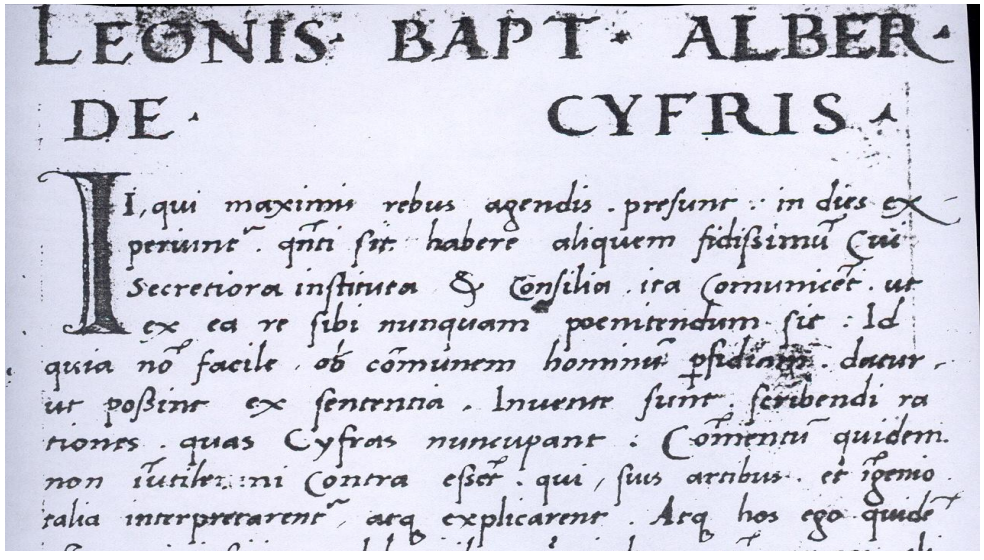
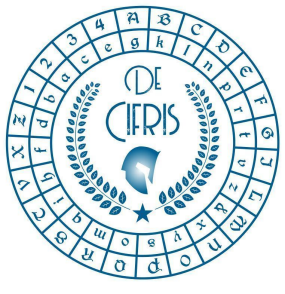
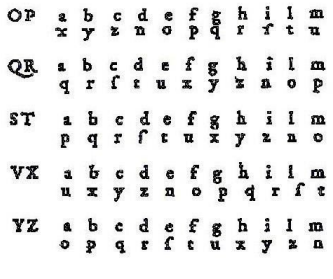

LEONIS BAPT. ALBER.
DE CYFRIS.

II, qui maximis rebus agendis præsunt : in dies ex
periuntur, quàm sit habere aliquem fidissimum Cui
Secretiora instituta & Consilia ita communicet, ut
ex ea re sibi nunquam pœnitendum sit : Id
quia nō facile ob cōmunem hominū ꝓfidiam datur,
ut possint ex sententia. Inuenta sunt scribendi ra
tiones, quas Cyfras nuncupant : Comentu quidem
non futile, ni Contra esset, qui, suis artibus, et ingemo
dalia interpretarent, atq; explicarent. Atq; hos ego quide




OP a b c d e f g h i l m
x y z n o p q r f t u
QR a b c d e f g h i l m
q r f t u z y z n o p
ST a b c d e f g h i l m
p q r f t u z y z n o
VX a b c d e f g h i l m
u z y z n o p q r f t
YZ a b c d e f g h i l m
o p q r f t u z y z n

Mercoledì 2 Febbraio 2022 – ore 16:00

Seminario Online via Zoom

Seminario congiunto UMI - Gruppo Crittografia e Codici e Iniziativa De Componendis Cifris - Gruppo MathCifris

Irene Villa

Università di Trento

The classification of planar monomials over fields of order a prime cubed

Abstract: In finite fields of odd characteristic, planar functions play an important role. They present a one-to-one connection with commutative semifields and they can be used to construct finite projective planes. Moreover, in cryptographic scenarios, they correspond to perfect nonlinear functions, providing an optimal resistance to linear and differential cryptanalysis when used in DES-like cryptosystems.

The Dembowski-Ostrom conjecture states that, up to adding constants or linear terms, the only planar functions over finite fields are necessarily DO polynomials, that are polynomials with only quadratic terms. This conjecture was proved true for polynomials over prime fields, for monomials over fields of square order and for monomials over fields of order p^4 with p>3. Instead, it was shown false for fields of characteristic 3, with the smallest counterexample being over the finite field with 3^4 elements. In this seminar, we fill a gap by giving a complete classification of planar monomials over fields of order p^3, establishing the DO conjecture in this case. The proof makes use of Hermite's criteria to eliminate all potential exponents that are not DO exponents.

The result presented is a joint work with Robert Coulter and Emily Bergman.

Link al seminario su Zoom
ID riunione: 873 4652 9312
Passcode: 415743

Referente	Associazione De Componendis Cifris	UMI
Norberto Gavioli	seminari@decifris.it segreteria@decifris.it matematica@decifris.it	seminariumi-cc@googlegroups.com