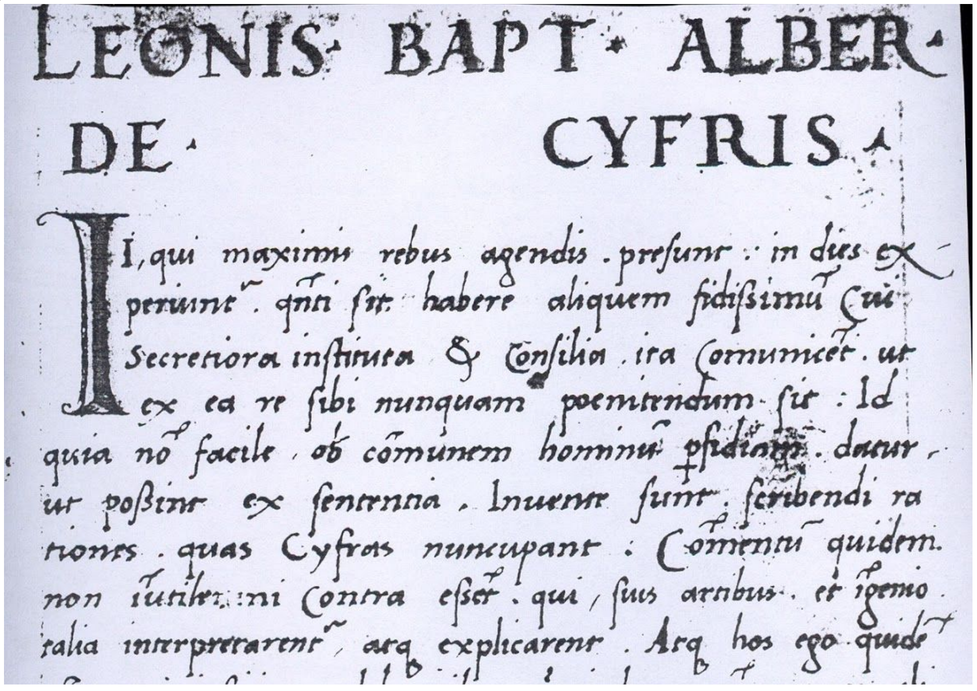

LEONIS· BAPT· ALBER·
DE· CYFRIS·
II, qui maximis rebus agendis · preſunt : in dies ex
periunt · qnti ſit habere aliquem fidiſsimu cui
Secretiora inſtituta & Conſilia · ita comunicet · ut
ex ea re ſibi nunquam poenitendum ſit : Id
quia no facile · ob comunem hominu pfidiam · datur ·
ut poſsint ex ſententia · Inventa ſunt · ſcribendi ra
tiones · quas Cyfras nuncupant : Comentu quidem
non inutile: ni contra eſſet · qui / ſuis artibus · et ingenio
talia interpretarentur · 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

Thursday 7th March 2019 – at 11:00 a.m.
Seminar Room -1, Department of Mathematics

Claudio Orlandi
Aarhus University - Denmark

Quisquis: A New Design for Anonymous Cryptocurrencies

Abstract: Despite their usage of pseudonyms rather than persistent identifiers, most existing cryptocurrencies do not provide users with any meaningful levels of privacy. This has prompted the creation of privacy-enhanced cryptocurrencies.

In this talk, I will discuss some limitations of existing privacy-aware cryptocurrencies and introduce QuisQuis, a novel proposal for achieving anonymous and private transactions in a provable way from standard cryptographic assumptions.
Based on joint work with Prastudy Fauzi and Rebekah Mercer (Aarhus University) and Sarah Meiklejohn (UCL London), available on the Cryptology ePrint Archive: Report 2018/990.

Contact person: Massimiliano Sala

CONTATTI
Associazione De Componendis Cifris

direttore@decifris.it
segreteria@decifris.it