

une technique de transmission multiporteuse mise au point au CCETT : l'unique onde électromagnétique porteuse est remplacée par plusieurs milliers d'ondes porteuses, portées par des fréquences proches, simultanément transmises. Dans cette transmission parallèle de plusieurs milliers d'ondes porteuses, chaque porteuse transporte moins d'un millième du débit total et peut donc être modulée 1 000 fois plus lentement que si elle était seule. La durée pendant laquelle on transmet un point de la constellation étant égale à quelques centaines de microsecondes au lieu de quelques centaines de nanosecondes pour la modulation monoporteuse classique, on élimine les interférences entre deux émissions successives en les espaçant d'une courte durée destinée à absorber les échos.

Cette transmission multiporteuse résout un autre problème de la diffu-

sion hertzienne terrestre. La portée d'un émetteur de télévision est de l'ordre de quelques dizaines de kilomètres. Lorsqu'une antenne de réception capte les signaux de deux émetteurs, elle reçoit d'abord le signal émis par l'émetteur le plus proche, et un peu après, le signal émis par l'émetteur le plus éloigné. Ce second signal est identique au premier, mais décalé dans le temps, si bien qu'il est équivalent à un écho du premier signal. Pour éviter que deux émetteurs ne se brouillent mutuellement, on fait émettre les émetteurs voisins à des fréquences porteuses différentes (c'est également le cas pour la transmission radio analogique : lorsqu'on change de région, la fréquence des stations FM change). Les fréquences, si précieuses, sont ainsi gaspillées.

Comme la transmission multiporteuse est peu sensible aux échos, deux émetteurs voisins fonctionnant sur la

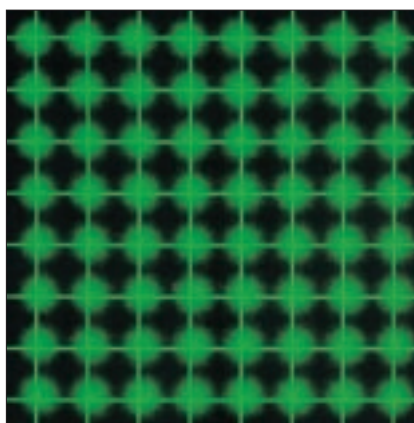
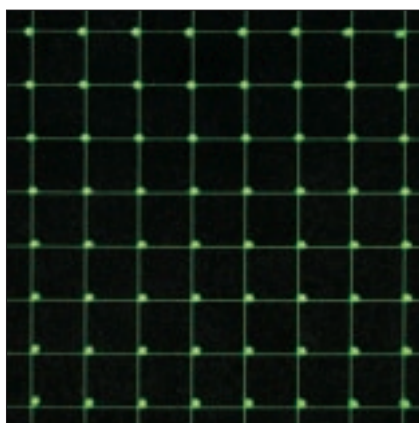
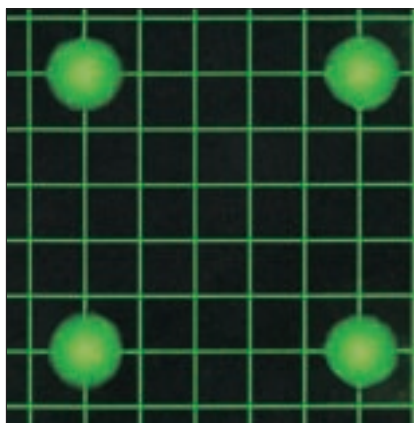
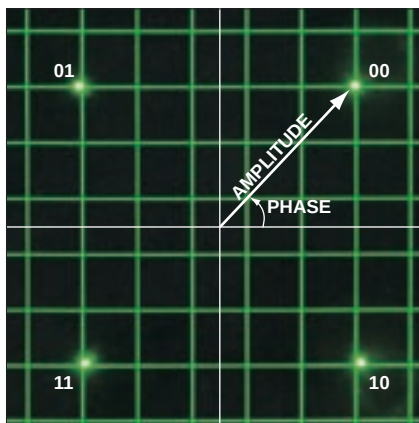
même fréquence ne se brouillent plus. Un grand territoire peut être couvert avec autant d'émetteurs que nécessaire, tous fonctionnant sur la même fréquence. On gagne ainsi un facteur dix dans l'utilisation de la bande passante. La modulation multiporteuse résiste également aux brouillages involontaires dus à une télévision analogique qui émettrait à proximité : si quelques porteuses numériques sont brouillées, la proportion de l'information perdue reste assez faible pour que le système correcteur d'erreurs la recouvre intégralement.

