RFC 9583 : Application Scenarios for the Quantum Internet

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 27 février 2025

Date de publication du RFC : Juin 2024

https://www.bortzmeyer.org/9583.html

Peut-être, dans le futur, nous aurons un Internet quantique, où les communications utiliseront à fond les surprenantes propriétés de la physique quantique. Ce RFC se penche sur les applications que cela pourrait avoir, et les utilisations possibles.

Un Internet quantique, décrit dans le RFC 9340[1], ce serait un Internet où les machines terminales <https://www.bortzmeyer.org/terminal-host.html> et les routeurs utiliseraient des propriétés purement quantiques, comme l'intrication. Ces divers engins seraient reliés par des liens, par exemple des photons circulant en dehors de tout câble, une configuration bien adaptée à l'utilisation de la quantique. Si vous voulez apprendre plus en détail ce que pourrait être un Internet quantique, voyez l'article de Wehner, S., Elkouss, D. et R. Hanson, « "*Quantum internet : A vision for the road ahead*" <http://science.sciencemag.org/content/362/6412/eaam9288.full> », publié dans Science. Rappelons qu'il n'y a pas de perspective réaliste de grand remplacement de l'Internet classique : l'Internet quantique va venir en plus, pas à la place.

À quoi va pouvoir servir un Internet quantique ? On peut imaginer, par exemple, des calculs quantiques répartis, ou de la synchronisation d'horloges atomiques.

Un peu de terminologie, ensuite. La section 2 du RFC définit les termes importants. Ce sont ceux du RFC 9340 plus, notamment :

— Qubit : unité d'information en calcul quantique. Sa valeur, quand on le mesure, est 0 ou 1, comme un bit classique mais, tant qu'il n'a pas été mesuré, ce n'est qu'une probabilité. Diverses particules élémentaires peuvent être utilisées pour faire un qubit, par exemple les photons et, pour chaque particule, tout degré de liberté (comme le spin) peut servir à encoder le qubit.
— Paires de Bell : deux qubits intriqués, par exemple (en utilisant la notation de Dirac) (—00¿+—11¿)/Sqrt(2).

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc9340.txt

— NISQ ("*Noisy Intermediate-Scale Quantum*") : l'état actuel des calculateurs quantiques, petits et faisant plein d'erreurs.
— « Préparer et mesurer » : se dit des protocoles quantiques les plus simples, où on prépare des qubits et où on les mesure ensuite. Le protocole de distribution quantique de clés BB84 est un exemple <https://doi.org/10.1016/j.tcs.2014.05.025>.
— Téléportation : déplacer quantiquement un qubit d'un point à un autre (c'est moins évident que pour déplacer un bit). Notez qu'il existe une différence subtile entre téléporter un qubit et le transmettre mais l'explication de cette différence est au-dessus de mes forces.

Revenons maintenant aux applications, le but de ce RFC. Il y a plusieurs catégories :

— Cryptographie quantique (terme sans doute excessif - il s'agit plutôt d'aider des opérations cryptographiques par la quantique - mais largement utilisé),
— Capteurs quantiques,
— Calcul quantique.

Voyons-les dans l'ordre. D'abord, utilisations de la quantique pour aider la cryptographie. (Au passage, la cryptographie post-quantique est tout le contraire : elle utilise des calculateurs classiques pour faire de la cryptographie qui résiste aux calculateurs quantiques.) Cela inclut :

— Distribution quantique de clés (dont j'ai déjà dit du mal <https://www.bortzmeyer.org/communication-quantique.html>).
— Négociation byzantine rapide : une solution quantique au problème des généraux byzantins <https://dl.acm.org/doi/10.1145/1060590.1060662>.
— Argent quantique : la quantique peut tout, même gérer de l'argent. Plus fort que les cryptomonnaies ! Après tout, une propriété essentielle des états quantiques est le fait qu'on ne puisse pas les copier. C'est certainement utile pour l'argent mais ce n'est pas facile à faire (cf. les attaques décrites dans « "*Cryptanalysis of Three Quantum Money Schemes*" <https://link.springer.com/chapter/10.1007/978-3-030-17659-4_14> »).

