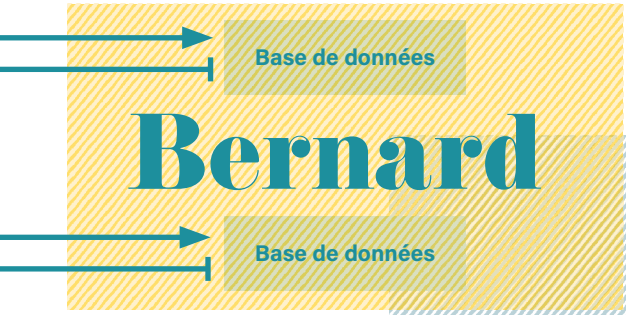

LE PROTOCOLE QUANTIQUE DE CONFIDENTIALITÉ DES REQUÊTES

Comment garantir la confidentialité des requêtes sur internet ? Décrivons le protocole quantique proposé par Seth Lloyd et ses collègues italiens. On suppose qu'Alice effectue des requêtes dans la base de données de Bernard, et qu'elle ne souhaite pas que Bernard sache de quelle requête il s'agit. Dans ce qui suit, la notation de Dirac $|message\rangle$ signifie qu'un message binaire (une suite de 0 ou 1) a été placé dans un registre de mémoire quantique (formé de bits quantiques). Ainsi, la notation $|question\ j\rangle$ signifie qu'Alice souhaite découvrir le $j^{\text{-ième}}$ enregistrement dans la base de données de Bernard. Alice utilise un registre de mémoire contenant n bits quantiques, ce qui lui permet d'effectuer 2^n requêtes distinctes. On suppose qu'Alice connaît le contenu $|réponse\ 0\rangle$ d'un registre de référence, qui est la réponse à la requête $|question\ 0\rangle$. Afin de vérifier que Bernard ne l'espionne pas, Alice soumet deux requêtes successives dans un ordre arbitraire, non connu de Bernard, et attend la réponse après chacune d'elles. Chaque requête est placée dans un registre quantique à n bits quantiques. Par exemple, elle choisit comme première requête $|question\ j\rangle$, tandis que la seconde requête est la superposition quantique : $|question\ j\rangle + |question\ 0\rangle$, qui lui permettra *a posteriori* de vérifier si, oui ou non, Bernard a tenté de découvrir quelle était sa requête. Une fois reçue la première requête, $|question\ j\rangle$, la base de données de Bernard retourne, grâce à l'utilisation d'une RAM quantique, la réponse $|réponse\ j\rangle$. Cette réponse est véhiculée par un second registre quantique, accolé à la question d'Alice. Autrement dit, Alice reçoit le message : $|\psi_1\rangle = |question\ j\rangle\ |réponse\ j\rangle$. Alice envoie ensuite sa seconde requête $|question\ j\rangle + |question\ 0\rangle$. L'interrogation de la base de données de Bernard a pour résultat de renvoyer à Alice sa seconde requête complétée par les réponses, sous la forme : $|\psi_2\rangle = |question\ j\rangle\ |réponse\ j\rangle + |question\ 0\rangle\ |réponse\ 0\rangle$. Bernard ne sait jamais si le registre qu'il reçoit d'Alice est celui contenant la superposition, ou l'autre registre, ce qui signifie qu'il ne peut pas extraire l'information sur j sans risquer de perturber le registre. À la fin du protocole de communication, Alice mesure le contenu du second registre de $|\psi_1\rangle$ pour déterminer $|réponse\ j\rangle$. Elle peut alors utiliser cette réponse pour vérifier que la superposition du second état $|\psi_2\rangle$ a été préservée. Si ce n'est pas le cas, elle sait en vertu du théorème de non-clonage quantique que Bernard a tenté de connaître sa requête. Le protocole quantique de confidentialité des requêtes est en fait très similaire à un protocole de cryptographie quantique, qui permet l'échange sécurisé de clés secrètes.

Michel Planat
Institut FEMTO-ST, Besançon