DES PROGRÈS BIENVENUS EN CRYPTOLOGIE

L'art du chiffrement progresse: une percée inattendue a été réalisée concernant l'existence des fonctions «à sens unique», essentielles en cryptologie. Ce progrès mathématique nous rapproche d'un monde où la sécurité sera assurée.

L'AUTEUR

JEAN-PAUL DELAHAYE
professeur émérite à l'université de Lille et chercheur au laboratoire Cristal (Centre de recherche en informatique, signal et automatique de Lille)

La cryptologie traite de la cryptographie (le chiffrement des messages), de la cryptanalyse (les méthodes pour casser les codes secrets), de l'art de fabriquer des suites pseudoaléatoires et des méthodes pour élaborer des systèmes de signatures numériques. Cette science est particulièrement difficile et on ignore souvent qu'elle repose, pour l'essentiel, sur des hypothèses mathématiques que l'on n'a pas encore réussi à démontrer.

Les chercheurs sont persuadés que les méthodes qu'ils retiennent et recommandent sont sûres et que celles utilisées dans le domaine de la sécurité informatique (commerce en ligne, cartes bancaires, communications chiffrées, etc.) ont été soumises à toutes sortes de tests et de filtres qui ont éliminé les plus fragiles. Reste que les mathématiciens n'ont pas démontré que les méthodes utilisées en pratique sont inviolables. De telles démonstrations existent certainement: «Nous devons savoir, nous saurons» (*«Wir müssen wissen. Wir werden wissen»*), affirmait le mathématicien allemand David Hilbert... mais aujourd'hui nous n'en disposons pas!

Pour cette raison, toute avancée théorique qui nous rapproche d'une situation où l'on démontrerait l'inviolabilité absolue des méthodes utilisées en cryptologie est importante. Une telle avancée qui concerne les fonctions «à sens unique» vient d'être obtenue.

Qu'est-ce qu'une fonction à sens unique? Pour une fonction f de x à sens unique, il est facile de calculer $f(x) = y$, mais l'inverse n'est pas vrai: il est difficile pour un y donné de trouver un x tel que $y = f(x)$. Ainsi, comme nous le verrons plus loin, s'il est facile de multiplier des nombres entiers, il est difficile de mener l'opération inverse, c'est-à-dire de trouver les diviseurs d'un nombre.

En informatique et dans la suite de cet article, «algorithme rapide» signifie algorithme fonctionnant en temps polynomial, c'est-à-dire en un nombre d'étapes majoré par la valeur d'un polynôme de la variable «taille des données». On utilise le mot «temps» car chaque étape prend un certain temps. Un calcul facile est un calcul faisable par un algorithme rapide.

Prenons un exemple pour illustrer ce que l'on entend par temps polynomial. Quand on calcule $2n$ pour un entier n comportant l chiffres décimaux (l est la longueur de la donnée n) il faut faire un nombre d'opérations élémentaires (appel à une table de multiplication ou d'addition, report de retenue, décalage) qui est inférieur à $2l$ (polynôme $2l$). Par exemple:
$2\times347 = 2\times7+(2\times4)\times10+(2\times3)\times100$
$= 4+10+8\times10+6\times100 = 4+9\times10+6\times100 = 694$
(un premier passage ne prend pas en compte les retenues) soit l opérations, un second passage fait le report des retenues, soit au plus l opérations. En tout on a au plus $2\times l$ opérations. Si le nombre n avait 100 chiffres, on aurait le résultat avec un maximum de 200 opérations. L'addition et la multiplication apprises à l'école sont de tels algorithmes rapides.

Mentionnons une dernière précision. Il existe une méthode de chiffrement prouvée

Jean-Paul Delahaye a récemment publié: **Au-delà du Bitcoin** (Dunod, 2022).

inviolable, celle du « masque jetable » (*voir l'encadré 3*), mais elle exige, pour chiffrer un message, une clé de chiffrement aléatoire de la même taille que le message, et on ne peut l'utiliser qu'une fois. Cela rend la méthode inutilisable sauf dans quelques rares cas. La recherche de méthodes sûres ne s'intéresse donc qu'aux méthodes utilisant des clés de chiffrement courtes et réutilisables. Tous les travaux évoqués ici se situent dans ce cadre.

