# La cryptographie face à la menace quantique

Le cryptologue Benjamin Wesolowski nous explique comment renforcer les méthodes cryptographiques afin de les rendre résistantes face à l'avènement éventuel de l'ordinateur quantique.

**Comment le mathématicien que vous êtes en est-il venu à concevoir des codes secrets ?**

**Benjamin Wesolowski1**. D'aussi loin que je me souvienne, j'ai toujours aimé les mathématiques. J'ai donc suivi cette passion, qui m'a conduit à intégrer l'École polytechnique fédérale de Lausanne, où j'ai passé ma licence, mon master, puis mon doctorat. C'est là que j'ai vraiment découvert la cryptologie, une discipline qui a tout de suite séduit l'amoureux des mathématiques que j'étais (et que je suis toujours) ! Mais cette histoire a peut-être commencé bien avant : enfant, j'adorais les jeux d'espion dans les magazines qui consistaient à déchiffrer un texte codé.

**Un parcours qui vous a mené jusqu'à devenir lauréat de l'ERC Starting Grant 2023. De quoi s'agit-il ?**

LIRE L'ARTICLE EN FRANCAIS