Vous êtes-vous jamais posé la question : comment mes données sont-elles protégées, et pendant combien de temps encore? Bonjour, je m'appelle Asya et je suis contente de vous présenter ce sujet qui m'a captivée. Ma problématique portera sur la cyber-sécurité dans le domaine du quantique ; plus spécifiquement : comment l'invention d'ordinateurs quantiques pourrait être une menace pour notre sécurité. Je vais tout d'abord vous présenter le système de sécurité mis en place de nos jours, je vous énoncerai ensuite le problème que rencontreront ces systèmes très prochainement. Pour conclure, je remettrai en perspective nos avancées actuelles et nos solutions.

La cyber sécurité concerne la protection de nos données donc en quelque sorte, celle de nos identités. Nos systèmes de sécurité sont aujourd'hui basés sur un processus nommé RSA ; c'est un algorithme à chiffrement asymétrique nous permettant d'encoder et de décoder des messages à partir de calculs. Contrairement au système symétrique, qui utilise 1 même clé pour chiffrer et déchiffrer un message, celui-ci utilise 2 clés par utilisateurs. La première est une clé publique à laquelle tout le monde a accès, tant dis que la deuxième est une clé privée que seul son utilisateur peut voir. Notons qu'il est impossible de calculer la clé privée à partir de la clé publique. Pour vous illustrer un exemple : visualisez 2 personnes, par convention, Alice et Bob, qui veulent s'envoyer des messages privés (Je vous ai fait un schéma du processus sur le support). Pour ce faire, Alice va encoder son message en utilisant la clé publique de Bob. Tout le monde peut donc voire le message encodé, mais seul Bob pourra le décoder en utilisant sa clé privée.

Tenter de déchiffrer ce message par force brute, c'est-à-dire essayer toutes les combinaisons possibles, serait inutile car une clé publique de 256 bits, peut figurer un entier d'environ 77 chiffres. RSA est très efficace car pour le casser, il nécessite des calculs de factorisation en nombre premier de très grande taille et nous n'avons pour l'instant pas d'ordinateurs assez puissants pour faire ces calculs rapidement. Avec un entier de cet ordre-là (77 chiffres), ce déchiffrement prendrait environ 300 000 Millions d'années en utilisant des supers calculateurs.

Cependant, dans les années 80, Richard Feynman énonce les premières théories d'une nouvelle informatique : celle dite quantique ; cette dernière utilise des calculateurs quantiques reprenant des caractéristiques de la physique quantique dont la superposition et l'intrication quantique. Un ordinateur quantique utilise une superposition de 0 et de 1, il utilise des qubits et non plus des bits, cela signifie qu'ils peuvent représenter une combinaison de 0 et de 1 en même temps. L'action de les intriquer revient à rendre possible toutes les configurations des états des qubits, augmentant ainsi la performance de l'ordinateur. Je vous ai fait le schéma d'un exemple d'intrication avec 3 qubits sur votre support : 3 qubits ont 8 combinaisons possibles ; avant intrication, nous avons 3 jauges, tant dis qu'après, nous en avons 8. Ce sont 8 états quantiques possibles.

Les ordinateurs classiques utilisent des signaux électriques grâce aux électrons. Ceux quantiques utiliseraient des photons et non plus des électrons. Malheureusement pour la cryptographie, cela représente un danger pour notre système RSA. Peter Shor, en 1994, nous présente un algorithme permettant de casser ce dernier : L'algorithme de Shor. RSA repose toute sa sécurité sur le fait de trouver les diviseurs d'un nombre n qui est un problème difficile avec un temps de calcul astronomique. D'après Shor, les calculs de son algorithme

ne sont pas quantiques, mais classiques ; cependant, le temps nécessaire à ces calculs est le problème que résoudraient les calculateurs quantiques.

