Rapport de stage d'ingénieur

Développement d'une architecture de sécurité sur smartphone, déployable sur le réseau de distribution quantique de clés du projet européen SECOQC

Effectué du 1 juillet 2008 au 31 décembre 2008

Dans le département Informatique et Réseaux
de Télécom ParisTech

et au sein du projet SECOQC

"Development of a Global Network for Secure Communication based on Quantum Cryptography"

Guerra Roberto

Cycle Master Paris 2009

Encadrant de Stage : Romain Alléaume

Avant tout développement sur cette expérience professionnelle, il apparaît opportun de commencer ce rapport de stage par des remerciements, à ceux qui m'ont beaucoup appris au cours de ce stage, et à ceux qui ont eu la gentillesse de faire de ce stage un moment très profitable.

Je remercie tout d'abord Romain Alléaume, mon maître de stage, qui m'a dirigé et accompagné tout au long du projet SECOQC.

Je remercie Michel Riguidel et Philippe Laurier qui m'ont spécialement aidé dans la dernière partie de mon stage.

Je remercie toute l'équipe ARC Vienne, spécialement Oliver Maurhart, Andreas Happe et Thomas Themel, qui m'ont aidé au développement de ma partie du projet et m'ont accueilli à Vienne.

Je remercie Aurélien Bocquet et Dario Rossi, qui m'ont prêté l'équipement indispensable au bon déroulement de la démonstration.

Finalement je remercie tout le personnel de Telecom ParisTech avec une mention spéciale à David Elkouss, Gianluca La Mantia et Marco Nicoletti. Sans vous ce stage aurait été bien différent !

I. Introduction

Du 1er juillet 2008 au 31 décembre 2008, j'ai effectué un stage au département Informatique et Réseaux (INFRES) de l'école d'ingénieurs Telecom ParisTech. Encadré par Mr. Romain Alléaume, enseignent-chercheur en Information Quantique, au cours de ce stage j'ai pu m'intéresser à la définition et développement d'architectures de sécurité visant à profiter des nouvelles technologies de distribution quantique de clés. Au-delà d'enrichir mes connaissances techniques, ce stage m'a permis de comprendre le fonctionnement d'un projet européen à grande échelle et des différents enjeux qui se mettent en place.

Jusqu'au 10 octobre 2008 mon stage a consisté essentiellement en la participation au projet européen SECOQC : "Development of a Global Network for Secure Communication based on Quantum Cryptography", où j'ai développé une application sur smartphone permettant des communications sécurisées grâce au réseau de distribution de clés du démonstrateur SECOQC. Ce projet a culminé avec une démonstration à grande échelle du projet sur un réseau quantique métropolitain, du 8 au 10 octobre à Vienne. L'élaboration de ce rapport a pour principale source les différents enseignements tirés du développement de cette application et de la relation avec l'équipe de développeurs du projet travaillant à Vienne. Le reste de mon stage a consisté en la participation au projet SEQURE : "Symmetric Encryption with Quantum Key Renewal", avec le groupe Thales, où me basant sur les résultats de SECOQC, j'ai commencé à définir une interface d'injection de clés distribuées quantiquement dans des chiffreurs Mistral.

En vue de rendre compte de manière fidèle et analytique des mois passés au sein d'INFRES, il apparaît logique de présenter à titre préalable l'environnement du stage, puis de préciser les différentes missions que j'ai pu effectuer et finalement les nombreux apports que j'ai pu en tirer.

II. L’environnement du stage

1. Environnement Telecom ParisTech

a. Organisation interne de l’Ecole

Telecom ParisTech ou l'École Nationale Supérieure des Télécommunications (ENST) est une grande école d’ingénieurs publique française, spécialisée dans le domaine des technologies de l'information et de la communication fondée en 1878.

L'école fait partie de l'Institut TELECOM et c’est un des membres fondateurs de ParisTech, établissement public réunissant 11 écoles d'ingénieurs considérées comme les meilleures dans leurs domaines respectifs. On y trouve notamment l’École Polytechnique, Mines ParisTech ou Arts et Métiers ParisTech.

Le personnel de l’école est distribué en 9 services, tous sous la direction du directeur Yves Poilane.

1. **Direction de la Formation Initiale :** Elle définit la politique de formation initiale (Cycles Ingénieurs et Masters) des élèves et contrôle la mise en œuvre de celle-ci.
2. **Direction de la Formation Continue :** Elle définit la politique de formation continue et contrôle la mise en œuvre de celle-ci.
3. **Direction de la formation par la Recherche :** Elle pilote les études doctorales, gère la relation avec les établissements d'enseignement supérieur et administre le corps des enseignants-chercheurs.
4. **Direction de la Recherche :** Elle propose et met en œuvre les axes stratégiques de l'Ecole dans le domaine de la recherche.
5. **Direction de l’Innovation et du développement :** Elle élabore les axes stratégiques de l'Ecole dans les domaines de l'innovation, de l'entrepreneuriat et des relations avec les entreprises.
6. **Direction de la Communication :** Elle propose et met en œuvre la politique de communication interne et externe de l’Ecole.
7. **Direction de Ressources Humaines :** Elle est responsable de la mise en œuvre de la politique RH de l’Ecole en ce qui concerne les salariés, les stagiaires, les apprentis, les allocataires et, pour certains domaines, les élèves.
8. **Secrétariat Général :** Il est responsable de la gestion des différentes ressources de l'Ecole (humaines, financières, informatiques et matérielles), dans un cadre d'optimisation de l'utilisation de celles-ci.
9. **Départements d’enseignements-recherche** : Les 205 enseignants-chercheurs et 330 doctorants sont distribués en 4 départements spécialisés.
    - Informatique et Réseaux (INFRES).
    - Traitement du Signal et de l’Image.
    - Communications et Electronique.
    - Sciences Economiques et Sociales

Mon stage s’est déroulé au sein du département Informatique et Réseaux.

Note : Pour plus de détails a propos des services, départements et leurs responsables veuillez voir l’organigramme en Annexe I.

b. Organisation du département Informatique et Réseaux

Le département INFRES a pour missions la formation initiale, la formation continue, la recherche scientifique et contractuelle et la formation par la recherche, dans le domaine de l'informatique et des réseaux.

Ce domaine comprend l'informatique de la cognition, de l'interaction personne-machine et de l'intelligence artificielle, les mathématiques pour l'information, les communications et le calcul, les réseaux numériques de toute nature et leurs caractéristiques (mobilité, sécurité, gestion...) et l'informatique des systèmes des logiciels et des services.

Le département est organisé en une cellule administrative et technique, et en quatre groupes d'enseignement-recherche sous la direction du chef de département Michel Riguidel:

- Mathématiques de l'Information, des Communications et du Calcul (MIC^2).
- Réseaux, Mobilité et Sécurité (RMS).
- Systèmes, Logiciels, Services (S^3).
- Interaction, Cognition et Complexité (IC^2).

Physiquement le département est distribué entre les sites Barrault et Dareau de Telecom Paristech.

c. Cadre de travail

Mon stage s'est déroulé essentiellement dans le site Dareau de Telecom ParisTech, au bureau DB-311 que je partageais avec un enseignant-chercheur de l'Université Polytechnique de Catalogne en année sabbatique.

Les affaires administratives de mon stage tels que l'obtention du badge, le remboursement des frais de mission et d'autres, ont été gérées par Hélène Melkebeke, membre de la cellule de support administratif du département. Les affaires techniques telles que l'obtention d'un PC, un écran ou des câbles ont été gérées par Patrick Clément, assistant de travaux et technicien du département.

Mes différentes tâches ont été encadrées par Romain Alléaume, enseignant-chercheur dans le groupe Mathématiques de l'Information, des Communications et du Calcul spécialisé en Information Quantique. Les objectifs à atteindre m'étaient fixés mais les solutions techniques pour y arriver étaient ma responsabilité. En ce sens-là j'ai travaillé en complète autonomie dans les longues phases de développement en soi. Des réunions périodiques avec mon encadrant me permettaient de lui informer de mes progrès.

Les conditions de travail ont été assez souples avec une grande liberté au niveau horaire. C'est moi qui gérait mon temps pourvu que le travail soit bien fait et à temps, ce qui me donnait une grande indépendance. C'est pourquoi j'essayais de me fixer des objectifs pour chaque journée et une fois accomplis je me permettais de partir.

2. Environnement SECOQC

a. Description du projet

Le projet SECOQC, “Development of a Global Network for Secure Communication based on Quantum Cryptography”, a permis d’établir des nouveaux standards et des percées significatives en cryptographie quantique, tant sur le plan des systèmes matériels que des architectures de sécurité et des protocoles pour l’établissement de réseaux quantiques de distribution de clés.

Son but a été de permettre le déploiement d’applications sécurisées, incluant téléphonie et vidéoconférence, sur un réseau global de distribution de clés quantiques (QKD Network), fournissant ainsi un niveau de sécurité sans précédent. Huit liens quantiques on était combinés pour former pour la première fois un vrai backbone quantique, déployé dans un réseau métropolitain afin d’interconnecter différents bâtiments de Siemens Austria à Vienne.

