CARTE BLANCHE

Des maths dans le passe sanitaire

Par ÉTiENNE GHYS

Les QR codes sont gorgés de mathématiques. Le passe sanitaire est constitué de 7225 petits carrés blancs ou noirs, rangés en 85 lignes et 85 colonnes, qui permettent d'encoder le statut vaccinal, ou le résultat d'un test, ou le-certificat de rétablissement . Cela pose quelques problèmes mathématiques et infotmatiques très intéressants.

Le premier problème est géométrique . Le lecteur optique qui scanne le QR code voit le carré en perspective, sous la forme d'un quadrilatère quelconque. Il faut donc redresser la perspective: c'est assez facile. Il faut aussi reconnaître le haut et le bas, la droite et la gauche. Là a ussi, c'est assez facile car trois des quatre coins sont ornés par de petits carrés 7 x 7 facilement reconnaissaples. Parfois, le QR code est présenté sur une feuille qui a été pliée ou froissée, et les lignes et les colonnes ne sont pas droites : il faut les rectifier. Tréize carrés 5 x 5, également reconnaissables, sont répartis dans le grand carré pour aider le logiciel à remettre tout cela d'aplomb.

Le deuxième problème vientdu fait que le lecteur peut se tromper car certains petits carrés peuvent être endommagés. Il faut utiliser des codes correcteurs d'erreurs qui produisent des messages volontairement redondants, pour être sûr de récupérer ce dont on a besoin. Les pilotes d'avion le savent depuis longtemps en énonçant « Papa, Tango, Charlie» au lieu de « PTC ». Les QR codes utilisent une méthode plus élaborée, inventée par Irvipg Reed et Gustave Solomon en 1960 et fondée sur des théorèmes profonds d'arithmétique. La lecture peut se fil:i.re-C'Orrettement;n1ême si 30 % éles pt, carrés sont illisibles. Faites une tache d'encre au milieu de votre passe sanitaire e't vo s errezqu'il es,:: ore valable.

Code secret et dentifrice

Enfin, il faut pouvoir garantir l'authenticité du document. Là en core, on utilise des méthodes mathématiques et informatiques très subtiles. Tout le monde peut lire le contenu du certificat (à condition de connaître un peu d'informatique), mais il est accompagné d'une << signature digitale», cryptée et infalsifiable, produite à partir du contenu du message en utilisant un code secret asymétrique. L'idée est que certaines opérations sont faciles à faire et presque irn-'possiblesà défaire. Ne dit-on pas qu'il est plus facile de faire sortir le dentifrice du tube quede l'yfaire entrer? Le tube en question est encore mathématique,fondé sur de l'arithmétique du XIX• siè cle, grandement améliorée par des informaticiens du XX•. Grâce à ces méthodes, l'application Tous-AntiCovid Verif peut garantir l'authenticité: on peut vérifier une signature qu'un faussaire n'aurait pas pu produire.

Tout n'est pas parfait pour autant et les malversations sont possibles. Des codes d'accès aux serveurs de i,\ssurance-maladie • peuvent être dérobés, ou un soignant mal-honnête pourrait faire mi faux certificat de vaccination . D'autre part, TousAnti - Covid Verif ne garantit que la validité du passe et ne donne pas d'au.tres informations que le nol)1et la date de naissance. Le QR code contient néanmoins d'autres données, comme la date de vaccination , le type de vaccin, etc., destinées aux passages de frontières et qui ne devraient pas être accessibles à tous. Même si ce n'est pas légal, d nombreux sites Internet permettent pourtant de lire et de stocker le contenu c;omplet des passes sanitaires.

Deux siècles de mathématiques se sont écoulés depuis que les travaux pionniersde Carl Friedrich Gauss ou Evariste Galois ont permis l'émergeQce de la cryptographie moderne . Ils auraient été les premiers surpris de voir qu'ils sont à l'origine de ces petits carrés npirs et blancs. La science prend son temps et réserve des surprises. ■

Etienne Ghys
Mathématicien, secrétaire perpétuel de l'Acadé mie des sciences, directeur de recherche (CNRS) a·l'ENS Lyon.
etienne.ghys@ens-lyon.fr