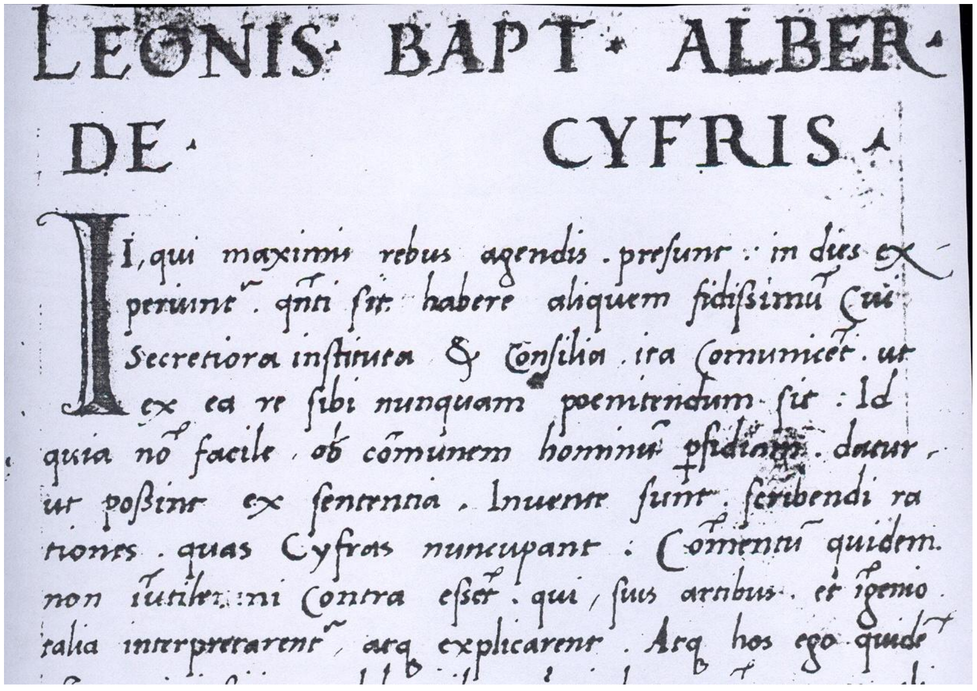

LEONIS· BAPT· ALBER·
DE· CYFRIS·

Ii, qui maximis rebus agendis . preſunt : in dies ex-
periunt̃ . quanti ſit habere aliquem fidiſsimũ cui
Secretiora inſtituta & Conſilia . ita comunicet . ut
ex ea re ſibi nunquam poenitendum ſit : Id
quia nõ facile . ob cõmunem hominũ pfidiam . datur .
ut poſsint ex ſententia . Inuentę ſunt . ſcribendi ra
tiones . quas Cyfras nuncupant : Cõmentũ quidem .
non inutile : ni Contra eſset . qui , ſuis artibus . et ingenio .
talia interpretarent̃ , atq explicarent . Atq hos ego quidẽ

MathCifris
UMI

UNIVERSITÀ DEGLI STUDI
DI TRENTO
Dipartimento di Matematica

OP	a	b	c	d	e	f	g	h	i	l	m
	x	y	z	n	o	p	q	r	ſ	t	u
QR	a	b	c	d	e	f	g	h	i	l	m
	q	r	ſ	t	u	x	y	z	n	o	p
ST	a	b	c	d	e	f	g	h	i	l	m
	p	q	r	ſ	t	u	x	y	z	n	o
VX	a	b	c	d	e	f	g	h	i	l	m
	u	x	y	z	n	o	p	q	r	ſ	t
YZ	a	b	c	d	e	f	g	h	i	l	m
	o	p	q	r	ſ	t	u	x	y	z	n

Wednesday 2nd November – at 10:00 a.m.

online seminar – live from the “Seminar Room -1”, Povo 0

Luca Mariot

Radboud University

Behind the scenes of a new construction for bent functions: a tour among cellular automata, Latin squares and linear recurring sequences.

Abstract:

Bent functions are a particular class of Boolean functions reaching the highest possible nonlinearity; as such, they have many interesting applications for the design of symmetric ciphers, as well as for error-correcting codes and sequences. Despite their simple definition, a complete characterization of bent functions is still far out of reach, even after more than four decades of research on the topic. In particular, the related literature sports a multitude of different constructions, and nowadays introducing a new one requires careful examination of the functions it generates, to assess whether they are equivalent to previously known classes.

This talk is about one such new construction of bent functions, giving a "behind the scenes" story that shows how we arrived at this result. We use mutually orthogonal latin squares based on cellular automata to define a Hadamard matrix associated to a bent function. Next, we explain the connection with linear recurring sequences and partial spreads. We conclude with some encouraging results on the rank distribution of our bent functions, which indicate that many are neither in the Maiorana-McFarland class nor in the Desarguesian partial spread.

Registration for the online event to *be made by* 1st November via the following link:

click here

Subscribers will receive the Zoom ID one hour before the start of the event

Contact person: Massimiliano Sala

CONTATTI
Associazione De Componendis Cifris

seminari@decifris.it
segreteria@decifris.it