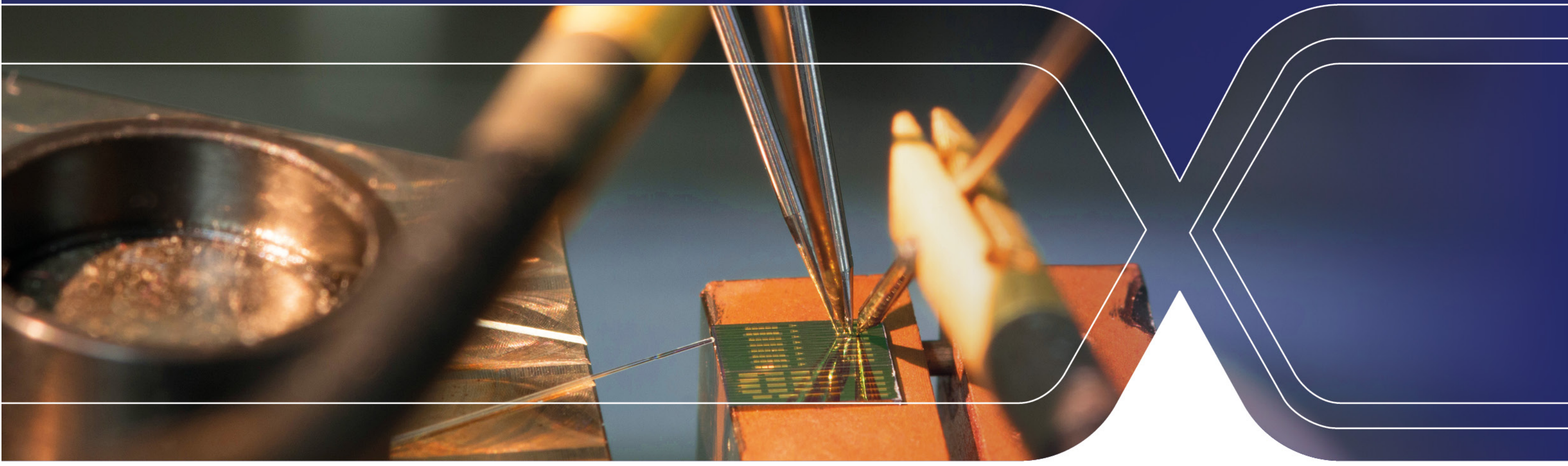
Application Note

PICs for Quantum Key Distribution

JePPIX
Platform for Photonic Integration



The Era of Digital Information

We spend an average of almost seven hours a day engaging with digital media[1], working (remotely) on a computer, streaming movies or series online, or consulting our doctor via email on our smartphones. Every day, we generate, send, and receive large amounts of digital information and, for the most part, hope that sensitive information is secure on these networks. Internet security currently relies on various encryption methods, providing varying degree of data security. Especially with the dawn of quantum computers, most classically employed encryption algorithms become vulnerable to interception and eavesdropping. Trustworthy data transit, storage and internet usage thus requires unbreakable security protocols beyond classical encryption.

Quantum Key Distribution

Quantum Key Distribution (QKD) was proposed by Bennett and Brassard in 1984, as a secure, post-quantum communication method. The QKD protocol uses principles based on quantum physics to exchange cryptographic keys only known between sender and receiver. Photons are the quantum particles used for information transmission over an optical network. Any attempt of interception or eavesdropping can be detected, because the observation of a quantum state will cause a perturbation, directly detectable in transmission errors[2]. Therefore, QKD can enable validated, secure communication channels, particularly important to security critical infrastructures, such as banks, governments, and the military.

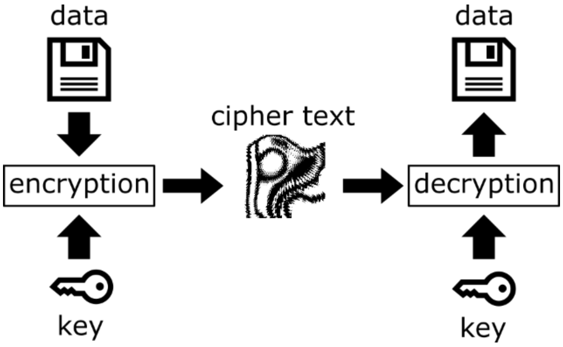


Figure 1: Basic principle of cryptography. Adapted from [3].

