9.12.2020 *Quantum Cryptography: Public Key Distribution and Coin Tossing* by Charles H. Bennett and Gilles Brassard *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, 175-179 (1984)*

Questions/Tasks/Stimulations:

o Bibliometrics: What do you know about the authors and impact of the paper? o In which sense the paper is a milestone? o Which problem exactly is addressed in this publication?

o Describe/Explain the “Quantum Public Key Distribution” (= BB84 protocol). Make clear: what are the essentials required for the protocol. Which of them are most challenging to realize?

o Illustrate the security of the BB84 protocol by explaining a simple eavesdropping attack (e.g. intercept-resend strategy). Which other attacks are possible? Discuss the term ‘side-channel’ in this context.

o How would you experimentally realize Alice and Bob to implement the BB84 protocol? Provide a sketch.

o Who performed the first experiment (implementation) based on the BB84 protocol? How close did this experiment follow the original idea?

o Describe/Explain the “Quantum Coin Tossing” protocol. In which way is it different/similar to the BB84 protocol and why is it important.

o Which protocol would have higher relevance in real-world applications and why? o Report about experimental implementations of “quantum coin tossing”, also

referred to as “quantum coin flipping”.

o Explain/Discuss the possibility of loopholes, i.e. “cheating”, in quantum coin tossing.

o Are commercial products for quantum communication available? Which technology are the based on? How about the price?