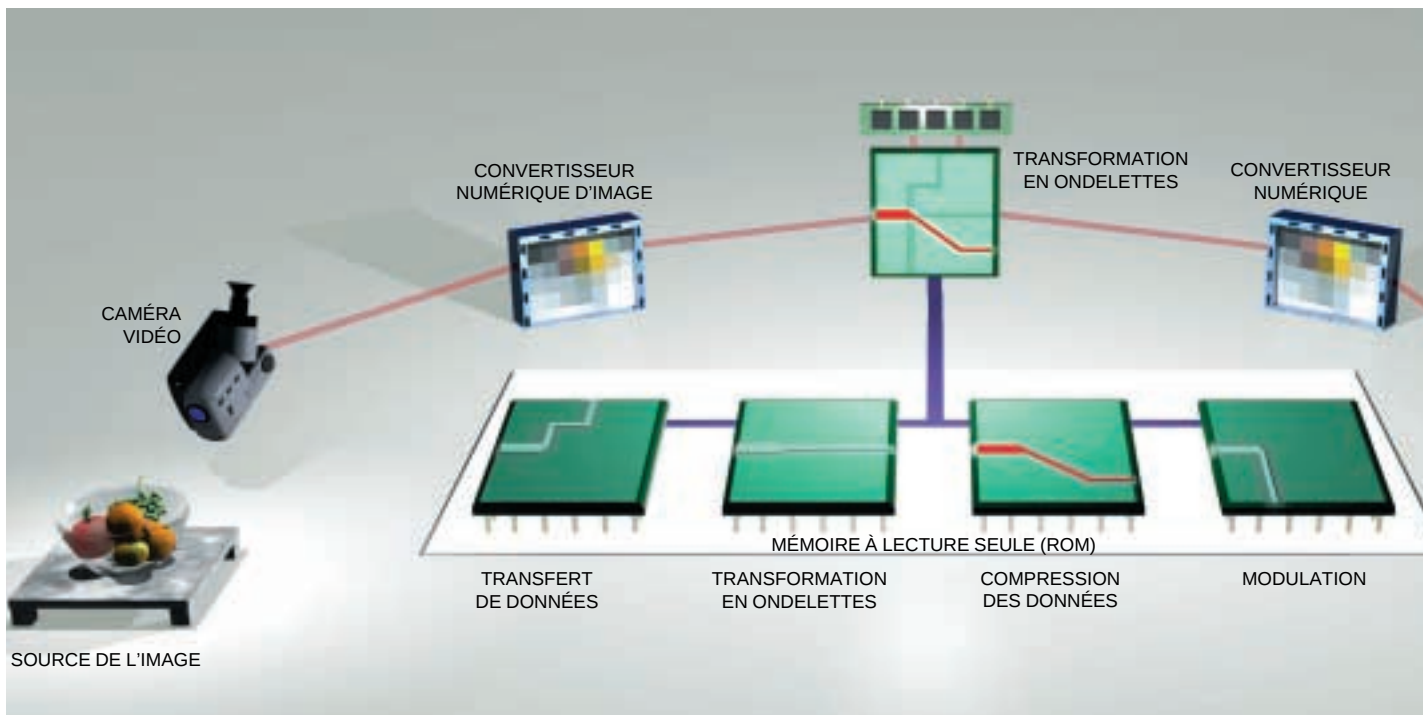




5. CE SYSTÈME PROTOTYPE de communication vidéo utilise un unique circuit configurable pour exécuter quatre fonctions qui sont normalement effectuées par des puces distinctes. Une puce mémoire conserve les quatre configurations utiles et les charge successivement dans le processeur configurable. Une première configuration permet d'abord au processeur adaptable d'acquérir des données

vidéo numériques. Puis la puce est rapidement configurée pour mettre l'information vidéo sous une forme comprimée, et modifiée encore pour préparer la transmission. Enfin, les circuits reçoivent la dernière configuration, qui leur permet de moduler et de transmettre l'information vidéo. Dans le récepteur, les quatre configurations sont appliquées dans l'ordre inverse de celui de

Calcul en temps réel

Le concept de système configurable est né simultanément aux États-Unis et en Europe, dès l'introduction des circuits logiques configurables par la Société *Xilinx*, en 1986. Le premier système couplant un microprocesseur à des circuits reconfigurables a été conçu à l'INRIA (Institut national de recherches en informatique et en automatique) en 1987.

