

Un dispositif efficace (voir la figure 3) pour produire des paires de photons intriqués est un oscillateur paramétrique optique : en traversant un cristal spécifique, un photon unique engendre deux photons qui sont intriqués (ici, dont les polarisations sont perpendiculaires).

Il est beaucoup plus difficile d'intriquer deux photons indépendants déjà existants, comme il est nécessaire de le faire dans un analyseur d'état de Bell, car cela implique que les deux photons (A et X) perdent leurs caractéristiques propres. En 1997, notre groupe de recherche (Dik Bouwmeester, Jian-Wei Pan, Klaus Mattle, Manfred Eibl et Harald Weinfurter), travaillant à l'Université d'Innsbruck, a résolu ce problème dans le cadre de notre expérience de téléportation (voir la figure 4). Dans notre expérience, une brève impulsion de lumière ultraviolette produite par un laser traverse un cristal et crée les photons intriqués A et B. Le premier se propage vers Claude, et le second vers Jean. Un miroir renvoie l'impulsion ultraviolette à travers le cristal, où elle crée une autre paire de photons, C et D (ceux-ci sont également intriqués, mais nous

n'utilisons pas leur intrication). Le photon C atteint un détecteur, qui nous avertit que son partenaire D est prêt à être téléporté. Le photon D passe à travers un polariseur, que nous pouvons orienter de toutes les manières imaginables. Le photon polarisé obtenu est notre photon X, celui que nous voulons téléporter, et il est envoyé vers Claude. Après avoir traversé le polariseur, X est un photon indépendant, il n'est plus intriqué. Et même si nous savons quelle est sa polarisation, puisque nous avons réglé le polariseur, Claude, elle, ne la connaît pas. Nous réutilisons la même impulsion ultraviolette pour nous assurer que Claude a les photons A et X en même temps.

Nous devons alors mesurer des états de Bell : pour cela, Claude combine ses deux photons (A et X) en utilisant un miroir semi-réfléchissant, c'est-à-dire un dispositif ayant une couche très mince et translucide d'argenture, de telle sorte qu'un photon qui la frappe a 50 pour cent de chances de la traverser et 50 pour cent de chances d'être réfléchi. En termes quantiques, le photon est une superposition de ces deux possibilités (voir la figure 5).

Supposons maintenant que les deux photons qui arrivent sur le miroir viennent de directions opposées, leurs trajectoires étant alignées de façon que le rayon réfléchi de l'un corresponde au rayon transmis de l'autre, et *vice versa*. Un détecteur attend au bout de chaque rayon. D'ordinaire, les deux photons sont réfléchis indépendamment, et ils ont une chance sur deux d'arriver dans des détecteurs différents. Cependant, si les photons sont impossibles à distinguer et atteignent le miroir au même instant, ils interfèrent quantiquement : certaines configurations s'annulent et ne se réalisent pas, tandis que d'autres se renforcent et sont plus fréquentes. Quand les photons interfèrent, leur probabilité de finir dans des détecteurs différents n'est plus que de 25 pour cent. De plus, ce cas de figure correspond à un état de Bell des deux photons bien particulier parmi les quatre possibles : c'est celui que Claude obtenait précédemment quand elle avait «de la chance». Le reste du temps (75 pour cent des cas), les deux photons arrivent au même détecteur, ce qui correspond aux trois autres états de Bell, sans toutefois permettre de déterminer auquel on a affaire.

Les ordinateurs quantiques

L'application la plus concrète de la téléportation quantique en dehors de la recherche en physique fondamentale est sans doute l'informatique quantique. Un ordinateur classique fonctionne avec des éléments binaires, qui prennent une valeur définie, soit 0, soit 1 ; un ordinateur quantique utilise des bits quantiques, ou *qubit*. Les *qubits* peuvent être dans des superpositions quantiques de 0 et de 1, comme un photon peut être dans une superposition de polarisations horizontale et verticale. En envoyant un seul photon, le téléporteur quantique de base transmet un unique *qubit*.

L'idée d'une superposition de nombres peut sembler étrange, mais, comme le disait Rolf Landauer, d'IBM, «quand nous étions petits et que nous apprenions à compter sur nos doigts classiques et très collants, nous étions bien loin de la mécanique quantique et de la superposition. Nos doigts bien distincts nous donnaient une mauvaise intuition. Nous pensions que nous pouvions lever trois doigts, puis quatre. Nous ne comprenions pas qu'il était possible d'avoir une superposition des deux possibilités».

Un ordinateur quantique travaille simultanément sur de nombreuses entrées différentes. Par exemple, il pourrait faire tourner un algorithme simultanément sur un million d'entrées, en utilisant un nombre limité de qubits, équivalant au nombre d'éléments binaires qu'un ordinateur classique utiliserait pour faire tourner cet algorithme une fois sur une seule entrée. Les théoriciens ont prouvé que les algorithmes tournant sur des ordinateurs quantiques peuvent résoudre certains problèmes plus vite (c'est-à-dire en moins d'itérations) que tous les algorithmes connus tournant sur un ordinateur classique. Parmi ces problèmes, citons la recherche d'éléments dans une base de données, et la factorisation des grands nombres utile pour le codage et le décodage.

Pour l'instant, seuls les composants les plus rudimentaires des futurs ordinateurs quantiques ont été fabriqués : des portes logiques pouvant traiter un ou deux qubits. La mise au point d'un ordinateur quantique, même de faible capacité, est encore éloignée. L'un des problèmes clefs est le transfert fiable des données entre différentes portes logiques ou processeurs, au sein d'un ordinateur quantique isolé ou sur un réseau quantique. La téléportation quantique constitue une solution.

En outre, Daniel Gottesman de Microsoft et Isaac Chuang d'IBM ont récemment démontré qu'on pouvait construire un ordinateur généraliste à partir de trois composants de base : des particules intriquées, des téléporteurs quantiques et des portes agissant sur un seul *qubit* à la fois. Ce résultat est important, car les portes à un *qubit* sont technologiquement beaucoup plus accessibles que les portes à deux qubits. L'astuce pour construire une porte à deux qubits à partir d'un téléporteur consiste à téléporter deux *qubits* de l'entrée de la porte à sa sortie, en utilisant des paires intriquées soigneusement adaptées. Les paires intriquées sont modifiées de sorte que la sortie de la porte reçoive les *qubits* traités comme il convient. La mise en œuvre de la logique quantique arbitraire revient alors à préparer des états intriqués prédéfinis et à les téléporter. Il faut cependant admettre que la mesure de l'état de Bell complet, nécessaire pour la téléportation, est une sorte de traitement à deux *qubits*.

