

# Spécialité de Master « Optique, Matière, Plasmas »

Stage de recherche (4 mois minimum, à partir de début mars 2012)

Proposition de stage pour l'année 2011-2012 (**ne pas dépasser 1 page**)

Date de la proposition : janvier 2012

<b>Responsables du stage :</b>			
Nom :	Diamanti	Prénom :	Eleni
Tél :	01 45 81 71 14	Fax :	
Courriel :	eleni.diamanti@telecom-paristech.fr		
<b>Nom du Laboratoire :</b>			
Code d'identification (UMR,UPR,...) :	UMR 5141	Nom du Directeur :	Henri Maître
Site Internet :	http://iq.enst.fr		
Adresse :	23 avenue d'Italie, 75013 Paris		
Lieu du stage :	23 avenue d'Italie, 75013 Paris		

<b>Titre du stage /internship title : Etude d'un canal caché dans des systèmes de cryptographie quantique</b>
Résumé/summary Le travail de l'équipe Information Quantique de Télécom ParisTech se situe dans le domaine du traitement de l'information quantique. Ce domaine offre la perspective de communications futures de meilleure qualité et de plus grande sécurité. Dans les récentes années, une de ses applications les plus importantes, la distribution quantique de clés, a connu des progrès importants qui ont mené au développement de systèmes commerciaux et à l'implémentation du premier réseau de cryptographie quantique télécom, dans le cadre d'un grand projet européen dans lequel notre équipe était fortement impliquée. La sécurité inconditionnelle de protocoles de distribution quantique de clés, c'est-à-dire leur sécurité contre un espion possédant des ressources infinies, est en principe prouvée. En pratique, cependant, celle-ci dépend du modèle choisi pour décrire les composants physiques qui constituent le système implémenté. Si le système n'est pas parfaitement décrit par ce modèle, alors de l'information secrète peut être perdue au profit de l'espion. Ce type de perte est dénommé « canal caché ». L'apparition des canaux cachés est en général liée à des composants photoniques, tels que des sources, des détecteurs ou des modulateurs, imparfaits et non fiables. Heureusement, une fois identifiées et modélisées, les attaques d'espionnage liées aux canaux cachés peuvent être éliminées grâce aux lois de la physique, nous permettant ainsi de regagner une sécurité absolue. Dans ce stage, nous proposons d'étudier <b>un canal caché potentiel lié au bruit acoustique généré par des modulateurs à base de niobate de lithium utilisés couramment dans les systèmes de cryptographie quantique</b> . En effet, à cause de leurs propriétés piézo-électriques, ces composants sont sujets à des vibrations mécaniques quand ils sont excités par un courant électrique de haute fréquence. Un espion pourrait en conséquence accéder à l'information précieuse de la modulation appliquée en exploitant cet effet. La dépendance directe de la tension à la quelle le modulateur est soumis avec les vibrations mécaniques générées a été constatée dans notre laboratoire ; la prochaine étape sera la caractérisation détaillée de cette dépendance et, surtout, l'étude des émanations acoustiques et la possibilité de leur utilisation en distance, par exemple avec un système d'interférométrie. Bien que nécessitant quelques développements théoriques assez simples, le sujet est principalement expérimental et il fait appel à l'optique sous toutes ses formes (classique, fibrée, non linéaire et quantique). Durée de stage minimale : 3 mois

<b>Ce stage pourra-t-il se prolonger en thèse ? Possibility of a PhD ? :</b>			
<b>Si oui, financement de thèse envisagé/ financial support for the PhD :</b>			
Lasers et Matière	<input checked="" type="checkbox"/>	Physique des Plasmas	<input type="checkbox"/>
Optique de la science à la technologie	<input checked="" type="checkbox"/>	Lumière, Matière : Mesures Extrêmes	<input checked="" type="checkbox"/>

Fiche à transmettre (fichier pdf **obligatoirement**) sur le site <http://stages.master-omp.fr>