Mentor

Prof. Enes Pasalic; PhD

Research field

1.01.00 - Natural sciences and mathematics / Mathematics

Faculty member of UP and the research programme

UP Andrej Marušič Institute,
UP Faculty of Mathematics, Natural Sciences and Information Technologies

research programme: **P1—0404 Mathematical modelling and encryption: from theoretical concepts to real-life applications**

Other information about the mentor

E-mail: enes.pasalic@upr.si

A brief description of the future young researcher training

The framework of the training programme:
The young researcher (YR) will join the research program P1—0404 Mathematical modelling and encryption: from theoretical concepts to real-life applications and the research projects listed below, as well as to numerous bilateral projects implemented at UP IAM (http://p1-0285.iam.upr.si/en/bilateral-projects) and UP FAMNIT (www.famnit.upr.si/en/research).

YR will also be actively involved in new projects applications and organization of international conferences at UP IAM and UP FAMNIT.

The research program has diversified research cooperation with similar research groups abroad (USA, Canada, Spain, China, South Korea, Australia, New Zealand, Israel, Russia, Austria, Slovakia, Italy and Hungary). YR will actively participate in this international scientific and research cooperation.

Within the research program and projects, various areas of mathematics are considered: YR's work will be primarily conduct research in cryptography and different topics of discrete mathematics.

In the course of his/her training, YR will be working on some specific problems related to certain combinatorial properties of discrete structures of importance in cryptography. More precisely, certain polynomials over finite fields fulfil some necessary cryptographic design criteria, thus being suitable to be used in many cryptographic primitives. Though there are several known classes of these perfect combinatorial objects, some generic and efficient construction methods remain to be discovered. A broader existence of such mappings can be confirmed by computer simulations, however a theoretical background related to their structure and interplay of its so-called coordinate functions is currently unknown. The main objective of the proposed research is to deepen our understanding of how these objects are built and in particular a novel approach, introduced recently by Enes Pasalic et al., based on the spectral analysis, is supposed to be employed. This method has already given some partial answers related to some specific classes of Boolean functions that are necessary building blocks of such mappings. Nevertheless, their exact interplay in spectral domain needs to be precisely characterize which would be a significant progress in this field. This research will, apart from pure mathematical tools, strongly rely on efficient programming related to recognition of spectral patterns.

List of research programmes and projects:

Code	Title	Duration
P1—0404	Mathematical modelling and encryption: from theoretical concepts to real-life applications	1.1.2019—31.12.2024
J1—1694	Designing certain perfect discrete combinatorial objects in spectral domain	1.7.2019—30.6.2022
J1—9108	Semiregular elements in 2-closures of solvable groups	1.7.2018—30.6.2021

Preferable area of study for the young researcher
Mathematical Sciences, doctoral degree study programme Mathematical Sciences, UP FAMNIT

Other useful skills and competences for the position:
English language (advance - intermediate level)

Useful links

UP Andrej Marušič Institute (http://www.iam.upr.si/en/)
UP Faculty of Mathematics, Natural Sciences and Information Technologies (https://www.famnit.upr.si/en)