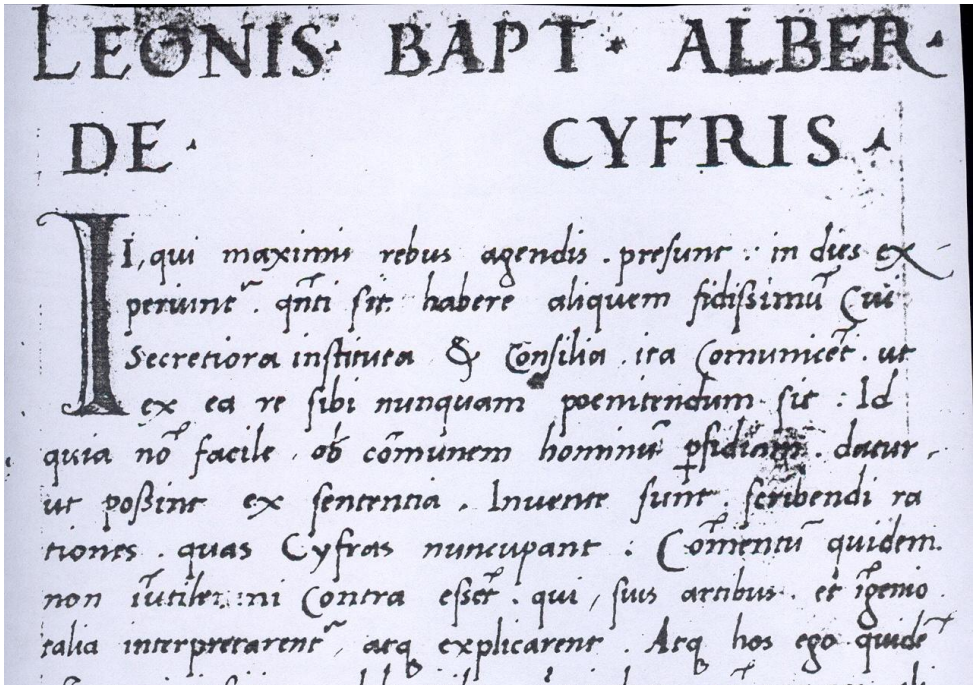
LEONIS BAPT. ALBER-
DE CYFRIS.

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 : 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 13th December 2022 – at 3:00 p.m.
Online Seminar via Zoom

Emanuele Giunta

IMDEA Software Institute, Universidad Politécnica de Madrid

On the Impossibility of Algebraic Vector Commitments in Pairing-Free Groups

Abstract: Vector Commitments allow one to (concisely) commit to a vector of messages so that one can later (concisely) open the commitment at selected locations. In the state of the art of vector commitments, algebraic constructions have emerged as a particularly useful class, as they enable advanced properties, such as stateless updates, subvector openings and aggregation, that are for example unknown in Merkle-tree-based schemes. In spite of their popularity, algebraic vector commitments remain poorly understood objects. In particular, no construction in standard prime order groups (without pairing) is known.
In this paper, we shed light on this state of affairs by showing that a large class of concise algebraic vector commitments in pairing-free, prime order groups are impossible to realize.
Our results also preclude any cryptographic primitive that implies the algebraic vector commitments we rule out, as special cases.
This means that we also show the impossibility, for instance, of succinct polynomial commitments and functional commitments (for all classes of functions including linear forms) in pairing-free groups of prime order.

Iscrizione all'evento online da effettuare entro il giorno 12 dicembre 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