Sécurité Analogique de l'Information : (Sécurité du Futur)

HADJ-SAID Naima, ALI PACHA Adda
Université des Sciences et de la Technologie d'Oran USTO
BP 1505 El M'Naouer Oran 31036 ALGERIE
alipacha@yahoo.com

Résumé : La sécurisation de l'information est aujourd'hui, essentiellement fondée sur les algorithmes de calcul dont la confidentialité dépend du nombre de bits nécessaires à la définition d'une clé cryptographique. Si ce type de système a fait ses preuve, la puissance croissante des moyens de calcul menace la confidentialité de ces méthodes cryptographiques classiques. Les ordinateurs puissants sont certes capables de chiffrer et de déchiffrer rapidement l'information, mais leur vitesse de calcul autorise parallèlement la cryptanalyse, qui a pour objectif de « casser » un code en découvrant la clé, par exemple en testant toutes les clés possibles. La seule évocation du principe de l'ordinateur quantique, aux capacités de calcul potentiellement colossales, a déclenché un choc, même chez les plus farouche convaincus de la cryptographie algorithmique. Pour pallier cette inquiétude, deux méthodes ont émergé ces dix dernières années, bien différentes dans leur principe des méthodes classiques :

1. La cryptographie quantique : La technique se base sur la polarisation des photons qui rend compte de leur moment angulaire interne. Le résultat d'une mesure de polarisation peut prendre deux valeurs possibles, assimilables au système binaire 0 et 1.
2. La cryptographie continue par un signal chaotique : consiste à ajouter au message à transmettre un signal chaotique. L'émetteur envoie à un récepteur ce signal chaotique où le message est noyé. Connaissant les caractéristiques du signal chaotique initial, le récepteur sait extraire le message du signal reçu.

Dans cette communication on essaye de faire en outre, d'une part l'introduction à la sécurité quantique et du chaos chiffrant et d'autre part, étudier la possibilité de mettre le chaos à la disposition de la cryptographie algorithmique (cryptographie à clé secrète) pour cela, il faut chercher des modèles mathématiques adéquats pour sécuriser l'information, et que ses derniers satisfassent les conditions du chaos.

Mots Clés : Cryptographie; Cryptanalyse; Chaos; Quantique.

Introduction

La théorie de l'information et la cryptographie conventionnelle (algorithmique) prennent pour acquis que les communications numériques peuvent toujours être espionnées de façon passive ou enregistrées pour usage futur, même par une personne qui ne peut en comprendre le sens.

Enregistrer une communication chiffrée incompréhensible peut servir à quelqu'un qui espère découvrir la clé cryptographique à une date ultérieure, peut-être après avoir accumulé suffisamment de texte chiffré pour faciliter la cryptanalyse. On voit donc, qu'il y a aujourd'hui une perpétuelle remise en cause de la cryptographie par la cryptanalyse. C'est une sorte de véritable combat. Les progrès de la cryptanalyse entraînent nécessairement des progrès en cryptographie et vice-versa. C'est une évolution sans fin.

On peut se demander si la confidentialité des messages ne se trouve pas alternée dans ces progressions ?

La réponse est bien évidemment **NON** cela s'explique par :

D'une part : L'existence d'une catégorie d'algorithmes de sécurité d'information en cycle de recherche. Ce sont des algorithmes à base de la cryptographie analogique comme ceux de la cryptographie quantique et de la cryptographie continue par un signal chaotique.

La cryptographie quantique est fondée sur la mécanique quantique et les propriétés très particulières de la matière dans ce domaine. Elle utilise comme véhicule de transmission un canal quantique. Grossièrement, chaque bit du message serait codé avec un photon.

Par contre, le principe du chiffrement par chaos consiste à ajouter au message à transmettre un signal chaotique. L'émetteur envoie à un récepteur ce signal chaotique où le message est noyé. Connaissant les caractéristiques du signal chaotique initial, le récepteur sait extraire le message du signal reçu. Ce type de cryptographie par chaos a émergé au début des années 1990, lorsqu'on a compris comment reproduire à l'identique du chaos.

