Shafi Goldwasser, Ronald L. Rivest and Mike Sipser

Project Overview

- **Focus on designing secure cryptographic protocols in multi-party(distributed) and two-party scenarios.**

- **Emphasis is on the development of novel frameworks and theoretical provably secure solutions to problems arising from applications.**

Shafi Goldwasser, Ronald L. Rivest and Mike Sipser

Progress Through June 2000

- **Invented novel Commitment Schemes which are perfectly binding and perfectly information hiding, using a third party and secure communication channels [Rivest, Rivest-Ohta]**

- **Showed optimal lower bounds for All-or-Nothing-Transforms [Dodis-Sahai - Smith]**

- **Significant efficiency improvements on secure threshold protocols in the erasure free model [Jarecki - Lysyanskaya]**

- **Developed a new, more refined, model for studying the security of block ciphers [Reyzin - Ramzan]**

- **Designed identification protocols for asynchronous environments such as the web [Goldwasser et al]**

Shafi Goldwasser, Ronald L. Rivest and Mike Sipser

Research Plan for the Next Six Months

• A resource which is heavily used in threshold cryptography is for the dedicated servers to share in advance, in an off-line set-up stage, randomness to be used later during the on-line protocol.
We plan to work on eliminating the need for advance shared randomness and hopefully replacing it by pseudo-random generation on-line.

• We plan to explore receipt-free multi-party computation, which has particular application to electronic voting.

• In a recent breakthrough, Reyzin, Rivest, and Ramzan were able to develop a simple necessary and sufficient condition for determining when a block cipher of a relatively general form is secure against adaptive chosen plaintext attacks. We hope to develop similar conditions for determining security against adaptive chosen plaintext and ciphertext attacks. The overall goal is to gain a more fundamental understanding of what makes block ciphers secure.