Fiche d'avancement à mi-parcours

Nom du projet : VISQ, VoIP avec Sécurité Quantique .....

Chef de projet / Ecole : Patrick Bellot, ENST .....

Autres écoles participantes : ENST/INFRES et ENST/COMELEC .....

RAPPEL DES OBJECTIFS DU PROJET

Ce projet est l'étude de la faisabilité actuelle d'un lien téléphonique utilisant la Voix sur IP (Voice over IP, VoIP), inconditionnellement sécurisé grâce à la cryptographie quantique. Inconditionnellement sécurisé signifie ici qu'un attaquant disposant de moyens illimités (en moyens de calculs, en temps, etc.) ne pourra pas avoir une connaissance, même partielle, de la communication protégée. La seule attaque possible sur un tel système est l'attaque de type « Denial of Service » empêchant le fonctionnement de la ligne en la coupant par exemple.

Si les principes physiques de la cryptographie quantique sont connus depuis longtemps, ses différents protocoles et technologies d'implémentation font encore l'objet d'une recherche active. Il apparaît opportun de disposer aujourd'hui d'un démonstrateur de validation opérant aux longueurs d'ondes des télécommunications, intégrant les traitements matériels et logiciels et la couche applicative, dans une approche de sécurité globale (optique, électronique et logicielle).

Le projet est celui d'une plate-forme de recherche et de démonstration pour la sécurisation de la voix sur IP par la cryptographie quantique.

Le projet comporte trois sous-projets correspondant à trois niveaux physiques:
- la couche « optique quantique » ;
- la couche « interface électronique et génération d'aléa » ;
- la couche « logicielle ».

AVANCEMENT DES TRAVAUX PAR RAPPORT AU PROGRAMME PRÉVU

L'avancement des travaux est conforme au programme prévu. Les travaux ont été menés par les trois sous-équipes impliquées avec communications régulières en réunion.

Couche « optique quantique »

Dans cette période, on a un avancement consistant premièrement de l'implémentation de l'émetteur (Alice) générant, par un modulateur électro-optique intégré unique, la constellation QPSK permettant la représentation antipodale des deux états binaires sur deux bases orthogonales conjuguées. Coté récepteur (Bob), on a suivi une progression en deux voies :

- La première consiste à réaliser la plate-forme VISQ en utilisant la technologie éprouvée de comptage de photons : réalisation d'un récepteur à délai interférométrique utilisant des compteurs de photons à 1550nm ; mesure du contraste avec des états cohérents : un taux d'erreur quantique (QBER) asymptotique de quelques % semble accessible à notre montage en l'état ; mesure des constantes de temps de diffusion de la phase et de la polarisation montrant une stabilité en boucle ouverte de quelques minutes, dans un environnement thermique et phonique protégé ; synchronisation de l'émission et de la réception optique et optimisation des fenêtres d'ouverture des photo détecteurs, inférieures à 10ns, pour minimiser les comptes obscures et la réduction de contraste qui en résulte.
-
- La deuxième voie consiste à réaliser une expérimentation sur un montage super homodyne susceptible d'augmenter le débit, de relaxer les contraintes de stabilisation de la phase et de la polarisation, de transmettre la synchronisation numérique et enfin d'améliorer le taux d'effacement. Exploration des caractéristiques, potentialités et limites atteignables avec des montages super homodynes : gain en vitesse, gain de mélange, écrasement du bruit thermique, mécanismes d'auto-référenciation en phase

optique, en polarisation et en horloge numérique. Etudes sur les aspects de décision post-détection. Impact du transfert des effacements liés à l'efficacité quantique en erreurs classiques (BER) liées aux décisions post-détection. Coexistence du BER et QBER.

Les difficultés rencontrées sont de deux ordres :

- Même si on travaille avec une configuration différentielle en multiplexant une référence de la porteuse optique forte, des fluctuations aléatoires de phase et polarisation entre le signas quantique et la référence pour le (super)homodynage sont inévitables dans la liaison, notamment dans l'interféromètre chez Bob. Donc on a commencé a étudier des configurations de conception des signaux et schémas de détection et traitement du signal post détection pour une éventuelle contreréaction optoélectronique.

