**1. L’ordinateur quantique fait partie des fantasmes du physicien au même titre que la fusion nucléaire. C’est la solution ultime et définitive au problème du traitement de l’information au même titre que la fusion nucléaire apparaît comme la solution au problème de notre approvisionnement énergétique.**

**Le principe de la théorie est acquis en ce sens que nous savons aujourd’hui que rien dans les lois de la physique – telles que nous les connaissons – ne s’oppose à ce que l’ordinateur quantique voie le jour, dans un avenir indéterminé.**

**Des problèmes restent ouverts au niveau de son mode de programmation, certainement très différent de celui de l’ordinateur classique, et surtout au niveau technologique, au point que certains n’hésitent pas à penser que la naissance de cet ordinateur ultime sera sans cesse repoussée. Il va de soi qu’on y travaille partout dans le monde : Allemagne, G-B, USA, Japon.**

**3. L’ordinateur classique semble donner toute satisfaction : il calcule tout ce qui est calculable pourvu qu’il dispose d’une réserve de mémoire potentiellement infinie.**

**L’ordinateur quantique ne calcule rien que son homologue classique ne calcule déjà, alors pourquoi s’en inquiéter ? Pour le rendre plus compact ou moins gourmand en énergie ? Ce serait se donner beaucoup de mal pour un bénéfice minime.**

**La vraie réponse : pour qu’il calcule plus vite ! L’ordinateur classique calcule déjà très vite et encore plus vite si on met plusieurs processeurs en parallèle mais il se fait que c’est encore très insuffisant pour régler de nombreux problèmes complètement hors de son atteinte. Tel le calcul du spectre de l’atome d’azote dans un temps raisonnable.**

**Il convient de noter à ce stade que l’accélération que l’on vise n’a rien à voir avec un hypothétique décuplement de la fréquence du processeur, qui passerait de 3GHz à 30 GHz, par exemple; ce serait gagner un facteur 10 mais ce serait encore très insuffisant pour l’exécution des tâches que nous avons en vue.**

**Ce qu’il nous faut, c’est un mode de calcul fondamentalement nouveau. Par exemple, la nature calcule le spectre de l’atome d’azote presque instantanément lorsqu’on excite une ampoule remplie de ce gaz par une tension électrique suffisante ! D’où l’idée que l’ordinateur quantique pourrait faire aussi bien.**

**4. Même en mathématique élémentaire, il existe quantité de problèmes intraitables en un temps raisonnable par un ordinateur classique : il semble qu’ils appartiennent à une classe de complexité inaccessible au calcul numérique classique.**

**Multiplier deux nombres entiers n’est certainement pas un problème complexe même si les nombres sont très grands. Avec la méthode apprise à l’école élémentaire, le temps de calcul du produit de deux entiers comportant n chiffres est au pire proportionnel à n2.**

**On peut même faire mieux avec une méthode plus sophistiquée, typiquement de l’ordre de n ℓg n. On dit que la multiplication appartient à une classe de complexité polynomiale.**

**Voilà pourquoi multiplier deux nombres de 300 chiffres décimaux est possible en quelques fractions de secondes sur un ordinateur classique cadencé à disons 1 GHz.**

**5. Le problème inverse, appelé factorisation, est beaucoup plus complexe : retrouver les facteurs premiers à partir de la donnée du produit. Aucune méthode de factorisation polynomiale n’est connue. Sûrement pas le crible d’Eratosthène, qui exige de passer en revue tous les nombres premiers jusqu’à N=2n/2.**

**La plus rapide, connue à ce jour, fait mieux mais c’est loin d’être suffisant :**

**Exp[1.7 n1/3 ℓn(n)2/3 ]**

**Factoriser un nombre de 1000 chiffres binaires exigerait 10 milliards d’années sur un ordinateur classique, un peu moins si on met en place des stratégies de parallélisation GPU !**

**Il existe peut-être un algorithme de factorisation fonctionnant en temps polynomial mais personne ne le connaît et on doute sérieusement que cela soit possible. Le record actuel, datant de 2010, a vu la factorisation de RSA768 après 220 opérations élémentaires, effectuées par une armée de processeurs mis en parallèle.**

**Qui devrait s’inquiéter de ce genre de problèmes ? Chacun de nous, qui se sent concerné par la sécurité de ses données confidentielles, bancaires par exemple, on y reviendra dans la deuxième partie de cet exposé : une clé de 1024 bits risque de n’être plus sûre à partir de 2015.**

**6. La théorie qui va nous occuper ne se préoccupe que d’une seule chose : s’assurer que rien dans les lois de la physique (que nous connaissons) ne s’oppose à ce que l’on encode l’information au niveau atomique et qu’on la traite à l’aide d’un réseau de portes logiques quantiques.**

**Cette théorie ne se préoccupe pas de savoir comment on peut réaliser expérimentalement les montages théoriques donc construire un véritable ordinateur quantique.**

