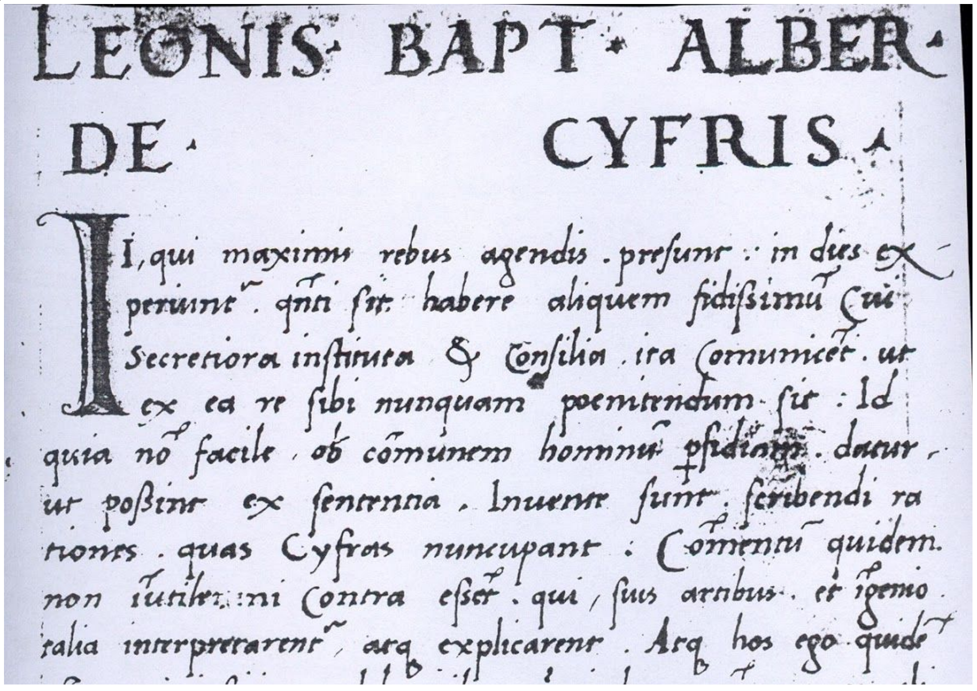

LEONIS BAPT· ALBER·

DE· CYFRIS·

I, qui maximis rebus agendis presunt: in dies ex
periunt̃. qn̄ti 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. Inuenti sunt scribendi ra
tiones. quas Cyfras nuncupant: Cōmentū quidem.
non inutile: ni Contra esset. qui, suis artibus. et igenio.
talia interpretarent̃, atq explicarent. Atq hos ego quide

De Cifris Athesis

UNIVERSITÀ DEGLI STUDI
DI TRENTO
Dipartimento di Matematica

DE CIFRIS

FONDAZIONE
BRUNO KESSLER

ICT
CENTER FOR INFORMATION AND
COMMUNICATION TECHNOLOGY

Thursday 18th June 2020 – at 11:00 a.m.
Online seminar via Zoom

Federico Mazzone
University of Trento

Paillier homomorphic encryption and its application to build a share conversion protocol

Abstract: In this seminar we will talk about one of the public-key cryptosystems introduced by Pascal Paillier. We will start defining what is a n-th residuosity class and presenting the Composite Residuosity and the Composite Residuosity Class problems. We will see how these two problems are related with the milestone problems of the public key cryptography: factorization and root extraction. Then we will describe the encryption/decryption scheme and briefly discuss its correctness, security and complexity. Finally, we will prove the homomorphic properties of this cryptosystem and we will show how to exploit them in order to create a multiplicative-to-additive share conversion protocol.

Percorso di Eccellenza Matematica

Iscrizione all'evento online *da effettuare entro il 17 giugno* 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

direttore@decifris.it
segreteria@decifris.it