شبكة المعلومات الجامعية

بسم الله الرحمن الرحيم

شبكة المعلومات الجامعية

التوثيق الالكتروني والميكروفيلم

شبكة المعلومات الجامعية

جامعة عين شمس

التوثيق الإلكتروني والميكروفيلم

قسم

نقسم بالله العظيم أن المادة التي تم توثيقها وتسجيلها علي هذه الأقراص المدمجة قد أعدت دون أية تغيرات

يجب أن

تحفظ هذه الأقراص المدمجة بعيدا عن الغبار

HARDWARE SECURITY MODULE FOR LOW POWER INTERNET OF THINGS APPLICATIONS BASED ON DYNAMIC PARTIAL RECONFIGURATION

By

Nagham Samir Abo-Dief Abdel-Raziq

A Thesis Submitted to the
Faculty of Engineeringat Cairo University
in Partial Fulfillment of the
Requirements for the Degree of
MASTER OF SCIENCE
in
Electronics and Communications Engineering

FACULTY OF ENGINEERING, CAIRO UNIVERSITY
GIZA, EGYPT
2020

HARDWARE SECURITY MODULE FOR LOW POWER INTERNET OF THINGS APPLICATIONS BASED ON DYNAMIC PARTIAL RECONFIGURATION

By

Nagham Samir Abo-Dief Abdel-Raziq

A Thesis Submitted to the
Faculty of Engineeringat Cairo University
in Partial Fulfillment of the
Requirements for the Degree of
MASTER OF SCIENCE
in
Electronics and Communications Engineering

Under the Supervision of

Prof. Dr. Ahmed H. Khalil
Professor
Specialization Department
Faculty of Engineering, Cairo University

Dr. Hassan Mostafa Hassan
Associate Professor
Department of Electronics and Communication Engineering
Faculty of Engineering, Cairo University

FACULTY OF ENGINEERING, CAIRO UNIVERSITY
GIZA, EGYPT
2020

HARDWARE SECURITY MODULE FOR LOW POWER INTERNET OF THINGS APPLICATIONS BASED ON DYNAMIC PARTIAL RECONFIGURATION

By

Nagham Samir Abo-Dief Abdel-Raziq

A Thesis Submitted to the
Faculty of Engineeringat Cairo University
in Partial Fulfillment of the
Requirements for the Degree of
MASTER OF SCIENCE
in
Electronics and Communications Engineering

Approved by the
Examining Committee

Prof. Dr. Ahmed H. Khalil	Thesis Main Advisor
Dr. Hassan Mostafa Hassan	Advisor
Prof. Dr. Amin Mohamed Nassar	Internal Examiner
Dr. Mohamed Abdelghani Salem (German University in Cairo)	External Examiner

FACULTY OF ENGINEERING, CAIRO UNIVERSITY
GIZA, EGYPT
2020

Engineer's Name:	Nagham Samir Abo-Dief Abdel-Raziq
Date of Birth:	30/9/1992
Nationality:	Egyptian
E-mail:	nagham.samir2014@gmail.com
Phone:	01118847199
Address:	Kornish-Elnile, Misr ElQadima, Cairo- Egypt
Registration Date:	1/3/2016
Awarding Date:	/ /2020
Degree:	Master of Science
Department:	Electronics and Communications Engineering

Supervisors:

Prof. Dr. Ahmed H. Khalil
Dr. Hassan Mostafa Hassan

Examiners:

Prof. Dr. Ahmed H. Khalil	(Thesis main advisor)
Prof. Dr. Amin Mohamed Nassar	(Internal examiner)
Dr. Mohamed Abdelghani Salem (German University in Cairo)	(External examiner)

Title of Thesis:

Hardware Security Module for Low Power Internet of Things Applications Based on Dynamic Partial Reconfiguration

Key Words:

Internet of Things (IoT); Dynamic Partial Reconfiguration (DPR); Advanced Encryption Standard (AES); Field Programmable Gate Array (FPGA);

Summary:

This work implements hardware security module for low power internet of things applications on Zynq-7000 evaluation kit. The new DPR technique is used to switch among the different levels of security depending on the variant energy profile of IoT device. Implementing encryption algorithm using DPR combines the advantage of hardware performance and software flexibility. A test environment is established to measure the effectiveness of the new technique.

Table of Contents

List of Tables

List of Figures

List of Nomenclature

AD	associated data
AE	Authenticated Encryption
AEAD	Authenticated Encryption with Associated Data
AES	Advanced Encryption Standard
API	Application Programming Interface
APR	Auto Place and Route
ASIC	Application Specific Integrated Circuits
AXI	Advanced eXtensible Interface
BFA	Brute Force Attack
BRAM	Block RAM
CA	Constant Addition
CAESAR	Competition for Authenticated Encryption: Security, Applicability, and Robustness
CBC	Cipher Block Chaining
CCM	Counter with Cipher Block Chaining Message Authentication Code
CFB	Cipher Feed Back
CFB	Cipher FeedBack
CLB	configurable logic block
CPLD	Complex Programmable Logic Device
DEC	Decryption engine
DPA	differential power analysis
DPR	Dynamic partial reconfiguration
EAX	Encryption-then-Authentication-then-Translate
EAX – prime	Encryption-then-Authentication-then-Translate-prime
ECB	Electronics Code Book
ENC	Encryption engine