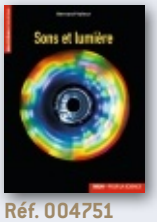


Sons et lumière

Bernard Valeur

Peut-on associer une couleur à un son comme Newton et bien d'autres après lui s'y sont essayés ? Comment le son peut-il être transformé en lumière et inversement ? Voilà quelques-uns des sujets traités dans ce livre, largement illustré, fondé sur une structure originale mettant en parallèle la lumière et le son.

Réf. 004751

Éditions Belin / Pour la Science 2008
160 pages – 24,25 euros – ISBN 978-2-7011-4751-2

Lumière et luminescence

Bernard Valeur

Fonctionnement d'un écran plat, azurants optiques qui rendent le linge ou le papier « plus blanc que blanc », bioluminescence du plancton : voilà quelques exemples de phénomènes lumineux, parmi bien d'autres, détaillés dans ce livre superbement illustré, à l'interface entre la chimie, la biologie et la physique.

Réf. 003603

Éditions Belin / Pour la Science 2005
208 pages – 25,40 euros – ISBN 978-2-7011-3603-5

La supraconductivité

Stephen Blundell

La supraconductivité est l'un des phénomènes les plus intriguant de la physique : à basse température, certains corps font léviter les aimants ! Cet ouvrage détaille la formidable découverte de la supraconductivité et nous fait partager la frénésie créatrice des physiciens quantiques pour en percer les mécanismes.

Réf. 006123

Éditions Belin / Pour la Science 2011
168 pages – 18,25 euros – ISBN 978-2-7011-6123-5

La bombe et les hommes

Aleksandra Kroh

Ce livre raconte l'histoire des hommes qui ont été marqués par la bombe nucléaire : ceux qui l'ont conçue, testée et perfectionnée, ses victimes civiles et militaires ou encore ceux qui approuvèrent son utilisation… Un récit crucial, alors que la France peine à tourner la page de ses 210 essais nucléaires.

Réf. 005501

Éditions Belin/Pour la Science 2011
176 pages – 18,80 euros – ISBN 978-2-7011-5501-2

LA SÉLECTION POUR LA SCIENCE C'EST AUSSI…

Galilée
Le découvreur du monde

Enrico Bellone

Éditions Belin/Pour la Science 2003
160 pages – 16,25 euros
ISBN 978-2-8424-5054-0

Réf. 075054

Einstein
Le père du temps moderne

Silvio Bergia

Éditions Belin/Pour la Science 2004
160 pages – 16,25 euros
ISBN 978-2-8424-5071-7

Réf. 075071

Fermi
Un physicien dans la tourmente

Michelangelo De Maria

Éditions Belin/Pour la Science 2002
160 pages – 16,25 euros
ISBN 978-2-8424-5049-6

Réf. 075049

Pour commander ces ouvrages www.pourlascience.fr/librairie *

ou en renvoyant le bon de commande ci-dessous.

* Pour commander les titres édités par *Le Pommier* : www.editions-belin.fr

BON DE COMMANDE

POUR LA SCIENCE

à retourner accompagné de votre règlement à : Groupe Pour la Science • 628 avenue du Grain d'Or • 41350 Vineuil • Tél. : 0 805 655 255 • e-mail : pourlascience@daudin.fr

❑ **Oui, je commande les livres présentés dans la sélection de *Pour la Science*.** Je reporte les titres, prix et références à 6 chiffres correspondant aux ouvrages choisis :

Titre	Réf.	Prix
		€
		€
		€
		€
		€
Frais de port (4,90 € France – 12 € étranger)	+	€
Total à régler	=	**€**

J'indique mes coordonnées :

Nom : _____

Prénom : _____

Adresse : _____

_____

C.P. : _____ Ville : _____

Pays : _____ Tél.* : _____
*facultatif

E-mail* : _____@_____
*pour recevoir la newsletter Pour la Science (à remplir en majuscules).

Je choisis mon mode de règlement :

❑ par chèque à l'ordre de *Pour la Science*

❑ par carte bancaire

Numéro _____

Date d'expiration _____

Cryptogramme _____

Signature obligatoire

DPL416

Belin ÉDITEUR INDÉPENDANT DEPUIS 1777 — Le Pommier

En application de l'article 27 de la loi du 6 janvier 1978, les informations ci-dessus sont indispensables au traitement de votre commande. Elles peuvent donner lieu à l'exercice du droit d'accès et de rectification auprès du groupe Pour la Science. Par notre intermédiaire, vous pouvez être amené à recevoir des propositions d'organismes partenaires. **En cas de refus de votre part, merci de cocher la case ci-contre ❑.**

LOGIQUE & CALCUL

La cryptographie visuelle

Une information cachée peut apparaître instantanément à notre œil qui, presque aussi bien qu'un ordinateur, l'extrait d'images grises.

