UNIVERSITÀ DEGLI STUDI
DI TRENTO

Dipartimento di Matematica

"Post-quantum Cryptography"

Docente: Prof. Massimiliano Sala

Assistenti: dott.ssa Michela Ceria, dott. Alessio Meneghetti, dott. Federico Pintore

Lingua: il corso si tiene in italiano, con parte del materiale in inglese.

Luogo: Roma

Ore di lezione: 30 ore di lezione e 10 ore di laboratorio.

Periodo: 7 – 11 maggio 2018

A chi è rivolto

Il corso è rivolto a professionisti operanti nel campo della sicurezza informatica (PA o aziende private). Il corso è adatto sia a professionisti (di formazione tecnica, informatica o ingegneristica) interessati a vedere gli aspetti algebrici/matematici, sia a persone con buone competenze matematiche, interessate a vedere le applicazioni crittografiche.

Abstract:

The security of post-quantum cryptosystems is based on the hardness of mathematical problems which are not solvable with quantum computer as yet.
The course will provide an overview, including the recent NIST proposals, and will focus on four main paths for post-quantum cryptography:

- Lattice-based cryptography (including NTRU);
- Code-based cryptography (including McEliece);
- Multivariate cryptography (including Oil-Vinegar);
- Isogeny-based cryptography (including SIDH).

Organizzazione e logistica

Il corso sarà effettuato nel mese di maggio 2018, da lunedì 7 a venerdì 11 (compresi).
Le lezioni si terranno la mattina dalle 9:00 alle 13:00 e il pomeriggio dalle 14:00 alle 18:00.

Costo del corso

La deadline per le iscrizioni al corso è il 20 aprile 2018.
Il numero minimo di partecipanti è 4, il numero massimo è 8.
Il costo didattico totale per il singolo corso è di 1500 euro a persona (esente da IVA).

Informazioni
Per ogni informazione contattare la dott.ssa Francesca Stanca (cryptolabmat@unitn.it).

Modalità di pagamento
Il pagamento della relativa quota dovrà essere effettuato a ricezione della fattura, mediante bonifico bancario a:

Banca Popolare di Sondrio
p.zza Centa, 14 - 38122 Trento, Italy

IBAN: IT06 N 05696 01800 000003108X60
Swift: POSOIT22

Causale: CRITTO18.