# SECURE SECRET SHARING

By

**Utpal Bhupendrabhai Patel**
Enrollment No.:140370702551

Guided by

**Mr. Nileshkumar Kakade**
M.Tech(C.E)
Assistant. Professor, IT Department

A **Thesis** Submitted to
Gujarat Technological University
In Partial Fulfillment of the Requirements for
The Degree of Master of Engineering
In **Computer Engineering**

May – 2016

**Computer Science and Engineering Department**
**Parul Institute of Engineering & Technology**
**P.O: Limda, Ta.: Waghodia, Dist.: Vadodara**

# Secure Secret Sharing

## Submitted By

Utpal B. Patel

## Supervised By

Mr. Nileshkumar Kakade

Assistant professor

Parul Institute of Engineering and

Technology, P.O: Limda, Ta. Waghodia,

Dist.: Vadodara

## ABSTRACT

Secret sharing is an important means to achieve confidentiality and data privacy. Secret sharing scheme was first introduced by Shamir in 1979. Secret sharing deals with splitting a secret information with various players. The goal of the secret sharing is security of secret, privacy and hiding information. There are numerous techniques available for secret sharing e.g. polynomial, Chinese remainder theorem, vector space, matrix projection. Techniques have characteristics like threshold, proactive, verifiable. Proactive secret sharing scheme allow user to change share in case of doubt of theft. In this work we propose the proactive secret sharing scheme used on homomorphic techniques. Our scheme consist of three phases of share construction, share renewal, share reconstruction. Central authority splits an encrypted secret with each parties using homomorphic property of paillier encryption i.e. subtraction. In renewal process two or more parties relate share with each other for to generated renewed share. In reconstruction process all parties share will be add to central authority then encrypted secret will be generated. Central authority will decrypt encrypted secret using secret key then original secret will be generated. Our schemes unique features is share can be renewed any time, Each party can choose secret of their own choice, If any two parties have same content share then also encrypted share will be different due to non-deterministic property of paillier encryption.