A

Project Report

On

COST EFFECTIVE RESOURCE ALLOCATION OF OVERLAY ROUTING RELAY NODES

Submitted to

Department of
Computer Science and Engineering

By

KAVATI VENNELA	(216Y5A6602)
DUGYALA SATHVIKA	(206Y1A6618)
VADALA NIHARIKA	(206Y1A6650)
PEDDAPELLI VARSHA	(206Y1A6641)

Under the guidance

Of

Mr.G.RANADHEER REDDY
Asst.Professor

Department of Computer Science & Engineering

SUMATHI REDDY INSTITUTE OF TECHNOLOGY for WOMEN

(Approved by AICTE, New Delhi; Affiliated to JNTU, Hyderabad)

Ananthasagar(Vill), Hasanparthy(M), Warangal – 506 371 (A.P.), Website : www.sritw.org

2022-2023

PRINCIPAL
Sumathi Reddy Institute of Technology for Women
Ananthasagar (V), Hasanparthy (M)
WARANGAL - 506 371 (T.S.)

SUMATHI REDDY INSTITUTE OF TECHNOLOGY for WOMEN

(Approved by AICTE, New Delhi; Affiliated to JNTU, Hyderabad)

Ananthasagar(Vill), Hasanparthy(M), Warangal – 506 371 (A.P.), Website : www.sritw.org

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

CERTIFICATE

This is to certify that the project entitled **"COST EFFECTIVE RESOURCE ALLOCATION OF OVERLAY ROUTING RELAY NODES"** is submitted by KAVATI VENNELA(216Y5A6602), DUGYALA SATHVIKA(206Y1A6618), VADALA NIHARIKA(206Y1A6650) and PEDDAPELLI VARSHA(206Y1A6641) to the department of Computer Science and Engineering during academic year 2022-23.

Mr.G.RANADHEER REDDY
Project Guide

Dr.E.SUDARSHAN
Head of the Department

S.R.I.T. FOR WOMEN * WARANGAL *

PRINCIPAL
Sumathi Reddy Institute of Technology for Wo
Ananthasagar (V), Hasanparthy (M)
WARANGAL - 506 371 (T.S.)

ABSTRACT

Side-channel analysis (SCA) exploits the information leaked through unintentional outputs (e.g., power consumption) to reveal the secret key of cryptographic modules. The real threat of SCA lies in the ability to mount attacks over small parts of the key and to aggregate information over different encryptions. The threat of SCA can be thwarted by changing the secret key at every run. Indeed, many contributions in the domain of leakage resilient cryptography tried to achieve this goal. However, the proposed solutions were computationally intensive and were not designed to solve the problem of the current cryptographic schemes. In this paper, we propose a generic framework of lightweight key updating that can protect the current cryptographic standards and evaluate the minimum requirements for heuristic SCA-security. Then, we propose a complete solution to protect the implementation of any standard mode of Advanced Encryption Standard. Our solution maintains the same level of SCA-security (and sometimes better) as the state of the art, at a negligible area overhead while doubling the throughput of the best previous work.

Principal
Sumathi Reddy Institute of Technology for Women
Ananthasagar (V), Hasanparthy (M)
WARANGAL - 506 371 (TS)