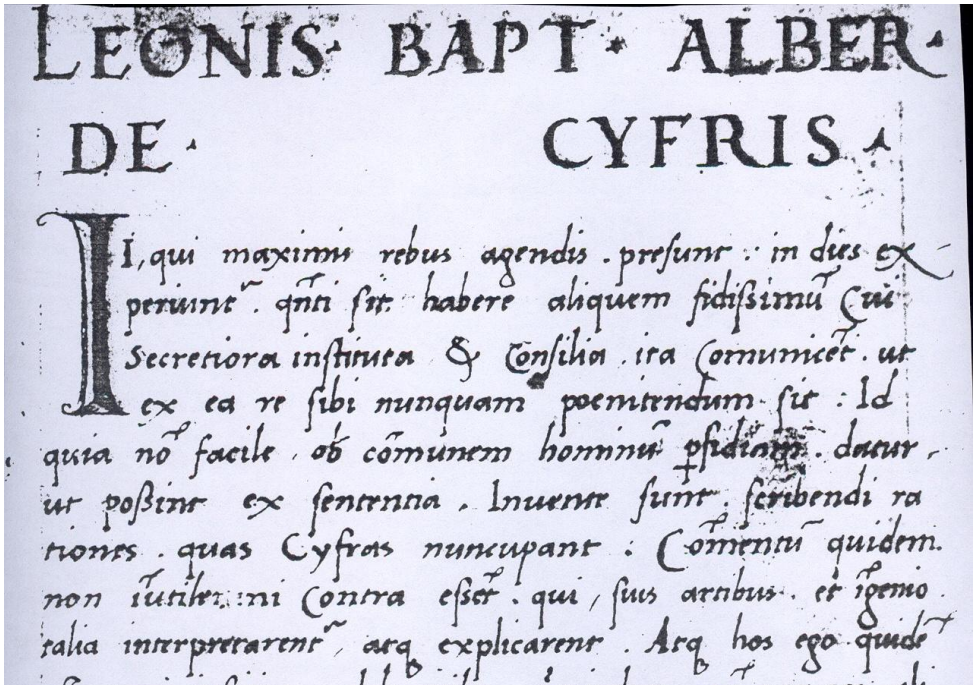
LEONIS BAPT. ALBER-
DE CYFRIS

II, qui maximis rebus agendis . presunt : in dies ex-
periunt . quã sit habere aliquem fidissimũ cui
Secretiora instituta & Consilia . ita Communicet . ut
ex ea re sibi nunquam poeniteudum sit : Id
quia nõ facile . ob cõmunem hominũ pfidiam . datur .
ut possint ex sententia . Inuenta sunt scribendi ra
tiones . quas Cyfras nuncupant : Comentũ quidem
non iutibrum Contra esset . qui , suis arnibus . et igemo
talia interpretarent , arq explicarent . Arq hos ego quide

De Cifris Athesis

UNIVERSITÀ DEGLI STUDI DI TRENTO
Dipartimento di Matematica

FONDAZIONE BRUNO KESSLER
ICT CENTER FOR INFORMATION AND COMMUNICATION TECHNOLOGY

Thursday 20th May 2021 – at 10:00 a.m.
Online Seminar via Zoom

Annamaria Iezzi

Université de la Polynésie Française

Strumenti per fare crittoanalisi nei grafi di isogenie supersingolari

Abstract: I grafi di isogenie supersingolari possono essere considerati probabilmente i protagonisti di un sottocampo recente e molto attivo della crittografia post-quantistica, che prende il nome, in inglese, di *isogeny-based cryptography*. Le proprietà di questi grafi, i cui vertici corrispondono a curve ellittiche supersingolari su campi finiti e i cui archi rappresentano isogenie tra curve, non sono state ancora completamente esplorate, ed è proprio questa struttura "sconosciuta" ad essere alla base della sicurezza di alcuni crittosistemi basati sulle isogenie, come SIKE (nominato "candidato sostituto" al terzo round della competizione del NIST).

In questo seminario cercheremo di fornire una panoramica dei principali strumenti che si possono utilizzare quando si studiano i grafi di isogenie supersingolari, sottolineando le connessioni tra di essi: parleremo allora di anelli di endomorfismi, algebre di quaternioni, moduli di Tate, Bruhat-Tits trees, etc.

Iscrizione all'evento online *da effettuare entro il 19 maggio* tramite il seguente link:

click here

Gli iscritti riceveranno l'ID Zoom un'ora prima dell'inizio dell'evento.

Contact person: Massimiliano Sala

CONTATTI
Associazione De Componendis Cifris

segreteria@decifris.it
seminari@decifris.it