

infalsifiables et vérifiables *a posteriori*. L'utilisation de fonctions de hachage au sein des pages ajoutées périodiquement aux fichiers blockchains semble introduire un hasard dans ces blockchains qui par ailleurs sont publiques et infalsifiables car conservées en de multiples exemplaires lisibles par tous. Cependant, une étude publiée en 2018 par Cécile Pierrot, de Sorbonne Université, à Paris, et Benjamin Wesolowski, de l'École polytechnique fédérale de Lausanne (EPFL), a montré qu'en réalité de telles sources pourraient être manipulées par des acteurs assez puissants. Même si cela peut avoir un certain intérêt d'utiliser l'aléa des blockchains en le mêlant à d'autres sources, une balise aléatoire ne doit pas se fonder sur cette méthode seule.

Plus intéressant, le cryptologue Arjen Lenstra, de l'EPFL, et Benjamin Wesolowski, ont récemment introduit deux idées nouvelles susceptibles de renforcer la confiance envers les balises aléatoires modernes.

La première idée est de permettre aux acteurs qui le souhaitent de participer à ce qui est produit. Entre deux émissions successives, on permettrait à quiconque le souhaite d'envoyer des nombres à la balise. Tous ces nombres seraient regroupés en un seul dont on calculerait l'empreinte, et l'on mêlerait celle-ci aux résultats du mécanisme local (quantique ou autre) de la balise, par exemple par le biais d'une somme modulo 2 comme quand on mélange plusieurs balises. De plus, le site de la balise autoriserait la vérification que les nombres envoyés sont bien pris en compte.

Le fait de pouvoir envoyer ses propres données assurerait que, même si tous les autres intervenants et la balise forment une association dont le but est de vous tromper, elle ne réussira pas. Le fait que vous interveniez ne vous donne heureusement pas le pouvoir de manipuler la balise et cela même en vous coordonnant avec tous les intervenants extérieurs, car la composante locale (avec une somme modulo 2) rend vaine toute tentative de biais.

DES FONCTIONS DONT LE CALCUL NÉCESSITE UN DÉLAI

La seconde idée est plus subtile, mais la plus importante peut-être pour assurer qu'aucune manipulation n'est possible, même par la balise. Elle utilise le concept de *fonction vérifiable à délai* ou VDF (le sigle anglais), objet d'intenses recherches depuis trois ans.

Une VDF est une fonction qui, lorsqu'on lui confie un fichier quelconque, le transforme en une séquence de chiffres aléatoires, comme le fait une fonction de hachage (voir l'encadré 3). Mais en plus, elle le fait de telle façon que le calcul ne peut pas être mené en moins d'une certaine durée (par exemple 30 secondes), et que la vérification de son

résultat final est quasi instantanée: calculer est long, vérifier est rapide.

Même si une balise aléatoire combine des sources extérieures, selon la première idée, un problème persiste qu'une VDF va résoudre. Le problème est qu'au moment où la balise mélange les données extérieures (qu'elle ne contrôle pas) et une donnée locale, par exemple présentée comme quantique, elle pourrait s'arranger, connaissant les données extérieures, pour que la combinaison avec ce qu'elle introduit (prétendument tiré d'un mécanisme quantique), conduise à un résultat final biaisé comme elle le souhaite. En clair, à cause de la donnée locale qu'elle introduit, la balise garde une possibilité de tricherie. Comment rendre impossible cette manipulation?

Voici la solution d'Arjen Lenstra et Benjamin Wesolowski. La balise exige que les données externes qu'elle prendra en compte lui soient parvenues durant les 30 premières secondes de l'intervalle de temps de 60 secondes entre deux émissions (en t , et en $t+60$). Elle-même, à l'instant $t+30$, engage sa donnée (par exemple quantique) en publiant son empreinte. La balise combine les données extérieures et la sienne et, à partir du résultat, effectue le calcul de la VDF qui exige 30 secondes. Le résultat de ce calcul est connu et publié par la balise à l'instant $t+60$ (il ne peut pas l'être avant) avec la donnée dont la balise n'avait communiqué que l'empreinte à l'instant $t+30$. Tout le monde peut vérifier instantanément que le calcul fait par la balise est correct (c'est la propriété de vérifiabilité instantanée) et qu'elle n'a pas changé sa donnée (puisque'elle en avait publié l'empreinte).

