PhD positions in Cryptology

Centre for Research on Cryptography and Security (CRoCS), Masaryk University, is looking for two excellent, motivated, self-driven doctoral students to work in the area of information security and cryptology. The PhD students will join the group of Vashek Matyas and a project (starting 1. 1. 2016) funded by the Czech Science Foundation. The project focuses on randomness analysis of outputs of cryptographic primitives, and its goal is to find defects in cryptographic functions using automated supervised construction of statistical tests of randomness.

The work to be undertaken will be focused on randomness analysis, but it is also in intersection with genetic algorithms, statistics, data analytics and algebra.

The positions are fully funded with funding provided by Masaryk University and the Czech Science Foundation.

The PhD students are expected to have a MSc degree or equivalent at the start of their study, and a solid background in computer science or engineering, with some background in either statistics or algebra. Relevant research papers (author's pre-print can be requested from Vashek Matyas or Marek Sýs):


Contact:  
Vashek Matyas, Marek Sýs  
Centre for Research on Cryptography and Security,  
Faculty of Informatics,  
Masaryk University.

Email:  
matyas@fi.muni.cz, syso@mail.muni.cz