Présentation & sujet de thèse

Développement d'un protocole pour l'échange de clé quantique et intégration à une bibliothèque logicielle

Thomas Prévost - I3S - MDSC

TABLE DES MATIÈRES

Présentation personnelle

Thomas Prévost - 23 ans

Badminton - randonnée - natation

Apprendre de nouvelles choses, intérêt scientifique

Informatique et programmation, intérêt pour la cyber

Formation

- PEIP aux Lucioles
- Ingénieur SI aux Templiers
  - Spécialité cyber sécurité
  - Préférence pour les matières scientifiques aux projets

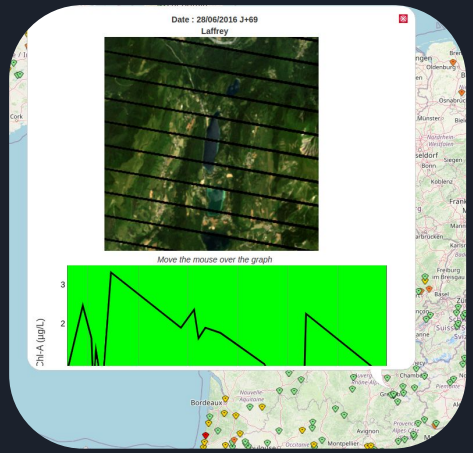
Formation

Double master MAE de management en dernière année

Expériences professionnelles

Stage de 1ere année

- Architecture et maintenance des systèmes
- Analyse des données scientifiques
- Maintenance des sites web de rendu des données scientifiques



eye on water, santé des lacs en Europe

ACRI ST

Hébergement des données de l'agence spatiale européenne

- Participation active à la recherche scientifique
  - Evolution du climat
  - Protection des océans
  - Agriculture responsable
  - ...

Stage de recherche en 3e année

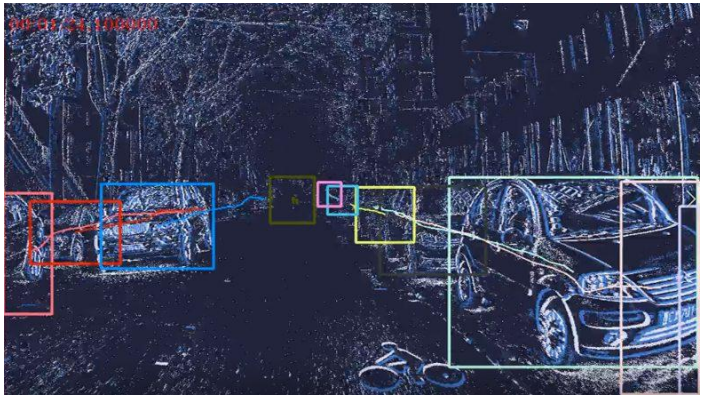
- Intégration d'algorithmes d'IA bio inspirés de type réseaux de neurones à spikes (avec Benoît Miramond)

- Traitement des données en provenance d'une caméra évènementielle

- Intégration sur une cible embarquée (partenariat avec Renault)

LABORATOIRE D'ELECTRONIQUE ANTENNES ET TELECOMMUNICATIONS

Equipe EDGE (réseaux de neurones embarqués)



Apprentissage en entreprise (4A et 5A)

- DevSecOps Cloud (Azure) OpenBackend C++

- Maintenance des backends de réservation

amadeus

Présentation du sujet de thèse

Bruno Martin (I3S) et Olivier Alibart (InPhyNi)

Intégration d'algorithmes de distribution quantique de clé à une librairie

- Encapsulation d’un protocole d’échange de clés de sécurité garanti par les lois quantique
- Protocoles BB84, E91 ou BBM92

- Intégration à une bibliothèque cryptographique (comme OpenSSL ou IPSec)
- Accès transparent pour l’utilisateur à la sécurité quantique

L’art de partager un secret…

Comment transmettre un secret à quelqu’un que je ne connais pas ?

