DeCifris@univaq

Norberto Gavioli

norberto.gavioli@univaq.it

Dipartimento di Ingegneria e Scienze dell'Informazione e Matematica
Università degli Studi dell'Aquila

EVENTO CONOSCITIVO DELL'ASSOCIAZIONE DE COMPONENDIS CIFRIS
Roma, 22 gennaio 2018

Crittografia al Dipartimento di Ingegneria e Scienze dell'Informazione e Matematica

Didattica

Diversi corsi di laurea interessati

- Matematica
- Informatica
- Ingegnerie Informatica, Automatica e delle Telecomunicazioni

A fronte di un unico insegnamento "Combinatorics and Cryptography".

Inizialmente nasce come corso di "Algebra Concreta" con contenuti di tipo applicativo, erogato dal corso di laurea in matematica. Viene successivamente fuso con corsi di teoria dei codici e crittografia erogati dalle ingegnerie.

Interessi di ricerca

Siamo interessati agli aspetti algebrici della crittografia in particolare

- Applicazioni della teoria dei gruppi alla crittografia (chiave pubblica, word problem, conjugacy search problem, sicurezza di cifrari a blocchi. . .)
- Crittografia basata sulle curve ellittiche (index calculus, summation polynomials, . . .)
- Crittografia basata su reticoli e anelli di polinomi (NTRU e sue generalizzazioni)
- Schemi di scambi di chiave basati su strutture algebriche (gruppi, anelli, algebre anche non associative)
- Applicazioni della crittografia (firma digitale, applicazioni blockchain, . . .)

Risorse

Al momento partecipiamo a un PRIN con un progetto di algebra e crittografia coordinato dal prof. Massimiliano Sala di Trento.

Risorse umane

- due docenti di algebra
- altri docenti interessati
- un ricercatore (appena chiamato dal Dipartimento)
- un postdoc (in arrivo marzo/aprile 2018)
- uno studente di dottorato
- studenti di tesi triennali e magistrali su più corsi di laurea

Altre dotazioni: laboratorio con accesso dedicato a un cluster GPU (Caliban)

Altre Attività

- Recente coinvolgimento in progetti PON
- Progetti culturali con scuole superiori (percorso di crittografia alternanza scuola lavoro,. . .)
- Interesse verso iniziative scientifiche, divulgative e culturali (convegni, stages, gare di crittografia, . . .)
- Interesse verso collaborazioni esterne