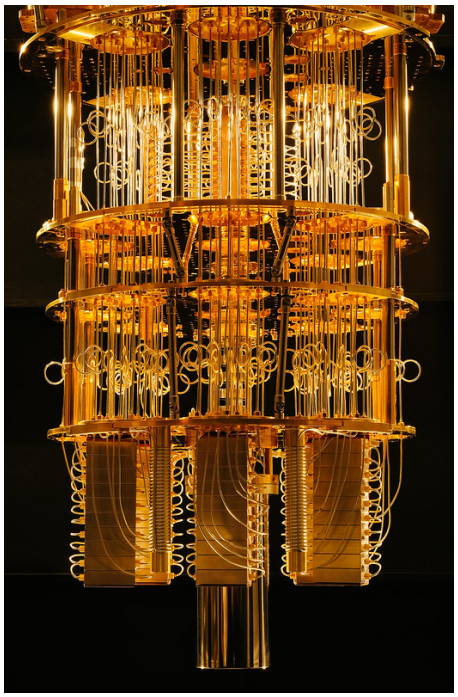
Cryptographie post-quantique à base de réseaux

Une implémentation d'un *Ciphertext-Policy Attribute-Based Encryption*

Quentin Bodini--Lefranc Damya Bouizegarene Rémi Germe
Théodore Halley Manan Kaila

PSC INF04

avril 2024



L'ordinateur quantique d'IBM, l'*IBM Q*.
Source : IBM España

Résumé

Dans le cadre de notre *projet scientifique collectif* (PSC), nous avons cherché à étudier et implémenter un schéma de *chiffrement par attributs*. Il s'agit d'un protocole cryptographique permettant de mettre en place une politique de contrôle d'accès sur les données. Dès lors, il n'est possible pour un utilisateur de déchiffrer le message que s'il a les *attributs* nécessaires.

On propose dans un premier temps une étude détaillée du schéma considéré introduit par Z. Brakerski et V. Vaikuntanathan en 2022 [1] , avant d'aborder plus en détail l'implémentation que l'on en propose. L'apport de notre travail est avant tout de fournir une implémentation fidèle de ce schéma, jusqu'alors jamais réalisée.

Mots-clefs : Cryptographie post-quantique, Réseaux euclidiens, Chiffrement asymétrique, Implémentation.

1. Zvika Brakerski and Vinod Vaikuntanathan. Lattice-inspired broadcast encryption and succinct ciphertext-policy ABE. In Mark Braverman, editor, *13th Innovations in Theoretical Computer Science Conference, ITCS 2022*, volume 215 of *LIPIcs*. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2022