- Il faudrait pouvoir chiffrer les messages…
- …Mais comment se mettre d’accord sur l’algorithme et la clé de chiffrement ?

L’art de partager un secret…

Comment transmettre un secret à quelqu’un que je ne connais pas ?

clés publiques et privées

clé publique

Génère clé symétrique

clé symétrique chiffrée à l’aide de la clé publique

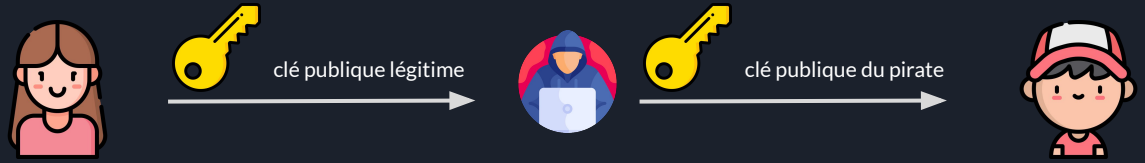
Déchiffre la clé symétrique à l’aide de la clé privée

échangent des messages chiffrés avec la clé commune

Inconvénients des systèmes à clé publique

- Lent et gourmand en ressources

- Attaques de l'homme du milieu: comment garantir l'authenticité de la communication ?

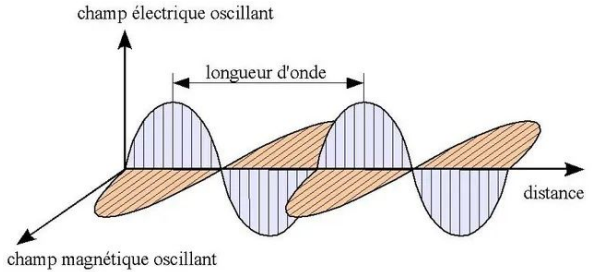


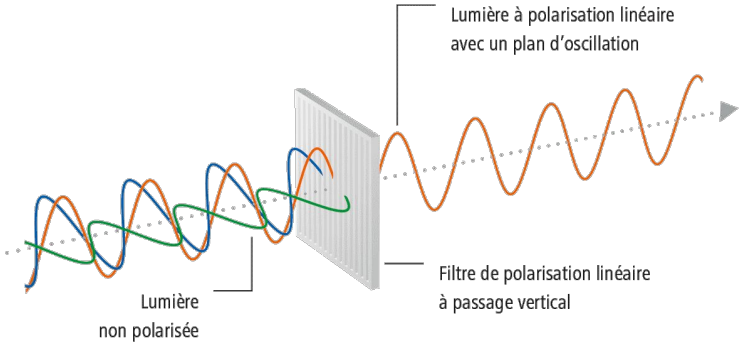
- Vulnérables aux attaques d'un ordinateur quantique (l'algorithme de Shor permet de retrouver la clé privée depuis la clé publique)

  -> "Harvest now, decrypt later"

Introduction à la sécurité quantique

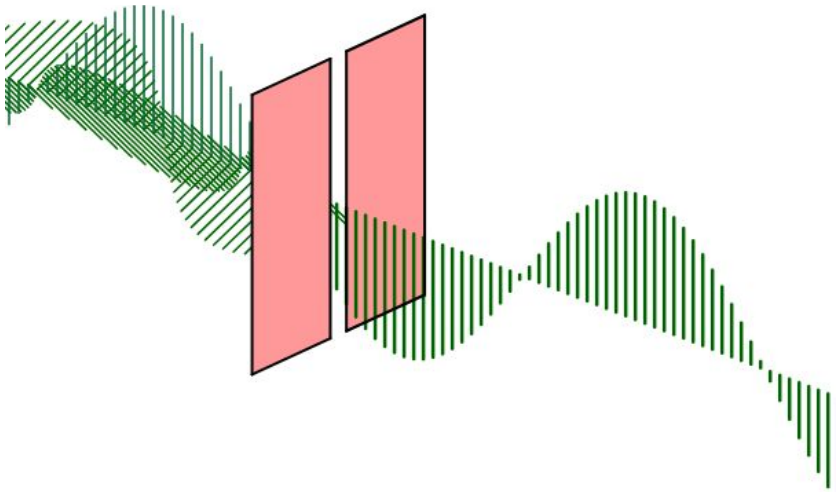
Polarisation: direction d'oscillation du champ électrique et du champ magnétique





