Dans le cas de L'Aquila, par exemple, un aspect est peu souvent rappelé, voire jamais : les experts de la commission des grands risques, tous de grands chercheurs, sont intervenus en partie en réponse à une alerte d'un autre scientifique travaillant à l'observatoire national du Gran Sasso (le plus grand laboratoire souterrain du monde en physique des particules), qui utilisait une technique controversée – la détection de radon, notamment le radon 222. Pour ce scientifique, qui n'est pas un chercheur mais un technicien, l'émission de radon 222 serait un signe précurseur robuste de la survenance d'un séisme.

L'hypothèse du radon est connue. Elle a fait l'objet de publications et de rares revues critiques. Sept jours après le tremblement de terre, l'Institut français de radioprotection et de sûreté nucléaire (IRSN), qui étudie les émissions de radon depuis plus de vingt ans, a publié son point de vue sur cette hypothèse à la lumière des publications scientifiques sur le sujet. Pour l'IRSN, si l'on enregistre bien des variations des teneurs en radon dans les zones sismiques, indiquant que la circulation des fluides souterrains est perturbée par les contraintes et déformations qui préparent ou accompagnent les tremblements de terre, on ne peut passer de ce constat à une prévision de séisme : on est en effet incapable d'associer aux variations observées des informations telles que la profondeur du foyer, l'épicentre et la magnitude du séisme susceptible de survenir.

Il n'est pas de mon ressort de juger de la pertinence de cette technique, de sa pertinence relative par rapport aux autres ou encore du bagage théorique qui la soutient. Certes, le radon ne permet pas de détecter avec certitude un séisme – tout comme les autres techniques mises en œuvre. Mais là n'est pas la question. La question est de savoir si cette hypothèse a droit à la considération scientifique au même titre que les autres hypothèses. Or elle n'a visiblement pas été prise au sérieux par la commission italienne des grands risques.

Ce fait, que l'on peut considérer comme marginal, est pourtant un révélateur de la difficulté majeure à penser la science comme le lieu d'expression d'un pluralisme. Il questionne sur la méthode scientifique elle-même, sur la façon de composer avec une multiplicité de savoirs, sur la capacité d'accueillir la diversité comme une valeur constitutive des sciences. Est-il possible aujourd'hui d'accueillir plusieurs hypothèses explicatives concurrentes qui, entre elles, sont incompatibles ? Dans le cas de L'Aquila, comme dans de nombreux exemples qui font le grain des sciences contemporaines (ainsi, on s'aperçoit aujourd'hui que la maladie d'Alzheimer a d'autres versants que neurologique), la pertinence d'un savoir scientifique ne tient pas à sa capacité à évacuer le « bruit » épistémique qui dérangerait ses certitudes ou qui bousculerait le courant principal du moment, mais plutôt à accueillir en son sein la diversité des perspectives, des disciplines, des points de vue, des styles et des démarches.

Une bonne science n'est ni une science neutre ni une science sans contexte, mais une science consciente de son implication radicale dans le réel. Ainsi, l'enjeu aujourd'hui n'est pas tant de construire des savoirs scientifiques robustes, mais bien des savoirs pertinents. Et le temps des sciences impliquées exige que ce critère de pertinence devienne le nouvel objet de la responsabilité sociale des sciences. ■

© CLAUDIO LATTANZIO /epa/Corbis

SEPT SCIENTIFIQUES ONT ÉTÉ CONDAMNÉS EN 2012 à six ans de prison ferme pour homicide par imprudence après le tremblement de terre en avril 2009 à L'Aquila *(ci-dessus)*, en Italie. Ils étaient accusés d'avoir sous-estimé le risque de séisme. Pourtant, aucune technique ne permet de prévoir un séisme avec certitude. Qui est le vrai responsable ?

L'AUTEUR

Léo COUTELLEC est chercheur en épistémologie et éthique des sciences contemporaines à l'université Paris-Sud et à l'Espace éthique Île-de-France.

