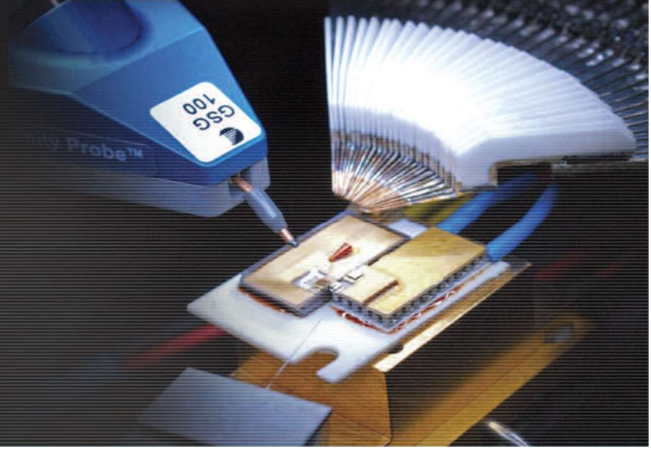


Photonic Integrated Circuits for Quantum Communications

The current global Internet relies for its security on encryption algorithms which are based upon mathematical complexity. Examples of this include factoring large prime numbers (RSA) and the discrete logarithms (Diffie-Hellman), both of which are impossible to break with current classical computers in a reasonable timescale. This could change however, with the predicted arrival of the quantum computer in the next decade or two. Quantum computers which are configured to use appropriate algorithms, such as that by Peter Shor [1] will enable factorization to be achieved in polynomial, rather than exponential time – threatening the security of data in transit or stored in the Internet. Even more importantly long-lived sensitive data (such as medical records or oil and gas surveys) encrypted by current schemes will be at risk in the future – the traffic merely has to be captured today and kept until quantum computers are available. Mathematical methods to counter this risk are currently being studied [2], the so-called 'post-quantum' algorithms. There is no guarantee that a mathematical flaw will not be found in them in the future. There are solutions which rely on the principles of quantum mechanics and is fundamentally unbreakable if implemented correctly. Quantum Key Distribution (QKD) was proposed by Bennett and Brassard in 1984, (BB84) [3] swiftly followed by Ekert with entanglement based QKD (E91) [4]

Introduction to QKD

The implementation details of QKD are too complex to be described in an application note, however QKD systems can broadly be classified into three principal families.

Prepare and measure protocols such as BB84, within which a single photon is transmitted randomly in one of a pair of bases using properties such as polarization, or more commonly optical phase. These single photons are detected by a receiver which randomly chooses the basis of measurement.

After the measurements information about basis choice is exchanged between transmitter, Alice, and receiver, Bob, enabling a possible eavesdropper to be detected.

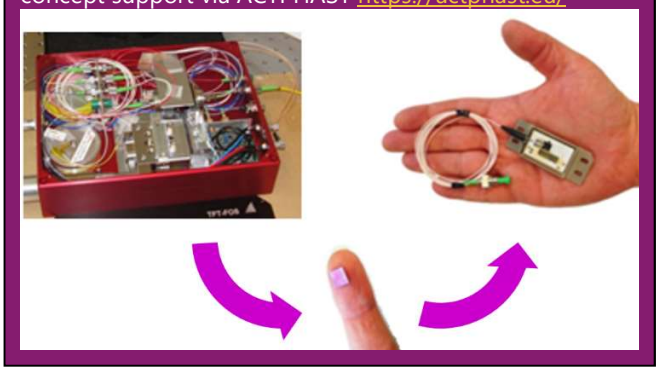
Entanglement based protocols such as E91 generates a pair of entangled photons and propagates them to two receivers. These receivers randomly and independently measure the photon in one of 3 bases. If the chosen bases are different it is possible to perform a test to determine whether there is an eavesdropper present. If not then the entangled photons detected with the same basis will be perfectly anti-correlated and thus able to produce secure keys.

Continuous variable QKD is very different from the discrete variable systems described briefly above CV-QKD uses a coherent light source and encodes a continuously variable random value on to both optical quadratures of the signal. Bob then performs homodyne

Photonic Integrated Circuits (PICs)

Also known as optical chips, PICs can contain tens to hundreds of optical components. While electronic ICs consist of transistors, capacitors and resistors, a PIC consists of, for example, lasers, modulators, waveguides, photodetectors and filters, all integrated on a single substrate. These PICs are nowadays extensively used commercially, mainly in datacom and telecom, becoming popular also in sensing.

PIC technology has now become accessible to users without a cleanroom, through so-called multi-project wafer runs and open foundries. Indium phosphide based technology is commercially available through SMART Photonics and Heinrich Hertz Institute. Silicon nitride technology is commercially available at LioniX Intl. Access is coordinated by the JePPIX platform: http://www.jeppix.eu/. Silicon photonics technology is also accessible through the ePIXfab Silicon photonics alliance platfom http://www.epixfab.eu/ - H2020 actions related are: i) specific to bio-photonics PIX4life https://pix4life.eu/ ii) generic packaging https://pixapp.eu/ and iii) proof-of-concept support via ACTPHAST https://actphast.eu/



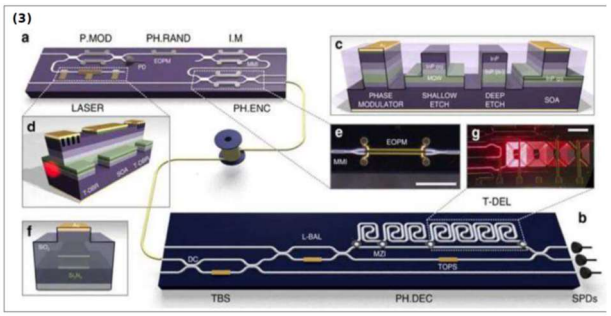


Figure 1. Integrated photonic devices for quantum key distribution [5].

measurements on a randomly chosen quadrature he compares the noise characteristics of the received signal with those of a vacuum channel to determine the presence of eavesdroppers.