Les acteurs extérieurs n'ont pas pu agir sur le résultat, car ils ne connaissaient pas la donnée de la balise, restée secrète jusqu'à $t+60$, et que le résultat en dépend.

Plus important, la balise n'a pas pu proposer une donnée conduisant à un résultat qui l'arrange. En effet, dès l'instant $t+30$, elle a figé la donnée qu'elle proposait (en publiant l'empreinte) et il lui a fallu 30 secondes pour savoir comment cette donnée combinée aux autres données venant de l'extérieur (qu'elle ne connaissait pas entièrement avant $t+30$) produisait le résultat. Dans le protocole, ni un fournisseur de données externes ni la balise elle-même ne peuvent tricher. Le résultat dépend de toutes les données et il est donc vraiment aléatoire, si un seul des fournisseurs de données (local ou externe) en livre qui soient aléatoires.

On dispose ainsi de méthodes cryptographiques pour concevoir et réaliser des balises aléatoires fiables et sécurisées. Rien ne semble interdire ou limiter les applications exigeant des balises parfaitement sécurisées. On peut désormais exiger des sites internet de jeux, des loteries et lotos divers qu'ils se fondent de manière transparente sur de telles balises. ■

BIBLIOGRAPHIE

K. Pietrzak, **Simple verifiable delay functions**, dans *IACR Cryptology ePrint Archive*, n° 627, 2018.

D. Boneh et al., **Verifiable delay functions**, dans H. Shacham et A. Boldyreva (éd.), *Advances in Cryptology – CRYPTO 2018*, Springer, 2018.

C. Pierrot et B. Wesolowski, **Malleability of the blockchain's entropy**, *Cryptography and Communications*, vol. 10(1), pp. 211-233, 2018.

A. Lenstra et B. Wesolowski, **Trustworthy public randomness with sloth, unicorn, and trx**, *Int. J. of Appl. Crypt.*, vol. 3(4), pp. 330-343, 2017.

J. Bonneau et al., **On Bitcoin as a public randomness source**, *IACR Cryptology ePrint Archive*, n° 1015, 2015.

La balise aléatoire de Mads Haarh : www.random.org

La balise aléatoire du NIST : <https://beacon.nist.gov>

La balise aléatoire de l'université du Chili : <https://random.uchile.cl/en/>

Un site collectant les derniers travaux sur les VDF : <https://vdfresearch.org/>

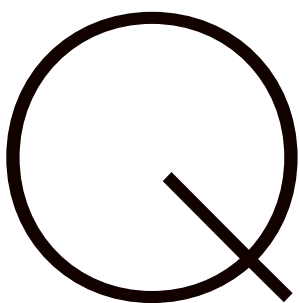
L'AUTEUR



LOÏC MANGIN
rédacteur en chef adjoint
à Pour la Science

OÙ SE CACHE LE TRIFLUOROMÉTHYLE ?

Un artiste-plasticien rend hommage à un nouveau type de réaction chimique, respectueux de l'environnement, qui aidera à préparer des composés inédits comportant un groupe trifluorométhyle, souvent intéressant en pharmacologie.



u'ont en commun l'antidépresseur Prozac, l'antipaludéen Lariam, l'anti-VIH Sustiva... ? Outre leur effet dirigé contre quelque chose, leurs principes actifs (respectivement fluoxétine, méfloquine, éfavirenz et fipronil) sont tous dotés d'un groupe chimique trifluorométhyle (CF_3). À la liste précédente, on aurait pu ajouter un autre « produit » qui partage cette particularité : une œuvre récente (voir page ci-contre) de Patrick Barrès, enseignant-chercheur au Laboratoire de recherche en audiovisuel – savoirs, praxis et poétiques en art, à l'université de Toulouse ! Où est le trifluorométhyle ?

Tout commence dans les laboratoires de Géraldine Masson, de l'Institut de chimie des substances naturelles, à l'université Paris-Saclay, et celui d'Emmanuel Magnier, de l'institut Lavoisier, à l'université de Versailles-Saint-Quentin. Avec leurs collègues, ils ont récemment mis au point une méthode de synthèse de composés trifluorométhylés, à l'aide de réactions plus respectueuses de l'environnement.

