Appendix 05
QKD Hardware Components

1 Photon sources

There are three different classes of devices for photon sources.

1.1 Damped laser

This type is most commonly found in mature devices. In the BB84 protocol, time windows are defined that are just short enough for the receiver, Bob, to reliably distinguish them with his measuring instruments. Alice attenuates the laser's light with a filter to such an extent that it emits a photon only in a fraction of the defined time windows. Most time windows remain dark. Typically, the filter and the length of the time slots are adjusted so that approximately 20% to 50% of all time slots contain photons. With this type of device, Alice does not know which time slots contain photons. She performs her encoding operations in all slots, but Bob receives measurable photons only in the filled time slots.

The reason for this strategy is as follows:

The light from a laser consists of photons, which in this context can be thought of as particles of light. A filter absorbs most of them and lets only a few through. Which photon gets through is purely random, so the photons do not exit the device at fixed time intervals. Instead, the time intervals are purely random. The temporal distribution can be described by a Poisson distribution. If the number of emitted photons is approximately equal to the number of time slots, then there will be many time slots in which the laser emits two or more photons. These multi-photon pulses are not a problem for the actual key exchange, but they give the eavesdropper Eve the opportunity to carry out a photon-splitting attack, which is described in more

detail below. The fewer photons the laser emits per second, the less frequently dangerous multi-photon pulses occur. However, they cannot be completely avoided.

Low-power lasers are technically very mature, robust, low-maintenance, and relatively inexpensive compared to other components (starting at around 600 euros). The pulse rate (number of time slots per second) for this type of device is typically in the range of 1 billion pulses per second. Because only a certain fraction of these contain photons, approximately 200 million photons per second are typically emitted.

1.2 Heralded photon sources

A special crystal is bombarded with high-energy photons. Some of these photons are converted within the crystal into pairs of two lower-energy photons. Alice uses one of the two photons in the pair in the same way as with the attenuated laser. She encodes it and sends it to Bob. Alice detects the other photon in the pair using a detector. This detected photon thus acts as a herald, signaling the arrival of the transmitted photon. With this type of device, Alice therefore knows in which time windows photons are on their way to Bob. But more importantly, this method results in much fewer multi-photon pulses.

Here, too, there are many empty time slots, and the photons arrive at Bob's end at just as irregular intervals as with the attenuated laser. However, in currently available devices, the rate is only about 2 to 5 million photons per second.

Although the cost of operating and maintaining these devices is slightly higher than that of attenuated lasers, the reason heralded photon sources are rarely used is not only the lower photon rate but also the higher purchase price. Such devices start at around 25,000 euros.

1.3 Deterministic single-photon sources

Within this class, there are devices based on different physical principles (quantum dots, color centers, ion traps, ...), but they all share the common feature that an externally controlled clock allows the generation of a photon stream at constant time intervals, and that the proportion of multi-photon pulses is very low. Thus, a very high-quality photon stream is obtained.

However, these devices are very expensive to operate because they require a cryostat that must cool the photon source to temperatures just above absolute zero. A complete system, including the cryostat, costs 100,000 euros or more to purchase.

Typically, between 50 and 200 million photons are emitted per second. However, rates of up to 1 billion have also been reported.

1.4 Overview of Photon Sources

The following table provides a rough and simplified overview of photon sources for the BB84 protocol and related protocols (Prepare-and-Measure, Discrete Variable)

Device Type	Photons per second	Multi-pulse?	Operator	Purchase (in €)
attenuated laser	200,000,000	yes	inexpensive	600
emitted photons	4,000,000	yes	inexpensive	25,000
deterministic sources	200,000,000	no	expensive	100,000

2 Single-photon detectors

2.1 Role of single-photon detection in QKD systems

Single-photon detectors are the central receiving component in discrete QKD (DV-QKD) and entanglement-based approaches. In these protocols, information is encoded in the states of individual photons (e.g., polarization, phase, or time bins); each recorded event is directly incorporated into the raw key generation. The detector thus determines both the usable event rate and the noise and error components, which must later be compensated for by error correction and privacy amplification.

This role becomes particularly evident in field operation: With high channel losses, the useful signal rate decreases, while dark counts and many background contributions remain approximately constant. Consequently, detector noise, time resolution, and saturation behavior become the dominant factors for range, stability, and key rate.

2.2 Device Types and Applications

In practice, QKD-compatible single-photon detectors are primarily classified according to the suitable wavelength range and required operational effort. For fiber-optic QKD, the telecom band (1310/1550 nm) is decisive, while free-space links and many entanglement-based setups are frequently operated in the visible or near-infrared range (e.g., around 810–850 nm).

Semiconductor-based **avalanche detectors** (avalanche photodiodes) operating in Geiger mode (SPADs, single-photon avalanche diodes) are the most common type. A single photon can trigger an avalanche, which is read out as a digital "click." Silicon SPADs are particularly suitable for visible and near-infrared wavelengths up to about 900–1000 nm, making them an obvious choice for free-space QKD, testbeds, and many entanglement-based setups. They are often available as compact modules with moderate (often thermoelectric) cooling and are therefore relatively easy to integrate.