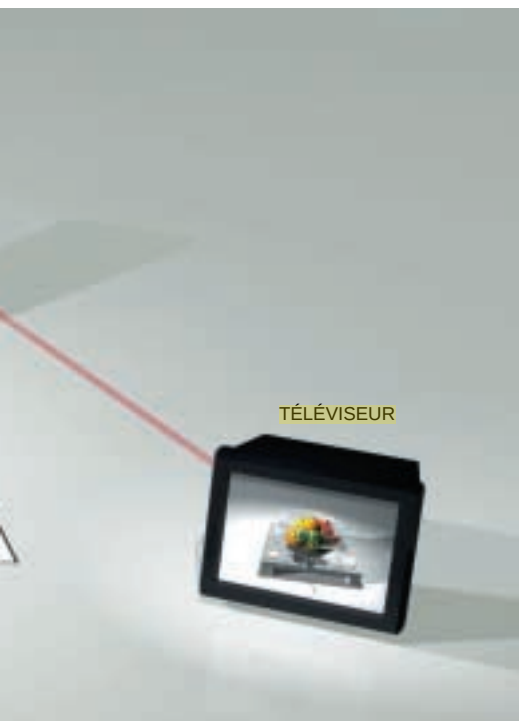
Parallèlement, des architectures similaires ont été mises en œuvre dans les « émulateurs » de logique (*QuickTurn* dès 1987, *Hewlett-Packard* plus récemment). Ceux-ci utilisent de très grandes quantités de circuits configurables (plusieurs centaines) pour simuler des circuits intégrés avant leur fabrication. Ces émulateurs de logique, devenus indispensables pour la conception des microprocesseurs modernes, n'ont cependant qu'une seule fonction : simuler de très grands circuits. En revanche, les systèmes reconfigurables proprement dits ont des fonctions aussi diverses que celles du microprocesseur, auquel ils ajoutent des fonctions spécifiques. On a ainsi le meilleur de deux mondes : universalité du logiciel et performances du matériel spécifique à chaque application.

Le système reconfigurable *DECPeRLe1*, réalisé en 1992 au Laboratoire de recherche de la Société *Digital Equipment*, à Paris, pour le prix et le volume d'une station de travail de l'époque, détient encore aujourd'hui sept records absolus de vitesse — toutes techniques confondues, du super ordinateur au circuit intégré sur mesure. Ce système

est le plus performant pour le codage et le décodage par la méthode de chiffrement à clés publiques RSA. Le même système reste le seul à répondre aux besoins d'acquisition et de filtrage de données en temps réel exprimés par le CERN pour son futur accélérateur de particules (LHC). Des performances de calcul en temps réel équivalentes à celles de ce système configurable s'obtiendraient avec un ordinateur classique au prix d'une multiplication par 100 des fréquences d'horloge les plus élevées.

Par leur souplesse et le nombre de connexions potentielles (on peut faire sortir directement des centaines de fils de ces circuits), les systèmes reconfigurables sont d'excellentes interfaces entre les ordinateurs et des dispositifs externes variés. Dans le cas d'une caméra numérique à haute résolution, telle celles de l'astronomie ou de l'imagerie médicale, on y programme à la fois l'interface, le protocole de communication, et aussi les fonctions de filtrage de l'image et l'adaptation du débit des données reçues par l'ordinateur hôte. On obtient ainsi un système d'acquisition optimal, qui peut s'adapter aux évolutions des caméras ou aux besoins d'acquisition par simple reconfiguration. C'est à travers des applications de ce type que les systèmes reconfigurables sont aujourd'hui passés du stade de la recherche à celui de produits industriels.

