Le quantum computing a une histoire relativement jeune puisque qu'il a été théorisé dans les années 80. Il correspond à l'application de le théorie quantique, décrivant les interactions entre éléments à l'échelle de l'infiniment petit (i.e. comment les atomes et autres particules plus petites interagissent entre eux), appliqué au domaine du calcul informatique. Par conséquent, le quantum computing correspond à l'utilisation de particules à l'échelle quantique (atomes, électrons, photons), en vue d'améliorer les performances de nos dispositifs informatiques.

A mesure que les technologies avancent l'AGI intelligence artificielle generale et le QC quantum computing deviennent des sujets brulants , si ces innovations offrent de grandes opportunites , elles posent aussi des risques notamment pour la securite des donnees

I. L'impact du Quantum computing

le quantum computing utilise des pricipes de la physique quantique qui permettent de resoudre certains problemes beaucoup plus rapidement qu'un pc (ordinateur classique) . l'un des grands defis pour la cryptographie est que les ordinateurs quatiques pourraient dechiffrer des donnees proteges par des systemes actuels

Exemple:

l'algorithme de Shor permet de factoriser des grands nombres en quelques secondes ce qui brise la securite du RSA un systemes de chiffrement les plus utillises aujoud'hui

II.les risques de l'AGI

L'AGI ((intelligence artificielle generale) pourrait egalement representer une menace pour la securite des donnees . Contrairement a l'IA actuelle , qui est specialisee dant des taches precises , L'AGI pourrait comprendre et manipuler des algorithmes de chiffrement de maniere beaucoup plus efficace

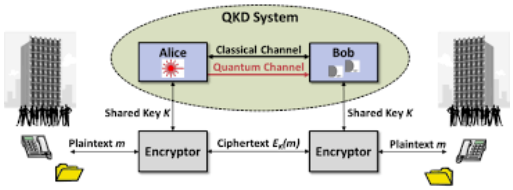
Exemple:automatiser des attaques et casser des systemes de securites comme AES

III:secteurs affectes et estimation des risques

plusieur secteurs seront particulieremant vulnerables a ces technologies futures ,surtout autour des 10 ans futur, lorsque les ordinateurs quantiques devraient etre suffisamment puissants pour casser des systemes de chiffrement courants

Exemple:Secteur financier,sante , Commerce electronique …

IV:les solution en cours QKD quantum key distribution



HSBC "DOING NOTHING IS SIMPLY NOT AN OPTION"

Conclusion

Même si l'AGI et le quantum computing promettent de révolutionner le monde, ils soulignent aussi la nécessité de repenser la sécurité des données. ces technologies pourraient briser les systèmes de chiffrement utilisés aujourd'hui pour sécuriser des données sensibles. Il est donc crucial de commencer dès maintenant à préparer des solutions de chiffrement adaptées à l'ère quantique pour protéger les secteurs critiques.