François-Xavier Standaert

LA TRANSPARENCE COMME SOURCE DE SÉCURITÉ

Une carte à puce chiffre, calcule, protège. Mais entre les mains d'un adversaire, capable de mesurer sa consommation électrique ou son rayonnement électromagnétique, le dispositif parle malgré lui et trahit ses secrets. Depuis vingt ans, **François-Xavier Standaert, que rien ne prédestinait à la cryptographie, explore ces interstices, là où les algorithmes parfaits rencontrent la physique imparfaite, avec une approche paradoxale: la sécurité sans obscurité.**

Rédaction: Nelson Garcia Sequeira **Photos:** Black & Write

Né en 1978, il n'a pas passé son enfance à jouer avec des codes secrets. Pourtant, il est désormais l'une des références mondiales de la cryptographie matérielle, auréolé de trois bourses ERC, d'un titre d'IACR Fellow et du Prix quinquennal du FNRS 2025 en sciences exactes appliquées. Rigoureux et discret, il préfère braquer la lumière sur les systèmes plutôt que sur lui-même, mais a consenti à livrer «ses secrets», le temps de nos questions.

Vous avez découvert la cryptographie «par hasard et par chance». Expliquez-nous cette rencontre?

FRANÇOIS-XAVIER STANDAERT «En effet, c'est arrivé tardivement, grâce à un mémoire supervisé par Jean-Jacques Quisquater. Il rendait le sujet passionnant, en insistant sur les contributions scientifiques fondamentales de la cryptographie et leurs applications. Mon intérêt pour la recherche date de cette époque. Rétrospectivement, l'activité de recherche et la liberté qu'elle offre me correspondent. Même si d'autres sujets auraient pu m'intéresser, je suis ravi d'être tombé sur ce domaine, qui encourage l'interdisciplinarité (mathématiques, physique, électronique, informatique), mêle théorie et pratique, et dont les applications posent des questions sociétales importantes.»

Remontons plus loin, pourquoi des études d'ingénieur?

FXS «J'ai grandi dans une famille plutôt littéraire, avec une scolarité assez classique et un intérêt pour les maths, sans que ce soit exclusif. J'ai choisi l'ingénierie pour la rigueur de ces études et le confort intellectuel que procure (parfois) le fait de travailler sur des questions formulées clairement. Par exemple, le côté absolu d'une preuve ou le fait de réfléchir à des hypothèses mathématiques ou physiques réfutables. Mais j'ai toujours eu conscience que peu de vrais problèmes se résolvent exclusivement par la technique.»

Que gardez-vous de votre passage à l'EPL?

FXS «En tant que Bruxellois, c'était d'abord la possibilité de vivre à Louvain-la-Neuve… De ces années, je retiens la richesse d'un campus complet, où j'ai croisé des étudiants et des étudiantes de toutes les facultés.

Son ingénieur(e) modèle

Invité à désigner une figure scientifique inspirante, François-Xavier Standaert nomme **Alan Turing**. Un choix presque évident, qui résonne avec son propos. «Il est un excellent exemple de chercheur dont les réflexions étaient particulièrement larges, posées à un niveau extrêmement fondamental, et dont l'impact concret a été majeur.» Mathématicien de génie, père de l'informatique moderne, décisif dans la victoire alliée en déchiffrant Enigma, le cryptologue britannique a changé le cours de l'histoire depuis un bureau. **Difficile de trouver meilleur symbole de ce que la recherche fondamentale peut accomplir.**

Je garde aussi d'excellents souvenirs du cursus en tant que tel, en particulier de l'ambiance collaborative, assez éloignée des clichés d'études élitistes ou individualistes.»

Après votre doctorat, direction Columbia et le MIT, que vous a apporté cette expérience américaine?

FXS ▸ «Beaucoup de choses. Scientifiquement, j'ai été confronté à des approches plus théoriques de la recherche en cryptographie, qui ont fortement nourri la suite de mon parcours. De façon générale, les États-Unis offraient énormément de possibilités, de l'accès à des chercheurs de pointe aux facilités de financement. Comme l'UCLouvain, Columbia et le MIT sont des campus complets, avec une émulation incessante. J'aurais pu y rester plus longtemps et j'y suis toujours retourné avec plaisir. Je n'ai jamais envisagé de m'y installer, car je reste plus en phase avec le modèle social et éducatif européen. Mais c'est à cette époque qu'est née mon envie de rester dans le monde académique.»

