DES BALISES QUI ÉMETTENT DU BON HASARD

Des sources publiques de nombres aléatoires, infalsifiables et contrôlables *a posteriori*, sécuriseraient de nombreux protocoles, comme les tests de médicaments, les tirages au sort du loto ou le choix des jurés d'assises.

RENDEZ-VOUS

P.80 *Logique & calcul*
P.86 *Art & science*
P.88 *Idées de physique*
P.92 *Chroniques de l'évolution*
P.96 *Science & gastronomie*
P.98 *À picorer*

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)

Produire un hasard parfait avec une absolue certitude est difficile; au sens mathématique, c'est même impossible (*voir l'encadré 1 page ci-contre*). Cependant, on admet que les méthodes à base de mécanique quantique créent un hasard probablement correct, et même que certaines méthodes purement algorithmiques donnent des séquences aléatoires si proches du hasard parfait qu'on peut les utiliser en toute tranquillité.

Nous examinerons ici la création sécurisée d'aléas publics et la mise à disposition d'un hasard infalsifiable, utile dans de nombreuses situations. Cette création de hasard sera le fait de balises aléatoires (en anglais: *random beacons*), des phares numériques émettant des nombres (binaires ou autres) aléatoires que tout le monde peut voir et que nul ne peut fausser et anticiper. On utilise parfois le terme «source publique d'aléas», mais nous préférerons le terme de balise aléatoire.

PILE OU FACE PAR TÉLÉPHONE...

Le jeu de pile ou face par téléphone pose ce problème du partage d'une source de hasard. Vous voulez jouer mais vous n'avez pas confiance en la personne au bout du fil, ni elle en vous. Il est donc impossible que l'un de vous lance la pièce et indique le résultat à l'autre. Il faudrait utiliser un fournisseur extérieur en qui vous auriez confiance tous les deux et qui ne pourrait être influencé ou acheté par aucun des joueurs. Ce fournisseur indépendant pourrait être une balise aléatoire. Pour satisfaire vos attentes, elle doit posséder certaines propriétés.

(a) Elle doit émettre périodiquement, à intervalle de temps fixé, des nombres aléatoires que des entités éloignées peuvent observer (par Internet) simultanément en ayant la certitude d'observer la même chose.

(b) La source doit être impossible à prédire et à truquer; autrement dit, il faut qu'interviennent dans le résultat des éléments que personne (ni l'émetteur ni les joueurs) ne puisse anticiper ou manipuler.

(c) Il faut que chacun puisse vérifier après une émission quels nombres ont été émis, pour chaque date d'émission et cela avec la certitude que rien n'a été modifié après l'émission, ni par la balise elle-même ni bien sûr par un acteur étranger à la balise. C'est la vérifiabilité *a posteriori*.

Avec une telle balise aléatoire, jouer à pile ou face par téléphone est facile. Les joueurs décident que le bit produit à un instant donné, convenu entre eux, fixera le résultat du tirage: par exemple 0 pour *pile*, 1 pour *face*; et attendent l'émission de ce bit par la balise, qui désignera le gagnant sans tricherie possible.

Si un site de jeux sur internet prétend tirer seul au hasard les gagnants d'une loterie ou distribuer des cartes à partir d'un jeu bien mélangé, il n'est pas raisonnable de lui faire confiance, car il peut faire gagner qui il veut et manipuler les distributions de cartes... et cela s'est déjà produit. En revanche, s'il indique précisément comment, à partir d'une balise aléatoire sûre et indépendante, il déduit les gagnants ou obtient le mélange du jeu de cartes, et que chacun peut vérifier qu'il respecte le protocole fixé, il ne pourra pas tricher.

Jean-Paul Delahaye a notamment publié: **Les Mathématiciens se plient au jeu**, une sélection de ses chroniques parues dans *Pour la Science* (Belin, 2017).

