Tribhuvan University

Institute of Science and Technology

Performance Analysis of eSTREAM Cipher Finalists: HC-128, Salsa20/12, Rabbit & SOSEMANUK

Dissertation

Submitted to: -

Central Department of Computer Science & Information Technology

Tribhuvan University, Kirtipur, Nepal.

In partial fulfillment of the requirements

For the Master's Degree in Computer Science & Information Technology

By

Dil Bahadur Budhathoki

Jun 15, 2016

Tribhuvan University

Institute of Science and Technology

Central Department of Computer Science and Information Technology

Supervisor's Recommendation

I hereby recommend that this dissertation prepared under my Supervision by **Dil Bahadur Budhathoki** entitled **"Performance Analysis of eSTREAM Cipher Finalists: HC-128, Salsa20/12, Rabbit & SOSEMANUK"** in partial fulfillment of the requirements for the Master's Degree in Computer Science & Information Technology be processed for the evaluation.

.....

Asst. Prof. Nawaraj Paudel

Head of Department

Central Department of Computer Science & Information Technology

Kritipur, Kathmandu, Nepal

(Supervisor)

Date: - Jul 06, 2016

Tribhuvan University

Institute of Science and Technology

Central Department of Computer Science & Information Technology

LETTER OF APPROVAL

We certify that we have read this dissertation and in our opinion it is satisfactory in the scope and quality as a dissertation in partial fulfillment of the requirements for the Master's Degree in Computer Science & Information Technology.

Evaluation Committee

……

Asst. Prof. Nawaraj Paudel

(Supervisor)

(Head of Department)

Central Department of Computer Science and Information Technology

Kritipur, Kathmandu, Nepal

……..	……
Mr. Lochan Lal Amatya	Asst. Prof. Sarbin Sayami
(Director, Wireless Service Directorate, NTC)	(CDCSIT, T.U.)
(External Examiner)	(Internal Examiner)

Date: - Jul 6, 2016

Tribhuvan University

Institute of Science and Technology

Central Department of Computer Science and Information Technology

Declaration

"I, **Dil Bahadur Budhathoki**, declare that the Master by Research thesis entitled **Performance Analysis of eSTREAM Cipher Finalists: HC-128, Salsa20/12, Rabbit & SOSEMANUK** contain no sources other than listed, this thesis is my own work."

…….

Dil Bahadur Budhathoki

Jun 15, 2016

ACKNOWLEDGMENTS

It's a pleasure for me to thank my Supervisor, **Asst. Prof. Nawaraj Paudel**, Head of Computer Science & IT Department, T.U., Kathmandu, Nepal, for his constant encouragement, support and advices.

I greatly acknowledge to respected Professors and Lecturers **Prof. Dr. Shashidhar Ram Joshi, Prof. Dr. Subarna Shakya, Asst. Prof. Dheeraj Kedar Pandey, Asst. Prof. Sarbin Sayami, Asst. Prof. Lalita Sthapit, Mr. Jagdish Bhatta, Mr. Arjun Singh Saud, Mr. Bishnu Gautum, Mr. Bikash Balami,** of **CDCSIT, TU**, for providing valuable suggestions and huge knowledge as well as inspirations.

I would like to thank my friends and family for their encouragement and support. I would like to give my special thanks to my friend *Mr. Chhetra Bahadur Chhetri* for helping to provide necessary resources to complete this work.

ABSTRACT

Stream cipher algorithms are most powerful tools in symmetric cryptography. These algorithms perform either bit wise or byte wise encryption in a simple way just doing XOR operation between key and message (plain text). Stream cipher algorithms are about 5 to 10 times faster than AES, TDES (block cipher). In stream cipher, creating key stream by randomizing the bits is most important thing. These algorithms are useful normally in GSM mobile communication, Hard disk encryption, Multimedia encryption and fast Software encryption etc. In this thesis, those stream cipher finalists from eSTREAM project run by ECRYPT are studied, analyzed and implemented in Java Programming using NetBeans 8.0.2. Considering their other parameters constant, performance analysis is studied here in this thesis.

The empirical performance shows that Rabbit cipher is found to be better if the message size is very small. When message size is increased, then performance of Rabbit decreases and performance of Salsa20/12 increases in a far better way as compared to other algorithms. HC-128 has showed considerable performance in some cases of message size where as SOSEMANUK was found not to be good. Therefore, while inputting different and big size of message, performance of Salsa20/12 gets increased and it is found to be the best algorithm for the large size message in the targeted architecture computer.

Keywords: - Plaintext, Cipher text, Stream Ciphers, eSTREAM, HC-128, Salsa20/12, Rabbit, SOSEMANUK, XOR operation etc.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

AES	Advanced Encryption Standard
ANSI	American National Standards Institute
API	Application Programming Interface
CSPRNGs	Cryptographically Secure Pseudorandom Number Generators
DES	Data Encryption Standard
ECRYPT	European Network of Excellence in Cryptology
FSM	Finite State Machine
GSM	Global System for Mobile communication
HC	Hongjun Cipher
IDE	Integrated Development Environment
IV	Initialization Vector
JVM	Java Virtual Machine
LFSR	Linear Feedback Shift Register
NESSIE	New European Schemes for Signature, Integrity and Encryption
NLFSR	Nonlinear Feedback Shift Register
OTP	One Time Pad
PKI	Public Key Infrastructure
PRNGs	Pseudo Random Number Generators
RC4	Ron's Cipher Four
RSA	Rivest Shamir Adleman
SHA	Secure Hash Function
SOSEMANUK	Snow Snakes
SSL	Secure Socket Layer
TDES	Triple Data Encryption Standard
TRNGs	True Random Number Generators
XOR	Exclusive OR