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

Shafi Goldwasser, Ronald L. Rivest and Michael Sipser

Project Overview

Goals of the project:

- Strengthen the foundations of security-enabling technologies
- Explore novel cryptographic primitives, protocols and applications
- Investigate related algorithmic questions

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

Shafi Goldwasser, Ronald L. Rivest and Michael Sipser

Progress Through June 2002

- Collusion-resistant fingerprints: improved lower bounds on the fingerprint size
- Signature scheme and efficient protocols for proving the knowledge of a signature without revealing any other information, and applications for anonymous credential systems
- Secure multi-party protocols in the asynchronous setting, and applications to broadcast in asynchronous point-to-point networks
- Testing of visual properties in binary images