



(<https://corps.dealersdescience.com/>)



# Damien Robert

## Comment recherche-t-on les mathématiques ?

Damien Robert est directeur de recherche en mathématiques à Inria. Il étudie la cryptographie, discipline qui permet notamment de rendre nos informations confidentielles sur internet. À travers notre échange, Damien Robert nous explique son travail de mathématicien et nous raconte comment il en est arrivé à faire corps avec la recherche.

Damien Robert débute ses études à Lyon en classes préparatoires de mathématiques, qui lui permettent d'entrer à l'École Nationale Supérieure à Paris. Il intègre pour la première fois une équipe Inria à Nancy, lorsqu'il effectue sa thèse en cryptographie. Ce domaine lui permet de lier deux disciplines qui lui sont chères : les mathématiques et l'informatique. Il continue en s'expatriant aux États-Unis, chez Microsoft Research, pour y effectuer un post-doctorat, toujours sur la cryptographie. Il est finalement recruté à Bordeaux, comme chargé de recherche chez Inria, l'institut national de recherche en sciences et technologies du numérique. En juillet dernier, Damien Robert saisit l'opportunité d'être responsable d'une nouvelle équipe-projet au sein du centre Inria de l'université de Bordeaux : CANARI. À la même période, ses dix années d'expérience lui permettent de candidater pour être finalement promu directeur de recherche.

### La cryptographie, ça signifie cryptomonnaie ?

La cryptographie est une discipline vieille de plusieurs millénaires. Elle concerne la cryptomonnaie depuis quelques années, mais ce n'est qu'une petite partie de tout ce qui peut y être associé. La cryptographie est la science des messages secrets, elle était donc déjà utilisée par Jules César pour faire passer des informations confidentielles à ses troupes. De nos jours, elle est notamment utilisée sur internet pour garantir la confidentialité de nos données. Il faut savoir que ces dernières, lorsqu'elles doivent être protégées, sont chiffrées. C'est ainsi que nous retrouvons le lien avec les mathématiques !

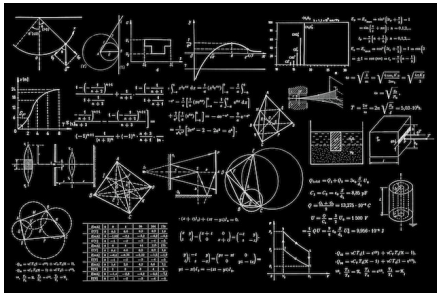


**La manière dont je pratique les mathématiques est même amusante : ça devient des expériences comme en physique ou en chimie.**



## Concrètement, sur quoi Damien Robert travaille ?

Damien Robert travaille à rendre les informations confidentielles toujours plus confidentielles. Il nous explique que l'innovation technologique pourrait faire apparaître dans un futur plus ou moins proche, des ordinateurs quantiques. Ces derniers seraient bien plus performants, pour certains algorithmes, que nos ordinateurs actuels et seraient donc capables de déchiffrer rapidement et facilement les données que nous voulons protéger sur internet. Damien Robert cherche ainsi des méthodes pour les défendre afin qu'elles puissent rester confidentielles durant plusieurs dizaines d'années, dans l'hypothèse où les ordinateurs quantiques seraient un jour créés. Il fait ce qu'on appelle de la cryptographie post-quantique. Il travaille sur ces thématiques dans le cadre du projet CIAO, financé par l'Agence nationale de la recherche.



© Dan Cristian Paduret

## Faire des maths, ce n'est pas juste faire des équations ?

La recherche en mathématiques, particulièrement en cryptographie, est loin de se limiter à écrire des équations sur un tableau. Le travail de recherche de Damien Robert, comme celui de ses comparses chimistes et biologistes, consiste à expérimenter. La différence est qu'il ne teste pas des réactions chimiques dans une fiole ou n'observe pas des cellules au microscope. En réalité, il expérimente en entrant des objets mathématiques sur son ordinateur, dans des algorithmes. Ses derniers lui permettent d'étudier par exemple des formules, qui pourront ensuite être appliquées à la cryptographie. Damien Robert précise cependant qu'une partie du cliché est vraie : les mathématiciens travaillent tout de même en écrivant des chiffres et des nombres. Nous avons d'ailleurs pu le remarquer en passant dans les couloirs de l'institut des mathématiques de Bordeaux (IMB – CNRS, université de Bordeaux, Bordeaux INP), qui héberge les membres de l'équipe-projet CANARI. En effet, les tableaux de nombreux bureaux étaient couverts d'équations très complexes ! Cependant, ces réflexions se font à plusieurs, explique Damien Robert. Les échanges avec les collègues, notamment ceux étudiant des objets plus théoriques, font partie intégrante du travail en recherche scientifique.



Comment devient-on mathématicien ? Nous avons demandé à Damien Robert, ce dernier nous a avoué être passionné des mathématiques depuis l'enfance. C'est aussi avec l'émission *C'est pas sorcier* et les magazines *Sciences et vie Junior* qu'il s'intéresse davantage aux sciences. Un livre va particulièrement le marquer : *Le Théorème du Perroquet*, une intrigue policière tournant autour des mathématiques. C'est après cette lecture qu'en classe de quatrième, il commença à s'amuser à démontrer des théorèmes, comme celui de Pythagore.

Marthe Cazet

Retour sur la page Portraits  
(<https://corps.dealersdescience.com/portraits-scientifiques/>)

## Les partenaires de l'événement