En effet, si le bruit devient supérieur à p, le reste n'est plus comme il faut (car le quotient augmente de 1 ou plus) pour connaître la somme et le produit des deux bits codés. La méthode n'est bonne qu'à la condition d'opérer un nombre limité d'opérations successives. Pour un calcul dépendant de plusieurs dizaines de bits $b_1, b_2, ..., b_k$ présents dans une expression complexe utilisant beaucoup de XOR et de ET, le résultat obtenu par l'opérateur extérieur risque d'être devenu illisible à celui qui lui a confié le calcul. La méthode sans le perfectionnement qui va venir ne fonctionne qu'avec des calculs assez limités. C'est là qu'intervient la deuxième idée majeure de Craig Gentry. Elle consiste à nettoyer périodiquement le bruit pour éviter qu'il ne devienne trop important.

Pour cela, on fait déchiffrer le résultat du calcul partiel avant qu'il ne soit trop brouillé. Ce nettoyage enlève tout le bruit. On l'effectue en demandant à l'opérateur extérieur d'appliquer la fonction de déchiffrement sur le résultat partiel, c'est-à-dire de diviser par p et examiner la parité du reste obtenu. Suprême astuce : puisqu'on ne fait pas confiance à l'opérateur extérieur, on ne lui communique pas la clef de déchiffrement (le nombre p), mais on lui demande de faire ce déchiffrement par un calcul homomorphe utilisant la méthode qu'on vient de décrire ! Ce n'est possible bien sûr que si ce calcul homomorphe du déchiffrement n'est pas trop complexe, c'est-à-dire n'exige pas, une fois traduit en XOR et en ET, une succession trop longue de calculs ; on s'en assurera.

Cela semble assez fou et cela ressemble à l'opération consistant à s'élever dans les airs en tirant sur ses bottes… c'est d'ailleurs pourquoi le nom donné à cette phase du calcul est *bootstrapping*. Pour que la phase de *bootstrapping* soit possible, il faut qu'un minimum d'opérations soient faisables sans que le bruit qui s'introduit soit devenu trop grand, et cela oblige à prendre des nombres entiers très longs pour p et les q_i, mais cela marche, et on dispose donc d'une méthode de calcul pleinement homomorphe comme on en rêvait. L'opération de *bootstrapping*, en nettoyant autant de fois que nécessaire les calculs partiels, rend possible des séries d'opérations aussi longues qu'on le souhaite de XOR et de ET ; et on peut donc faire exécuter tout calcul par un opérateur extérieur qui ignorera ce qu'il calcule.

Puisque la taille des bits chiffrés $\mathscr{C}(b)$ est nécessairement grande, les calculs effectués par l'opérateur extérieur sont très lourds, énormes comparés à ce qu'il faudrait faire si on ne souhaitait rien cacher, mais le but est atteint : on sait déléguer des calculs sans dévoiler ni les données ni le résultat.

Encore quelques ordres de grandeur à gagner

Les travaux très nombreux sur ce sujet menés depuis 2009 ont visé à réduire les surcoûts en taille et en lourdeur de calcul des systèmes homomorphes. On progresse et des réalisations logicielles utilisant les idées mathématiques de ces travaux tentent de rendre les systèmes utilisables en pratique. La série d'opérations nécessaires au chiffrement de données par l'algorithme AES (*Advanced Encryption Standard*), très largement utilisé dans le monde entier, sert de repère pour mesurer les progrès des différents programmes de chiffrement homomorphe. On est ainsi passé, pour l'exécution de ce calcul test par un système homomorphe, de plusieurs heures (sur une machine courante) à quelques secondes.

C'est remarquable, mais pour que réellement on puisse envisager de confier massivement les calculs qu'on veut faire sur des données confidentielles à des opérateurs extérieurs qui les exécuteraient sans rien y voir, il faudra encore attendre un long moment, que le surcoût ait diminué de plusieurs ordres de grandeur.

Certains experts tels que l'Américain Bruce Schneier restent réservés tant les surcoûts sont encore élevés. Aujourd'hui, la formidable idée de la cryptographie homomorphe est utile, par exemple pour la conception de systèmes de vote. Cependant, malgré une série d'idées intéressantes qui ont prouvé qu'elle était possible dans sa forme la plus générale, sa mise en œuvre pour tous, permettant plus de sécurité et une meilleure confidentialité sur les réseaux, devra encore attendre un peu. ■

L'AUTEUR

J.-P. DELAHAYE est professeur émérite à l'Université de Lille et chercheur au Centre de recherche en informatique, signal et automatique de Lille (CRISTAL).

BIBLIOGRAPHIE

X. Yi *et al.*, **Homomorphic Encryption and Applications**, Springer, 2014.

V. Cortier et S. Kremer, **Vote par Internet,** *Interstices*, 2013 (https://interstices.info/jcms/int_68258/vote-par-internet).