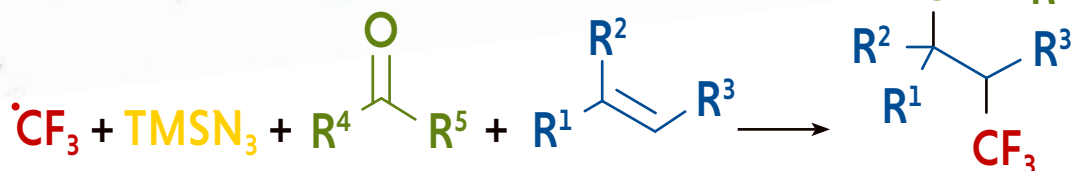
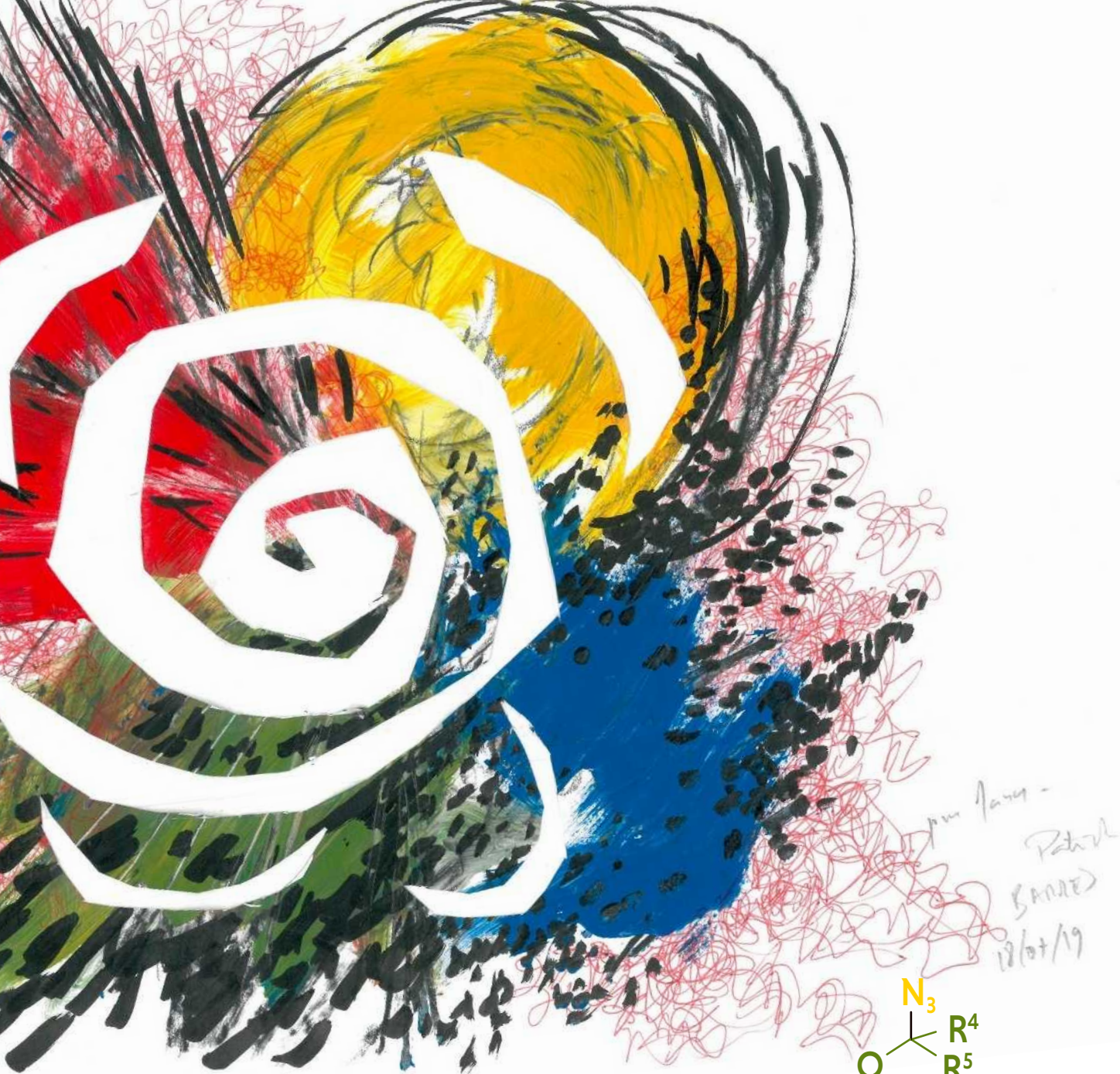
La piste suivie est celle de la photocatalyse d'oxydo-réduction dont l'un des pionniers fût, au début des années 1980, par Alain Deronzier, de l'université de Grenoble. L'idée est d'utiliser un photocatalyseur qui, éclairé, passe dans un état excité et peut alors donner ou recevoir un électron et ainsi démarrer une réaction, voire plusieurs, et dans le cas qui nous intéresse un processus dit « radicalaire » (un seul électron est engagé).

