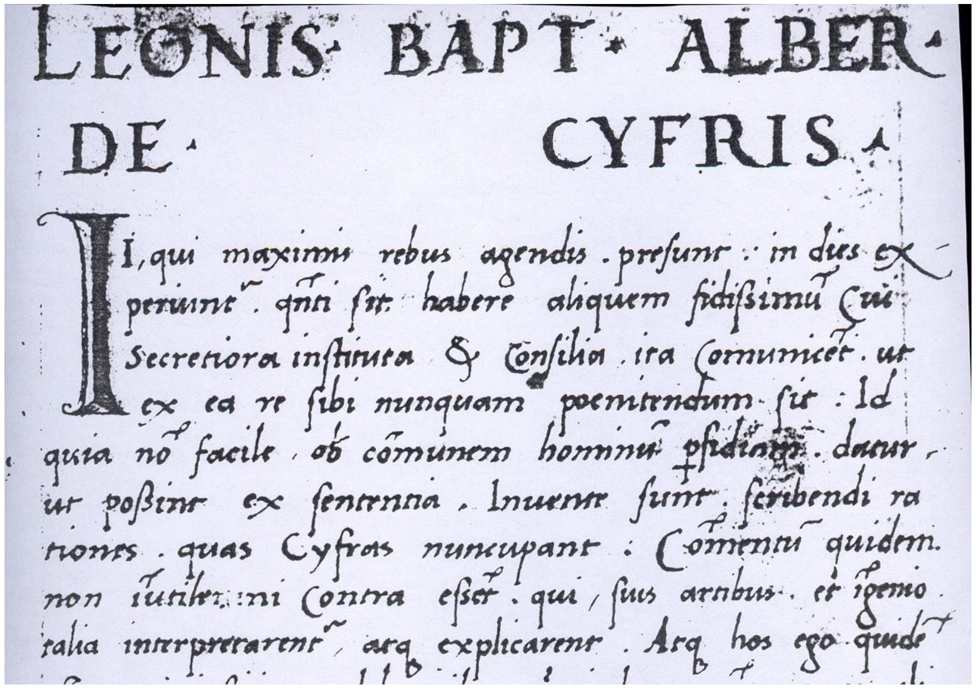

LEONIS BAPT· ALBER·
DE· CYFRIS·

I, qui maximis rebus agendis presunt : in dies experiunt'. qnti sit habere aliquem fidissimu cui Secretiora instituta & consilia ita comunicet . ut ex ea re sibi nunquam poenitendum sit : Id quia no facile ob comunem hominu pfidiam . datur . ut possint ex sententia . Inventa sunt scribendi rationes . quas Cyfras nuncupant : Comentu quidem non inutile nisi contra esset . qui, suis artibus . et ingenio talia interpretarentur . atq explicarent . Atq hos ego quide

# De Cifris Schola Latina

Dipartimento di Informatica
Sapienza Università di Roma

disim

Roma Tre Università degli Studi

Università di Roma Tor Vergata

## Tuesday 30th November 2021 – at 14:30

## Federico Pintore

## Università di Bari

# Collision on isogeny graphs and the security of the SIDH-based identification protocol

**Abstract**: The digital signature schemes that have been proposed so far in the setting of the Supersingular Isogeny Diffie-Hellman scheme (SIDH) were obtained by turning an interactive identification protocol by De Feo, Jao and Plût into non-interactive schemes. The security of the resulting schemes is therefore deduced from that of the base identification protocol. In this talk, we revisit the proofs that have appeared in the literature for the special soundness property of the above-mentioned SIDH-based identification protocol. The existence of some special cycles in supersingular isogeny graphs make such previous proofs fail.

This conference is in-person. It will be held at the Aula Dal Passo of the Department of Mathematics of the University Tor Vergata. To attend, it is compulsory to have a valid Green pass or vaccination card.

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

CONTATTI
**Associazione De Componendis Cifris**

seminari@decifris.it
segreteria@decifris.it