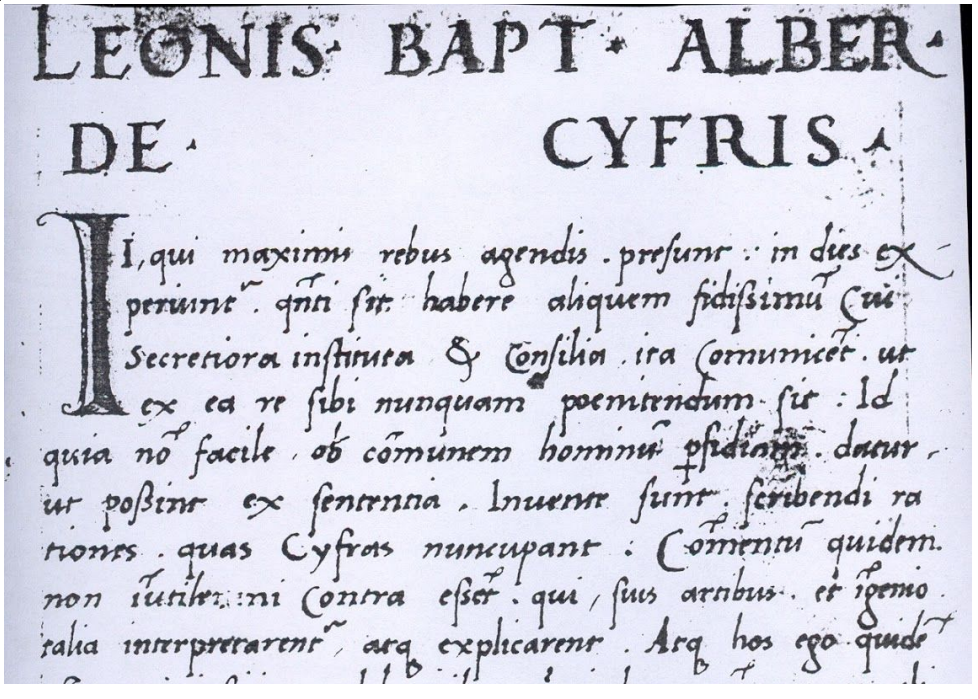
LEONIS BAPT. ALBER-
DE CYFRIS

II, qui maximis rebus agendis . presunt : in dies ex
periuntur . quã sit habere aliquem fidissimũ cui
Secretiora instituta & Consilia ita Communicet . ut
ex ea re sibi nunquam poeniteadum sit : Id
quia nõ facile . ob cõmunem hominũ pfidiam . datur
ut possint ex sententia . Inuenta sunt scribendi ra
tiones . quas Cyfras nuncupant : Comentu quidem
non iutile . ni Contra esset . qui , suis armis . et igemo
talia interpretarent , arq explicarent . Arq hos ego quide

De Cifris Athesis

UNIVERSITÀ DEGLI STUDI DI TRENTO
Dipartimento di Matematica

FONDAZIONE BRUNO KESSLER
ICT CENTER FOR INFORMATION AND COMMUNICATION TECHNOLOGY

Monday 16th December 2019 – at 10:00 a.m.
University of Trento
Room A219, "Polo Ferrari" - Povo 1 - *Via Sommarive, 5*

LUCA MARIOT
Università Milano Bicocca

Boolean Functions, S-boxes and Evolutionary Algorithms

Abstract: Boolean functions and S-boxes are a fundamental building block in the design of symmetric ciphers. Indeed, the security of several approaches such as the combiner model for stream ciphers or the substitution-permutation network for block ciphers can often be reduced to the cryptographic properties of the underlying Boolean functions and S-boxes. However, finding a Boolean function or an S-box with an appropriate trade-off of properties represents a difficult combinatorial optimization problem which is not amenable to exhaustive search, as soon as the number of variables becomes too high. In this respect, Evolutionary Algorithms (EAs) represent an interesting heuristic method to address this optimization problem.

In this talk, we give a general survey of the literature concerning the use of EAs for optimizing the cryptographic properties of Boolean functions and S-boxes. Starting from the seminal works in the late 90s based on Genetic Algorithms to evolve balanced nonlinear Boolean functions, we will then show the most recent and successful approaches based on Genetic Programming, that allowed to evolve optimal S-boxes defined by cellular automata.

Contact person: Massimiliano Sala

CONTATTI
Associazione De Componendis Cifris

direttore@decifris.it
segreteria@decifris.it