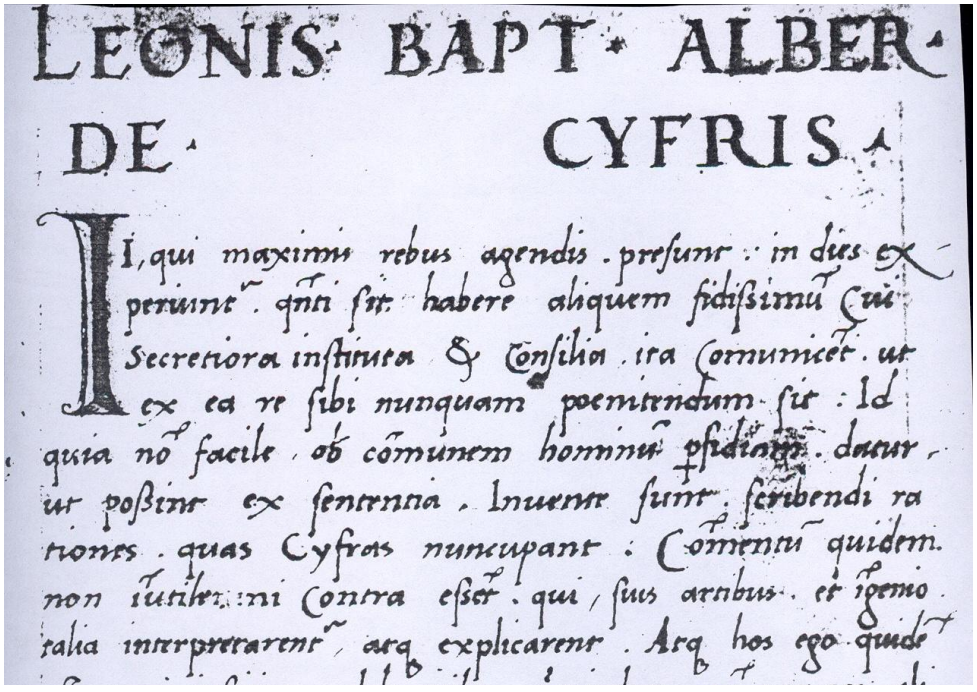
LEONIS BAPT. ALBER-
DE CYFRIS.

II, qui maximis rebus agendis præsunt: in dies ex-
periuntur quàm sit habere aliquem fidissimum cui
Secretiora instituta & Consilia ita communicet, ut
ex ea re sibi nunquam pœnitendum sit: Id
quia nō facile ob cōmunem hominū pfidiam dabur,
ut possint ex sententia. Inuenta sunt scribendi ra
tiones, quas Cyfras nuncupant: Commentū quidem
non iucundum contra esset, qui, suis armis, et igemo
talia interpretarent, atq explicarent. Atq hos ego quide

PostQuantumCifris

Thursday 9th June 2022 – at 4:00 p.m.

Online Seminar via Zoom

Edoardo Persichetti

Florida Atlantic University

Developing Innovative Frameworks for Efficient Code-based Signatures

Abstract: Code-based cryptography is one of the most popular areas of research in the post-quantum family. Yet, while solutions for encryption and key exchange are now recognized to be stable and have reached a good level of performance, the same can't be said for signature schemes. Several protocols have been proposed over the years, the near entirety of which have either been broken, or exhibit very undesirable features, leading to impractical schemes. In this talk, I will discuss a variety of recent approaches based on zero-knowledge that are able to offer transformative solutions, paving the way for truly practical schemes.

The seminar will be at: Università Politecnica delle Marche, Facoltà di Ingegneria, Aula 155/d1 (+ streaming)

Registration for the online event to *be made by* 8th June via the following link:

click here

Subscribers will receive the Zoom ID one hour before the start of the event

Contact person: Marco Baldi (m.baldi@staff.univpm.it)

CONTACTS
De Componendis Cifris Association

segreteria@decifris.it
seminari@decifris.it