BIBLIOGRAPHIE

L. Coutellec, **La Science au pluriel,** Quæ, 2015.

L. Coutellec, **Le temps des sciences impliquées,** *Écologie & Politique*, n° 51, 2015.

L. Coutellec, **De la démocratie dans les sciences,** Matériologiques, 2013.

Réagissez au Point de vue sur www.pourlascience.fr

ENTRETIEN

Apple et le FBI : « Un système de chiffrement muni d'une trappe serait catastrophique »

Les données que contient un téléphone peuvent être cruciales dans une enquête judiciaire, mais prévoir un moyen d'y accéder en contournant le cryptage menace les libertés individuelles. Un compromis est-il possible ?

David POINTCHEVAL, chercheur au CNRS, est directeur adjoint du département d'informatique de l'ENS à Paris.

Dans l'enquête sur le massacre de San Bernardino commis fin 2015, le FBI n'arrivait pas à lire les données chiffrées du téléphone du tueur. Il a donc demandé l'aide du constructeur de l'appareil, Apple, qui a refusé. Les enquêteurs ont finalement réussi à débloquer le téléphone, mais, à terme, une solution envisagée par les autorités est que les logiciels de chiffrement soient dotés d'une trappe donnant accès, en cas d'enquête, aux informations cryptées. Sont ainsi posées de nombreuses questions sur la protection de la vie privée, mais aussi sur les moyens techniques qui offriraient un compromis. L'éclairage de David Pointcheval, directeur de recherche au CNRS, directeur adjoint du département d'informatique de l'ENS et responsable de l'équipe Inria Cascade.

POUR LA SCIENCE

Le chiffrement semble omniprésent sur nos ordinateurs et nos téléphones portables. Quel en est le principe ?

DAVID POINTCHEVAL : Aujourd'hui, quand vous faites un achat en ligne ou que vous envoyez un courriel, les informations sont chiffrées pour des raisons de sécurité. En général, l'objectif est de protéger vos données d'un usage malhonnête. Mais on ne peut éviter que le chiffrement soit parfois un frein à une enquête, en protégeant les données d'une personne ayant des activités criminelles.

Pour comprendre les enjeux du conflit entre Apple et le FBI, il faut présenter les deux types de chiffrement, l'un dit symétrique et l'autre asymétrique. Le premier sert, par exemple, à chiffrer les données sur votre appareil. Il est la version moderne des codes utilisés par le passé : le mécanisme qui transforme vos données en un code illisible utilise une clé que vous êtes le seul à détenir. Et cette même clé sert à retraduire vos données en clair. Si vous voulez communiquer un message chiffré à un interlocuteur, celui-ci doit aussi détenir la clé de déchiffrement. Or, en général, vous ne partagez pas un tel secret avec le destinataire.

En 1976, les Américains Whitfield Diffie et Martin Hellman ont trouvé une solution (pour laquelle ils viennent de recevoir le prix Turing, l'équivalent du prix Nobel en informatique) : le chiffrement asymétrique. La méthode comprend deux clés, l'une privée et l'autre publique. Le destinataire d'un message à chiffrer vous envoie sa clé publique, que vous utilisez pour coder le message. Mais seule la clé privée du destinataire peut déchiffrer ce dernier.

L'algorithme RSA (du nom de ses inventeurs Ronald Rivest, Adi Shamir et Leonard Adleman) met en œuvre ce chiffrement asymétrique. La clé publique y est un nombre très grand, produit de deux nombres premiers. La clé privée est formée justement par ces deux nombres premiers. La sécurité du système est fondée sur le fait que trouver les facteurs premiers à partir de la clé publique prendrait beaucoup trop de temps.

PLS

Quelle est la robustesse de ces méthodes de chiffrement ?

D. P. : L'algorithme symétrique standard AES *(Advanced Encryption System)* impose que les clés du chiffrement soient d'au moins 128 bits, soit environ 30 caractères. L'attaque classique consiste en une énumération exhaustive des combinaisons possibles. Pour donner une idée, une clé de 256 bits représente autant de combinaisons qu'il y a d'atomes dans l'Univers observable. D'autres types d'attaques ont été tentés, mais aucune n'a mis AES en défaut, pour l'instant.

Pour l'algorithme RSA, certaines attaques sont plus performantes que l'énumération exhaustive. Il y a quinze ans, on recommandait d'utiliser une clé de 150 chiffres (décimaux) ; elle est maintenant de 600 chiffres, afin que le temps de calcul requis pour trouver les facteurs premiers reste hors de portée.

