ID de Contribution: **1** Type: **Non spécifié**

Algorithmes quantiques de base

lundi 7 juin 2021 10:00 (1h 15m)

Cet exposé vise à présenter les algorithmes quantiques de base, en particulier ceux ayant un impact potentiel en cryptographie. Parmi eux, les algorithmes de type Simon et Grover qui permettent d'accélérer la recherche de valeurs vérifiant une propriété particulière (par exemple une clé cryptographique), et les algorithmes basés sur l'utilisation de
la transformée de Fourier, comme ceux introduits par Shor qui permettent de factoriser des entiers ou de calculer des logarithmes discrets en temps polynomial.

Orateur: Dr ARNAULT, François (Université de Limoges)

Classification de Session: Quantique