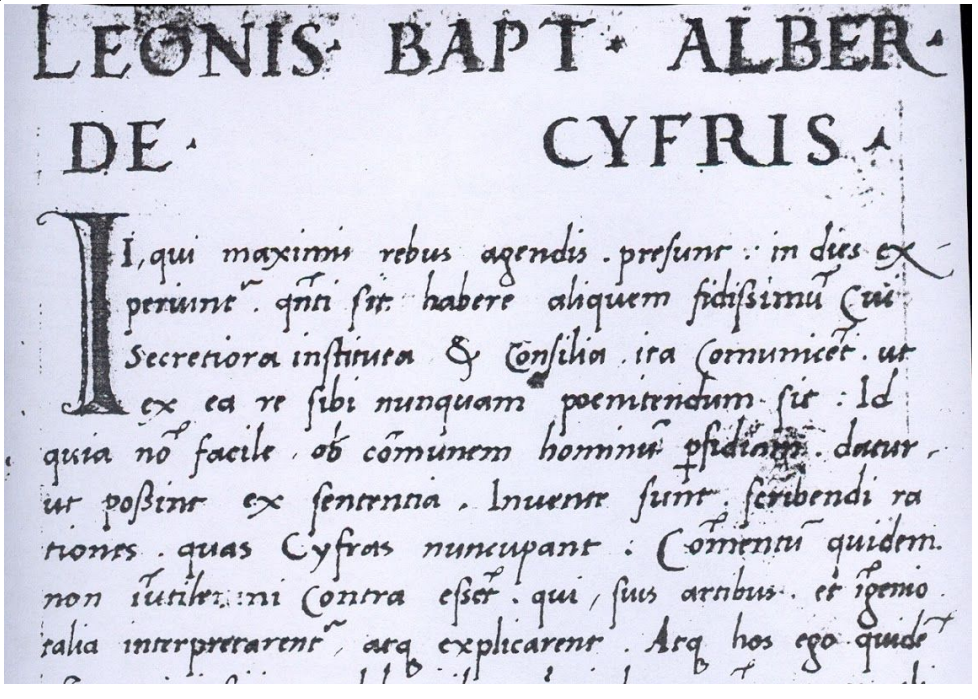
LEONIS BAPT. ALBER-
DE CYFRIS.

II, 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 poeniteadum sit : Id
quia nõ facile . ob cõmunem hominũ ꝓfidiam . datur
ut possint ex sententia . Inuenta sunt . scribendi ra
tiones . quas Cyfras nuncupant : Comentũ quidem
non iutilissimi Contra esset . qui , suis armis . et igemo
talia interpretarent , atq explicarent . Atq hos ego quide

De Cifris Athesis

UNIVERSITÀ DEGLI STUDI DI TRENTO
Dipartimento di Matematica

FONDAZIONE BRUNO KESSLER
ICT CENTER FOR INFORMATION AND COMMUNICATION TECHNOLOGY

Tuesday 11th June 2019 – at 10:00 a.m.
Seminar Room -1, Department of Mathematics

Marco Calderini
University of Bergen

On equivalence relations of Boolean functions

Abstract: The nonlinearity and differential uniformity are properties of a vectorial Boolean function measuring its resistance to linear and differential attacks. APN and AB functions provide optimal resistance against these attacks. Among the equivalence relations that have been defined for Boolean functions, preserving these cryptographic properties, there are the EA-equivalence and the more general CCZ-equivalence.

The notion of CCZ-equivalence is difficult to handle, indeed checking whether two given functions are CCZ-equivalent or not is hard. Also building functions CCZ-equivalent (but not EA-equivalent) to a given function is hard.

In the first part of this talk, we will discuss some properties of the CCZ- and EA-equivalence and their relations.
In the last part, we will discuss the equivalence between some classes of APN functions.
We will reduce the list of known families of polynomial APN functions by excluding all equivalent cases.

Contact person: Massimiliano Sala

CONTATTI
Associazione De Componendis Cifris

direttore@decifris.it
segreteria@decifris.it