



# Quantum Key Distribution Technology White Paper

January 2021

The KEEQuant Technology White Paper serves as an introduction to the topic of quantum key distribution (QKD).

**Quantum key distribution is a paradigm shifting technology** that transforms the landscape of secure communication. It enables long term security by leveraging quantum physics and information theory to prove that the exchanged secret keys can be trusted. This can not be achieved with any other type of technology today.

In the following document, we highlight how QKD relates to classical cryptography, how it works and is typically implemented, what environment it lives in and how it can be scaled and miniaturized to make it commercially attractive up to mass market roll-out.

*KEEQuant GmbH*  
*info@keequant.com*

## Table of contents

1	How Cryptography works Today
2	The Weak Link
3	The Quantum Computing Threat and why to worry now
4	Quantum Key Distribution – the Solution
5	A software alternative: Post-Quantum Cryptography
6	A typical QKD System
7 – 8	QKD Technology Options
9	The Environment of a QKD System
10 – 11	Miniaturization and Scalability

## Why care?

Cryptography is an important pillar of the information age, and for our civilization as a whole.

It secures nearly all **modern communication** – ranging from highly critical fields such as the exchange of classified government documents, to seemingly benign aspects as the confidentiality of a personal financial transaction.

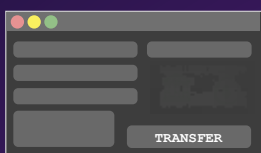
All **critical infrastructure**, the underpinning of our society, is protected by cryptography. This includes banks and healthcare, the telecommunication backbone network, governmental services, navigation services, industrial internet, data centers, and the energy grid.

**Without an intact cryptographic infrastructure, our world would go off the rails.**

## An example from everyday life

Let's illustrate how cryptography works today, when you use online-banking (because you can't wait to finally invest in our endeavour after reading this document):

### User Browser



Encrypt data with shared key

Decrypt confirmation using shared key

Show success

Request **authentication**  
*Is receiver truly the Bank?*

Bank uses RSA to authenticate

Establish **shared key** using  
**asymmetric cryptography**, e.g. ECDH

Browser sends transaction data  
**symmetrically encrypted** with AES

### Bank Server



Decrypt data using shared key

Book money  
Transfer

Bank confirms transaction data **integrity**  
using hash functions, e.g. SHA384

This example emphasizes that there are three major aspects to cryptography, needed to ensure secure communication:

**Authenticity**


*the message originated from the expected party*

**Confidentiality/Encryption**

*the message can only be read by authorized parties*

**Integrity**

*the message content wasn't changed during transmission*



**Where  
is the  
weak  
link?**

Let's take a closer look at the Confidentiality/Encryption aspect: Ideally, we would want to use symmetric encryption from the very beginning of a communication, as it can be made resilient even against the attacks of a quantum computer. However, symmetric encryption needs a **shared key**. That is a key which is identical on both parties' sides, it's what the word *symmetric* actually refers to. But how would the two parties agree on such a key, when they haven't established a secure channel yet in the first place? Here, **asymmetric cryptography** comes into play, to establish such an initial shared key.

**This step is the weak link.**

## A deeper dive into why today's cryptography is at risk

Why is today's cryptography assumed secure?

Asymmetric cryptography, also known as public-key cryptography, is based on mathematical *one-way problems*: The calculation is easy to be performed one way, but it's very hard to back-calculate the input if given only the output.

