06.01. Artur K. Ekert: *Quantum Cryptography based on Bell's Theorem.* Physical Review Letters 67, 661 (1991).

Presenter (10 min):

Sketch the key result. (Hint: Do not spend too much time on section 3)

Bibliometrics: what do you know about the author? Which papers and results does it build on? What are the implications of this result? Why is the paper a milestone?

Questions:

1. What is the goal of the Ekert protocol?

2. Compare to the BB84 protocol. What is the main difference?

3. Explain the protocol in 5 steps.

4. Why is the No-cloning-theorem of crucial importance? What are the conditions in the No-cloning theorem? Explain and derive the No-Cloning-Theorem.

5. Are there any realizations? What is the main obstacle for a technological application?

6. Is it possible to measure a quantum state without disturbing it?

7. Why is the BB84 protocol more popular?

8. What is the main drawback? Talk about loopholes.

9. Are there other technological applications for entanglement? If so, talk about examples.

10. Is the successful implementation of an Ekert protocol proof of non-locality?

11. What does it mean, if Eve can eavesdrop within the Ekert protocol without Alice and Bob notificing it?

12. Is it possible to disprove nonlocality?

13. Is the notion of nonlocality important for the Ekert protocol? What is the figure of merit for a successful implementation?

14. What are the requirements for device independent QKD?