Les résultats du projet, après 4 années intenses de travail, ont été présentés lors d’une démonstration et conférence à grande échelle à Vienne, du 8 au 10 octobre 2008. De nombreuses entreprises telles que Toshiba, Siemens, Thales, Hewlett-Packard ou Nokia Siemens Networks, en plus d’universités et centres de recherches de renommée internationale tels que l’université de Cambridge ou le KTH ont participé à ce projet.

Note : Pour une liste complète des entreprises et des institutions qui ont participé voir Annexe II.

b. Cadre de Travail

Mon travail au sein du projet s’est déroulé en parallèle au travail d’une équipe d’experts scientifiques et développeurs des Austrian Research Centers (ARC), dont le rôle était de développer les protocoles et les applications pour la démonstration, en plus d’organiser la conférence en elle-même.

Depuis mon poste à Paris, j’ai été en constante communication avec l’équipe de Vienne moyennant le mail et un système de tickets online. Ce système consistait en un site web où tous les développeurs impliqués dans le projet pouvaient déposer des tickets avec des doutes ou des remarques à propos de leur travail et celui de la cellule à Vienne, ainsi que des bugs ou problèmes rencontrés dans leur software.

Les applications et librairies développées à Vienne étaient essentielles pour que ma partie du projet puisse fonctionner correctement et ce site servait également à distribuer les différentes versions de leur software aux développeurs externes.

Pendant mon séjour à Vienne j’ai travaillé directement dans les bâtiments de Siemens Austria avec l’équipe ARC, qui m’a aidé à déployer mon application dans le réseau quantique métropolitain.

III. Les travaux effectués

1. Le projet SECOQC

a. Problématique et objectif de la mission

Le réseau développé au sein de SECOQC permet la distribution de clés cryptographiques avec un niveau de sécurité sans précédent. Ces clés peuvent alors être utilisées par toute sorte d'applications afin de sécuriser des communications : chiffrement, authentification, etc.

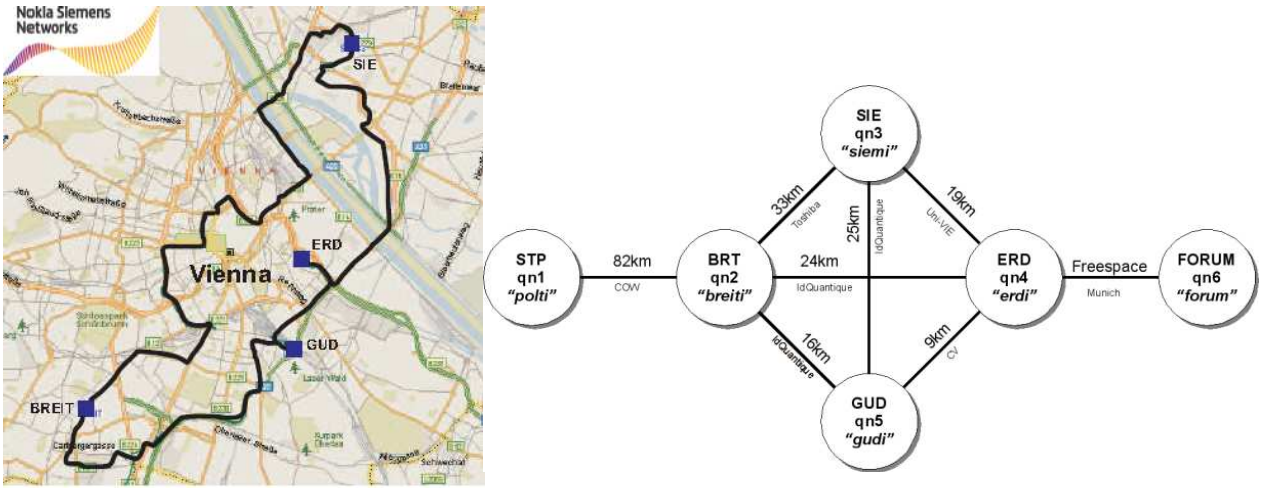
Ma mission était de définir une architecture de sécurité puis de développer une application qui profiterait de cette technologie afin de sécuriser entre autres les canaux a priori les plus vulnérables : les réseaux sans fils. Cette application serait installée dans un smartphone et permettrait d'échanger des fichiers chiffrés et authentifiés avec un serveur.

Le fonctionnement de l'application serait montré au cours de la conférence SECOQC. C'était donc nécessaire de développer une visualisation adéquate de la sécurité de l'application.

b. Etude du réseau et des protocoles SECOQC : Mai 2008

La première phase de ma mission a débuté deux mois avant le début officiel de mon stage sous forme de brique Projet Libre. Elle a consisté en l'étude du réseau SECOQC et des différents protocoles qui ont été mis en place pour réaliser la distribution de clés.

Le réseau consistait en un total de 8 liens quantiques, 7 fibres optiques et un lien FreeSpace, qui interconnectaient 6 nœuds quantiques. A ce stade du projet le lien FreeSpace n'était pas encore assuré. Chaque lien était formé par deux QKD Devices et un canal qui les reliait entre eux. Tous les liens étaient hétérogènes et utilisaient des technologies quantiques différentes.



Figures 1 et 2 : Plan et schéma du réseau métropolitain SECOQC à Vienne

Chaque nœud était formé physiquement par une machine (Node Module, Figure 3) à laquelle étaient connectés n QKD Devices, un pour chaque nœud auquel celui-ci était relié.

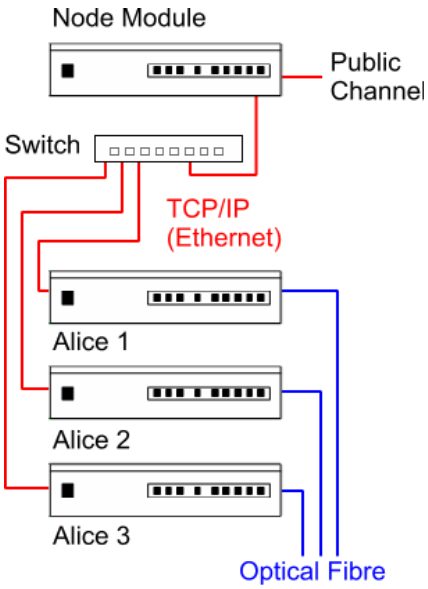


Figure 3 : Schéma d'un nœud quantique connecté à 3 liens

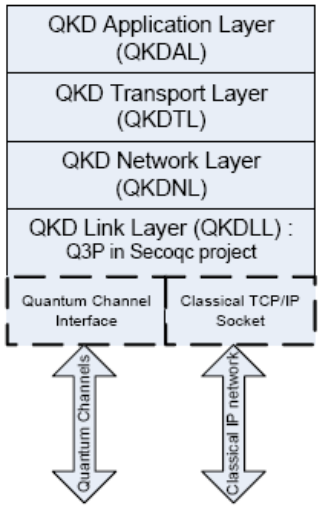


Figure 4 : Couches du réseau SECOQC

Basés sur TCP/IP, des nouveaux protocoles de liaison, réseau et transport ont été développés pour répondre aux besoins spécifiques d'un réseau QKD : le protocole Q3P (Quantum Point to Point Protocol)), la couche QKD-NL (Quantum Key Distribution Network Layer) et la couche QKD-TL (Quantum Key Distribution Transport Layer). (Figure 4)

Grace à ces nouveaux protocoles on peut échanger des clés de façon sécurisée entre deux nœuds n'importe-lesquels du réseau. (Figure 5)

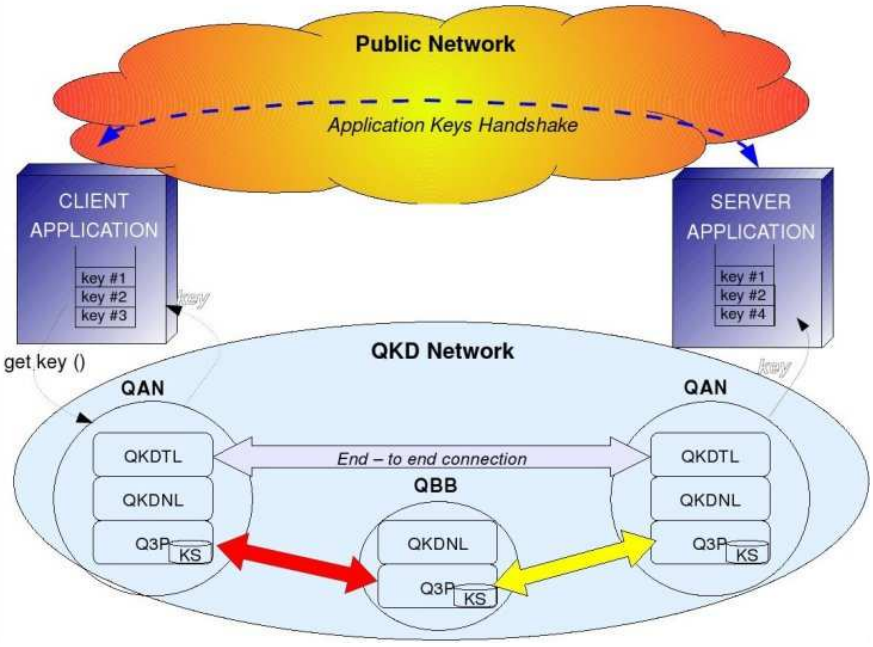


Figure 5 : Obtention de clés End-to-End

Malgré tout les liens entre les nœuds d'accès et les applications restent non sécurisés.

