Otto-von-Guericke-Universität Magdeburg
Fakultät für Mathematik

Auf Einladung des Institutes für Algebra und Geometrie spricht

Herr Prof. Dr. Enes Pasalic

University of Primorska, Faculty of Mathematics, Natural Sciences and Information Technologies (UP FAMNIT)
Koper, Slowenien

über das Thema

On certain nonlinear actions in cryptography

Ort: Otto-von-Guericke-Universität Magdeburg, Gebäude 02, Raum 20

Zeit: Dienstag, 10. Dezember 2019, 13.00 Uhr

Zu diesem Vortrag laden wir alle Interessierten herzlich ein.

Prof. Dr. Alexander Pott

Abstract: Functions that map from $GF(2)^n$ to $GF(2^m)$, commonly called vectorial Boolean functions, are of special interest in cryptography and also have applications in coding theory, sequences, association schemes and other related combinatorial objects. In particular, certain particularly important properties of these mappings remain preserved when applying affine transforms both to their input and output. These transforms then give rise to a whole affine equivalence class of a single object considered. However, in certain cases some suitable nonlinear transforms may also be applied that also efficiently preserve most of the characterising properties of these objects.

The main goal of this talk to give an overview of these discrete objects of special importance, to provide their characterisation in different terms and to discuss the above mentioned nonlinear actions briefly.

The presentation will be self-contained, thus only elementary background in discrete mathematics is necessary.