Version abrégée

CONFINÉS dans le prototypage de systèmes numériques il y a encore quelques années, les FPGA (*Field Programmable Gate Array*) concurrencent aujourd'hui les circuits ASIC (*Application-Specific Integrated Circuits*) dans certaines applications. Les nouvelles familles de FPGA disposent par exemple de cellules logiques destinées à l'optimisation d'opérateurs arithmétiques ou de mémoires synchrones facilitant le calcul par tables. Les FPGA s'avèrent en outre moins onéreux que l'ASIC pour de petites séries et bénéficient des meilleures technologies de gravure. La conception de systèmes performants nécessite néanmoins une exploitation judicieuse des ressources d'un FPGA.

Nous illustrons cette problématique en étudiant quelques coprocesseurs destinés aux algorithmes de cryptage RC6 et IDEA. La principale difficulté de RC6 consiste à calculer la fonction $f(X) = (X \cdot (2X + 1)) \bmod 2^w$, où X est un nombre entier positif de w bits. Nous proposons un opérateur évaluant efficacement $f(X)$ en exploitant les spécificités architecturales de la famille Virtex de Xilinx. Pour un opérande de 32 bits, notre circuit se révèle 55 % plus compact et 18 % plus rapide que celui proposé par la NSA. CryptoBooster, notre premier prototype proposé pour IDEA, offre un débit de 102 Mbits/s sur un circuit XCV1000-4 de la famille Virtex. L'exploitation du jeu d'instructions multimédias d'Itanium, le nouveau processeur d'Intel et Hewlett Packard, permet toutefois l'obtention de meilleures performances. Cette constatation a motivé une étude plus détaillée des aspects arithmétiques de l'algorithme de cryptage. Le débit de CryptoBooster II, le système résultant de ce travail, s'avère supérieur à 3 Gbits/s sur le même FPGA. Toutes les opérations arithmétiques d'IDEA s'effectuant chiffre de poids faible en tête (mode *LSDF* ou *Least Significant Digit First*), la conception d'une unité de calcul sérielle consiste à interconnecter les opérateurs en prenant soin de les synchroniser correctement. Le système obtenu, baptisé CryptoBooster III, constitue un *pipeline* au niveau du chiffre.

Si un système sériel requiert également des opérations débutant par le chiffre de poids fort (mode *MSDF* ou *Most Significant Digit First*), telles la division ou la racine carrée, l'insertion de registres mémorisant les résultats entre deux circuits travaillant dans un mode différent est indispensable. Ces contraintes réduisent le débit du système tout en compliquant son contrôle. Une représentation redondante des nombres permet la suppression de la propagation de retenue survenant lors de l'addition et, par conséquent, l'évaluation sérielle de n'importe quelle fonction chiffre de poids fort en tête. Cette philosophie de calcul, appelée arithmétique en-ligne, se révèle très efficace

pour des applications de contrôle embarqué, l'analyse de séquences génétiques ou les réseaux de neurones artificiels.

M. Ercegovac, le père de l'arithmétique en-ligne, a défini des méthodes de conception d'opérateurs en-ligne destinés aux fonctions arithmétiques et algébriques. Nous proposons une nouvelle approche de calcul en-ligne de certaines fonctions élémentaires ($\sin(x)$, $\cos(x)$, e^x, ...) exploitant des lectures de tables et des évaluations de polynômes. Nous décrivons finalement la bibliothèque VHDL d'arithmétique en-ligne réalisée grâce à ces outils.