Plusieurs semaines ont été nécessaires afin de bien comprendre le fonctionnement global du réseau et des liens quantiques.

c. Test et débugage du software ARC : Mai – Septembre 2008

L'étape suivante a consisté à l'étude et débugage du software que la cellule de Vienne était en train de développer. Essentiellement ce software permettait, grâce au protocole QKD-TL, d'échanger des clés aléatoires entre deux machines. La figure 6 montre le fonctionnement global du protocole. Le point « QKD-TL » représente le réseau QKD tout entier. Cet échange était censé se faire à travers ce réseau et donc sécurisé grâce au protocole Q3P, mais le software pouvait être utilisé également sans cette sécurisation.

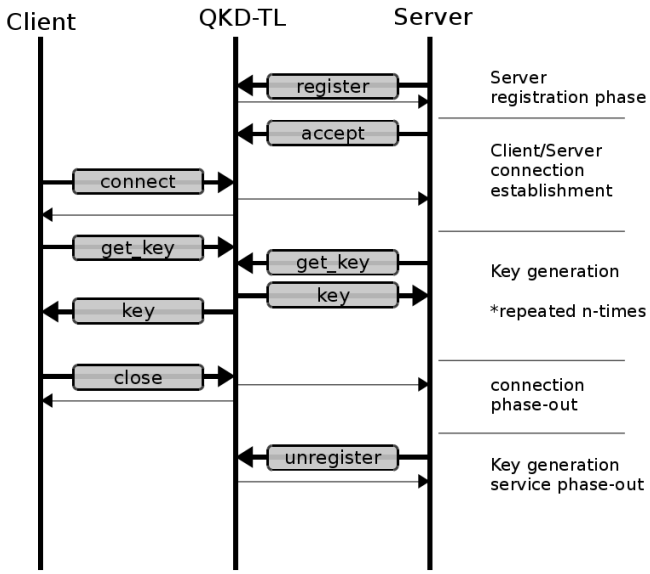


Figure 6: Fonctionnement du protocole QKD-TL

Ce software était nécessaire pour le bon fonctionnement du réseau QKD et donc de mon application. J'ai dû donc étudier le fonctionnement de ce software, le tester et signaler les éventuels bugs à l'équipe ARC. La nature du software imposait travailler sous Unix. J'ai choisi Ubuntu en raison de sa simplicité.

Pour cela j'ai développé quelques applications en C qui utilisaient les librairies développées à Vienne et testé leur bon fonctionnement. Après quelques tests les bugs étaient nombreux et les applications ne marchaient pas comme elles auraient dû marcher.

Cette étape s'est donc prolongée pendant des mois puisque l'équipe ARC actualisait périodiquement leur software et librairies en essayant de résoudre les problèmes, et il fallait retester tout. Les actualisations n'étaient pas toujours efficaces et souvent des problèmes étaient résolus mais de nouveaux apparaissaient.

Finalement en début Septembre tous les bugs semblaient être résolus et tout semblait marcher comme il fallait.

d. Définition de l'architecture globale de sécurité : Juin 2008

Parallèlement au test du software ARC, avec Mr. Alléaume j'ai commencé à étudier les possibles architectures qu'on pouvait mettre en place. On a contacté Artur Hecker, enseignant-chercheur en réseaux et sécurité pour lui demander son avis. La problématique essentiellement était comment gérer l'accès du smartphone au réseau quantique.

- **Architecture globale**

Après quelques jours de réflexions on a défini l'architecture globale suivante :

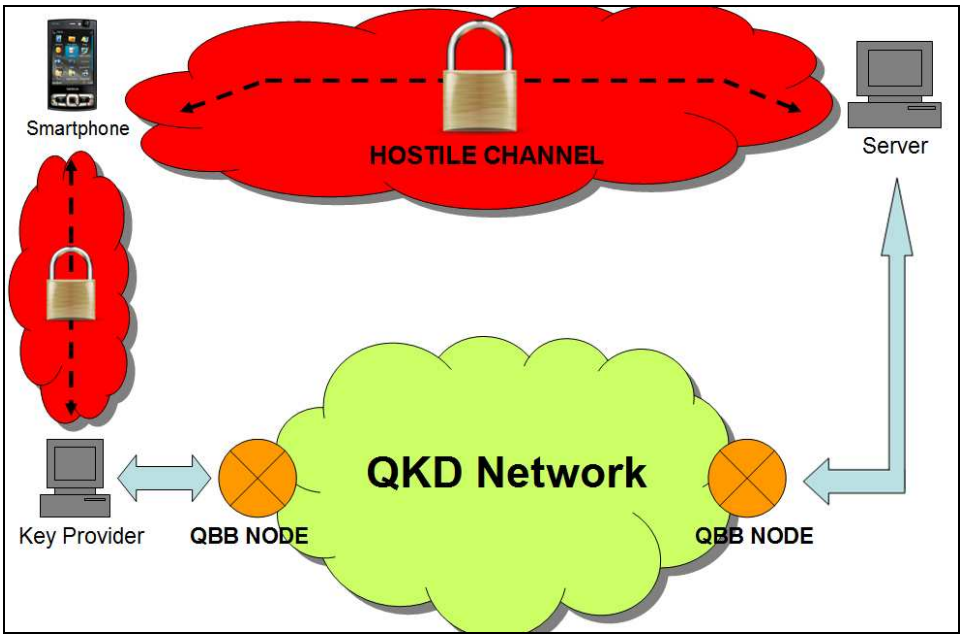


Figure 7 : Schéma de l'architecture globale de sécurité à développer

Le smartphone veut communiquer avec un Serveur, qui est connecté à un des nœuds quantiques. Pour ceci il a besoin de clés, qui doivent être partagées avec ce Serveur. Il va donc contacter un Key Provider, connecté à un autre Nœud à travers un canal qui sera bien sûr fortement sécurisé. La procédure de distribution de clés va alors se déclencher et le Key Provider et le Serveur vont recevoir leurs clés. Le Key Provider va envoyer ces clés au Smartphone qui les utilisera pour sécuriser la connexion avec le Serveur.

Le principal avantage de cette approche, à part bien sûr la sécurité, est qu'elle est facilement adaptable à plusieurs serveurs. Imaginons qu'on trouve n serveurs connectés au réseau. Le smartphone n'aurait qu'à négocier les clés que avec un unique Key Provider pour accéder à n'importe quel de ces serveurs. On peut donc établir une communication 100% sécurisée en One Time Pad avec n serveurs, tout en négociant avec un seul partenaire. (Figure 8)

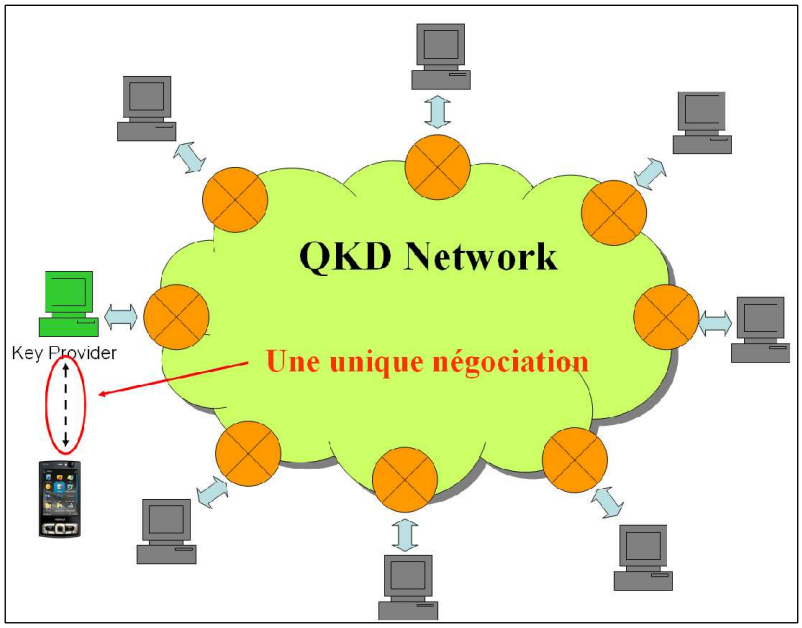


Figure 8 : Schéma de l'extension de l'architecture à n serveurs.

Si on regarde un peu plus loin, on pourrait connecter un smartphone à chacun de ces Serveurs, qui seraient à leur tour Key Providers pour leurs smartphones respectifs. On pourrait donc obtenir une communication totalement sécurisée entre smartphones, qui pourraient être situés n'importe où tant qu'ils puissent se connecter à leur Key Provider. Il suffirait qu'ils aient un accès Internet.

- **Election du smartphone et du langage de programmation**

Initialement on avait pensé à utiliser un iPhone dans la démonstration mais plusieurs facteurs nous ont amené à changer d'avis. D'un côté obtenir un certificat pour pouvoir développer dessus n'était pas évident, le développement était en version Beta et il fallait des mois d'attente pour l'obtenir. De l'autre, le langage à utiliser (Objective C) était nouveau pour moi et pas évident à maitriser rapidement. Finalement j'ai décidé d'utiliser un NOKIA N95, qui était programmable en J2ME (Java pour mobiles) et n'était pas excessivement cher. Ce langage était aussi nouveau pour moi mais il est très semblable à Java/Swing et je me voyais capable de le maitriser rapidement. En raison de compatibilités avec le smartphone on a décidé que toute la programmation de l'architecture (Key Provider et Serveur) se ferait en Java.