D'autre part : Vu les ressources technologiques onéreuses allouées à ces deux méthodes et leur complexité de réalisation. On a pense mettre le chaos à la disposition de la cryptographie algorithmique. Car, voulant faire une étude sur la cryptanalyse on a remarqué que les cryptogrammes (cryptographie à clé secrète) ont

un comportement chaotique [5]. C’est pourquoi, il nous faut chercher d’abord des modèles mathématiques adéquats pour sécuriser l’information, et que ses derniers satisfassent les conditions du chaos.

Le chaos est un comportement à long terme imprévisible qui provient d’un système dynamique déterministe à cause de la sensibilité des conditions initiales [6]. Le chaos n’est pas un désordre complet, c’est un désordre dans un système dynamique déterministe qui est toujours prévisible à court terme.

1. CRYPTOGRAPHIE QUANTIQUE

La cryptographie quantique [2, 3] est née au début des années 70. Elle repose sur le principe d'incertitude d'Heisenberg, qui est au cœur de la physique quantique, donne lieu à des phénomènes cryptographiques inédits, irréalisables avec les dispositifs de transmission conventionnels en affirmant que certaines quantités ne peuvent pas être mesurées simultanément.

Ainsi, il permet d'établir un canal de communication que nul ne peut espionner sans risquer de perturber la transmission de façon détectable par ses usagers légitimes, et ces quelque soit la technologie dont dispose l'espion.

A. Principe d'Incertitude d'Heisenberg

Un état quantique est constitué de plusieurs paramètres, par exemple la position et la vitesse d'une particule.

Le principe d'Heisenberg stipule que si l'on mesure avec précision un paramètre (la vitesse par exemple), l'état quantique de la particule est perturbé.

Ainsi, il est possible de distribuer une clef secrète aléatoire à deux utilisateurs qui ne partagent initialement aucun secret, de façon sécurisée contre des espions même de puissance de calcul infinie. Il en résulte donc un canal de communication dont les transmissions ne peuvent pas être lues ou copiées sans connaître une information-clé utilisée pour la transmission. Une fois cette clef secrète établie, elle peut être utilisée avec un système cryptographique classique.

B. Propriétés des photons polarisés

Dans certain type d’algorithme quantique le transport de la clé "quantique" est transporté par les photons individuels, ces composants élémentaires de la lumière.

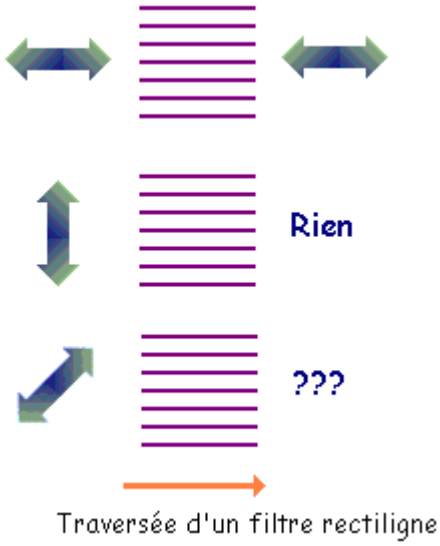
La lumière polarisée peut être produite en faisant passer un rayon de lumière ordinaire à travers un polariseur, que ce soit un filtre Polaroïd ou un cristal de calcite. L'axe de polarisation du faisceau est déterminé par l'orientation du polariseur d'où émerge le faisceau. La production de photons polarisés isolés est théoriquement possible mais s'avère difficile à réaliser d'un point de vue technologique. Nous ferons initialement comme s'il était réaliste d'obtenir de tels photons isolés avec une polarisation définie.

Chaque photon peut être polarisé, c'est-à-dire que l'on impose une direction à son champ électrique. La polarisation est mesurée par un angle qui varie de 0° à 180°.

Dans un protocole [3] dû aux canadiens CH. Bennett et G.Brassard, la polarisation peut prendre 4 valeurs : 0°, 45°, 90°, 135°.

Pour les photons polarisés de 0° à 90°, on parle de polarisation rectiligne, pour ceux polarisés de 45° à 135°, de polarisation diagonale.

Il nous faut pouvoir détecter la polarisation des photos. Pour cela, on utilise un filtre polarisant suivi d'un détecteur de photons.



Si un photon polarisé à 0° rencontre un filtre polarisant orienté à 0°, il traverse ce filtre polarisant et est enregistré par le détecteur placé juste après.

Si un photon polarisé à 90° rencontre le même filtre, il est immédiatement stoppé, et le détecteur n'enregistre rien.

