1 Résumé du projet en français

L'objectif central du projet SEQURE (Symmetric Encryption with QUantum key REnewal) est de mettre en oeuvre un système opérationnel de cryptage rapide de données, sur un lien en fibre optique installée, avec de très fortes exigences de sécurité garanties par le fait que le renouvellement de la clé sera assuré par un protocole quantique (distribution quantique de clé, ou QKD).

Le projet réunit deux partenaires industriels (Thales Research and Technologies : TRT et Thales Communications : TCF) et deux partenaires académiques (Ecole Nationale Supérieure des Télécommunications : ENST et Institut d'Optique : IO), afin de développer et de mettre en œuvre tous les aspects d'un lien crypté à haut débit, allant des preuves de sécurité et des dispositifs quantiques, jusqu'aux protocoles de réseau assurant le renouvellement rapide de la clé utilisée par un dispositif de cryptage symétrique.

En ce qui concerne la liaison quantique, les partenaires mettront en oeuvre deux protocoles qu'ils ont déjà brevetés : le premier utilise des compteurs de photons, avec un codage temporel des bits secrets ("variables discrètes", TRT), et le second utilise une détection homodyne et des états cohérents modulés ("variables continues", IO et TRT). En ce qui concerne le cryptage des données, un encrypteur rapide (Gbit/sec) sera mis en oeuvre par TCF, en utilisant des techniques éprouvées. Ces deux dispositifs seront reliés par l'intermédiaire d'un contrôleur et d'un logiciel appropriés, mis en oeuvre par l'ENST.

En plus de la conception et de la réalisation d'un lien crypté rapide, les recherches envisagées sont susceptibles d'avoir des répercussions notables sur le développement de protocoles de réseaux quantiques sécurisés. Du côté "quantique", les débouchés envisagés sont une augmentation du débit et de la distance de transmission des clés secrètes, et l'obtention de meilleures preuves de sécurité. Du côté "réseaux", des questions cruciales sont d'une part le développement de nouveaux algorithmes de cryptage exploitant mieux la sécurité quantique "inconditionnelle", et d'autre part la mise en oeuvre de liens standardisés entre les générateurs quantiques de clé et la couche applicative. Cet aspect des recherches sera relié aux efforts entrepris pour standardiser l'utilisation des protocoles quantiques, dans le cadre du Projet Intégré Européen SECOQC, qui inclut les partenaires du présent projet.

Les objectifs du projet SEQURE s'inscrivent dans la perspective globale d'une intégration de protocoles quantiques dans des applications dédiées ayant une forte exigence de sécurité. Des efforts importants sont actuellement consacrés à ce sujet par de nombreux groupes de recherche académiques et industriels au niveau mondial. Les résultats de SEQURE seront diffusés dans cette vaste communauté par des conférences et des publications scientifiques, et pourront être exploités par d'autres projets comme SECOQC ou SINPHONIA.

Il est aussi prévu d'effectuer dans le cadre de SEQURE une étude de marché concernant les liens cryptés à haute sécurité. Il est déjà établi que le renouvellement quantique de clé possède plusieurs avantages par rapport aux méthodes classiques : la sécurité de la clé est inconditionnelle plutôt qu'algorithmique, et les taux de production de clé accessibles actuellement permettent un taux de renouvellement qui peut améliorer la sécurité des chiffrages symétriques comme AES. Les segments de marché concernés sont par exemple gouvernementaux, bancaires ou militaires. L'étude de marché déterminera le volume de ces segments, ainsi que les critères pertinents pour les futurs clients potentiels.

En conclusion, le succès de SEQURE serait l'indicateur du franchissement de plusieurs étapes importantes, en direction de l'utilisation d'un système efficace et compétitif pour le cryptage à forte exigence de sécurité. Ceci pourrait avoir un impact élevé sur le déploiement de solutions de sécurité basées sur la cryptographie quantique.