late nights, weekends, and holidays that I have missed. Thank you for your unending encouragement, understanding, and assistance with all of my projects.

Dear …. Thanks for all ….

Abstract

The revolution in information and communication technology has become linked to the development of societies in our time, as it is considered the most important means of transferring developing societies to more developed societies. So, The Egyptian government wants to create a digital Egypt and society that uses technology in all aspects of life. As a result, it aims to improve government agencies' digital services as well as the development of information, and communication technology infrastructure. All of this need strong information security to provide privacy and confidentiality of the information in circulation.

Information security is the science that provides data protection from all threats, risks, and security breaches through tools and measures taken for this matter. Encryption holds a special place in information security sciences, it is the backbone to ensure the confidentiality of information because it protects the data from attackers and unauthorized persons. Encryption systems are classified as asymmetric or symmetric based on their key distribution. In asymmetric encryption, the encryption depends on private and public keys. On the other hand, symmetric encryption depends on only symmetric keys for encrypting and decrypting the data.

Researchers have become more interested in generating both private keys, public keys, and symmetric keys. There is a lot of research for the generation of encryption keys.

This thesis provides a study in the realm of symmetric encryption that uses chaotic systems to produce strong and secure subkeys. Generation subkeys for Advanced encryption standard (AES) and Blowfish encryption algorithm.

AES and Blowfish are strong symmetric block cipher encryption algorithms. Both Encryption algorithms use symmetric key for encryption and

Decryption. Using strong symmetric key for encryption algorithm adds strong resistance against different attacks, so it's important issue to design strong symmetric key.

Chaotic systems describe very complicated dynamical system that difficult to predict and control. chaotic systems have some properties like deterministic that means the chaotic systems have a mathematical model that describe the system behavioral. Also chaotic systems are very sensitive to initial conditions (butterfly effect) and any change in initial condition leads to a significant change in the system behavioral and the output [1].

Making a modification to blowfish encryption algorithm is proposed by replacing the standard round function by light weight function to reduce the resources utilization area and increase the speed. Where the standard blowfish consumes large resources from the FPGA platform.

Numerical analysis is applied to the proposed technique, we utilized MATLAB to test our proposed technique through simulation, numerical operations. Statistical Tests (Entropy, Mean Square Error, Correlation Coefficient and NIST test) have been done on the output of the proposed encryption algorithms

Hardware digital realization of all introduced systems is implemented using the Xilinx Virtex_5 Field Programmable Gate Arrays (FPGA) kits. Also, the proposed technique is designed using VHDL and Xilinx ISE 14.7 tool is used in both VHDL simulation and hardware implementation stages.

Key words (CHAOTIC SYSTEMS, LORENZ SYSTEM, FPGA, AES, BLOWFISH).

Table of Contents

Chapter 5: Proposed Modified Blowfish Algorithm Based On Improved Lorenz Attractor

Chapter 6: Conclusion And Future work

References……………………………………………………………………….....67

List of Figures:

List of Tables

Abbreviations

AES	Advanced Encryption Standard
PRNG	pseudorandom number generators
MHz	Mega Hertz
FPGA	Field programmable gate array
LUT	Look Up Tables
Ke	Encryption Key
Kd	Decryption Key
1_D	One Dimension
H_D	High Dimension
IDEA	International Data Encryption Algorithm
DSA	Digital Signature Algorithm
RSA	Ron Rivest, Adi Shamir, and Leonard Adleman
DoS	Denial of Service
Ku	Public key
Kr	Private key
ECBC	Enhanced Cipher Block Chaining
CBC	Cipher Block Chaining
NSA	National security agency
NIST	National Institute of Standards and Technology
UACI	Unified Averaged Changed Intensity
NCPR	Number of Changing Pixel Rate
MSE	Mean Square Error

Chapter (1)

Introduction

1.1 Overview

Information and Communication Technology has become an essential aspect of our daily lives. We use it to interact with others, share data, shop, do paperwork, and even make restaurant reservations. It's tough to envision modern life without them and their global connectedness. Despite its benefits, computer network interconnection poses major risks.

Because the Information Revolution is evolving at such a rapid pace, all users of this technology must be mindful of the hazards associated with implementing cutting-edge technology. Complete ability to secure and preserve information from theft and malicious use of it so that the information revolution does not harm those who benefit from it.

Security demands for special information communications networks such as Military Networks or Company Networks require a proprietary and unique encryption method to provide a high level of secrecy. When interacting with peers demands safe communications, encryption methods are responsible for guaranteeing end-to-end secrecy for the payload data packets.

This dissertation reviews the most valuable encryption algorithms additionally investigates the security concerns and provides remedies for securing communication networks.

Furthermore; This study is being conducted to improve network performance as well as security services on networks.

1.2 Problem Statement

Due to the fact that encryption operations performed by any protocols increase the number of operations, and slows down the data rate, hence Encryption may have a negative effect on the quality of services (QOS) offered