Tárgyleírás

Tárgy neve: Post-quantum cryptography

Tárgyfelelős neve: dr. Kutas Péter

Tárgyfelelős tudományos fokozata: PhD

Tárgyfelelős MAB szerinti akkreditációs státusza: AT

Az oktatás célja angolul / Aim of the subject:

Knowledge

- They have comprehensive and up-to-date knowledge and understanding of the general theories, contexts, facts, and the related concepts of IT, particularly – depending on their chosen specialization – in the areas of program design, synthesis and verification, logical programming, programming languages, computing models, computer architectures, operating systems, computer networks, distributed systems, database management systems, information theory, code theory, and cryptography.
- They have comprehensive and up-to-date knowledge of the principles, methods, and procedures for designing, developing, operating, and controlling IT processes, particularly – depending on their chosen specialization – in the areas of program design methods; design, construction and management of complex software systems and databases in modern database management systems; service-oriented program design; the design, construction and management of information systems; the design and development of tools and services for the internet; the design, development and management of database systems; the design, construction and management of distributed systems, cryptography, data security and data protection.

Abilities

- They are able to apply their mathematical, computer science and informatics skills in a novel way in order to solve tasks in IT research and development.
- They are able to formalize complex IT tasks, to identify and study their theoretical and practical background and then to solve them.
- They are able to perform design, development, operation, and management tasks when operating complex software systems, database management systems, corporate information systems, decision support systems, and expert systems.

- Under professional guidance, they are able to carry out scientific research on their own, and to prepare for further studies at postgraduate level.

Attitude:

- They follow professional and technological developments in their IT field.
- They are committed to critical feedback and evaluation based on self-examination.
- They are committed to lifelong learning, and are open to acquiring new IT competencies.
- They accept and make their co-workers apply the ethical principles of work and organizational culture as well as those of IT scientific research.
- They share their knowledge and consider it important to disseminate professional IT results.
- They consider it important to propagate and realise environmentally conscious behaviour and social responsibility, and they promote them with the help of information technology.
- They are committed to having quality requirements met and to analysing them with IT tools.
- They are open to proactive collaboration with IT and other professionals.

Autonomy, responsibility:

- They take responsibility for their professional decisions made in their IT-related activities.
- They undertake to meet deadlines and to have deadlines met.
- They bear responsibility for their own work as well as for the work of their colleagues they work together with in a project.
- Regarding mission critical IT systems, they can be entrusted with developing and operational responsibilities that are in accordance with their professional competencies.

Az oktatás tartalma angolul / Major topics:

Hidden subgroups and applications to discrete log and factoring. Introduction to lattices and hard problems about lattices. Lattice reduction (Lagrange, Hermite, LLL). General lattice-based schemes (GGH, Ajtai-Dwork), their cryptanalysis, NTRU and attacks. LWE and SIS, Regev key exchange, Micciancio one-way-fuction. Ring-LWE, Module-RWE problems, modern lattice-based schemes. Ideals of polynomial rings, Gröbner-bases. Oil and Vinegar digital

signature, attacks. UOV, HFE, Rainbow schemes and attacks. Error correcting codes, Mceliece cipher, Rank metric codes and protocols. Wave and furthet code-based signitures. Elliptic curves, isogenies. SIDH key exchange and attacks. HHS framework, CSIDH, CSi-FiSh. KLPT algorithm, GPS and SQISign digital signatures. Hash-based cryptography.

A számonkérés és értékelés rendszere angolul / Requirements and evaluation:

Exam

Irodalom / Literature:

Chris Peikert: A decade of lattice-based cryptography, https://eprint.iacr.org/2015/939.pdf

Neil Koblitz: Algebraic aspects of cryptography, Springer, 2010

Luca De Feo: Mathematics of isogeny-based cryptography, https://arxiv.org/abs/1711.04062

Dan Bernstein, Johannes Buchmann, Erik Dahmen: Post-quantum cryptography, Springer, 2009.

Various further parts from the literature.