InGaAs/InP SPADs are used for telecommunications wavelengths. They are practically the standard solution for fiber-based DV-QKD, but they come with typical trade-offs, particularly regarding afterglow and the resulting dead times. In "gated" operation, the detector is active only within defined time windows; this can reduce the effective dark count per active window and make afterpulsing more manageable, but requires a precise timing/clocking architecture. In "free-running" operation, events are registered asynchronously; this simplifies certain architectures but requires careful management of dead time and afterpulsing.

Superconducting detectors, particularly **SNSPDs (Superconducting Nanowire Single-Photon Detectors)**, are considered a high-performance alternative. In many system designs, they combine high detection efficiency with very low dark count rates, low dead time, and good time resolution. This makes them attractive for high loss budgets and long distances, as well as for scenarios with very low photon counts. The main challenge lies in operation at cryogenic temperatures (typically a few kelvins), including the cryosystem and operational peripherals.

Transition-edge sensors (TES) can operate with photon-count resolution and achieve very high efficiencies, but they require millikelvin temperatures and are therefore primarily relevant in research and specialized applications.

Detector arrays (multi-channel SPAD or SNSPD arrays) enable parallelization and higher overall count rates, but increase the effort required for calibration, channel balancing, and monitoring.

Upconversion concepts nonlinearly convert photons from the telecom band to shorter wavelengths and then detect them using silicon detectors. Such architectures can combine individual advantages but increase system complexity (pump source,

nonlinear stage, additional filters) and introduce additional noise paths that must be transparently evaluated within QKD budgets.

The number of channels must also be considered for system planning: polarization-based protocols typically require multiple detectors, and time-bin/interference receivers require at least two channels. The choice of detector technology therefore directly affects the cost, space requirements, spare parts strategy, and maintenance effort of the entire system.

2.3 Key Performance Indicators and Practical Trade-offs

Detector selection is rarely based on a single peak value; what matters is the interplay of key metrics under the specific link and protocol conditions. Consistent measurement conditions are essential for comparability, particularly wavelength, temperature, time window/gate width, defined dead time, and the definition of dark count (e.g., whether post-pulse components are included).

Detection efficiency (PDE/SDE): Higher efficiency increases the raw detection rate and improves distance margins because more valid events are generated with the same loss budget. For QKD, system efficiency is crucial, i.e., including coupling losses (fiber connection, free-space optics), filters, polarization management (if applicable), and readout electronics.

Dark count rate (DCR) and background: Dark counts are clicks without a useful photon. They increase the error rate (QBER) and become particularly critical at high loss levels because they become more dominant relative to the useful signal rate. In free-space operation, ambient light and atmospheric scattering are additional factors. Here, the detector, optical filtering (spectral and spatial), and temporal windowing must be designed in conjunction.

Afterpulsing: In InGaAs SPADs in particular, trap effects lead to correlated afterpulses following a true event. In practice, hold-off periods and/or fast gating are therefore used. This reduces the maximum usable count rate and influences which clock rates, pulse widths, and average photon counts are appropriate for the overall system.

Dead time, maximum count rate, and saturation: After a click, the detector requires a recovery time. At high event rates, this can lead to saturation and statistical distortions. Short dead times are advantageous for high-rate QKD; however, in SPAD systems, the dead time is often intentionally extended to suppress afterpulsing. For system design, therefore, not only the nominal dead time but also the behavior under realistic event rates must be evaluated.

Timing jitter: Timing jitter determines how narrow detection windows can be set. Smaller windows reduce dark count and background contributions per bit, but

require stable synchronization and low drift in optics and electronics. Time-bin and interference protocols are particularly sensitive to this.

Operational Stability and Monitoring: Temperature dependencies affect efficiency, dark count rate, and afterpulsing. Equally relevant are polarization dependencies, mechanical stability of the coupling, and robust monitoring (count rates, temperature, optical input power) to detect deviations early and perform calibrations in a controlled manner.

Safety Relevance: Single-photon detectors are among the components of QKD systems where physical non-idealities and operational constraints can have a direct influence on the resulting detection statistics. The technical literature describes, among other things, effects such as saturation, time-dependent changes in detection efficiency, unwanted triggering mechanisms, and the deliberate exploitation of specific operating modes. Such effects can manifest themselves in altered count rates, temporal correlations, or systematic distortions of the measurement data and are closely linked to parameters such as input power, time windowing, dead time, temperature control, and readout logic.

2.4 Cost and Integration Aspects

Costs and integration effort vary greatly depending on technology, number of channels, and operational infrastructure.

- **Semiconductor-based Si-SPAD modules** often cost in the range of a few **thousand to a few ten thousand euros** per channel and can be integrated compactly (including moderate cooling).
- **InGaAs SPAD solutions** for telecom wavelengths are typically more expensive because cooling, quench/gating electronics, and stability requirements are more demanding; in practice, a **five-figure amount** per channel is often to be expected, especially since multiple channels may be required.
- **SNSPD systems** are generally complete packages consisting of a detector head, multi-channel readout, and cryogenic system. The investment often ranges **from the high five-figure to six-figure range**; additionally, operating costs (power, service), space requirements, and maintenance processes must be taken into account.

A pragmatic selection heuristic applies: For short to medium distances and moderate clock rates, robust semiconductor detectors are often sufficient. For very high loss budgets, strict QBER specifications, or maximum range, the trade-off shifts in favor of superconducting detection, provided that the infrastructure and operational concept realistically accommodate the cryogenic technology.