L’informatique quantique et le DNS

Bureau du directeur de la technologie de l’ICANN

Paul Hoffman
OCTO-031
11 février 2022

ICANN

TABLE DES MATIERES

Le présent rapport fait partie de la série de documents publiés par le Bureau du directeur de la technologie (OCTO) de l'ICANN. Vous trouverez sur la page des publications de l'OCTO une liste des documents de la série. Si vous avez des questions ou des suggestions par rapport à ces publications, veuillez les envoyer à octo@icann.org.

Ce document soutient la finalité stratégique de l'ICANN qui vise à améliorer la responsabilité partagée du maintien de la sécurité et de la stabilité du système des noms de domaine (DNS) par le biais du renforcement de la coordination du DNS en partenariat avec les parties prenantes concernées. Il s'inscrit dans le cadre de l'objectif stratégique de l'ICANN relatif au renforcement de la sécurité du DNS et du système des serveurs racine du DNS (RSS).

Résumé analytique

Au cours des dernières années, les ordinateurs quantiques ont attiré l'attention de la communauté des experts en sécurité en raison de la possibilité qu'ils puissent compromettre les algorithmes cryptographiques les plus couramment utilisés. Pour l'instant, il n'existe pas d'ordinateurs quantiques suffisamment puissants pour le faire, mais avec les progrès de la technologie, certains algorithmes utilisés aujourd'hui pourraient un jour être facilement cassés par ce nouveau type d'ordinateur. Il est toutefois difficile de prévoir dans combien de temps cela pourrait se produire car la technologie de l'informatique quantique est encore récente et la construction et l'exploitation d'ordinateurs quantiques restent extrêmement coûteuses.

De nouveaux algorithmes supposés résistants aux ordinateurs quantiques sont en cours de normalisation. Le présent rapport passe en revue des travaux récents qui permettent de mieux estimer à quel moment la communauté du système des noms de domaine (DNS) devra envisager l'adoption de nouveaux algorithmes cryptographiques.

1 Introduction

Certains algorithmes de la cryptographie moderne reposent sur la complexité de certains problèmes mathématiques dont la résolution prend énormément de temps. Les ordinateurs quantiques pourraient être en mesure de résoudre ces problèmes beaucoup plus vite, ce qui affaiblirait la sécurité apportée par ces algorithmes. Les ordinateurs basés sur des principes quantiques sont radicalement différents de ceux largement utilisés au cours des 70 dernières années. Dans les ordinateurs quantiques, le traitement des données repose sur des bits quantiques, appelés *qubits*, et non pas sur les bits binaires que l'ensemble des ordinateurs utilisent aujourd'hui.

La construction d'ordinateurs quantiques à grande échelle permettrait de résoudre certains problèmes insolubles pour la technologie informatique actuelle, car les ordinateurs quantiques peuvent traiter simultanément un grand nombre de processus complexes. Les ordinateurs actuels, dits *ordinateurs classiques*, peuvent certes gérer plusieurs processus en parallèle, mais les ordinateurs quantiques peuvent le faire à l'aide de connexions plus efficaces entre les portions de données en cours d'analyse.

Les concepts sur lesquels reposent les ordinateurs quantiques font l'objet de théories depuis près de 50 ans, mais leur construction reste extrêmement difficile, même à très petite échelle. L'information contenue dans les qubits est assez fragile, si bien que ceux-ci doivent être complètement isolés de l'environnement extérieur et gardés à des températures proches de zéro degré Kelvin pendant les calculs. Cela nécessite beaucoup de ressources et d'espace physique. Les qubits sont aussi très sujets aux erreurs pendant les calculs. Un ordinateur quantique a besoin de centaines, voire de milliers de qubits refroidis supplémentaires pour corriger les erreurs de chaque qubit lors du calcul. La fabrication d'un ordinateur quantique avec des millions de qubits pourrait ainsi s'avérer impossible en raison de contraintes liées au refroidissement et à la communication.