DES FONCTIONS PRÉSUMÉES À SENS UNIQUE

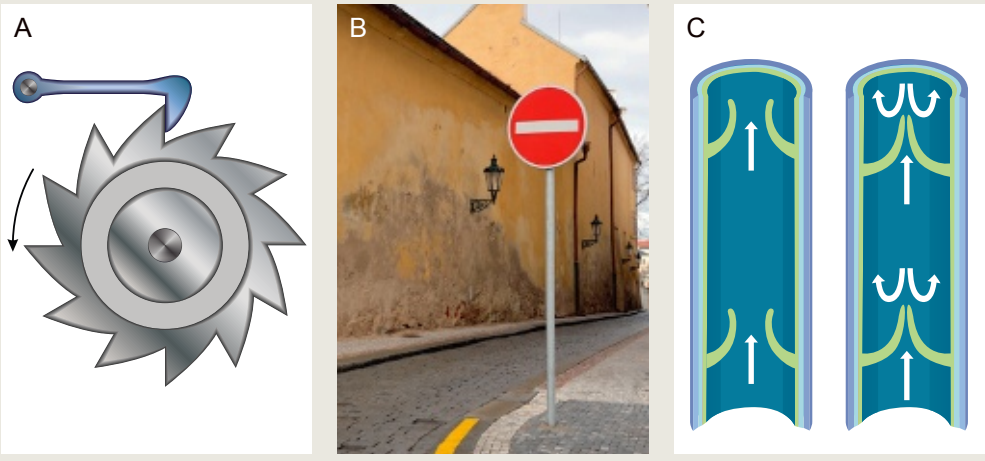
Récemment, les mathématiciens Yanyi Liu et Rafael Pass, de l'université Cornell, aux États-Unis, ont établi des liens entre l'existence de fonctions à sens unique et la théorie de la complexité de Kolmogorov. Cette théorie, qui traite de la complexité des objets numérique (par exemple un message chiffré), appartient à un autre domaine de l'informatique qu'on pensait sans rapport direct avec la cryptologie. Les résultats obtenus ne résolvent pas totalement l'énigme des fonctions à sens unique, mais lui font faire un bond en avant qui a été salué par toute la communauté des codes secrets et a déclenché une série de travaux dont on espère qu'ils porteront de nouveaux fruits.

Les fonctions à sens unique permettent de faire un peu tout ce qu'on souhaite en cryptologie : définir des méthodes de chiffrement à clé secrète résistantes aux attaques ; programmer des générateurs pseudoaléatoires dont personne ne peut deviner le fonctionnement, même en les observant fonctionner pendant longtemps ; proposer des signatures électroniques dignes de confiance. Les fonctions à sens unique sont ainsi un composant de base à partir duquel on construit les fonctions les plus utiles de la sécurité informatique. Aussi, les réponses aux questions autour des fonctions à sens unique fourniraient les démonstrations mathématiques qui manquent pour garantir définitivement l'inviolabilité des méthodes utilisées aujourd'hui en cryptologie.

Reprenons l'exemple de la plus simple des fonctions présumées à sens unique, le produit de nombres entiers : au couple d'entiers $x = (a, b)$, cette fonction associe rapidement $f(x) = a \times b$, le produit de a et de b. Elle est présumée à sens unique car on ne connaît aucun algorithme rapide qui l'inverse, c'est-à-dire qui,