IMPOSSIBLE HASARD PARFAIT

Les méthodes algorithmiques de production de suites aléatoires ne donnent pas des suites aléatoires au sens fort défini par Per Martin-Löf en 1965. En effet, « être produit par un algorithme » entraîne que celui qui détient l'algorithme peut anticiper ce qui sera produit. De plus, ce qui est produit par un algorithme peut être compressé en un fichier de taille au plus égale à la taille du programme de l'algorithme ; or ce qui est authentiquement aléatoire est incompressible. Les décimales de π, en particulier, sont produites par des algorithmes tirés de séries numériques classiques et ne constituent donc pas une suite aléatoire au sens fort.

Les méthodes physiques (loterie, bruit thermique, mécanique quantique, etc.) ne produisent des suites aléatoires au sens fort que (1) sous l'hypothèse que les théories associées (par exemple la mécanique quantique) sont les bonnes théories qui régissent la physique du mécanisme producteur, ce qui est impossible à prouver, et (2) si le dispositif physique producteur a été correctement monté et ne subit aucune manipulation, et en particulier n'est victime d'aucune porte dérobée. Il se peut donc que les méthodes quantiques produisent de véritables suites aléatoires, mais l'affirmer est impossible car cela reviendrait à affirmer que la mécanique quantique est une théorie qui ne sera jamais remise en cause, et que l'on a bien modélisé le dispositif physique utilisé, deux affirmations risquées, comme le montre l'histoire de la physique.

Il en va de même plus généralement pour tous les sites internet qui proposent des jeux où le hasard intervient, et cela concerne aussi les loteries nationales, lotos et autres jeux d'argent organisés à grande échelle. Tous devraient proposer des procédures de tirage non plus fondées sur des dispositifs physiques locaux que certains ont su manipuler, mais sur des balises aléatoires sécurisées dont l'utilisation serait rendue parfaitement contrôlable *a posteriori* grâce aux données enregistrées.

L'utilisation de balises aléatoires concerne d'autres domaines et devrait y être obligatoire. Si une entreprise qui produit des médicaments assure qu'elle teste au hasard les lots mis en circulation, il est souhaitable que le système de tirage au sort qu'elle utilise pour ces contrôles soit fondé sur un tirage aléatoire extérieur, car c'est la seule façon d'être certain que l'entreprise ne choisisse pas les cobayes à sa convenance.

Lorsqu'un tribunal désigne au hasard des jurés ou qu'une procédure politique choisit aléatoirement des représentants, il serait souhaitable, pour garantir l'absence de biais et de manipulations, que la procédure elle aussi se fonde sur une balise aléatoire indépendante publique et autorisant des contrôles *a posteriori*.

D'autres exemples concernent les applications décentralisées, par exemple liées aux blockchains et aux monnaies cryptographiques. Ils confirment l'importance de bonnes balises aléatoires et, depuis quelques années, le sujet préoccupe les informaticiens et les cryptologues qui ont, nous le verrons, élaboré des idées subtiles afin que personne ne triche.

Explorons pas à pas le problème de la création de balises aléatoires sûres.

LA MÉTÉO, UNE BALISE ALÉATOIRE ?

Notre premier exemple de balise élémentaire donnant un aléa public pour le pile ou face par téléphone s'appuie sur la météo. La balise serait déduite des publications sur internet de Météo-France. Elle produirait un bit par jour en se fondant sur la température à midi relevée par Météo-France à la station météorologique de Paris-Montsouris. Cette température serait arrondie au dixième de degré inférieur et un 0 (correspondant à *pile*) serait produit si le premier chiffre après la virgule de la température est pair et un 1 (correspondant à *face*) serait produit si le premier chiffre est impair.

Un site internet donne cette température « officielle » et peut donc, sans intermédiaire, servir de balise aléatoire : www.infoclimat.fr/observations-meteo/temps-reel/paris-montsouris/07156.html. La température à midi y est chaque jour définitivement inscrite sur le site et reste ensuite accessible. On trouve par exemple les données suivantes : 11,8 °C pour le 28 novembre 2019 à midi, qui donnerait un 0, donc *pile* ; 9,5 °C pour le 29 novembre 2019 à midi, qui donnerait un 1, donc *face* ; 7,8 °C pour >