2 Summary in English

The main goal of the project SEQURE (Symmetric Encryption with QUantum key REnewal) is to develop a complete system capable of performing fast data encryption over an installed fibre optics link, with extremely high security standards, guaranteed by the fact that the key renewal is realized via Quantum Key Distribution (QKD).

The project gathers two industrial partners (Thales Research and Technologies: TRT and Thales Communications : TCF) and two academic partners (Ecole Nationale Supérieure des Télécommunications : ENST and Institut d'Optique : IO), in order to develop and implement all aspects of a high-speed encrypted link, from quantum security proofs and hardware, up to network protocols for fast renewal of the secret keys used for symmetric encryption.

On the QKD side, the partners will implement two proprietary protocols: one based on photon counting in a time-coding protocol ("discrete variables", TRT), and another one using homodyne detection and Gaussian-modulated coherent states ("continuous variables", IO and TRT). On the data transmission side, a Gbit/sec encryptor will be implemented by TCF using established techniques. The quantum device generating the keys and the classical device encrypting the data will be interfaced using a controller device and software, designed to store, manage and dispatch the secret keys, and realized by ENST

While a central goal for the project is to design and demonstrate a fully integrated and working Link Encryption system, the planned research may lead to other substantial research breakthroughs for quantum-based network security. On the "quantum" side this includes faster key generation rates, longer transmission distances, and new results on security proofs. On the "network" side, crucial issues are new encryption algorithms exploiting the fast key renewal rate and the information-theoretic security offered by QKD, and network-oriented interfaces between QKD links and encryption devices. This part of the research will be inspired by the efforts towards standardization, initiated within the European Integrated Project SECOQC, in which the present partners are also involved.

The project objectives have to be placed in the global perspective of integrating QKD in dedicated security applications. A lot of efforts are currently spent in this direction in many academic and industrial research groups among the world, motivated by the comparative advantages of QKD over what is currently realizable with classical cryptographic methods. The results obtained in SEQURE will be communicated to a broad scientific community through scientific publications and dissemination, and may be exploited in particular within other European projects such as SECOQC or SINPHONIA.

In addition, it is planned within SEQURE to perform a market study regarding link encryption devices for high security applications. What can already be asserted is that key renewal via Quantum Key Distribution presents several essential advantages over what is realizable classically : the security of the key is unconditionnal and not computational, while the achievable key generation rates allow for fast key renewal that can improve the global security of symmetric ciphers such as AES. The concerned market segments are constituted by activity domains for which high security is a necessity: government, banks, OEM, military. The market study will determine the total volume of these market segments, as well as the purchasing and deployment criteria of the potential future clients.

As a conclusion, the success of SEQURE will imply that major steps have been made towards the realization of an efficient, competitive and highly secure system for Link Encryption. This could have a high impact on the deployment of QKD-based security solutions.