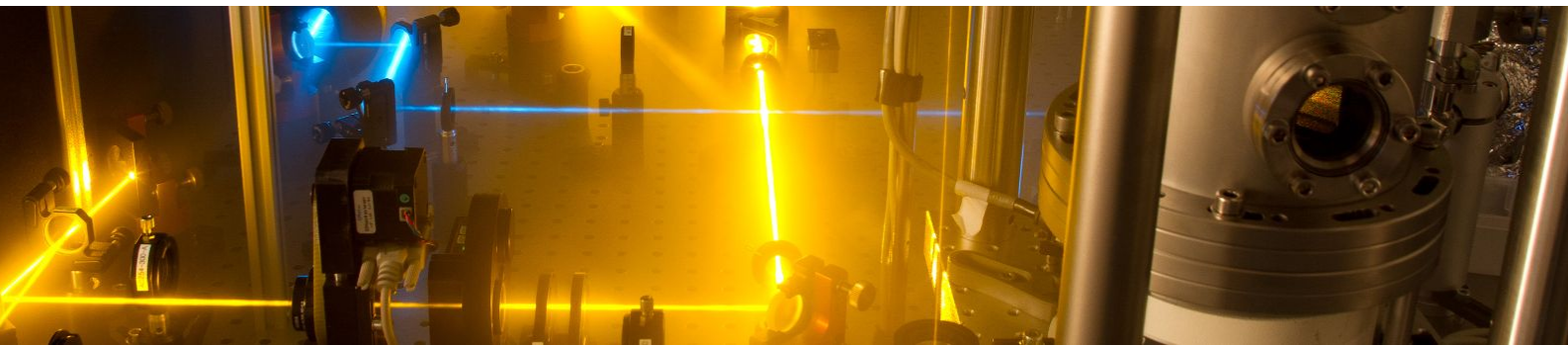
A simple example is multiplication and factorization. Asking what 11 times 13 is, will give an answer quickly. But finding the prime constituents of 143 in your head is going to take some time. Likewise, computers perform multiplication very quickly, while the time required to perform prime factorization scales exponentially with the size of the number – it is a very hard computational problem.

In Algorithms like *Elliptic-Curve Diffie-Hellman (ECDH)* the malicious eavesdropper has to perform the hard calculation in order to break the encryption chain. The legitimate communication partners however hold a secret, which the eavesdropper does not have access to. This allows them to solve the mathematically hard problem, giving them an advantage over the eavesdropper and allowing them to securely establish a key.

What if a part of today's crypto breaks?

All technologies combined provide very high security. But if one of the links in the chain breaks, this security is compromised. There exists such a risk for the RSA key exchange protocol that uses the hard problem of factoring a large number into its prime constituents. It becomes insecure when a way has been found and implemented that allows to factor large numbers in feasible time scales.

Peter Shor invented an algorithm (*Shor's algorithm*) that, run on a quantum computer, does exactly that. It factors large numbers efficiently into their prime constituents.



## Why worry now?

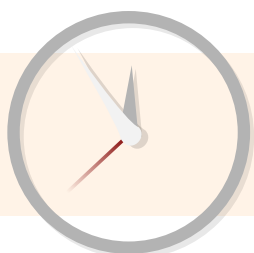
[1] *Status of quantum computer development:* [www.bsi.bund.de/DE/Publikationen/Studien/Quantencomputer/quantencomputer\\_node.html](http://www.bsi.bund.de/DE/Publikationen/Studien/Quantencomputer/quantencomputer_node.html), Jan 2021

A **quantum computer** with the required computational power does not yet exist — at least not publicly known. *For a state of the art analysis, we recommend a study performed by the German Federal Office for Information Security (BSI) [1].*

But chances are, it will scale to relevant computational power over the course of the next decade. If the shelf life of the information we want to protect is sufficiently long, all encrypted data can be recorded in the meantime and decrypted later. This means that a solution has to be developed, tested, certified, and deployed long before a quantum computer matures to full capacity. This is called a **store now, decrypt later** attack.

Additionally, well funded state actors store the bulk of the internet traffic in purposely constructed, very large data centers. This allows for a later decryption of the data using supercomputers, once a smart mathematician figures out a way to crack the underlying mathematical problems. If the mathematician acts under confidentiality, the cryptography chain is broken without anyone besides the state actor knowing.

