# NTT-Sponsored Research in Cryptography and Information Security, and Algorithmic Development

Professor Shafi Goldwasser
Professor Ronald L. Rivest
Professor Michael Sipser
(MIT Lab for CS)

## Project Overview

- Covers a broad range of topics in security, complexity, and algorithms.
- Particular focus on:
  - distributed cryptographic protocols
  - electronic voting
  - quantum computation
  - probabilistic property checking

## Progress Report (to 6/99)

- New cryptographic primitive (verifiable pseudo-random functions) fully characterized.
- EVOX electronic voting software improved, demonstrated, used.
- New and surprisingly efficient algorithms for classical problems (such as insertion in an ordered list) on a quantum computer.

## Research Plans (for next six months)

- Develop threshold encryption schemes secure against chosen-ciphertext attack.
- Improve scalability and security of electronic voting.
- Developing more efficient search algorithms for quantum computers.