Science des secrets et secrets des sciences mathématiques et informatique

Entretien avec Jacques Stern (*réalisé par Valérie Schafer*)

Professeur émérite à l'École normale supérieure, membre du collège de l'ARCEP (Autorité de régulation des communications électroniques et des postes) depuis 2012, Jacques Stern a commencé sa carrière dans les années 1970 en tant que mathématicien, avant de se tourner vers l'informatique, en particulier la cryptologie. De l'Université de Caen à l'École normale supérieure il nous explique son passage des mathématiques à l'informatique, les liens et les différences entre les deux disciplines, son rôle dans le développement en France de la cryptologie, pour lequel – au-delà de ses propres travaux – il a notamment été récompensé de la médaille d'or du CNRS en 2006, du RSA Award for Excellence in the Field of Mathematics en 2007 ou encore du prix Science et Défense en 2008.

Valérie Schafer [1]

Valérie Schafer : *Avant de nous pencher sur votre parcours dans la cryptologie j'aimerais que nous revenions sur votre première spécialisation. Vous avez été mathématicien. Élève de l'École normale supérieure, vous avez même été reçu premier à l'agrégation de mathématiques en 1971.*

1. Valérie Schafer, ISCC, CNRS/Paris-Sorbonne/UPMC. Entretien co-publié avec la revue *Technique et Science Informatique* (TSI).

Jacques Stern : Très jeune déjà, les mathématiques m'ont attiré. En plus je dois reconnaître que j'y réussissais assez bien, peut-être avec un peu de facilité, donc tout convergeait pour m'amener à devenir mathématicien. Je suis entré à l'École normale par goût mais bien d'autres disciplines comme l'histoire, les langues et les cultures étrangères m'intéressaient. Je ne suis pas univoque, mais je suis devenu mathématicien.

Après l'École Normale, je me suis senti attiré au sein des mathématiques par des questions qui sont aux confins de la plus extrême abstraction. J'étais fasciné par les travaux de Gödel ou de Turing.

Gödel par une sorte de tour de force de la pensée a réussi à montrer que la méthode déductive portait en elle-même sa propre limitation. Il a ainsi établi que n'importe quel système fondé sur la déduction demeurait incapable de donner une réponse de mathématicien (une preuve ou un contre-exemple) à tous les problèmes possibles et donc n'englobait qu'une partie d'entre eux. C'était fascinant !

La deuxième étape, restée ouverte par Gödel et franchie par Turing, était le problème de la décision.

V. S. : *C'est-à-dire ?*

J. S. : C'est déjà les prémices de l'informatique. Imaginons un processus mécanique qui autorise une forme de calcul extrêmement générale par l'intermédiaire d'une suite d'instructions à réaliser pas à pas, un algorithme comme disent maintenant les informaticiens mais ce mot, devenu d'usage courant, est maintenant partout. Un tel processus peut-il faire mieux et régler le problème de Gödel ? Turing a répondu par la négative.

V. S. : *On est dans les années 1930 avec Gödel et Turing.*

J. S. : Oui, je vois les mathématiques et l'informatique selon une perspective historique...

Et l'histoire continue. Ainsi, quand j'étais encore au lycée, sont apparus les travaux de Paul Cohen qui a donné une réponse du même type que celle de Gödel et Turing, mais cette fois à des questions précises, posées par des mathématiciens à des mathématiciens. Concernant le problème du continu de Cantor, il a démontré que la formalisation des mathématiques ne permet de répondre ni positivement ni négativement. Kurt Gödel a fait la moitié du chemin en 1938 et cela s'est terminé par les recherches de Paul Cohen dans les années 1960. Ces résultats m'ont marqué.

Après 1971 et mon agrégation de mathématiques, j'ai commencé à travailler sur les problèmes de la logique et de la théorie des ensembles. J'ai effectué une thèse, je suis ainsi devenu mathématicien et j'ai été nommé assez jeune professeur à l'Université de Caen.