Jean VUILLEMIN, École normale supérieure
Patrice BERTIN, École des mines de Paris



Bryan Christie

départ. Ainsi le circuit démodule les données, décompresse l'image, puis l'envoie à un convertisseur numérique-analogique afin d'afficher l'image sur un écran. Notre système est capable de traiter huit images par seconde.

de 16 sous-clés. Lors de la seconde étape, chaque sous-clé traite ensuite les données séparément : l'ensemble des 16 sous-clés chiffre ou déchiffre chaque bloc de 64 bits. Lorsqu'un ordinateur est simultanément utilisé par plusieurs personnes, chaque paire d'utilisateurs utilise une clé distincte, et le système de chiffrement doit changer de clé chaque fois que des parties de messages arrivent des différents utilisateurs.

Toutefois, la clé cryptographique reste constante pendant qu'un long bloc de données transite sur le réseau. Par exemple, si deux personnes communiquent à travers un réseau protégé, ils échangent une seule fois une clé cryptographique protégée, puis utilisent cette clé tout au long de leur dialogue afin d'engendrer les sous-clés pour chaque session de chiffrement ou déchiffrement.

Avec une puce configurable, le logiciel calcule les valeurs des sous-clés une fois pour toutes, et le circuit de traitement de données peut être optimisé pour ces sous-clés spécifiques. Ainsi peut-on éviter de consacrer une partie de la puce au calcul des sous-clés. Ces économies nous ont permis d'installer l'algorithme DES sur un circuit adaptable comprenant 13 000 portes logiques au lieu des 25 000 portes nécessaires

avec des circuits classiques. Lorsque la clé de chiffrement doit être changée, l'utilisateur peut rapidement calculer la configuration nécessaire pour la nouvelle sous-clé, puis reconfigurer la puce pour la suite du calcul.

Les prototypes que nous avons mis au point pour l'identification de cibles et le chiffrement démontrent que les circuits configurables conduisent à des ordinateurs puissants. De nombreuses autres applications, tels les communications numériques, le traitement des données radar et la conception assistée par ordinateur, tireraient parti de telles puces.

Le futur de l'informatique configurable

L'informatique configurable est un domaine très jeune : bien que Gerald Estrin, de l'Université de Los Angeles, en ait établi les principes dès la fin des années 1960, les premiers essais datent de quelques années seulement. De plus, les circuits configurables actuels, avec au mieux 100 000 portes logiques, n'exploitent pas toutes les possibilités de cette technique. Les futurs circuits seront bien plus grands : comme pour la plupart des circuits intégrés classiques, le nombre d'éléments intégrés sur un circuit adaptable double tous les 18 mois environ. Ainsi, avant la fin de cette décennie, les circuits adaptables comprendront probablement un million d'éléments logiques.

Les chercheurs et les industriels résolvent aujourd'hui les problèmes de conception qui ont retardé l'adoption de l'informatique configurable. Les circuits configurables actuels ne sont utilisables qu'avec des algorithmes opérant sur les bits individuels, tels que la comparaison de formes et l'arithmétique des nombres entiers, mais ils sont mal adaptés aux opérations numériques telles que la multiplication de haute précision ou les calculs en virgule flottante. Des circuits multiplicateurs spécialisés, comme ceux utilisés dans les microprocesseurs et dans les processeurs de traitement numérique du signal (DSP), peuvent être optimisés pour fonctionner plus efficacement que les circuits multiplicateurs réalisés à partir de logique configurable. De surcroît, la mémoire intégrée des circuits configurables, nécessaire pour le stockage des résultats intermédiaires, reste trop faible. Ainsi, de nombreux programmes nécessitent une impor-

tante mémoire externe pour fonctionner avec des circuits modifiables : le transfert des données entre le circuit et la mémoire ralentit les calculs et consomme plus d'énergie (la consommation d'énergie est gênante, parce qu'elle s'accompagne d'une dissipation de chaleur nuisible au bon fonctionnement des circuits).

