UNIVERSITÉ DE GENÈVE

COMMUNIQUÉ DE PRESSE

Genève | 1er novembre 2021

ATTENTION: sous embargo jusqu'au 3 novembre 2021, 17h heure locale

Sécuriser les transferts de données grâce à la relativité

Une équipe de l'UNIGE a implémenté une nouvelle manière de sécuriser les transferts de données fondée sur le principe physique de la relativité.

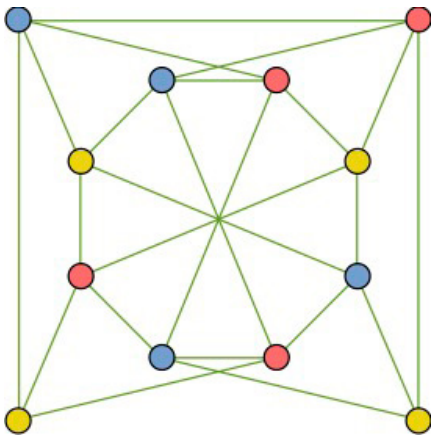
Le volume des données transférées ne cesse de croître, sans qu'on puisse pour autant garantir la sécurité absolue de ces échanges, comme en témoignent les cas de piratage fréquemment révélés par les médias. Pour lutter contre le hacking, une équipe de l'Université de Genève (UNIGE), en collaboration avec des chercheurs de l'Université McGill (Canada), a mis au point un nouveau système fondé sur la preuve à divulgation nulle de connaissance, dont la sécurité repose sur le principe physique de la relativité: aucune information ne peut voyager plus vite que la lumière. Ainsi, un des principes fondamentaux de la physique moderne permet de sécuriser le transfert des données. Ce systèmes permet notamment à des utilisateurs de s'identifier en toute confidentialité sans divulguer la moindre information personnelle, promettant des applications dans le domaine de cryptomonnaies et de la block-chain. Ces résultats sont à lire dans la revue *Nature*.

A l'heure actuelle, lorsqu'une personne – que l'on nomme le prouveur – veut confirmer son identité, par exemple lorsqu'elle veut retirer de l'argent à un bancomat, elle doit fournir ses données personnelle au vérificateur, dans notre exemple la banque, qui traite ces informations (le numéro d'identification et le code pin, par exemple). Tant que le prouveur et le vérificateur sont les seuls à connaître ces données, la confidentialité est garantie. Si d'autres personnes mettent la main sur ces informations, par exemple en piratant le serveur de la banque, la sécurité est compromise.

La preuve à divulgation nulle de connaissance comme solution

Pour contrer ce problème, il faudrait que le prouveur puisse confirmer son identité, sans pour autant rendre accessibles ses données personnelles: c'est le principe de la preuve à divulgation nulle de connaissance. «En d'autres termes, lorsque je vais vouloir prouver quelque chose à quelqu'un, je ne vais pas lui démontrer les étapes qui vont servir de preuves, car la personne aurait accès à toutes les informations et pourrait les reproduire, explique Nicolas Brunner, professeur au Département de physique appliquée de la Faculté des sciences de l'UNIGE. Au contraire, je vais parvenir à lui apporter la preuve demandée, sans pour autant lui transmettre la moindre information la concernant, empêchant toute reprise des données.»

Le principe de la preuve à divulgation nulle de connaissance, inventé au milieu des années 80, est mis en pratique depuis quelques années, notamment pour la cryptomonnaie. Ces implémentations souffrent toutefois d'une faiblesse, puisqu'elles sont fondées sur une hypothèse mathématique (le fait qu'une fonction de codage soit difficile à décoder). Si cette hypothèse venait à être réfutée – ce qu'on ne peut pas exclure–, la sécurité est compromise car les données deviendront accessibles. Aujourd'hui, l'équipe genevoise démontre en pratique un système radicalement différent: une preuve à divulgation de connaissance nulle relativiste. La sécurité y est fondée sur un concept de physique, le principe de la relativité,



Un graphe avec son 3-coloriage. Pour chaque arrête, on vérifie que les deux sommets connectés sont de couleurs différentes.

