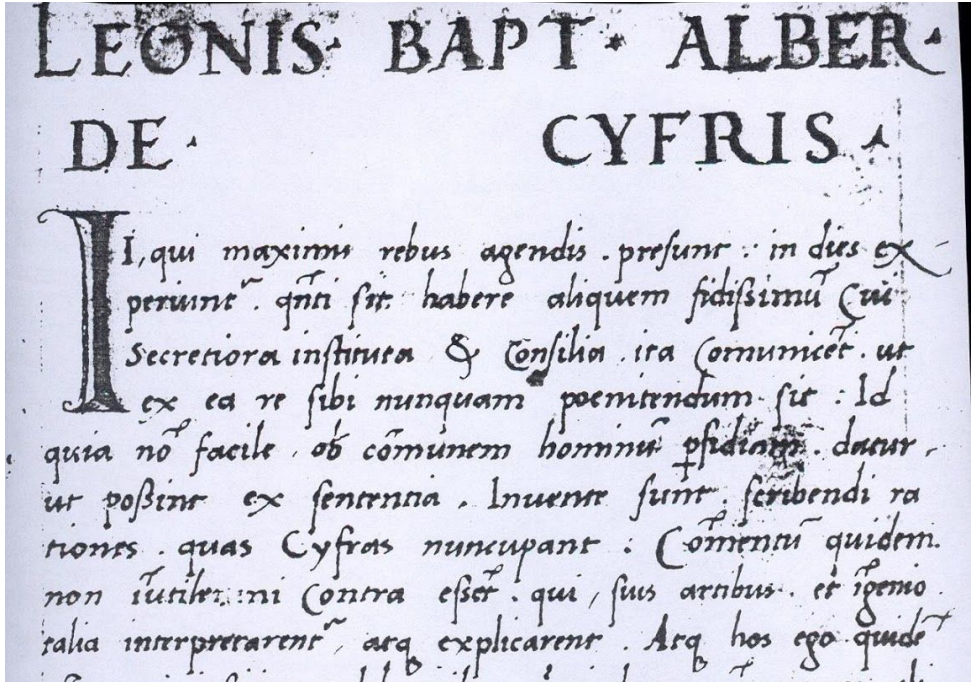
LEONIS BAPT. ALBER.
DE CYFRIS.

Ii, qui maximis rebus agendis . presunt : in dies ex
periuntur . quanti sit habere aliquem fidissimu cui
secretiora instituta & consilia ita communicet . ut
ex ea re sibi nunquam poeniteudum sit : Id
quia no facile . ob communem hominu ptidiam . datur
ut possint ex sententia . Inuenta sunt scribendi ra
tiones . quas Cyfras nuncupant : Commentu quidem
non iutilem . ni Contra esset . qui , suis artibus . et igemo
talia interpretarent , arq explicarent . Arq hos ego quide

De Cifris Schola Latina

Monday 12th – Tuesday 13th October 2020 – at 11.00
Virtual conference on Google Meet
https://meet.google.com/iij-ftpf-xxr

Gianluca Brian

Università di Roma La Sapienza

Leakage-Resilient Non-Malleable Secret Sharing

Abstract: Secret Sharing enables a dealer to split a secret into a set of shares in such a way that certain authorized subsets of share holders can reconstruct the secret, whereas all unauthorized subsets cannot learn any information about the secret. Typical applications include data storage, threshold cryptography and multi-party computation, and sometimes additional security requirements are needed. We focus on leakage-resilient non-malleability, achieved when the scheme remains secure even in the presence of leakage and tampering attacks. The first part of the seminar is dedicated to an introduction to secret sharing with all the necessary security notions, including the ones of leakage-resilience and non-malleability. Here, we also show some examples, applications and some general results. In the second part, we go into detail and show the current state of the art of leakage-resilient non-malleable secret sharing, along with some recent constructions.

Contact person: Daniele Venturi

CONTATTI
Iniziativa De Componendis Cifris

seminari@decifris.it
segreteria@decifris.it