[MATHÉMATIQUES]

MESSAGE BIEN ARRIVÉ ?

Pour qu'un message soit acheminé de façon fiable et adressé à la bonne personne, la transmission de l'information s'entoure de règles de sécurité auxquelles les mathématiques apportent leur contribution. Ingénieusement utilisés dans l'industrie, certains grands principes mathématiques sont ainsi impliqués dans la construction de codes correcteurs. Ces codes peuvent détecter, voire corriger, les erreurs susceptibles de survenir lors du stockage ou de la transmission de l'information. « Ils sont élaborés différemment selon le support d'information et le canal de diffusion concernés, explique Philippe Lebacque au Laboratoire de mathématiques de Besançon. Mais dans tous les cas, et par définition, ils consistent à ajouter de la redondance à l'information afin de garantir l'intégrité du message initial ».

Les codes correcteurs peuvent détecter, voire corriger, les erreurs susceptibles de survenir lors du stockage ou de la transmission de l'information

Un exemple de code élémentaire consiste à ajouter un bit dit de parité à un mot formé de 0 et de 1, de sorte que la somme des bits soit paire. Si la valeur d'un bit change lors de la transmission, cette somme sera impaire, ce qui témoigne d'une erreur de transmission. Les codes linéaires, eux, sont intéressants pour la rapidité et le faible coût d'encodage et de décodage.

La téléphonie mobile a par exemple recours aux systèmes suivants : les turbo codes, basés sur l'entrelacement des données, et les codes de Reed-Solomon, consistant à « évaluer des polynômes », qui sont des sommes de puissances des éléments d'un corps fini.

Si ces codes sont largement utilisés dans l'industrie, ils font aussi l'objet de recherches fondamentales. Philippe Lebacque étudie les codes de Goppa, codes géométriques généralisant les codes de Reed-Solomon. Il ne s'agit plus ici de travailler avec des polynômes, mais avec des espaces de fonctions rationnelles sur des courbes ou des surfaces algébriques : c'est l'évolution qui sous-tend les travaux de recherche menés au LMB dans ce domaine.