- **Election des protocoles de communications et des algorithmes de sécurité**

Toutes les communications se feraient en TCP/IP, indépendamment du support physique. Ceci permettrait au Smartphone d'être situé n'importe où au monde tant qu'il ait accès au réseau quantique à travers une connexion TCP/IP.

Les algorithmes de sécurité ont été fixés un peu plus tard, au-fur-et-à-mesure que le développement avançait.

e. Etude du langage de programmation : Juin 2008

Après l'élection du smartphone j'ai dû rapidement apprendre le langage de programmation J2ME. Des visites à la bibliothèque de l'école et à des sites web divers m'ont permis de rapidement le maitriser. En ce moment je ne disposais pas du N95 et donc j'ai dû trouver un émulateur de téléphone pour pouvoir tester.

f. Développement de l'application : Juin – Septembre 2008

Cette étape a été la plus longue et complexe de mon stage. Je me suis fixé une série d'objectifs progressifs à atteindre qui profitaient de la réussite de l'objectif antérieur. Ainsi à la fin de chaque phase j'avais une application qui fonctionnait, et chaque phase supplémentaire était une amélioration de celle-ci. L'objectif de cette démarche était d'avoir en tout moment une application qui marchait tout en la complexifiant à chaque nouvelle phase.

On peut les résumer de la façon suivante.

Initialement, le développement a été fait en local sur une même machine.

1. **Développement d'une application non sécurisée pour échanger des fichiers entre un smartphone et un Serveur :** le smartphone se connecte en TCP/IP au Serveur et lui envoie un flux de données que le Serveur sauvegarde ou vice-versa.

2. **Chiffrement AES de la connexion Smartphone – Serveur :** à l'aide de clés déjà présentes des deux côtés, le Smartphone et le Serveur chiffrent en AES les fichiers d'un côté et les déchiffrent de l'autre. On parle de clés de Service. J'ai choisi AES car c'est un algorithme standardisé, avec des performances de sécurité prouvées.

3. **Authentification HMAC dans la connexion Smartphone – Serveur :** à l'aide des clés de Service, le Smartphone et le Serveur utilisent un HMAC pour authentifier les fichiers en plus de les chiffrer.

4. **Mise en place du Key Provider :** le smartphone se connecte au Key Provider, qui lui envoie des clés de Service déjà présentes des côtés Key Provider – Serveur de façon non sécurisée. Il les utilise pour sécuriser la connexion avec le Serveur.

5. **Sécurisation de la connexion Smartphone – Key Provider :** à l'aide de clés déjà présentes des côtés Smartphone – Key Provider qu'on appellera clés d'Accès, ce dernier chiffre et authentifie les clés de Service avant de les envoyer au Smartphone. Ce dernier les déchiffre et les utilise pour sécuriser la connexion avec le Serveur.

A ce stade on a donc deux catégories de clés :

- clés d'Accès : pour sécuriser la connexion Smartphone – Key Provider, qui sont pré-échangées entre eux.

- clés de Service : pour sécuriser la connexion Smartphone – Serveur, qui sont pré-échangées entre le Key Provider et le Serveur, puis envoyées par le Key Provider au Smartphone.

6. Obtention quantique des clés de Service : les clés de Service sont maintenant envoyées au Serveur et au Key Provider grâce au software de l'équipe ARC. Pour que ceci soit possible je développe deux programmes en C qui utilisent des librairies spéciales. Ces programmes seront appelés depuis le programme Java des cotés Key Provider et Serveur. Les particularités de ce programme font que je sois obligé à supprimer l'option de recevoir des fichiers depuis le Serveur, on pourra seulement les envoyer. Par contre on pourra recevoir des informations en mode texte et les montrer à l'écran.

7. Obtention des clés d'Accès : je développe un nouveau programme en Java Swing pour pré-échanger les clés du côté Key Provider-Serveur, en les gardant dans une base de donnés du coté Key Provider et dans une carte mémoire du coté Smartphone. Ces clés seront générées aléatoirement grâce à un algorithme basé sur SHA 256 .Voir Figure 9.

La sécurité de l'application toute entière correspond à la sécurité de son lien le moins sécurisé. Utiliser une sécurité totale dans la distribution de clés perd son sens si la sécurité des algorithmes postérieurs est faible. Il faut donc que les algorithmes de sécurité soient le plus performant possibles. On décide de les améliorer.

8. Amélioration du chiffrement : J'élimine AES comme mode de chiffrement et j'utilise du One Time Pad, qui est le meilleur chiffrement au sens mathématique ; incassable tant que la clé n'est jamais réutilisée.

9. Amélioration de l'Authentification : j'élimine HMAC comme mode d'authentification et j'installe Evaluation Hash. Il s'agit du même algorithme de d'excellentes performances utilisé au réseau quantique pour l'authentification. Pour ceci je dois adapter un code expérimental en C à Java. De plus je rajoute un password pour sécuriser la connexion Smartphone – Key Provider. Ce password est composé de 12 caractères en base 64 générés aléatoirement suivant le même algorithme que les clés. Ainsi j'obtiens une double authentification : du terminal grâce à l'Evaluation Hash et aux clés d'Accès de la carte mémoire, et de l'Utilisateur grâce au password.

10. Gestion d'erreurs : les différentes erreurs possibles doivent être gérées : password erroné, fichier erroné, etc.

Jusqu'à ce moment l'application était fonctionnelle mais il restait à développer la visualisation, indispensable pour une démonstration.

11. Visualisation : toutes les échanges de clés doivent être visualisées lors de la démonstration, je développe donc une visualisation graphique de celles-ci en Java Swing. On est capable de visualiser l'évolution des clés d'Accès et de Service dans le Smartphone et dans le Key Provider, et des clés de Service dans le Serveur. Voir Figure 11.

12. Test sur deux machines : j'installe l'application sur deux machines, équivalentes à Key Provider et Serveur.

13. Test dans le smartphone : finalement j'abandonne l'émulateur de smartphone et je teste les différentes versions dans le vrai téléphone.

g. L'application achevée : Septembre 2008

L'application était prête en mi Septembre. Voici son fonctionnement en mode envoi de fichiers:

Phase d'enregistrement : Figure 9

- Le nouvel utilisateur de l'application va physiquement à son Key Provider et connecte une carte de mémoire vide.
- Le Key Provider l'identifie comme un nouvel utilisateur et lui demande de s'enregistrer.
- L'utilisateur reçoit une certaine quantité de clés, un code client et un password. Le code et la clé sont enregistrés d'un côté dans la carte, et dans une base de données de l'autre. Le hash du password (SHA 256) est enregistré dans la base de données.

Figure 9 : Fenêtres successives lors de la phase d'enregistrement

Phase de service : Figure 10

- L'utilisateur veut envoyer un fichier au Serveur, il insère sa carte, déclenche l'application et choisit l'option d'envoyer un fichier.
- Son password lui est demandé, puis quel fichier il veut envoyer.

Figure 10: Fenêtres successives lors de la phase de service

Le reste du fonctionnement est automatique.

- Le Smartphone se connecte en TCP/IP au Key Provider et lui envoi son code client, l'adresse IP et le port du serveur (configurables au menu principal), la longueur de clé qu'il a besoin, son password chiffré et l'Evaluation Hash.
- Grace à sa base de données indexée par le code client, le Key Provider vérifie l'Evaluation Hash et le password.
- Le Key Provider et le Serveur déclenchent alors la Quantum Key Distribution et demandent des clés de Service au réseau quantique.
- Le Key Provider chiffre les clés de Service et les envoie authentifiées avec l'Evaluation Hash au Smartphone.
- Le Smartphone les déchiffre, vérifie l'Evaluation Hash et les utilise pour chiffrer le fichier et l'authentifier, puis il l'envoie.
- Le Serveur déchiffre le fichier, vérifie l' l'Evaluation Hash et le sauvegarde.

On peut voir ces étapes dans la figure suivante, qui fait partie de la visualisation de l'application.