Maintenant, si le photon est polarisé diagonalement (45° ou 135°), une fois sur deux, il traverse le filtre, et une fois sur deux, il est stoppé.

Si on peut distinguer entre une polarisation à 0° et à 90°, il est impossible de distinguer en même temps entre une polarisation à 45° et à 135°.

De la même façon, on peut utiliser un filtre polarisant orienté à 45° : il laisse passer les photons polarisés à 45°, stoppe ceux polarisés à 135°, et se comporte aléatoirement avec ceux à 0° et 90°.

Bien que la polarisation varie de façon continue, le principe d'incertitude interdit qu'une mesure sur un photon isolé révèle plus qu'un bit d'information à propos de sa polarisation.

Si un faisceau lumineux avec un angle de polarisation a traverse un filtre avec un angle d'orientation b , les photons individuels se répartissent de manière dichotomique et probabiliste, chacun étant transmis avec une probabilité $\cos^2(a-b)$ ou absorbé avec $\sin^2(a-b)$ probabilité complémentaire.

Les photons se comportent de manière déterministe seulement lorsque les deux axes sont parallèles (transmission certaine) ou perpendiculaires (absorption certaine).

C. Distribution de la clé

Pour que deux personnes puissent communiquer de façon totalement sécurisée, il faut d'abord qu'elles possèdent la même clé de cryptographie.

Un émetteur Alice doit pouvoir faire parvenir sa clé à un destinataire Bob sans altération de l'information et sans qu'un tiers Eve puisse intercepter ou en tout cas déterminer cette clé.

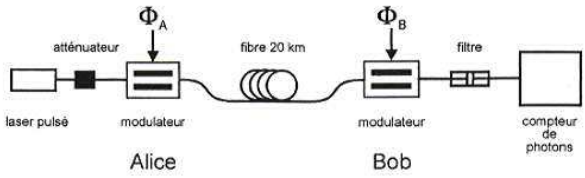


Figure 1. schéma explicatif du système développé à Georgia Institute of Technology (GTL)-CNRS Telecom.

Alice code la clé sur l'amplitude et la phase des impulsions et envoie l'information à travers un faisceau de lumière cohérente pulsée.

A l'autre bout, Bob reçoit cette information ; il la traite, l'évalue et la corrige en tenant compte des bruits associés.

Un échange se tient alors entre Alice et Bob afin de déterminer ce que chacun a reçu et interprété. Eve peut à tout instant intervenir, tenter d'intercepter et de décoder le message.

Mais la possibilité qu'a Eve d'évaluer et de corriger les bruits associés afin d'extraire une valeur correcte est limitée. Il existe en effet 4 types de bruit [2]:

1) Bruit électronique du détecteur de Bob,

2) Bruit lié à une détection homo dyne efficace : c'est une détection interféromètrique sensible à la phase du signal optique, par opposition à hétérodyne, où cette information de phase est perdue.

3) Bruits d'émission et

4) Bruits de transmission.

Or, la correction d'erreur pour Eve ne peut se faire que sur le bruit de la transmission.

D. Principe de Chiffrement Quantique

La cryptographie quantique code les bits de données grâce à la polarisation des photons.

Le texte du message préalablement codé sous forme de bits classiques est représenté par un ensemble de photons dont l'état quantique correspond à ces bits, selon le principe incertitude Heisenberg, il est impossible de distinguer deux états sans effectuer des mesures qui modifieront l'état du photon détecté par le destinataire.

La cryptographie quantique consiste donc, à utiliser un canal où circulent des photons polarisés à des angles différents, 0 ou 90 degrés; 45 ou 135 degrés, pour déterminer entre deux personnes une clé secrète qu'ils sont les seuls à connaître.

2. La théorie du chaos

En 1986, c'est à un congrès international organisé par la Royal Society à Londres que le chaos a été défini comme un "comportement stochastique se produisant dans un système déterministe". Même si aucune définition du chaos ne fait l'unanimité chez les scientifiques, celle-ci possède l'avantage de bien exprimer tout le paradoxe d'un comportement à l'apparence aléatoire mais gouverné malgré tout par une ou des lois.

E. Théorie de Base

De façon plus précise, les systèmes chaotiques sont caractérisés par un comportement imprévisible et à l'apparence désordonnée, par une nature déterministe et par une sensibilité aux conditions initiales.