**Actuellement, l’histoire qui va nous intéresser comporte donc une part de spéculation mais elle vaut d’être contée, d’autant plus qu’elle offre la meilleure approche pédagogique pour expliquer les lois qui prévalent dans l’infiniment petit.**

**7. L’ordinateur classique encode et traite l’information, sous formes de bits 0 ou 1. N’importe quel système physique classique à deux états peut convenir et actuellement on se sert de transistors.**

**On différencie un 1 d’un 0 par la présence d’une tension électrique de disons 3 V aux bornes d’une « capacité » de quelques femto farad.**

**Ce système physique mobilise 100 000 électrons pour une énergie stockée de l’ordre de 107 kT (105 eV).**

**L’avantage est une grande stabilité, à température ordinaire.** **L’inconvénient est la relative lenteur d’une inversion 0-1 et la dissipation de chaleur due aux frottements.**

**Si on augmente la vitesse on augmente la dissipation donc la température.** **Si on diminue la tension électrique, on diminue la dissipation (= on peut compacter davantage) mais la stabilité est moindre.**

**L’alternative quantique, consiste à encoder l’information au niveau le plus élémentaire qui soit, le noyau, l’atome ou le photon.**

**8. Il existe plusieurs possibilités d’encodage du qubit au niveau atomique. Les premiers essais fructueux ont été réalisés avec des noyaux atomiques porteurs d’un moment magnétique qui s’orientent spontanément dans un champ extérieur, tels de petits aimants.**

**Une autre possibilité consiste à utiliser des photons de lumière. C’est l’approche que j’ai choisie car elle est plus intuitive. Même avec un photon unique, plusieurs possibilités d’encodage existent :**

**- Le plus simple consiste à encoder le qubit selon les états spatiaux du photon. On considère des photons uniquement capables de déplacer d’ouest en est (selon x), vers D0 qui l’absorbe, ou de sud en nord (selon y), vers D1 qui l’absorbe. On pose qu’ils encodent 0 ou 1, respectivement.**

**- Un autre encodage est possible, reposant sur les états de polarisation du photon selon deux directions orthogonales, x et y. Cette fois c’est un polariseur analyseur qui fait office de détecteur, n’absorbant un photon que s’il est polarisé perpendiculairement à sa direction passante.**

**9. Il ne suffit pas d’encoder l’information, il faut encore pouvoir la manipuler. L’opération la plus simple à laquelle on peut soumettre un qubit isolé, c’est l’inversion.**

**- Un simple miroir (ou un prisme à réflexion totale) effectue l’inversion entre les états spatiaux : le miroir fonctionne comme une porte NOT.**

**- Si on utilise les états de polarisation, nous verrons qu’une lame biréfringente convenablement taillée inverse le qubit.**

**10. En informatique classique, un bit d’information vaut nécessairement 0 ou 1 d’où il résulte que Not est la seule opération que peut subir un bit isolé. En informatique quantique, les choses sont plus compliquées.**

**Pour le voir, considérons une lame semi transparente, qui partage le faisceau incident en deux sous-faisceaux d’intensités égales. Si l’on atténue considérablement l’intensité du faisceau incident, on constate que les détecteurs enregistrent l’arrivée des photons de façon imprévisible. Les physiciens sont convaincus que la suite des 0 et des 1, qui encode les détections successives, ne présente aucune régularité détectable donc qu’elle est parfaitement aléatoire au sens de Kolmogorov (Aucun programme plus court que Print[suite] ne peut l’imprimer).**

**Jusque-là, les choses paraissent étranges mais pas au point de défier le sens commun : peut-être y-a-t 'il un mécanisme caché au niveau de la lame que nous ne comprenons pas mais qui est responsable de la réflexion ou de la transmission des photons individuels, les partageant entre les canaux comme dans cette analogie hydraulique ?**

**11. Pourtant, l’analogie hydraulique ne vaut rien et pour le voir, il suffit de compléter le montage : on dispose symétriquement 2 miroirs, 2 lames semi transparentes et 2 détecteurs (= Interféromètre MZ).**

**Vu la symétrie du montage, on s’attend à ce que les détecteurs enregistrent à nouveau aléatoirement un photon sur deux, or ce n’est pas du tout ce que l’on observe car le détecteur D0 enregistre, à lui seul, l’arrivée de tous les photons !**

**Richard Feynman a beaucoup insisté sur le fait qu’en présence d’observations singulières, le physicien a intérêt à ne pas fantasmer. La meilleure attitude consiste à chercher, en priorité, un modèle calculatoire qui rend compte des faits observés puis seulement de lui trouver une interprétation.**

**La physique quantique est un modèle calculatoire qui a pour ambition non de prédire les occurrences de détection - c'est impossible puisqu’elles sont aléatoires - mais seulement la probabilité de ces détection.**

**Ici cette probabilité vaut 1 en D0 et 0 en D1. Pour progresser, il faut formaliser les rôles de M, D et L.**

**12. Le modèle calculatoire de la mécanique quantique utilise deux outils :**

**- le vecteur d’état qui décrit l’état du photon à tout instant, dans l’exemple, |0> si le photon se déplace d’ouest en est (selon x) et |1> s’il se déplace de sud en nord (selon y).**