*La théorie des ensembles fut créée par Georg Cantor à la fin du XIX*e *siècle. Cependant, le caractère extrêmement général et abstrait de la notion d'ensemble permit de produire des paradoxes rendant la théorie contradictoire (cf. théorie élémentaire des ENSEMBLES). Pour échapper à ces paradoxes et fournir un cadre abstrait adéquat au développement des mathématiques, le concept d'ensemble a dû être sérieusement codifié. Plusieurs théories formalisées des ensembles furent élaborées, en particulier : la théorie des types de Whitehead et Russell, la théorie des ensembles de Zermelo et Fraenkel, créée pour l'essentiel par Zermelo et enrichie par Fraenkel, et la théorie des classes de von Neumann, Bernays et Gödel.*

Extrait de l'article Ensembles (Théorie des),
écrit par Jacques Stern pour l'*Encyclopedia Universalis*
http://www.universalis.fr/encyclopedie/ensembles-theorie-des-theorie-axiomatique/

In the late 1870s, German mathematician Georg Cantor put forth a hypothesis that said any infinite subset of the set of all real numbers can be put into one-to-one correspondence either with the set of integers or with the set of all real numbers. All attempts to prove or disprove this conjecture failed until 1938, when Kurt Gödel showed it was impossible to disprove the continuum hypothesis.

Despite having never worked in set theory, Cohen proved the extremely surprising result that both the Continuum Hypothesis and the Axiom of Choice—two of the most basic ideas in mathematics—were actually undecidable using the axioms of set theory. This result, which meant that conventional mathematics could neither prove nor disprove concrete and well known mathematical assertions, caused healthy turbulence among philosophers, logicians and mathematicians concerned with the concept of truth [. . .]".

Dawn Levy, "Paul Cohen, winner of world's top mathematics prize, dies at 72", Stanford Report, March 28, 2007,
http://news.stanford.edu/news/2007/april4/cohen-040407.html

V. S. : *C'était en 1979 ?*

J. S. : Absolument et cette nomination a été une double chance : d'une part devenir professeur me donnait la liberté de ne plus penser à l'évolution de ma carrière, mais à l'évolution de ma réflexion scientifique, d'autre part à Caen personne ne s'intéressait réellement à la logique et à la théorie des ensembles. J'ai engagé alors une vraie période de réflexion. Le choix d'être mathématicien, de faire de la logique, de la théorie des ensembles, était un choix de passion, mais cela ne me suffisait pas, ou peut-être était-ce trop ambitieux. Je m'explique. Les mathématiques – demandez à Cédric Villani, célèbre médaillé Fields qui a suivi certains de mes cours à l'ENS – sont une science qui ouvre des perspectives très profondes tout en portant en elle-même une réelle esthétique. Mais je la vois aussi comme une science un peu aux confins de la pensée : on se bat contre l'infini et c'est un combat qu'il n'est pas forcément possible de poursuivre très longtemps. Les maths s'inscrivent par ailleurs dans une perspective parfois tellement longue qu'on n'est pas assuré d'en voir les conséquences ultimes, surtout quand on travaille comme je le faisais dans un domaine limité par le nombre des collègues et extrêmement abstrait, loin des applications.

En un mot, le manque d'applications de ma discipline et son élitisme me gênaient. Quand on est à l'École normale supérieure et qu'on entre dans une communauté scientifique internationale de mathématiciens, on est bien sûr un peu préparé à l'élitisme. Je me souviens de ce mot d'un spécialiste de la théorie des ensembles à qui je parlais d'un des dix meilleurs spécialistes de la discipline, me répondant avec humour : « Es-tu certain qu'il y ait dix spécialistes ? ».

Je trouvais à Caen un environnement où j'étais seul, où je ne pouvais faire équipe et j'étais convaincu qu'il fallait que je réoriente ma perspective. Quand on est spécialiste des fondements des mathématiques, comment réoriente-t-on sa perspective ?

J'étais logicien et je démontrais, en particulier, ce qu'on nomme des résultats d'indécidabilité. En d'autres termes, j'essayais de montrer que tel ou tel problème est au-delà des limites de ce que peuvent atteindre les mathématiques, qu'il est donc impossible de le résoudre.

Pourquoi les avais-je entrepris ? Parce que je pensais – et je pense toujours – que les résultats les plus profonds des mathématiques du vingtième siècle sont précisément les résultats d'impossibilité obtenus par Kurt Gödel en 1930 et par Alan Turing en 1936. Le théorème de Gödel, c'est le paradoxe du menteur : quel sens donner à l'assertion « je mens » ? En effet, en disant « je mens » ou bien je mens réellement, et alors je dis la vérité, ou bien je dis en fait la vérité mais c'est donc que je mens. Le tour de force de Gödel est d'avoir, pour reproduire le paradoxe du menteur, su rendre les mathématiques capables de parler d'elles-mêmes, ce qu'on nomme parfois l'arithmétisation

de la syntaxe. Le pas suivant, celui de Turing, est la mécanisation de l'activité mathématique par la notion de machine de Turing, ordinateur avant l'heure.

En étais-je satisfait ? Oui et non. Oui, car il est fascinant de participer à la continuation d'une grande aventure intellectuelle. Non, car rien de concret ne me semblait pouvoir découler d'un résultat d'impossibilité de plus.