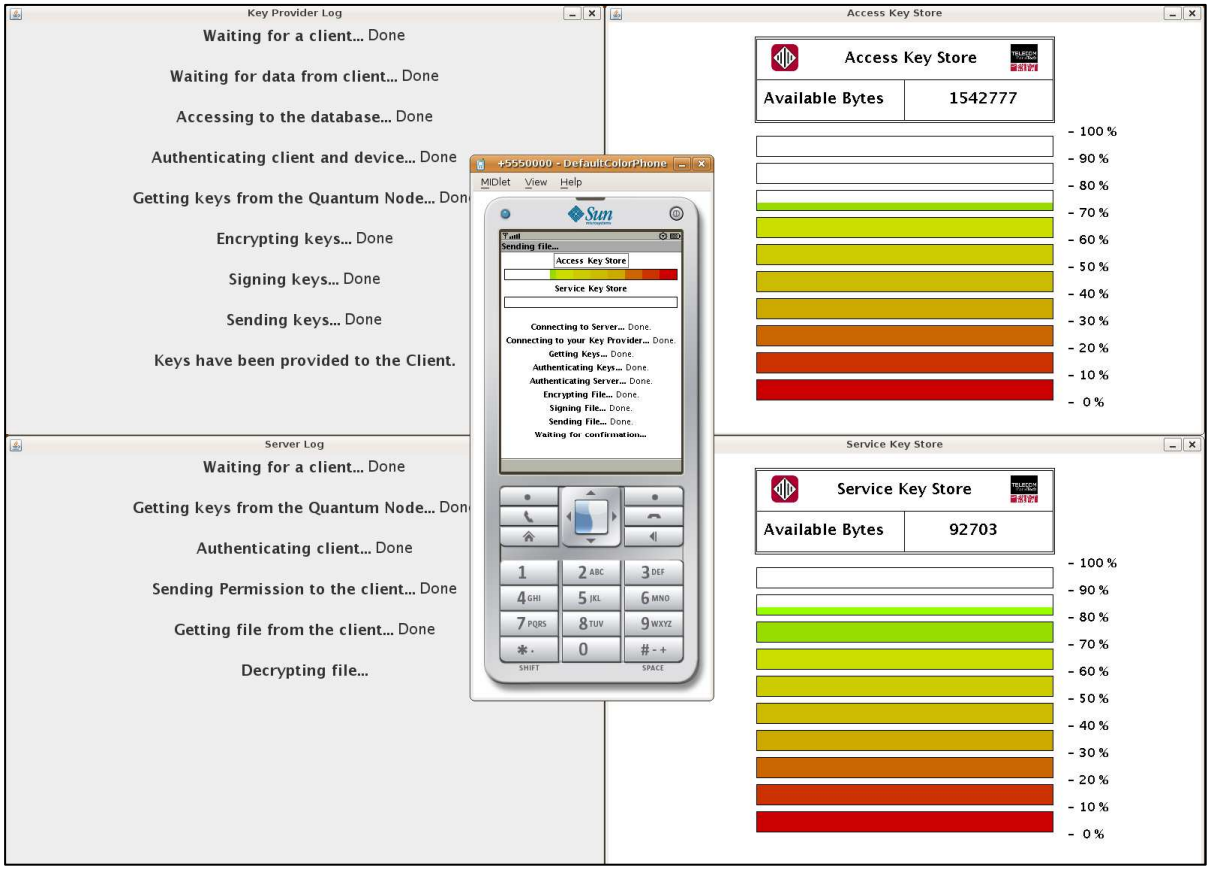


Figure 11 : Part de la visualisation graphique de l'application finale

Phases alternatives :

- Egalement on peut recevoir des informations en mode texte depuis le serveur et les montrer à l'écran.
- On peut consulter en tout moment le niveau de clés d'Accès depuis le menu principal.
- Si la réserve de clés se vide il faut retourner au Key Provider, où il faudra s'authentifier et puis on recevra des nouvelles clés et un nouvel password.

i. La préparation du séjour à Vienne : Septembre 2008

Pendant la fin du mois de septembre je me suis occupé essentiellement d'affaires de logistique car on a été informés que s'était à nous d'emmener tout le matériel nécessaire pour la démonstration.

Jusqu'à ce moment j'avais travaillé avec des PC fixes, mais si on devait tout emmener il me fallait des laptops. J'ai dû donc me débrouiller pour que quelqu'un nous prête ces laptops, installer Ubuntu dessus et puis réinstaller toute l'application. Egalement on nous a prêté une borne Wifi et quelques câbles.

On a aussi dû décider qu'est-ce qu'on allait montrer exactement pendant la démonstration puisqu'on ne disposerait que d'un écran. On a décidé qu'on enverrait une photographie et qu'on ne montrerait que le mouvement de clés entre Smartphone et Key Provider, et non entre Smartphone et Serveur car finalement le plus important de l'application était l'accès au réseau, qui est géré par le Key Provider. Pour une démo en live, il vaut mieux rester simple et ne pas montrer trop d'information qui pourrait confondre le public.

j. Le séjour à Vienne : 5-10 octobre 2008

Le 5 octobre commençait la partie la plus intense de mon stage. La démonstration devait se présenter le 8 octobre à 14h et donc on n'avait que deux jours pour tester son fonctionnement. A Paris les tests avaient été faits sans le réseau quantique qui finalement est le cœur de l'application, donc on n'avait pas de garanties absolues que tout allait bien se passer. Au cas où il y aurait eu un problème grave les possibilités de la résoudre à temps étaient minimales.

Le 6 octobre j'ai rencontré l'équipe ARC de Vienne avec Mr. Alléaume et on est allé dans le nœud ERD pour tester les différentes applications. On a décidé alors de connecter le Serveur au nœud ERD et le Key Provider au nœud FORUM (Voir Figures 1 et 2), pour des raisons de proximité géographique. On utiliserait donc le lien Freespace. Avec l'assistance d'Oliver Maurhart, j'ai configuré les tables de routage et quelques fichiers de configuration par rapport à la configuration du réseau SECOQC (Voir Annexe III pour les détails du réseau). Egalement j'ai installé un software sur les laptops qui allait me permettre de visualiser l'état du réseau quantique en tout moment, et donc de compléter la visualisation de la démonstration. L'après-midi j'ai commencé les tests. Après quelques petites optimisations tout marchait bien. Finalement le fait de tout emmener a été un gros avantage car du coup à Vienne les tests on été beaucoup plus simples, car quasiment tout était déjà installé et configuré.

Le 7 octobre j'ai testé l'application dans la salle et avec l'équipement qu'on allait utiliser le lendemain, ce qui m'a permis d'optimiser la visualisation par rapport à la résolution du projecteur qu'on allait utiliser. J'ai également assisté aux derniers tests de l'équipe ARC.

Le 8 octobre a commencé la démonstration et conférence. C'était la journée la plus « politique » avec la presse et des représentants des institutions européennes entre autres. Le matin a consisté essentiellement en une présentation du réseau et une démonstration de téléphonie et vidéoconférence entre nœuds sécurisée grâce aux clés issues du réseau QKD. Le flux téléphonique était chiffré en One Time Pad, c'était donc mathématiquement incassable mais par contre les réservoirs de clés du réseau se vidaient très rapidement car ce protocole exige une énorme quantité de clés. La vidéoconférence était par contre chiffrée en AES, elle était donc moins sécurisée mais beaucoup plus optimale au niveau consommation de clés. Une simulation d'attaque au réseau a été réalisée pour observer comment elle était rapidement détectée et la communication continuait sans problèmes. Sauf un petit détail tout c'est bien passé. Pendant la pause déjeuner j'ai fait un dernier test de mon application.

A 14 heures Mr. Alléaume a commencé son talk pendant lequel il allait présenter l'application. Mon rôle était de gérer l'application et la visualisation pendant qu'il la présentait. La démonstration consistait en réaliser une photo en live de l'audience grâce au smartphone et l'envoyer au Serveur grâce à l'application. Pendant ce temps une visualisation des échanges de clés entre le Key Provider et le Smartphone serait montrée, en plus d'une visualisation de l'état du réseau quantique. Finalement je me connecterais au Serveur via SSH et je montrerais qu'effectivement la photo a été bien reçue. Tout a marché correctement. Le reste de l'après-midi a consisté en divers talks a propos de l'état de l'art de la cryptographie quantique tout au long de la planète.

Pendant les deux jours qui restaient, les plus grands experts au monde en cryptographique quantique ont présenté leurs dernières réussites en matière d'émetteurs et détecteurs quantiques, incluant des propositions de standardisation.

Vendredi soir ma participation au projet SECOQC était finie.

Pour plus de détails a propos du programme de la conférence voir Annexe IV ou consulter le site www.secoqc.net.

2. Le projet SEQURE

a. Problématique et objectif de la mission

Après la fin du projet SECOQC j'ai commencé à travailler dans un nouveau projet réunissant deux partenaires industriels (Thales Research and Technologies et Thales Communications) et deux partenaires académiques (Telecom ParisTech et l'Institut d'Optique) : le projet SEQURE (**S**ymmetric **E**nrcyption with **Qu**antum key **Re**newal).

L'objectif central du projet est de mettre en œuvre un système opérationnel de cryptage symétrique rapide de données grâce à des chiffreurs Mistral de Thales, sur un lien en fibre optique , avec de très fortes exigences de sécurité garanties par le fait que le renouvellement de la clé sera assuré par un protocole quantique.

Le projet devait développer et mettre en œuvre tous les aspects d'un lien crypté à haut débit, allant de la mise en place des dispositifs quantiques, jusqu'aux preuves de sécurité et protocoles de réseau assurant le renouvellement rapide des clés distribuées quantiquement.

Ma mission était, en me basant sur les résultats de SECOQC, de commencer à définir une interface d'extraction de clés des dispositifs quantiques et d'injection sur les chiffreurs. On peut voir le principe dans la figure suivante.

