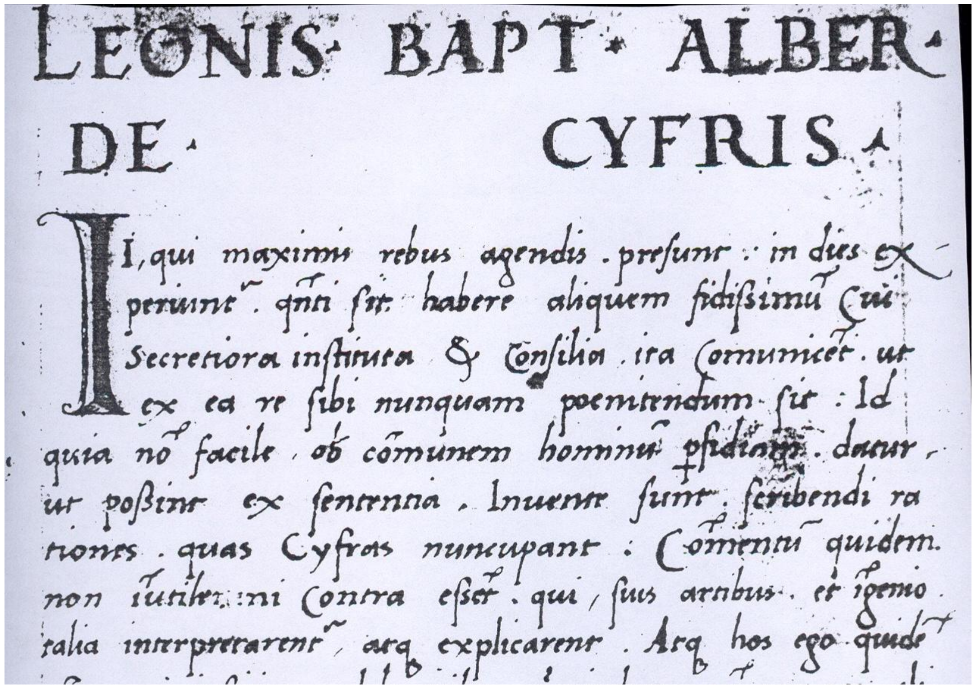

LEONIS BAPT ALBER
DE CYFRIS

Ii, qui maximis rebus agendis . preſunt : in dies experiunt͂ . q̃nti ſit habere aliquem fidiſsimũ cui Secretiora inſtituta & Conſilia . ita Comunicet . ut ex ea re ſibi nunquam poenitendum ſit : Id quia nõ facile . ob cõmunem hominũ pfidiam . datur , ut poſsint ex ſententia . Inuente ſunt . ſcribendi rationes . quas Cyfras nuncupant : Comentũ quidem non inutile . nisi Contra eſset . qui , ſuis artibus . et igenio talia interpretarent͂ , atq explicarent . Atq hos ego quide

De Cifris Schola Latina

Dipartimento di Informatica
Sapienza Università di Roma

disim

De Cifris

Università degli Studi di Roma Tor Vergata

DMF Roma Tre Università degli Studi

Martedì 31 Maggio 2022 – 14.30

Annamaria Iezzi

Università di Napoli

Computing the endomorphism ring of a supersingular elliptic curve

Abstract: In recent years, isogeny-based cryptosystems have captured the attention of the math/crypto community for their conjectured resistance to quantum attacks. In this context, the most promising protocols have supersingular elliptic curves defined over finite fields as central objects, and their security is based on the mathematical problem of computing an isogeny between two supersingular elliptic curves E and E'. It has been shown that this problem can be reduced to the computation of the endomorphism rings of E and E'. In this talk, after reviewing the mathematical and cryptographic context, we will present an improved algorithm for computing the endomorphism ring of a supersingular elliptic curve over a finite field. This is joint work with Jenny G. Fuselier, Mark Kozek, Travis Morrison and Changningphaabi Namoijam.

Il seminario sarà in presenza, presso l'Aula Dal Passo del Dipartimento di Matematica dell'Università Tor Vergata.

Qui troverete poco prima dell'inizio del seminario il collegamento per partecipare in forma telematica via Teams.

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

CONTATTI

Iniziativa De Componendis Cifris

seminari@decifris.it
segreteria@decifris.it