**We are facing a threat to society, which will become real in the next coming years. The time to prepare is now, and Quantum Key Distribution is the solution.**

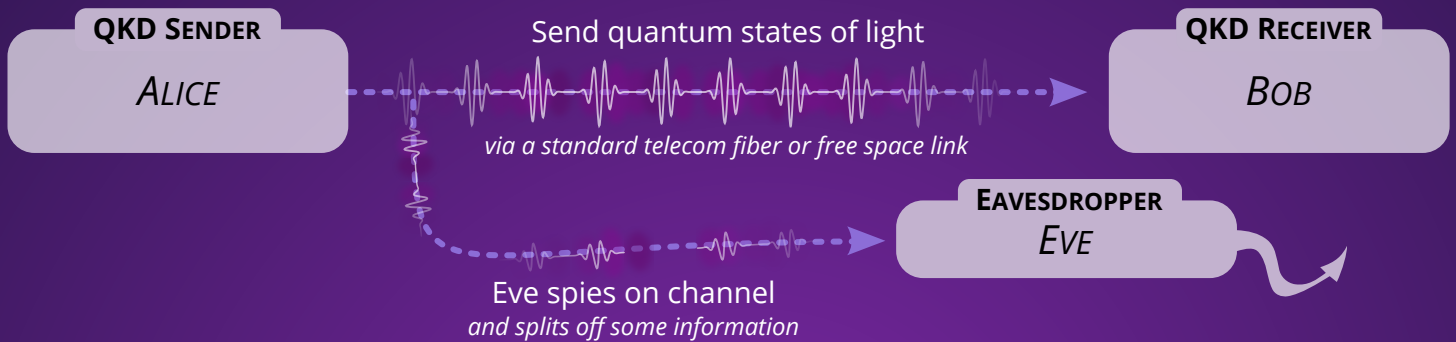


**Quantum Key Distribution (QKD)** focuses on the **initial key exchange** in the chain of conventional cryptography.

Using resources only available through quantum physics brings a unique advantage: **its security can be proven using information theory**. This constitutes a novelty in cryptography and a paradigm shift in data security.

*In the following, we show the typical steps of (CV-)QKD.*

## Step I Quantum State Exchange



## Step II Calculate Amount of Mutual Information



a)

Alice and Bob have a **public discussion** about a **randomly chosen subset** of the exchanged states, and what Bob measured

b)

The QKD security proof now allows them to **calculate the amount of information** in their data, that is mathematically guaranteed to not be available to Eve.

c)

If the projected resulting key size is zero, the loss in the channel is too large. This might, but needn't be due to Eve spying. **If the projected size is greater zero, we finally make the key...**

## Step III Distilling the Secret Key



**The QKD-Postprocessing error correction** leads Alice and Bob to hold identical keys on both sides.

**Privacy amplification** has eliminated any information from the key that Eve might have picked up, to a desired arbitrarily small residual amount.

## Step IV Hand over the secure key to encryptors with confidence.

What if?

**What if currently deployed crypto software could be adapted to be more resilient or even immune to the threat of the quantum computer?** This is precisely the idea behind what is called *post-quantum cryptography* (PQC) or *quantum-resistant algorithms* (QRA).

Why should PQC be any more secure than today's deployed crypto?

**PQC is once again based on mathematical one-way problems** that are believed to be secure against all of today's known quantum computer algorithms. While RSA key exchange and *Elliptic-Curve Diffie-Hellman* (ECDH) key exchange are based on prime factorization and discrete logarithms, new PQC methods, like lattice-based cryptography, are based on the learning with errors/finding shortest vector problem.

Can PQC be broken?

Quantum computer algorithm development has just started, as massive research and development efforts are launched all around the world in this emerging field. It is therefore impossible to predict whether PQC will actually remain secure – the next quantum algorithm discovery might as well be just around the corner, breaking PQC or its implementations. Once again, the mathematician working under confidentiality for his employer might keep an already existing attack undisclosed, so for all we know, PQC might already be jeopardized. **PQC shares this weakness with its cryptographic predecessors, it has no fundamental long term safeguard.**

Why use PQC if quantum computers might break it again?

