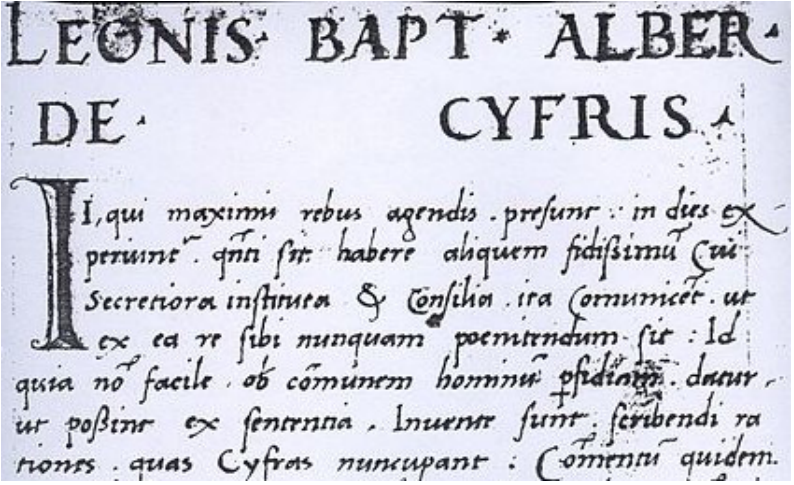
LEONIS BAPT. ALBER
DE CYFRIS

De Cifris Augustae Taurinorum

Tuesday 15 March 2022 - 14:30

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

Chiara Marcolla

TII - Technology Innovation Institute

Searchable Encryption and a practical construction

Abstract: Searchable Encryption (SE) allows data owners to efficiently outsource their data to the cloud and retrieve and update the targeted dataset without privacy violation. In the last years, researchers focused on *Dynamic Symmetric Searchable Encryption* (DSSE) schemes, which support modifications to the encrypted dataset such as document insertion or deletion. In this talk, after an introduction on searchable encryption, we are going to illustrate an efficient verifiable DSSE scheme, secure against an active adversary, which achieves an optimal efficiency - security tradeoff under the lowest configuration requirements on the client-side.

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