Finalement, nous voyons que ce système de RSA pourrait bientôt être dépassé, représentant ainsi un risque pour nous et beaucoup de nos systèmes. Il est donc nécessaire de trouver un autre moyen de sécuriser nos données avant de développer ce nouvel ordinateur. (Si la transition du classique au quantique est mal faite, cela représentera un souci pour nous. Comment ? La vitesse de calcul de ces ordinateurs sera trop rapide à casser nos systèmes de sécurité, et nous n'aurons pas le temps de réagir.)

MERCI POUR VOTRE ATTENTION

Réponses aux questions

Pourquoi ce sujet ?
J'étais déjà intéressée à la sécurité informatique mais je ne m'y connaissais pas du tout, lorsque j'ai vu qu'il y avait un chapitre sur la sécurisation dans le programme de NSI, J'ai vu une opportunité pour pouvoir en apprendre plus sur ce sujet. De plus, je pense qu'avec le monde technologique qui évolue constamment, la sécurisation de nos données doit être notre priorité.
Contrairement à la cyber sécurité, la quantique était un sujet tout à fait nouveau pour moi, mais il m'a subitement captivée pour son coté plutôt philosophique et inconnu.

Pensez-vous que le monde quantique existera très prochainement ?
J'ai du mal à penser le contraire, voyant où nous en sommes et la vitesse à laquelle notre monde évolue, je doute que nous ayons atteint le sommet. La quantique existe déjà, il faut maintenant l'optimiser. Google a déjà créé un petit calculateur quantique de 72 qubits, il en va de même pour IBM qui entre en deuxième place avec son calculateur de 50 qubits. Avec ce nombre de qubits, ces calculateurs ne sont pas encore à puissance maximale, ils sont loin d'avoir atteint la limite.

De quelles avancées et solutions parlez-vous ?
Aujourd'hui, plusieurs pays et compagnies veulent atteindre la suprématie quantique, cela signifie de parvenir à résoudre un calcul qu'aucun ordinateur classique n'aurait pu accomplir dans un délai raisonnable.
Nos solutions sont pour l'instant très claire, il faut que l'on trouve un autre moyen de protéger nos données avant qu'il ne soit trop tard.

Des exemples ?
Par exemple, Google affirme déjà l'avoir atteinte avec un petit ordinateur quantique du nom de Sycamore de 72 qubits qui a résolu un problème de traditionnellement 10000 ans de résolution en 3 min. Il est en compétition avec IBM, Intel et Microsoft.

D'où vient le nom du système ?
C'est un acronyme utilisant les trois noms des mathématiciens ayant trouvé ce système : Rivest Shamir Adleman en 1977

C'est quoi un algorithme ?
C'est une suite d'instructions décrivant de manière précise les étapes de la résolution d'un problème mathématique.

C'est quoi chiffrement asymétrique ?

C’est un procédé qui intègre deux clés de chiffrement, procédé d’échange de clé sécurisé

Avez-vous un autre exemple qui utilise chiffrement asymétrique ?
RSA (chiffrement et signature)
DSA (signature)
Protocole d’échange de clés Diffie-Hellman (échange de clés)

Sur quels genres de calculs se base RSA? Démonstration ?
RSA est basé sur des calculs mathématiques qui prendraient des siècles à résoudre. La clé privée est constituée de deux nombres de très grande taille. Le produit de ces deux nombres résulte en la clé publique. La seule manière que quelqu’un pourrait y avoir accès, serait en factorisant ou en cassant petit à petit la clé publique, qui est souvent 600 chiffres ou plus, pour arriver aux deux chiffres initiaux de la clé privée.

Clé ?
De l’information, normalement une suite de nombres et de lettres

Comment la calculer ?
N = p x q (p et q sont grand nbr premiers privés)
N = clé publique
p et q = clé privée

C’est quoi un super calculateur?
Un ordinateur nous permettant de faire des calculs rapidement et efficacement

C’est qui Richard Feynman ?
Richard Feynman est un physicien américain du XXème siècle

Pourquoi cette nouvelle informatique ?
Il conçoit cette dernière en la pensant susceptible d’accélérer nos recherches autour des molécules (car elles sont aussi des objets quantiques, donc plus facile selon lui avec une même machine)

Le quantique ?
Relatif à l’étude physique de la matière et des éléments qui la composent, théorie des photons. Ensemble de théories physique nées au XXème siècle qui décrivent le comportement des atomes et des particules.