Propriété quantique de la polarisation

Un seul filtre polarisant

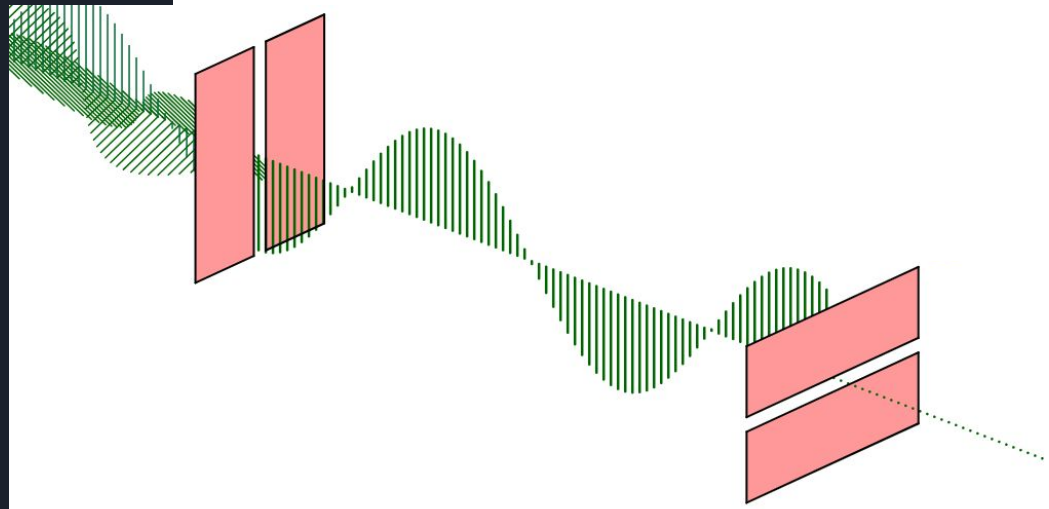


Propriété quantique de la polarisation

2 filtres orthogonaux

Expérience reproductible avec les lunettes de cinéma 3D !

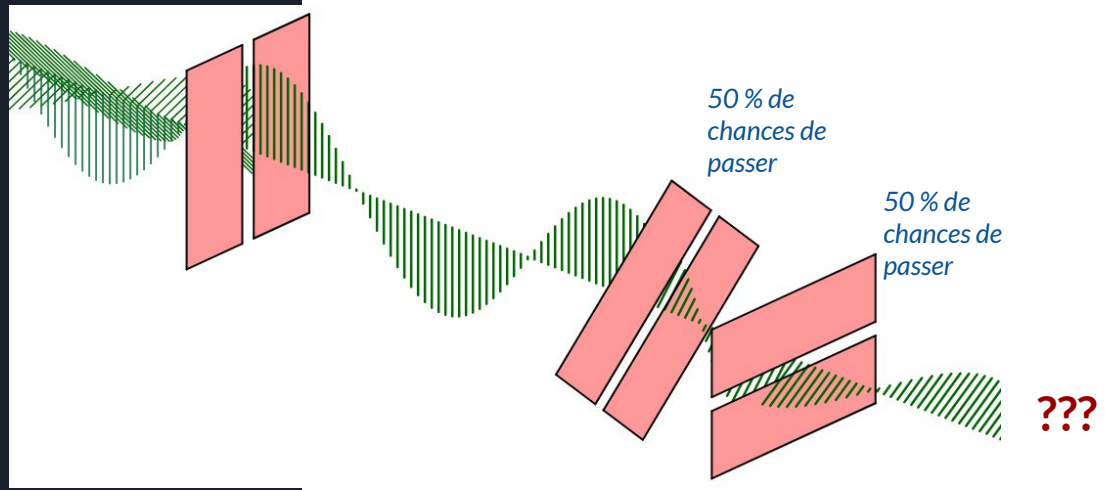
Notre premier filtre ne laisse passer que la polarisation verticale, puis le second ne laisse passer que la polarisation horizontale…