- Une autre difficulté rencontrée c'est le taux d'extinction fini dans la référence forte, qui peut être plus intense que le signal quantique. On étudie actuellement des alternatives pour une solution pratique, tout en conservant le débit effectif.

On étudie actuellement la possibilité de implémentation d'un schéma de DSP sur le signal de post-détection, comme alternative a l'estimation de la phase en boucle ouverte.

Couche « interface électronique et génération d'aléa »

La carte d'interface électronique est tournée d'une part vers la couche logicielle et d'autre part vers la couche d'optique quantique :

- Interface logicielle \ carte matérielle. Le service d'interfaçage entre le logiciel et la carte VISQ est opérationnel. Du côté du logiciel, une bibliothèque C/C++ (Linux et Windows) présente une API pour construire une application cliente telle que BB84. La bibliothèque reçoit des commandes et renvoie des blocs de mémoire de 1 Mbit (par session). Du côté de la carte VISQ, des lectures / écritures rapides dans le FPGA Stratix ont été mises en place. Une fonction de génération d'aléa déséquilibré à 25 % de '1' grâce à l'algorithme R = R & (R >> 1) a été programmé en Verilog et VHDL et intégré dans le FPGA Stratix. La limitation actuelle concerne la vitesse de communication entre la carte et l'application distante, car le lien est de type USB. Le code actuel gère les sockets. Le travail en cours consiste à intégrer ethernet directement sur la carte VISQ. Pour cela, un driver ethernet ENC28J60 sous GNU/Linux est développé. Le network driver a été créé comme un pilote virtuel (localhost interface), mais il faut écrire le code lié à la partie matérielle.

- Interface avec les composants optiques. La première étape a consisté à définir les besoins du système de transmission optique : les signaux nécessaires à sa commande, les signaux à recevoir et à traiter. Nous avons défini les niveaux de tensions ainsi que les formes d'ondes, les fréquences de fonctionnement. Les signaux de commande d'Alice et de Bob ainsi que la gestion des données reçues (enregistrement dans une pile FIFO) sont programmé en VHDL, simulés et synthétisé dans un FPGA Stratix. Le FPGA ne pouvant générer que des signaux logiques, 3,3V - 0V, il a fallu créer une interface analogique pour adapter les niveaux de tensions, sans dégrader les signaux hautes fréquences. Nous avons testé un certain nombre de solutions différentes avant d'arriver à une solution satisfaisante. La carte d'interface est maintenant en cours de fabrication et sera testé avec le FPGA.

Du point de vue du générateur aléatoire dans la carte, nous avons réalisé un générateur d'aléa vrai, qui passe tous les tests du NIST. La rapidité du générateur s'appuie sur une structure originale en boucle ouverte. Le principe est d'utiliser la méta-stabilité dans l'échantillonnage d'une ligne de délais unitaires d'environ 25 ps. Le segment de la ligne qui présente la plus grande méta-stabilité sert de germe à un pseudo-générateur d'aléa. Le débit obtenu est égal à la fréquence d'horloge du FPGA, de l'ordre de 100 MHz. Ce générateur a été présenté conjointement avec le groupe de communications quantiques dans une communication à la conférence ECOC, et un article plus conséquent est en cours de rédaction.

Couche « logicielle »

La couche logicielle assure différentes fonctions :
- implémentation du protocole de cryptographie quantique BB84 ;
- stockage des clés inconditionnellement sécurisées ;
- distribution des clés inconditionnellement sécurisées ;
- expansion éventuelle des clés avec l'algorithme BBS ;
- application VoIP avec codage Vernam utilisant les clés ci-dessous.

