Relativistic quantum cryptography (E8)

Non-Examinable (Graduate Level)

Dr. Damián Pitalúa-García

Quantum cryptography exploits quantum properties (for example, the no-cloning theorem) to guarantee higher security than what can be achieved by classical cryptography. Relativistic quantum cryptography further exploits the principle of no-superluminal signalling to guarantee even higher security in some scenarios. The course gives an introduction to quantum cryptography, focusing on relativistic quantum cryptography.

The course will cover a selection of topics including:

- Quantum key distribution
- Quantum tokens
- Quantum position verification
- Tasks and schemes in relativistic quantum cryptography

Prerequisites

Familiarity with undergraduate level quantum mechanics is essential. This course will assume knowledge of basic concepts in quantum information like the Dirac notation, pure and mixed states, density matrices and the postulates of quantum mechanics. Familiarity with a first course in quantum information (e.g., from Part II or Part III Quantum Information) would be highly advantageous. Familiarity with basic concepts of special relativity (e.g., spacetime diagrams and light cones) will also be beneficial.

Literature

1. C. H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. In Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India, 175–179, (1984).
2. S. Wiesner. Conjugate coding. SIGACT News, 15: 78-88, (1983). http://dl.acm.org/citation.cfm?doid=1008908.1008920
3. A. Kent. Unconditionally Secure Bit Commitment. Physical Review Letters, 83: 1447–1450 (1999). http://link.aps.org/doi/10.1103/PhysRevLett.83.1447
4. A. Kent, W. J. Munro and T. P. Spiller. Quantum tagging: Authenticating location via quantum information and relativistic signaling constraints. Physical Review A 84: 012326 (2011). http://link.aps.org/doi/10.1103/PhysRevA.84.012326
5. H. Buhrman, N. Chandran, S. Fehr, R. Gelles, V. Goyal, R. Ostrovsky and C. Schaffner. Position-based quantum cryptography: Impossibility and constructions. SIAM Journal on Computing, 43: 150–178 (2014). http://dx.doi.org/10.1137/130913687

Additional support

A discussion session can be organised.