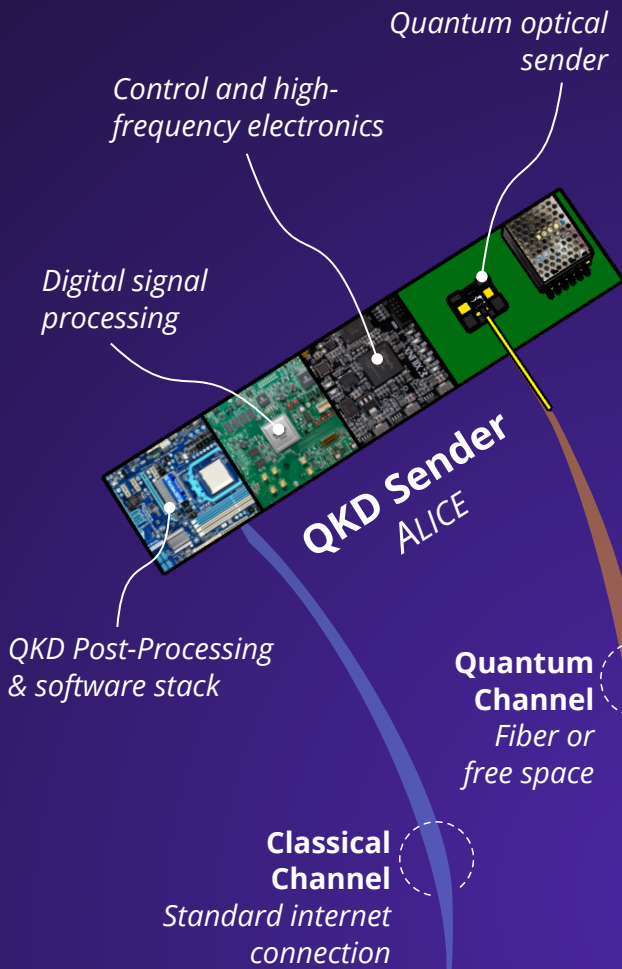
No one knows if and when quantum computers break PQC. It is nevertheless reasonable to develop software-based solutions that *might* be broken, to replace the currently deployed technologies that *certainly will* be broken. In some cases, such software-based solutions may be easier to deploy than QKD, which requires dedicated hardware and quantum-suitable networks.

How will PQC and QKD work together in practice?

The software-based PQC may be a good choice for consumer-grade, low-security or low shelf-life cryptographic applications due to its lower deployment cost. QKD, on the other hand, is at first aimed at high-security, critical infrastructure, and long shelf-life information and may later, when costs decrease, be adapted to consumer needs.

Importantly, during a denial of service attack or if an implementation loophole of either technology is discovered, secure keys cannot be exchanged. **We thus envision using QKD and PQC as mutual complements**, acting as a fallback for each other. Practically, this can be achieved through mathematical key derivation functions and may be relevant for high security applications.

*On the following page, we showcase a typical QKD system.*



## Quantum Optical Sender (Alice)

The sender unit needs a light source, and some form of optical modulator, to encode the quantum states. Commonly an optical attenuator is used to bring light intensities down to the quantum level.

## Digital Signal Processing (DSP)

The QKD DSP is used both on the sender and receiver sides. First, it ensures the low-level light modulation envelope is optimized for quantum state transfer. Upon reception, the acquired data points are corrected for channel distortion such as phase fluctuations due to effects in the fiber.

## Control and High Frequency Electronics

On the hardware level, both sender and receiver require analog-to-digital conversion and vice-versa, as well as signal processing electronics. Furthermore, some form of central processing unit takes care of system control and automation.

## Software Stack

A software with user interface controls and monitors the system and its components.

