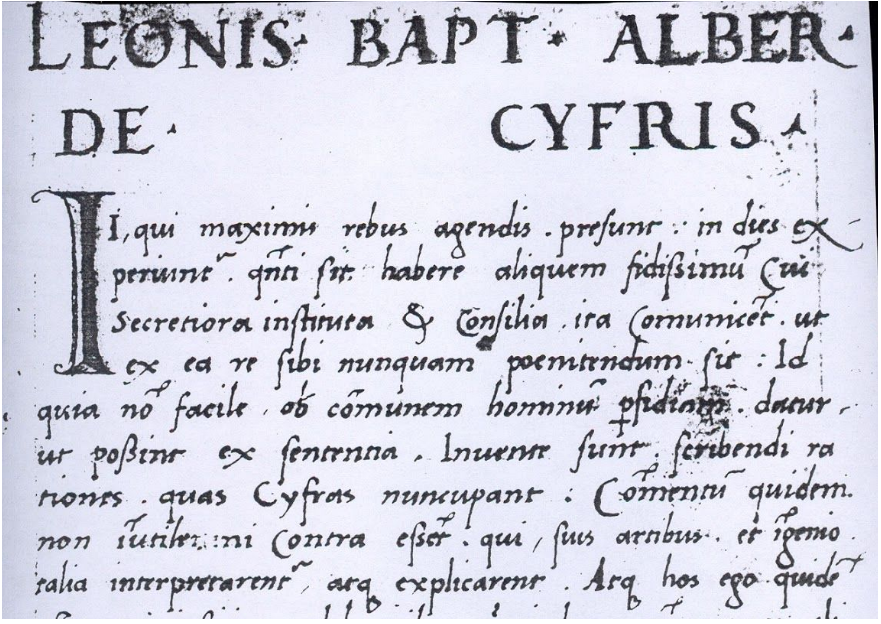

LEONIS BAPT ALBER

DE CYFRIS

Ii, qui maximis rebus agendis presunt: in dies experiunt quanti sit habere aliquem fidissimum cui secretiora instituta & consilia ita committeret, ut ex ea re sibi nunquam poenitendum sit: Id quia non facile ob comunem hominum perfidiam datur, ut possint ex sententia. Inuenti sunt scribendi rationes quas Cyfras nuncupant: Comentum quidem non iutile nisi contra esset: qui, suis artibus, et ingenio talia interpretarent, atq explicarent. Atq hos ego quidem

De Cifris Schola Latina

Monday 13th May 2019 - at 12h00
Seminar Room M3
Department of Mathematics and Physics
Largo San Leonardo Murialdo 1 - Polo Aule

Luca De Feo

Universitè de Versailles

Abstract:

Isogenies of elliptic curves have recently come under the spotlight thanks to their applications in post quantum cryptography. The two prominent isogeny-based primitives, SIDH and CSIDH, provide,respectively, the key encapsulation with the lowest communication complexity among all candidates to the NIST post-quantum competition,and the only known efficient post-quantum non-interactive key exchange. Computational problems related to isogenies have been studied for more than 30 years, owing to their connections to elliptic curve cryptography. I will thus start by reviewing the relevant computational problems, and highlight some recent results. I will then introduce isogeny graphs, and explain how they are useful in cryptography; in particular I will point out what they are good for, what they are not-so-good at, and what they are absolutely terrible at. Finally, I will present some research perspectives and some important open problems.

Contact Person: Giulio Codogni

CONTACTS

Associazione De Componendis Cifris

direttore@decifris.it
segreteria@decifris.it