|  |  |
| --- | --- |
| **Course title** | **Theory of quantum cryptography** |
| **School name and date** | Quantum cryptography, July 17 – July 29, 2023 |
| **Teaching staff** | Dr hab. Karol Horodecki, prof UG, mgr inż. Jan Wasilewski, Dr. Mikołaj Czechlewski, mgr. Leonard Sikorski, Dr Anubhav Chaturvedi, mgr. inż. Marek Winczewski |
| **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 describes the basics of quantum mechanics and some quantum resources such as entanglement and Bell nonlocality. It further introduces today's used quantum cryptographic protocols, such as BB84, E91, and B92, as well as fundamental facts about lower bounds on the key rate achievable by quantum means both in a single shot and asymptotic case. Further, device-independent and semi-device-independent quantum key distribution is introduced and thoroughly discussed. The challenges and theory of design of the future quantum Internet are described in detail, including the generations of quantum repeaters. Finally, the upper bounds on the secret key rate are presented both in device-dependent and device-independent quantum key distribution regimes. | |
| **Course contents** | |
| 1. **Introduction to quantum information theory formalism, phenomena of entanglement and Bell non-locality**   Axioms of the Quantum Mechanics, von-Neumann measurement and POVMs, elements of information theory including the notion of Shannon entropy, mutual information and conditional mutual information and their quantum counterparts, the notion of entanglement, the protocol of teleportation and entanglement swapping, the notion of non-locality, Bell inequalities including CHSH and Chain Bell inequality.   1. **Quantum key distribution protocols**   Threats to classical cryptography by quantum computing (elements of Shor’s and Simon’s algorithm for breaking RSA and some non-quantum block ciphers). Protocols including BB84, E91, B92, SARG04, and the performance of some of them. Lower bound on key-rate achievable by Devetak-Winter protocol. The idea of security of the BB84 (Shor-Preskill proof). Definitions of min and max entropies, single shot lower and upper bounds on secret key rates (Renner-Renes bounds).   1. **Device and semi-device-independent quantum key distribution**   Standard Quantum Device Independent protocol based on (3,2,2,2) scenario, the idea of the proof of security in a) iid scenario including technique based on Jordan’s lemma b) non-iid – based on the entropy accumulation theorem. Overview of the variants of these protocols. Lower bounds on their performance, the definition of several loopholes, 3 Experimental realizations of QDI protocol that cover the loopholes. Semi-device independent protocol by Pawłowski & Brunner, their variants and performance. The scenario of the non-signaling adversary, the protocol of Hänggi & Renner in this scenario.   1. **Quantum secured-Internet challenges and achievements**   The challenge of no-cloning theorem, three generations of Quantum Internet, comparison of the latter, practical distillation protocols including DEJMS and EPL-D and their optimization, key repeaters no-go, Christandl-Ferrara bound, optimization involved in network layers. Model inspired by TCP/IP stack: Application, Transport (qubit transmission), Network(long distance entanglement), Link (robust entanglement generation), and Physical (attempt entanglement generation). Quantum Network and Link Layer protocols.   1. **Upper bounds on QKD key rates**   Upper bounds on device-dependent quantum key distribution based on entanglement measures – squashed entanglement and relative entropy of entanglement, multiplex channel-based upper bounds on device-dependent key for states and channels, Upper bounds on quantum device independent key via intrinsic non-locality, cc-reduced squashed non-locality and relative entropy of entanglement, the gap between device independent and dependent key, the paradigm of non-signaling eavesdropper and upper bounds on key rates in the latter scenario. | |
| **Literature** | |
| M.A. Nielsen, I.L. & Chuang, 2011. *Quantum Computation and Quantum Information: 10th Anniversary Edition*, Cambridge University Press.  V. Zaptero, T. van Leent, R. Arnon-Friedman, W-Z. Liu, Q. Zhang, H. Weinfurter and M. Curty  npj Quantum 9, 10 (2023) “Advances in device-independent quantum key distribution” I. W. Primaatmaja, K. T. Goh, E. Y.-Z. Tan, J. T.-F. Khoo, S. Ghorai, and Ch. Lim “Security of device-independent quantum key distribution protocols: a review” Quantum 7, 932 (2023)  Esther Hänggi, Doctoral thesis, ETH Zurich, 2010  S. Wehner, D. Elkouss, R. Hanson “Quantum Internet: A vision for the road ahead” Science  19 Vol 362, Issue 6412 (2018) | |
| **Contact** | karol.horodecki@ug.edu.pl |