SENS UNIQUE POUR NOS ARTÈRES… ET LA CRYPTOLOGIE

1 **Partout dans le monde, on a besoin de systèmes qui ne fonctionnent que dans un sens. En mécanique on utilise des cliquets *(A)*. Sur la route, chacun connaît les sens uniques *(B)*. En biologie, les veines et les artères doivent ne laisser passer le sang que dans un sens et des valves forcent cette circulation en sens unique *(C)*.**
Les analogues mathématiques de ces sens uniques sont les fonctions à sens unique : passer de *x* à *f(x)* est rapide, mais connaissant seulement *y*, trouver un *x* tel que *f(x)* = *y* est difficile.
Une fonction *f* à sens unique peut être calculée efficacement, mais toute méthode algorithmique rapide de calcul utilisant éventuellement le hasard et tentant d'inverser *f* échoue statistiquement.
S'il existe une fonction à sens unique alors la conjecture mathématique P ≠ NP est vraie. Rappelons que cette conjecture, considérée comme la plus importante de l'informatique théorique, affirme qu'il existe des problèmes dont on peut vérifier la solution en temps polynomial, mais qu'on ne peut pas résoudre en temps polynomial. Il n'est pas vrai cependant que résoudre la conjecture P ≠ NP permettrait de proposer une fonction à sens unique. Prouver l'existence de fonctions à sens unique est donc un problème plus difficile que résoudre la conjecture P ≠ NP. On connaît grâce à un résultat récent une propriété équivalente à l'existence de fonctions à sens unique.
Ce progrès inattendu est une avancée théorique profonde dans un domaine où les blocages sont très forts.



© Fouad A. Saad/Shutterstock ; © Offscreen/Shutterstock ; © Motion Drama/Shutterstock

pour tout nombre n (qui n'est pas un nombre premier), calcule rapidement au moins une factorisation de n sous la forme du produit de deux nombres a et b plus grands que 1 : $n = a \times b$. On ne connaît pas d'algorithme rapide qui l'inverse, mais on ne sait pas démontrer qu'il n'en existe pas. Le produit est donc seulement présumé à sens unique, et quand on l'utilise en sécurité informatique, on prend un risque.

On ne sait pas même prouver que ces fonctions dont on a besoin existent

D'autres fonctions présumées à sens unique sont décrites dans l'encadré 4.

Il est vraiment gênant de ne pas savoir démontrer que les fonctions utilisées et que l'on espère à sens unique le sont vraiment. Pire, il est très ennuyeux de ne pas savoir s'il existe une seule fonction à sens unique, car on ne sait pas même prouver que ces fonctions dont on a besoin existent. Prouver qu'il en existe est un premier pas incontournable pour concevoir une méthode de chiffrement dont on prouverait qu'elle est «incassable» (*voir plus loin les mondes cryptographiques d'Impagliazzo*).

Notons toutefois qu'un résultat remarquable dû au mathématicien ukrainien, maintenant aux États-Unis, Leonid Levin, a permis de ramener la recherche de fonctions à sens unique à un problème unique. Leonid Levin a identifié une fonction dont il a démontré qu'elle est à sens unique si, et seulement si, il existe des fonctions à sens unique. En clair, tout le problème des fonctions à sens unique se concentre sur elle. Cette fonction qui serait à sens unique est qualifiée d'universelle. Malheureusement, elle est assez compliquée et artificielle et en pratique, il serait difficile de construire à partir d'elle des fonctions cryptographiques utiles. Le progrès apporté récemment sur le sujet par Yanyi Liu et Rafael Pass a consisté à construire une autre fonction à sens unique universelle, plus naturelle. C'est un progrès théorique, dont l'utilisation pratique est envisageable. Elle permet surtout d'y voir plus clair dans les bases de la cryptologie informatique qui étaient bloquées.

Avant d'expliquer l'énoncé nouveau démontré par Yanyi Liu et Rafael Pass voyons l'autre composant qui y intervient : la complexité de Kolmogorov d'un objet numérique A. Il s'agit de la taille du plus court programme qui produit A, par exemple le programme qui l'imprime. On note cette fonction $K(A)$. Elle est parfaitement définie dès que l'on fixe le langage de programmation utilisé pour écrire les programmes. Dans cette définition, on n'impose aucune limite au temps de calcul des programmes recherchés, seule leur taille minimale importe.

