Road-Map TIPE

Mise en Situation :

Aujourd'hui, l'immensité du volume de données échangées et l'ampleur des enjeux qui y sont liés (sécurité bancaire, confidentialité, respect de la vie privée...) ainsi que la puissance de calcul croissante à dont nous disposons nous obligent à mettre en oeuvre des moyens de sécuriser nos échanges de données toujours plus sécurisés. L'avènement de l'ère de l'Ordinateur Quantique pourrait mettre en péril tous les moyens actuellement mis en oeuvres. Toutefois, de nouvelles méthodes faisant appel à la mécanique quantique pourraient nous permettre d'atteindre un niveau de sécurité proche de la perfection, au prix de forte contraintes techniques de mise en place.

1 Préambule :

- Rapide présentation de la Cryptographie
- Notion de Protocole
- " Cassabilité " d'un Protocole

2 L'Ordinateur Quantique : Arme Nucléaire de la Cryptographie

L'Algorithme de Shor : Fondement de la problématique → possibilité de casser tous les protocoles Classiques actuels.

- Implémentation
- Mise en évidence de la nécessité de l'Ordinateur Quantique
- Présentation de données statistiques (matplotlib)
- Animations ? (haute valeur ajoutée mais reste à voir ce qui serait intéressant à faire)

3 La Révolution de la Cryptographie Quantique :

- Rapide présentation des fondements de la Physique Quantique → inégalités d'Heisenberg, fonction d'onde, modèle probabiliste...
- Le Protocole E91 → principe de fonctionnement
- Le Phénomène d'Intrication Quantique
  - Vulgarisation du Principe
  - Etude Théorique du Phénomène