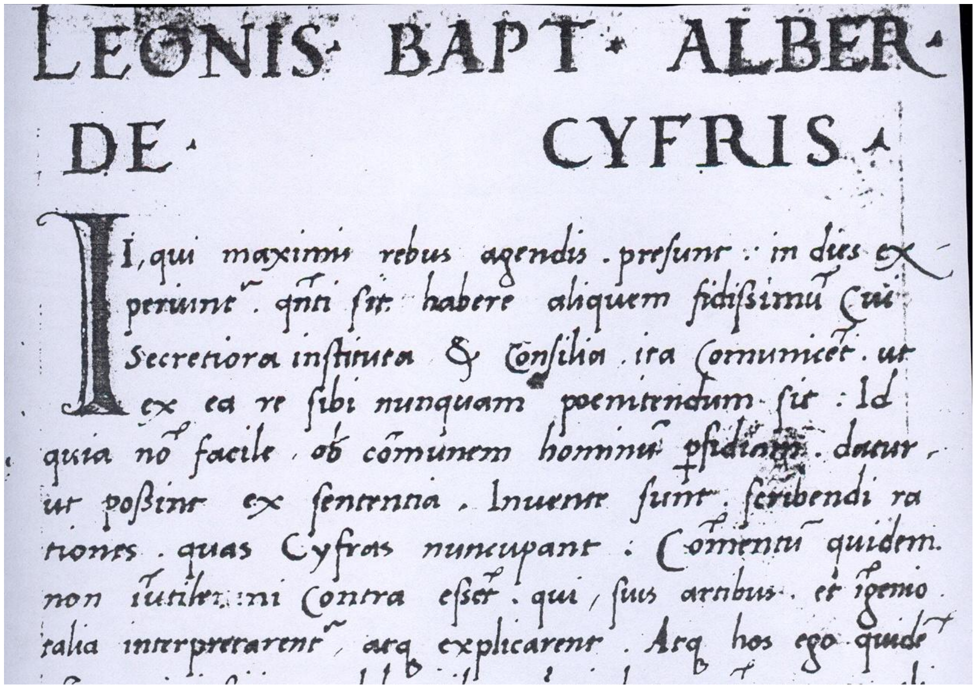

LEONIS BAPT. ALBER.
DE CYFRIS.

Ii, qui maximis rebus agendis preſunt: in dies experiunt quanti ſit habere aliquem fidiſſimū cui Secretiora inſtituta & conſilia ita comunicet: ut ex ea re ſibi nunquam poenitendum ſit: Id quia nō facile ob cōmunem hominū pfidiam datur, ut poſſint ex ſententia. Inventæ ſunt ſcribendi rationes quas Cyfras nuncupant: Cōmentū quidem non inutile: niſi contra eſſet: qui ſuis artibus et ipſemo talia interpretarentur atq explicarent. Atq hos ego quidē

PostQuantumCifris in Ancona

Thursday 1st December 2022, 11:30 a.m.

Information engineering department (DII) library (q. 165)
Università Politecnica delle Marche
and online

Alessio Meneghetti

Università di Trento

On a link between Code-Based and Multivariate-Based Cryptosystems

Abstract: In this talk we present an explicit polynomial-time map between MLD and MQ from which it is possible to derive the equivalence of the two problems, and therefore the possibility of studying code-based cryptosystems via methods from commutative algebra and vice-versa.

Giovanni Tognolini

Università di Trento

Towards a Post Quantum OTS Scheme using QC-LDPC Codes

Abstract: In this talk we present a novel post-quantum code-based digital signature algorithm whose security is based on the difficulty of decoding Quasi-Cyclic codes in systematic form, and whose trapdoor relies on the knowledge of a hidden Quasi-Cyclic Low-Density-Parity-Check (QC-LDPC) code. We then prove its correctness and discuss possible vulnerabilities.

Registration for the online event to be made by 30th 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 (m.baldi@univpm.it)

CONTACTS
De Componendis Cifris Association

segreteria@decifris.it
seminari@decifris.it