2 L'EMBARRAS DU CRYPTOLOGUE

Utiliser le masque jetable ?
Il est bien prouvé robuste à toute attaque,
mais il est trop difficile à mettre en œuvre donc peu utilisable.

Disposer d'un système de chiffrement satisfaisant (utilisable et démontré robuste) ?

S'appuyer sur la fonction à sens unique proposée par Leonid Levin ?
Non, elle est malcommode, et elle n'est pas prouvée à sens unique.

S'appuyer sur la fonction à sens unique liée à la complexité de Kolmogorov ?
Non, elle est plus probablement à sens unique, mais ce n'est pas encore prouvée.

S'appuyer sur les fonctions présumées à sens unique qu'on connaît ?
Ce n'est pas totalement satisfaisant, mais il faut s'en contenter…
… en attendant de nouveaux progrès.

LA COMPLEXITÉ DE KOLMOGOROV EN TEMPS LIMITÉ

Malheureusement, les mathématiciens ont démontré que la fonction $K(A)$ est une fonction non calculable par algorithme, comme l'est la fonction d'arrêt découverte par Alan Turing en 1936 (fonction qui à un programme associe 1 si son exécution s'arrête, et associe 0 si le programme ne s'arrête jamais). Une version plus raisonnable de la complexité de Kolmogorov a donc été introduite qui prend en compte le temps de calcul. On la dénomme «complexité de Kolmogorov en temps limité» et elle est définie dans ce qui suit.

On se donne une fonction qui à tout entier n en associe un autre $t(n)$. Ce nombre $t(n)$ indique le temps maximal accordé aux programmes qu'on veut utiliser pour produire des objets numériques de taille n. La complexité de Kolmogorov en temps limité pour $t(n)$ notée $K^t(A)$ est alors la taille du plus court programme qui produit A en utilisant au plus $t(n)$ pas de calcul.

On pourra, par exemple, considérer qu'il n'est pas raisonnable de consacrer plus de n^5 pas de calcul pour obtenir les objets A dont la taille est n, et rechercher le programme le plus court en nombre de symboles qui fait cela

pour un objet donné. Autrement dit, $K^t(A)$ est la taille de la représentation la plus économique de A quand on accepte de ne mener que des calculs comportant au plus n^5 pas de calcul. Lorsqu'on cherche à compresser des objets numériques (comme des messages numériques) et que l'on souhaite que le temps de décompression ne soit jamais trop long, alors la complexité en temps limité $K^t(A)$ est la notion pertinente. Elle présente un gros avantage sur $K(A)$, elle est calculable : une fois $t(n)$ fixé, il existe des algorithmes qui calculent $K^t(A)$ pour tout objet numérique A.

Il se trouve malheureusement que calculer $K^t(A)$ est difficile en pratique et qu'il faille inévitablement pour ce faire mener de très longs calculs : la fonction $K^t(A)$ est calculable, mais difficile à calculer ! Dire que $K^t(A)$ est difficile à calculer signifie que la proportion des objets A de taille n dont aucun algorithme rapide ne réussit à calculer $K^t(A)$ est non négligeable quand n tend vers l'infini.

Le résultat démontré par Yanyi Liu et Rafael Pass est maintenant simple à formuler. Pour toute fonction $t(n)$ telle que $t(n) \geqslant cn$ (avec $c > 1$), il existe des fonctions à sens unique si, et seulement si, $K^t(A)$ est difficile à calculer. Ce résultat ne permet pas de répondre à la question de l'existence des fonctions à sens unique, mais il indique une question naturelle, simple et équivalente, associée à une théorie mathématique sans lien direct avec la cryptologie et étudiée depuis longtemps.

À vrai dire on pense que $K^t(A)$ est difficile à calculer, et donc l'intuition assez claire qu'on a concernant $K^t(A)$ donne un argument simple et puissant pour penser qu'il existe des fonctions à sens unique.