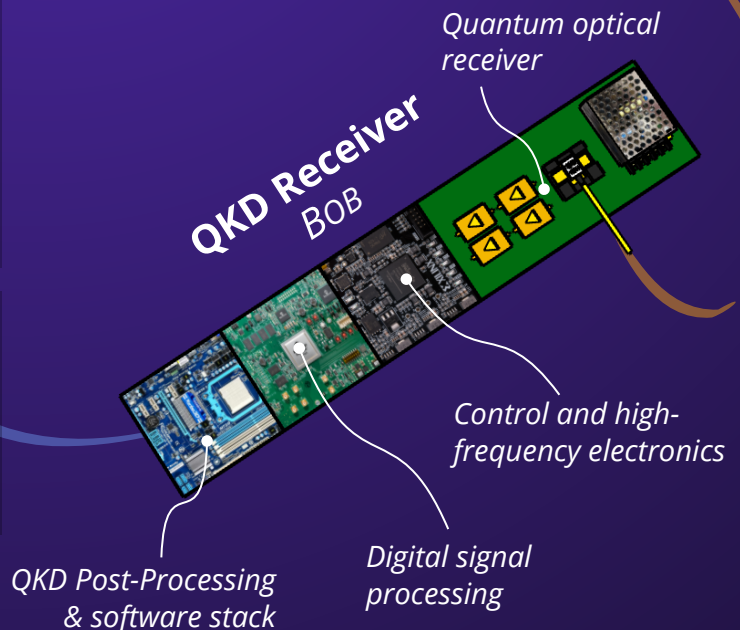
## QKD Post-Processing (PP)

The QKD-PP is used to detect the eavesdropper from the raw measurement data, throw away the data if necessary and to correct the data for errors and privacy, so a secure key is generated.

## Quantum Optical Receiver (Bob)

On the receiver side, some kind of detection unit is necessary to convert the light into electrical signals that are further processed.

*Shown system pictures are exemplary.*





What options are there to implement the sender?

Of course there are several choices for hardware implementation of a typical QKD system. In the following, we outline these choices and give an overview of their advantages and drawbacks.

The main choice is which light source shall be used. It can either be a **single photon source**, an **attenuated laser**, or an **entanglement source**.

Single photon sources currently exist mainly for academic purposes and are not viable technology choices because of their size and cost. Future developments may make this more commercially attractive. Their advantages for QKD are however limited at this point, since the key rate improvement coming from the usage of single photons does not constitute a significant improvement.

Entanglement sources have a very similar technological state as single photon sources, but tend to be slightly cheaper and can be made a bit smaller. The main advantage is that no optical modulation is required, since the quantum information is intrinsic to the entangled photon pair that is emitted.

Lasers are a highly developed technology and thus cheap, small and may be attenuated easily. They constitute the best option for QKD systems at this moment in time – both from a technological as well as an economical viewpoint. **Our systems use commercial off-the-shelf telecom lasers in the sender.**

What options are there to implement the receiver?

One of the main distinctions for the receiver lies in the choice of the detector. One may either use a **single photon detector** or a **coherent detector**. This choice is also commonly reflected in two distinct protocol families: **Discrete-variable (DV-)QKD** and **continuous-variable (CV-)QKD**.

The term *discrete-variable* acknowledges the fact that a single photon detector may either trigger or not trigger in a given time window. It leads to a discrete number of measurement outcomes (1 or 0 for each detector).

*Continuous-variable* refers to the fact that in a coherent detector, the electric field of light is measured, which may take any continuous value of amplitude and phase.

Single photon detectors typically come in either of two forms: the *avalanche photodiode* (APD), or the *superconducting single photon detector* (SNSPD).

What options are there to implement the receiver? (continued...)

SNSPDs have better photon-to-electron conversion efficiencies and have fewer false detection events (*dark counts*). Their disadvantage is that they require liquid helium cooling and are thus as big as a room-height rack cabinet and have costs of the order of 100k€. In consequence they are attractive only for scenarios where the receiver is not a significant factor in the overall system architecture. This may be the case for satellite ground stations.

APDs have smaller form factors than SNSPDs, cost less, and do not require such drastic cooling, which makes them commercially much more attractive. However, they are also less performant in terms of dark counts and photon conversion efficiency. There are some ongoing scientific efforts to realize APDs on a photonic integrated circuit, thus improving the level of integration into a photonic-chip based system. However, this technology and its field applicability have yet to be shown.