Il y a aussi des capteurs quantiques ; intriqués, ils permettent des mesures particulièrement sensibles (voir « "*Multiparameter Estimation in Networked Quantum Sensors*" <https://journals.aps.org/prl/abstract/10.1103/PhysRevLett.120.080501> » ou, par exemple, pour la synchronisation d'horloges, « "*A quantum network of clocks*" <https://arxiv.org/pdf/1310.6045.pdf> »).

On connait également les possibilités de la physique quantique pour le calcul, notamment via la possibilité de casser des algorithmes de cryptographie. On peut envisager des calculateurs quantiques répartis, où plusieurs calculateurs séparés travailleraient ensemble, donnant l'impression d'un calculateur unique. Il pourrait également exister du calcul quantique en aveugle, où le calcul serait fait sur des données, sans avoir les données en question, ce qui serait utile pour la confidentialité. (Oui, cela semble magique, mais c'est souvent comme cela dans le monde quantique, et ce calcul en aveugle est détaillé dans la section 4.2. Voir « "*Private quantum computation : an introduction to blind quantum computing and related protocols*" <https://www.nature.com/articles/s41534-017-0025-3.pdf> ».)

La section 4 présente ensuite des scénarios d'usage plus détaillés, par exemple sur la distribution quantique de clés (voir l'article sceptique <https://cyber.gouv.fr/en/publications/should-quantum-ke
de l'ANSSI), le calcul en aveugle et le calcul quantique réparti.

Tout cela est bien joli mais, pour passer de ces applications futuristes à un vrai Internet quantique, il faut des machines, et les connecter. La section 5 du RFC détaille ce qui sera nécessaire pour ce déploiement. Actuellement, on a quelques centaines de qubits physiques dans les plus gros calculateurs (et ce sont des NISQ, avec beaucoup d'erreurs), ce qui est très insuffisant. Suivant la classification de Wehner, le RFC cite six étapes possibles vers un Internet quantique :

— Première étape, des répéteurs de confiance (et donc pas de sécurité de bout en bout, c'est la situation actuelle de pas mal de réalisations quantiques lourdement vantées dans les médias ignorants, dans les articles technobéats sur la QKD),
— Deuxième étape, quand l'utilisateur final peut lui-même préparer et mesurer des qubits,
— Ensuite, chemin quantique de bout en bout, donc de la vraie distribution quantique de clés, par exemple,

— À la quatrième étape, les répéteurs peuvent agir sur les qubits (section 5.1 pour les détails), ce qui permettra plein d'autres applications comme le calcul en aveugle,
— Puis ils deviennent capables de correction d'erreurs, ce qui évite de consommer plein de qubits physiques pour faire un qubit logique,
— Et enfin, sixième et dernière étape, quand le nombre de qubits sera suffisant pour faire toutes les applications dont on rêve.

Cette image vient de l'article « "*Quantum internet : A vision for the road ahead*" <http://science.sciencemag.org/content/362/6412/eaam9288.full> :

Comme toujours dans un RFC, il y a une section sur la sécurité, qui douche toujours un peu les espoirs. Ce n'est pas tout de communiquer, il faut aussi le faire de manière sûre. Si la distribution quantique de clés résiste à toute tentative d'espionnage (elle est protégée par la physique, et pas par la mathématique mais attention quand même <https://link.aps.org/doi/10.1103/PhysRevA.78.042333>), une autre technologie quantique fait courir des risques à la cryptographie, les calculateurs quantiques peuvent casser des algorithmes très utilisés comme RSA et ECDSA. Dans un monde (très futuriste…) où on aurait des calculateurs quantiques significatifs (CRQC = "*Cryptographically Relevant Quantum Computers*") reliés par un réseau quantique pour qu'ils se partagent les calculs, toutes les clés RSA du monde seraient cassées rapidement. Il est donc important de travailler dès maintenant sur la cryptographie post-quantique.

À ce stade, la constatation est que malheureusement nous n'avons pas encore d'Internet quantique pour faire des ping et des traceroute…