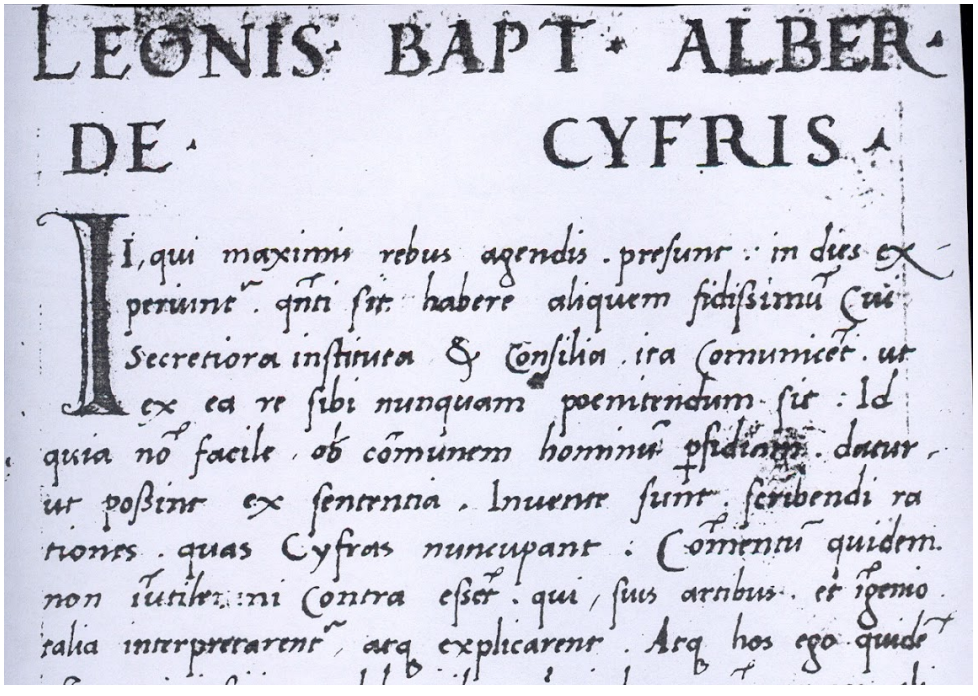
LEONIS BAPT. ALBER-
DE CYFRIS

II, qui maximis rebus agendis . presunt : in dies ex-
periuntur . quã sit habere aliquem fidissimũ cui
Secretiora instituta & Consilia ita Communicet . ut
ex ea re sibi nunquam poeniteadum 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 iutile : ni Contra esset . qui , suis armis . et igemo
talia interpretarent , arq explicarent . Arq hos ego quide

PostQuantumCifris

Tuesday 7th december 2021 – at 3:00 p.m.

Online Seminar via Zoom

Cecilia Boschini

Technion

How to do Efficient Signature Verification without Leakage

Abstract: Digital signatures are fundamental for data authenticity and integrity verification. Their widespread use makes the study of efficient algorithms to verify their correctness very important. Until now though such improvements have been done mostly at an implementation level, and often the lack of an appropriate study of the security of the new scheme resulted in introducing vulnerability instead of improving efficiency. In this talk we will show how to do a formal analysis of the security of a signature when a new, more efficient verification algorithm has been substituted to its original verification procedure. After having defined what we mean by "being more efficient" and "preserving security", we will show how to use our model on some examples by showing a new efficient verification algorithm for some post-quantum signatures.

Registration for the online event to *be made by* 6th Decem*ber* 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