Patrick Barrès s'est emparé du résultat des chimistes et a souhaité le représenter symboliquement. De fait, les quatre zones colorées correspondent à autant de

réactifs mis en jeu : des alkènes, c'est-à-dire des molécules carbonées à double liaison (*en bleu*) ; un composé carbonyle, comportant une double liaison entre un atome de carbone et un d'oxygène (*en vert*) ; le triméthylsilyl azide $(\text{CH}_3)_3\text{SiN}_3$, noté TMSN_3 (*en jaune*) ; enfin, le réactif d'Umemoto qui apporte le groupe trifluorométhyle (*en rouge*). La spirale découpée brouille les cartes et, en apportant une dynamique à l'œuvre, renvoie à la réaction elle-même. Quelle est-elle ?

Grâce au photocatalyseur, ici le $[\text{Ru}(\text{bpy})_3(\text{PF}_6)_2]$, le rouge et le bleu s'associent, le jaune et le vert font de même, et





les deux paires interagissent enfin pour former le composé recherché (*voir la formule ci-dessus*). Tous les réactifs sont réunis en une seule fois, la réaction étant dépendante d'une part de la quantité de chacun et, d'autre part, de leur réactivité.

Pour optimiser le résultat, on utilise une lumière adaptée au photocatalyseur, en l'occurrence du bleu pour le ruthénium (Ru). Les conditions requises sont plutôt douces, sans chauffage, et les produits utilisés sont peu toxiques (on utilisait auparavant des réactifs à base d'antimoine, beaucoup plus nocif). Au final, la production de déchets est limitée

au maximum et le coût énergétique notablement réduit.

Revenons à l'œuvre. L'artiste précise: «L'ensemble s'articule autour d'un nœud, défini comme le sujet de la peinture et comme une métaphore de la fusion des éléments sous l'effet de la réaction photocatalysée.» Divers systèmes graphiques, comme les hachures, les taches éparpillées, l'enchevêtrement de lignes fines... ajoutent un effet vibratoire empêchant l'œil d'accommoder et que d'aucuns, chimistes en premier lieu, pourraient rapprocher des vibrations qui agitent toute molécule, notamment lors d'une réaction.

Mais on ne doit pas y voir, Patrick Barrès insiste, une représentation figurative de ce qui se passe dans les récipients des chimistes. Tout n'est qu'évocation, suggestion... une vraie (al)chimie douce qui n'a rien contre quoi que ce soit. ■

G. Levitre et al., *Org. Lett.*, vol. 21(15), pp. 6005-6010, 2019.



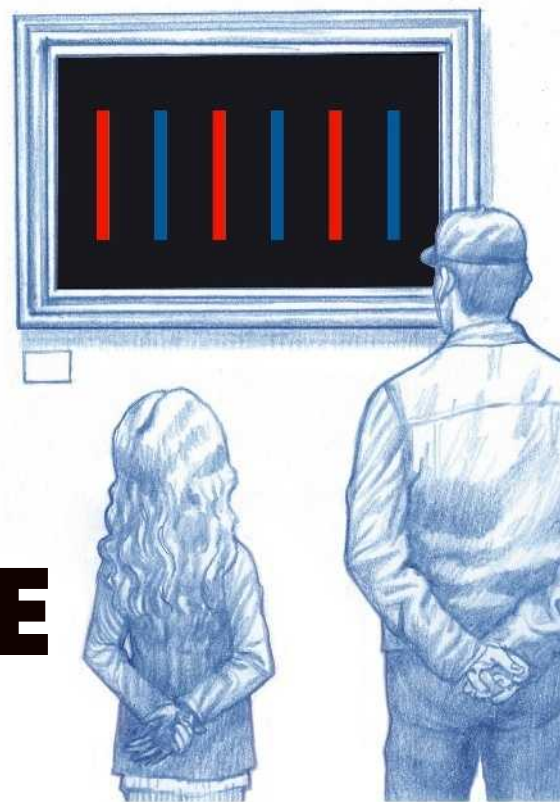
L'auteur a publié:
**Pollock, Turner, Van Gogh,
Vermeer et la science...**
(Belin, 2018)

