Les ordinateurs quantiques pourraient menacer la sécurité informatique

Les ordinateurs quantiques pourraient menacer la sécurité informatique Selon un rapport de l'Académie nationale des sciences, de l'ingénierie et de la médecine des États-Unis, il est urgent de faire évoluer les systèmes de sécurité par chiffrement pour se préparer à l'avènement d'ordinateurs quantiques capables de casser en très peu de temps les technologies de cryptage existantes. Le chiffrement est aujourd'hui le pilier de tous les systèmes de défense cyber. Qu'il s'agisse de protéger les données personnelles et les communications des particuliers ou de sécuriser des réseaux ultra sensibles, le principe repose sur l'idée qu'il faudrait au supercalculateur le plus puissant un temps incommensurable pour casser les algorithmes de cryptage. Toutefois, cette construction sécuritaire pourrait s'effondrer avec l'arrivée d'ordinateurs quantiques qui promettent un bond exponentiel dans la puissance de traitement et pourraient casser le meilleur chiffrement existant. Nous sommes encore très loin d'une telle réalité, mais un groupe d'experts de l'Académie nationale des sciences, de l'ingénierie et de la médecine des États-Unis a décidé de tirer la sonnette d'alarme. Des standards de chiffrement « post quantique »
Dans leur rapport intitulé Quantum Computing Progress and Prospects (2018), ils estiment qu'il est urgent de commencer à créer des systèmes de chiffrement susceptibles de résister à la puissance d'un ordinateur quantique. Selon eux, l'adoption d'une telle cryptographie pourrait prendre une vingtaine d'années. Or, il n'est pas impossible que des ordinateurs quantiques apparaissent avant

cela. Et l'on imagine, dès lors, le danger potentiel que cela pourrait représenter si ces machines étaient utilisées par des États ou des individus pour mener un cyber guerre ou lancer des attaques malveillantes. Le document des experts souligne le fait que nombre d'institutions publiques et privées ont besoin de sauvegarder des données sensibles pendant des décennies et qu'il est, par conséquent, impératif d'anticiper les menaces futures qui pourraient compromettre les systèmes de chiffrement actuels. La solution passe par la définition de nouveaux standards « post quantique » sur lesquels planche notamment le National Institute of Standards and Technology (agence du département du Commerce des États-Unis). Une première série de propositions ont été soumises au NIST le mois dernier, parmi lesquelles figurent notamment celles de l'Inria (BIG QUAKE), des universités de Bordeaux, Limoges et Toulouse (RQC et HQC), Sorbonne Université, CNRS, Inria (Dual Mode MS). Source web par: futura sciences