Propriété quantique de la polarisation

Et avec un filtre intermédiaire orienté à 45° ?

C’est donc la mesure qui crée l’état



Sécurité de la transmission quantique d'un photon

(Pour les protocoles d'échange de clés BB84 comme E91)

- Un attaquant qui tenterait de lire un photon modifierait donc son état quantique (qubit), et serait donc détecté

- Intuition: **théorème de non-clonage**: il est impossible de cloner parfaitement l'état d'un qubit

Sécurité de la transmission quantique d'un photon

(Pour les protocoles d'échange de clés BB84 comme E91)

La sécurité repose donc non plus sur la difficulté calculatoire de retrouver un message, mais sur la détection pendant l'échange de clé d'un attaquant qui écoute le message

L'intérêt de la QKD est donc de proposer une confidentialité persistante parfaite

Limitations

Très complexe à mettre en oeuvre:

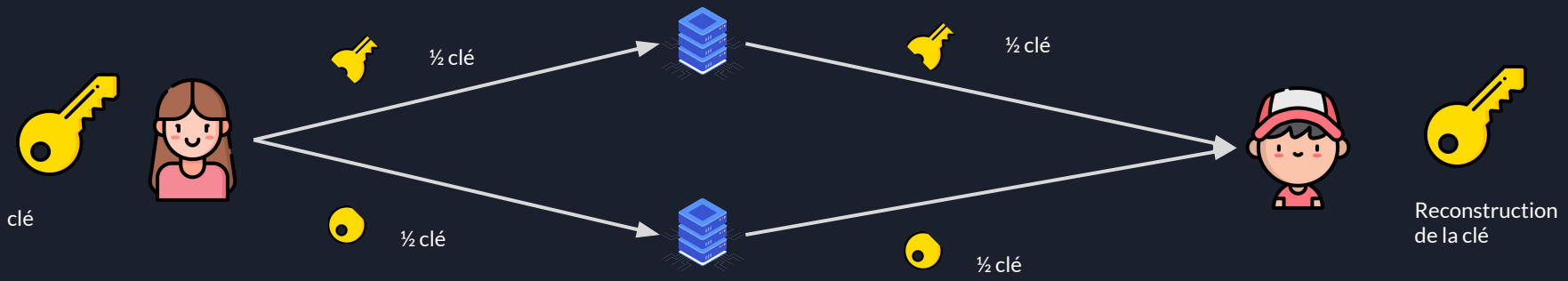
- Génération de photons uniques
- Attaques sur les détecteurs
- Obligation d'authentifier les 2 parties
- …

Application dans un protocole d’échange de clé quantique

Problème: les fibres ne peuvent transmettre les photons uniques qu’à une distance limitée (max 200 km)

Application dans un protocole d’échange de clé quantique

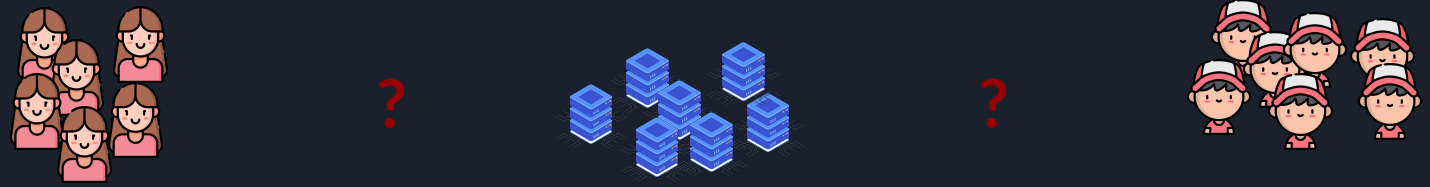
Création d’un protocole de routage en cas d’absence de lien direct:



Application dans un protocole d'échange de clé quantique

Création d'un protocole de routage en cas d'absence de lien direct:

- Comment passer de 2 utilisateurs à n x n sur le même canal ?