LES AUTEURS



JEAN-MICHEL COURTY et ÉDOUARD KIERLIK
professeurs de physique à Sorbonne Université, à Paris

DE LA PROFONDEUR AVEC DU ROUGE ET DU BLEU



Certaines images colorées, bien que planes, sont perçues comme ayant du relief. L'effet trouve son explication dans les aberrations chromatiques et la physiologie de l'œil humain.

Goethe l'a mentionné dans son *Traité des couleurs* de 1810 : quand nous regardons certaines images composées de rouge et de bleu, les parties rouges semblent saillantes par rapport au plan de l'image, tandis que les parties bleues paraissent en creux (*voir l'illustration ci-dessus*). Cet effet a été utilisé comme procédé pour donner en peinture une impression de profondeur.

L'origine de l'effet est en grande partie physique et tient aux aberrations chromatiques de l'œil, semblables à celles des objectifs photographiques de mauvaise qualité : selon leur couleur, ou plus exactement leur longueur d'onde, les rayons

lumineux ne sont pas déviés de la même façon lorsqu'ils passent de l'air à l'intérieur de l'œil ou de l'objectif.

QUAND LA LUMIÈRE SE DISPERSE

Les aberrations chromatiques résultent de la dispersion de la lumière, observée par exemple lorsqu'un prisme de verre décompose un pinceau de lumière blanche. À chacune des interfaces air-verre, la composante bleue de la lumière est davantage déviée que sa composante rouge. Plus généralement, la lumière émerge du prisme en étant dispersée selon les couleurs de l'arc-en-ciel.

Pour comprendre ce phénomène et être quantitatif, nous avons besoin de

l'indice de réfraction de chaque milieu traversé, rapport entre la vitesse de la lumière dans le vide et la vitesse de la lumière dans le milieu. Ce nombre caractérise l'intensité de l'interaction de la lumière avec le milieu et dépend de la longueur d'onde lumineuse, et c'est de lui dont dépend directement l'angle de déviation des rayons.

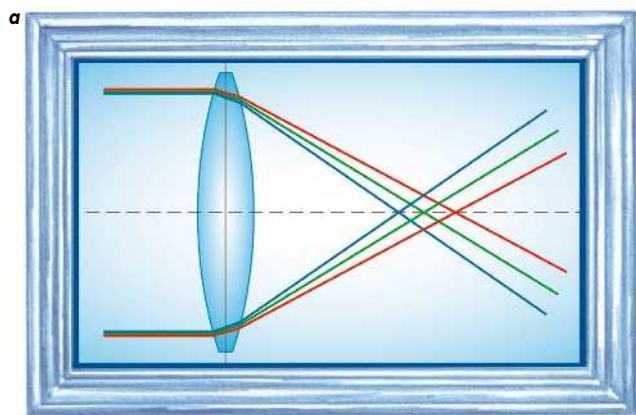
L'air, peu dense, a un indice moyen de 1,0003, proche de 1, et son caractère dispersif est en conséquence faible. Tel n'est pas le cas du verre, comme l'illustre l'expérience avec le prisme, ou, pour notre sujet, de la cornée : l'indice moyen de celle-ci est 1,37, très proche de celui de l'eau (1,33), mais il varie de 0,012 entre la lumière rouge (0,65 micromètre

ABERRATIONS CHROMATIQUES

L'indice de réfraction optique, dont dépend l'angle de déviation des rayons lumineux lorsqu'ils traversent l'interface de deux milieux, varie selon la longueur d'onde. Ainsi, lorsqu'un faisceau de lumière composite traverse une lentille convergente, les rayons se focalisent en des points plus ou moins distants selon leur longueur d'onde, donc selon leur couleur : la partie rouge de la lumière se focalise le plus loin, la partie bleue se focalise le plus près (a). Cette « aberration chromatique » de base a pour conséquence d'autres aberrations de même nature, par exemple du bleu qui, dans une image, bave sur le bord gauche d'un objet et du rouge qui bave sur son bord droit (b).