Votre domaine, la cryptographie matérielle, reste peu connu du grand public. Comment l'expliquer?

FXS ▸ «La cryptographie est la science qui étudie la sécurité de l'information. Parmi ses objectifs, celui d'apporter des garanties de sécurité fortes contre des adversaires capables d'intercepter les messages d'une communication. Grâce à un dispositif électronique, type carte à puce (bancaire, identité, SIM), on peut chiffrer ces messages et les rendre inintelligibles. Mais, dans certains contextes, un adversaire peut obtenir un accès physique au dispositif et mesurer sa consommation électrique ou son rayonnement électromagnétique. Sans précautions particulières, cette mesure, sorte "d'électroencéphalogramme" de la carte à puce, donne des indices critiques sur ses secrets, susceptibles de compromettre leur sécurité. Ce passage, de l'abstraction mathématique à la réalisation physique des algorithmes cryptographiques, et les défis qu'il pose, sont au cœur de mes recherches.»

Votre approche repose sur un principe contre-intuitif: la «sécurité sans obscurité», c'est-à-dire révéler le fonctionnement d'un système pour mieux le protéger…

FXS ▸ «Notre but est de nous prémunir d'un adversaire qui connaît parfaitement le système attaqué. Alors que le réflexe habituel est de cacher les spécifications des systèmes à protéger, travailler sur des systèmes ouverts permet de baser la sécurité sur une bonne séparation des tâches, entre des hypothèses physiques, qu'on peut chercher à réfuter, et leur amplification mathématique. En d'autres mots, on veut passer d'audits de sécurité, qui concluraient "je n'ai pas vu d'attaque", à des arguments formels et quantitatifs, permettant de borner l'efficacité des meilleures attaques. Notre équipe de recherche s'attaque ainsi au sophisme du silence: "absence de preuve n'est pas preuve d'absence". C'est totalement accepté pour les algorithmes cryptographiques, curieusement pas encore pour leurs implémentations.»

Comment prouver que la démarche «ouverte» fonctionne?

FXS ▸ «L'enjeu est de montrer qu'arrivés à un certain niveau de maturité scientifique, mieux vaut baser la sécurité sur la compréhension des phénomènes observés que sur l'espoir – difficile à quantifier – que l'adversaire se limitera à une mauvaise compréhension de ceux-ci. Cette démarche peut se heurter à des réticences pratiques, car les audits sont moins exigeants, donc confortables. À nous de démontrer que les "garanties de sécurité sans obscurité" sont dignes de confiance, et pas moins efficaces.»

Concrètement, à quoi ressemble votre travail au quotidien?

FXS ▸ «Parvenir à ces résultats soulève une série de questions: conceptuelles, formelles, physiques, statistiques, d'ingénierie, etc. Ce qui est passionnant, c'est qu'on travaille simultanément sur différents niveaux de vérité: absolue pour les preuves de sécurité, réfutable formellement pour les hypothèses mathématiques, réfutable expérimentalement pour les hypothèses physiques, qui doivent être comprises comme un objectif d'implémentation. Il est facile, mais inutile, de démontrer des résultats sur base d'hypothèses qu'on ne pourra jamais réaliser en pratique: d'où l'obligation de tout traiter de façon unifiée. On cherche donc un équilibre constant entre rigueur mathématique et réalisme physique, ce qui demande d'interagir avec des chercheurs aux profils très différents, au sein de notre groupe de recherche ou ailleurs. Pour cela, il faut trouver un langage commun, une démarche riche, qui accapare l'essentiel de mon temps.»

Annoncé comme *the next big thing*, l'ordinateur quantique est-il une menace pour la cryptographie?