Cette dernière caractéristique implique qu'il existe une disproportion entre les différences minimes initiales et celles, immenses, à plus long terme. Après un temps que l'on nomme caractéristique. Cette propriété spécifique des systèmes chaotiques entraîne l'impossibilité de prédire adéquatement leur évolution dans le temps, sauf à très court terme. De plus, cette prédiction précoce n'est possible que si les variables étudiées sont isolées des facteurs confondants, qui interagissent entre eux en tout temps et à toutes les échelles dans un système chaotique naturel.

1) Attracteur

L'attracteur est un environnement dans lequel chaque point qui est situé à proximité de ce dernier tend au fur et à mesure de l'atteindre quand le temps tend vers l'infini. Donc, l'état du système en équilibre.

2) l'Exposant de Lyapunov

Les exposants de Lyapunov évaluent la vitesse (taux) auxquelles les orbites avoisinantes convergent où divergent. Approximativement l'exposant de Lyapunov est une constante de temps λ dans l'expression de la distance entre deux orbites proches, exp.(λ.t) :

- Si λ est négative il y'a convergence des orbites et le système est insensible aux conditions initiales.

- Cependant pour λ positive cette distance croit exponentiellement et le système dépend des conditions initiales.

3) Bifurcation

La bifurcation est l'étude de la variation des solution d'un problème non linéaire c'est à dire la variation de la stabilité en fonction des variations des paramètres. C'est donc un changement qualitatif dans le comportement dynamique à la suite d'une petite variation dans les paramètres du système.

F. Reproduire le chaos :

La reproduction du chaos semble impossible : par essence, le chaos a souvent été assimilé a l'absence d'ordre et perçu comme une réalité non désirable. La théorie du chaos nous enseigne qu'au contraire ce dernier ne se situe pas à l'opposé de l'ordre mais contient également son propre ordre en autant qu'on lui permette de se manifester, un nouvel ordre peut émerger du chaos dans la mesure où l'on accepte de revoir certains paradigmes.

En 1990, Thomas Carroll et Louis Pecora ont réussi à reproduire de manière exact un signal électrique chaotique. C'est la synchronisation des signaux chaotiques.

Ainsi, la découverte de la synchronisation des signaux chaotiques a permis d'utiliser le chaos comme moyen actif de modulation de l'information, et la synchronisation

d’un récepteur autorise l’extraction de l’information initialement noyée dans la « porteuse » chaotique. C’est le principe de la cryptographie continue par chaos.

G. Cryptographie Continue par un Signal Chaotique :

La méthode qui vient d'être développée [4] consiste à crypter optiquement le signal à transmettre sous forme d'un chaos en longueur d'onde généré par une diode laser. Celle-ci est munie d'un élément non linéaire en longueur d'onde et d'une boucle de contre-réaction qui introduit un retard entre le signal émis par la diode laser et le signal qui lui est réinjecté.

La diode laser émet alors de la lumière dont la longueur d'onde fluctue rapidement au cours du temps, et de façon chaotique. L'émission en longueur d'onde s'apparente à celle d'un bruit de fréquence déterministe, dont le spectre est comparable à celui d'un bruit blanc.

L'originalité de cette méthode réside dans le fait que la non linéarité à l'origine du chaos ainsi produit est une non linéarité en longueur d'onde et non en énergie, comme c'est généralement le cas.

- L'un des avantages est d'éviter d'opérer avec des densités de puissance élevées - ce qui pose souvent des problèmes de stabilité de fonctionnement et de vieillissement de matériaux en optique non linéaire. Cette particularité permet d'obtenir un chaos extrêmement stable au cours du temps, dont de plus, le paramètre de bifurcation peut être facilement contrôlable.

- Le second avantage est de pouvoir modifier de façon très simple la fonction non linéaire à l'origine du chaos, c'est-à-dire, en termes de cryptage, la clef utilisée pour coder les signaux.

L'intérêt réside dans le fait que le chaos, qui constitue la clef de cryptage, peut être facilement modifié par le biais de son diagramme de bifurcation tout en permettant des débits de transmission élevés adaptés aux fibres optiques.

Ce procédé de cryptage s'applique à tout type de signal, analogique ou numérique.