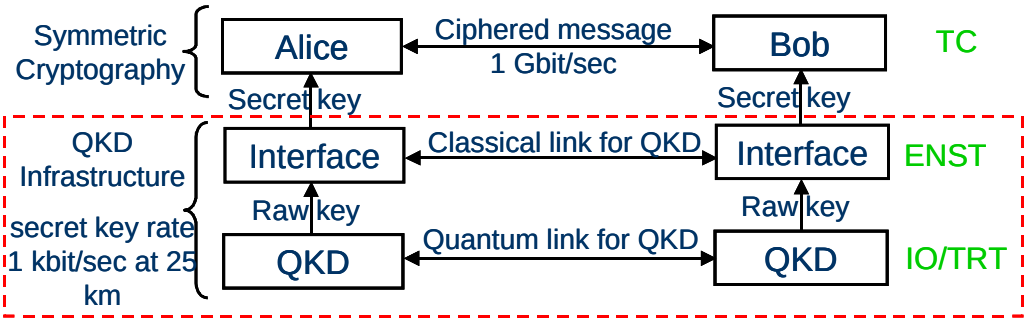


Figure 12 : Principe du projet SEQURE.

b. Définition de deux options pour l'interface : Novembre 2008

J'ai défini deux possibles options pour la distribution de clés jusqu'aux chiffreurs, en analysant les avantages et les inconvénients de chacune d'elles.

- **Option 1 :** Utiliser la couche/protocole QKD-TL.

La première option consiste en utiliser le même protocole que j'ai utilisé pour extraire des clés du réseau QKD à SECOQC, le protocole QKD-TL. Dans ce cas-là, les clés qui arrivent aux chiffreurs ne sont pas les clés qui ont été distribuées quantiquement. Ces clés sont générées aléatoirement d'un des cotés du lien et envoyées vers l'autre chiffrées en One Time Pad grâce au protocole Q3P qui utilise les clés quantiques. Ces clés sont alors injectées dans les chiffreurs Mistral.

Avantage : Permet de réutiliser une grande partie su software développé à SECOQC, il peut donc être implémenté assez vite.
Inconvénient : QKD-TL a été pensée pour être utilisée dans un réseau avec plusieurs sauts, il n'est pas du tout optimale pour un seul lien.

- **Option 2 :** Utiliser un protocole Q3P modifié.

A SECOQC, la sécurisation des liens était assurée par le protocole Q3P. Or se protocole était invisible pour les applications, il ne faisait que créer des tunnels dans le réseau quantique qui étaient sécurisés automatiquement. Cette sécurisation était gérée par une partie su software appelée Crypto Engine. Cette option impliquerait réécrire ce protocole de façon que les fonctions normalement gérées par le CryptoEngine soient assurées par les chiffreurs Thales.

Avantage : Bien plus optimal à la sécurisation d'un lien unique.
Inconvénient : On ne dispose pas du code source du Q3P, le réécrire pourrait impliquer une énorme charge de travail.

Vendredi 12 décembre une réunion est prévue avec les responsables du projet aux locaux de Thales à Colombes. Pendant cette réunion je vais présenter à l'équipe Thales ces deux options d'implémentation et la charge de travail qu'impliquent. Cette réunion devrait marquer la fin de mon stage.

3. Etude du chiffrement entropique

Parallèlement aux principales missions techniques j'ai réalisé une étude bibliographique de la possibilité d'utiliser une technologie expérimentale appelée chiffrement entropique afin de profiter des clés issues d'un réseau QKD.

Il s'agit d'un chiffrement qui garantit qu'aucune fonction du message en clair ne peut être déduite du message chiffré si l'entropie du message en clair est suffisamment élevée.

En notation mathématique, on dira que un chiffrement Y() est (t, ε) entropiquement sûr , si pour une entropie minimale d'au moins t, pour tout adversaire A et pour toute fonction f(), il existe un adversaire A' tel que :

$$\left| \Pr[\mathcal{A}(Y(X)) = f(X)] - \Pr[\mathcal{A}'() = f(X)] \right| \leq \epsilon$$

Cet objectif peut être atteint avec des clés beaucoup plus courtes que la longueur du message à transmettre. Ces caractéristiques sont idéales pour le chiffrement de clés issues d'un réseau QKD (dont leur entropie est très élevée) afin de pouvoir les transmettre en dehors du réseau. Ce chiffrement serait donc une alternative au One Time Pad pour pouvoir accéder à ces clés.

J'ai conclu que les études en ce domaine restent surtout au niveau théorique. On ne connaît pas d'algorithmes entropiques pratiques présentant une sécurité prouvée qui soient utilisables dans les réseaux quantiques actuels. Certains mécanismes ont été cependant identifiés pour générer ces algorithmes de chiffrement, basés sur des graphes et des fonctions XOR universelles.

III. Les apports du stage

1. Difficultés rencontrées

Mes plus importantes difficultés sont venues du fait que j'étais le seul à travailler dans le développement de mon application, du coup si j'étais bloqué par quelque chose que techniquement je ne savais pas comment faire je n'avais personne à qui demander son avis. Ceci a souvent ralenti mon travail car quelquefois il m'a fallu quelques jours pour résoudre un problème que quelqu'un avec plus d'expérience aurait sans doute trouvé rapidement. De plus le fait d'être tout seul impliquait une responsabilité totale dans le bon déroulement du développement.

Une autre source de difficultés a été le fait de travailler avec un délai clair et incontournable. L'application devait être prête pour le 8 octobre absolument. Ceci a provoqué qu'au début je me suis senti un peu dépassé par le volume de travail que j'avais à faire et je ne savais pas par où commencer. Ceci s'est reproduit les jours avant la démo, car je n'avais que deux jours pour faire marcher l'application à Vienne.

La démonstration a entrainé aussi une bonne dose de stress, car tout mon travail depuis mai se jouait en 5 minutes devant plus de 200 personnes incluant la presse et les plus grands experts au monde en cryptographie quantique. De plus des milliers de personnes suivaient la démonstration en live sur internet.

Initialement j'ai aussi trouvé quelques difficultés à gérer mon temps. Pendant les premiers mois il y avait beaucoup de travail à faire et souvent je sortais trop tard du bureau car je voulais à tout prix terminer mon travail avant de partir.

L'obtention du téléphone a aussi entrainé un problème car une fois acheté (sur internet) le délai de livraison a été inexplicablement long. Du coup j'ai dû continuer à tester dans l'émulateur pendant des semaines quand il s'imposait de tester sur le vrai téléphone. Plus l’application serait complexe et plus l'origine des éventuels problèmes serait difficile à repérer.

Le fait de travailler en coordination avec l'équipe ARC a entrainé aussi des difficultés, car mon travail dépendait du leur pour fonctionner. C'est à dire que si l'équipe à Vienne n'avançait pas j'étais plus ou moins bloqué et donc je ne pouvais pas avancer non plus. Par contre quand ils faisaient un grand pas j'avais beaucoup de travail à faire pour adapter mon application à leur travail. Souvent j'ai dû contourner un certain point ou attendre pour le traiter car sans le software de Vienne je ne pouvais pas l'aborder. Les releases de software avaient souvent trop de bugs ou leur mode de fonctionnement n'était pas expliqué nulle part, ce qui ralentissait mon travail. De plus le système de tickets était parfois lent et quelquefois une réponse à un doute essentiel pour continuer mon travail arrivait une semaine après l'avoir posé.

La plupart de ces problèmes m’ont cependant permis de développer des compétences certaines.

2. Solutions apportées et compétences acquises

Tout d'abord ce stage m'a permis d'améliorer énormément mes capacités techniques en matière d'administration UNIX, MAC OS et réseaux IP, et de développement C, Java, Swing et J2ME, qui s'imposaient pour le développement de l'application.

Le fait d'être le seul à y travailler m'a permis d'acquérir une grande autonomie dans mon travail et d'apprendre à « me débrouiller », sans attendre que d'autres solutionnent mes problèmes. Quand j'étais bloqué par un obstacle j'ai appris à chercher et à trouver moi même des solutions, en consultant avec mes collègues du département, en visitant la bibliothèque ou en cherchant pendant des longues heures sur internet. De plus j'ai pris l'habitude de prendre souvent l'initiative, car finalement la plupart des décisions techniques étaient ma responsabilité.

J'ai développé une grande rigueur dans mon travail, imposée par les délais et les objectifs. J'ai également appris à bien gérer mon temps et à planifier mes taches, en créant des programmes clairs de travail et des objectifs progressifs à atteindre. J'ai pris l'habitude de gérer des volumes de travail très variables selon les jours. De plus pendant la démonstration j'ai acquis une bonne gestion du stress qui a priori n'était pas évidente, vues les circonstances.

Le travail en coordination avec Vienne m'a donné une expérience de travail dans une équipe internationale dont les parties ne travaillent pas nécessairement de la même manière, au même rythme ou avec les mêmes priorités. Il a fallu être patient et comprendre d'autres façons de travailler. De plus j'ai appris à me coordonner avec des gens qui ne travaillent pas dans le même environnement que moi et avec qui la communication n'est pas toujours évidente. J'ai appris à comprendre l'interdépendance dans une équipe de travail et les problèmes que peut provoquer. J'ai aussi développé des qualités de communication scientifique qui s'imposaient pour bien se comprendre. De plus j'ai pu connaître le fonctionnement d'un projet internationale à grande échèle: les enjeux économiques, l'établissement des partenariats et le financement, la complexité de l'organisation, etc.

