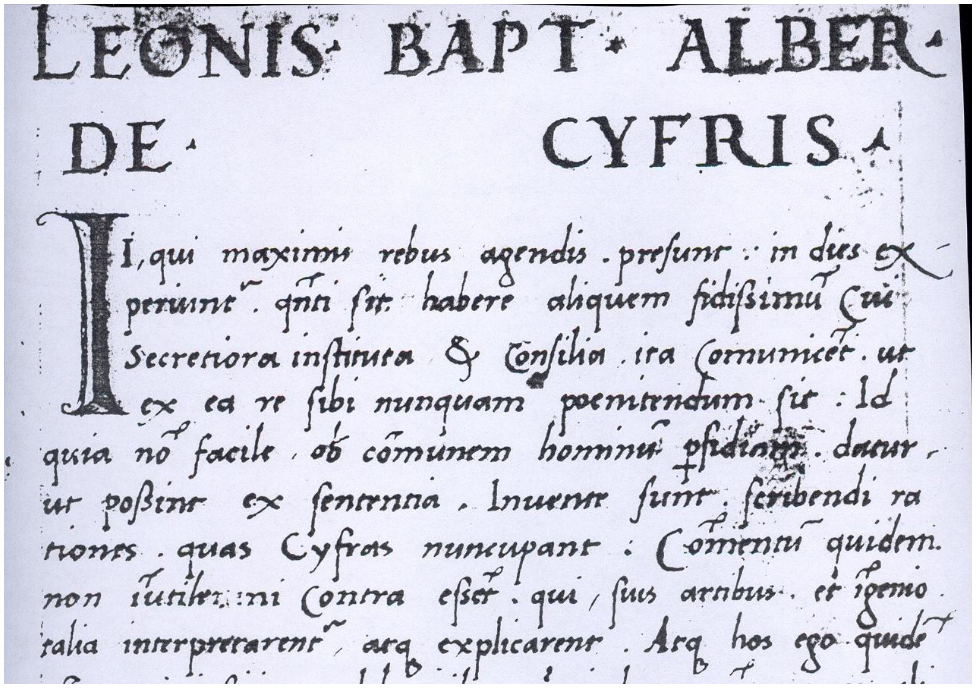

LEONIS BAPT ALBER
DE CYFRIS

II, qui maximis rebus agendis presunt : in dies ex
periunt . quanti 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 . Inuente sunt . scribendi ra
tiones . quas Cyfras nuncupant : Comenti quidem
non inutiler nisi contra esset . qui / suis artibus . et ingenio
talia interpretarent , atq explicarent . Atq hos ego quide

PostQuantumCifris

Tuesday 2nd november 2021 – at 3:00 p.m.

Online Seminar via Zoom

Paolo Santini

Università Politecnica delle Marche

Recent advances in code-based encryption and digital signatures

Abstract: Code-based cryptography is widely recognized as one of the most promising solutions to build efficient public-key cryptosystems with post-quantum security. Initiated by Robert McEliece in 1978, this kind of cryptosystems is constructed around the so-called Syndrome Decoding Problem (SDP), that is, the problem of decoding a random looking linear code. The original McEliece proposal, based on binary Goppa codes, is still essentially unbroken but features rather large public keys and is not well suited to be turned into a digital signature scheme. Along the years, researchers have proposed several alternatives, aiming to face these issues. In this talk we will recall the most important modern solutions, such as encryption schemes based on Low-Density Parity-Check (LDPC) and Moderate-Density Parity-Check (MDPC) codes, and signature schemes obtained from random and pseudo-random codes.We will outline the pros and cons of the considered schemes, and eventually mention possible research goals and directions.

Registration for the online event to *be made by* 1st *November* via the following link:

click here

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

Contact person: Marco Baldi

CONTACTS
De Componendis Cifris Association

segreteria@decifris.it
seminari@decifris.it