How Quantum Cryptography Works

Application Fields for COUNT® Modules

Data security and data exchange are topics with increasing importance. How do you prevent data from being intercepted by a third party? The solution lies in cryptography: The message must be encoded. But what if the key exchange is intercepted? This is where quantum cryptography comes into play.

The idea behind so-called quantum key distribution (QKD) is to use single photons instead of entire photon bundles. This way an eavesdropper (referred to as "Eve" in quantum mechanics) cannot simply divert the photons that are sent from Person A to Person B (referred to as "Alice" and "Bob," respectively, in quantum mechanics). Eve would have to copy and then detect the photons to prevent the interception from being detected by Bob. This is precisely what quantum mechanics renders impossible (the so-called "no cloning theorem").

Figure 1 depicts what key generation for coding and decoding data can look like. This so-called BB84 protocol (developed by Bennett and Brassard in 1984) uses the polarization of photons as a means of generating a key sequence. Alice selects one of four polarization states – H (horizontal), V (vertical), +45°, and -45° – and sends such a photon to Bob. She must first indicate which bit value the two orthogonally arranged polarization states have: 0 or 1. In our example, H corresponds to 0, V corresponds to 1, 45° correspond to 0, and -45° correspond to 1. If Bob receives such a photon, he decides whether to measure based on H/V or 45°/-45° and ultimately makes a note of the polarization state (and thus the bit value) of the photon. Bob communicates with Alice in the classic sense, and they compare their base selection. This information, which is of no use to Eve because she does not know the exact results, is sufficient for Alice and Bob to determine which bit values they can use for their key [1].

Germany & Other Countries
Laser Components GmbH
Tel: +49 8142 2864 – 0
Fax: +49 8142 2864 – 11
info@lasercomponents.com
www.lasercomponents.com

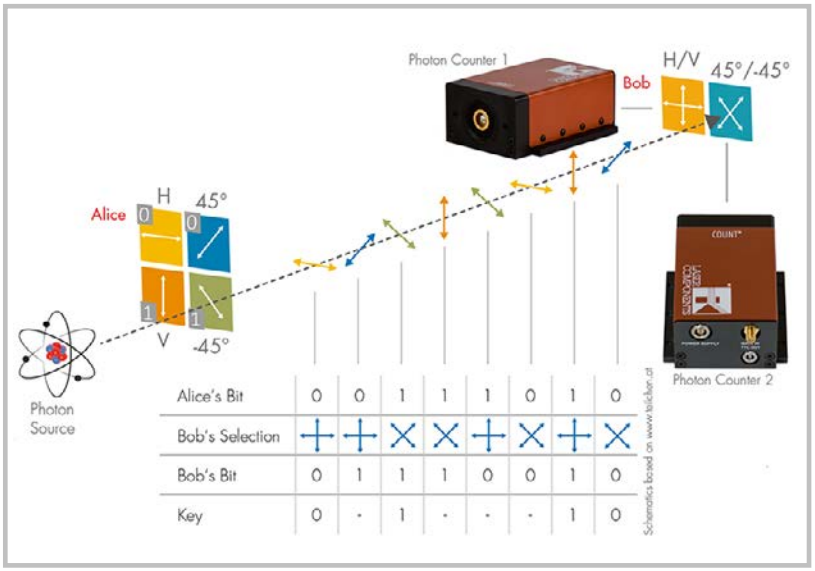
France
Laser Components S.A.S.
Tel: +33 1 39 59 52 25
Fax: +33 1 39 59 53 50
info@lasercomponents.fr
www.lasercomponents.fr

United Kingdom
Laser Components (UK) Ltd.
Tel: +44 1245 491 499
Fax: +44 1245 491 801
info@lasercomponents.co.uk
www.lasercomponents.co.uk

Nordic Countries
Laser Components Nordic AB
Tel: +46 31 703 71 73
Fax: +46 31 703 71 01
info@lasercomponents.se
www.lasercomponents.se

USA
Laser Components USA, Inc.
Tel: +1 603 821 – 7040
Fax: +1 603 821 – 7041
info@laser-components.com
www.laser-components.com

Figure 1: Schematics of the quantum key



A further development of the BB84 protocol uses entangled photons, which strongly correlate in their properties, that are sent from a single source to Alice and Bob simultaneously. One such source was developed, for example, by experimental physicists in Prof. Weihs' photonics group at the University of Innsbruck: a pulsed Sagnac source of polarization-entangled photons [2]. Here a nonlinear crystal is used that produces two lower-energy photons at a wavelength of 808 nm from a higher-energy photon at 404 nm. The photons are detected using two "COUNT" SPADs by LASER COMPONENTS.

As secure as these methods are in theory, in practice there is a lot of room for error. The most significant sources of error are the single photon detectors: In theory, they are perfect, identical, and have a detection efficiency of 100%; however, in practice, this is never the case. It is precisely this discrepancy in the detection efficiency of two detectors that quantum hackers use to access the key [3]. An alternative method "blinds" the SPADs with the help of a light pulse and uses the "blind time" of the detector to intercept information [4].

Thanks to the identification of sources of error by quantum hackers, research groups have been able to work on approaches for solutions to these problems and develop a "measurement unit-independent" version of the QKD [5].

[1] (for more information, see www.weltderphysik.de/gebiet/technik/quanten-technik/quanten-kryptographie/)

[2] (see www.uibk.ac.at/exphys/photonik/people/parametric-downconversion.html)

[3] (see arxiv.org/abs/quant-ph/0702262)

[4] (see arxiv.org/pdf/1008.4593v2.pdf)

[5] (see arxiv.org/abs/1109.1473)

Germany & Other Countries
Laser Components GmbH
Tel: +49 8142 2864 – 0
Fax: +49 8142 2864 – 11
info@lasercomponents.com
www.lasercomponents.com

France
Laser Components S.A.S.
Tel: +33 1 39 59 52 25
Fax: +33 1 39 59 53 50
info@lasercomponents.fr
www.lasercomponents.fr

United Kingdom
Laser Components (UK) Ltd.
Tel: +44 1245 491 499
Fax: +44 1245 491 801
info@lasercomponents.co.uk
www.lasercomponents.co.uk

Nordic Countries
Laser Components Nordic AB
Tel: +46 31 703 71 73
Fax: +46 31 703 71 01
info@lasercomponents.se
www.lasercomponents.se

USA
Laser Components USA, Inc.
Tel: +1 603 821 – 7040
Fax: +1 603 821 – 7041
info@laser-components.com
www.laser-components.com