**- Un opérateur est associé à chaque obstacle rencontré par le photon. Lorsqu’un photon rencontre un obstacle son état bascule dans un nouvel état que l’on calcule en lui appliquant l’opérateur correspondant :**

**Nouvel état = Opérateur(Ancien état)**

**Par exemple, on construit un modèle fiable si on pose que l’opérateur « miroir » se note : |0><1|+|1><0|. Pour que ce formalisme rende fidèlement compte de la réalité, il faut impérativement que les vecteurs obéissent à des règles calculatoires précises.**  **On voit qu’une algèbre se dégage.**

**13. Il serait difficile de trouver une algèbre plus simple que celle-là !**

**Le produit intérieur d’un vecteur d’état par lui-même s’appelle sa norme au carré.**

**Un détecteur est un obstacle sur la trajectoire du photon donc on lui associe un opérateur D (non unitaire dans ce cas car le détecteur absorbe le photon. Certains parlent de projecteur pour cette raison).**

**Pour prédire la probabilité qu’un détecteur enregistre l’arrivée d’un photon, il suffit de calculer le carré de la norme de D|photon>.**

**14. L’opérateur associé au détecteur de photon dans l’état |i> se note, D= |i><i|.**

**L’opérateur associé aux détecteurs a évidemment été choisi pour rendre compte du fait que D0 détecte avec certitude les photons dans l’état |0> et jamais ceux dans l’état |1> (Et l’inverse pour D1 ).**

**15. Ne perdons pas de vue notre objectif : expliquer le comportement étrange du photon lors du passage au travers de l’interféromètre de M-Z. Nous connaissons les opérateurs associés au miroir et aux détecteurs, reste la lame semi transparente. Elle a pour effet de faire entrer le photon dans un état de superposition quantique : le photon n’emprunte pas au hasard une des trajectoire, il les emprunte simultanément !**

**Une porte logique qui superpose les états de cette manière porte le nom de Hadamard. (NB : Une lame semi-transparente ne coïncide exactement avec une porte de Hadamard qu’en y adjoignant des lames retardatrices convenablement choisies (Par exemple, une réflexion sur un milieu plus réfringent s’accompagne d’un déphasage de p). Elles ne figurent pas ici pour ne pas compliquer le schéma).**

**On vérifie que le formalisme prédit correctement que les détecteurs D0 et D1 détectent les photons avec la probabilité 1/2.**

**La première caractéristique du monde quantique est l’absence de frottements. La deuxième caractéristique est la possibilité qu’ont les systèmes d’entrer dans des états de superposition.**

**16. Nous sommes maintenant équipés pour analyser le comportement du photon lorsqu’il traverse l’interféromètre de M-Z. Il suffit de suivre l’état du photon dans chacune des étapes qu’il subit.**

**On constate que le formalisme calculatoire adopté rend bien compte du fait que la direction de propagation du photon initial n’est pas affectée et que c’est donc toujours le même détecteur qui reçoit les photons préparés dans l’état initial |0> (ou |1>).**

**On voit qu’en logique quantique, la question de savoir quel chemin le photon a suivi dans l’interféromètre est vide de sens : contrairement à ce qui se passe en logique classique une porte n’est pas nécessairement ouverte ou fermée mais peut être les deux à la fois.**

**Le modèle calculatoire décrit a été adopté parce qu’il décrit toutes les expériences faites à ce jour, pas seulement MZ.**

**17. Il reste à interpréter le modèle algébrique qui réussit à décrire correctement les observations expérimentales.**

**Il faut abandonner l’idée que la lame séparatrice distribue les photons au hasard selon l’un ou l’autre canal. L’interprétation admise est que chaque photon emprunte virtuellement les deux trajets simultanément et que tout ce que les détecteurs sont capables d’enregistrer, c’est le résultat de l’interférence entre les deux trajectoires possibles.**

**Si l’on tente de contourner l’obstacle en essayant de voir quel chemin les photons empruntent réellement (par exemple en interposant un troisième détecteur sur le canal inférieur) alors l’interférence quantique disparaît et les probabilités de détection des photons correspondent à la prédiction classique.**

**18. Pour information, on peut pousser le bouchon plus loin et imaginer un réseau triangulaire de portes de Hadamard, ici représentées par des lames semi transparentes.**

**Intuitivement, on penserait que le photon choisit son chemin au hasard lors du franchissement de chaque lame de telle sorte qu’au bilan il simule le jeu de billard classique que voici.**

**Il n’en est rien : le calcul quantique, un peu fastidieux, prédit que les détecteurs enregistrent l’arrivée des photons selon une loi bien différente de la loi binomiale classique et qui privilégie certains détecteurs !**

**Note ; dans ce schéma les lames sont équipées de déphasages (non représentés) tels que le seul changement de signe correspond à une transmission dans le sens S-N.**

