HUBERT COMON-LUNDH

LA CRYPTOGRAPHIE EN MOUVEMENT

La passion pour les casse-tête mathématiques semble venir des tréfonds de son enfance. « J'ai toujours aimé les problèmes exprimés assez simplement mais dont la solution n'est ni évidente, ni forcément simple. Et c'est souvent cette forme que revêtent les problèmes de recherche en informatique. » Mais avant de s'y frotter, ce fils d'ingénieur choisit, au sortir d'une agrégation de mathématiques, d'enseigner les vertus de cette discipline… durant quatre ans. « Il est important de bouger régulièrement ! »

Fort de cet adage, Hubert Comon plaque alors le monde lycéen pour « entrer » en recherche. Direction l'Institut national Polytechnique de Grenoble, pour une thèse d'informatique. C'est à l'occasion d'un séminaire que le thésard rencontre, en 1986, son « maître » Jean-Pierre Jouannaud. À quatre mains, ils publient des articles sur la réécriture comme outil de démonstration automatique[1] : cela consiste *grosso modo* à remplacer des expressions arithmétiques par des expressions toujours arithmétiques mais plus simples.

SON OBJECTIF : DÉVELOPPER LA « VÉRIFICATION » POUR ACCROÎTRE LA CONFIANCE DANS LES LOGICIELS ET MATÉRIELS INFORMATIQUES.

À partir de là, tout s'enchaîne. Hubert Comon entre en 1989 au CNRS, par les portes du Laboratoire de recherche en informatique (LRI), à Orsay. Cinq ans plus tard, le voici directeur de recherche, ayant entre-temps récolté une médaille de bronze du CNRS. S'installer dans son poste ? Jamais. L'occasion de changer lui sera donnée *via* l'École normale supérieure de Cachan : il s'agit d'y créer, avec quelques collègues, un laboratoire d'informatique associé au CNRS.

À évoquer ce projet « vraiment exaltant », son visage s'éclaire d'un large sourire. Le Laboratoire Spécification et Vérification (LSV) est inauguré en septembre 1996. « Je pense, explique-t-il, que c'est le meilleur endroit au monde pour faire de la recherche en informatique, grâce à un mode de fonctionnement unique et une grande homogénéité scientifique. » Fort d'une quarantaine de personnes, le lieu a en effet de quoi séduire sur le plan collectif – les tâches et les décisions sont partagées par l'ensemble du laboratoire, chacun suivant attentivement les travaux de tous les autres – autant que sur le plan scientifique.

L'idée de départ : réunir des compétences en démonstration automatique, en théorie des automates et systèmes distribués et en spécification. Objectif : développer ainsi la « vérification », domaine de pointe qui sert à accroître notre confiance dans les logiciels et matériels informatiques. « Il comporte un enjeu économique et sociétal énorme puisque tout le monde est confronté un jour ou l'autre aux bugs mais aussi, à une autre échelle, aux erreurs logicielles ou matérielles susceptibles d'entraîner des catastrophes aéronautiques – pensez à l'explosion d'Ariane 5 –, des pertes financières gigantesques ou encore des fraudes comme dans le cadre du vote électronique ! » À la clé, des collaborations avec les industriels pour lesquelles Hubert Comon déploie beaucoup d'énergie… Sans toujours y trouver son compte de temps pour formaliser et développer de nouvelles techniques.

En 2000, l'appel du large se fait à nouveau sentir. Ce sera Stanford, et l'occasion de réorienter ses thèmes de recherche vers la sécurité des protocoles cryptographiques. Ces petits programmes – exécutés sur des machines distantes et communiquant entre eux, à l'instar d'un téléphone et d'un central téléphonique – utilisent des primitives cryptographiques, par exemple le chiffrement[2]. Même incassable, ce dernier peut faire l'objet d'attaques ciblées sur des failles de conception. « Notre rôle consiste à rechercher systématiquement de telles fraudes, ou plus rarement, à prouver leur absence. »

IL PART AU JAPON METTRE AU POINT UN PROGRAMME DE RECHERCHE SUR LES PROTOCOLES CRYPTOGRAPHIQUES.

2001. Hubert Comon choisit de quitter le CNRS pour rejoindre l'équipe enseignante de l'ENS de Cachan. Coup de tête ? « Pas du tout. Ce fut une décision mûrement réfléchie : recevoir le salaire d'un chercheur sans être assez utile à la société ne me convenait plus. De mon point de vue, il me semblait plus efficace de valoriser nos recherches par l'enseignement. » Cela sans abandonner vraiment ses travaux.

Le « démon » de la recherche va le reprendre en 2007. Ayant obtenu un congé sabbatique d'un an puis une délégation à l'Institut national de recherche en informatique et en automatique (INRIA), notre lauréat part au Japon mettre au point un programme

SCIENCES ET TECHNOLOGIES DE L'INFORMATION ET DE L'INGÉNIERIE (ST2I)
LABORATOIRE SPÉCIFICATION ET VÉRIFICATION (LSV)
CNRS / ÉCOLE NORMALE SUPÉRIEURE DE CACHAN
CACHAN
http://www.lsv.ens-cachan.fr/

de recherche sur les protocoles cryptographiques. Pourquoi le pays du Soleil Levant ? Certes pour baigner dans un environnement scientifique réputé. Mais aussi « par curiosité et goût personnel. Car ce pays a une culture et des paysages merveilleux ».
On l'aura compris, Hubert Comon reste, à 50 ans, un insatiable curieux.

[1] L'objectif de la démonstration automatique est de faire rechercher (et trouver) des preuves mathématiques par l'ordinateur.
[2] Opération par laquelle une donnée intelligible est rendue inintelligible afin d'en protéger la confidentialité.