Péter Hudoba

EIT Digital Budapest DTC

PhD topic: Cryptology based on combinatorical problems

PhD supervisor: Dr. Péter Burcsi, ELTE

Industrial partner: Daniel A. Nagy (ePoint Systems Ltd.)

Contact: hudi1989@gmail.com

> 'At the EIT Digital Doctoral School I want to learn how I can be a better project manager, team leader or CEO. With this knowledge, I plan to lead my company from being a startup to being recognized in Europe, or join a big company in a high position.

Achievements & further plans

Péter has just started his PhD studies, his research topic is cryptography based on combinatorial problems. In one hand, the main subject is to invent **new cryptographic primitives** which are **not breakable by a quantum computer**. These computers are now small and cannot break the classical systems (RSA, ElGamal), but they can pose a really big threat in the next 10-20 years. On the other hand, he is focusing on the improvement of the existing ones, because they have a public key that is too large compared to the well-known ones and they have slower encrypting algorithms. When he finishes his PhD studies, he plans to join a cryptographic team to make the digital communication more secure in Europe.

> In order to keep confidental industrial information secure at a low cost, we need to develop stronger, faster and more compact encryptions to save bandwidth, processor time and storage capacity.

Educational status at Spring semester of 2016:

RA · OR · BMD · GH · Mobility · BDExp.

Reserach topic

His research aims to improve the post-quantum algorithms and develop new primitives to make the communication more stable and secure in the future. He is working with well-known problems from different parts of mathematics, because a strong problem that cannot be solved in polynomial time can be a good base for a new public key encryption, digital signature or a one-way function.

Currently, he is focusing on the Secure multi-party computation that helps voting via unsecured medium without sharing your exact vote, or validating a key between two parties without risks and so on. These algorithms are important too, for example, because after we built up a secured channel, we have to authenticate our partner again at a lower communication and computational cost.

There are existing cryptographic systems (digital signature and public key encryption) that cannot be broken by a quantum computer, but those are not so effective, so we have to continue the development of new primitives that can be widely used in the future networking, when quantum computers will pose a real threat to computers.