Pour éviter ces écueils, les électroniciens et les informaticiens mettent au point les premiers circuits configurables à mémoire intégrée. À l'Institut de technologie du Massachusetts, André DeHon et Thomas Knight ont proposé un circuit qui stocke les données des multiples configurations dans une mémoire intégrée. En un seul cycle d'horloge, soit quelques dizaines ou centaines de nanosecondes, la puce bascule d'une configuration à une autre, sans effacer les données partiellement traitées.

Parallèlement, Brad Hutchings, de l'Université Brigham Young, a utilisé l'informatique configurable pour construire un ordinateur à jeu d'instruction dynamique. Ce système, qui allie un microprocesseur classique et un coprocesseur configurable, démontre le potentiel de la reconfiguration automatique utilisant des configurations mémorisées. Lors de l'exécution du programme, le circuit demande une reconfiguration chaque fois qu'il détecte l'absence d'un circuit spécifique nécessaire au calcul. On peut ainsi créer et mémoriser un grand nombre de configurations de circuit, et les activer de la même façon qu'un programmeur appelle un sous-programme.

Le groupe *Colt*, dirigé par Peter Athanas, de l'Institut polytechnique de Virginie, étudie une technique de reconfiguration durant l'exécution nommée *Wormhole* («trou de ver»), qui

se prête à l'informatique répartie. Un flot de données crée une logique dédiée à mesure qu'il traverse les circuits configurables.

John Wawrzynek et ses collègues de l'Université de Berkeley étudient des systèmes qui combinent un microprocesseur et un processeur configurable. À partir d'un programme ordinaire, un logiciel de compilation spécial engendre une combinaison d'instructions-machine et de configurations du processeur configurable qui accélèrent l'exécution du programme.

Les processeurs configurables ne remplaceront jamais les microprocesseurs pour les tâches généralistes, mais les circuits à configurations variables joueront certainement un rôle croissant dans la mise au point de systèmes informatiques performants. La puissance de calcul des processeurs configurables en fait des systèmes de choix chaque fois qu'une adaptation rapide aux données est requise.

Progressivement, la frontière entre processeurs programmables et processeurs configurables s'estompera : les circuits configurables comprendront une mémoire interne augmentée et des multiplicateurs spécialisés, comme les microprocesseurs classiques ; inversement, les microprocesseurs de la prochaine génération pourront modifier dynamiquement certaines parties de leur circuit, un peu comme les processeurs configurables. De la même manière que les ordinateurs reliés au réseau Internet peuvent télécharger des logiciels spécialisés pour effectuer des tâches particulières, les futures machines pourront charger de nouvelles configurations de circuits. Dans dix ans, les ordinateurs comprendront un mélange de puces programmables et de puces configurables.

John VILLASENOR et William MANGIONE-SMITH travaillent au Département d'ingénierie électrique de l'Université de Los Angeles.

M.J. WIRTHLIN et B.L. HUTCHINGS, *A Dynamic Instruction Set Computer*, in *Proceedings of the IEEE Symposium on FPGAs for Custom Computing Machine*, avril 1995, IEEE Computer Society Press, 1995.

J. VUILLEMIN, P. BERTIN, D. RONCIN, M. SHAND, H. TOUATI et P. BOUCARD, *Programmable Active Memories : The Coming of Age*, in *IEEE Trans. on VLSI*, vol. 4, pp. 56-69, mars 1996.

John VILLASENOR, Brian SCHONER, Kang-Ngee CHIA, Charles ZAPATA, Hea Joung KIM, Chris JONES, Shane LANSING et Bill MANGIONE-SMITH, *Configurable Computing Solutions for Automatic Target Recognition*, in *4th IEEE Symposium on FPGAs for Custom Computing Machines (FCCM '96)* April 1996.

Ray BITTNER et Peter ATHANAS, *Wormhole Run-Time Reconfiguration*, in *FPGA '97 : ACM/SIGDA International Symposium on Field Programmable Gate Arrays*, Special Interest Group on Design Automation (SIGDA), ACM, 1997.