Discours prononcé par Jacques Stern le 13 décembre 2006
lors de la remise de la médaille d'or du CNRS,
`http://www.di.ens.fr/users/stern/data/discours-or-1312.pdf`

V. S. : *C'est alors que vous allez vers l'informatique...*

J. S. : Au milieu des années 1970, il y avait une certaine effervescence intellectuelle liée à l'émergence de l'informatique. Évidemment cela englobait un tas de choses, allant du simple usage de l'informatique à une approche plus théorique et plus conceptuelle, disons une informatique de la pensée. Cette dernière, à l'instar des mathématiques, se présente comme une science, à ceci près que ce n'est plus principalement une science déductive, c'est une science dont l'objet est aussi mécanique. Vous n'êtes plus en combat avec l'infini, mais avec la machine. Je définis l'informatique comme la science qui étudie la mécanisation de l'abstraction.

V. S. : *C'est ce qui vous attire alors vers l'informatique ?*

J. S. : Au milieu des années 1970 sont apparus simultanément de nouveaux progrès dans deux disciplines d'informatique théorique pas si éloignées de ma formation : la complexité algorithmique et la cryptologie.

La première permet de revisiter le travail de Turing à la lumière du développement des ordinateurs. Turing est un précurseur génial. À l'époque de sa thèse sur la décision, il n'y avait pas de machine. Il a donc imaginé une machine informatique abstraite, la machine de Turing, qui reproduit les actions les plus élémentaires de quelqu'un faisant des calculs en suivant une liste d'instructions. Mais dans les années 1960/1970 il y avait de vraies machines dont les performances étaient limitées non par l'impossibilité de résoudre le problème de la décision mais par des contraintes bien plus terre à terre de temps de calcul et d'espace mémoire. Ces contraintes appelaient une nouvelle théorie mathématique, qui pût en rendre compte. La théorie de la complexité a ainsi établi que certains algorithmes dits polynomiaux s'identifiaient à ce qu'une machine peut exécuter raisonnablement tandis que d'autres restaient intrinsèquement hors d'atteinte dans la pratique. La théorie a toutefois échoué à classer dans l'une ou l'autre catégorie nombre de problèmes combinatoires simples. La question demeure ouverte et est connue sous le nom de problème P = NP. Pour rester simple, disons que la lettre P représente ce que les algorithmes polynomiaux peuvent

résoudre et la lettre NP ce qu'ils peuvent simplement vérifier si la solution leur est fournie. La question de l'identité de P et NP a été posée par un certain nombre de chercheurs des années 1960/1970, dont Stephen Cook. On rencontre ainsi un problème qui n'est pas sans analogie avec celui de Turing. Il reste ouvert et, en 2000, Landon Clay l'a inclus dans les sept défis mathématiques pour lesquels une récompense de un million de dollars est offerte [2]...

V. S. : *Et la cryptologie ?*

J. S. : Cette « nouvelle discipline », qui n'était en fait pas si nouvelle, venait d'émerger pour des raisons très différentes de celles de la complexité et qui relèvent plutôt des liens entre informatique et télécommunications. Le réseau Arpanet avait donné lieu aux premiers échanges de mails et déjà les pionniers pensaient que d'ici une trentaine d'années il y aurait de gigantesques flux d'information à travers toute la planète. Entre autres choses, ils menaient des recherches sur la question de la sécurité de ces échanges, sur les méthodes pour garantir l'origine d'un message, son intégrité, la confidentialité de son contenu. Des méthodes existaient – la cryptologie venait de très loin dans l'histoire –, mais elles n'étaient pas directement applicables à l'environnement qu'ils anticipaient.

À peu près au moment où j'ai cherché ma voie, sont apparues une question et une réponse. La question d'abord. Elle a été posée dans un article fondateur de deux mathématiciens américains, Diffie et Hellman. Ils ont montré que pour réaliser, dans l'environnement de ce que l'on appelait pas encore Internet, les fonctionnalités de la cryptologie, il faudrait inventer un nouveau mécanisme, devant permettre de s'adresser en toute confiance à quelqu'un que l'on n'a jamais rencontré. Ils ont posé ce problème auquel ils ont fourni une réponse partielle, fondée sur l'idée qu'on ne pourrait plus conserver une symétrie parfaite entre l'expéditeur et le récepteur d'un message, mais qu'il faudrait établir une certaine asymétrie. Cette asymétrie était mathématiquement définie. Et, deux ans après, trois autres scientifiques, Rivest, Shamir et Adleman ont produit le premier système cryptographique qui réalise l'asymétrie réclamée : le RSA.