Malgré ces efforts, chaque canal de télévision terrestre, avec une largeur de 8 mégahertz, ne peut acheminer qu'un débit maximum de 35 mégabits par seconde, ce qui correspond, après correction des erreurs de transmission, à un débit utile de 25 mégabits par seconde. Ce débit reste bien inférieur aux 38 mégabits par seconde du câble ou du satellite : on transmet moins de programmes sur un canal de télévision terrestre que sur un canal du câble ou du satellite. En revanche, contrairement aux téléviseurs qui reçoivent les programmes par câble ou par satellite, les récepteurs terrestres seront librement déplacés tels les téléphones sans fil. On expérimente même des récepteurs à écran plat, alimentés par batterie, et installés à l'arrière des voitures ou dans les transports en commun.

Tous dans le tuyau

Que ce soit par satellite, par câble ou par diffusion terrestre, les canaux de transmission numérique ont conservé leur largeur en fréquence des temps analogiques. Or, grâce à la compression, la place nécessaire à un programme numérique de qualité identique à celle des programmes analogiques a diminué. La quarantaine de mégabits par seconde d'un canal de satellite ou d'un canal de réseau câblé est partagée entre plusieurs programmes. Ce nombre est compris entre deux et vingt selon que l'on y place des programmes en haute définition ou des programmes de qualité réduite (comme les émissions de téléachat).

Les suites de bits sont regroupées en paquets de plusieurs sortes : des paquets vidéo, audio, de sous-titres, de télétexte, de messages de contrôle d'accès, etc. Ces paquets ne sont pas tous indépendants et l'on doit conserver la synchronisation entre le son et l'image. Avant la transmission, les paquets des



4. LES DONNÉES NUMÉRIQUES qui sont transmises par les diffuseurs sont décomposées en séquences que l'on peut représenter par des points dans un quadrillage. À intervalles de temps réguliers, on module l'amplitude et la phase d'une onde porteuse afin de coder l'un des points de cette « constellation ». Pour la transmission par satellite, la constellation est composée de quatre points (*en haut, à gauche*). Les données sont ainsi transmises par séquences de deux bits. Sur le câble, on transmet un point parmi 64 (*en bas, à gauche*) à chaque période, soit six bits ($2^6=64$). Le parcours du signal sur de grandes distances introduit du bruit : le signal reçu (*à droite*) n'est pas constitué de points, mais de taches, qui, lorsqu'elles se recouvrent introduisent des erreurs dans la transmission. Ainsi, pour les satellites, on choisit une constellation à quatre états : les points sont éloignés et se recouvrent moins facilement que dans la constellation à 64 états.

différents composants sont rassemblés en un seul flot : les paquets qui correspondent aux images de *France 2* sont mélangés aux paquets audio de *France 2* (son stéréo, voire plusieurs sons pour un programme multilingue) et aux paquets de sous-titre, etc. Comme ces paquets peuvent être transmis par des moyens asynchrones, voire, dans certains cas, par des itinéraires différents, ils sont munis d'une étiquette qui indique leur rang par rapport aux autres. À la réception, les paquets sont classés selon l'ordre indiqué par les étiquettes et présentés à l'écran dans le bon ordre et au rythme indiqué. Ensuite, les flots des différentes chaînes sont rassemblés en un seul flot global (TF1, *France 2*, *France 3*, etc.).

Finalement, plusieurs de ces flots numériques globaux sont mélangés, soit entre eux, soit avec des signaux analogiques, à des fréquences différentes. Ils sont alors prêts pour la transmission sur le même réseau. On entend ici par «réseau» un ensemble de satellites, un réseau câblé ou un ensemble d'émetteurs terrestres (voir la figure 1).