La fonction à sens unique universelle qui se déduit du travail de Liu et Pass ne peut guère servir pour les applications, mais on espère qu'on en tirera d'autres fonctions qui seront utilisables en pratique pour concevoir des méthodes cryptographiques (fonctions de chiffrement, générateurs pseudoaléatoires, etc.) dont la preuve de robustesse se déduira de la preuve qu'elles sont à sens unique. En s'appuyant sur ces fonctions, on prendrait donc uniquement le risque que la complexité de Kolmogorov en temps limité soit rapide à calculer, ce qui est jugé hautement improbable. Sans y être totalement, on peut dire « on y est presque » et tout semble en place pour qu'un dernier pas en avant donne enfin une théorie mathématique permettant de prouver la robustesse des méthodes utilisées en cryptologie.

En se fondant sur ce qu'on a appris, on prendra alors moins de risques qu'en utilisant les fonctions présumées à sens unique (mais non prouvées à sens unique) qui sont aujourd'hui au cœur de toutes les méthodes utilisées. Le résultat n'indique donc pas comment démontrer que

3

LE MASQUE JETABLE : SÛR MAIS PEU PRATIQUE

Le masque jetable, également dénommé « chiffre de Vernam », est une méthode de chiffrement inventée par l'ingénieur américain Gilbert Vernam (1890-1960) et perfectionné par le général américain Joseph Mauborgne (1881-1971). On démontre que ce système est impossible à casser, mais il a les inconvénients majeurs *(a)* d'exiger que les clés utilisées soient aussi longues que les messages qu'on veut chiffrer, et *(b)* d'exiger que les clés soient aléatoires et ne soient utilisées qu'une seule fois chacune. Ceux qui veulent le pratiquer doivent donc échanger de longues clés par un moyen sûr (par exemple une rencontre), ce qui le rend inadapté à la plupart des situations. Cet article évoque les progrès théoriques faits concernant des méthodes de chiffrement n'ayant pas recours à des clés aussi malcommodes que celles du masque jetable.

Il existe des versions du masque jetable dans toutes les bases de numération, mais voici son principe expliqué en utilisant un message supposé écrit en base 2. Le message est une suite de 0 et de 1, par exemple 011 100 1101, et la clé de chiffrement est aussi une suite de 0 et de 1, par exemple 111 011 0100.

Le message chiffré s'obtient en appliquant le « ou exclusif » (XOR) entre le chiffre en position 1 du message et le chiffre en position 1 de la clé, puis entre les chiffres en position 2, etc.

Nous savons que : 0 xor 0 = 0 ; 0 xor 1 = 1 ; 1 xor 0 = 1 ; 1 xor 1 = 0.

Message clair : 0 1 1 1 0 0 1 1 0 1
Clé : 1 1 1 0 1 1 0 1 0 0
Message chiffré : 1 0 0 1 1 1 1 0 0 1

Le déchiffrement du message s'opère par celui qui reçoit le message en calculant le XOR entre le message chiffré reçu et la clé qu'il connaît.

Message chiffré : 1 0 0 1 1 1 1 0 0 1
Clé : 1 1 1 0 1 1 0 1 0 0
Message déchiffré : 0 1 1 1 0 0 1 1 0 1

La preuve que ce système est impossible à casser provient du fait que lorsqu'on a un message chiffré entre les mains, selon la clé qui a été utilisée tout message initial est possible. Si on ignore la clé, rien ne permet donc de tirer quoi que ce soit du message chiffré qui peut provenir de n'importe quel texte de la même longueur.

Autrefois on se servait de bandes percées de trous aléatoires qu'on n'utilisait qu'une seule fois pour mettre en œuvre le chiffrement du masque jetable. Le téléphone rouge – en réalité un téléscripteur – entre Washington et Moscou pendant la guerre froide a fonctionné un moment avec un système de ce type.

© Fer Gregory/Shutterstock

nos méthodes sont mathématiquement sûres, mais il formule un problème simple qui concentre la difficulté, et permet en quelque sorte de minimiser les risques.

Le résultat nous fait aussi progresser dans l'identification du monde dans lequel nous vivons quand on l'envisage avec un œil de cryptologue. Précisons ce point, à la fois amusant et mathématiquement éclairant.

