DAILY SCIENCE
DÉCOUVREZ LA SCIENCE, LA RECHERCHE ET L'INNOVATION "MADE IN BELGIUM"

FRANÇOIS-XAVIER STANDAERT REND LA CRYPTOGRAPHIE LUMINEUSE

Publié le 8 août 2017

SERIE (2/5) « Les maths? C'est passionnant! »

B125. D'emblée, lettres et chiffres s'accordent dans les couloirs au charme désuet du département des mathématiques de l'UCL, à Louvain-la-Neuve. François-Xavier Standaert, 39 ans, y explique volontiers, et avec une infinie clarté, son domaine d'action. Ce Chercheur qualifié FNRS, professeur à l'école polytechnique de Louvain est membre de l'Institut de recherche ICTEAM (information, communication technologies, electronics and applied mathematics).
« *Je fais des recherches en cryptographie*, explique François-Xavier Standaert. *Il s'agit de la science qui étudie la sécurité de l'information. Plus précisément, je m'intéresse aux failles de sécurité qui peuvent apparaître lorsqu'on passe de la description mathématique d'une méthode de chiffrement (ou de signature) - ce qu'on appelle des algorithmes - à leur mise en œuvre concrète, dans une carte à puce (ou un téléphone portable, un ordinateur). L'exemple le plus connu est le cas des attaques dites « par canaux cachés », dans lesquelles un adversaire effectue une mesure de consommation (càd une sorte d'électroencéphalogramme) de la carte à puce pour en extraire des informations secrètes.* »
La question de la transparence

Cette faille de sécurité étant de nature physique, s'en prémunir nécessite de modéliser - à savoir représenter toutes sortes de situations, objets, structures du monde réel - le comportement des objets mettant en œuvre les algorithmes. Ce type de question mène à des réflexions plus générales sur la nécessité de comprendre le fonctionnement des systèmes électroniques pour quantifier leurs risques, et donc l'intérêt de travailler avec des systèmes les plus ouverts possible (par exemple en rendant publics leurs détails de conception). Ce problème de la transparence dans les systèmes d'information se retrouve en fait dans beaucoup d'applications liées à la sécurité, mais aussi à la vie privée (par exemple dans les applications « big data » – dont la modélisation est également complexe).

Liberté, interdisciplinarité

A t-il toujours aimé les maths ? « *Oui mais c'était loin d'être exclusif.* » Comme pas mal de mathématiciens de haut vol, le Professeur Standaert était aussi très attiré vers les matières littéraires même s'il a finalement opté pour des études d'ingénieur électronique qui lui permettaient de combiner son intérêt pour les maths et la physique. En revanche, du monde de la recherche il n'avait aucune idée avant son TFE (travail de fin d'études) et c'est par hasard (et par chance précise-t-il) qu'il choisit alors son orientation de recherche.

« *J'aurais sûrement pu être intéressé par d'autres sujets ; je pense que l'activité de recherche et la liberté qu'elle permet me plaisent en soi. Je suis ravi d'être tombé sur la cryptographie, car c'est un thème de recherche qui permet l'interdisciplinarité (mathématiques, physique), mélange théorie et pratique, et dont les applications posent des questions sociétales et philosophiques qui me semblent importantes.* »

Son TFE était déjà lié à des questions de mise-en-œuvre d'algorithmes cryptographiques dans des circuits électroniques.

« *J'ai eu l'occasion d'approfondir ce travail, poursuit-il, dans le cadre d'une thèse de doctorat – toujours à l'UCL, sous la supervision du Professeur Jean-Jacques Quisquater. Initialement plutôt orienté vers des questions très concrètes (mon projet de thèse était lié à la compression et à la sécurisation d'images pour le cinéma numérique), je me suis progressivement intéressé à des problèmes plus abstraits.* »

A la fin de sa thèse, le jeune ingénieur part en post-doc à Columbia University et au MIT Medialab, où il rencontre d'excellents mathématiciens. Il y travaille notamment sur la formalisation des attaques par canaux cachés.