Le point faible des systèmes de chiffrement se situe souvent au niveau du logiciel qui réalise le chiffrement. Par exemple, en 2013,

© Pour la Science - n° 463 - Mai 2016

lorsque Edward Snowden a annoncé que la NSA (l'Agence américaine de sécurité) récoltait des données sur les citoyens américains en outrepassant ses prérogatives, un des programmes de la NSA exploitait des failles présentes dans certains logiciels de chiffrement. L'agence est obligée d'utiliser ce genre d'approches car, malgré ses moyens informatiques, elle ne parvient probablement pas à casser le code symétrique ou à factoriser les clés publiques du RSA.

PLS

Avec les révélations d'Edward Snowden, les gens se sont demandé comment mieux protéger leur vie privée. Quelle a été la réponse des grands groupes informatiques tels que Google ou Apple ?

© shutterstock.com/Suwin

DANS LE CONFLIT QUI OPPOSE APPLE AU FBI, le second voudrait que le groupe informatique développe un logiciel pour accéder aux données chiffrées d'un téléphone. Apple refuse, dans la mesure où un tel logiciel affaiblirait la protection de la vie privée des utilisateurs.

D. P. : Une autre technique d'écoute de la NSA était de se brancher directement sur les serveurs des grands opérateurs américains de téléphonie ou d'Internet. Les données y sont chiffrées par l'opérateur (et non par l'utilisateur) au cas où une personne malveillante s'introduirait sur les serveurs. La NSA a eu accès aux clés de déchiffrement des opérateurs – avec ou sans leur aide, difficile de le savoir –, elle avait alors accès aux données de tout le monde.

Les grands groupes ont compris qu'ils devaient s'extraire de la chaîne de chiffrement des données pour éviter une telle situation et ainsi améliorer la sécurité des données des utilisateurs. De fait, les dernières versions des iPhone et des téléphones Android permettent aux utilisateurs de chiffrer leurs données sur le téléphone avec une clé qu'Apple, par exemple, ne connaît pas.

Les autorités ne peuvent plus solliciter l'opérateur pour déchiffrer les données sur le téléphone. C'est une partie du problème qui opposait Apple et le FBI. Par ailleurs, les iPhone sont dotés d'un système qui efface toutes les données si le mot de passe est entré de façon erronée dix fois de suite, une option qui empêche le FBI de s'attaquer au téléphone sans risquer de perdre les données.

Apple, qui a coopéré par le passé avec les autorités dans des situations similaires, refuse aujourd'hui de fournir son aide. Le constructeur explique que le logiciel qui devrait être développé pour accéder aux données menace de façon générale la vie privée des utilisateurs d'appareils iPhone. L'enjeu de ce contentieux est celui des logiciels de chiffrement munis d'une trappe, c'est-à-dire un accès utilisable par les autorités pour contourner le cryptage et accéder aux données.

PLS

La plupart des industriels soutiennent Apple. Une voix qui détonne est celle d'Adi Shamir. Quels sont ses arguments ?

D. P. : Selon Adi Shamir (le S dans RSA), Apple devrait collaborer dans ce cas précis. D'abord, le tueur étant mort et clairement coupable, sa vie privée n'est pas à défendre.

Il y a aussi un argument technique. Depuis la version 8 du système d'exploitation des téléphones Apple, les données sont chiffrées sur le terminal avec une clé inconnue d'Apple. Mais d'après Adi Shamir, Apple aurait les moyens de désactiver l'effacement après dix codes de déverrouillage erronés, rendant possible la recherche exhaustive des codes de déverrouillage sans endommager le contenu du téléphone. C'est cette dernière « trappe » qu'Adi Shamir souhaiterait qu'Apple n'ait plus les moyens d'utiliser. Apple ne pourrait alors plus aider le FBI.

Une trappe est une faille voulue dans le logiciel de chiffrement, une catastrophe en termes de sécurité

Dans le cas du téléphone du tueur de San Bernardino, le FBI a annoncé le 28 mars qu'il aurait débloqué le téléphone sans l'aide d'Apple. Néanmoins, la question fondamentale demeure. Il y aura certainement d'autres affaires avec des téléphones que le FBI ne saura pas décrypter et la question d'une trappe surgira de nouveau.