FXS ▸ «Oui, car un tel ordinateur serait capable d'invalider les hypothèses mathématiques sur lesquelles se basent des standards déployés (chiffrement, signature, etc.). La communauté scientifique a fort heureusement anticipé cette menace, via un processus de recherche et de standardisation pour construire de nouveaux schémas, reposant sur des hypothèses dites "post-quantiques", qui ne seraient pas invalidées par un ordinateur quantique. Cependant, ces nouveaux schémas ont été conçus sans envisager la sécurité face aux attaques physiques. Leur protection pose donc de nouveaux défis, qui pourraient aussi motiver la conception de nouveaux algorithmes, conjuguant au mieux sécurité post-quantique et sécurité matérielle.»

L'autre «révolution» en cours, c'est l'IA. Faut-il s'en inquiéter?

FXS ▸ «La question de l'apprentissage automatique est plus diffuse, dès lors plus difficile à anticiper. À ce stade, beaucoup de questions de fiabilité, de confiance ou de sécurité liées à ces outils, dont une partie est déjà déployée ou en cours de déploiement, restent ouvertes. Ce domaine est aussi parasité par des intérêts financiers ou stratégiques, qui rendent difficile une discussion sereine et objective des risques. L'IA est un bon exemple de sujet dont les questions ne se résoudront pas exclusivement par la technique.»

L'ingénieur(e) du XXIe siècle

En cryptographie, une hypothèse non réfutable ne vaut rien. François-Xavier Standaert applique la même exigence à sa vision du métier d'ingénieur: trois qualités concrètes, issues de l'expérience, pas du manuel.

CURIOSITÉ

C'est souvent en essayant de comprendre ce que d'autres chercheurs trouvaient intéressant dans leurs propres questions qu'il a trouvé les outils, les techniques ou les collaborations qui lui ont permis d'avancer.

ORIGINALITÉ

S'autoriser des chemins moins balisés, oser des questions qu'on est seul à se poser, car toutes les trajectoires sont possibles et elles sont parfois guidées par le hasard ou par la chance.

RIGUEUR

La capacité à formuler clairement une question, à construire une réponse réfutable, à distinguer ce qu'on sait de ce qu'on suppose: c'est cela le cœur du métier d'ingénieur, et cela ne se démode pas.

Vous évoquiez les questions sociétales posées par les applications. Pouvez-vous développer, en particulier, le volet démocratique?

FXS ▸ «Si la cryptographie apporte des solutions pour assurer les propriétés de base de la "démocratie en ligne" qui se développe actuellement, encore faut-il permettre au citoyen de les comprendre de façon fine et transparente. Il me semble, par exemple, délicat d'imposer des solutions qu'on ne peut auditer publiquement. À cet égard, ma recherche rappelle que transparence et sécurité vont de pair plus qu'elles ne s'opposent.

Plus généralement, des tentatives pour réduire la sécurité et la vie privée en ligne refont régulièrement surface. Malgré des buts louables (terrorisme, pédocriminalité, etc.), ces solutions affaiblissent les garanties de sécurité offertes à la population par la cryptographie, tout en complexifiant le contrôle démocratique. En outre, ces "solutions affaiblies", qui peuvent porter préjudice à des droits fondamentaux, reflètent une compréhension superficielle des enjeux, car un acteur mal intentionné ne les emploiera jamais. Les mécanismes de surveillance augmentent aussi les risques de vol de secrets industriels, fragilisent les systèmes lors des changements de régime, etc. La recherche académique permet de mettre ces risques en lumière.»

La cryptographie peut mener à des technologies à «usage double»: civil et militaire. Quelle place pour l'éthique?

FXS ▸ «Toute technologie présente des risques de mauvaise utilisation: ce n'est pas nouveau, et les universités ont mis en place des comités indépendants pour y faire face. Le véritable enjeu est de trouver un équilibre entre risque et ouverture, car la recherche fonctionne mieux quand elle est ouverte: sans publication des idées, des méthodologies ou des données, un résultat scientifique ne peut être ni vérifié ni réfuté. Plus la communauté scientifique est large, plus ce processus est efficace. C'est pourquoi le FNRS et le Conseil européen de la recherche (ERC) encouragent cette ouverture, encore plus essentielle pour un acteur de petite taille comme la Belgique.»