Les parties rouges des images paraissent saillantes par rapport aux parties bleues. Cet effet est dû aux aberrations chromatiques affectant les rayons lumineux quand ils entrent dans les yeux.



de longueur d'onde) et la lumière bleue (0,45 micromètre de longueur d'onde), aux deux bouts du spectre visible. Selon les lois de Descartes, avec un rayon incident à 45 degrés, on obtient un écart de 0,3 degré entre les rayons réfractés rouge et bleu.

Cet écart est du même ordre de grandeur que la dispersion dans les verres communs. Il paraît faible, mais a pourtant des conséquences pour les systèmes optiques fondés sur la réfraction. Par exemple, une lentille éclairée par un faisceau parallèle de lumière rouge et bleue focalisera la composante bleue en un point plus proche d'elle que la composante rouge (voir l'encadré ci-dessus). Cela signifie que les conditions pour former

l'image nette d'un objet bleu diffèrent de celles requises pour un objet rouge situé à la même distance.

On s'en aperçoit sur certaines photographies réalisées avec des objectifs de piètre qualité. Par exemple, si l'on a réglé l'objectif pour que la composante bleue d'un objet soit nette, alors la composante rouge sera floue et bavera sur le fond. Cet effet est bien visible lorsque la photographie présente des séparations franches entre un objet très clair et un fond sombre, ou inversement : le bord n'est pas net, mais paraît légèrement irisé.

Si l'on s'écarte du centre de l'image, ce qui correspond à des rayons lumineux d'angles d'incidence plus élevés, à l'effet de flou s'ajoute un décalage entre la partie

bleue et la partie rouge de l'image. L'irisation des bords des objets clairs s'accroît donc et on distingue un bord bleu d'un côté et rouge de l'autre !

Les aberrations chromatiques constituent un défaut que l'on peut corriger par des moyens optiques ou numériques, mais les céphalopodes (poulpes, calmars, etc.) l'ont peut-être tourné en avantage. Ces animaux n'ont qu'un seul type de cellules rétiniennes et ne voient donc qu'en

Les auteurs ont notamment publié :
En avant la physique !, une sélection de leurs chroniques (Belin, 2017).



> « noir et blanc ». Leur comportement montre pourtant qu'ils distinguent les couleurs. D'après une étude publiée en 2016 par les Américains Christopher et Alexander Stubbs, la forme très particulière de la pupille de ces mollusques aurait pour effet d'amplifier les aberrations chromatiques dans leur œil. Cela permettrait aux céphalopodes, à partir des différences de netteté des images formées sur leur rétine, de discriminer les couleurs.

LA VISION BINOCULAIRE DONNE DU RELIEF AUX COULEURS

Pour en revenir à l'œil humain, comment les aberrations chromatiques conduisent-elles à une illusion de relief? On remarque aisément que cet effet disparaît lorsqu'on ferme un œil. Il s'agit donc d'une conséquence de la vision binoculaire. Quand nous regardons un objet, nous orientons les yeux pour que son image se forme sur la fovéa, la région de la rétine où la concentration de cellules photoréceptrices est la plus élevée, c'est-à-dire où la résolution est la meilleure. Or la fovéa n'est pas située sur l'axe optique du système composé de notre cornée et notre cristallin: la direction de visée optique et l'axe optique sont décalés de 5 degrés.

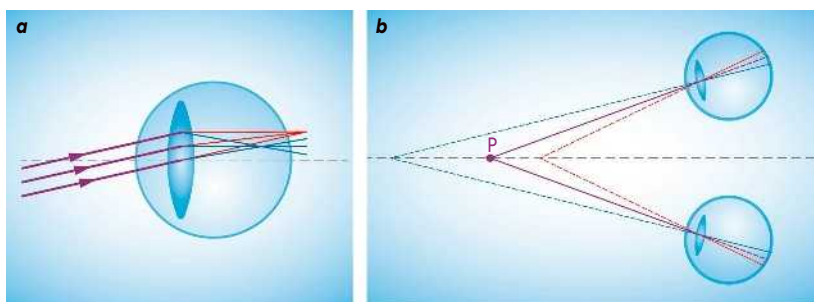
À cause de ce décalage angulaire, les rayons issus du point visé arrivent obliques par rapport à l'axe optique et on a donc les deux effets mentionnés plus haut: la distance de focalisation et la position latérale de la composante bleue des rayons diffèrent de celles de la composante rouge. Les yeux étant symétriques par rapport au milieu du visage, les décalages latéraux entre bleu et rouge sont inversés d'un œil à l'autre, et notre cerveau interprète cela comme une différence de distance (*voir l'encadré ci-dessus*).

