Rapport de la députée Forteza sur les technologies quantiques

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 12 janvier 2020

https://www.bortzmeyer.org/rapport-forteza-quantique.html

Le 9 janvier 2020, la députée Paula Forteza a rendu le rapport « Quantique : le virage technologique que la France ne ratera pas <https://forteza.fr/2020/01/09/quantique-le-virage-technologique-que-l> ». Quelques points sur ce rapport.

Le terme de « quantique » a un fort potentiel de "*hype*" <https://fr.wiktionary.org/wiki/hype> pour les années à venir (surtout depuis l'annonce par Google de l'obtention de la suprématie quantique <https://ai.googleblog.com/2019/10/quantum-supremacy-using-programmable.html>). Dans le contexte de la physique, il désigne quelque chose de clair (mais pas forcément de simple à comprendre !) Appliqué aux technologies, c'est plus compliqué. Et ce rapport couvre toutes les utilisations futures de la quantique, ce qui fait beaucoup. Globalement, le rapport est rigoureux sur la partie scientifique (il y a eu de bons conseillers, et ils ont été bien écoutés, donc des point délicats comme la différence entre qubits physiques et logiques, toujours oubliée par les marketeux, est bien décrite) mais plus contestable sur la partie politique. Je ne vais pas reprendre tous les points (lisez le rapport <https://forteza.fr/wp-content/uploads/2020/01/A5_Rapport-quantique-public-BD.pdf>, vous ne vous ennuierez pas, et vous apprendrez des choses) mais seulement ceux qui me semblent particulièrement discutables.

Le point le plus curieux concerne la distribution quantique de clés (parfois appelée par abus de langage « cryptographique quantique »). La partie technique du rapport note à juste titre les nombreuses limitations (le rapport parle de « verrous ») de cette technique, que ses promoteurs présentent comme la solution magique à tous les problèmes de sécurité de l'Internet (ce qu'elle n'est pas <https://www.bortzmeyer.org/communication-quantique.html>). Mais la partie « propositions » du rapport oublie complètement ces limitations et assène qu'il faut mettre le paquet pour le développement de la QKD. On dirait vraiment que l'analyse de la technologie et les recommandations ont été écrites par des personnes différentes.

Le rapport est plus cohérent sur la question de la cryptographie post-quantique (cf. aussi mon exposé à pas Sage En Seine <https://www.bortzmeyer.org/pas-sage-en-seine-quantique.html>

et le point de vue très différent de Renaud Lifchitz <https://www.nolimitsecu.fr/informatique-quantique>.) Encore que la partie résumée à l'attention des décideurs, comme souvent, présente le problème comme sans doute plus proche qu'il ne l'est (et propose de commencer à déployer les solutions en 2022 !) Le rapport semble pousser au déploiement immédiat d'algorithmes post-quantiques, alors qu'aucun n'est normalisé. (Et, puisqu'il s'agit d'un rapport officiel, on peut noter que le RGS, et notamment son annexe cryptographique, ne sont pas mentionnés.) Si vous voulez en savoir plus sur la cryptographie post-quantique, je vous recommande l'exposé de Magali Bardet lors de la JCSA de juillet 2019 <https://www.afnic.fr/fr/l-afnic-en-bref/actualites/actualites-generales/11553/show/9eme-editio html>.

Ensuite, ce rapport reprend malheureusement le style de tant de rapports officiels précédents : pas d'autre proposition que de donner beaucoup d'argent à Atos ou Thales dans l'espoir que cela fera avancer les choses, meccano institutionnel (créer un comité machin), discours sur la grandeur de la France et sa maitrise de toutes les technologies et toutes les sciences, référence à la "*startup*" magique, croyance que la recherche fondamentale se pilote d'en haut (on annonce bien haut que la quantique est une priorité et paf, cela suffit à ce que les résultats arrivent), et surtout, aucune remise en cause des obstacles que rencontre actuellement la recherche. Par exemple, le rapport propose d'« encourager » (ça ne coûte rien…) les chercheurs à candidater à des programmes de financement européens mais sans se demander pourquoi il n'y a pas davantage de telles candidatures. (C'est en partie parce que les chercheurs passent déjà plus de temps dans la paperasserie et dans la chasse aux subventions que dans la recherche. Mais on ne pouvait pas attendre d'une députée du parti du gouvernement qu'elle critique l'organisation actuelle de la recherche.)

Le rapport propose de fournir un calculateur quantique accessible en ligne (pardon, le rapport dit « "*cloud*" », c'est plus poétique) pour faire du QCaaS ("*Quantum Computing as a Service*"). C'est déjà proposé par IBM <https://quantum-computing.ibm.com/> et AliBaba <http://quantumcomputer.ac.cn/>. Cela ne veut pas dire qu'il soit inutile d'en créer d'autres, meilleurs et/ou différents mais cela ne montre pas une énorme ambition.

D'autre part, certaines propositions auraient mérité d'être développées, notamment sur les moyens à mettre en œuvre. Ainsi, la proposition de créer des enseignements d'algorithmique quantique dans vingt cycles d'enseignement supérieur est une très bonne idée mais pas un mot n'est dit sur le recrutement d'enseignants, alors que justement les compétences en ce domaine ne sont pas largement répandues.

Le rapport, je l'ai dit, est globalement rigoureux, mais dérape quand même parfois par exemple quand, à propos de programmation, il pointe l'importance de développer des langages de programmation adaptés, de haut niveau (ce qui est une très bonne idée) mais cite ensuite comme exemple Q#, qui est justement un langage de très bas niveau, où on manipule les portes logiques directement. Vous imaginez programmer un ordinateur classique ainsi ? Seule la syntaxe de Q# est « de haut niveau », les concepts manipulés ne le sont pas. Au passage, si vous êtes prorgrammeur ou programmeuse, le site de questions/réponses StackExchange a une déclinaison sur le calcul quantique <https://quantumcomputing.stackexchange.com>.

Un point que j'ai apprécié, par contre, est l'insistance sur les « technologies habilitantes ». Il s'agit de toutes les techniques qui permettent de réaliser des dispositifs quantiques, notamment la cryogénie. C'est à juste titre que le rapport rappelle qu'un ordinateur quantique n'est pas seulement composé de qubits, c'est d'abord un gros réfrigérateur.

Sur la forme, je note l'abus de termes en anglais, qui n'aide pas à la compréhension.

Notez que l'IETF a un travail en cours sur la cryptographie post-quantique <https://datatracker.ietf.org/doc/draft-hoffman-c2pq/> et un groupe de recherche sur les réseaux quantiques <https:

//datatracker.ietf.org/rg/qirg/about/>, qui a produit plusieurs documents intéressants <https://datatracker.ietf.org/rg/qirg/documents/> (je vous recommande le RFC 9340 [1], qui explique bien la quantique, avant d'expliquer ce que pourrait être un réseau quantique. Le RIPE-NCC a déjà organisé un hackathon sur ce sujet <https://labs.ripe.net/Members/elena_signorelli/your-quantum-internet-hackathon-report-for-2018>.)

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