Les algorithmes de ces différentes fonctions ont tous été implémentés en C/C++ et testés. Nous avons alors choisi une architectures en trois couches de serveurs. Trois serveurs sont présents chez Alice et les co-serveurs sont présents chez Bob. Chacun de ces serveurs est un programme indépendant et les serveurs communiquent par envoi de messages UDP ou TCP (*sockets*). Les trois serveurs sont :

- Le serveur BB84, sa fonction est d'attendre de l'interface électronique des données (qubits mesurés et bases des mesures) de l'ordre de 1 Mbits, puis d'effectuer le protocole BB84 afin d'en extraire une clé

inconditionnellement sécurisée dont la longueur dépendra des taux d'erreurs de la couche optique et de la présence éventuelle d'un espion. Ce serveur a été implémenté en suivant les algorithmes décrits dans la littérature. Nous avons ajouté une couche d'authentification basée sur les fonctions de hachage universelles de Wegman-Carter. Chaque fois que le serveur BB84 a produit 64Ko de clé, il demande au serveur de clés de les stocker.

- Le serveur de clés, ses fonctions sont multiples. D'abord, il reçoit les clés produites par le serveur BB84 sous forme de blocs de 64Ko. La taille de 64Ko a été retenue car le serveur de base de données MySQL propose un type BLOB (Binary Large Object) de cette taille. Les clés sont stockées et possèdent un identifieur unique sous la forme d'un entier. Nous avons, pour des facilités d'implémentation, limité le contenu de la base de données à 256 enregistrements de 64Ko, ce qui correspond à une avance d'environ 1h30. Le serveur de clé est aussi responsable de la distribution de clés au serveur applicatif VoIP après une négociation de Qalité de service (QoS). Si le stock de clé ou le débit de production de clé est insuffisant, il peut être nécessaire d'expanser les clés produites. Le meilleur algorithme pour cela semble est BBS et il est implémenté dans le serveur de clés.

- Le serveur VoIP, ce serveur implémente la norme GSM 06.10 parce qu'elle a un débit maximal de seulement 13 Kbits/sec dans chaque direction (soit 26Kbits/sec au total) et parce que les paquets de données envoyés sur le réseau ont une taille fixe, ce qui facilite la gestion des clés de codage. Le serveur VoIP demande ses clés au serveur de clé et code les paquets de données en utilisant le codage de Vernam (seul codage inconditionnellement sécurisé).

Le choix d'avoir trois serveurs à chaque extrémité a été dicté par des considérations de disponibilité. Par exemple, il ne faudrait pas que la VoIP soit bloquée en l'attente d'un message relatif au stockage des clés. L'inconvénient est la multiplicité des canaux de communications. Ainsi, le serveur de clés doit communiqué avec son homologue mais aussi avec le serveur BB84 en dessous de lui et avec le serveur VoIP au-dessus de lui et avec le serveur de base de données MySQL.

Pour les mêmes raisons, chaque serveur est composé de plusieurs *threads* (processus légers). Par exemple, le serveur de clés a une thread recevant les messages du serveur BB84 et stockant les clés dans la base de données MySQL. Il possède aussi une deuxième thread recevant les messages de demande de clés de la part du serveur VoIP.

Les difficultés rencontrées concernent la mise au point de protocoles entre les différents acteurs du système. Nous sommes entrain d'y travailler et une première version du système devrait être testée fin septembre.

EVENTUELLEMENT, DIFFICULTÉS RENCONTRÉES

(SCIENTIFIQUES, ORGANISATIONNELLES , ADMINISTRATIVES…)

Pas de difficultés particulières dans le domaine organisationnel ou administratifs.

Les diffcultés scientiofiques sont décrites contextuellement dans la section « Aspects scientifiques ».

VALORISATION DES TRAVAUX ENVISAGÉE

(PROJETS ANR, EUROPÉENS, BILATERAUX, COLLOQUES, WORKSHOPS, CONFERENCES…)

Le site WEB http://visq.enst.fr affiche l'état du projet.

Le générateur d'aléa a été présenté conjointement avec le groupe de communications quantiques dans une communication à la conférence ECOC, et un article plus conséquent est en cours de rédaction.

Un article commun sera élaboré dès que la plate-forme sera opérationnelle.

Un projet ANR-RNRT a été soumis pour permettre de faire vivre la plate-forme en collaboration avec des partenaires. Le projet n'a pas été retenu mais il est classé premier en liste d'attente.