Cryptography

Cryptography is the process of encrypting information, such that its cipher text is unintelligible to any unauthorized person. Figure 1 illustrated this process. Information is encrypted on the sender's side with a secret key to obtain the cipher text. The cipher text is sent to the receiver, who decrypts the text with the key. This data transfer only remains safe, if the key is only in the possession of authorized personnel[3].

[1] https://www.forbes.com/sites/johnkoetsier/2020/09/26/global-online-content-consumption-doubled-in-2020/

[2] https://www.idquantique.com/quantum-safe-security/overview/quantum-key-distribution/

[3] https://marketing.idquantique.com/acton/attachment/11868/f-020d/1/-/-/-/-/Understanding%20Quantum%20Cryptography_White%20Paper.pdf

InP Photonic Integrated Circuits (PICs)

Optical chips or PICs can contain tens to hundreds of optical components. While electronic integrated circuits (EICs) consist of transistors, capacitors, and resistors, a PIC consists of, for example, lasers, modulators, photodetectors, and filters, all integrated on a single substrate. Several application fields, such as data- and telecom, sensing, and lidar are already using or are considering the use of PICs for their products. This PIC technology is accessible to users without a cleanroom, through so-called multi-project wafer runs and open access foundries. InP based technology is commercially available through SMART Photonics and Fraunhofer Heinrich-Hertz-Institut. Access is individually coordinated by JePPIX.

Key Distribution

For decryption of the cipher text, the sender and receiver need to be in possession of the key. In the Public Key Cryptography protocol, the receiver would send a public key (certified by a trusted partner) to the sender. This very practical solution if prone to vulnerability due to technological advances and mathematical progress: more processing power or new algorithms might crack the encoded key faster than expected. QKD solves the key distribution challenge, by ensuring absolute security of the cryptographic key exchange, based on the detection of the perturbation any observation causes on a quantum state.

QKD Protocols

Various QDK protocols have emerged, generally using the quantum properties of photons: polarization or phase. These protocols can be broadly classified into three principals:

1) Prepare and measure protocol

The sender transmits a single photon randomly in one of a pair of bases, using either polarization of phase of the photons. The receiver randomly selects their measurement base, allowing detection of any eavesdropper when comparing the measurement information with the sender.

2) Entanglement-based protocol

This protocol used entangled photons, which are sent to two different receivers. Each receiver detects in a randomly chosen base. Comparing the measured correlation allows eavesdropper detection.

3) Continuous-variable QKD

This QKD protocol uses modulation of a continuously variable random value on top of both optical quadratures of the signal from a coherent light source. The receiver choses a random quadrature for his homodyne detection scheme and by comparing the measurement information with the sender, eavesdroppers can be detected.

Photonic integration circuits (PICs) are emerging as a potential key technology for highly integrated QKD hardware solutions[4]. Especially Indium Phosphide-based PICs offer many of the required components for integration of QKD senders or receivers, given this platform offers integration of narrow-linewidth lasers, coherent receivers and polarization splitters. Development of quantum communication technologies and deployment of QDK protocols into the optical telecommunication network infrastructure is driven by research institutions and commercial companies alike. European projects, e.g. CiViQ[5], have been established to focuses on cost-efficient, high-integration and high-performance continuous-variable QDK. Comercial solutions are already on the market, offered by, e.g., ID Quantique, Toshiba, QuintessenceLabs and MagiQ Technologies Inc.

Discuss your application with us

If you are interested in knowing more about the capabilities and use of InP PIC technology for QKD, contact JePPIX. The JePPIX Pilot Line[6] provides low entrance-threshold to mature-manufacturing.

[4] https://www.vlcphotonics.com/2020/08/27/a-novel-integrated-optical-transmitter-for-quantum-communications/

[5] www.civiquantum.eu

[6] http://www.jeppix.eu/pilotline