MIT CSAIL

CRYPTOGRAPHY AND INFORMATION SECURITY GROUP

The Cryptography and Information Security Group seeks to develop techniques for securing tomorrow's global information infrastructure by exploring theoretical foundations, near-term practical applications, and long-range speculative research.

Principal Investigators:

Shafi Goldwasser
Telephone: 617-253-5914
Email: shafi@csail.mit.edu

Vinod Vaikuntanathan
Telephone: 617-324-8444
Email: vinodv@csail.mit.edu

Silvio Micali
Telephone: 617-253-5949
Email: silvio@csail.mit.edu

Butler Lampson
Telephone: 617-253-6004
Email: blampson@microsoft.com

Ronald Rivest
Telephone: 617-253-5880
Email: rivest@mit.edu

Yael Tauman Kalai
Telephone: 617-253-5851
Email: tauman@mit.edu

CSAIL / MIT

Website:
toc.csail.mit.edu/cis

Location:
The Cryptography and Information Security (CIS) Group is located in the Ray and Maria Stata Center at MIT.

Research Group Address:
Cryptography and Information Security Group
MIT CSAIL
32 Vassar Street
Cambridge, MA 02139

Research Vision

We aim to understand the theoretical power of cryptography and the practical engineering of secure information systems, from appropriate definitions and proofs of security, through cryptographic algorithm and protocol design, to implementations of real applications with easy-to-use security features.

Areas of Research

- Security of cryptographic algorithms and protocols
- Algorithms and theory
- Security and cryptography
- Quantum computing
- Machine learning
- Cryptographic policy

Research Activities

- Lattice-based Cryptography
- Fully Homomorphic Encryption
- Program Obfuscation
- Cryptography and Quantum Computing
- Security and Privacy in Machine Learning
- Blockchains and Cryptocurrencies
- Voting Systems

Industry Applications

- Cybersecurity
- Wireless

In the News

- Algorand Founder Silvio Micali Breaks Down How To Construct A Fast And Secure Blockchain In A World Full Of Adversaries (link)

- By securely aggregating sensitive data from cyber-attacks, the SCRAM platform from MIT CSAIL can quantify an organization's level of security and suggest what to prioritize. (link)

MIT CSAIL

"In the late 1970s, we didn't even have the World Wide Web, it was impossible to imagine that our method would become what it is today. Right now, each time we make an online purchase, the transaction's security is based on our encryption technology."

– Ronald Rivest

Current People in the Cryptography and Information Security Group

Principal Investigators

Shafi Goldwasser
Silvio Micali
Ronald Rivest
Vinod Vaikuntanathan
Butler Lampson
Yael Tauman Kalai

Postdocs, Graduate Students, and Researchers

Rishab Goyal
Alex Lombardi
Leo de Castro
Lisa Yang
Lalita Devadas
Surya Mathialagan
Neekon Vafa