Shafi Goldwasser, Ronald Rivest and Mike Sipser

Project Overview

- Quantum computation
- Threshold encryption
- Signature schemes
- Probabilistic property testing

Project 9807-12&26: Cryptography, Info. Security and Algorithm Dev.

Shafi Goldwasser, Ronald Rivest and Mike Sipser

Quantum Computation offers potentially the possibility of great speed improvement over classical computation.

Examples:

Shor's factoring algorithm

Grover's searching algorithm

Our recent work:

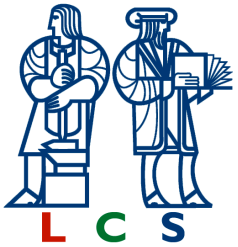
Simpler analysis of Grover's algorithm applied to counting, in preparation, by Ohta and Sipser

Plans: Beat Grover's algorithm.

Project 9807-12&26: Cryptography, Info. Security and Algorithm Dev.

Shafi Goldwasser, Ronald Rivest and Mike Sipser

ntt mit



Cryptography: Develop underlying security technology for secure internet applications with emphasis on rigorous and provable techniques.

Recent Work (details on following slides):

- Threshold Cryptography
- Subgroup Signatures

Plans:

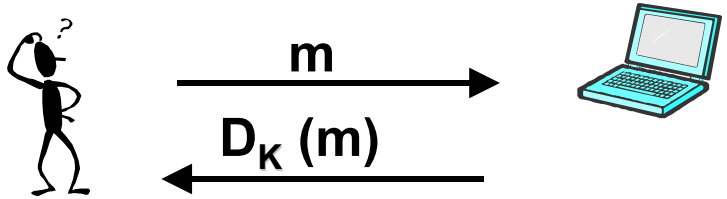
- Electronic Voting
- Concurrent Protocol Design

Project 9807-12&26: Cryptography, Info. Security and Algorithm Dev.

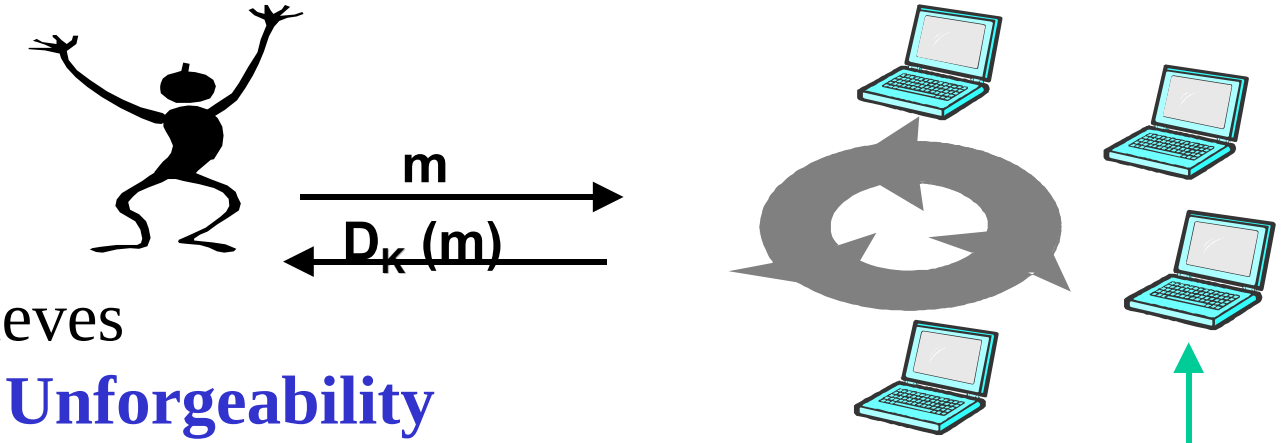
Shafi Goldwasser, Ronald Rivest and Mike Sipser

Threshold cryptosystems: **Decryption is traditionally implemented with a**

Single Server



Threshold Cryptosystem **protects against malicious faults using a** Distributed Protocol:



Achieves

- **Unforgeability**
- **Robustness**

If (# Faulty Players)
≤ Threshold

Malicious Faults:

- **breaking down**
- **sending wrong messages**

Results: First threshold cryptosystems secure in the presence of *adaptive adversary* in the following two powerful adversarial models:

- Concurrent Model, by **Anna Lysyanskaya**
- Erasure-Free Model, by **Stanislaw Jarecki and Anna Lysyanskaya**

[Both results to be presented at Eurocrypt 2000]

- In both models, we exhibit cryptosystems secure against *adaptive chosen ciphertext attack* (the strongest notion of security)

Project 9807-12&26: Cryptography, Info. Security and Algorithm Dev.

Shafi Goldwasser, Ronald Rivest and Mike Sipser

- Problem: several members of a given group need to sign a document. For example, a corporation requires signatures of three senior officers for any large transaction.
- Traditionally, handwritten signatures provide for:
  - Flexibility: any subgroup can sign the document.
  - Accountability: anyone who signs the document can be individually identified and held responsible.
- No satisfactory digital solution provides both.
  - Using several single-signer signatures is inefficient:
  - "Multi-signatures" and "Group Signatures" lack flexibility.
  - "Threshold signatures" lack accountability.
- Recent Work : "Provable-Subgroup Signatures", by Micali, Ohta and Reyzin
  - **An efficient scheme providing complete flexibility and individual accountability**
  - **A general, formal model in which to analyze the security of such schemes**.

Project 9807-12&26: Cryptography, Info. Security and Algorithm Dev.

Shafi Goldwasser, Ronald Rivest and Mike Sipser

Probabilistic Property testing is a new algorithmic technique which examines only constant probabilistic samples of the input and works in complexity independent of the size of the input trading off speed for accuracy. It has been applied with great success to testing NP-hard graph properties, testing algebraic and combinatorial functional properties such as linearity and monotonicity, and testing properties of classical linear algebra structures.

High Lights

- property testing of NP hard Graph problems such as graph coloring in constant time by Goldwasser, Goldreich and Ron

Recent Work

- "Improved Testing Algorithms for Monotonicity", by Dodis, Goldreich, Lehman, Raskhodnikova, Ron, and Samorodnitsky, appeared in the Proceedings of RANDOM, August 1999

Future Plans

- Apply property testing to properties such as routing and congestion on graphs resulting from the web