CLAIMS

1. A method of identifying occurrence of a blinding attack in a quantum cryptography system, the method comprising the steps of:

providing a light emitter at a receiver of the quantum cryptography system, wherein the light emitter is different from a transmitter of a quantum cryptography signal to be received by the receiver, wherein the light emitter is different from a transmitter of a blinding attack signal directed at the receiver, and wherein at least a portion of light emitted from the light emitter is detectable by a single photon detector of the receiver;

switching the light emitter off during a normal operation mode of the single photon detector;

measuring a first number of detection events registered in the single photon detector in a first time period, T1, with the light emitter switched on; and

identifying the occurrence of the blinding attack based on the first number of detection invents.

2. The method of claim 1, wherein T1 is randomly initiated.

3. The method of claim 1, wherein T1 is contiguous in time, or distributed over one or more time intervals.

4. The method of claim 1, comprising setting a power of the light emitter to a first level such that, when the light emitter is switched on, the single photon detector is in a first operation mode in which only a flag state detection event caused by the light emitter being turned on and fake state detection events as part of the blinding attack are detectable in T1.

5. The method of claim 4, wherein the occurrence of the blinding attack is identified if at least one fake state detection event is registered in the single photon detector in T1 and/or wherein the occurrence of the blinding attack is identified if no flag state detection event is registered in the single photon detector in T1.

6. The method of claim 1, comprising setting a power of the light emitter to a second level such that, when the light emitter is switched on, the single photon detector is in a second operation mode in which single photon detection events, detection events caused by the light emitter and fake detection events as part of the blinding attack are detectable in T1.

7. The method of claim 6, wherein identifying the occurrence of the blinding attack comprises measuring a second number of detection events registered in the single photon detector in a second time period, T2, with the light emitter switched off, and identifying the occurrence of the blinding attack based on a comparison of the first and second numbers of detection events.

8. The method of claim 7, wherein the occurrence of the blinding attack is identified if the rate of detection events in T1 is not larger, by a statistically significant difference, than the rate of detection events in T2.

9. The method of claim 6, wherein T2 is randomly initiated, and/or wherein T2 is contiguous in time, or distributed over one or more time intervals, and/or wherein T1 and T2 have the same length.

10. The method of claim 1, comprising setting a power of the light emitter to a third level such that, when the light emitter is switched on for a single pulse time interval as T1, the single photon detector is in a third operation mode in which only a single detection event caused by the light emitter is detectable with approximately unit probability during the single pulse time interval.

11. The method of claim 10, wherein the occurrence of the blinding attack is identified if no detection event caused by the light emitter is registered in the pulse time interval.

12. A receiver for a quantum cryptography system, the receiver comprising:

a single photon detector;

a light emitter, wherein the light emitter is different from a transmitter of a quantum cryptography signal to be received by the receiver, wherein the light emitter is different from a transmitter of a blinding attack signal directed at the receiver, and wherein at least a portion of light emitted from the light emitter is detectable by the single photon detector;

wherein the light emitter is configured to be off during a normal operation mode of the single photon detector; and

a processor configured to measure a first number of detection events registered in the single photon detector in a first time period, T1, with the light emitter switched on and to identify the occurrence of the blinding attack based on the first number of detection invents.

13. The receiver of claim 12, wherein T1 is randomly initiated.

14. The receiver of claim 12, wherein T1 is contiguous in time, or distributed over one or more time intervals.

15. The receiver of claim 12, wherein a power of the light emitter is set to a first level such that, when the light emitter is switched on, the single photon detector is in a first operation mode in which only a flag state detection event caused by the light emitter being turned on and fake state detection events as part of the blinding attack are detectable in T1.

16. The receiver of claim 15, wherein the processor is configured to identify the occurrence of the blinding attack if at least one fake state detection event is registered in the single photon detector in T1 and/or wherein the processor is configured to identify the occurrence of the blinding attack if no flag state detection event is registered in the single photon detector in T1.

17. The receiver of claim 12, wherein a power of the light emitter is set to a second level such that, when the light emitter is switched on, the single photon detector is in a second operation mode in which single photon detection events, detection events caused by the light emitter and fake detection events as part of the blinding attack are detectable in T1.

18. The receiver of claim 12, wherein identifying the occurrence of the blinding attack comprises measuring a second number of detection events registered in the single photon detector in a second time period, T2, with the light emitter switched off, and the processor is configured to identify the occurrence of the blinding attack based on a comparison of the first and second numbers of detection events.

19. The receiver of claim 18, wherein the processor is configured to identify the occurrence of the blinding attack if the rate of detection events in T1 is not larger, by a statistically significant difference, than the rate of detection events in T2.

20. The receiver of claim 12, wherein T2 is randomly initiated and/or wherein T2 is contiguous in time, or distributed over one or more time intervals and/or wherein T1 and T2 have the same length.

21. The receiver of claim 12, wherein a power of the light emitter is set to a third level such that, when the light emitter is switched on for a single pulse time interval as T1, the single photon detector is in a third operation mode in which only a single detection event caused by the light emitter is detectable with approximately unit probability during the single pulse time interval.

22. The method of claim 21, wherein the processor is configured to identify the occurrence of the blinding attack if no detection event caused by the light emitter is registered in the pulse time interval.