

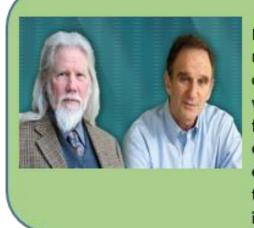
ACM A.M. Turing Award Winners in Cryptography

Cryptography and Information Security (CrIS) Lab

Analysis of Algorithms Artificial Intelligence Combinatorial Algorithms Computational Complexity Computer Architecture Cryptography Data Structures Databases Education Error Correcting Codes Finite Automata Graphics Interactive Computing Internet Communications List Processing Numerical Analysis Numerical Methods Object Oriented Programming Operating Systems Personal Computing **Program Verification Programming** Programming Languages Proof Construction Software Engineering

Verification of Hardware and Software Models Computer Systems Machine Learning Parallel Computation





WHITFIELD DIFFIE, MARTIN HELLMAN (2015)

Diffie and Hellman introduced a radically new method of distributing cryptographic keys called "Diffie-Hellman key exchange", which went far toward solving one of the fundamental problems of cryptography; key distribution. Their work on public-key cryptography has made encryption technologies accessible to individuals and companies.

Public Key Cryptography

Oblivious Transfer, Broadcast, and **Byzantine Agreement**



SHAFI GOLDWASSER, SILVIO MICALI (2012)

Goldwasser and Micali's work helped make cryptography a precise science. The mathematical structures they created such as formal notions of privacy, adversaries, pseudorandomness, interactive proofs, and zeroknowledge proofs are key tools of modern cryptography.

Multiparty Computation, Verifiable Secret Sharing, and Zero-Knowledge

CrIS Lab Research

Secret Sharing Schemes



RONALD L. RIVEST, ADI SHAMIR, LEONARD M. ADLEMAN (2002)

Rivest, Shamir, and Adleman invented the RSA algorithm, which was one of the first practical public-key cryptosystems. While Rivest invented symmetric key encryption algorithms such as RC2, Shamir made advances in differential cryptanalysis and identity-based cryptography. Adleman was the first to successfully use DNA to compute an algorithm, and is referred to as the "Father of DNA computing".

Contact:

Cryptography and Information Security (CrIS) lab Room 329, Department of Computer Science & Automation Indian Institute of Science Email: cryptology.iisc@gmail.com

Talk: **Turing Awardees in** Cryptography

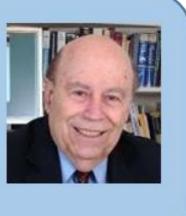




Alan M. Turing was an English computer scientist, mathematician, logician, cryptanalyst and theoretical biologist. He was highly influential in the development of theoretical computer science, providing a formalisation of the concepts of algorithm and computation with the Turing machine, which can be considered a model of a general purpose computer. Turing is widely considered to be the father of theoretical computer science and artificial intelligence.

MICHAEL O. RABIN (1987)

Rabin invented the Rabin cryptosystem, the first asymmetric cryptosystem whose security was proved equivalent to the intractability of integer factorization. His later work concerns cryptographic problems for preventing piracy on the internet. His other important contributions include his concept of non deterministic machines, the Rabin-Karp String Search Algorithm, the Miller- Rabin primality test, and probabilistic automata.



Commitment Schemes, **Coin Tossing** Protocol

MANUEL BLUM (1995)

The notion of commitments, ar important tool in cryptography, was introduced through Blum's protocol for flipping a coin over the telephone. Some of his other work includes the Blum Blum Shub pseudorandom number generator, the Blum-Goldwasser more recently cryptosystem, and CAPTCHAs.



Secure Computation

ANDREW CHI-CHIH YAO (2000)

Yao introduced the paradigm of secure function evaluation through the famous "Millionaire's Problem" . His technique of garbled circuits is fundamental in large-scale secure computation problems, like privacy-preserving matching in DNA databases. He is also well known for his contributions to the theory of computation, complexity-based theory of pseudorandom number generation, and computational entropy and its use for characterization of encryption security.



Convenor: Arpita Patra

Lab Members: Ajith Suresh, Divya Ravi, Megha Byali, Pratik Sarkar and Swati Singla

Visitors: Chaya Ganesh, Yashvanth Kondi and Gayathri Annapurna