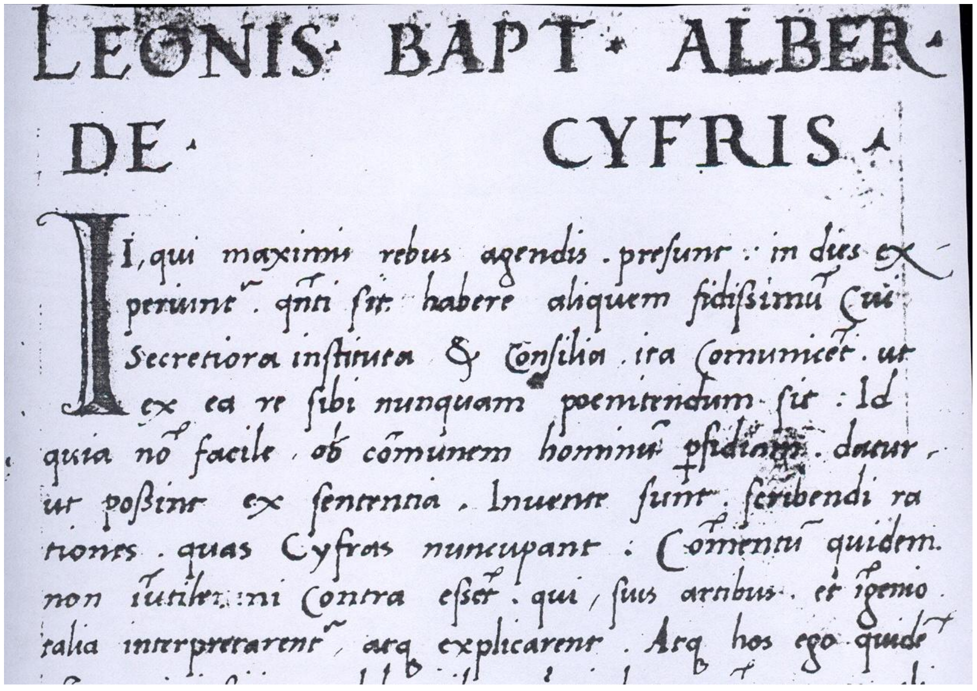

LEONIS· BAPT· ALBER·
DE· CYFRIS·

Ii, qui maximis rebus agendis . preſunt : in dies ex-
periunt̄ . 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 inutile . ni Contra eſſet . qui ſuis artibus . et ingenio .
talia interpretarent̄ , atq explicarent . Atq hos ego quidē

PostQuantumCifris

Tuesday 5th April 2022 – at 3:00 p.m.

Online Seminar via Zoom

Shi Bai

Florida Atlantic University

Lattice algorithms for variants of LWE

Abstract: The learning with errors (LWE) problem introduced by Regev (STOC'05) is one of the fundamental problems in lattice-based cryptography. It has been used extensively as a security foundation, for public-key encryption, signatures, fully homomorphic encryption (FHE), pseudo-random functions (PRF) and many others. One standard strategy to solve the LWE problem is to reduce it to a unique SVP (uSVP) problem via Kannan's embedding and then apply a lattice reduction to solve the uSVP problem. In this talk, we will discuss and compare various lattice algorithms for solving LWE, and then give some concrete estimates for breaking various variants of LWE (e.g. generic, small secrets, restricted samples). In the end, we will discuss some recent developments on lattice reduction algorithms with their application to LWE.

Registration for the online event to *be made by* 4th April 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