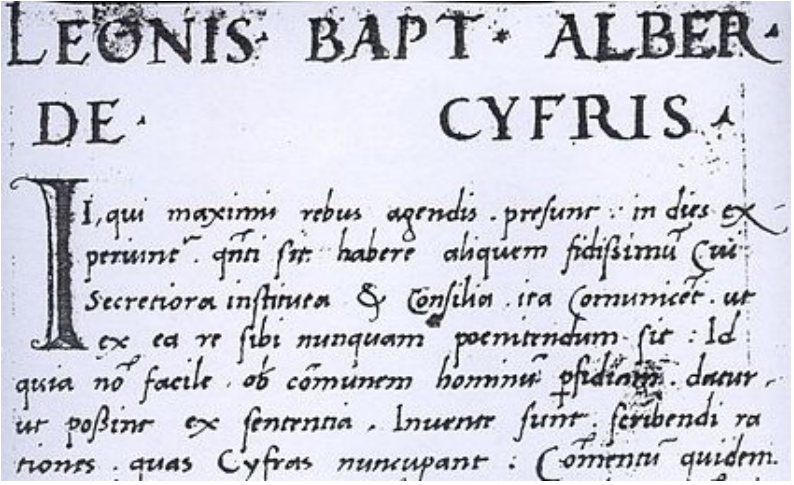


# De Cifris Augustae Taurinorum

quadrans FOUNDATION Telsy

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

DIPARTIMENTO DI MATEMATICA GIUSEPPE PEANO
UNIVERSITÀ DI TORINO

**Tuesday 17 May 2022 - 14:30**

Online on the Zoom platform at http://tiny.cc/crypto_webinar


## Gessica Alecci
## Politecnico di Torino


## A study on the use of Pell hyperbolas in DLP-based cryptosystems


**Abstract:** The group structure of the Pell hyperbolas finds numerous applications in various cryptosystems and in particular in Public-Key Encryption (PKE) schemes whose security is based on DLP, such as the ElGamal PKE scheme. In this talk, we will show a generalization of the group structure on Pell hyperbolas and provide a parameterization from both an algebraic approach and a geometrical interpretation. Moreover, we will introduce some novel ElGamal schemes over the Pell hyperbola discussing their advantages from a computational point of view thanks to a particular parametrization.



**For Information:** danilo.bazzanella@polito.it, fabio.fiori@food-chain.it, guglielmo.morgari@telsy.it, lea.terracini@unito.it.


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