Jean-Paul DELAHAYE

La moindre des qualités que doit posséder un homme d'honneur consiste à garder un secret. La plus grande consiste à oublier ce secret.
Al-Muhallab (672-720)

La cryptographie moderne propose des méthodes nouvelles et parfois extraordinaires pour cacher de l'information, puis, au prix de quelques calculs, pour la retrouver. L'ordinateur y joue un rôle central : le plus souvent, il n'est pas envisageable de s'en passer, ni pour chiffrer ni pour déchiffrer le message caché.

Il existe cependant une famille de procédés où l'ordinateur n'est pas obligatoire pour le déchiffrement. L'œil humain, associé à la puissance de calcul du système visuel de notre cerveau, sait opérer le calcul qui extrait un message clair de données aléatoires, et réussit l'opération avec une surprenante efficacité.

La « cryptographie visuelle » est le domaine spécialisé de la cryptographie qui s'occupe de développer et de perfectionner ce type de méthodes, nées en 1994 d'un travail de Moni Naor et Adi Shamir (le *S* du système de cryptage RSA).

La méthode de cryptographie visuelle de base est fondée sur le principe du « masque jetable ». Nous partons d'une image M (le masque) dont les pixels, uniquement noirs ou blancs, ont été tirés au hasard, et d'une image S de même taille, elle aussi composée uniquement de pixels noirs ou blancs, mais qui représentent le secret. L'image S, qu'on souhaite cacher et faire parvenir à un correspondant, peut être un dessin, une photo ou un texte, l'essentiel étant qu'elle soit de la même taille exactement que M et qu'elle ne comporte que des pixels noirs ou blancs.

Combiner le masque et le secret

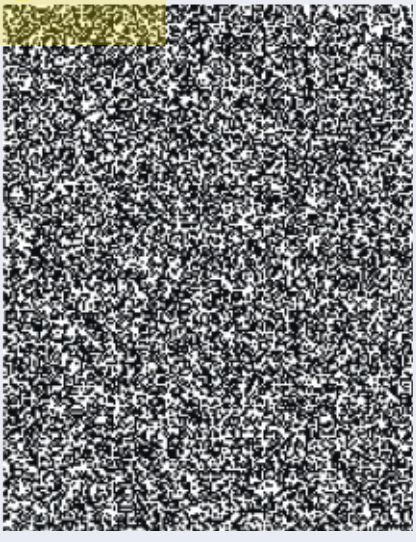
À l'aide d'un logiciel de dessin ou d'un programme, on opère le « ou exclusif » (en informatique, on le note XOR) entre les pixels de M et ceux de S. Cela donne une image chiffrée C. En clair : pour chaque emplacement

1. La méthode du masque jetable

Les pixels du masque M *(a)* sont choisis aléatoirement, noir ou blanc. L'image secrète est S *(b)*. L'image chiffrée C *(c)*, de même taille que M, est calculée informatiquement en opérant un « ou exclusif », noté XOR, entre M et S : un pixel de C est blanc si les pixels de S et de M sont tous les deux blancs ou tous les deux noirs, sinon il est noir. L'image chiffrée C semble aléatoire, comme M.

La superposition d'un transparent sur lequel est imprimé M et d'un transparent sur lequel est imprimé C fait apparaître l'image secrète S plongée dans du « gris » *(d)*. L'œil a extrait l'information secrète. Cette superposition (M OU C) correspond à l'opération logique OU entre les deux images. Si l'on dispose de versions informatiques de M et de S, on peut opérer le OU EXCLUSIF (XOR) entre M et C, ce qui redonne parfaitement l'image secrète S *(e)*. Les lecteurs souhaitant disposer des images ci-contre sous forme de fichiers informatiques les trouveront en : http://www2.lifl.fr/~delahaye/PLS416.

a MASQUE : M



b IMAGE SECRÈTE : S

de pixel, si le pixel de M est le même que celui de S, on dessine sur C un pixel blanc, sinon on dessine un pixel noir. Le message chiffré C résulte ainsi d'un XOR entre le masque M et le secret S, c'est-à-dire C = M XOR S.

