|  |  |
| --- | --- |
| **Course title** | **Implementations of quantum cryptography** |
| **School name and date** | Quantum cryptography, July 17 – July 29, 2023 |
| **Teaching staff** | Dr hab. Karol Horodecki, prof. UG, mgr Bianka Wołoncewicz, Dr Mikołaj Czechlewski, mgr Maciej Stankiewicz, Dr hab. Marcin Pawłowski, prof. UG |
| **Forms of classes, the realization and number of hours** | |
| 1. **Forms of classes** | Lectures, problem sessions |
| 1. **The realization of activities** | Lecture with discussion, multimedia presentation, problem solving |
| 1. **Number of hours** | 20 (lecture) + 10 (problem session) |
| **Suggested prerequisite knowledge** | |
| Elements of Linear Algebra, Foundations of Physics | |
| **Brief description of the course** | |
| The course introduces the basics of quantum optics and various aspects of the physical realization of quantum key distribution (QKD) protocols. It describes the family of attacks based on imperfections of the implementation of the QKD protocols and possible attacks on the future quantum network infrastructure. It also introduces private randomness as a cryptographic resource and describes how to obtain it from weak sources of private randomness by quantum-cryptographic means. | |
| **Course contents** | |
| 1. **Introduction to Quantum optics**   Quantum-optical elements such as beam splitters, polarized beam splitters, half wave-plate, etc., and their physical properties, generation of entanglement, reading simple quantum-optical experimental setups related to quantum cryptography, mathematical formalism of quantum optics including  Fock space, 2nd quantisation, basic operator algebra,  quantum states of light, commutation relations   1. **Practical QKD protocols**   Practical realizations of BB84, BBM92, E91 and COW protocols including the impact of optical elements such as photodetectors, optical fibres, nonlinear crystals on their efficiency and security. Parameters important for practical applications such as distance, key generation rates and costs will be discussed for both: existing implementations and future possibilities. The current state of the solutions available on the market will be presented.   1. **Attacks on quantum key distribution devices and quantum Internet**   Attacks on quantum-key distribution devices, including – beam splitter attacks, different path lengths attack, various blinding attacks on quantum detectors, decoy quantum key distribution Measurement-Device-Independent quantum key distribution and its performance, attacks on quantum Internet including re-routing attacks, and their counter-measure.   1. **Private randomness as a quantum cryptographic resource**   Application of private randomness in cryptography and beyond, NIST standards, quantum random number generators – from dependent to independent quantum to classical randomness extractors, leftover hash lemma, examples of classical extractors, sources of weak randomness definition and examples, no-go theorem for Santha-Vazirani source, quantum DI random number generators, private randomness amplification, and expansion. Independent states, private randomness distillation in the bipartite scenario. | |
| **Literature** | |
| * Feihu Xu, Xiongfeng Ma, Qiang Zhang, Hoi-Kwong Lo, Jian-Wei Pan „Secure quantum key distribution with realistic devices” Rev. Mod. Phys. 92, 025002 (2020) * T. Satoh, S. Nagayama, S. Suzuki, T. Matsuo, M. Hajdušek and R. V. Meter, "Attacking the Quantum Internet," in IEEE Transactions on Quantum Engineering, vol. 2, pp. 1-17, 2021, Art no. 4102617, doi: 10.1109/TQE.2021.3094983. * Bera MN, Acín A, Kuś M, Mitchell MW, Lewenstein M. *“Randomness in quantum mechanics: philosophy, physics and technology”*. Rep Prog Phys. 2017 Dec;80(12):124001. doi: 10.1088/1361-6633/aa8731. PMID: 29105646. * C. Gerry, P. Knight *“Introduction to Quantum Optics”* Cambridge University Press 2012 | |
| **Contact** | karol.horodecki@ug.edu.pl |