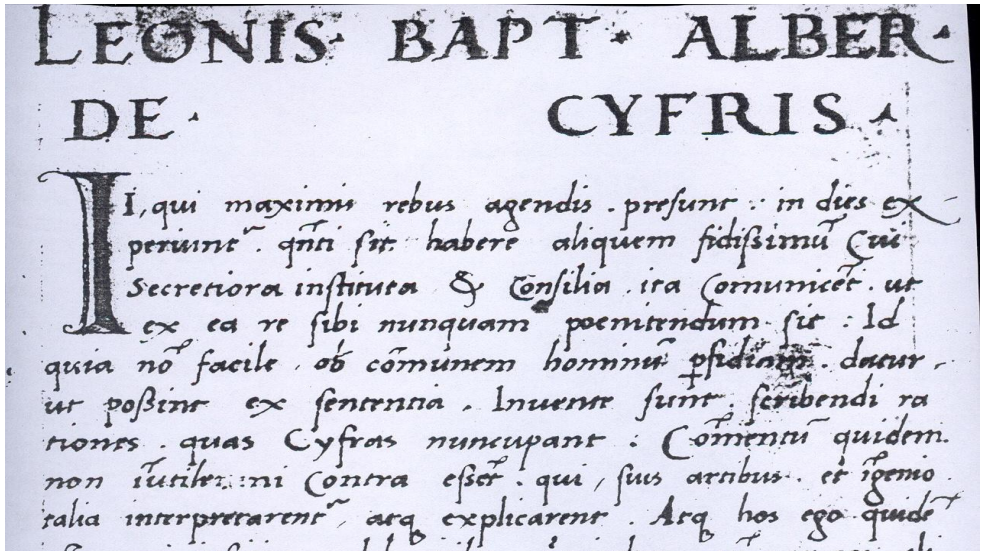

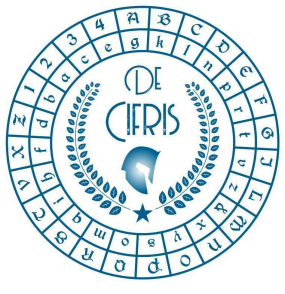

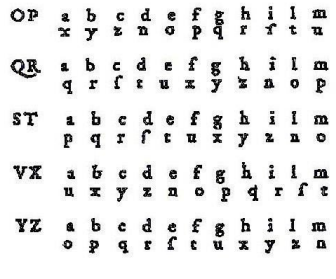

Mercoledì 1 Dicembre 2021 – ore 16:00

Seminario Online via Zoom

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

Daniele Bartoli

Università degli Studi di Perugia

Teoremi di tipo Hasse-Weil e classi rilevanti di funzioni polinomiali

Abstract: Numerose funzioni polinomiali su campi finiti hanno rilevanti applicazioni in crittografia e teoria dei codici.

Tra queste, funzioni APN, funzioni PN, permutazioni APN e i polinomi di permutazione sono state ampiamente studiate negli ultimi anni.

Per indagare la non esistenza di tali funzioni, o per costruire famiglie infinite, varietà algebriche su campi finiti sono un utile strumento. In questo contesto, un ingrediente chiave è una stima del numero di punti razionali di tali varietà algebriche e per questo teoremi di tipo Hasse-Weil (Lang-Weil, Serre, . . .) giocano un ruolo fondamentale.

Questo seminario è una rassegna dei risultati ottenuti con tale approccio.

Link al seminario su Zoom

ID riunione: 842 1530 1691
Passcode: 526760

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