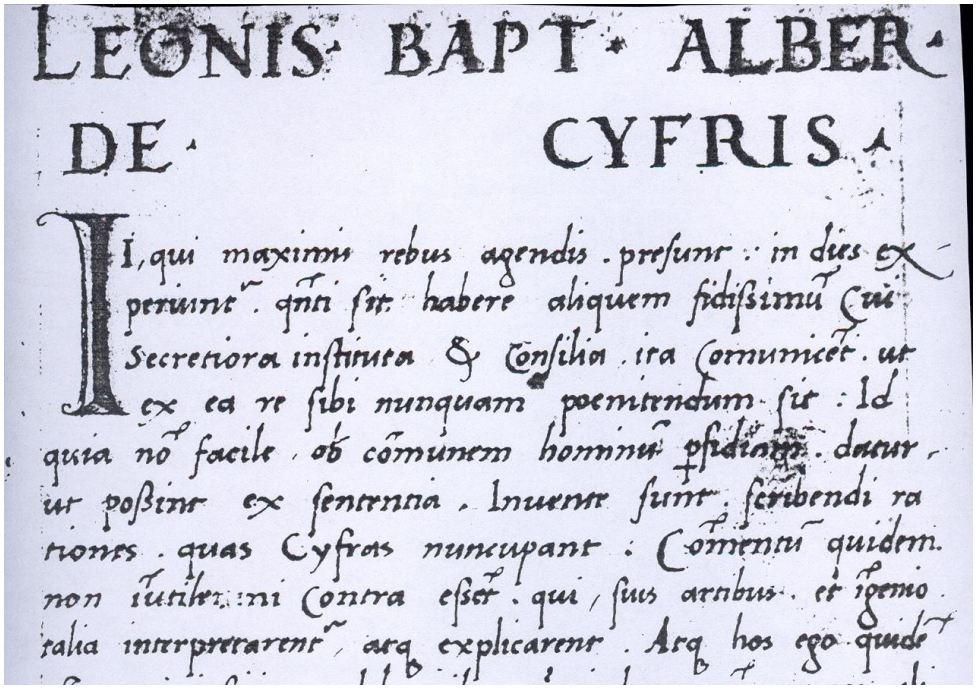
LEONIS BAPT. ALBER-
DE CYFRIS

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 poeniteadum sit : Id
quia nõ facile . ob cõmunem hominũ pfidiam . datur .
ut possint ex sententia . Inuenta sunt scribendi ra
tiones . quas Cyfras nuncupant : Comentũ quidem
non iutibrum Contra esset . qui , suis armis . et igemo
talia interpretarent , arq explicarent . Arq hos ego quide

De Cifris Athesis

UNIVERSITÀ DEGLI STUDI DI TRENTO
Dipartimento di Matematica

CENTER FOR CYBERSECURITY
FONDAZIONE BRUNO KESSLER

Tuesday 10th May 2022 – at 4:00 p.m.
Online Seminar via Zoom

Marco Martinoli

Proton AG

Cryptography vs Real World

Abstract:

The main purpose of cryptography, enabling secure and private communication among intended parties, can be achieved only when cryptographic algorithms and protocols find their way into real-world applications. Unfortunately, once in the wild, the attack surface widens and many theoretical assumptions on which security proofs on paper are based no longer hold. Practical attacks against schemes and bypass against protocols arise, even if the underlying cryptographic primitives are deemed secure. Two examples are considered: side-channel attacks against implementations of cryptographic algorithms and man-in-the-middle attacks in public key infrastructures.

Iscrizione all'evento online da effettuare entro il giorno 9 maggio 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

segreteria@decifris.it
seminari@decifris.it