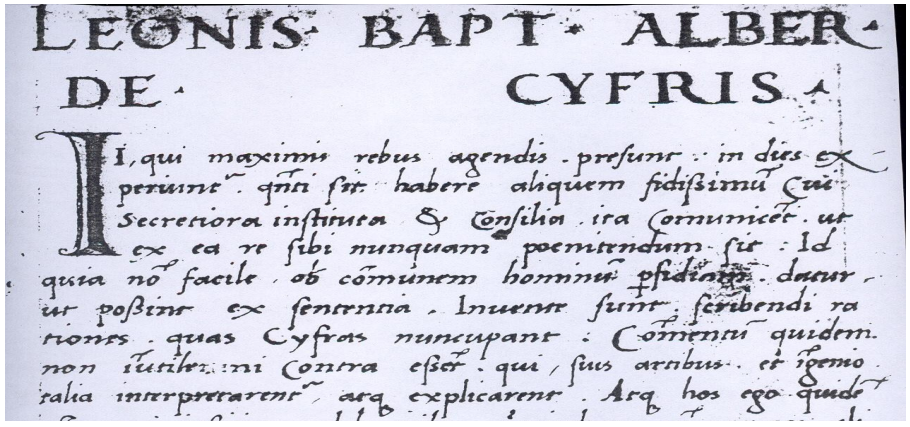
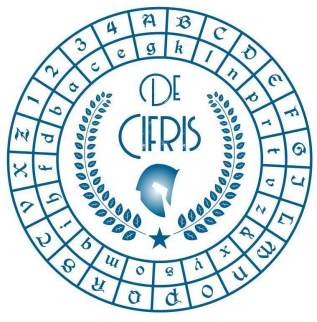
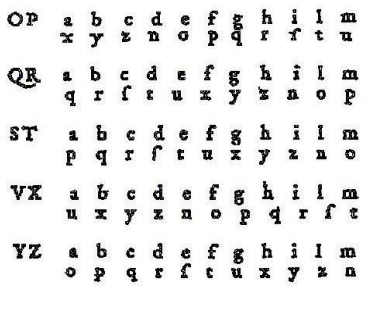

LEONIS BAPT. ALBER
DE CYFRIS

Il, qui maximis rebus agendis præsunt : in diis ex
perijmt. qnti sit habere aliquem fidissimu Cui
Secretiora instituta & Consilia ira Communicet. ut
ex ea re sibi nunquam poenitendum sit. Id
quia no facile, ob cõmunem hominu ꝓfidiaꝫ. datur
ut possint ex sententia. Inuenit sunt scribendi ra
tiones. quas Cyfras nuncupant. Comenti quidem
non iustis: mi Contra esset. qui, suis armis. et ꝓmo
talia interpretarent. arq explicarent. Arq hos ego quide




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

Mercoledì 5 Maggio 2021 – ore 15:00

Seminario Online via Zoom

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

Luca De Feo

IBM Research, Zurigo

La corrispondenza di Deuring effettiva – la chiave per la prossima generazione di crittografia basata sulle isogenie?

Abstract: Nel 1997, nel corso di un seminario alla Scuola Normale Superiore di Parigi (ENS Ulm), Jean-Marc Couveignes presentava un'idea tanto visionaria quanto incompresa: in un vasto tentativo di generalizzazione del problema del logaritmo discreto, egli (re)introduceva la nobile e venerata teoria della Moltiplicazione Complessa (CM) in crittografia. Il piano era audace: piuttosto che dannarsi a gestire l'ingestibile CM in caratteristica 0, come si era tentato fino ad allora in crittografia sulle curve ellittiche, Couveignes costruiva direttamente sui lavori di Deuring e Waterhouse che rendevano la CM effettiva in caratteristica positiva, attraverso algoritmi di calcolo d'isogenie. Piano talmente audace che cadde nell'oblio per due lustri.

Avanti-veloce ad oggi, l'algoritmo quantistico di Shor per il logaritmo discreto, lo sviluppo della crittografia post-quantistica, e la scoperta di algoritmi più efficaci per la CM effettiva hanno riportato le idee di Couveignes alla ribalta, rappresentate principalmente dal nuovo protocollo di scambio di chiave CSIDH e dai suoi derivati. Nel frattempo la crittografia a base d'isogenie ha avuto modo di svilupparsi anche in altre direzioni, sfruttando il formalismo dei grafi d'isogenie supersingolari ed i notevoli teoremi sui loro autovalori.

Ma i lavori di Deuring e Waterhouse hanno una portata che va al di là della CM, fornendo, come dimostrato da Kohel, Lauter, Petit e Tignol, una corrispondenza di categorie pressoché effettiva tra ordini massimali di algebre di quaternioni e curve supersingolari. In principio timidamente proposta come uno strumento per la crittanalisi, Galbraith, Petit e Silva furono i primi ad avere l'intuizione che la corrispondenza effettiva di Deuring (per le curve supersingolari, quindi) potesse servire come un'ulteriore generalizzazione delle idee di Couveignes. L'intuizione si è appena concretizzata in maniera spettacolare in SQISign, il protocollo di firma digitale post-quantistico più compatto conosciuto fino ad ora.

In questa presentazione spero di riuscire a presentare, in maniera semplice ed accessibile, la corrispondenza di Deuring effettiva, i suoi algoritmi e i suoi problemi ritenuti difficili, accompagnandola di riferimenti alle applicazioni crittografiche.

Link al seminario su Zoom

ID riunione: 847 3303 9501
Passcode: 350323

Referente:

Norberto Gavioli

Associazione De Componendis Cifris

seminari@decifris.it
segreteria@decifris.it
matematica@decifris.it

UMI

seminariumi-cc@googlegroups.com