CRYPTOGRAPHY OF THE FUTURE

The technology developed by DLR offers possibilities about the future of quantum key transmission

By Bernadette Jung *

DEVELOPMENT FOR CRYPTOGRAPHY

A successful experiment by the German Aerospace Center (Deutsches Zentrum für Luft- und Raumfahrt; DLR) in cooperation with the Ludwig-Maximilians-Universität (LMU) in Munich has opened up new possibilities in cryptography.

For the first time, researchers have managed to transmit a quantum key from a fast-moving object. The quantum data was sent from an aircraft to a ground station via a laser beam.

Key exchange based on quantum mechanics is considered to be absolutely secure against eavesdropping. The quantum mechanical states of individual photons are used for the encryption; attempts at interception disturb the behaviour of the particles and so can be detected immediately.

However, quantum cryptography has only been put to limited use so far – the data is usually transmitted via glass fibre so that only limited distances can be bridged.

The current flight experiment now proves that the encryption technology can also be used with fast-moving objects and can be integrated into existing optical communications systems.

In future, quantum data might also be distributed globally via satellite in this way.

UNIQUE EXPERIMENT

The quantum key transmission experiment took place in Oberpfaffenhofen, using the optical ground station at the DLR Institute for Communications and Navigation and the DLR Dornier Do 228-212 research aircraft.

DLR was also responsible for flight certification and campaign planning.

The aircraft was fitted with a laser system for the experiment, combining a transmitter for data communication with a second transmitter for the quantum cryptography. The laser beam sent from the aircraft was received by the ground station, recorded with specially developed measuring equipment and analysed.

The detailed assessments have now been published in the journal 'Nature Photonics'.

The particular challenge with the experiment was directing the light signals precisely onto the ground station telescope. To do this, the researchers managed to achieve a targeting accuracy of thousandths of a degree while flying.

"We didn't know how well this would work; it had never been done before. But we were able to create absolutely stable reception with good tracking for several minutes. It was great to experience," reports Florian Moll from the DLR Institute of Communications and Navigation.

LASER SYSTEMS DEVELOPED IN HOUSE

The communication laser developed by DLR has already been tested in previous projects and consists of two units. The coarse alignment unit is outside, on the fuselage of the Do 228-212, where a small glass dome protects the rotating mirror lens. In addition to this, there is the fine alignment unit inside the aircraft.

A sophisticated sensor and very rapidly moving mirror ensure that vibrations from the aircraft are compensated for in a frequency range of up to 100 hertz. This is the only way the laser beam can be directed with sufficient accuracy. The transmitter is also used for optical tracking; that is, for automatically tracking the aircraft.

In the quantum key transmission experiment, a reference signal was also sent with the communication laser, enabling synchronisation between the aircraft and the ground station.

A group led by LMU physicist Harald Weinfurter developed the laser used for the quantum cryptography specifically for this experiment. Using this system, it is possible to generate extremely weak laser pulses and thus exploit the quantum properties of individual photons. This forms the basis for encryption technology that cannot be intercepted.

The laser source was successfully integrated into the DLR laser system for the experiment, with no special requirements. *"This shows that quantum cryptography can be an add-on for existing systems,"* says Sebastian Nauerth from LMU.

A STEP INTO THE FUTURE

Key distribution cannot be intercepted – today from the air to the ground, tomorrow the challenge will be from space to the whole world.

The current results open up new possibilities for quantum cryptography.

The conditions for the flight experiment and the angular velocity of the aircraft at the ground station were comparable with communication via satellite, so the researchers will be using the knowledge they have acquired in new work and future developments.

For Moll and his colleagues, the goal is ambitious: *"We obviously want to make our technology applicable for satellites as well."*