Technological challenges

In general, photonic integration is extremely well suited to making transmitter or 'Alice' chips. There is currently much work being undertaken to decrease the loss in active PICs and be able to integrate the single photon detectors required for DV QKD or the high-power linear PIN diodes needed for CV-QKD.

PIC implementations

Sibson et al. [5] from Bristol have used the European integrated photonics platforms to produce both transmitter and receiver chips for a DV QKD system based upon optical phase. The transmitter, or 'Alice' chip was produced on the InP Oclaro platform and features both phase and intensity modulators based on reverse biased Stark effect phase shifters. It also uses an integrated DBR laser as the single wavelength light source. A very low loss substrate is unnecessary for an Alice chip, as the output must be at single photon levels, so waveguide loss is not an issue. The overall Alice PIC size was 6x2mm. In contrast the Bob chip is very sensitive to loss and was thus made using the passive TRIPLEX silicon oxy-nitride platform. The 2x32mm Bob used comprises several interferometers and tunable delay lines which are adjusted using thermo optic phase shifters. The passive nature of the TRIPLEX platform means that off chip single photon detectors are still required.

Silicon Photonics based integrated QKD systems are gaining popularity, particularly for 'Alice' chips, where loss is not such an acute factor. Their potential compact form factor and the capability of using 2D gratings to launch orthogonal polarizations into fibre have proved valuable in several demonstrations. For instance, Bunandar et al. [6] have performed a 46km field trial using a silicon PIC, shown in Fig 2 as the Alice, but with a non-integrated Bob.

In most CV-QKD systems in addition to the quantum signal, a reference local-oscillator signal is also launched in the orthogonal polarization state. This is particularly well suited to 2D grating couplers found in silicon photonics.

Discuss your application with us

If you want to learn more on the use of PIC technologies for the implementation of photonic chips for quantum communications, please contact the PICs4All consortium. Our consortium can support you in the techno-economic evaluation of photonic integration

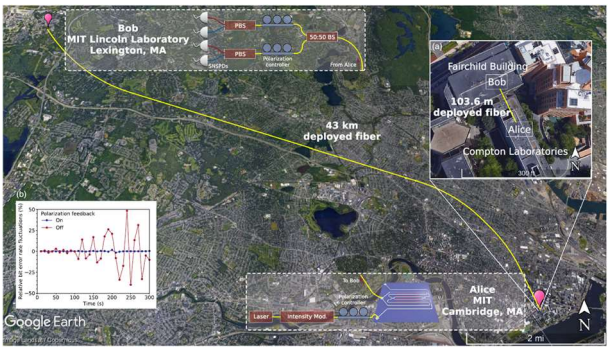
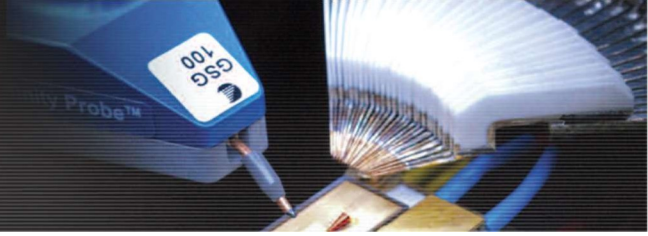


Figure 2. Metropolitan Quantum Key Distribution with Silicon Photonics [6]

geared towards your products and applications. Support may be given as well in the design and characterization. In the framework of the EU H2020 PICs4All project the partners offer free-of-charge guidance to companies, research institutes and academia interested in development and implementation of their commercial products, using photonic devices. The PICs4All consortium is funded under the EU Horizon 2020 programme and brings together expertise of nine European Application Support Centers (ASCs). The ASCs can guide you through the existing eco-system of design houses, foundries, packaging and test services.

Contact information

Nikos Bamiedakis, Adrian Wonfor
Email nb301@cam.ac.uk aw300@cam.ac.uk
Centre for Photonic Systems, Engineering Dept
University of Cambridge. UK



References

1. P.W. Shor, “Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer,” Proceedings of the 35th Annual Symposium on Foundations of Computer Science, Santa Fe, NM, Nov. 20-22 (1994)
2. https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Post-Quantum-Cryptography-Standardization
3. C. H. Bennett and G. Brassard. "Quantum cryptography: Public key distribution and coin tossing". In Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, volume 175, page 8. New York, 1984
4. A. K. Ekert, “Quantum cryptography based on Bell’s theorem,” Phys. Rev. Lett. 67, 661 (1991).
5. P. Sibson, et al., “Chip-based quantum key distribution”, Nature Communications volume 8, Article number: 13984 (2017)
6. D. Bunandaret et al., "Metropolitan Quantum Key Distribution with Silicon Photonics". Phys. Rev. X 8, 021009. 2018.