

Invitation à la soutenance de thèse

DISTRIBUTION QUANTIQUE DE CLÉS À TRAVERS LA TURBULENCE ATMOSPHÉRIQUE :
LIAISONS SÉCURISÉES SATELLITE-SOL

*QUANTUM KEY DISTRIBUTION THROUGH ATMOSPHERIC TURBULENCE: SECURE
SATELLITE-TO-GROUND LINKS*

Valentina Marulanda Acosta

Lundi 04 décembre 2023, à 15h30

Campus Pierre et Marie Curie ; Couloir 25-26, Salle 105
4 Place Jussieu, 75005 Paris

Devant le jury composé de

M. Giuseppe Vallone	Università degli Studi di Padova	Rapporteur
M. Thomas Jennewein	University of Waterloo	Rapporteur
Mme Ghaya Reka	Telecom Paris	Examinatrice
M. Andrew Thain	ADS Toulouse	Examineur
Mme. Eleni Diamanti	CNRS, Sorbonne Université	Directrice de thèse
M. Jean-Marc Conan	ONERA, DOTA	Encadrant
Mme. Caroline Lim	LNE-SYRTE	Encadrante
M. Daniele Dequal	ESA-ESTEC	Invité

Résumé

Les exigences sans cesse croissantes des systèmes de télécommunication modernes en termes de débit, ainsi que la menace imminente que pose l'augmentation de la puissance de calcul des ordinateurs modernes sur les méthodes cryptographiques actuelles, font de la transmission sécurisée des données à la fois une exigence essentielle et un grand défi, et donc un domaine d'étude très actif.

La distribution quantique des clés (QKD) permet l'échange de clés cryptographiques dont le niveau de sécurité ne dépend pas de la complexité d'un algorithme mathématique mais repose intrinsèquement sur l'exploitation des propriétés de la mécanique quantique.

Cependant, le déploiement des systèmes QKD via des réseaux fibrés terrestres, est fortement limité en distance, et n'atteint que quelques centaines de kilomètres, en raison de l'atténuation exponentielle subie par les signaux transmis par fibre optique.

Les méthodes d'amplification des répéteurs de communications optiques classiques ne sont pas compatibles avec un signal quantique, et en raison du manque de maturité technologique concernant les répéteurs quantiques, les relais satellite se présentent comme une alternative intéressante pour l'établissement de liaisons quantiques intercontinentales sécurisées.

Nous présentons ici, dans le contexte d'un lien QKD descendant entre un satellite en orbite basse et le sol, un modèle complet du canal atmosphérique satellite-sol prenant conjointement en compte la turbulence, sa correction partielle par optique adaptative (OA) les pertes géométriques et les fluctuations de pointage à bord du satellite. Nous utilisons ce modèle pour évaluer les performances de trois protocoles QKD - à variables continues et à variables discrètes, avec des photons uniques ou intriqués - pour différentes conditions de turbulence, différents degrés de correction par OA, différents scénarios de configuration du lien (diamètre télescope, altitude du satellite...) tout en prenant en compte la taille finie de la séquence d'états ou de symboles émise.

Les résultats obtenus montrent l'intérêt de l'utilisation d'un système d'OA : en effet, la performance en termes de taux de génération de clé de tous les protocoles analysés s'améliore en considérant une correction par OA. Cette augmentation du taux de clé est particulièrement significative pour les scénarios de forte turbulence, d'opération diurne et pour le protocole QKD à variables continues (CV).

L'apport de l'OA est de plus démontré et quantifié dans une configuration très prometteuse exploitant l'émission de deux photons intriqués vers deux stations sol depuis un relais satellite qui n'est pas forcément de confiance. Afin de valider nos résultats de simulation, nous avons aussi commencé à implémenter un banc de test expérimental à partir d'une émulation simplifiée du canal atmosphérique et d'un système CV-QKD. Nous expliquons les difficultés rencontrées pendant cette mise en œuvre ainsi que les solutions proposées et des idées sur les perspectives de l'étude.

Mots clés

Optique adaptative, Communications optiques par satellite, Communications quantiques, QKD.