PLS

Quelles seraient les conséquences d'un système équipé d'une trappe ?

D. P. : Si l'État américain impose aux industriels de prévoir une trappe dans les systèmes de chiffrement, ce sera catastrophique. Tous les spécialistes de la cryptographie s'accordent à dire que c'est une très mauvaise solution. Une trappe est une faille volontairement installée dans le logiciel de chiffrement. Comment garantir qu'elle sera bien protégée de toute intrusion non officielle ? Cette trappe serait évidemment munie d'une clé détenue par le FBI, mais comment cette agence assurera-t-elle que la clé ne tombe pas entre de mauvaises mains ?

Par ailleurs, une fois que les États-Unis auront imposé aux opérateurs la mise en place d'une trappe, tous les autres gouvernements exigeront la même chose. Autant de risques de voir des fuites et de mauvaises utilisations de ces trappes. Cela ne menacera pas seulement les données des criminels, mais aussi la vie privée de tout le monde.

Calculer avec des données chiffrées

Il est théoriquement possible de demander à un tiers de traiter des données même si votre requête et les données sont chiffrées. Le chiffrement complètement homomorphe permet ce tour de force. Les travaux dans ce domaine ont bien progressé.

Le principe est simple. Imaginons que vous chiffriez simplement vos données d_1, d_2, d_3 en les multipliant par une constante C (la clé de chiffrement). Vous envoyez les données chiffrées Cd_1, Cd_2 et Cd_3 sur le serveur tiers. Vous pouvez alors demander à l'opérateur d'effectuer certains calculs simples sur ces données, telle leur moyenne. Il suffit alors de diviser par C le résultat que l'opérateur vous renvoie pour obtenir la moyenne de vos données. Ce faisant, l'opérateur n'a pris connaissance ni des vraies données ni de leur moyenne.

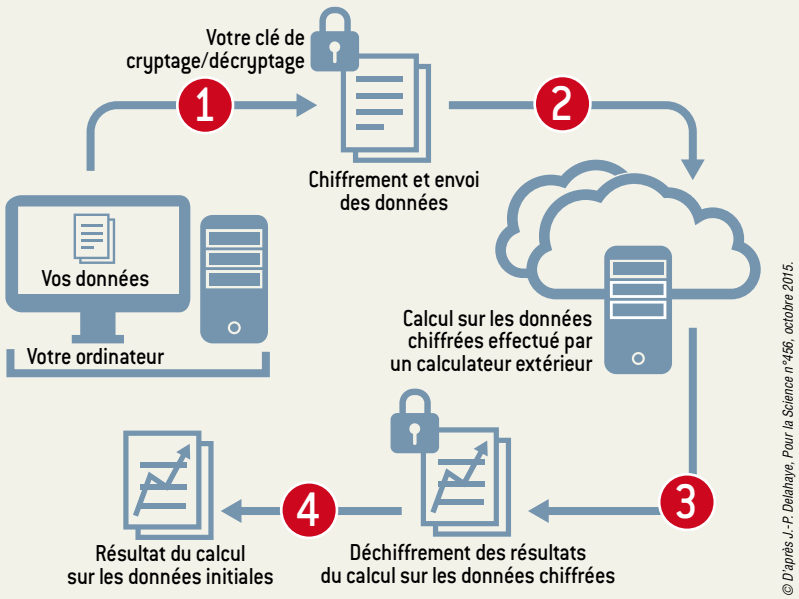
Certaines demandes peuvent être effectuées dans ces conditions, mais d'autres ne sont pas possibles sans révéler la clé de chiffrement.

Pour exécuter toutes sortes de calculs, le système de chiffrement doit être complètement homomorphe, c'est-à-dire qu'il doit présenter deux propriétés : $\mathscr{C}(d_1+d_2)=\mathscr{C}(d_1)\oplus\mathscr{C}(d_2)$ et $\mathscr{C}(d_1\times d_2)=\mathscr{C}(d_1)\otimes\mathscr{C}(d_2)$, où $\mathscr{C}$ est l'opération de chiffrement, d_1 et d_2 deux données, $\oplus$ et $\otimes$ deux opérations propres au chiffrement. L'opérateur tiers exécute les opérations $\oplus$ et $\otimes$ sur les données chiffrées, ce qui revient à additionner ou multiplier les données initiales.

