Abstract

Oberwolfach Workshop:

Cryptography

Dates:

19 Jan - 24 Jan 2025   (Code: 2504)

Organizers:

Johannes Buchmann, Darmstadt
Shafi Goldwasser, Berkeley
Yael Tauman Kalai, Cambridge MA
Vinod Vaikuntanathan, Cambridge MA

The science of cryptography lies at the very foundations of trust in current and future systems and devices for communication and computation. In the last decade, there have been spectacular advances in cryptography, in the areas of encrypted computation, program obfuscation, verifiable outsourcing of computation, mathematical foundations including elliptic curves and isogenies, and lattice-based cryptography, cryptographic techniques in machine learning, and more. The Oberwolfach workshop in cryptography will bring together experts from mathematics and computer science such as algorithmic number theory and algebra, quantum computation and complexity theory, in order to discuss recent advances and make progress in constructing the new generation of cryptographic systems that protect the future of information and computation.