**19. Pour aller plus loin, il faut discuter les états de polarisation du photon ce qui est intuitivement moins évident car la polarisation de la lumière ne se voit pas à l’œil nu.**

**Cependant une expérience toute simple révèle qu’un cristal de calcite rend deux images distinctes en réfraction : c’est le phénomène de biréfringence optique.**

**20. Ces deux images proviennent du fait que la réfraction ne se fait normalement que pour les photons polarisés (ici selon y) perpendiculairement au plan défini par l’axe optique et la direction incidente. Pour les photons polarisés parallèlement à ce plan, la réfraction est anormale selon un angle que la théorie calcule.**

**Si la lumière incidente mélange des photons polarisés n’importe comment, deux images en résultent.**

**Le cas le plus intéressant est quand l’angle a vaut 90° : les deux images sont confondues et les photons sont dans un état de superposition polarisatoire. Il nous faut redessiner la figure en perspective pour y voir plus clair.**

**21. Poser a=90° signifie que l’on taille le cristal parallèlement à l’axe optique : les trajectoires spatiales demeurent confondues et les états de polarisation entrent en superposition.**

**Une lame de ce type permet de modifier à la demande l’état du qubit de polarisation. L’opérateur s’écrit en toute généralité de façon plutôt barbare mais seuls quelques cas particuliers sont intéressants, obtenus en jouant sur l’angle b et sur d, via l’épaisseur de la lame.**

**22. Les trois lames les plus utiles sont celles qui présentent un angle  valant 45°, 22.5° ou 0°.**

**23. Voici résumés les deux modes d’encodage d’un qubit à l’aide d’un photon isolé ainsi que les opérations élémentaires qu’il peut subir.**

**24. Deux portes de Hadamard et deux portes de déphasages suffisent pour préparer n’importe quel qubit dans n’importe quel état de superposition :**

**a|0>+b|1>, (|a|2+|b|2=1).**

**Bien noter qu’une mesure isolée ne permet pas de connaître cet état avec exactitude : elle ne peut donner que 0 ou 1 avec les probabilités |a|2 et |b|2.**

**En conséquence, il est impossible de cloner un qubit inconnu, un point qui s’avérera essentiel lors de la transmission quantique des clés cryptographiques.**

**25. On ne va pas très loin avec un qubit isolé : on ne peut coder que 0 et 1.**

**n qubits assemblés constituent un registre permettant d’encoder tous les entiers de 0 à 2n-1.**

**Notre but est de soumettre ce registre à toutes sortes de portes logiques correctement assemblées afin de pouvoir calculer tout ce qui est calculable au départ de cet entier, par exemple son carré ou son cube. Ce calcul par porte quantique est effectivement possible mais comme il doit être effectué de façon réversible, il faut prévoir des qubits supplémentaires initialisés à 0 qui servent de papier brouillon.**

**En fait, nous voulons pouvoir faire beaucoup mieux que cela, à savoir effectuer ce même calcul sur tous les entiers à la fois ! Comment une telle chose peut-elle être possible ?**

**26. A ce stade on doit bien admettre que les portes de Hadamard et de déphasages ne suffisent certainement pas. Certes chaque qubit a bien été préparé dans un état de superposition maximale mais on n’a pas couvert tous les cas de superposition du registre complet : seules les configurations séparables en un produit (tensoriel) de facteurs sont accessibles par cette méthode.**

**Jamais on ne pourra, de cette façon, préparer le registre dans un état non séparable. Pour y parvenir, il nous manque quelque chose.**

**27. Ce qui nous manque c’est une porte qui agit conditionnellement sur un qubit (cible) selon l’état d’un autre qubit (contrôle). La porte CNot est celle que nous cherchons : elle inverse le qubit cible si et seulement si le qubit contrôle vaut 1.**

**C’est à l’état embryonnaire la porte qui permettra de coder des instructions du type If Then Else.**

**Un problème qui se pose est que piloter l’état d’un photon à partir de l’état d’un autre photon n’est pas possible en optique linéaire (des solutions existent en optique non linéaire où le deuxième photon modifie l’indice de réfraction des obstacles rencontrés par le premier photon, effet Kerr, …).**

**Cependant, grâce au fait que le photon autorise deux modes distincts d’encodage de qubits, il est possible de dessiner une porte CNot sur base d’un photon isolé. Deux versions existent selon que l’on pose :**

**Contrôle = qubitpos et  cible = qubitpol**

**28. La porte CNot permet de créer l’état intriqué qui nous faisait défaut.**

**La première caractéristique du monde quantique est l’absence de frottements. La deuxième caractéristique est le phénomène de superposition. La troisième est l’intrication qui peut lier les états de deux qubits au sein d’un registre.**

