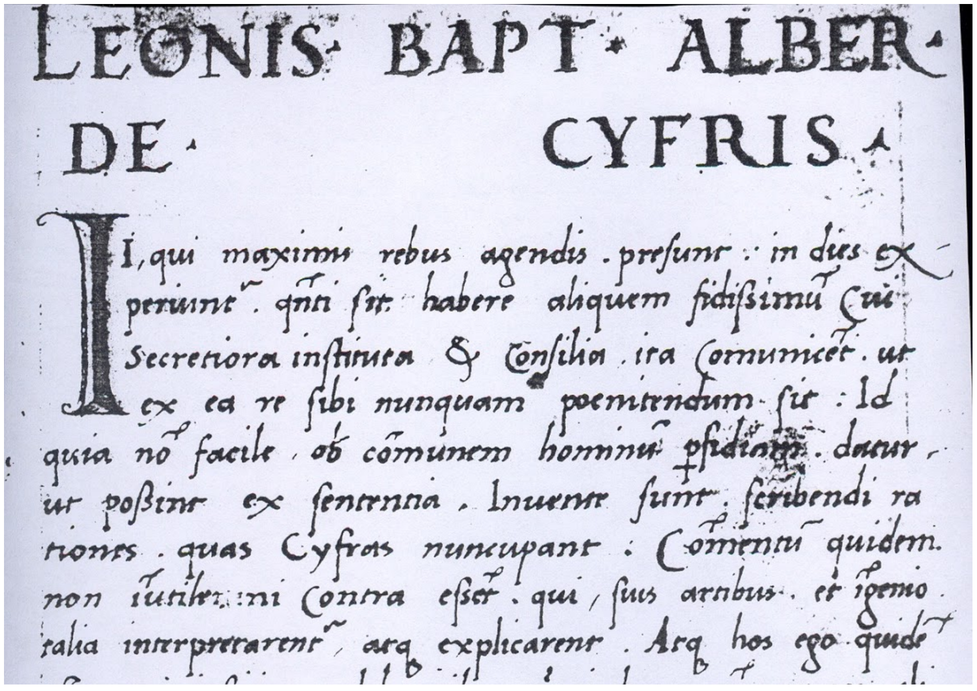

LEONIS· BAPT· ALBER·
DE· CYFRIS·

Ii, qui maximis rebus agendis . preſunt : in dies ex-
periunt . qnti 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 . Inuente ſunt . ſcribendi ra
tiones . quas Cyfras nuncupant : Cōmentū quidem .
non iutile ; ni contra eſset . qui , ſuis artibus . et igenio .
talia interpretarent , atq explicarent . Atq hos ego quidē

De Cifris Athesis

UNIVERSITÀ DEGLI STUDI
DI TRENTO
Dipartimento di Matematica

FONDAZIONE
BRUNO KESSLER
ICT
CENTER FOR INFORMATION AND
COMMUNICATION TECHNOLOGY

Monday 11th February 2019 – at 9:00 a.m.
Seminar Room -1, Department of Mathematics

Federico Pintore

University of Oxford - UK

Cryptographic primitives from elliptic curve isogenies - An overview and some preliminary results

Abstract: Post-Quantum Cryptography is a newborn branch of Cryptography that aims to develop cryptosystems whose security relies upon mathematical problems assumed to be hard even for quantum computers. Some of such cryptosystems exploit the properties of isogenies between supersingular elliptic curves, and base their security on the difficulty of computing an isogeny between two given supersingular elliptic curves. The first primitives based on this problem were introduced by Jao, De Feo and Plût in 2014, and many others have followed in recent years. All of them lead to the birth of Isogeny-based Cryptography.

The goal of this talk is to give an overview of the cryptosystems that are already part of Isogeny-based Cryptography, what is still missing, and some of our recent preliminary results.

Contact person: Massimiliano Sala

CONTATTI
Associazione De Componendis Cifris

direttore@decifris.it
segreteria@decifris.it