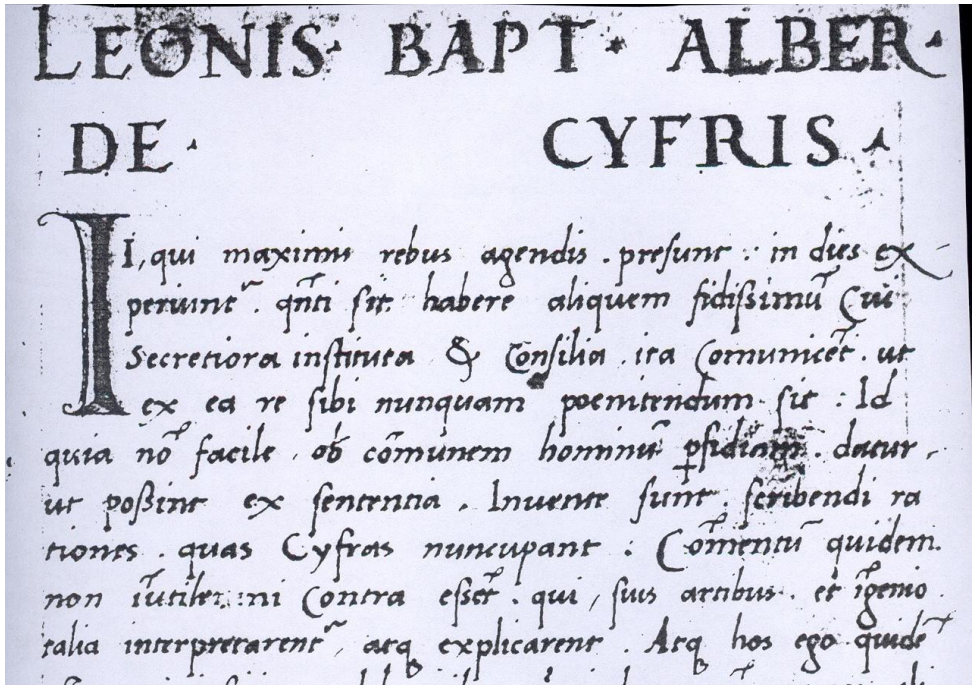
LEONIS BAPT. ALBER-
DE CYFRIS.
Il qui maximis rebus agendis presunt : in dies ex-
periunt qnti sit habere aliquem fidissimu cui
Secretiora instituta & Consilia ita communicet. ut
ex ea re sibi nunquam poeniteudum sit : Id
quia no facile ob comunem hominu pfidiam. datur
ut possint ex sententia. Inuenta sunt scribendi ra
tiones. quas Cyfras nuncupant : Comentu quidem.
non iutilem. ni Contra esset. qui, suis armis. et igemo
talia interpretarent, arq explicarent. Arq hos ego quide

De Cifris Schola Latina

ROMA TRE UNIVERSITÀ DEGLI STUDI

DIPARTIMENTO DI INFORMATICA

SAPIENZA UNIVERSITÀ DI ROMA

disim

Università di Roma Tor Vergata

Martedì 15 febbraio 2022 – ore 14:30

Luca De Feo

IBM Zurigo

Crittografia a Base di Isogenie

Abstract: Le isogenie sono morfismi di varietà abeliane. La loro teoria algoritmica è sviluppata da oltre 30 anni, motivata in parte dall'algoritmo di Schoof-Elkies-Atkin per il conteggio di punti, algoritmo fondamentale in crittografia ellittica. I progressi algoritmici hanno portato negli ultimi 20 anni allo sviluppo di una nuova branca della crittografia, detta a base d'isogenie. L'oggetto centrale di questa disciplina non è più una curva ellittica isolata, bensì un grafo di curve ellittiche legate da isogenie. I grafi d'isogenie esibiscono diverse strutture combinatorie interessanti (foreste, grafi di Cayeley, grafi espansori) e offrono dei problemi computazionalmente difficili come la ricerca di cammini. Su queste basi, siamo oggi in misura di costruire un vasto spettro di primitive crittografiche: cifratura e firma digitale resistenti agli attacchi quantistici, crittografia a orologeria, sistemi a soglia, ecc. In questo talk darò un'introduzione alla teoria delle isogenie di curve ellittiche su corpi finiti e spiegherò come la crittografia è costruita a partire da esse.

Il seminario sarà in presenza, presso l'Aula Dal Passo del Dipartimento di Matematica dell'Università Tor Vergata. Per partecipare bisogna avere il Super Green Pass o un certificato equivalente.

Per accedere al seminario via Teams:

click here

http://www.mat.uniroma2.it/~ricerca/geomet/SeminariGeometria2122/Abstracts2122/Luca_DeFeo.html

Il link per accedere apparirà un'ora prima dell'inizio del seminario

Contact person: Giulio Codogni (codogni@mat.uniroma2.it)

CONTATTI
Associazione De Componendis Cifris

seminari@decifris.it
segreteria@decifris.it