**29. Une troisième porte s’avère utile (qu’on peut construire à partir des deux premières), la porte CCNot (Toffoli).**

**Elle inverse le qubit cible si et seulement si deux qubits de contrôle valent 1.**

**3 qubits étant nécessaires, on pourrait penser que 2 photons sont nécessaires, l’un codé selon ses états de position et de polarisation et l’autre selon sa position seulement. Cette solution fonctionne certainement mais on peut faire mieux.**

**30. En théorie un seul photon peut faire le travail d’encodage à condition de recourir à 3 lames semi-transparentes selon le schéma indiqué.**

**Il suffit d’ajouter la lame qui inverse la polarisation sur le trajet convenable pour que cette porte CCNot fonctionne avec un photon unique.**

**31. Cette porte CCNot permet de construire un semi-additionneur binaire, qui calcule a+b modulo 2 ainsi que le report correspondant. C’est le tout début de l’aventure calculatoire.**

**32. Le semi-additionneur binaire calcule a+b modulo 2 ainsi que le report correspondant. Jusque-là rien de très excitant car l’ordinateur classique fait très bien cela depuis belle lurette.**

**C’est ici que les portes de Hadamard entrent en action : il devient possible de calculer les 4 instances de l’addition (modulo 2) simultanément donc en un seul passage ! Cela s’appelle un calcul massivement parallèle.**

**33. Observons l’évolution du registre à mesure du franchissement des portes quantiques.**

**La mesure du premier qubit de sortie donnerait 0 ou 1 une fois sur deux mais cette valeur ne nous intéresse pas. Seul nous intéresse le contenu des qubits 2 et 3. Ils donnent les 4 réponses possibles avec la probabilité ¼.**

**Revers de la médaille, on ne peut prendre connaissance que d’un seul résultat à la fois et encore on ne sait pas forcément quelle instance a été calculée !**

**Il semblerait qu’on n'ait pas progressé beaucoup et pourtant il existe des cas où certaines subtilités vont faire toute la différence !**

**34. Essayer tous les facteurs premiers possibles jusqu’à tomber sur le bon est faisable sur un ordinateur classique mais pour un nombre de 1000 chiffres binaires, nous savons que l’âge de l’univers ne suffirait pas.**

**L’inconvénient de cette méthode fruste c’est qu’elle met tous les facteurs premiers sur un pied d’égalité.**

**L’art de la programmation quantique, c’est de privilégier des solutions probables quitte à demander à un ordinateur classique de vérifier la solution trouvée, ce qui ne prendra plus qu’un temps tout-à-fait raisonnable si le problème appartient à NP.**

**36. Le premier algorithme quantique évolué (mis au point par Shor) est celui du calcul de la transformée de Fourier discrète d’une suite.**

**Il trouve une application spectaculaire dans le domaine sensible de la cryptographie. Voici, pour démarrer, un rappel de l’état de l’art en ce domaine.**

**Lorsqu’on veut envoyer un message à un correspondant par voie numérique, la première chose à faire est de le numériser.**

**Le codage ASCII sur 7 bits permet de coder 27 = 128 caractères ce qui est largement suffisant même en acceptant toutes sortes de caractères plus ou moins exotiques.**

**37. Le transfert digital se faisant généralement par paquets de 8 bits (octets), on préfixe généralement chaque code par un ‘0’ excédentaire, non significatif.**

**Voici plusieurs représentations équivalentes du message :** **« Alerte à Rio ».**

**38. Si l’on veut protéger la confidentialité du message, il convient de le crypter.**

**En cryptographie classique, il n’existe qu’une seule méthode de cryptage prouvée absolument sûre : c’est le masque jetable.**

**Le masque est une clé secrète qu’on applique au texte clair, en fait, on ajoute le masque au texte clair modulo 2 : une case du message crypté est blanche si les cases de même rang du texte clair et de la clé sont de même couleur sinon elle est noire.**

**Le décryptage s’effectue très simplement en réappliquant le même masque au message crypté.**

**39. L’émetteur et le receveur doivent donc se mettre préalablement d’accord sur un masque secret (on dit aussi une clé).**

**Même une attaque par force brute, consistant à essayer toutes les clés ne peut réussir. Il y en a bien une qui traduit : alerte à rio, mais il y en a une autre qui décode : tout va bien !**

**Cette méthode n’est parfaitement sûre que si le masque respecte les exigences suivantes :**

* **Il doit être de même longueur que le message**
* **il doit être aléatoire**
* **Il ne peut être utilisé qu’une seule fois**

**Enfreindre une seule de ces trois règles fragilise la méthode.**

**On peut légitimement se demander quel est l’intérêt d’une méthode qui exige de communiquer de façon sûre un masque aussi long que le message : autant envoyer le message tout de suite ! Je reviendrai sur cette remarque tout à la fin de l’exposé.**

**40. Au lieu de masquer un message, on peut décider de le brouiller.**

**Aucune méthode de brouillage utilisant une clé courte et réutilisable n’est sûre à 100%. La NSA fut la première à se préoccuper d’imposer une norme internationale basée sur un brouillage et une clé secrète.**