Accès protégé

Comment limiter l'accès aux programmes payants ? Ce contrôle d'accès est effectué grâce à des suites de nombres totalement imprévisibles à qui-conque n'en connaît pas le principe de construction. Pour cette raison, ces suites sont nommées pseudo-aléatoires. Comment deviner, par exemple, que la suite 2 5 7 2 9 1 0 1 1 2 3 5 8 se poursuit par 3, si l'on ignore que chaque chiffre est le reste de la division par dix de la somme des deux chiffres précédents ? Quand on additionne une telle suite au flot numérique des images, lors de l'émission, on transmet une série de nombres qui, utilisés sans décryptage, engendrent une image incohérente. Des variantes de cette technique permettent de créer des images cryptées qui conservent quelque lisibilité malgré une très mauvaise qualité, afin de susciter l'envie de les obtenir en clair. Toutefois, seule la soustraction, dans un décrypteur associé au téléviseur, de la suite secrète de nombres aux données reçues cryptées recrée les images initiales.

L'appareil de décryptage retrouve la suite secrète s'il connaît les deux valeurs initiales (2 et 5, dans notre exemple) qui constituent la clé instantanée de décryptage. Cette clé est la même pour tous les récepteurs, mais elle diffère pour



5. LES ÉCHOS apparaissent, en transmission analogique, lorsqu'un récepteur capte le signal de deux émetteurs terrestres proches. Comme ces deux émetteurs ne sont pas à la même distance, les deux signaux reçus sont décalés, ce qui provoque les échos. En télévision numérique, le problème sera résolu par l'utilisation de la transmission multiporteuse.

chaque émission cryptée. Cette clé, dont la durée de vie ne dépasse pas quelques secondes, est transmise sous forme chiffrée dans un message spécial nommé ECM (*Entitlement Checking Message*, soit «message de contrôle du cryptage»), qui contient aussi les références de l'émission (il s'agit, par exemple, de la retransmission d'un match de football). L'appareil de décryptage s'assure d'abord que le message ECM qu'il reçoit n'a pas été falsifié en vérifiant sa signature électronique ; les algorithmes d'authentification des ECM reçus sont secrets. Lorsque la carte à puce introduite dans le récepteur confirme que l'abonnement «football» a bien été payé, la clé instantanée est déchiffrée, et l'image reçue est décryptée. Sinon, le décrypteur refusera de calculer la clé, mais proposera l'achat du match si un crédit suffisant figure sur la carte à puce.

Le flot des ECM est permanent pour autoriser un décryptage rapide en cas de changement de chaîne. Comment les abonnements mémorisés par la carte à puce sont-ils mis à jour ? Grâce à un autre message, l'EMM (*Entitlement Management Message*, soit «message de gestion du cryptage»), également protégé du piratage par signature électronique. Cette fois, les EMM sont particuliers à chaque usager, c'est-à-dire à chaque carte à puce. Ils permettront de faire évoluer à distance les droits de cet usager. Les systèmes concurrents diffèrent par leurs

méthodes – jalousement gardées secrètes – de chiffrement des clés et d'authentification des messages EMM ou ECM reçus. En raison de ces différences, les appareils de décryptage des systèmes concurrents sont différents.

Voilà presque 60 ans, les premières émissions expérimentales diffusées de la tour Eiffel montraient la faisabilité d'une technique – la télévision – dont les répercussions sociales étaient alors inimaginables. Sommes-nous aujourd'hui, avec la télévision numérique, à la veille d'un bouleversement du même type ? Sans doute pas : nous n'avons franchi qu'un pas vers la révolution numérique, qui mariera de façon indissociable séquences vraies et images de synthèse. La révolution numérique se borne pour l'instant à élargir le choix du kiosque audiovisuel : limité hier à quelques quotidiens généralistes, il proposera désormais plusieurs dizaines ou centaines de revues spécialisées sur papier glacé.

Jean-Pierre HÉNOT, Vincent MICHON et Bertrand SUEUR ont travaillé, à Rennes, au Centre commun d'études de télédiffusion et télécommunication (CCETT) du groupe *France Télécom*.

Nicholas NEGROPONTE, *L'homme numérique*, Éditions Robert Laffont, 1995.

Hervé BENOÎT, *La télévision numérique*, Éditions Dunod, 1998.