

## Archéologie

### Une rare panoplie romaine

**D**ans la seconde moitié du III<sup>e</sup> siècle, un incendie ravage la réserve d'une villa rurale située à Saint-Clément, près de Sens. Dans la masse compacte qui a rempli sa cave et protégé son contenu de l'air, l'Inrap vient de retrouver près de 200 outils agricoles. Ce matériel correspond bien à ce que préconisaient les auteurs antiques de traités d'agronomie.

Par exemple, dans le chapitre X de *De re rustica*, Caton l'Ancien (234-149 avant notre ère) dresse la liste suivante des « instruments en fer » à fournir à son intendant : huit fourches, huit sarcloirs, quatre pelles, cinq houes, deux râtaux à quatre dents, trois faux à foin, six faux à chaume, cinq croissants, trois haches, trois coins, un pilon à blé, deux pelles à feu... Cette liste est très similaire à celle de la panoplie d'outils agricoles romains de Saint-Clément qui, à ce stade, est sans équivalent.

F. S.

## Mathématiques

### Andrew Wiles reçoit le prix Abel

**L'**Académie norvégienne des sciences et des lettres a décerné le prix Abel 2016 à Andrew Wiles, de l'université d'Oxford, pour « son éblouissante démonstration du dernier théorème de Fermat en utilisant la conjecture de modularité sur les courbes elliptiques semistables, et ouvrant une nouvelle ère en théorie des nombres ».

L'histoire commence en 1637, lorsque Pierre de Fermat énonça une conjecture : « Il n'existe pas de solution entière pour l'équation  $x^n + y^n = z^n$  quand  $n$  est strictement plus grand que 2. » Près de 350 ans plus tard, en 1993, Andrew Wiles en donna la preuve. Elle consistait à démontrer d'abord une autre conjecture, dite de Taniyama-Shimura, dont le lien avec la conjecture de Fermat avait été établi en 1984. La conjecture de Taniyama-Shimura stipule que « pour chaque courbe elliptique, il existe une forme modulaire correspondante ». Andrew Wiles, spécialiste des courbes elliptiques (objets définis par des équations cubiques à deux variables) et des formes modulaires (objets abstraits avec un haut degré de symétrie), a prouvé le lien d'équivalence entre ces objets et, du même coup, le grand théorème de Fermat.

S. B.

## Géophysique

### Comment l'olivine se déforme

**U**ne équipe animée par Patrick Cordier, de l'université de Lille, vient d'observer directement la propagation d'une dislocation dans un cristal d'olivine, l'un des principaux silicates dont est constitué le manteau terrestre. Or une meilleure connaissance de ce phénomène dans les roches mantelliques est nécessaire pour améliorer notre description des mécanismes de la dérive des continents.

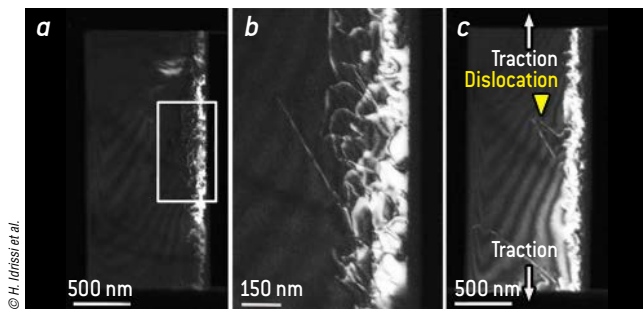
Les dislocations sont des fronts internes au cristal, où les liaisons interatomiques sont brisées. Elles naissent lorsque – par choc, compression ou étirement – on déforme un matériau cristallin afin d'y créer des contraintes, c'est-à-dire la mise sous pression de certains plans internes. Pour en créer, l'équipe de Patrick Cordier a mis au point un appareil capable de tirer aux deux extrémités d'un nanocristal d'olivine sans le briser, de sorte que des dislocations peuvent s'y

propager à température ambiante, au sein d'un microscope électronique par transmission. Cette nouvelle méthode rend les observations plus fiables que celles des expériences précédentes à température élevée.

Les chercheurs sont parvenus à mesurer les modalités de la propagation des dislocations dans l'olivine. Présentes en grand nombre dans le minéral, elles interagissent, s'enchevêtrent et tendent à s'accumuler aux interfaces entre grains cristallins, ce qui explique que la roche se déforme sans rompre, bref, sa ductilité. Désormais appréciée sur des bases expérimentales plus solides, la ductilité de l'olivine est l'un des paramètres des modèles numériques décrivant la façon dont les roches mantelliques se déforment pour rendre possible le glissement des plaques tectoniques.

F. S.

H. Idrissi et al., *Science Advances*, vol. 2(3), e1501671, 2016



En (a), l'échantillon d'olivine avant déformation. En (b), l'intérieur du rectangle montrant une couche endommagée. En (c), la naissance d'une dislocation (triangle) sur le point de se propager dans l'olivine.

#### Coup de vieux pour *Homo floresiensis*

En 2003, on annonçait la découverte, sur l'île indonésienne de Florès, d'*Homo floresiensis*. Haute de un mètre, cette espèce humaine était dotée d'un cerveau de 400 centimètres cubes et aurait été encore présente il y a 18 000 ans. Une époque aussi récente semblait peu plausible. Ses découvreurs viennent de réétudier de fond en comble la grotte où *H. floresiensis* a été mis au jour. Ils concluent que son fossile date d'il y a entre 100 000 et 60 000 ans, une fourchette temporelle beaucoup moins problématique.