**DES, IDEA ou AES sont de ce type : elles sont commodes mais non sûres à 100 %. Voici le schéma IDEA.**

**IDEA découpe le message en blocs successifs de 16 bits chacun qu’il combine (4 à la fois) avec les bits d’une clef secrète également découpée en blocs de 16 bits.**

**8 tours ½ sont utilisés et les blocs de 16 bits de la clef subissent une permutation circulaire portant sur 25 bits, à chaque tour.**

**représente Xor**   **représente l’addition modulo 216**   **représente la multiplication modulo 216+1**

**41. Avantage : (dé)cryptage binaire très rapide** **Inconvénient : pas sûr à 100 %**

**Certes, la longueur de la clé les protège contre une attaque par force brute (2128 = 1077, presqu’autant que d’atomes dans l’univers !) mais une attaque astucieuse, par ex. algébrique, n’est pas à exclure :**

**si en fouillant les poubelles (ne souriez pas, c’est comme cela qu’on espionne) on peut se procurer assez de couples « texte clair-texte codé », il suffirait de résoudre :**

**textecodék = fbooléenne(texteclairk, clé) (k=1,2,3, …)**

**DES a régné très longtemps comme standard américain mais il n’est plus sûr. Le standard actuel est l’AES des belges Joan Daemen et Vincent Rijmen.**

**Logiciels didactiques décrivant AES :** [**http://www.formaestudio.com/rijndaelinspector/**](http://www.formaestudio.com/rijndaelinspector/)

**42. Indépendamment du manque éventuel de sécurité, deux problèmes demeurent non résolus à ce stade si l’on veut généraliser la cryptographie au commerce via Internet :**

**- Transmettre la clé secrète**

**- Signer le message afin de l’authentifier**

**L’arithmétique modulaire apporte une solution élégante à ces deux problèmes. La clé de transmission n’a plus besoin d’être secrète, elle est au contraire publiée dans un annuaire officiel accessible à tous.**

**43. L’arithmétique modulo N ne considère que les entiers de 0 à N-1. Tous les autres entiers sont réduits à cet intervalle en leur ôtant N autant de fois qu’il le faut. Voici la table de multiplication modulo 7.**

**L’inverse d’un entier, b, b-1 mod N n’existe que ssi : pgcd(b,N)=1**

**Si N est premier tout est simple : tout entier possède son inverse**

**Si N n’est pas premier, seuls ceux qui sont premiers avec N en possède un (ils sont en nombre f(N) ).**

**Calculer l’inverse modulaire de b est très facile via l’algorithme d’Euclide étendu.**

**44. Principe du RSA. Chaque utilisateur publie 2 entiers , N et exp, dans un annuaire consultable en ligne.**

**- N doit être le produit de deux nombres premiers très grands, p et q, gardés eux absolument secrets.**

**- exp ne doit posséder aucun facteur commun avec (p-1)(q-1) et il doit être plus grand que la longueur des tranches de chiffres utilisées lors du codage.**

**Alice veut envoyer un message à Bob : elle utilise pour cela la clé publique de Bob et son exposant; le canal de transmission n’a pas besoin d’être protégé.**

**On ne connaît qu’une seule méthode de décodage et elle exige de connaître les facteurs premiers de N. Bob connaissant p et q, il peut décoder. Eve qui intercepte le message ne peut rien faire car elle n’a aucun moyen de factoriser N en un temps raisonnable.**

**45. La sécurité de RSA repose sur deux conjectures non démontrées, à ce jour. Ces 2 points faibles sont :**

**Rien ne prouve qu’il soit nécessaire de factoriser pour décoder.**

**Rien ne prouve que la factorisation demeure éternellement difficile.**

**Les informaticiens (mais aussi les utilisateurs que vous êtes, en ce qui concerne la protection de vos données bancaires !) ont confiance - peut-être bien à tort - en la validité de ces conjectures. Quelqu’un casserait même le code qu’il n’est pas sûr qu’il publierait ses résultats !**

**46. Un avantage essentiel de RSA est qu’il permet de signer un message.**

**Au lieu d’envoyer le codage du texte clair à l’aide de la clé de Bob, Alice envoie le décodage qu’elle ferait avec sa propre clé secrète de ce codage.**

**Bob a tout ce qu’il faut pour décoder et être sûr que le message reçu est authentique, un point essentiel pour les transactions financières et autres.**

**47. Quel rapport avec l’ordinateur quantique ? Réponse : il peut factoriser tout entier exponentiellement plus vite que son homologue classique.**

**Voici une méthode de factorisation de N, élégante mais totalement inefficace sur un ordinateur classique.**

**Le principe est simple : on calcule la suite des puissances de 2 (ou de 3, …) modulo N; cette suite est nécessairement périodique et sa période est fatalement inférieure à N. Si l’on connaît cette période, on peut espérer trouver deux facteurs premiers de N avec une excellente probabilité.**

