Mentor	**Dr. Enes Pašalić**
Akademski/znanstveni naziv	docent, višji znanstveni sodelavec
Raziskovalno področje mentorja	Kriptologija / Cryptology
Članica UP in raziskovalna skupina	**Univerza na Primorskem** **Inštitut Andrej Marušič (UP IAM)** *Raziskovalna skupina UP IAM*
Več informacij	olga.kaliada@upr.si
Kratek opis raziskovalnega dela kandidata za mladega raziskovalca	Kriptografija je ena od najzanimivejših disciplin uporabne matematike, ki se neprestano razvija. Vključuje več znanstvenih disciplin: matematiko, računalništvo, teorijo informacij, če omenimo samo nekatere. Kriptografija je zaradi širokega nabora različnih disciplin ter velikega števila uporabnih aplikacij najbolj »vroča« raziskovalna disciplina s tesnimi povezavami z industrijo, varnostnimi projekti, patentnimi aplikacijami itn. Mladi raziskovalec bo delal na razvoju nekaterih enkripcijskih shem. V okviru njegovega dela bo veliko priložnosti za izmenjavo in sodelovanje z nekaterimi svetovno znanimi kriptografskimi centri na Danskem (DTU), Nemčiji (Otto-von-Guericke), Švedski (Lund), Franciji (Pariz), itn. Poleg homomorfnih enkripcijskih shem (ki imajo širok spekter aplikacij tudi v računanju v oblaku (cloud computing)), je načrtovanje enkripcijskih in avtentifikacijskih algoritmov v omejenih hardverskih okoljih eden od najbolj vznemirljivih izzivov moderne družbe. To načrtovanje se sooča s precej restriktivnimi implementacijskimi pogoji, istočasno pa morajo načrtovani algoritmi dosegati predpisano stopnjo varnosti. Glavna naloga doktorskega študija mladega raziskovalca bo nadaljnji razvoj zgoraj omenjenih algoritmov, kakor tudi kriptoanaliza enkripcijskih shem povezanih z RFID aplikacijami. Mladi raziskovalec bo doktorski študij opravljal na Univerzi na Primorskem, Fakulteti za matematiko, naravoslovje in informacijske tehnologije. Zaželeno je, da ima kandidat za mladega raziskovalca dodiplomsko izobrazbo iz matematike, ali pa dodiplomsko izobrazbo iz računalništva oziroma elektrotehnike. V vsakem primeru se zahteva visoka ocena iz matematike ter dobro povprečje ocen predmetov dodiplomskega študija. **Short description of scientific research program of PhD student:** Today's cryptology is one of the most interesting disciplines in applied mathematics, being under constant development. It comprises several disciplines such as mathematics, computer science, information theory, to name a few. This broad range of different disciplines and an extremely wide range of applications makes today's cryptography to be one of the hottest research topics with close relations to industry, security projects, patent applications etc. The PhD student will work on further development of certain encryption schemes with a plenty of possibilities for exchange programs and collaboration with the world

	leading groups in cryptography in Denmark (DTU), Germany (Otto-von-Guericke), Sweden (Lund), France (Paris) etc. Along with homomorphic encryption schemes (that have a wide range of applications e.g. in cloud computing) the design of encryption and authentication algorithms in restricted hardware environments is one of the most exciting challenges in modern society. These primitives are supposed to meet rather severe implementation conditions while at the same time achieving prescribed level of security. The major objective of PhD program is a further development of design techniques as well as cryptanalysis of encryption schemes related to RFID applications. PhD student is supposed to do his studying at University of Primorska, Faculty of Mathematics, Natural Sciences and Information Technologies. **Prerequisites:** It is desirable that the applicant has a math education as a background, though applicants from computer science and electrical engineering are also welcome. However, excellency in mathematics and overall good grades are requested.
Uporabne povezave	UP Fakulteta za matematiko, naravoslovje in informacijske tehnologije UP Inštitut Andrej Marušič