« *A cette époque, le sujet était un peu la chasse gardée des électroniciens confie François-Xavier Standaert. Au cours de ce post-doc j'ai réalisé que résoudre ce problème nécessiterait à la fois de bonnes hypothèses physiques (sur lesquelles travaillaient les électroniciens) et une « amplification mathématique » de la sécurité (spécialité des cryptographes). Mes projets de recherche depuis 10 ans (FNRS, ERC) sont tous liés à cette conviction.* »

Un modèle forcément imparfait

Ancré donc dans l'interaction entre mathématiques et modèles physiques, le Professeur Standaert travaille sur la théorie de l'information. Le principe est de quantifier l'information (d'un symbole, d'un mot, d'un système) à partir d'une probabilité d'apparition (intuitivement, un évènement est plus informatif s'il est surprenant).

« *Dans le cadre des « attaques physiques* , explique-t-il, *le problème est qu'on ne connaît pas cette probabilité a priori. Il faut donc la modéliser, et le modèle n'est jamais parfait. Dès lors, on ne mesure jamais l'information, mais uniquement une « information perçue », c'est-à-dire l'information qu'on peut extraire d'un système à partir d'un modèle forcément imparfait. Cela mène à beaucoup de questions fondamentales. En particulier, comment se convaincre que la connaissance qu'on a d'un système est suffisamment précise pour quantifier sa sécurité? Cette notion montre notamment qu'aller vers des systèmes ouverts est formellement nécessaire pour comprendre la sécurité.* »

C'est le cas des circuits cryptographiques, mais aussi des algorithmes de traitement de données utilisés dans les applications « big data ». Bien sûr, assurer la sécurité ou la vie privée dans des systèmes ouverts peut sembler plus compliqué : on ne peut plus baser celles-ci sur la méconnaissance qu'un adversaire aurait du système mais uniquement sur des propriétés physiques et mathématiques vérifiables, reproductibles.

« *C'est donc un contexte plus contraignant, mais il apporte des garanties beaucoup plus rigoureuses, assure l'ingénieur.* »

Optimal oui, mais jusqu'où ?

Pour le spécialiste en cryptographie, les mathématiques sont un outil de compréhension du monde mais aussi de création. Il y a selon lui dans les mathématiques un pouvoir d'analyse et de systématisation qui permet d'aller plus loin, plus vite, de dépasser l'intuition, d'être efficace.

« *Il y a dès lors aussi un risque qu'elles soient utilisées comme un outil de domination. L'abus du terme « optimal » en est un bon exemple. Le fait qu'un algorithme soit optimal n'implique pas que son exploitation soit systématiquement désirable, il ne sous-entend pas qu'on devrait accepter son utilisation sans comprendre son impact, ni que son résultat reflète une vérité objective.* »

A ce sujet, François-Xavier Standaert souligne son intérêt pour la littérature émergente sur les questions de « gouvernementalité algorithmique » et d'intelligence artificielle, qui mettent en évidence les différences et incompatibilités entre la rationalité humaine et la rationalité algorithmique (statistique), le fait que l'automatisation ait une tendance à restreindre l'autonomie humaine. Ces questions rappellent la nuance entre mathématiques et sciences et elles sont particulièrement d'actualité dans le cadre du déploiement sans cesse plus rapide de technologies pas toujours bien comprises ni maîtrisées.

Question de temps

La recherche doit-elle être toujours suivie d'applications concrètes ? Le jeune ingénieur ne le pense pas.

« *Comprendre des choses et créer des abstractions est intéressant en soi. La question des applications des mathématiques est souvent posée à trop court terme. Avoir une application en tête n'est pas une nécessité pour avancer. Réfléchir uniquement à des applications concrètes à court terme est même préjudiciable à une recherche de qualité et à des applications plus fondamentales en aval. Le monde physique pose tant de questions ; toute réflexion de qualité a un potentiel applicatif dans 10 ans, 100 ans. L'aventure mathématique ou scientifique est la plupart du temps une belle histoire*", conclut François-Xavier Standaert.

A cet égard, et pour répondre à notre dernière question, le Professeur de l'école Polytechnique de LLN estime que la (bonne) vulgarisation est intéressante au même titre qu'une (bonne) fiction qui donne à penser.