



UNIVERSITÀ DEGLI STUDI  
DI TRENTO

---

Dipartimento di Matematica

## “Cloud encryption: functional encryption e attacchi crittoanalitici”

**Organizzatore scientifico:** Prof. Massimiliano Sala

**Docenti:** prof. Massimiliano Sala, dott.ssa Carla Mascia

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

**Luogo:** Roma

**Ore di lezione:** 40 ore di lezione, compreso laboratorio e videolezioni

**Periodo:** dal 12 al 16 ottobre 2020

### 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:

I cifrari di tipo Functional Encryption permettono di eseguire una singola operazione prefissata sui dati cifrati senza svelarla alla piattaforma cloud che li ospita. Sebbene questi cifrari abbiano applicabilità limitata rispetto alla cifratura omomorfa, sono molto efficienti.

In questo corso saranno esaminati i principali sistemi di Functional Encryption, compresi quelli basati sulla Teoria dei Numeri, nonché gli attacchi crittoanalitici più pericolosi.

## **Organizzazione e logistica**

Il corso sarà effettuato a Roma nella settimana dal 12 al 16 ottobre 2020.

Le lezioni si terranno la mattina dalle 9:00 alle 13:00 e il pomeriggio dalle 14:00 alle 18:00, per un totale di cinque giorni consecutivi.

## **Costo del corso**

Il numero di partecipanti massimi è 10.

Il costo didattico totale per il singolo corso è di 2000 euro a persona (esente da IVA).

In caso di iscrizione di quattro persone, il costo è forfettariamente fissato in 7.334,00 euro.

## **Informazioni**

Per ogni informazione contattare la dott.ssa Francesca Stanca ([cryptolabmat@unitn.it](mailto:cryptolabmat@unitn.it)).

## **Modalità di pagamento**

Il pagamento della relativa quota dovrà essere effettuato a ricezione della fattura, mediante bonifico bancario.

INTESTAZIONE: Università degli Studi di Trento

BANCA: Banca Popolare di Sondrio - Piazza Centa, 14 - 38122 Trento, Italy

**IBAN: IT06 N 05696 01800 000003108X60**

**Swift: POSOIT22**

Causale: CRITTO20.