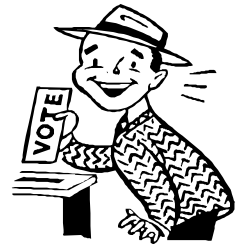
Shafi Goldwasser, Ronald L. Rivest, and Michael Sipser

Project Overview

Our overall goals are to improve the fundamental technologies capable of providing information security through the elaboration of appropriate protocol and adversarial models and through the development of provable secure cryptographic protocols and primitives. We are interested in significant applications (voting, e-cash) as well as mathematical foundations and related computational models (e.g. quantum computing).



Shafi Goldwasser, Ronald L. Rivest, and Michael Sipser

Progress Through December 2000

Progress on many fronts, including:

- amortized electronic cash
- signature algebras
- forward-secure digital signature schemes
- author identification by compression metrics
- exposure-resilient cryptography
- protocol security against *concurrent* and *reset* attacks

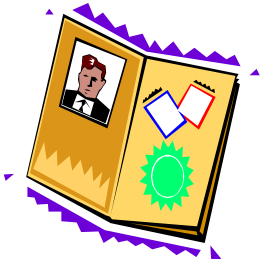
Shafi Goldwasser, Ronald L. Rivest, and Michael Sipser

Research Plan for the Next Six Months

Signature algebras: signature schemes with valuable algebraic properties.

Proof techniques: better methods for proving security of protocols.

Credential systems: better ways of demonstrating credentials without losing anonymity.



among others…