IV. Conclusion

Ce stage m'a permis d'être au cœur d'un projet à grande échelle qui a révolutionné l'état actuel de la cryptographie quantique. De plus j'ai pu développer des compétences certaines : l'autonomie, l'initiative, une capacité à s'adapter, des aptitudes variées, une gestion du stress, des qualités de communication scientifique, une rigueur dans les délais et les objectifs, et des compétences spécifiques dans mon domaine.

A titre de conclusion, il me semble intéressant de mettre en évidence les questions actuelles qui se posent sur l'avenir de la cryptographie quantique. Le succès du projet SECOQC prouve que la technologie est en train de développer un degré de maturité suffisant pour que les physiciens commencent à laisser la place aux ingénieurs, et de plus en plus d'entreprises commencent à s'intéresser à la technologie, comme le prouve le projet SEQURE de Thales. La problématique commence peu à peu à se déplacer du « comment construire des réseaux quantiques » à « comment les utiliser ». Les réseaux commencent donc à être prêts, il reste à développer des protocoles et des applications qui les utilisent pour sécuriser des communications réelles.

Je suis fier d'avoir été un des premiers à le faire.

V. Bibliographie

[1] O. Maurhart, M. Dianati et R. Alléaume."D-NET-07 Evaluation Report on the Protocols of the QKD Network", Technical Report, 20 avril 2007.

[2] M. Dianati, R. Alléaume, M. Gagnaire et X. Shen. "Architecture and Protocols of the Future European Quantum Key Distribution Network".

[3] M. Dianati et R. Alléaume. "Architecture of the SECOQC Quantum Key Distribution Network".

[4] A. Poppe, M. Peev and O. Maurhart "Outline of the SECOQC Quantum Key Distribution Network in Vienna", International Journal of Quantum Information, World Scientific Publishing Company, 25 février 2008.

[5] M. Peev, O. Maurhart, Th. Länger, Th. Lorünser, L. Salvail, R. Alléaume, M. Dianati, A. Marhold, A. Poppe, "Field Test of the SECOQC Quantum-Key-Distribution Network in Vienna"

[6] J. Bouda , S. Jank, O. Maurhart, R. Nagarajan, J.Pilz, P. Pluch. "Specification of the Key Store", Technical Report , Juin 2006.

[7] J. Bouda , S. Jank, O. Maurhart, R. Nagarajan, J.Pilz, P. Pluch. "Supporting Cryptographic Protocols for Q3P", Technical Report , Juin 2006.

[8] J. Bouda , S. Jank, O. Maurhart, R. Nagarajan, J.Pilz, P. Pluch. "Specification of the Cryptographic Engine", Technical Report , Juin 2006.

[9] O. Maurhart, A. Happe and T. Themel "QKD-TL Key Generation API", 22 avril 2008.

[10] L. Salvail, "Classical Post-Processing in SECOQC", Technical Report, 18 novembre 2005.

[11] P. Somlo, "Unconditional Authentication: An Overview".

[12] O. Maurhart. "SECOQC Demo-Network Configuration 0.2.1", 22 Septembre 2008.

[13] V. Shoup. "On Fast and Probably Secure Authentication Based on Universal Hashing", 4 décembre 1996.

[14] M. Fitzi "General Authentication Framework for QKD".

[15] Y. Dodis, A.Smith. "Entropic Security and the Encryption of High Entropy Messages", 1er septembre 2004.

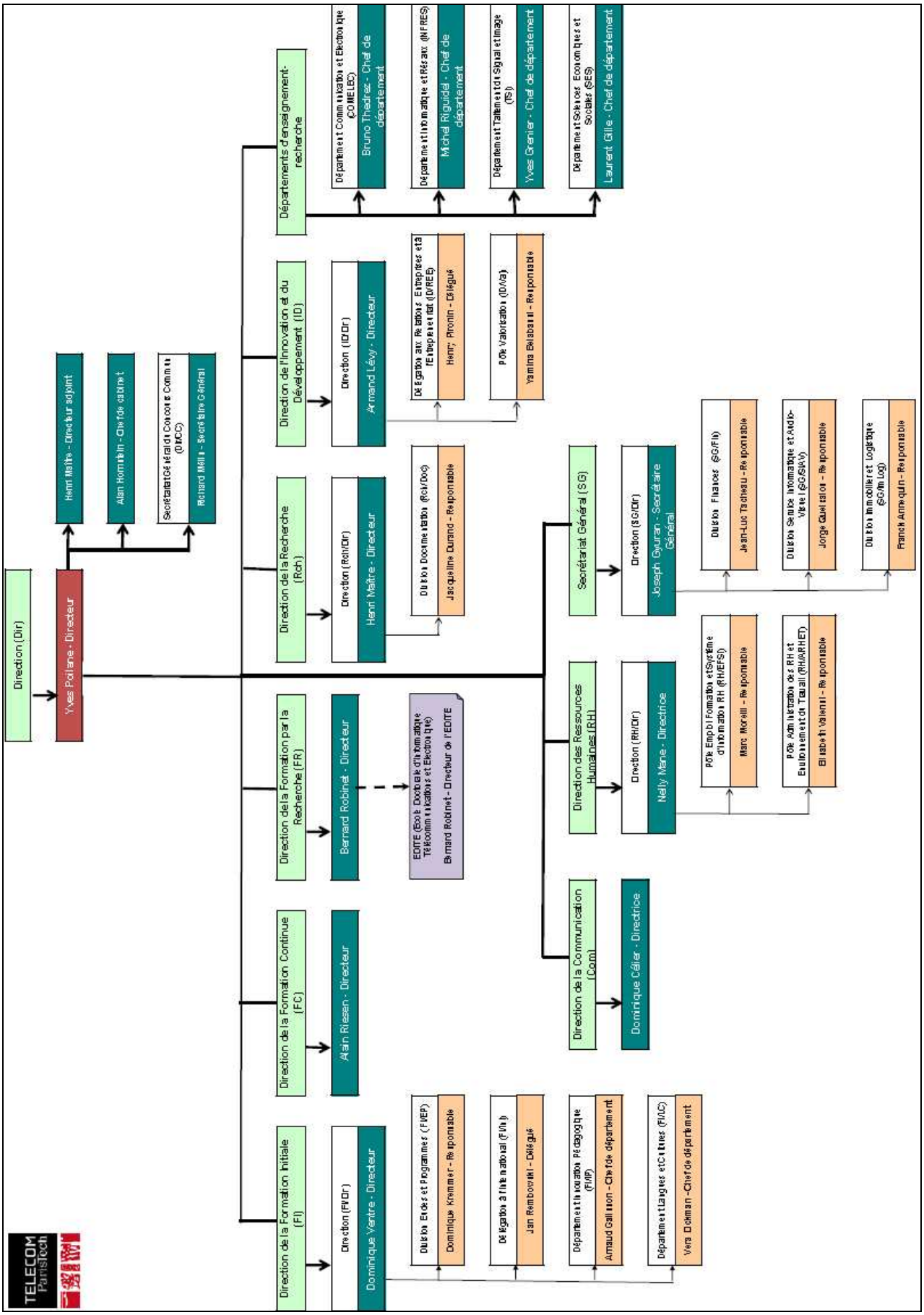
[16] A. Russell, H. Wang "How to Fool an Unbounded Adversary With a Short Key", IEEE Transactions on Information Theory, Vol. 52, N. 3, Mars 2006.

VI. Glossaire

- **AES :** Advanced Encryption Standard. Algorithme de chiffrement symétrique standardisé.
- **Evaluation Hash :** Algorithme d'authentification basé sur l'interprétation du message en clair comme un polynôme M(x) et du message authentifié comme M(k), k étant la clé d'authentification.
- **HMAC:** Keyed-Hash Message Authentication Code. Algorithme d'authentification calculé en utilisant une fonction de hachage cryptographique en combinaison avec une clé secrète.
- **QKD:** Quantum Key Distribution. Distribution de clés de chiffrement grâce à des méthodes quantiques.
- **QKD-TL :** QKD Transport Layer. Couche de transport du réseau QKD SECOQC et en même tant protocole qui la gouverne.
- **Q3P :** Quantum Point-to-Point Protocol. Protocole qui gouverne la couche liaison du réseau QKD SECOQC.
- **OTP:** One Time Pad. Algorithme de chiffrement où le message est combiné (XOR) avec une clé aléatoire qui n'est jamais réutilisée de même longueur que celui-ci.
- **SECOQC :** Development of a Global Network for Secure Communication based on Quantum Cryptography. Projet européen visant à déployer des applications sécurisées sur un réseau global de distribution de clés quantiques.
- **SEQURE:** Symmetric Enrcyption with Quantum key Renewal. Projet du groupe Thales en partenariat avec Telecom ParisTech et l'Institut d'Optique, visant à mettre en œuvre un système opérationnel de cryptage symétrique dont le renouvellement de la clé sera assuré par un protocole quantique.