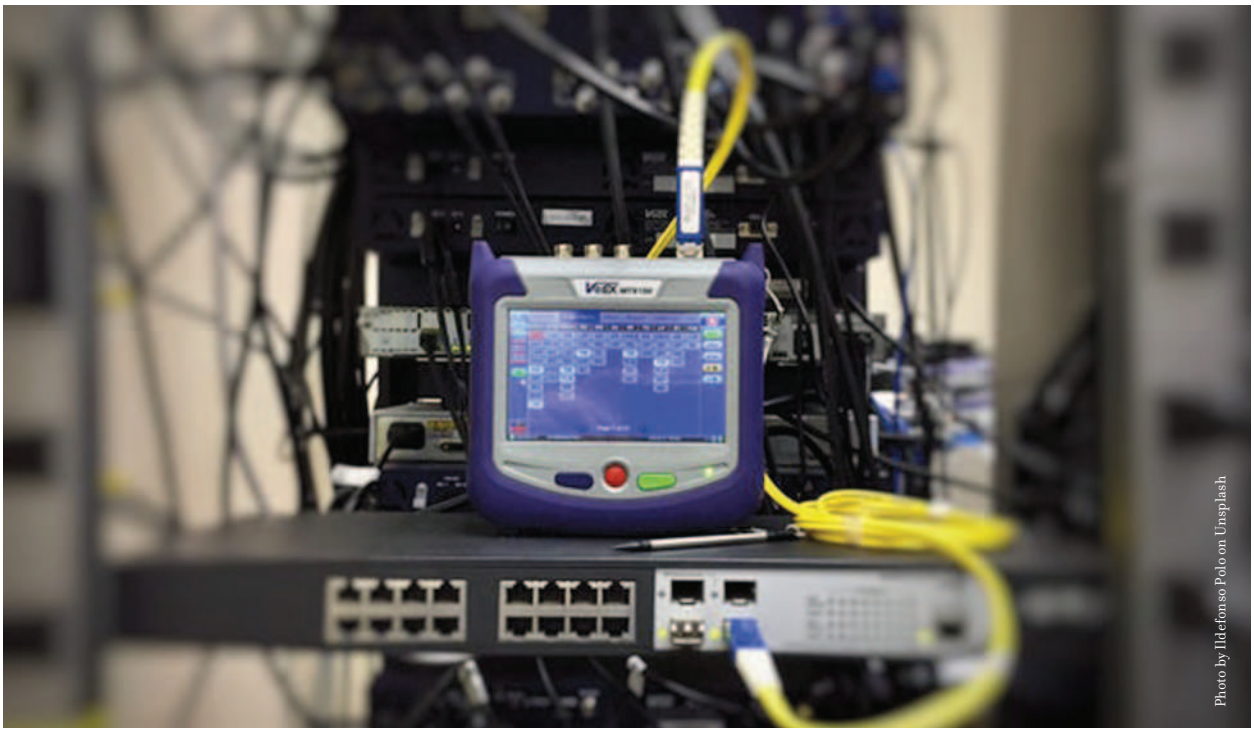

Photo by Ildefonso Polo on Unsplash

LA CULTURE DU SECRET

La cryptographie est une méthode également très répandue pour sécuriser l'information. Elle est omniprésente dans notre vie de tous les jours. Elle peut s'appuyer sur la théorie des nombres et la géométrie arithmétique, et se scinde en deux familles.
Les systèmes symétriques comportent deux clés secrètes, chacune détenue par l'un et l'autre des deux interlocuteurs, ce qui assure la fiabilité de l'information. Ces clés peuvent être partagées avec le fournisseur d'accès : l'inscription d'une clé secrète sur la carte SIM d'un mobile permet d'identifier l'interlocuteur sur le réseau.
Les systèmes asymétriques comportent une clé publique et une clé secrète, et assurent la confidentialité d'une information sur un réseau public. Ils concernent par exemple des messageries instantanées telles que WhatsApp ou Facebook Messenger. Dans cette configuration, ni les fournisseurs d'accès, ni l'État ne sont capables de décrypter les conversations privées. À chaque message transmis correspond un code unique : si quelqu'un perce le secret d'une clé, il ne pourra dans tous les cas avoir accès qu'à un seul message.
« De tels systèmes sont critiqués dans le cadre de la lutte contre le terrorisme, mais appréciés par les populations des pays totalitaires. »
Dans le domaine de la cryptographie, Philippe Lebacque et son équipe travaillent au LMB sur des outils permettant d'élaborer des cryptosystèmes susceptibles de résister au décryptage par ordinateur quantique.

[INFORMATIQUE]

CONNECTE-TOI, JE TE DIRAI COMMENT TU DORS

Les modèles mathématiques sont aussi partie prenante du développement d'applications informatiques de plus en plus spécialisées et opérationnelles sur mobiles. À la Haute Ecole Arc Ingénierie, Aïcha Rizzotti-Kaddouri est chercheuse et enseignante en applications mobiles et dispositifs portables. Ses différents projets de recherche s'appuient sur les ressources de l'établissement ou ceux de la HES-SO[1].
Les moyens et compétences en informatique permettent de maîtriser entièrement tous les maillons de la chaîne : acquisition des données, connexion Bluetooth, transmission des informations au serveur, gestion des bases de données, traitement des données, éventuellement envoi de messages d'alarme aux utilisateurs, le tout en assurant la sécurité du transfert et du stockage des informations. « Une application dédiée à la question du sommeil a par exemple été élaborée avec des étudiants de master, explique l'informaticienne. Ce travail a fait l'objet d'une communication lors d'une conférence internationale fin 2018. »
L'innovation réside dans le traitement combiné d'informations provenant de différentes sources, par une interface mobile.
Le concept sous-tend l'ensemble des travaux menés sous la houlette d'Aïcha Rizzotti-Kaddouri. Des données physiologiques, captées par un « bracelet de recherche » porté par une personne, sont associées à des informations d'ordre biologique et contextuel. Les données brutes transitent par l'intermédiaire du mobile vers des serveurs dédiés au *machine learning*, et le résultat personnalisé est envoyé à l'application mobile de l'utilisateur. Dans le cas du sommeil, on accède ainsi à des indications non seulement sur sa durée effective, mais aussi sur sa qualité. S'il n'est pas encore possible d'en qualifier les phases (sommeil profond, paradoxal…), cette analyse plus fine encore figure aux objectifs de développement de l'application. Dans la même veine, la somnolence est également dans la ligne de mire des chercheurs. En collaboration avec la Ligue pulmonaire neuchâteloise, un travail mené avec des

Interface mobile créée à la Haute Ecole Arc pour le suivi de la durée et de la qualité du sommeil

[1] *HES-SO : Haute Ecole Spécialisée de Suisse Occidentale*