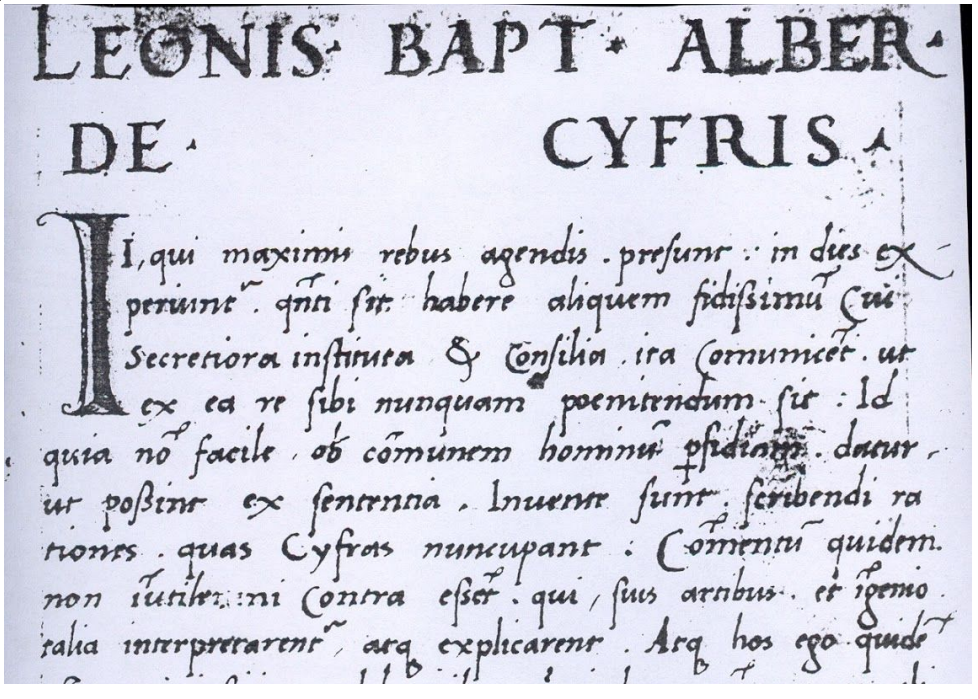
LEONIS BAPT. ALBER-
DE CYFRIS

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 poeniteudum 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 iutilem 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 10th September 2019 – at 9:00 a.m.
Department of Mathematics
Room A222, Povo 1, Via Sommarive, 9, Povo Trento

Chiara Bodei

Università degli Studi di Pisa

Control Flow Analysis for process algebras with applications to security

Abstract: Security is a growing concern in the development of software, especially magnified in the era of the Internet of Things, where digitally connected devices are intruding into our everyday life.

In this talk, we will focus on how Control Flow Analysis (CFA) can be applied to verify the security of systems. This static technique safely approximates the abstract behaviour of distributed systems, when specified in a process algebraic guise. These abstractions provide the basis for checking various properties.

We will present an excursus on the use of CFA that goes from some authentication properties of cryptographic protocols to some security properties of data in the Internet of Things.

Contact person: Massimiliano Sala

CONTATTI
Associazione De Componendis Cifris

direttore@decifris.it
segreteria@decifris.it