9807-12&26: Research in Cryptography, Information Security, and Algorithm Development

Shafi Goldwasser, Ronald L. Rivest and Michael Sipser

Project Overview

Our goal is to strengthen the foundations of security-enabling technologies. We explore novel cryptographic primitives, protocols, and applications. Our work ranges from the highly theoretical to the very practical.

9807-12&26: Research in Cryptography, Information Security, and Algorithm Development

Shafi Goldwasser, Ronald L. Rivest and Michael Sipser

Progress Through December 2001

- Secure multi-party protocols:
  - established limitations on the composition of authenticated Byzantine agreement and studied the consequences for secure multi-party computation
  - showed how to sequentially compose protocols where not all parties terminate at the same time
- Tamper-proof security
  - showed how to tolerate an adversary who can alter the secret key of an application
  - gave new protocols that tolerate reset attacks
- Electronic voting
  - gave a construction of robust mix-nets that implement anonymous channels instrumental for e-voting
- Cryptographic primitives
  - Tweakable block ciphers
  - Unique signatures
- Other work
  - Property testing
  - Cryptography over fields with unbounded computation
  - Fingerprinting
  - Cryptographic protocol compiler

9807-12&26: Research in Cryptography, Information Security, and Algorithm Development

Shafi Goldwasser, Ronald L. Rivest and Michael Sipser

Research Plan for the Next Six Months

- National ID card schemes
  - maintain privacy while enabling to provide quick identification when needed
  - address important issue in the U.S.
- Proof techniques
  - investigating security against stronger adversaries
  - towards automating proofs of security
- User authentication in pervasive environments
  - security with insecure basic components
  - authentication and yet privacy
- Cryptographic primitives
  - evidence suggests a lot of unexplored territory; inspiration from all-or-nothing transforms, tweakable block ciphers, cryptography over finite fields, unique signatures
- Security of routing protocols
  - routing is the most basic necessary functionality for the Internet
  - important to eliminate vulnerability of routing using cryptographic techniques