1) Chiffrement/ Déchiffrement:

L'opération de cryptage consiste alors à masquer le message par ce bruit. Ce masquage est d'autant plus efficace que la complexité du bruit est grande (en terme de physique du chaos, le chaos ainsi généré obéit à une équation différentielle à retard,

ou équation d'Ikeda ; la complexité du chaos obtenu est d'autant plus élevée que le paramètre de bifurcation est grand).

Le décryptage s'effectue en générant un second chaos en Longueur d'onde, identique au précédent. Pour cela, le système de décryptage utilise un générateur de chaos comportant les mêmes éléments que ceux utilisés pour produire le chaos de cryptage, notamment un retard et un élément non linéaire en longueur d'onde identiques aux précédents. Ce système fonctionne toutefois en boucle ouverte, le signal se propageant dans la boucle de commande étant le signal crypté que l'on veut analyser. Le signal alors produit est un chaos dont la comparaison au chaos de cryptage permet d'extraire le message.

2) Synchronisation des Signaux Chaotiques

Le décodage d'un système de chiffrement par chaos ne peut être obtenu que grâce à la synchronisation. La clé de cette synchronisation constitue aussi la clé en termes cryptographiques: elle est donnée par le déterminisme à l'origine de la trajectoire chaotique. Cette capacité de synchronisation des signaux chaotiques résulte d'une des différences fondamentales entre le bruit et le chaos. Alors que l'information est imprévisible, le chaos est prévisible à court terme, car il résulte d'un principe déterministe. Ce déterminisme propre à un signal chaotique résulte mathématiquement des propriétés d'une équation différentielle régissant la loi d'évolution du signal dans le temps.

La « magie » des processus chaotiques réside dans le fait que les solutions de ces équations sont tellement riches, qu'elles ont l'apparence d'un bruit aléatoire.

3. CRYPTOGRAPHIE ALGORITHMIQUE CHAOTIQUE

On introduit dans ce qui suit l'étude à la théorie du chaos et la possibilité de mettre le chaos à la disposition de la cryptologie. Mais, on doit d'abord prouver que les cryptogrammes ont un comportement chaotique, une fois qu'il est chaotique on peut résoudre le problème en utilisant des éléments chaotiques.

1) En algèbre, une fonction f est linéaire si elle satisfait la propriété suivante:

$f(x+y) = f(x)+f(y)$ et $f(ax) = af(x)$.

La non linéarité de f est définie comme étant la négation de la linéarité, c'est à dire que le résultat de f soit hors proportion de l'entrée x ou y.

2) Un système dynamique consiste en un espace d'état dont les coordonnées décrivent à chaque instant suivant une règle spécifique l'évolution futur de son l'état dynamique. Mathématiquement un système dynamique est décrit par un problème de valeur initiale, il peut être discret ou continue.

Pour qu'un système dynamique non linéaire soit chaotique [4], il doit avoir un grand ensemble de conditions initiales qui sont hautement instables. Le chaos est un système défini habituellement par une fonction f qui satisfait les trois propriétés suivantes:

H. Fonction est dense

Un système est topologiquement dense si quelque soient deux points distinctes de l'ensemble de valeur de sa fonction représentative$f$, il aura toujours un autre point image de f situé entre ces deux points.

I. Fonction est transitive

Un système est topologiquement transitif si on peut identifier un intervalle fini dans lequel les valeurs par la fonction f de tout point de cet intervalle demeure toujours dans cet intervalle.

J. Dépendance des conditions initiales

Une variation graduelle d'un paramètre correspond à une variation graduelle des solutions du problème d'un système dynamique. Cependant il existe un grand nombre de problèmes pour lesquels les nombres de solutions changent d'une façon brut, et la structure de ensemble des solutions varie dramatiquement quand un paramètre passe à une valeur critique.

La dépendance à la sensibilité qui est une caractéristique des systèmes chaotiques ne nécessite pas une croissance de perturbation exponentiel (exposant de Lyapunov positif).

K. Comportement Chaotiques des Cryptogrammes

Etant donné que le système cryptographique à clé secrète f reposant entièrement sur la clé de l'utilisateur chiffre toujours de la même façon pour cette même clé, car toutes ces opérations (tables et procédures) sont fixes et publics (connues de tous), et cette clé est utilisée pour coder et décoder des données.

Dans ce cas là, on peut se demander si nos cryptogrammes sont déterministes ou chaotiques.

