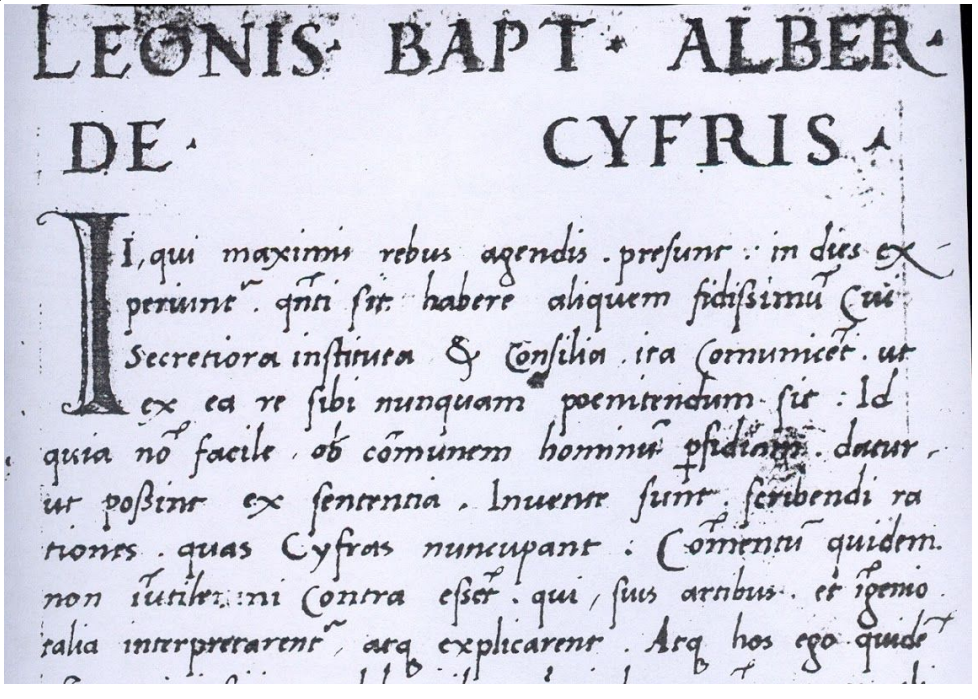
LEONIS BAPT. ALBER-
DE CYFRIS.

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 : Comentu quidem
non iutilissimi 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

FONDAZIONE BRUNO KESSLER
ICT CENTER FOR INFORMATION AND COMMUNICATION TECHNOLOGY

Monday 15th April 2019 – at 10:00 a.m.
Seminar Room -1, Department of Mathematics

Ottavio G. Rizzo

Università degli Studi di Milano

Moltiplicare efficientemente polinomi in caratteristica 2

Abstract: Il prodotto fra due elementi di un campo finito si riduce, essenzialmente, al prodotto di due polinomi sul campo base. Poiché elevamenti a potenza e quozienti si possono ridurre ai prodotti, calcolare rapidamente il prodotto fra due polinomi è essenziale per l'efficienza di qualsiasi algoritmo software o hardware che faccia uso di campi finiti: che si tratti di crittografia (pre- e post-quantistica), teoria dei codici, elaborazione di segnali digitali, ecc.

In questa presentazione vedremo i principali algoritmi nel caso in cui la base sia GF(2), a partire da Karatsuba fino ad una recentissima proposta di De Piccoli, Visconti e R.

Contact person: Massimiliano Sala

CONTATTI
Associazione De Componendis Cifris

direttore@decifris.it
segreteria@decifris.it