- Vérification formelle du protocole de sécurité *(ProVerif, Tamarin…)*

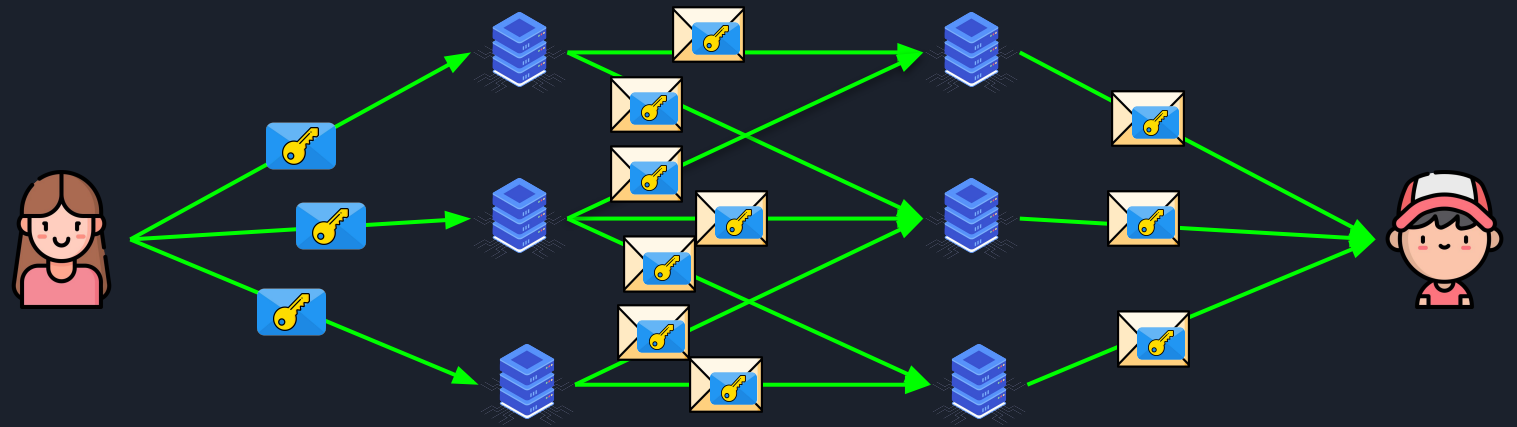
Solution: Partage de secrets récursif entre les noeuds intermédiaires

Le partage de secret de Shamir

Distribuer un partage à *n* personnes, de sorte qu'il faille au minimum *k <= n* partages pour retrouver le secret

- Générer un polynôme *P* aléatoire de degré *k-1* tel que *secret = P(0)*
- Distribuer les morceaux P(1), P(2), ..., P(n) aux différents acteurs
- Reconstruction du secret *P(0)* à partir de *k* morceaux par interpolation Lagrangienne

