Ref : 0011@2024-oct-09@16h53-CET@sc ; From : 0011@2023-nov-20@09h34-CET@sc ; Author : Serge Chaumette

Tous parcours / Informatique quantique

Fiche de TD / Cryptographie quantique

Serge Chaumette

Cryptographie quantique

Dans ce TD on s'intéresse à la **mise en œuvre d'une simulation de l'algorithme BB84** et de son utilisation.

Exercice 1 : vidéo et article de référence – *durée approximative totale : 30 minutes*

a. Visionner la vidéo référencée ci-dessous qui explique de manière simple le fonctionnement de B84
b. https://www.youtube.com/watch?app=desktop&v=OITZ24i5wX4
   durée approximative : 15 minutes

c. (re)lisez la section III (*Quantum Public Key Key Distribution*) de l'article original de Bennet et Brassard
   durée approximative : 15 minutes

Exercice 2 : préparation de la mise en œuvre – *durée approximative totale : 75 minutes*

Au vu de la vidéo et de ce que vous savez des *qbits* déterminez les processus et les classes d'objets qu'il sera nécessaire d'implémenter pour mettre en œuvre une simulation de l'algorithme BB84 et de son utilisation sans, puis avec présence d'un attaquant.

a. Lister (sous la forme de texte) les opérations nécessaires à la création et la manipulation d'un QBit
   durée approximative : 15 minutes
b. Implémenter le type QBit, i.e. les opérations listées en question a.
   durée approximative : 20 minutes
c. Ecrire un programme permettant de tester ces fonctions et effectuer le test
   durée approximative : 10 minutes
d. Implémenter la transmission d'un QBit entre deux processus (Alice et Bob) situés sur des machines différentes sur le réseau. Si vous n'êtes pas à l'aise avec la programmation réseau, vous pouvez utiliser des fonctions (Alice et Bob) au sein d'un unique processus.
   durée approximative : 30 minutes

Exercice 3 : mise en œuvre – *durée approximative totale : 55 minutes*

a. Mettez en œuvre la simulation de transfert d'une série de QBits telle que définie dans BB84. Ceci sera réalisé avec ou sans aspect réseau en fonction de l'approche que vous avez utilisée en question 2.d.
   durée approximative : 30 minutes

b. Déterminez le pourcentage de similarité entre les bits envoyés par Alice et ceux lus par Bob en l'absence d'attaquant
durée approximative : 10 minutes
c. Déterminez le pourcentage de similarité entre les bits envoyés par Alice et ceux lus par Bob en présence d'un attaquant (Eve)
durée approximative : 15 minutes

Exercice 4 : variantes (sans mise en œuvre) – *durée approximative totale : 25 minutes*

a. On interpose maintenant deux observateurs lors de la transmission (Eve et qui vous voulez). On calculera les résultats attendus avant de les obtenir par simulation (question 5.a)

b. On suppose maintenant trois polarisations possibles lors de la fabrication du qbit. On calculera les résultats attendus avant de les obtenir par simulation (questions 5.b)

Exercice 5 : mise en œuvre des variantes – *durée approximative totale : 60 minutes*

a. Mise en œuvre de la variante de la question 4.a
    1. Implémentez cette variante
        durée approximative : 10 minutes
    2. Mesurez le pourcentage de similarité entre les bits envoyés par Alice et ceux reçus par Bob en l'absence d'attaquant
        durée approximative : 10 minutes
    3. Mesurez le pourcentage de similarité entre les bits envoyés par Alice et ceux reçus par Bob en présence d'un attaquant (Eve)
        durée approximative : 10 minutes
b. Mise en œuvre de la variante de la question 4.b
    1. Implémentez cette variante
        durée approximative : 10 minutes
    2. Mesurez le pourcentage de similarité entre les bits envoyés par Alice et ceux reçus par Bob en l'absence d'attaquant
        durée approximative : 10 minutes
    3. Mesurez le pourcentage de similarité entre les bits envoyés par Alice et ceux reçus par Bob en présence d'un attaquant (Eve)
        durée approximative : 10 minutes

Exercice 6 : généralisation – *durée approximative totale : 30 minutes*

a. Etudiez la convergence du pourcentage de similarité lorsque le nombre d'observateurs tend vers l'infini dans le cas de deux polarités possibles et de deux valeurs possibles du qbit.

b. Etudiez la convergence du pourcentage de similarité lorsque le nombre d'observateurs tend vers l'infini dans le cas de P polarités possibles et de V valeurs possibles du qbit.