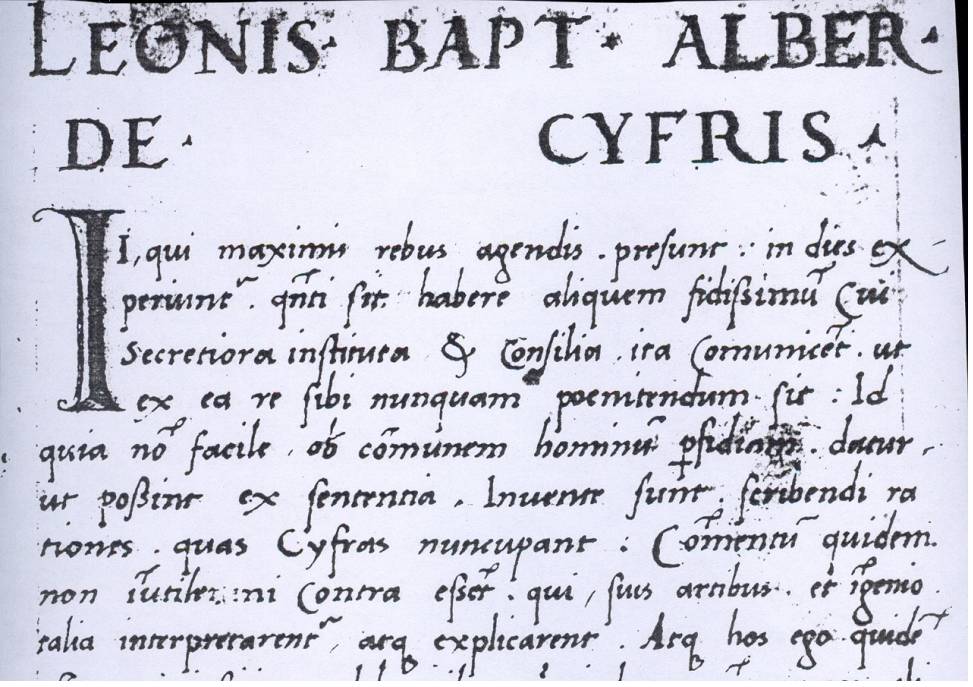
LEONIS BAPT. ALBER
DE CYFRIS
II, qui maximis rebus agendis . presunt : in dies ex
periuntur . quis sit habere aliquem fidissimu Cui
Secretiora instituta & Consilia ita Comunicet . ut
ex ea re sibi nunquam poeniteudum sit : Id
quia no facile . ob comunem hominu ffidiam . datur .
ut possint ex sententia . Inuenta sunt . scribendi ra
tiones . quas Cyfras nuncupant : Comentu quidem
non iutile: ni Contra esset . qui , suis armis . et iocno
ralia interpretarent , atq explicarent . Atq hos ego quide

# De Cifris Schola Latina

DIPARTIMENTO DI INFORMATICA

SAPIENZA UNIVERSITÀ DI ROMA

disim

ROMA TRE UNIVERSITÀ DEGLI STUDI

**Monday 24th June 2019 – at 14.30**
**Aula Seminari, Dipartimento di Informatica**
**Università di Roma La Sapienza**
**Via Salaria 113, Rome**


## Daniele Friolo

## Università di Roma La Sapienza


## Affordable Security or Big Guy vs Small Guy. Does the depth of your pockets impact your protocols?


**Abstract:** When we design a security protocol we assume that the humans (or organizations) playing Alice and Bob do not make a difference. In particular, their financial capacity seems to be irrelevant. In the latest trend to guarantee that secure multi-party computation protocols are fair and not vulnerable to malicious aborts, a slate of protocols has been proposed based on penalty mechanisms. We look at two well-known penalty mechanisms, and show that the so-called see-saw mechanism (Kumaresan et al., CCS 15), is only fit for people with deep pockets, well beyond the stake in the multi-party computation itself. Depending on the scheme, fairness is not affordable by everyone which has several policy implications on protocol design. To explicitly capture the above issues, we introduce a new property called financial fairness.


**Contact person:** Daniele Venturi


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

direttore@decifris.it
segreteria@decifris.it