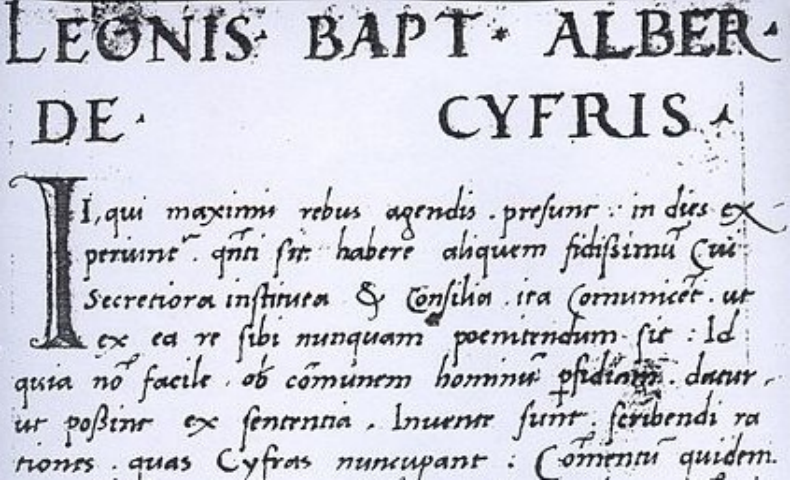
LEONIS BAPT. ALBER
DE CYFRIS

De Cifris Augustae Taurinorum

quadrans FOUNDATION Telsy

POLITECNICO DI TORINO
Dipartimento di Scienze Matematiche G.L. Lagrange

DIPARTIMENTO DI MATEMATICA GIUSEPPE PEANO
UNIVERSITÀ DI TORINO

Thursday, 18 April 2019 – at 14.00
Aula Buzano, Politecnico di Torino

Simone Dutto
Politecnico di Torino

An overview about elliptic curve cryptosystems and pairings

Abstract: In the last three decades, public key cryptography has become an indispensable component of our global communication digital infrastructure. Many of our most crucial communication protocols rely principally on three core cryptographic functionalities: public key encryption, digital signatures, and key exchange. This seminar focuses on one of the main systems adopted in implementing these functionalities: the Elliptic Curve Cryptosystems (ECC), whose security depends on the difficulty of the Discrete Log Problem in the group defined by an elliptic curve over a finite field. Another interesting system can be obtained by exploiting pairings on the divisor class group of an underlying algebraic variety, thus defining the Pairing-Based Cryptography (PBC). In particular, the Weil and Tate pairings will be of main interest, since they are the only known admissible pairings that are suitable for cryptography and they evolve cryptographic primitives of ECC when defined on elliptic curves.

For Information: fabio.fiori@food-chain.it, guglielmo.morgari@telsy.it, nadir.murru@polito.it, lea.terracini@unito.it.

CONTATTI
Associazione De Componendis Cifris
direttore@decifris.it, segreteria@decifris.it