M. Van Dijk *et al.*, **Fully homomorphic encryption over the integers,** *Advances in cryptology - EUROCRYPT 2010*, Springer, pp. 24-43, 2010.

C. Gentry, **Fully homomorphic encryption using ideal lattices,** *Proceedings of the 41st ACM Symposium on Theory of Computing*, pp. 169-178, 2009.

R. Rivest *et al.*, **On data banks and privacy homomorphisms,** *Foundations of Secure Computation*, Academic Press, pp. 169-180, 1978.

Retrouvez la rubrique Logique & calcul sur www.pourlascience.fr

SCIENCE & FICTION

La Force des Jedi, une question de puissance

Quand on s'interroge sur la puissance que doivent maîtriser les chevaliers Jedi pour utiliser la Force, on comprend que les élus soient peu nombreux.

Roland LEHOUCQ et Jean-Sébastien STEYER

Dans la saga *Star Wars*, la Force est la mystérieuse source du pouvoir des chevaliers Jedi. Dans l'épisode IV, *Un nouvel espoir*, Obi-Wan Kenobi explique que la Force est « un champ d'énergie créé par tous les êtres vivants. Il nous entoure et nous pénètre. Il lie la galaxie tout entière ». Bien que force et énergie soient des notions différentes en physique, cette définition implique que la Force est un réservoir d'énergie dans lequel les Jedi peuvent puiser à volonté. Comme l'énergie mesure la capacité d'un système à effectuer des transformations, on comprend que, pour réaliser leurs exploits, les Jedi en utilisent beaucoup.

La Force doit donc être un grand réservoir d'énergie, mais il n'est pas suffisant d'avoir accès à celle-ci, il faut aussi pouvoir l'extraire à un rythme suffisant. Autrement dit, c'est une question de puissance. Les Jedi en produisent-ils assez ? On peut quantifier cette puissance grâce aux films de la saga.

Commençons par examiner le cas de maître Yoda. Il apparaît pour la première fois à l'écran en 1980 dans l'épisode V, *L'Empire contre-attaque*. Il vit alors reclus sur la planète Dagobah et fait une démonstration de la Force en sortant le vaisseau *X-Wing* de Luke Skywalker du marais dans lequel il vient de sombrer. Quelle puissance le maître Jedi doit-il produire pour réaliser cet exploit ? Si l'on suppose qu'un *X-Wing* a les dimensions d'un avion de combat tel que le *Rafale*, il doit faire une quinzaine de mètres de long pour une masse d'au moins 25 tonnes à pleine charge. Yoda extrait le vaisseau du marais assez lentement, à une vitesse que l'on peut estimer à une cinquantaine de centimètres par seconde. Si la gravité de Dagobah est voisine de celle de la Terre, la puissance nécessaire pour réaliser cet exploit est d'au moins 100 kilowatts, soit la puissance d'une voiture ordinaire ! Par comparaison, quand Luke Skywalker s'entraîne en soulevant le droïde R2D2, qui doit peser une centaine de kilogrammes, de un mètre en environ une seconde, il fournit une puissance de seulement 1 kilowatt.

La Force est un réservoir d'énergie dans lequel les Jedi peuvent puiser à volonté.

Si Yoda est capable de bien d'autres exploits, c'est l'empereur Palpatine qui impressionne par son utilisation de la Force. Une scène de l'épisode VI, *Le Retour du Jedi*, nous permet de quantifier la puissance qu'il est capable de produire. Palpatine tente de convaincre Luke Skywalker de le rejoindre du côté obscur de la Force. Devant la résistance de ce dernier, il le torture, puis tente de le tuer en le frappant avec des éclairs émis par les extrémités de ses doigts. Alors que Yoda utilisait la Force de façon « antigravitationnelle », l'empereur fait appel à celle-ci pour se transformer en un puissant générateur de tension.

Les éclairs qui illuminent le ciel durant un orage résultent aussi de la grande différence de potentiel électrique entre le nuage

© 2015 Marc Boulay, marcboulay.fr, cassima-productions.com

LES SITH SONT LES PUISSANTS adversaires des Jedi. Comme eux, ils utilisent la Force pour alimenter leur sabre-laser ou pratiquer la télékinésie.

et le sol. Sous l'action du champ électrique qui en résulte, les molécules de l'air sont brisées, libérant ainsi des atomes d'oxygène et d'azote, principaux constituants de notre atmosphère. Si le champ électrique est assez intense, certains des électrons de ces atomes sont arrachés. L'air, un isolant électrique dans des conditions normales, devient alors conducteur et un éclair frappe le sol. Le champ électrique nécessaire pour produire ce phénomène d'ionisation de l'air est de l'ordre de 3,6 millions de volts par mètre pour de l'air sec à la pression atmosphérique.