Coherent detection relies on the interference of the weak quantum signals coming from the fiber or free space channel with what is called a local oscillator – essentially a bright laser that is part of the receiver. Also for electro-optical conversion, PIN diodes are used. The advantages of coherent detection are manifold: high electrical bandwidths, high conversion efficiencies, very low cost, implementable on photonic integrated circuits, omnipresence in today's telecommunication networks. The only downside of coherent detection seems to be that single photon detection may have some fundamental advantages in terms of achieving higher key rates or higher distances. Currently these do not outweigh all the advantages in techno-economic considerations and therefore make coherent detection favourable for QKD implementations.

Of course a QKD system is only one of many devices in a network. On the following page, we therefore give an overview of the environment a QKD system lives in.

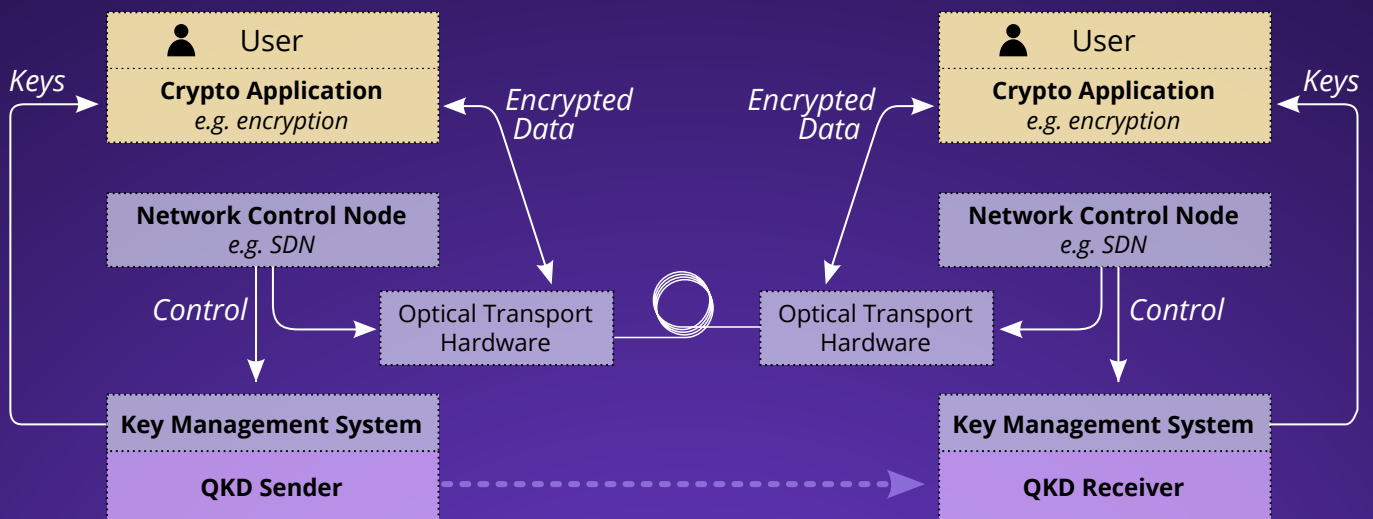
## Interfaces to other systems: **Key Management**

QKD systems produce keys. In order for an architecture with multiple parties to effectively use quantum keys, the key exchange has to be orchestrated. To allow this, the QKD system typically hands its keys over to a *key management system* (KMS) that handles the lifetime and secrecy of the keys. By synchronizing with other KMS at distant locations, a user application may retrieve matching keys on either side, whenever a cryptographic task is to be performed.

The archetypal cryptographic task is of course encryption. For example, a hardware encryptor module may ask for a key that is then used to securely transport data. The KMS instances on both sides then ensure the receiving end uses the appropriate key for decryption.

## Software-defined networking

Another interface is directed towards optical networking and management hardware. For example, software-defined networking hardware (SDN) controls routers to optimally use the fiber infrastructure, depending on the current network load. SDN systems may also be essential for uninterrupted service in the event of an outage in one of the links, by rerouting traffic accordingly. Since QKD systems have different requirements than standard optical transport hardware, QKD systems have to be properly interfaced with network management entities (e.g. SDN) in order to guarantee seamless integration. We show a typical network setup for a QKD system in the schematic below and outline how QKD can be miniaturized and scaled on the following pages.