#### L'Antarctique contribue à la montée des eaux

Au Pliocène, il y a près de 3 millions d'années, le niveau moyen des océans était plus haut qu'il ne l'est aujourd'hui. Or les modèles d'évolution de la calotte polaire antarctique, en particulier sa fonte, ne restituaient pas la bonne élévation du niveau des mers. Deux climatologues américains,

Robert DeConto et David Pollard, ont amélioré les modèles en incluant certains phénomènes de fragilisation de la calotte. Ils reproduisent correctement les événements du passé. Utilisé avec des scénarios climatiques, leur modèle prévoit que l'Antarctique pourrait contribuer jusqu'à un mètre à la montée des eaux d'ici 2100.

Suivez les dernières actualités de Pour la Science sur les réseaux sociaux



Retrouvez plus d'actualités sur [www.pourlascience.fr](http://www.pourlascience.fr)

## POINT DE VUE

### Science et responsabilité : une réflexion collective s'impose

*La controverse autour du tremblement de terre de L'Aquila en 2009, qui a conduit à la condamnation de scientifiques, nous oblige à repenser ensemble la représentation que nous nous faisons des sciences et donc, a fortiori, de leur responsabilité sociale.*

Léo COUTELLE

**L**e 22 octobre 2012, un verdict très attendu a soulevé une indignation assez unanime dans la communauté scientifique. Sept scientifiques de l'Institut italien de géophysique et vulcanologie, membres de la commission italienne des grands risques, ont été condamnés à six années de prison et 9 millions d'euros d'amende pour homicide par imprudence. Les scientifiques étaient accusés d'avoir sous-estimé le risque sismique à L'Aquila. Dans cette petite ville italienne, trois ans plus tôt, le 6 avril 2009, un tremblement de terre avait causé la mort de plus de 300 personnes, saccageant le centre historique et faisant des dizaines de milliers de sans-abri.

Or six jours avant le séisme, le 31 mars 2009, les membres de la commission, jugée compétente pour l'évaluation des risques sismiques, s'étaient réunis à L'Aquila pour donner un avis sur la probabilité qu'un tremblement de terre majeur y survienne. S'appuyant sur l'analyse d'une série de secousses ayant frappé L'Aquila pendant les mois précédents, la commission avait conclu, en substance, qu'il n'y avait pas lieu de s'affoler, qu'il n'y aurait pas de secousses plus importantes que celles des mois précédents. Six jours plus tard, l'Italie connaissait l'une de ses plus grandes catastrophes sismiques.

La réaction fut très vive dans la communauté scientifique, notamment par l'intermédiaire d'une pétition qui soulignait qu'une

telle condamnation était inacceptable parce qu'il était impossible de prédire un séisme avec précision, et donc que cette décision de justice ne prenait pas en compte la nature même de la connaissance scientifique.

On a aussi reproché au juge un verdict disproportionné et inapproprié : l'argument principal du réquisitoire contre les membres de la commission concernait le manquement aux vertus attendues de la communauté scientifique. Les scientifiques auraient mal

**Être éthiquement responsable,  
c'est être en capacité de  
« répondre de »  
et de « répondre à »**

communiqué, avec peu de prudence et de nuances. Pour nombre de scientifiques, en convoquant ainsi l'éthique des vertus du scientifique, en se faisant police des vertus, la justice dépassait ses attributions.

Le 10 novembre 2014, les sept scientifiques ont été acquittés en appel et, en novembre dernier, la Cour de cassation a appuyé cette décision. Cependant, quelle que soit l'issue du procès, la responsabilité des scientifiques est à repenser. En effet, étant donné la portée de la science sur nos existences, cette dernière ne peut plus être vue comme une entreprise désintéressée et unifiée dont le seul objectif est l'avancement des connaissances.

La responsabilité des scientifiques est engagée. Mais de quoi s'agit-il ? Au-delà de sa dimension juridique ou morale, la responsabilité comporte aussi une part éthique. Et être éthiquement responsable, c'est être en capacité d'une part de « répondre de », c'est-à-dire de rendre des comptes en raison d'une mission qui nous a été confiée, et, d'autre part, de « répondre à », c'est-à-dire de prendre en considération les attentes et les interrogations des individus ou collectifs avec qui nous sommes en relation.

Il ne s'agit donc pas seulement de savoir si l'on peut prédire un séisme avec certitude (responsabilité juridique) ou d'exiger certaines vertus dans la communication à son égard (responsabilité morale). La responsabilité éthique, notamment dans sa dimension sociale, exige un travail beaucoup plus profond qui consiste à réinterroger les valeurs et les finalités de la démarche scientifique. La science repose sur diverses valeurs ayant un rapport direct avec la façon de produire les connaissances, telles que la rationalité, la cohérence ou l'adéquation avec l'expérience. Mais d'autres, plus contextuelles, entrent aussi en jeu, telles que le bien-être, la justice ou l'intérêt économique. Comment prendre en compte leur influence dans le processus scientifique ? Autrement dit, parler de responsabilité sociale des sciences, c'est avant tout consentir à un effort conceptuel qui vise à renouveler la représentation que l'on peut en avoir. Il ne peut donc s'agir que d'une réflexion et d'une responsabilité collectives.

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



© 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*, *Matérialogiques*, 2013.

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. ■



Réagissez au  
Point de vue sur  
[www.pourlascience.fr](http://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.

**D**ans 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 débloquent 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,