**L’étape coûteuse est celle qui cherche la période de la suite. Bien noter que la suite commence par 1 et que scanner celle-ci à la recherche de la position du deuxième 1 ne fonctionne pas en temps polynomial. En moyenne la méthode n’est pas meilleure que le crible d’Eratosthène, elle est même pire.**

**48. Il existe bien une méthode de détection de la période d’une suite, basée sur la transformée de Fourier discrète de cette suite mais hélas aucune méthode de calcul de la TFD ne fonctionne non plus en temps polynomial sur un ordinateur classique même en adoptant la FFT (Fast Fourier Transform).**

**Commençons par rappeler le principe de la TFD : on peut extraire la période d’une suite en tricotant adroitement ses termes successifs.**

**Si par chance le nombre de termes de la suite est un multiple de la période, tout va bien : la TFD ne présente que des pics isolés et la position du premier pic (on ne compte pas le pic à l’origine) mène à la valeur de la période. Les autres pics fournissent toujours un sous-multiple de cette période.**

**49. Généralement, la période ne divise pas la longueur de la suite. On observe alors des pics plus ou moins étroits dont la position suffit pour trouver la période avec une bonne approximation.**

**50. La bonne nouvelle c’est qu’il existe un circuit quantique qui calcule en un seul passage la totalité de la TFD ! Ceci représente une accélération exponentielle par rapport au calcul classique qui exige le calcul en tout point.**

**NB. Sur ce diagramme, il manque une série de portes qui effectuent l’inversion des qubits de sortie, devant être lus dans l’ordre inverse; ce n’est qu’un détail sans importance.**

**51. Dans cet exemple (simpliste), on s’arrange pour que les 2 qubits d’entrée soient initialisés de manière à encoder la suite (s0, s1, s2,…, s7) :**

**(a0|0>+b0|1>) (a1|0>+b1|1>) (a2|0>+b2|1>)=s0|000>+s1|001>+ s2|010>+ …**

**Le circuit quantique calcule la TFD complète.**

**La mauvaise nouvelle c’est qu’on n'y a pas accès par la mesure ! Tout ce qu’on peut mesurer c’est l’état du registre de sortie (8 possibilités apparaissant avec des probabilités a priori inégales).**

**A première vue, on ne voit pas ce qu’on a gagné car pour remonter à la TFD complète il faudrait recommencer l’expérience un nombre énorme de fois et remonter aux s~ par tomographie, à partir des fréquences probabilistes trouvées.**

**Heureusement, nous n’avons pas besoin de connaître la TFD en tous points, seuls la position des pics nous intéresse. Or c’est exactement ce que donnent, avec une forte probabilité, les mesures du registre de sortie.**

**52. Voici l’exemple simplissime d’une suite de longueur 8 et de période 2. La mesure du registre de sortie ne peut donner que deux résultats : 000 (90% des cas) ou 100 (10% des cas).**

**Le premier cas n’est pas intéressant mais bien le deuxième qui permet de trouver la période. Bien noter que l’on n’a pas eu besoin de reconstruire la FFD complète, seule la position du ou des pics (hors l’origine) est important pour déterminer la période de la suite.**

**53. Voici, dans le modèle proposé, la factorisation (modeste !) de 15, construit sur base d’ une suite de longueur 28=256. La longueur, 2n, à prendre en considération doit idéalement être comprise entre N2 et 2N2. Ce point un peu technique est destiné à extraire la période dans tous les cas de figures par fractions continues. Le premier registre comporte donc 8 qubits. La réversibilité du calcul quantique exige un deuxième registre de bits ancillaires qui finiront à la poubelle mais qui sont des intermédiaires obligatoires de calcul.**

**Bien que le circuit calcule toute la TFD, une seule valeur de la TFD est accessible après mesure du premier registre ce qui peut paraître inacceptable.**

**54. Par bonheur, la probabilité qu’une valeur apparaisse est proportionnelle au carré de la TFD. Autrement dit, on est certain de mesurer une valeur de la TFD en un pic, si par chance la période divise la longueur de la suite.**

**55. Même si le nombre de termes de la suite n’est pas un multiple de la période, la probabilité de s’écarter d’un pic lors d’une mesure est très faible. Certes rien ne permet de prédire au voisinage de quel pic on se trouvera lors de la mesure mais un développement en fractions continues des quotients livre à tous les coups un sous-multiple de la période.**

**Il suffit de recommencer tout le processus un nombre raisonnable de fois pour remonter à la période avec une excellente probabilité. Aucune erreur n’est à craindre dans la factorisation finale car on peut contrôler les facteurs trouvés par simple multiplication.**

**56. La construction d’un ordinateur quantique casserait automatiquement la cryptographie RSA !**

**Le record actuel est cependant dérisoire : on a factorisé 15=3\*5 en 2001 à l’aide d’un codage NMR. On vient de réitérer cet « exploit » avec une puce optique (O Brien : Nature or Science 2009).**

**RSA n’est pas menacé dans l’immédiat mais les progrès sont à l’étude et il n’est jamais trop tôt pour préparer la parade.**