L'empereur, une vraie locomotive !

Si l'on estime que les éclairs produits par l'empereur ont une longueur de 3 à 4 mètres, tout se passe comme s'il était branché à un générateur d'une dizaine de millions de volts, à comparer aux 100 millions de volts mis en jeu dans la foudre. Pour évaluer la puissance produite par Palpatine, il faut aussi estimer l'intensité du courant qui circule dans l'éclair. Le seuil de perception d'un courant électrique par le corps humain est d'environ 2 milliampères. Des courants jusqu'à 300 milliampères passant à travers le corps durant plusieurs minutes peuvent provoquer des arythmies cardiaques réversibles, des marques visibles, des brûlures, des vertiges, voire une perte de connaissance. Au-dessus de 300 milliampères, le sujet perd connaissance. Si l'on suppose que l'empereur commence par une valeur « raisonnable » mais déjà très désagréable de l'ordre de 200 milliampères pour faire souffrir Luke, il produit une puissance de 2 mégawatts ! Et s'il s'énerve un peu pour atteindre une intensité de l'ordre de l'ampère, c'est plutôt 10 mégawatts que Palpatine est capable de produire, soit la puissance consommée par la locomotive d'un TGV Duplex !

Le sabre-laser est aussi un objet emblématique de la saga *Star Wars*. Au vu des dégâts que ces sabres peuvent causer, la question de la puissance qu'ils dégagent se pose aussi. Déterminons la puissance d'un sabre-laser en analysant la scène d'introduction de l'épisode I, *La Menace fantôme* (1999). On y voit Qui-Gon Jinn tenter de franchir une épaisse porte blindée. Pour cela, Qui-Gon plonge son sabre-laser dans la porte métallique, ce qui la chauffe intensément et finit par en fondre une partie.

Pour déterminer la puissance dégagée par le sabre-laser de Qui-Gon, il suffit d'estimer l'énergie nécessaire pour faire fondre la porte et de la diviser par la durée – de l'ordre de quelques secondes – mise pour y parvenir. L'énergie nécessaire dépend de la masse de métal à faire fondre et de ses propriétés thermodynamiques.

Faute d'information sur la nature du métal, supposons qu'il s'agisse d'acier. Tout autre métal ferait l'affaire, même si ses propriétés différentes modifient un peu la valeur numérique de notre réponse. Si la porte est en acier, sa masse volumique avoisine les 8 tonnes par mètre cube. Supposons que le volume fondu soit un cylindre d'environ 1 mètre de diamètre et d'une épaisseur de près de 60 centimètres, à l'image des portes des coffres du dépôt d'or de Fort Knox. Cela correspond alors à environ 4 tonnes d'acier. Pour faire fondre cette masse, il faut porter le métal de la température ambiante à sa température de fusion, puis payer le coût énergétique de la fusion elle-même. Le résultat du calcul est sans appel : il faut que le sabre-laser dégage au bas mot 1 gigawatt, soit la puissance d'un réacteur nucléaire !

Si le sabre-laser fonctionne avec une batterie, il faut que celle-ci soit capable de stocker une quantité considérable d'énergie. Et quand on voit l'autonomie des téléphones portables, qui font hélas des choses nettement moins ambitieuses qu'un sabre-laser, on se demande s'il existe vraiment une batterie suffisamment compacte capable d'en alimenter un digne de ce nom. En fait, la densité d'énergie d'un sabre-laser (le rapport entre l'énergie qu'il contient et la masse de sa batterie) est si élevée que la batterie serait réduite à ses constituants atomiques simplement en la chargeant ! Cela confirme que c'est bien en puisant dans l'énergie de la Force que les Jedi parviennent à utiliser leur sabre-laser et que seuls eux peuvent le faire efficacement. La maîtrise de la Force n'est pas à la portée de tout le monde. ■

R. LEHOUCQ est astrophysicien au CEA, à Saclay. J.-S. STEYER est paléontologue au CNRS-MNHN, à Paris.

ART & SCIENCE

Le mystère de la pastèque blanche

Dans une nature morte italienne du XVII^e siècle, une pastèque coupée montre une chair essentiellement blanche. Pourquoi ? Pour le savoir, retraçons l'épopée de ce fruit, régal des anges, de la tombe de Toutânkhamon jusqu'au Japon actuel.

Loïc MANGIN

L'été est déjà loin, mais vous vous souvenez encore de Céline, de Catherine, d'Alana et de celle qu'on appelle Sugar Baby… Ne vous méprenez pas, il ne s'agit pas de vos conquêtes estivales, mais de variétés de… pastèques *(Citrullus lanatus)*. Cette cucurbitacée est l'un des fruits les plus rafraîchissants qui soient et Mark Twain fait dire à son héros de *La Tragédie de Pudd'nhead Wilson* que la pastèque est « le roi, par la grâce de Dieu, de tous les fruits de la création. En avoir goûté, c'est savoir ce que mangent les anges ».