LES MONDES D'IMPAGLIAZZO

Une façon de mesurer à quel point on attend encore des résultats mathématiques en théorie de la cryptologie et à quel point on est ignorant a été présentée par Russell Impagliazzo il y a bientôt trente ans. Il a défini cinq mondes possibles dans lesquels la cryptologie est plus ou moins facile à développer. On peut alors résumer le problème de la cryptologie mathématique par une simple question : dans quel monde vivons-nous ? Voici ces cinq mondes possibles.

Dans le monde Algorithmica, la classe P des problèmes rapides à résoudre et la classe NP des problèmes dont la solution est rapide à vérifier sont égales : P = NP. Cela signifie qu'une cryptologie sécurisée est impossible. En effet, si on peut chiffrer un message rapidement (en temps polynomial) ce que l'on suppose toujours, alors la recherche du message clair (déchiffré) est un problème NP. Donc, si P = NP, cela signifie que trouver le message clair d'un message chiffré est toujours dans P (facile à retrouver). Pour une méthode de chiffrement précise, l'algorithme de déchiffrement n'est peut-être pas connu aujourd'hui, mais il existe si P = NP, et donc aucune méthode de chiffrement raisonnable (c'est-à-dire dans P) ne sera jamais définitivement à l'abri de l'attaque d'un bon mathématicien capable de trouver l'algorithme rapide de déchiffrement. Dans Algorithmica, aucune cryptologie n'est sûre en dehors du masque jetable.

Le second monde d'Impagliazzo est Heuristica. Dans ce monde P n'est pas égal à NP, mais tous les problèmes dans NP sont faciles à résoudre en moyenne par l'utilisation de méthodes particulières dites heuristiques. Il se peut qu'un problème soit difficile dans les pires cas (donc P ≠ NP), mais qu'en moyenne il soit facile (polynomial). Dans Heuristica c'est toujours le cas. Si Heuristica est notre monde, alors, à nouveau, aucune cryptologie ne peut être assurément robuste en dehors du masque jetable.

Dans le monde Pessiland, la situation pour un cryptologue est toujours très désagréable. On a bien P ≠ NP et contrairement à Heuristica, il existe des problèmes NP qui sont presque toujours impossibles à résoudre rapidement (pour lesquels il n'existe donc pas de bonnes heuristiques), mais il n'existe pas de fonction à sens unique : toutes les fonctions facilement calculables sont facilement inversibles. Les fonctions à sens unique sont indispensables en cryptologie, car, pour créer des méthodes de chiffrement sûres, il ne suffit pas de disposer d'un problème difficile à résoudre en moyenne, il faut en disposer qui proviennent de fonctions à sens unique. Pour le cryptologue, Pessiland n'est guère préférable à Heuristica.

Dans le quatrième monde d'Impagliazzo, Minicrypt, il y a des fonctions à sens unique et donc des problèmes NP sans heuristique efficace. Elles permettent la mise au point d'algorithmes de cryptologie dont on prouvera la résistance aux attaques. On espère au moins être dans ce monde et on fait souvent

4 FONCTIONS PRÉSUMÉES À SENS UNIQUE

Outre la fonction produit qui à deux entiers associe leur produit et qui est présumée à sens unique, il en existe plusieurs autres utilisées en cryptologie.

La fonction du sac à dos
On se donne un ensemble fini de nombres entiers A et un sous-ensemble B de A. Il est très rapide de calculer la somme des éléments de B. En revanche, si l'ensemble A est donné avec un entier m, trouver un sous-ensemble B de A dont la somme des éléments est m est en général difficile.