Avec ces deux propriétés, toutes les opérations logiques booléennes (ET, OU, etc.) sont définissables et il est possible d'effectuer toutes les manipulations désirées sur les données.

Le système RSA est homomorphe pour la multiplication, mais pas pour l'addition. En 2009, Craig Gentry a proposé le premier système complètement homomorphe. Celui-ci était impossible à mettre en pratique : les calculs à effectuer au moment du chiffrement et du déchiffrement étaient trop volumineux. Et la taille des données à manipuler par l'opérateur tiers était des millions de fois plus importante que celle des données avant chiffrement.

Les travaux récents ont permis de réduire le surcoût en taille des données et en lourdeur de calcul. Le système est déjà utilisable dans certains cas simples.



© D'après J.-P. Delahaye, Pour la Science n°456, octobre 2015.

PLS

La recherche en cryptographie propose-t-elle des solutions alternatives ?

D. P. : Les systèmes tendent aujourd'hui vers un chiffrement de bout en bout par l'utilisateur. Ses données, sur le serveur d'un opérateur tel Google, seront alors chiffrées. L'utilisateur ne pourra plus utiliser les outils de l'opérateur pour effectuer des opérations sur ses données, telle une recherche par mots-clés. En effet, comment soumettre une requête à Google si celui-ci ne peut pas lire les données ? C'est théoriquement possible avec le « chiffrement complètement homomorphe », proposé en 2009 par Craig Gentry, un chercheur d'IBM. Et mieux, il est possible d'obtenir une réponse pertinente, que l'opérateur ne voit pas, à une question qu'il ne connaît pas ! Ainsi, avec une requête sur des données cryptées, Google pourra effectuer les opérations que vous lui demandez.

Cette méthode de chiffrement est un grand axe de recherche actuel *(voir l'encadré ci-contre)*. Des progrès ont été réalisés pour réduire les temps de calcul. Par exemple, un calcul test par un système complètement homomorphe qui prenait plusieurs heures se fait maintenant en quelques secondes. On reste loin d'une mise en place à grande échelle, mais ce système sera la prochaine étape dans la sécurisation des données.

PLS

L'ordinateur quantique, s'il devient réalité, menacera-t-il les systèmes de cryptage ?

D. P. : Cette menace reste théorique, mais nous y réfléchissons déjà. L'ordinateur quantique exploite des propriétés de la physique quantique pour accroître les capacités de calcul. Ainsi, un algorithme adapté pourrait effectuer certaines opérations plus vite qu'avec un ordinateur classique. En particulier, nous avons déjà un algorithme quantique de factorisation. Le jour où un ordinateur quantique pourra l'utiliser, le système RSA sera obsolète. Nous étudions donc des systèmes de chiffrement classiques, dits postquantiques, dont le principe repose sur des problèmes difficiles que même les algorithmes quantiques ne peuvent résoudre efficacement – pour l'instant... ■

Propos recueillis par Sean BAILLY

© Pour la Science - n° 463 - Mai 2016

La Biostatistique a son instrument

Stata fournit les outils statistiques, graphiques et de traitement de données nécessaires à toute recherche impliquant de la biostatistique.

- Analyse de survie multi-niveaux
- Estimateurs pour les données de panel
- Calcul de puissance pour les tables de contingence
- Méthodes de rééchantillonnage et de simulation
- Imputation Multiple
- Convient aux mesures longitudinales ou transversales

Programmable

Précis

Exhaustif

ritme.com/stata

+33 (0) 1 42 46 00 42

Distributeur officiel en France, Suisse, Belgique et Luxembourg

RITME - 34 Bd Haussmann, 75009 Paris, France

RITME SCIENTIFIC SOLUTIONS

STATA® 14 release

© 2015 RITME. Stata est une marque déposée de StataCorp. Toutes les marques déposées sont la propriété de leurs sociétés respectives.