ACTUALITÉS

MATHÉMATIQUES

DES RETRAITS SÉCURISÉS GRÂCE À LA RELATIVITÉ RESTREINTE

Quand, lors d'un retrait d'argent au distributeur, on entre son code secret, il y a un risque de se le faire voler. Mais grâce à un protocole sécurisé, il est possible de s'authentifier sans dévoiler d'information exploitable par un fraudeur.

Comment confirmer votre identité à un distributeur de billets sans taper votre code secret ? Un protocole sécurisé, reposant sur la relativité restreinte, a été mis en œuvre.

Quand vous retirez de l'argent à un distributeur, vous devez taper un code secret pour confirmer votre identité. Cette opération est un point faible du système. De toute évidence, vous devez entrer votre code à l'abri de regards indiscrets. Mais plus difficiles à détecter, certains escrocs équipent des distributeurs de faux claviers ou de faux lecteurs de cartes qui enregistrent toutes vos informations. Existe-t-il une solution pour sécuriser cette étape d'identification ? En 1985, Shafi Goldwasser, du MIT, et ses collègues ont introduit le concept de preuve à divulgation nulle de connaissance. Dans le cas du distributeur, ce protocole permet de confirmer votre identité sans révéler d'informations (votre code secret) qu'un tiers mal intentionné pourrait exploiter, mais, pour des raisons techniques, il était difficile de le mettre en œuvre. Cependant, Sébastien Designolle, avec ses collègues de l'université de Genève et de l'université McGill à Montréal, vient d'en faire une démonstration concrète en s'appuyant sur la relativité restreinte.

En quoi consiste une preuve à divulgation nulle de connaissance ? Imaginez que vous ayez inventé une machine révolutionnaire et que vous craigniez qu'on vous vole vos idées. Comment prouver à autrui que vous avez bien construit l'objet sans en révéler les détails ? C'est là qu'intervient la preuve à divulgation nulle de connaissance. Elle consiste en un « fournisseur de preuve » et un « vérificateur ». Ce dernier, grâce à un jeu de questions-réponses, s'assure que le fournisseur de preuve a bien en sa possession ce qu'il affirme. Mais à la fin, le vérificateur n'a aucun détail sur la machine à part la garantie qu'elle existe.

La plupart des protocoles conventionnels de preuve à divulgation nulle d'information impliquent de résoudre des problèmes mathématiques difficiles telle la décomposition de grands nombres en leurs facteurs premiers. La robustesse du système dépend donc de la puissance des ordinateurs utilisés pour élucider le problème mathématique. Or les progrès techniques peuvent mettre en péril ces approches. En 1988, Avi Wigderson, à l'institut des études avancées de Princeton, et ses collègues ont montré