Un tel luxe ne pouvait mériter que les honneurs des peintres et, de fait, on trouve plusieurs représentations de la pastèque, par exemple dans une nature morte du Flamand Abraham Brueghel (1631-1690), ou bien dans une œuvre de l'Italien Giovanni Stanchi (1608-1675). Dans cette dernière *(voir page ci-contre)*, on distingue bien au moins deux pastèques, mais elles ne ressemblent guère à celles de votre été. Certes, parmi les variétés actuelles, on en trouve à chair rouge bien sûr, jaune, verte ou couleur crème, mais là, le cœur du fruit est surtout blanc et un peu rouge. Comment l'expliquer ?

Les anges peuvent se délecter de la pastèque – le roi de tous les fruits – depuis au moins 5 000 ans.

James Nienhuis, agronome à l'Université du Wisconsin, s'est intéressé au problème. D'abord, rappelons que l'essentiel de la chair d'une pastèque est le placenta hypertrophié où sont nichées les graines, le placenta reliant les ovules (avant fécondation) dans l'ovaire de la plante. Selon James Nienhuis, les pastèques actuelles résultent de sélections opérées par les cultivateurs de façon à obtenir un enrichissement en lycopène (un pigment rouge que l'on trouve aussi dans les tomates), et donc une chair bien rouge.

Pourtant, la pastèque qui apparaît dans la nature morte de Brueghel, peinte à la même époque que celle de Stanchi, est bel et bien rouge. La pastèque de l'Italien ne serait-elle pas mûre ? Si, la présence de graines noires est sans équivoque : le fruit a bien été cueilli à maturité.

Cette diversité illustrerait le processus de sélection en cours à cette époque pour l'obtention de la pastèque idéale. Il se poursuit aujourd'hui ; en témoignent les nouvelles variétés « sans pépins » (ou plutôt à pépins atrophiés) que l'on trouve dans nos commerces. Cette caractéristique résulte d'une triploïdie (les plants ont trois jeux de chromosomes au lieu de deux). La pastèque noire Densuke, qui ne pousse que dans le nord de l'île d'Hokkaido, au Japon, est aussi une variété récente. Sa rareté et son goût font qu'elle s'arrache à prix d'or : plusieurs milliers d'euros par spécimen !

Si la pastèque a conquis le monde (on en produit quelque 100 millions de tonnes

© Courtoisie de Christie's

LA PASTÈQUE de Giovanni Stanchi, peintre italien du XVII^e siècle, est intriguante : pourquoi ne ressemble-t-elle pas à celle que nous dégustons l'été ?

par an), on sait peu de choses sur son origine. En d'autres termes, la question est de savoir depuis combien de temps les anges mangent de la pastèque. À en croire les travaux de Harry Paris, du centre de recherches Newe Ya'ar, en Israël, ils peuvent s'en délecter depuis au moins 5 000 ans. En réunissant tous les traces historiques, il est parvenu à reconstituer l'épopée de la pastèque.

Les plus anciens vestiges archéologiques, des graines, ont été découverts en Libye. On a aussi trouvé des graines, ainsi que des représentations picturales, dans des tombes égyptiennes (dont celle de Toutânkhamon) datant pour certaines de 4 000 ans. Étonnamment, l'une des images montre un fruit oblong, semblable à ceux d'aujourd'hui, et distinct des variétés sauvages, plutôt sphériques et par ailleurs au goût amer. Les Égyptiens cultivaient donc des pastèques.

La capacité de stockage de l'eau était un atout dans ces régions sèches. Sans doute est-ce cela qui explique leur présence dans les tombes, les morts ayant besoin de se désaltérer durant leur long voyage. De tous ces témoignages, Harry Paris déduit que la pastèque est apparue dans le nord-est de l'Afrique, où elle a été domestiquée.

Des écrits révèlent que la pastèque a ensuite quitté sa région d'origine pour s'étendre autour de la Méditerranée. Dans son *Histoire naturelle*, au I^er^ siècle, Pline l'Ancien en vante les qualités réfrigérantes. Les médecins Dioscoride et Hippocrate ont également loué ses vertus curatives.

Prudence tout de même : on se souvient qu'en 2011, en Chine, trop dopées au forchlorfenuron, un engrais, des centaines de pastèques ont... explosé ! ■

H. Paris, **Origin and emergence of the sweet dessert watermelon, *Citrullus lanatus***, *Annals of Botany*, vol. 116(2), pp. 133-148, août 2015.