UNIVERSITÀ DEGLI STUDI
DI TRENTO

Dipartimento di Matematica

“Post-quantum Cryptography 2019”

Docente: Prof. Massimiliano Sala

Assistenti: Dott. Alessio Meneghetti, Dott. Giordano Santilli

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: 13 – 17 maggio 2019

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:

Il corso presenta una panoramica sulle quattro classi di cifrari post-quantum più studiati:

- Lattice-based cryptography;
- Code-based cryptography;
- Multivariate cryptography;
- Isogeny-based cryptography.

Visti i risultati del "**Round 2"** del "**NIST** standardization assessment", il corso si concentrerà sui cifrari *lattice-based* e, parzialmente, sui cifrari *code-based*.

Organizzazione e logistica

Il corso sarà effettuato nel mese di maggio 2019, da lunedì 13 a venerdì 17 (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 9 maggio 2019.
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: CRITTO19.