UNIVERSITÀ DI TRENTO | Dipartimento di Matematica

De Cifris Trends in Modern Cryptography
PROGRAM

Title and Date	Subject	Lecturers
1 - Course introduction Monday the 2nd - 15:00	• Sketch of the course • Introduction to post-quantum cryptography • Intro to cloud encryption • Intro to complexity theory	Massimiliano Sala, Marco Calderini (UNITN)
2 - Lattices mod 1 Tuesday the 3rd - 15:00	Linear algebra over lattices: • Basis of a lattice • Dimension of a lattice • Length and distance	Lea Terracini (UNITO)
3 - Lattices mod 2 Wednesday the 4th - 15:00	Determinant: • Fundamental Domain • Determinant • Hadamard's inequality • Hermite's Theorem	Giordano Santilli (UNITN)
4 - Problems over lattices Thursday the 5th - 15:00	• SVP e CVP • Appr-SVP • Gaussian heuristic • LLL • Babai's Closest Vertex Algorithm	Stefano Barbero (POLITO)
5 - Complexity of the problems for lattices Friday the 6th - 16:00	• Complexity of SVP • Complexity of CVP • Complexity of their approximate versions	Massimo Lauria (Roma Sapienza)
6 - NTRU encryption Monday the 9th - 15:00	• The encryption algorithm (classical) NTRU • The NTRU-HRSS-KEM (NIST submission round 2)	Nadir Murru (UNITN)
7 - Attacks to NTRU Tuesday the 10th - 15:00	• Coppersmith and Shamir • Other attacks	Andrea Visconti (UNIMI)
8 - LWE Wednesday the 11th - 15:00	• LWE on lattices • LWE on polynomial rings	Roberto Civino (UNIVAQ)
9 - Crystals & Saber Thursday the 12th - 17:00	• The cryptosystems Crystals, Kyber and Dilithium • The cryptosystem Saber	Andrea Basso (University of Birmingham)

10 - Problems on codes Friday the 13th - 15:00	• Linear codes • The MLD problem • The equivalence problem	Marco Timpanella (UNIPG)
11 - Code-based cryptography Monday the 16th - 15:00	• McEliece • Niederreiter • LEDAcrypt	Marco Baldi (UNIVPM)
12 - Foundations of multivariate crypto Tuesday the 17th - 15:00	• Definition of the MQ problem • Methods to solve multivariate polynomial systems • Special methods for the finite field case	Michela Ceria (POLIBA)
13 - Rainbow digital signature Wednesday the 18th - 16:00	• The digital signature scheme Rainbow • Security of Rainbow	Roberto La Scala (UNIBA)
14 - ABE-paring Thursday the 19th - 17:00	• Formal properties of pairings • Tate pairing • Weil pairing	Laura Capuano (ROMA3)
15 - ABE-IBE Friday the 20th - 15:00	• Boneh Franklin scheme • Fuzzy IBE	Annamaria Iezzi (UNINA)
16 - Ciphertext-policy ABE Monday the 23rd - 15:00	• CP-ABE based on lattices • CP-ABE based on pairings	Marco Pedicini (ROMA3)
17 - Key-policy ABE Tuesday the 24th - 15:00	• Key policy ABE • Revocable storage	Riccardo Longo (UNITN)
18 - FE I Wednesday the 25th - 15:00	• Introduction to Functional Encryption • Security notions and mathematical assumptions	Irene Villa (UNITN)
19 - FE II Thursday the 26th - 15:00	• Predicate Encryption (PE) • PE with public index • PE with private index	Carla Mascia (UNITN)
20 - Secure multi-party computation Friday the 27th - 15:00	• Security goals and proofs • MPC based on Threshold Secret Sharing • SPDZ	Mario Di Raimondo (UNICT)