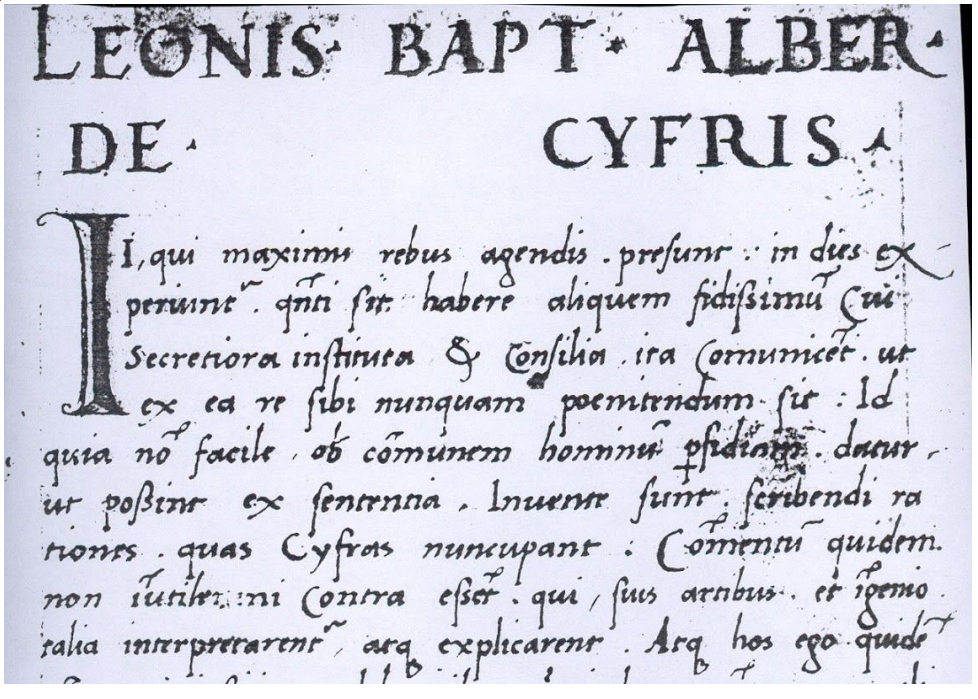
LEONIS BAPT. ALBER-
DE CYFRIS

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 : Comentu quidem
non iutilem Contra esset . qui , suis armis . et igemo
talia interpretarent , atq explicarent . Atq hos ego quide

# De Cifris Athesis

UNIVERSITÀ DEGLI STUDI DI TRENTO
Dipartimento di Matematica

FONDAZIONE BRUNO KESSLER
ICT CENTER FOR INFORMATION AND COMMUNICATION TECHNOLOGY

**Tuesday 10th September 2019 – at 10:00 a.m.**
**Department of Mathematics**
**Room A222, Povo 1, Via Sommarive, 9, Povo Trento**

## Carlo Blundo

## Università degli Studi di Salerno

### Privacy-preserving Information Sharing

**Abstract:** In this talk, we address privacy issues related to sharing information in a distributed system consisting of autonomous entities, each of which holds a private dataset. The entities are willing to share information computed as a function of their datasets. Nevertheless, no entity is willing to disclose its private data to other entities due to privacy concern. In this talk, we will focus on Private Set Intersection and its variants.

Private Set Intersection (PSI) refers to a setting where two parties each hold a set of private items, and wish to learn the intersection of their sets without revealing any information except for the intersection itself.

We will see how PSI can be used to solve several practical matching problems such as: find out whether any suspect is on a given flight, discover if tax evaders have accounts at foreign banks, execute a genetic paternity test, suggest advertisement recommendation, check document/multimedia similarity, run a biometric authentication protocol, steer shoppers within a shopping mall towards the shops selling their desired items without knowing the shopping list's content.

**Contact person:** Massimiliano Sala

**CONTATTI**
**Associazione De Componendis Cifris**

direttore@decifris.it
segreteria@decifris.it