Illustrations haute définition

et non plus sur une hypothèse mathématique. Le principe de la relativité – soit que l'information ne voyage pas plus vite que la lumière – est un pilier de la physique moderne, pas près d'être remis en question. Le protocole des chercheurs genevois offre donc une sécurité parfaite et garantie sur le long terme.

Une double vérification fondée sur un problème de trois-colorabilité

L'implémentation d'une preuve à divulgation nulle de connaissance relativiste implique deux paires distantes de vérificateur/prouveur, ainsi qu'un problème mathématique extrêmement difficile à résoudre. «Nous utilisons un problème de trois-colorabilité. Ce type de problème est constitué d'un graphe fait d'un ensemble de points connectés ou non par des liens, explique Hugo Zbinden, professeur au Département de physique appliquée de l'UNIGE. Chaque point est colorié par l'une des trois couleurs possibles – vert, bleu ou rouge –, et deux points qui sont liés entre eux ne doivent pas être de la même couleur.» Ces problèmes en trois colorabilités, ici fait de 5'000 points pour 10'000 liens, sont en pratique impossibles à résoudre, car il faut essayer toutes les possibilités. Dès lors, pourquoi faut-il deux paires de vérificateur/prouveur?

«Pour confirmer leur identité, les prouveurs ne devront plus fournir un code, mais démontrer au vérificateur qu'ils connaissent une manière de trois-colorier un certain graphe, poursuit Nicolas Brunner. Pour s'en assurer, les vérificateurs vont choisir au hasard un grand nombre de paires de points du graphe connecté par un lien, puis demander à leur prouveur respectif de quelle couleur est le point. Cette vérification se faisant de manière quasi simultanée, les prouveurs ne peuvent pas communiquer entre eux pendant le test, et ne peuvent donc pas tricher.» Ainsi, si les deux couleurs annoncées sont toujours différentes, les vérificateurs sont convaincu de l'identité des prouveurs, car ceux-ci connaissent effectivement un trois-coloriage de ce graphe. «C'est comme lorsque la police interroge deux criminels en même temps dans des bureaux séparés: il s'agit de contrôler que leurs réponses concordent, sans leur laisser la possibilité de communiquer entre eux», image Hugo Zbinden. Ici les questions étant quasi simultanées, les prouveurs ne peuvent pas se transmettre d'information, car il faudrait que celle-ci voyage plus vite que la lumière, ce qui est impossible. Finalement, pour éviter que les vérificateurs ne parviennent à reproduire le graphe, les deux prouveurs remanient sans cesse, et de manière coordonnée, le code couleur: ce qui était vert devient bleu, le bleu devient rouge, etc. «Ainsi, la preuve est faite et vérifiée, sans pour autant révéler la moindre information sur celle-ci», se réjouit le physicien genevois.

Un système fiable et ultra rapide

En pratique cette vérification est effectuée plus de trois millions de fois, le tout en moins de trois secondes. «Il s'agirait alors d'attribuer un graphe encodé à chaque personne», poursuit Nicolas Brunner. Dans l'expérience des chercheurs genevois, les deux paires de prouveur/vérificateur sont distantes de 60 mètres, afin de s'assurer qu'ils ne puissent pas communiquer. «Mais ce système peut déjà être utilisé par exemple entre deux succursales bancaires et ne nécessite aucune technologie complexe ou coûteuse», dit-il. Toutefois, l'équipe de recherche estime que dans un avenir très proche, cette distance pourra être réduite à 1 mètre. Dès qu'un transfert de données doit être fait, ce système de preuve à connaissance nulle relativiste garantirait une sécurité absolue du traitement des données et ne pourrait être hacké. «En quelques secondes, on garantirait une confidentialité absolue», conclut Hugo Zbinden.

contact

Nicolas Brunner
Professeur ordinaire
Département de physique appliquée
Faculté des sciences
+41 22 379 43 68
Nicolas.Brunner@unige.ch

Hugo Zbinden
Professeur associé
Département de physique appliquée
Faculté des sciences
+41 22 379 05 04
Hugo.Zbinden@unige.ch

DOI: 10.1038/s41586-021-03998-y

UNIVERSITÉ DE GENÈVE
Service de communication
24 rue du Général-Dufour
CH-1211 Genève 4

Tél. +41 22 379 77 17

media@unige.ch
www.unige.ch