C’est quoi Qubit?
L’état quantique qui représente l’unité de stockage d’information quantique. Composé d’une superposition de deux états

Bit ?
C’est une unité d’information binaire (valant 0 ou 1)

Définition intriquer?
Emmêler des choses, les enchevêtrer

C’est quoi une configuration ?
Une possibilité d’état quantique dans lequel se trouve la superposition du qubit.

Explication des jauges
Pour un outils de mesure pour voir l’état d’une de ces particules : Lorsque deux particules sont intriquées, elles se trouvent dans un état quantique unique. Cela signifie que tout changement d’état d’une de ces particules, changera instantanément celui de l’autre. Elles sont liées même avec longue distance.

Tout fonctionnement des niveaux d’énergie
Les ordinateurs classiques utilisent des signaux électriques occupés par des électrons. Ceux quantiques utiliseraient des photons et non plus des électrons. Un photon est une particule de lumière qui n’a pas de masse, elle ne subit donc pas les frottements lui permettant une vitesse de $3x10^8$ m/s. Elle peut aussi être interprétée comme une onde (principe de dualité ?). Avec le courant électrique, l’ordinateur ne comprend que deux signaux : 0 ou 1, donc, le courant passe ou le courant ne passe pas. Dans la quantique, nous nous concentrons sur les niveaux d’énergie qui sont chacun utilisés comme un nouveau signal. Les physiciens ont trouvé que l’infiniment petit n’acceptait pas toutes les énergies, d’où l’origine du mot quantique, les niveaux sont quantifiés. Chaque quantum d’énergie devient alors un signal nouveau, il y a donc une infinité de signaux, permettant aux transferts d’être d’autant plus rapides.(paquet d’énergie)

Toutes informations sur les photons
Un photon est une particule de lumière qui n’a pas de masse, elle ne subit donc pas les frottements lui permettant une vitesse de $3x10^8$ m/s. Elle peut aussi être interprétée comme une onde (principe de dualité ?).

C’est qui Peter Shor?
C’est un mathématicien américain du XXème siècle connu pour son travail sur le calcul quantique

Comment casse-t-il RSA ?
Pour trouver les diviseurs d’un nombre n, on prend au hasard un nombre a, on calcule les puissances de a modulo n (a % n), on identifie le motif périodique obtenu, on enlève le 1 en fin de motif, on prend le nombre du milieu, et en lui

rajoutant ou enlevant 1, on obtient les diviseurs de n. Cet algorithme n'est pas efficace à cause de la longueur du motif.
Ex : 15, on prend 2, on calcule les puissance de 2 % 15, on obtient la suite 2,4,8,1

Qui sont en tête ?
Google, IBM, Microsoft et Intel ont déjà conçu des petits ordinateurs avec entre 50 et 72 qubits. Google affirme pour l'instant avoir la suprématie quantique en ayant résolu un problème qui avec un ordinateur normal aurait prit environ 10000 ans en seulement 3 min.
Les deux pays en tête dans le domaine de l'informatique quantique sont l'Amérique et la Chine, tant dis que du coté sécurité informatique, c'est plutôt l'Australie qui se retrouve en tête.

Conséquences ?
Ces ordinateurs peuvent avoir des répercussions critiques sur l'économie mondiale par exemple. Ils pourraient entrainer des problèmes de sécurité nationale en pouvant décrypter les messages secrets de chaque pays, compagnies, individuels. Cela peut entrainer des paralysassions d'infrastructures critiques et de systèmes financiers…

Solutions ?
De développer un nouveau système permettant de sécuriser toutes nos données et information avant qu'il ne soit trop tard.

Avantages ?
Détection de cancer plus rapide, plus tôt. Meilleurs médicaments, progrès en machine learning.