Après avoir créé les images M et C, si vous imprimez M et C sur des transparents, vous constaterez que la superposition de M et de C fait apparaître S. Si vous disposez d'un ordinateur, vous verrez encore mieux l'image S en opérant un XOR entre M et C *(voir l'encadré 1)*.

Voici maintenant comment utiliser ce procédé pour faire circuler des informations secrètes et les envoyer à quelqu'un ne disposant pas d'ordinateur, cela d'une manière parfaitement sûre.

Alain souhaite envoyer des messages secrets à Béatrice. Ils se rencontrent une première fois et produisent une série d'images aléatoires, les masques M_1, M_2, ..., M_n, dont ils gardent chacun une copie et que bien sûr personne d'autre ne devra connaître. Ils peuvent aussi convenir de ces masques secrets en les faisant circuler sur le réseau : Alain les crée et les envoie à Béatrice, ou l'inverse. Cependant, si on utilise le réseau, il faut être certain au moment de l'échange des images M_1, M_2, ..., M_n que personne d'autre n'en prend connaissance. C'est possible en utilisant un canal de communication protégé, ou en utilisant un procédé cryptographique tel que le RSA qui permet sans risque ce type de partages à distance.

Alain n'est pas prêt à noircir à la main pixel par pixel l'image chiffrée C ! Aussi dispose-t-il des masques sous la forme de fichiers informatiques et il utilise un ordinateur pour produire les images chiffrées C. Béatrice, elle, n'aura besoin de rien d'autre que ses yeux pour le déchiffrage. L'opération de partage des masques réalisée, Alain et Béatrice vont échanger des secrets en parfaite sécurité par la poste ou en utilisant des émissaires, même si ceux-ci peuvent être douteux.

Un masque à usage unique

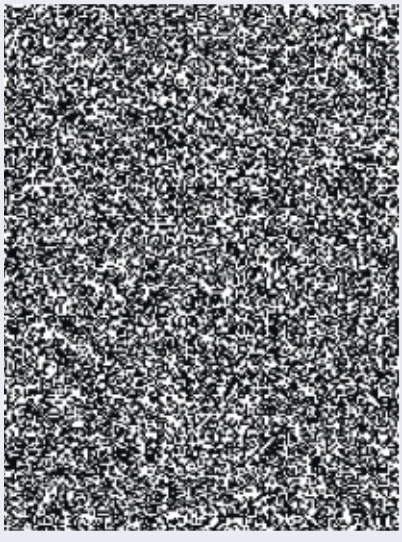
Lorsque Alain souhaite communiquer à Béatrice une image secrète S, il choisit l'un des masques M_i dont il dispose ; il utilise son ordinateur pour calculer l'image $C = M_i$ XOR S qu'il poste ou fait remettre sous la forme d'un transparent à Béatrice en lui indiquant le numéro *i* du masque utilisé. Ce numéro *i* peut être inscrit sans risque sur le transparent, car celui qui ne dispose pas des transparents M_1, M_2, ..., M_n ne peut rien faire de l'information *i*, pas plus qu'il ne peut tirer quoi que ce soit du transparent C. Alain peut aussi transmettre l'image chiffrée C en utilisant le réseau et demander à Béatrice d'imprimer le transparent C quand elle reçoit le fichier numérique.

Pour que Béatrice prenne connaissance de l'image secrète, elle superpose le transparent reçu C et le transparent du masque M_i dont elle dispose. Alain et Béatrice jetteront le masque M_i qu'il ne faudra plus jamais utiliser.

Pour que la méthode résiste aux attaques d'espions, il est essentiel que les images des masques M_1, M_2, ..., M_n soient aussi aléatoires que possible : il faut les produire avec de bons procédés de génération de suites aléatoires et ne surtout pas prendre pour masques des images représentant quelque chose. De plus, il ne faut jamais réutiliser un masque M_i : si vous le faites, plus aucune garantie de confidentialité ne pourra être assurée *(voir l'encadré 2)*.

En respectant cette double consigne de sécurité, le procédé est sûr, car ce système cryptographique est équivalent à la méthode du masque jetable (aussi dénommé *one-time pad* ou code de Vernam), dont

c IMAGE CHIFFRÉE : C = M XOR S



d IMAGE DÉVOILÉE : M OU C

e IMAGE RECONSTITUÉE : M XOR C