VII .Annexes

Annexe I. Organigramme de Telecom ParisTech

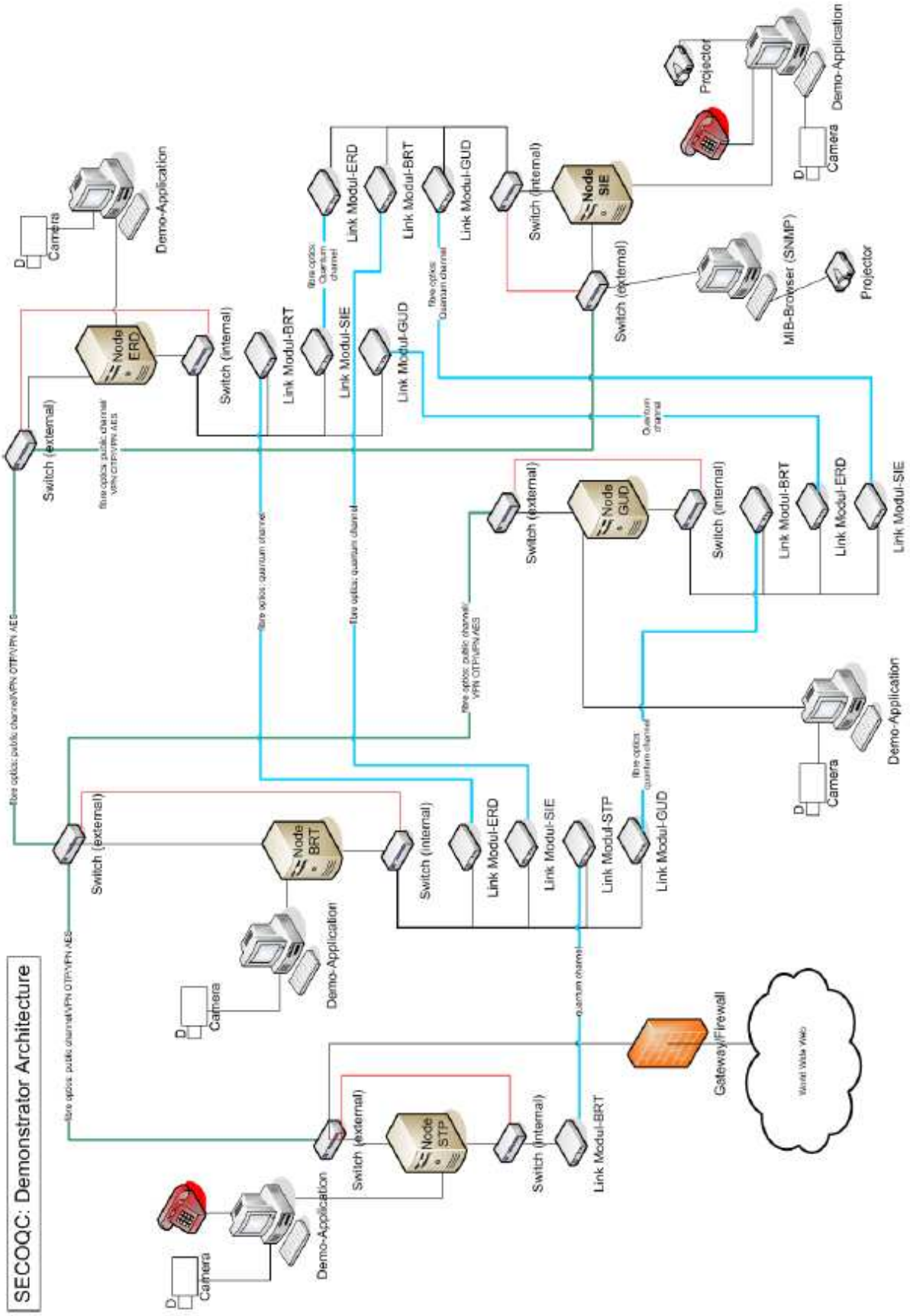


Annexe II. Liste des entreprises et institutions impliquées dans le projet SECOQC.

Pays	Entreprise / Institution
Australia	Quantum Communication Victoria, University of Melbourne.
Austria	Austrian Research Centers GmbH
	University of Vienna
	Aventec Handels, Produktions und BeratungsgesmbH
	Steinbeis Transfer Center
	University Of Klagenfurt
	Bearingpoint Infonova Gmbh
	Siemens AG Austria
Belgium	Université Libre De Bruxelles
Czech Republic	Palacky University, Olomouc
Denmark	University Of Copenhagen
	University Of Aarhus
European Union	Community Research and Development Information Service
Finland	Nokia Siemens Networks
France	CNRS, Université De Nice
	CNRS, Université De Orsay
	Smart Quantum
	Thales
	Ecole Nationale Supérieure Des Télécommunications
	Thales Communications
Germany	Ludwig-Maximilians Universität München
	University Erlangen-Nuernberg
	Techn. Universität Darmstadt
	Heinrich Heine Universität Düsseldorf
	Universitaet Karlsruhe (Th)
	Ernst & Young AG

Italy	Consiglio Nazionale Delle Richerche, Bologna
	Politecnico Di Milano
	Scuola Normale Superiore, Pisa
	Universita' Degli Studi Di Pavia
Russian Federation	Biometric Technologies, Ltd.
Sweden	Kungl Tekniska Högskolan, Royal Institute of Technology
Switzerland	Id Quantique SA
	University Of Geneva
	Université De Lausanne
United Kingdom	Heriot-Watt University
	University Of Cambridge
	Toshiba Research Europe Ltd.
	University Of Sheffield
	University of Bristol
	Hewlett-Packard Ltd
	University of Warwick
	QinetiQ Limited

Annexe III : Architecture du réseau SECOQC (sauf lien Freespace)



QKD Network Demonstration and Conference, October 8-10, 2008

Information Society Technologies

TIME	**WEDNESDAY** (Siemens)	**THURSDAY** (Technical Museum Vienna)	**FRIDAY** (Technical Museum Vienna)
9:00		**Keynote** *Artur Ekert – University of Cambridge and National University of Singapore*	**Invited and Contributed Talks** Invited: Differential Phase Shift Quantum Key Distribution *Yoshihisa Yamamoto – Stanford* Invited: Are QKD systems really useful (in practice)? *Hoi-Kwong Lo – Toronto* Device-Independent QKD *Antonio Acin – ICFO Barcelona* A novel single-mode quantum dot single photon source *Jean-Michel Gerard – Grenoble*
9:30	**Registration + Welcome Coffee**	**Security** Fundamentals of Quantum Information Security *Renato Renner – ETH Zürich* Security of Practical QKD Systems *Norbert Lütkenhaus – Waterloo*	
10:00	**Welcome Statements + Introduction + Film**		
10:30	**SECOQC QKD Network Demonstration**	Coffee Break	Coffee Break
11:00		SECOQC Prototype – Architecture *Oliver Maurhart – ARC* **Standardisation Initiative:** Novel Applications and Standardisation *Thomas Länger – ARC* ETSI Industry Specification *Gaby Lenhart – ETSI*	**Contributed Talks** Entanglement based QKD with 2 free-space optical links *Chris Erven – Waterloo* Practical scheme fibre-optical QKD with polarization qubits *Jean Pierre vonderWeid – PUC-Rio de Janeiro* Sidebands modulation scheme with dispersion compensation *Nicolas Pelloquin – Smartquantum* Field trial of diff.-phase-shift QKD using up-conversion detection *Toshimori Honjo – NTT*
11:30	**Questions to the Scientific Podium** *SECOQC Key Researchers*		
12:00	**Résumé** *Momtchil Peev – ARC*	**Poster session** | **ETSI ISG Kick-Off** *Members*	
12:30	**Lunch Break**		
14:00	Using QKD techn. to build secure networks *Romain Alléaume – ENST*	**QKD-Devices:** *G. Ribordy / M. Legré – IdQuantique* *Nicolas Gisin – GAP Univ. of Geneva* *Andrew Shields – Toshiba Research* *A. Zeilinger / H. Hübel – Univ. Vienna* *Philippe Grangier – CNRS Paris* *John Rarity – University of Bristol* *Harald Weinfurter – LMU Munich*	**Development of Novel Detector Schemes** Silicon Single Photon Avalanche Diodes for QKD *Sergio Cova – Politecnico di Milano* InGaAs/InP Single-Photon Avalanche Diode Detectors for QKD *Gerald Buller – Univ. Edinburgh* High-performance SPAD for QKD Networks *Mark Itzler – Princeton Lightwave Inc.* Superconducting nanowire photon number resolving detector *Francesco Marsili – Eindhoven* Rebirth of InGaAs for high bit rate single photon applications *Zhiliang Yuan – Toshiba* Telecom-band, sinusoidally gated APD for GHz clocked systems *Naoto Namekata – Nihon Univ.*
14:30	**Area specific foci** QKD in the context of **European strategies** *Jacques Bus – EU*		
15:00	QKD in **USA and Canada** *Richard Hughes – LANL, USA*		
15:30	Toward new generation - QKD in **Japan** *Masahide Sasaki – NICT, Japan* QKD in **Singapore** *Artur Ekert – Univ. of Singapore*		
16:00	Coffee Break	**Poster session** + Coffee + Discussions	Coffee Break
16:30	**Future aspects** The Future of Quantum Information *Anton Zeilinger - Vienna*		**SECOQC internal meeting** General Assembly
17:00			
17:30	Future Trends in QKD *Grégoire Ribordy – IdQuantique* QKD – A Roadmap to the Future: *Experts panel*		
18:00 21:30		**Conference reception**	online: **www.secoqc.net**