Face à ces questions, quel rôle doivent jouer les scientifiques?

FXS ▸ «Je le conçois comme un rôle d'éclairage pour des orientations à long terme; à l'opposé, je me sens rarement pertinent sur des questions d'actualité, sans le recul nécessaire. Je crois aussi que cet éclairage est plus utile quand il est défendu collectivement par des groupes de travail plutôt que par des positions individuelles. Je suis donc convaincu que le monde scientifique doit jouer un rôle sociétal, mais il est parfois mal utilisé, en particulier quand il contribue à une accélération médiatique, souvent vaine.»

Comment se porte la recherche fondamentale, notamment en termes de financement?

FXS ▸ «Je pense qu'on souffre d'un déséquilibre improductif entre une recherche fondamentale sous-financée et une recherche appliquée qui manque dès lors de bases solides pour peser sur les grandes questions de société. C'est souvent un socle très large de recherche fondamentale, ouverte à tous les sujets et indépendante des intérêts économiques et politiques, qui permet l'innovation et l'impact à long terme.»

Vous êtes vu comme une sommité dans votre domaine, que représente le Prix quinquennal du FNRS?

FXS ▸ «Le monde de la recherche est compétitif et, en raison de la nature des processus d'évaluation, il est rare de recevoir instantanément des retours dithyrambiques sur nos travaux. Être récompensé après autant d'années de travail est donc gratifiant. Cela souligne la cohérence de nos contributions pour réduire l'écart entre la compréhension théorique de la sécurité matérielle et les contraintes pratiques d'implémentation. J'espère que tous ceux et celles avec qui j'ai collaboré se sentent pleinement associés à cette distinction.»

Dans une interview, vous disiez avoir «nettement plus de raisons d'être reconnaissant que d'être fier»...

FXS ▸ «C'est un sentiment assez général. Je suis né dans un pays qui a investi plus de 20 ans dans mon éducation, j'ai grandi dans une famille dont les parents, universitaires, valorisaient l'enseignement et j'ai bénéficié de nombreuses rencontres inspirantes au cours de ma carrière. Il me semble donc que j'aie nettement plus de raisons d'être reconnaissant que d'être fier. Je n'aurais pas réalisé le même parcours avec des circonstances moins favorables.»

Dans un monde incertain, nombre de jeunes doutent de l'utilité de leur futur métier. Comment les guider?

FXS ▸ «Le doute me paraît normal, voire salutaire. Je pense qu'il peut être source de progrès, bien plus que les certitudes individuelles. Je rappellerais aussi que je ne suis pas né cryptographe. Une vocation ne se décrète pas, elle se construit, et parfois là où on ne l'attendait pas. Comprendre des choses en profondeur, ce qu'encouragent les études d'ingénieur et la recherche, me semble en tout cas rester une démarche enrichissante.» #

CURRICULUM VITAE

 # FORMATION
Ingénieur civil électricien et docteur en cryptographie (UCLouvain, 2001 et 2004).

 # SON PARCOURS
Lauréat d'une bourse Fulbright, il effectue des séjours de recherche à Columbia University et au MIT Medialab, puis revient à l'UCLouvain comme postdoctorant FNRS en 2005. Cofondateur de la spin-off IntoPix, il gravit les échelons du FNRS, jusqu'au titre de directeur de recherche. Professeur à l'EPL et membre de l'ICTEAM depuis 2013, il a été directeur élu de l'IACR (2017-2022) et en est le vice-président depuis cette année.

 # SIMPLE-CRYPTO
Engagé au-delà de la recherche, il cofonde SIMPLE-Crypto avec des collègues en 2022: une ASBL dédiée au développement d'implémentations cryptographiques open source. À mi-chemin entre monde académique et industrie, cette expérience met le modèle de sécurité sans obscurité à l'épreuve du réel et encourage la mutualisation des efforts sur des questions d'implémentations pointues. Elle résulte aussi d'une réflexion générale sur les modèles de valorisation en cryptographie, avec notamment pour objectif de protéger le fruit d'années de recherche publique contre un rachat dans un intérêt plus exclusif.»