**57. Juste retour des choses, la mécanique quantique qui casserait RSA contient tout ce qu’il faut pour construire une méthode cryptographique définitivement sûre du transfert de clé jetable dans un cadre mixte Brouillage pour la crypto et MQ pour la clé.**

**Voyons d’abord un montage insatisfaisant.**

**Alice et Bob se mettent d’accord sur l’orientation des axes x et y.**

**En pilotant aléatoirement l’orientation d’une lame biréfringente entre les angles 0° et 45°, Alice crée au compte-gouttes une suite de qubits qui constituent un masque jetable potentiel pour Alice et Bob.**

**Toutefois ce procédé n’est pas sûr car Eve peut espionner la ligne de transmission, mesurer les qubits, un à un, puis les renvoyer inchangés vers Bob. Eve sera en possession de la clé sans que ni Alice ni Bob ne soient en mesure de soupçonner qu’ils ont été espionnés. Il faut trouver autre chose.**

**NB. En pratique la commutation entre les modes doit se faire très rapidement (cellule de Pockels).**

**58. Pour rendre le procédé inviolable il faut procéder autrement :**

**Alice et Bob se mettent d’accord sur l’orientation des axes x et y.**

**Alice pilote aléatoirement l’orientation de la lame selon 4 angles distincts : 0°, 45°, 22.5° ou 67.5°. Elle génère ainsi une suite de qubits lus aléatoirement dans deux bases différentes. Elle conserve une trace des bases utilisées successivement.**

**Bob analyse les photons qui lui parviennent avec son analyseur orienté aléatoirement en mode xy ou en mode 45°. Il conserve, lui aussi, une trace des bases utilisées successivement.**

**59. Evidemment le même mode ne sera choisi en moyenne qu’une fois sur deux par Alice et Bob.**

**Alice et Bob se contactent (sans précaution particulière) pour déterminer à quels moments ils ont, par hasard, choisi la même orientation et ils ne conservent que les qubits pour lesquels l’orientation a été identique. Ils procèdent alors à un sondage sur ces qubits restants qu’ils échangent à haute voix afin de vérifier qu’ils sont identiques. Sans désaccord, ils jettent les qubits sondés et conservent les autres qui constituent la clé secrète cherchée. La méthode RSA peut alors démarrer.**

**Il importe peu qu’Eve écoute la transmission, elle ne pourra rien en faire. Si elle intercepte les qubits émis par Alice, les mesure (dans sa base à elle !) puis les renvoie tels quels à Bob, elle ne saura pas quelle base utiliser pour chaque photon. Ce qu’elle peut faire de mieux, c’est choisir une base orientée à 22.5° mais elle se trompera encore en moyenne dans 15% des cas, une erreur que Bob et Alice découvriront lors du sondage. Dans ce cas, Alice et Bob savent qu’ils ont été espionnés et ils interrompent le processus. En dernière analyse c’est l’impossibilité du clonage de qubits inconnus qui est à la base de la sécurité crypto-quantique.**

**60. La cryptographie est sans doute le premier champ d’application de la théorie quantique de l’information. L’échange sûr des clés sera certainement effectif avant qu’un ordinateur quantique digne de ce nom soit construit.**

**Le choix du système quantique ne fait pas l’unanimité (NMR, photons, …) et il dépend largement des écoles.**

**Deux obstacles non résolus sont la décohérence des états superposés et intriqués et la difficulté de concevoir un réseau de portes logiques qui ne croît pas exponentiellement avec le nombre de qubits traités.**

**Certains cherchent des systèmes qui présentent un temps de décohérence long par rapport au temps de calcul, d’autres préfèrent s’en remettre aux codes correcteurs d’erreurs.**

**Il est peu probable qu’on s’attache à construire un ordinateur universel au sens de Turing : cela n’aurait guère de sens pour un grand nombre de problèmes correctement traités par l’ordinateur classique. On attend plutôt un ordinateur classique avec des processeurs quantiques dédicacés aux calculs non polynomiaux, un ordinateur mixte en quelque sorte.**

**63. Très peu de conjectures sont démontrées dans le domaine des relations d’inclusions (strictes ou non) entre les diverses classes de complexité classiques et quantiques.**

**BQP qui regroupe les problèmes traitables en temps polynomial par un ordinateur quantique inclut certainement P et est inclus dans PSPACE.**

**Le détail n’est pas connu et le pointillé est là pour le rappeler : il est positionné dans l’état conjecturé le plus probable.**

**Même la position exacte du problème de la factorisation (F) n’est pas connue : on a simplement ordonné les conjectures dans l’ordre des plausibilités croissantes (???, ??, ?).**

**A noter que si F appartient à NPC, alors on aurait que l’ordinateur quantique résoudrait tous les problèmes NP complets en temps polynomial. La plupart des chercheurs estiment que ce serait trop beau pour être vrai.**

**Les problèmes indécidables ne sont pas concernés par les avancées quantiques.**