What is the state of the art?

Commercial QKD systems are typically able to cover link distances of up to 100 km with secret key rates of the order of a few kbit/s. The form factor and cost are typically a 19" rack mountable box and 100k€ for a sender and receiver pair.

Is there a path towards **miniature devices** and **scalable production**?

Most QKD systems nowadays utilize very generic commercial components, plugged together and operated with parameters suitable for QKD. As a consequence, most of the parts are larger and more costly than necessary. Obviously, these parts should be made smaller and cheaper. However, there is not always a clear path towards miniaturization of parts for every type of technology. Similarly, scalable production may depend on more than just technological factors. In the following we will analyze the different parts under the aspects of miniaturization and scalable production.

QKD control software

**Miniaturization:** Software controlling the QKD device easily runs on a microcontroller with sufficient performance to support smooth operation.

**Scalability:** Microcontrollers and FPGAs are not a limiting factor since they are available on the commercial mass market.

QKD post-processing software

**Miniaturization:** For the QKD post-processing software, heavy computational resources are currently required for CV-QKD, whereas DV-QKD is a bit better off, because the amount of data that needs to be computed is smaller. For both methods, an FPGA is probably the right tool to miniaturize and implement the post-processing steps in an efficient manner. Due to the higher amount of data, this will most likely be a tougher engineering challenge for CV-QKD.

**Scalability:** Microcontrollers and FPGAs are not a limiting factor since they are available on the commercial mass market.

QKD digital signal processing (DSP)

**Miniaturization:** For digital signal processing, ideally many techniques can be copied from classical telecommunication. These algorithms are commonly implemented on an application-specific integrated circuit (ASIC).

**Scalability:** The NRE costs for ASICs are high and typically some kind of de-risking investment is necessary to support ASIC development for markets which are not as big as for example the market for cell phones. Once the non-recurring engineering (NRE) cost has been expended, standard chip production techniques may be used for mass manufacturing and scalability is therefore possible.

QKD Module	EU27 State of the Art	Desired
Control Software	Desktop Computer	Microcontroller
CV-QKD Post-Processing	Powerful Server	FPGA
Digital Signal Processing	Desktop Computer	Microcontroller/FPGA/ASIC
Control & High-Freq. Electronics	Test & Measurement Devices	PCBA with High-Volume ICs
Quantum Optical Unit	Individual Optical Components	Integrated Photonic Circuits

## High frequency electronics

**Miniaturization:** For the electronic control and the high frequency electronics, most likely COTS integrated circuit chips can be used but of course have to be employed and operated to function with QKD requirements.

**Scalability:** The ICs required for electronic control and high frequency electronics are available on the commercial mass market. We envision to reuse components that are otherwise employed in standard telecommunication technology. This way availability and volume production is guaranteed.

## QKD Photonic Integrated Circuits (PICs)

**Miniaturization:** The quantum optical unit is currently a set of discrete electro-optical components. The goal is to miniaturize everything onto a small photonic integrated circuit (PIC). These are readily available, just like one orders printed circuit boards today. Brokers like the *Jeppix consortium* offer access to PIC foundries, which accept photonic designs and subsequently manufacture a corresponding PIC.

**Scalability:** PICs pose the greatest challenge since these would be custom made for QKD needs. In principle PICs may require a complex set of chemical processing steps to manufacture with bonding and packaging potentially imposing limiting factors. We are confident, that as the standard telecommunication industry also needs to do this and is still able to provide the right amount of units, we will overcome these challenges.

Note that DV-QKD receiver PICs are currently very hard to create, since there is no proper way to integrate APDs into a receiver PIC. This highly favours CV-QKD for mass production.

## Conclusion

**In conclusion all essential elements for volume production of (CV-)QKD are either available today from the telecom mass-market, or can be enabled by de-risking investments into miniaturized components.**

Quantum Key Distribution  
Technology White Paper

Jan 2021

© *KEEQuant GmbH*  
*info@keequant.com*