- Les cryptogrammes sont représentés sur 8 bits binaires par le code ASCII.
- L'ensemble ASCII des éléments 8-uplets binaires est une partie incluse dans l'espace vectoriel normé complet $\Re 8$. Donc cette ensemble est complet et par suite il est fermé, donc il est égale à son adhérence et delà il est **dense**.
- Toute fonction f de l'ensemble ASCII vers lui même est **transitive** par hypothèse.

On ce qui concerne la **dépendance des conditions initiales**, étant donné un seul bit erroné, afin de déchiffrer un message, de la clé personnelle de l'utilisateur produit un véritable déluge de modifications et donc brouillent d'avantage le texte crypté.

On conclut que les cryptogrammes d'un système cryptographique à clé secrète satisfait les trois conditions du chaos.

Donc, il nous faut établir d'abord un modèle mathématique chaotique et montrer qu'il décrit le système cryptographique d'une façon approprie, la CRYPTANALYSE CHAOTIQUE pourra être possible.

Conclusion

Le but de la cryptographie est de préserver les données confidentielles, qu'elles soient stockées localement sur une machine ou transmises sur un réseau, de l'indiscrétion des attaquants (adversaires, espions intercepteurs, intrus, opposants, oreilles indiscrètes, cryptanalystes, décrypteurs, ou ennemis). Les systèmes de chiffrages actuels découlent du postulat de base que tous les codes adaptés aux communications de masse peuvent être en définitive forcés, mais que l'on peut parvenir à une sécurité suffisante en rendant totalement irréaliste la quantité de travail qu'il faudrait fournir pour les forcer.

Pour casser ces algorithmes, la cryptanalyse met en œuvre une combinaison de raisonnement analytique, d'utilisation d'outils mathématiques, de recherche de motifs, de patience, de détermination et de chance.

Si la cryptographie quantique présente l'avantage de résoudre de manière absolue le problème de la confidentialité (elle est, par principe, « incassable »), elle reste limitée en terme de coût de mise en œuvre, et surtout en termes de débits maximum d'information: aujourd'hui, ces débits ne dépassent pas quelques dizaines de kilo bits par seconde.

La cryptographie par le chaos a prouvé sa faisabilité et sa vitesse de codage supérieure au giga bit par seconde, vitesse adaptée aux débits des réseaux de télécommunications modernes.

Par contre en ce qui concerne la cryptographie algorithmique chaotique, elle est a ses début, en attendant ceux qui nous confirme notre démarche.

Mais, la théorie des systèmes dynamiques non linéaires, (autre définition du chaos), est loin d'être la panacée que certains chercheurs imaginaient à ses débuts. Il n'en reste pas moins que ses concepts intéressants peuvent être appliqués à des problèmes bien ciblés par l'emploi de méthodes mathématiques rigoureusement choisies et adaptées aux systèmes sous étude.

La théorie du chaos nous enseigne qu'au contraire ce dernier ne se situe pas à l'opposé de l'ordre mais contient également son propre ordre en autant qu'on lui permette de se manifester.

Un champ aussi complexe que celui de la cryptologie (cryptographie et cryptanalyse) ne peut que bénéficier de l'ajout de tels moyens d'investigation si leurs forces, et surtout leurs limites, sont bien comprises.

Références

[1] B. SCHNEIER :''Cryptographie appliquée'', John Wiley & Sons, Inc., 1994.

[2] Mélanie Langlois,'Cryptographie Quantique – Solution au problème de Distribution de Clefs Secrètes', Université d'Ottawa, Décembre 1999.

[3] www.bibmath.netcrypto/moderne/quantique.php3.

[4] Laurent LARGER, « Cryptage de Signaux par Chaos en Longueur d'Onde », thèse de Doctorat, l'U.F.R

[5] des Sciences et Techniques de l'Université de FRANCHE-COMTE, Besançon, France, 1997.

[6] A. ALI-PACHA, N. HADJ-SAID, B. BELMEKKI, A. BELGORAF, « Chaotic Behaviour for the Secrete key of Cryptographic System », Revue Elsevier Science : Chaos, Solitons & Fractals, Volume 23/5 pp. 1549-1552, Accepted 5 May 2004. Available online 22 October 2004.

[7] Stewart, W. 1992. Dieu joue-t-il aux dés ? Les mathématiques du chaos. Flammarion.