Solution: Partage de secrets récursif entre les noeuds intermédiaires



Canal sécurisé indépendamment par QKD

Clé / secret

Partage de Shamir, threshold = 51%

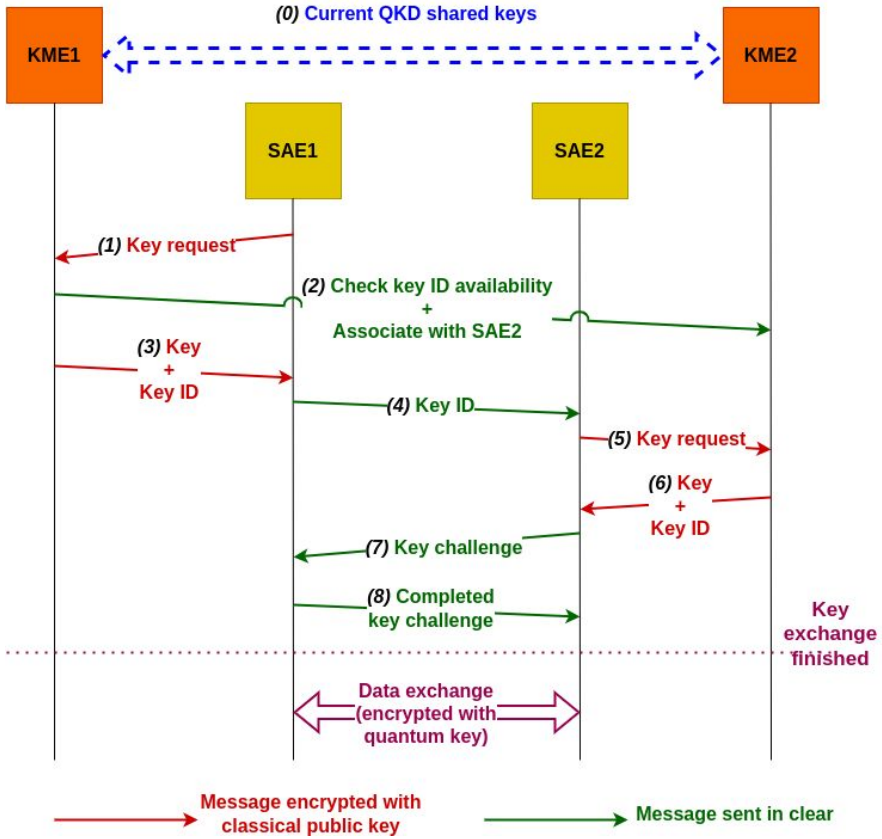
Application dans un protocole d'échange de clé quantique

Résumé

	Sécurité prouvée	Sécurité quantique	Confidentialité persistante parfaite
RSA/ECC			
Post-quantique			
Echange quantique de clé			

Démonstration: Intégration dans une bibliothèque cryptographique

- Intégration dans SSL/TLS via la bibliothèque RusTLS
- Démonstration d'une visioconférence chiffrée par le SSL/TLS modifié
- Rétrocompatible dans les 2 sens avec SSL/TLS classique
- Objectif: RFC
- Implémentation possible sur IPSec pour du tunneling cross-datacenters
- Respect de la norme ETSI GS QKD 014 v1.1.1

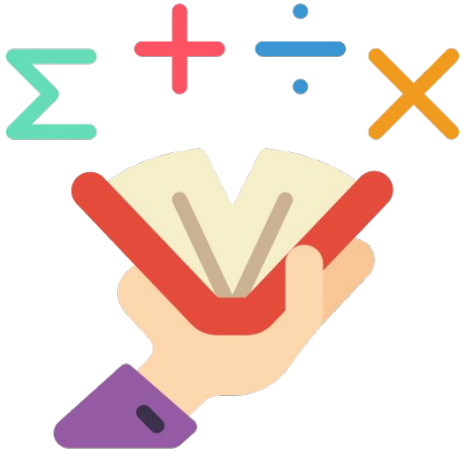


Souhait d’orientation du sujet de thèse

Orientation scientifique du projet

Sujet à la base orienté ingénierie

Je souhaiterais l'orienter vers son côté scientifique (physique quantique, mathématiques, analyse formelle…)



Conclusion

- J’aimerais profiter de cette opportunité pour apprendre le maximum sur la physique et la cryptographie

- J’espère passer un bon moment avec vous !

Merci !

Avez-vous des questions ?