Un calcul simplifié, en considérant un modèle rudimentaire d'œil avec la cornée comme surface réfractrice, confirme l'ordre de grandeur: la différence de profondeur apparente entre un objet bleu et un objet rouge situés à 80 centimètres des yeux est d'environ 16 millimètres, ce qui correspond bien à l'effet de profondeur perçu.

Reste que certaines personnes ne voient pas l'effet ou le voient inversé. Pourquoi? On s'est aperçu que la sensibilité des cellules rétinienne dépend de l'angle d'arrivée des rayons lumineux sur ces dernières: elle est cinq fois plus élevée pour les rayons qui passent par le centre de la pupille par rapport à ceux qui

DU RELIEF AVEC PAS MAL DE REGARD OBLIQUE...

Quand les rayons lumineux traversent l'œil de façon oblique, le point de focalisation de la composante rouge est non seulement un peu plus distant que celui de la composante bleue, mais les deux points sont aussi décalés latéralement (a). Quand on regarde un point P à une distance donnée (b), les yeux sont en fait dirigés vers un point plus distant afin que l'image de P se forme sur la fovéa, qui est décalée de 5 degrés par rapport à l'axe de l'œil. Les rayons issus de P arrivent alors de façon légèrement oblique par rapport à l'axe de l'œil. Si P est rouge, son image sur la rétine est décalée vers l'extérieur des deux yeux, tandis que si P est bleu, son image est décalée vers l'intérieur des deux yeux. En raison de cette différence angulaire, le cerveau interprète alors le point P rouge comme plus proche que le point P bleu.



passent par sa périphérie. C'est l'effet Stiles-Crawford.

Or à cause du décalage de la fovéa par rapport à l'axe optique, cet effet n'est pas symétrique. Autrement dit, la sensibilité pour les rayons passant par la gauche de la pupille diffère de celle pour les rayons passant par la partie droite. En fin de compte, tout se passe comme si la pupille effective, du point de vue optique, était décalée. Or un décalage de pupille affecte de façon différente les diverses couleurs, car cela revient à changer les angles d'incidence des rayons qui la traversent.

En mesurant cette variation de sensibilité chez diverses personnes, les chercheurs ont trouvé que l'effet Stiles-Crawford agit dans le sens contraire de l'aberration chromatique, jusqu'à éventuellement le compenser voire le surpasser – ce qui explique que, chez certains individus, l'effet de profondeur soit absent ou inverse.

L'explication est confirmée par le fait que lorsque l'image est très lumineuse, cette inversion du relief perçu disparaît. En effet, comme la pupille se contracte en réaction à la forte luminosité, les rayons arrivant sur la rétine ont tous des angles d'incidence à peu près égaux et sont alors tous perçus avec la même sensibilité par les cellules rétinienne; l'effet des aberrations chromatiques, avec le rouge qui jaillit de l'image et son bleu qui s'enfonce, reste alors entier. ■

BIBLIOGRAPHIE

M. Ozolinsh et K. Muizniece, **Color difference threshold of chromostereopsis induced by flat display emission**, *Frontiers in Psychology*, vol. 6, 337, 2015.

J. J. Vos, **Depth in colour, a history of a chapter in physiology optique amusante**, *Clinical and Experimental Optometry*, vol. 91(2), pp. 139-147, 2008.

J. Thompson et al., **Chromostereopsis : A multicomponent depth effect ?**, *Displays*, vol. 14(4), pp. 227-234, 1993.

J. J. Vos, **Some new aspects of color stereoscopy**, *Journal of the Optical Society of America*, vol. 50(8), pp. 785-790, 1960.

DURÉE LIBRE

Partie réservée au service abonnement Ne rien inscrire