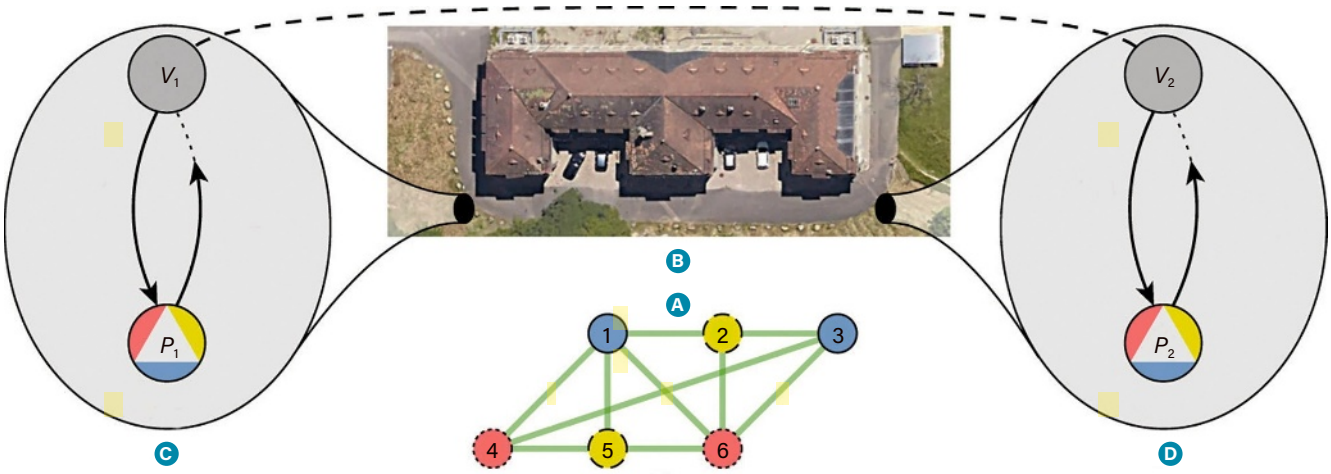

Schéma synthétique du protocole mis en place par Sébastien Designolle et ses collègues. Le graphe colorié *(A)* est partagé entre les deux dispositifs du fournisseur de preuve. Dans l'expérience, les deux dispositifs sont situés à 60 mètres l'un de l'autre *(B)*. Le vérificateur choisit au hasard une paire de sommets connectés par une arête, puis interroge simultanément les deux fournisseurs et demande à chacun d'annoncer la couleur d'un des deux sommets *(C, D)*. En répétant la procédure un grand nombre de fois, il est possible de s'assurer de l'identité du fournisseur de preuve.

qu'il était possible d'implémenter le protocole de preuve à divulgation nulle d'information tout en contournant le problème des capacités de calcul pour casser le code. L'idée consiste à avoir plusieurs fournisseurs de preuve qui essayent de convaincre le vérificateur. Le principe est le même que celui qui revient à interroger deux suspects d'un braquage dans deux cellules différentes pour voir si leurs réponses concordent ou s'ils sont en train de mentir et d'inventer des alibis.

Dans leur expérience, Sébastien Designolle et ses collègues ne cherchent pas à factoriser des grands nombres, mais à analyser un graphe colorié avec trois couleurs. Un graphe est constitué de sommets reliés par des arêtes. Pour un graphe donné, il est très difficile de montrer s'il est possible de le colorier avec seulement trois couleurs de sorte que toutes les paires de sommets reliés par une arête soient de couleurs différentes. Pour le cas qui intéresse les chercheurs, cela garantit qu'un espion ne pourrait pas facilement déterminer le coloriage d'un graphe.

Ici, deux fournisseurs de preuve partagent un graphe dont ils connaissent le coloriage. Le vérificateur choisit au hasard une paire de sommets connectés par une arête, puis interroge simultanément les fournisseurs et demande à chacun d'annoncer la couleur d'un des deux sommets. Le vérificateur itère de nombreuses fois cette opération pour s'assurer de la cohérence des réponses des deux fournisseurs de preuve. Dans l'expérience, le graphe contient 588 sommets et 1097 arêtes. Le vérificateur reproduit le test environ 500000 fois pour garantir la sécurité du protocole. Il peut ainsi confirmer l'identité des fournisseurs de preuve, sans pour autant connaître le coloriage du graphe (pour être précis, les fournisseurs de preuve partagent une série de coloriages qu'ils changent de la même façon à chaque question).

La sécurité du système repose sur les lois de la physique

Comme pour les suspects d'un braquage, les deux fournisseurs de preuve ne doivent pas pouvoir communiquer pour synchroniser leurs réponses. Il faut que le système de question-réponse opère plus rapidement que le temps nécessaire à un signal pour transiter d'un fournisseur de preuve à l'autre. Rappelons que la lumière se déplace dans le vide à la vitesse de 300000 kilomètres par seconde, une vitesse qui ne peut être dépassée d'après la relativité restreinte. Avec un distributeur de billets large de 1 mètre, la personne qui veut s'identifier utiliserait deux dispositifs servant de fournisseurs de preuve qu'elle insérerait aux deux extrémités de la machine. Le système devrait alors réaliser chaque test en moins de 3,3 nanosecondes ! Ce qui semblait techniquement infaisable.

Néanmoins, avec un protocole optimisé, les chercheurs s'en approchent. Dans une expérience, les deux fournisseurs de preuve sont distants de 400 mètres et les questions sont synchronisées grâce à une horloge GPS, dans une autre la distance est de seulement 60 mètres et la synchronisation se fait avec une fibre optique. Chaque test est effectué assez vite de sorte que les fournisseurs de preuve ne puissent pas communiquer entre eux, contraints par la relativité restreinte. Ces résultats montrent que le protocole d'identification sans divulgation d'information peut être implémenté sur des distances assez courtes. Et qu'il serait même encore possible de les réduire.

« Cette approche est vraiment intéressante, souligne Nicolas Brunner, physicien à l'université de Genève et coauteur des travaux, car la sécurité du système repose sur les lois de la physique, de la relativité restreinte, et non plus sur une hypothèse limitant le pouvoir de calcul ou le niveau de technologie de l'espion. » ■

Sean Bailly

P. Alikhani *et al.*, *Nature*, vol. 599, pp. 47-50, 2021