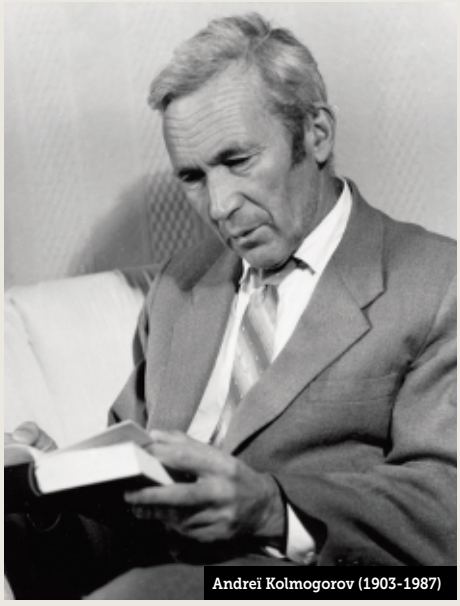
Exemple :
$A = \{3, 8, 11, 35, 175, 222\}$:
$B = \{8, 11\} \rightarrow m = 19$ *facile*
$A = \{3, 8, 11, 35, 175, 222\}$:
$m = 268 \rightarrow$ B ? *difficile*
Le nom du problème provient de l'idée qu'il n'est pas facile de savoir quels éléments choisir parmi tout ce qu'on souhaite mettre dans un sac à dos pour le remplir au mieux. La théorie de la complexité montre que le problème du sac à dos est NP-complet c'est-à-dire que le résoudre en temps polynomial permettrait de résoudre en temps polynomial tout problème NP.

Cela n'est hélas pas suffisant pour établir qu'au sens théorique fort *(voir l'encadré 1)* la fonction qui à B associe m est à sens unique, car être difficile dans le pire cas n'implique pas être difficile en moyenne.
Le système de chiffrement asymétrique de Merkle et Hellman qui était fondé sur le problème du sac à dos fut d'ailleurs révélé faible pour certains jeux des paramètres.

Le logarithme discret
On sait calculer rapidement a^b par exemple pour les entiers modulo n (opération consistant à prendre le reste de la division par n).
Ainsi $2^4 = 16 = 1 \pmod 3$.
En revanche, connaissant n (assez grand), la valeur de a et le nombre résultat $c = a^b \pmod n$, il est difficile en général de trouver b.
C'est le problème du logarithme discret, qui est aussi souvent utilisé en cryptologie.
$2^b = 6 \pmod{13}$
$2^b = 15 \pmod{19}$
$5^b = 20 \pmod{103}$
Quand on calcule modulo n plus n est grand plus la détermination de b est difficile.

5 COMPLEXITÉ EN TEMPS LIMITÉ

La complexité, inventée par le mathématicien soviétique Andreï Kolmogorov, d'un objet numérique *A* (par exemple une image) est la taille du plus petit programme qui permet de produire *A* (par exemple pour afficher *A* à l'écran). On la note K(*A*). Dans sa version de base, on n'impose pas de limite au temps de calcul des programmes courts qu'on recherche et qui seront donc parfois beaucoup trop lents.
La complexité de Kolmogorov en temps limité est encore la taille du plus petit programme qui produit *A*, mais cette fois on ne veut que des programmes qui calculent leur résultat en moins de $t(n)$ pas de calcul pour un objet *A* de taille *n*, où $t(n)$ a été fixé, par exemple $t(n) = n^3$.
On connaît des algorithmes de calcul tirés de séries infinies qui produisent *n* chiffres décimaux du nombre π en utilisant un temps de calcul inférieur à n^3. On en déduit que la complexité de Kolmogorov des *n* premiers chiffres de π en temps limité par n^3 est faible. On peut montrer qu'elle est inférieure à $c + \log(n)$ où *c* est le nombre de caractères nécessaires pour écrire le programme exprimant la série infinie, et $\log(n)$ le nombre de caractères servant pour écrire l'entier *n*.
De façon plus générale, calculer la complexité de Kolmogorov en temps limité est possible par algorithme. Il est cependant intuitivement clair qu'aucun algorithme ne peut y arriver rapidement. Yanyi Liu et Rafael Pass ont démontré qu'il existe des fonctions à sens unique (point central de la cryptologie mathématique) si, et seulement si, la complexité de Kolmogorov en temps limité est difficile à calculer. C'est une avancée importante qui débloque les recherches théoriques en cryptologie et dont on espère des retombées concrètes.


