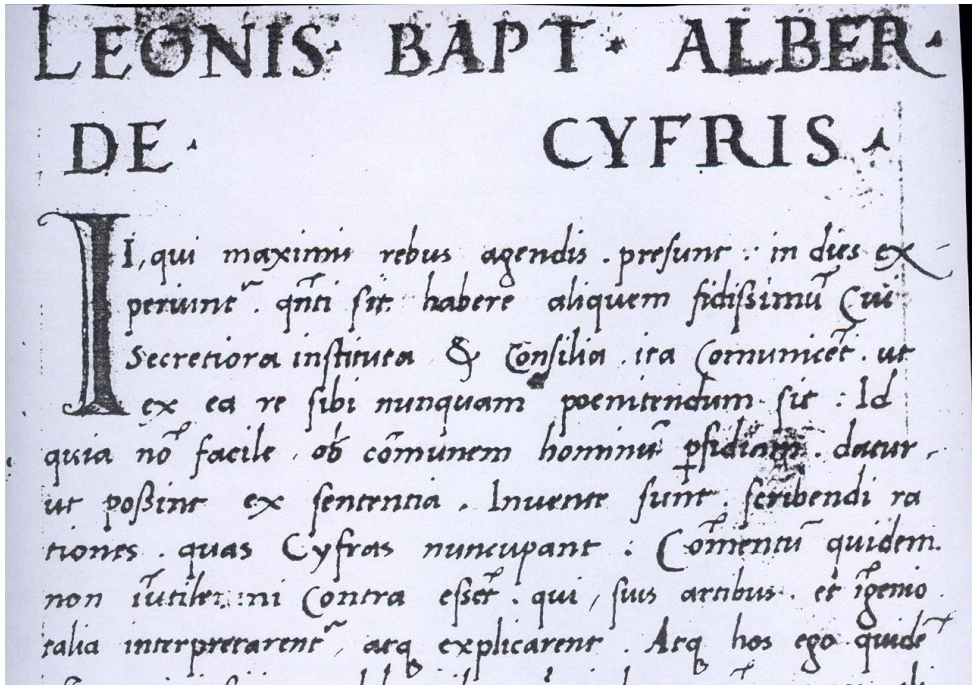
LEONIS BAPT. ALBER-
DE CYFRIS.
Il, qui maximis rebus agendis . presunt : in dies ex-
periunt . quã sit habere aliquem fidissimũ cui
Secretiora instituta & Consilia ita communicet . ut
ex ea re sibi nunquam poeniteudum sit : Id
quia nõ facile . ob cõmunem hominũ ꝓsidiatũ . datur
ut possint ex sententia . Inuenta sunt scribendi ra
tiones . quas Cyfras nuncupant : Comentu quidem
non iutilem Contra esset . qui , suis armis . et igemo
talia interpretarent , arq explicarent . Arq hos ego quide

De Cifris Schola Latina

Friday 18th June 2021 – at 11.00

Virtual conference on Webex

Roberto Civino

University of L'Aquila

On invariant subspaces in the Lai-Massey scheme and a primitivity reduction

Abstract: In symmetric cryptography, the round functions used as building blocks for iterated block ciphers are obtained as the composition of different layers acting as a sequence of bijective transformations providing global increasing complexity. The study of the conditions on such layers which make the group generated by the round functions of a block cipher a primitive group has been addressed in the past years, both in the case of Substitution Permutation Networks and Feistel Networks, giving to block cipher designers the recipe to avoid the imprimitivity attack, which exploits the invariance of some subspaces during the encryption. In the case of Lai-Massey schemes, where both Substitution Permutation Network and Feistel Network features are combined, the resistance against imprimitivity attacks has been a long-standing open problem. In this talk we show a generalization of such a scheme and we prove its resistance against the imprimitivity attack. Our solution is obtained as a consequence of a more general result in which the problem of proving the primitivity of a generalized Lai-Massey scheme is reduced to the simpler one of proving the primitivity of the group generated by the round functions of a strictly related Substitution Permutation Network. We show how this implies a reduction in the computational cost of invariant-subspace search.

Per accedere al seminario

click here

Numero riunione (codice di accesso): 137 906 9372

Password riunione: XsXJJPeN586

Contact person: Riccardo Aragona

CONTATTI

Associazione De Componendis Cifris

seminari@decifris.it

segreteria@decifris.it