AIN SHAMS UNIVERSTY
FACULTY OF ENGINEERING
CAIRO – EGYPT
Electronics and Communication Engineering Department

Secure and efficient symmetric-key encryption algorithm

Dissertation submitted to the faculty of Engineering – Ain-Shams University in partial fulfilled of the requirements for the degree of Master of Science in Electrical Engineering

Submitted By

Eng. Ahmed Mahmoud Salama Rayan

Electronics and Communication Eng. Department

Faculty of Engineering – Ain-Shams University

Supervised By

Prof. Dr. Ismail Mohamed Hafez

Professor in Electronics and Communication Eng. Department

Faculty of Engineering – Ain-Shams University (ASU)

Cairo – Egypt

Ass. Prof. Dr. Ahmed Ali Abdel-hafez

Communications Department

Military Technical Collage (MTC)

Cairo – Egypt

Cairo 2017

AIN SHAMS UNIVERSTY
FACULTY OF ENGINEERING
CAIRO – EGYPT

Examiners Committee

Name : Ahmed Mahmoud Salama Rayan
Thesis : Secure and efficient symmetric-key encryption algorithm
Degree: Master of Science

Name, Title, and Affiliate Signature

1. **Prof. Dr.** Talaat Abdel Latief Ibrahim El Garf ……
   Professor of Communications in Higher Technological Institute (HTI)

2. **Prof. Dr.** Salwa H. El- ramly ……
   Professor in Electronics and Communication Eng. Department (ASU)

3. **Prof. Dr. Ismail Mohamed Hafez** ……
   Professor in Electronics and Communication Eng. Department (ASU)

4. **Ass. Prof. Dr. Ahmed Aly Abdel-hafez** ……
   Communications Department (MTC)

Date: /01 /2017

STATEMENT

This dissertation is submitted to Ain Shams University in partial fulfillment of the degree of Master of Philosophy in Electrical Engineering**.**

The work included in this dissertation was out by the author in the department of electronics and Communication Engineering, Ain Shams University.

No part of this dissertation has been submitted for a degree or qualification at other university or institution.

Name : Ahmed Mahmoud Salama Rayan
Signature : …….....
Date : / / 2017

Abstract

Secure and efficient symmetric-key encryption algorithm

In 1997, a competition to choose a symmetric-key encryption algorithm instead of Data Encryption Standard algorithm (DES) was started by the National Institute of Standards and Technology (NIST). NIST specified the evaluation criteria for chosen the candidate algorithms relying on the analyses and comments received. These criteria are divided into two main categories:

i. Algorithm security.
ii. Algorithm implementation features.

Algorithm security was the main significant criteria, it includes characteristics as: algorithm strength to attacks, its mathematical foundation and the output randomness.

Finally, NIST selected five finalist algorithms (Rijndael, Serpent, RC6, MARS and Twofish). Then, NIST chose Rijndael to be the suggested Advanced Encryption Standard algorithm (AES).

Twofish algorithm, one of the last five candidate algorithms has a large security margin but also has some drawbacks as its structure is hard to analyses, the mingling of many processes makes it not easy to produce a fair analysis and imposes to searching for approximation mechanisms. Moreover, the use of key-dependent S-boxes increases the complexity and the effort needed to estimate the characteristics (differentials, linear …) of the structure.

In this thesis a proposal of a provably Secure Symmetric-key Encryption (SSE) algorithm based on Feistel structure is presented to overcome the previous drawbacks. A 16-round reversible Basic Feistel Network (BFN) is presented, besides construct a novel key schedule. It supports 128-bit and 256-bit symmetric key block cipher with 128-bit key size; its key size can be extended to 256 bits.

(SSE) algorithm is simple and pliable design, ease and efficient analysis. Strong Key dependent S-boxes layer is used to overcome the drawbacks (differential cryptanalysis – linear cryptanalysis) of fixed S-boxes. A proven security for each component is provided.

Its key schedule is secure and straight forward for analysis; reuse the Same Primitives that is used in the encryption algorithm. It provided 40 subkeys of expanded key SK_0, ..,SK_{39} and 16 rounds constant $RC_0, \ldots, RC_{15}$ for each round that is used with the S-boxes input of (SSE) algorithm.

Acknowledgement

First and Foremost I would like to thank ALLAH — the Ever-Living and the Sustainer of all existence, the One that neither begets nor is born and nor is there to Him any equivalent.

I feel honored to record my deepest sense of gratitude and thanks to my supervisors:

Prof. Dr. Ismail Mohamed Hafez (ASU)

Prig. Ass.Prof. Ahmed Ali Abdel-Hafez (Egyptian Armed Forces)

Thanks for their supervision, guidance, generous advice, criticism, and continuous encouragement throughout this research.

Many thanks go to my commander Prig. Ass.Prof. Ahmed Aly Abdel-Hafez for his advice, for the open door policy and for many useful feedbacks during the writing of this dissertation. I believe that your supervision has allowed me to grow up as a researcher.

Finally, I would like to thank my family to whom I owe a great deal. To my late father, my late mother, my sister, my brothers, my wife and my children.

I apologize for my wife and my children for all the long nights and weekends, and holidays which I missed. Thanks for your endless support, encouragement, understanding and helping me through all my work.

Dear …. Thanks for all ….

Ahmed Mahmoud Rayan

Cairo 2016

Dedication

To the soul of my late father and mother

List of Acronyms

Abbreviation	
AES	Advanced Encryption Standard
ANF	Algebraic normal form
BC	Before Christ
BFN	Basic Feistel Networks
CBC	Cipher Block Chaining
CFB	Cipher Feedback
CPU	Central Processing Unit
CTR	Counter
DES	Data Encryption Standard
DPA	Differential power analysis
ECB	Electronic Codebook
GCD	Greatest Common Divisor
GF	Galois Field
GFN	Generalized Feistel Networks
HW	Hamming Weight
IV	Initial Value
KC	Key Constant
MDS	Maximum Distance Separable
NBS	National Bureau of Standards
NIST	National Institute of Standards and Technology
NL	nonlinearity
OFB	Output Feedback
PC	Propagation Criterion
PKC	Public Key Cryptography
RC	Round Constant
RC6	Rivest cipher 6

S_boxes	Substitution boxes
SAC	Strict Avalanche Criterion
SHA	Secure Hash Algorithm
SKC	Secret Key Cryptography
SP	Substitution Permutation
SPA	Simple power analysis
SPN	Substitution Permutation Network
SSE	Secure Symmetric-key Encryption
STS	Statistical Test Suite
UFN	Unbalanced Feistel Networks
Wt	Weight of a Boolean function

List of Symbols

Symbol	
$\oplus$	Xor
$+$	Addition
$\leq$	Less than or equal
$\geq$	Large than or equal
$=$	equal
$\neq$	Not equal
$\equiv$	Congruent
$\in$	Belongs to
$\forall$	For all
$\exists$	There exists
$\sum$	Sum
$\mathbf{Z_p}$, GF (P)	Finite Fields of Order p
$\mathbf{Z}_{p^n}$, GF (p^n)	Finite Fields of prime p and n is the degree of irreducible polynomial
$\boldsymbol{W_t(f)}$	Hamming weight (HW) of function $\boldsymbol{f}$
d_H	Hamming Distance
$\boldsymbol{\varepsilon}$	bias
$F^{\wedge}$	Walsh-Hadamard transform
$\diamond$	scalar product over F_2

Table of Contents

List of Figures

Fig. No. Title **Page No.**