Andreï Kolmogorov (1903-1987)

l'hypothèse implicite que c'est vraiment notre monde. Pour le développement d'une cryptologie sécurisée il faut bien sûr identifier une fonction à sens unique, nous en tenons peut-être avec les fonctions universelles de Levin ou de Liu et Pass, mais pour être vraiment tranquille, il faudrait trouver la démonstration qu'elles sont à sens unique… ce qui n'est pas encore le cas !

Les méthodes de chiffrement que nous avons évoquées jusqu'à maintenant sont les méthodes symétriques : une clé permet le chiffrement d'un message, et la même clé permet le déchiffrement. Il existe cependant depuis les années 1970 une cryptologie à clé publique (dénommée aussi « cryptologie asymétrique ») : le chiffrement se fait par une clé qu'on peut rendre publique, mais il faut pour déchiffrer un message disposer d'une seconde clé, la clé privée qu'on cachera soigneusement. La possibilité de prouver que les méthodes asymétriques sont robustes aux attaques exige un peu plus que l'existence de fonctions à sens unique. Cela rend la robustesse de ces méthodes plus difficile à prouver que celle des méthodes symétriques. C'est le prix à payer pour avoir des approches plus pratiques à utiliser ! C'est cette situation qui justifie l'introduction du cinquième monde : Cryptomania.

LE PARADIS DU CRYPTOLOGUE

Dans Cryptomania, le cryptologue dispose de tout ce dont il rêve, y compris des fonctions à sens unique particulières nécessaires pour la cryptologie asymétrique. On espère que notre monde est Cryptomania, et on fait comme si c'était le cas puisque aujourd'hui on utilise largement des systèmes asymétriques. Soyons lucide et gardons à l'esprit que les utiliser est risqué, et plus risqué que l'utilisation des méthodes symétriques.

Nous ignorons dans quel monde nous sommes et depuis l'article d'Impagliazzo qui a décrit clairement les diverses éventualités, on a peu avancé ! Les progrès apportés par Liu et Pass n'ont pas pour conséquence l'élimination d'une des éventualités envisagées par Impagliazzo, mais reformulent les énigmes de la cryptologie et maintenant Pessiland pourrait être éliminé en montrant seulement que le calcul de $K^t(A)$ est difficile.

Pour terminer, signalons que les méthodes de calcul quantique obligent à reprendre certaines des questions évoquées dans cet article. Cette réflexion est en cours, car même avant que des calculateurs quantiques réellement puissants existent, et on n'est pas certain qu'il en existera un jour, les chercheurs ont déjà conçu des fonctions présumées à sens unique quantiques. Notons que le calcul des facteurs d'un nombre entier est faisable en temps polynomial par un ordinateur quantique et donc que la multiplication d'entiers n'est plus un candidat comme fonction à sens unique quantique.

Il est remarquable que les problèmes mathématiques soulevés par la cryptologie soient à la fois cruciaux pour le fonctionnement de notre société de plus en plus numérique et, en même temps, d'une déconcertante difficulté. Qui a dit que les mathématiques étaient inutiles ? ■

© Photo12/Sovfoto/UIG

BIBLIOGRAPHIE

Zhenjian Lu et I. Oliveira, **Theory and applications of probabilistic Kolmogorov complexity,** prépublication sur arXiv arXiv:2205.14718, 2022.

E. Klarreich, **Which computational universe do we live in ?,** *Quanta Magazine*, 2022.

S. Hirahara, **Meta-computational average-case complexity : A new paradigm toward excluding Heuristica,** *Bulletin of EATCS*, 2022.

P. Guillot et M. J. Durand-Richard, **Informatique et cryptologie : un déplacement des frontières,** *Intellectica*, 2020.

Yanyi Liu et R. Pass, **On one-way functions and Kolmogorov complexity,** *2020 IEEE 61st Annual Symposium on Foundations of Computer Science (FOCS)*, 2020.

R. Impagliazzo, **A personal view of average-case complexity,** *Proceedings of Structure in Complexity Theory. Tenth Annual IEEE Conference*, 1995.