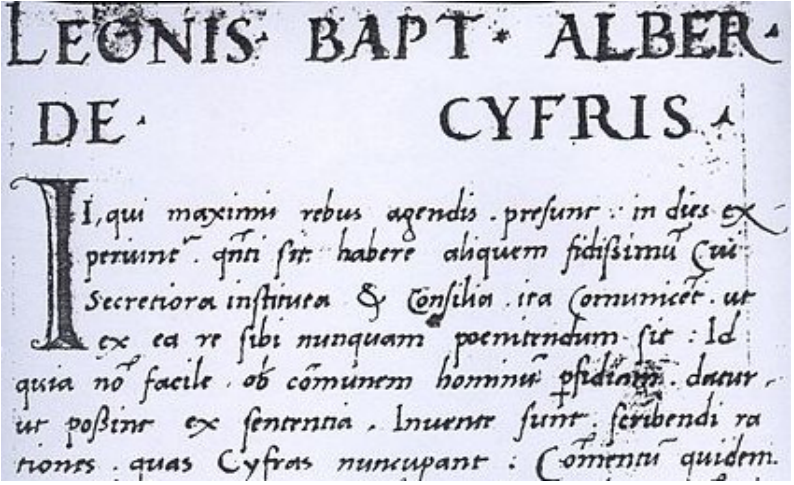

De Cifris Augustae Taurinorum

quadrans FOUNDATION Telsy

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

DIPARTIMENTO DI MATEMATICA GIUSEPPE PEANO
UNIVERSITÀ DI TORINO

Tuesday 18 January 2022 - 14:30

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

Javier Verbel

TII - Technology Innovation Institute

Practical complexities of probabilistic algorithms for solving Boolean polynomial systems

Abstract: Solving a polynomial system over a finite field is an NP-complete problem of fundamental importance in cryptography. In particular, the security of the so-called multivariate cryptosystems relies in the hardness of this problem. Recently, Lokshtanov et al. (2017) introduced a probabilistic algorithm that, in the worst-case, solves a Boolean polynomial system in time $O^*(2^{n\delta})$, for some $\delta \in (0,1)$ depending only on the degree of the system, thus beating the brute-force complexity $O^*(2^n)$. Later, Björklund et al. (2019) and then Dinur (2021) improved this method and devised probabilistic algorithms with a smaller exponent coefficient δ. In this talk, we are doing to explain the main ideas behind these algorithms and their asymptotically complexities. Also, we illustrate the complexity results that we obtained in practice by implementing them in C.

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