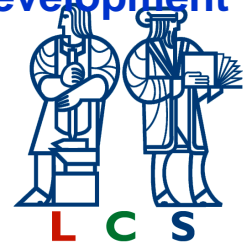




## Project Overview

**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.**



## Progress Through June 2001

Progress on many fronts, including:

- §§ Protocols secure against Resettable Attacks
- §§ Ring Signatures
- §§ Identity Escrow Schemes
- §§ Threshold Cryptography
- §§ Monotonicity Testing



## Research Plan for the Next Six Months

**Identify escrow applied to electronic voting**

**Specialized Workshop on Voting technologies**

**Explore Zero Knowledge Proofs of knowledge  
using non Black Box definitions**

*among others...*