Où se cache l’avantage quantique ?

Dans quelles situations un ordinateur quantique est-il vraiment plus puissant qu’un ordinateur classique ? C’est une question étonnamment subtile à laquelle les physiciens sont toujours confrontés, des décennies après l’avènement de l’ère quantique.

Il y a plus de quarante ans, le physicien Richard Feynman a souligné que la construction de systèmes reposant sur des principes quantiques permettrait d’accéder à des capacités de calcul supérieures à celles des ordinateurs « classiques ». Ce discours, prononcé en 1981, est souvent considéré comme un événement fondateur de l’informatique quantique. Feynman a terminé sa présentation sur une boutade désormais célèbre : « La nature n’est pas classique, bon sang, et si vous voulez faire une simulation de la nature, vous feriez mieux de la faire avec la mécanique quantique. »

Cette vision s’est concrétisée en 1994 quand le mathématicien Peter Shor a proposé la première utilisation potentiellement révolutionnaire des ordinateurs quantiques. Une importante partie de la sécurité du monde numérique repose sur l’hypothèse que la factorisation de grands nombres est une tâche difficile qui prend du temps. Or Peter Shor a montré comment manipuler les qubits – la version quantique des bits d’information qui peuvent être une combinaison de l’état « 0 » et de l’état « 1 » – pour y parvenir en un clin d’œil, du moins par rapport aux méthodes classiques connues.

LIRE L’ARTICLE