« [...] Futura-Sciences : Comment définiriez-vous la cryptologie ? Est-elle plutôt une branche des mathématiques ou une spécialité informatique ?

Jacques Stern : La cryptologie a d'abord été un art. Regardez les travaux du Florentin Leon Battista Alberti... Elle est ensuite devenue une technique. Aujourd'hui, c'est une science. Elle opère dans un certain environnement (actuellement l'informatique), met en œuvre une ingénierie (nous utilisons des

2. http://www.linternaute.com/science/science-et-nous/dossiers/07/defis-maths/1.shtml

outils, qui peuvent aller jusqu'au fer à souder) et se base sur des concepts mathématiques. Son objet est la trilogie fondamentale : l'intégrité (les informations doivent restées intactes), l'authenticité (l'origine ou la personne doivent être reconnues) et la confidentialité (les informations ne doivent pas être divulguées).

FS : Quelles ont été les évolutions déterminantes ?

Jacques Stern : La dernière date de 1976-1978 avec l'apparition de la cryptologie asymétrique. On a alors considéré qu'il existait une dissymétrie entre, d'une part, le fait de cacher un message et, d'autre part, l'opération à réaliser pour récupérer ce message. On a ainsi inventé le principe de la clef publique : le message est crypté par une méthode connue de tous mais seul le destinataire peut le lire.

FS : Quelle est la plus belle méthode, selon vous ? Et la plus utilisée aujourd'hui ?

Jacques Stern : Elles sont toutes belles ! La plus efficace et la plus utilisée dans le domaine de la cryptologie asymétrique est celle de Rivest, Shamir et Adleman, dite RSA. [. . .] »

Entretien de Jacques Stern pour le site futura-sciences.com
du 18 décembre 2007
http://www.futura-sciences.com/magazines/high-tech/infos/actu/d/informatique-jacques-stern-la-cryptologie-fait-partie-notre-vie-quotidienne-13954/

Ce système est aujourd'hui pratiqué en masse sur l'Internet. L'asymétrie sur laquelle il repose est un peu analogue à celle de P vs NP que j'évoquais précédemment et me permettait de réincorporer des questions auxquelles je m'étais intéressé, mais cette fois dans une perspective qui pouvait avoir des applications. Ce qui est asymétrique, avec un avantage d'un côté et un désavantage de l'autre, peut être utilisé pour protéger le contenu, l'intégrité, l'authenticité d'un message. Je me suis dit « Allons-y ! ».

V. S. : *Ce « Allons-y » vous le situez quand ?*

J. S. : Le papier séminal de Rivest, Shamir et Adleman date de 1978. Mon premier article significatif dans le domaine de la cryptologie date de 1987 [3]. Le « Allons-y »

3. Jacques Stern. Secret linear congruential generators are not cryptographically secure. *Proc. of the IEEE Symposium on Foundations of Computer Science* (1987), 421-426.

a pris un peu de temps, mais on ne se réveille pas un jour mathématicien et le lendemain informaticien ! Il y a eu un cheminement : à Caen j'ai motivé un certain nombre de collègues pour qu'ils fassent le trajet avec moi. On a commencé dans le domaine de la complexité, un sujet qui n'était pas à l'époque très central dans la vision de l'informatique française. Mes collègues informaticiens étaient plus les enfants de Gödel que de Turing, avec une approche fondée sur la logique. Mon évolution a pris quelques années et bien sûr, en parallèle, je continuais à travailler sur la logique et la théorie des ensembles.

V. S. : *Vous étiez d'ailleurs professeur de mathématiques.*

J. S. : En effet, à Caen j'avais un poste de professeur de mathématiques. À cette époque il y avait peut-être un seul professeur d'informatique dans le département de mathématiques. Mais il y avait parmi les jeunes collègues des gens intéressés et on nous a laissé faire.

V. S. : *Une communauté dédiée à la cryptologie existe-t-elle à ce moment, vers 1987 ?*

J. S. : Une communauté internationale a commencé à se constituer tout de suite après les apports de Rivest, Shamir et Andleman. Ils ont fait une découverte phare, pas tant par le fait de résoudre un problème techniquement très difficile, mais en proposant une solution extrêmement porteuse d'applications. Certains résultats ferment l'horizon, un peu comme ceux que j'avais obtenus en théorie des ensembles. Par exemple, une de mes contributions répondait à une question d'un mathématicien russe des années 1920, Nicolas Lusin, et j'ai donné la traditionnelle réponse de la théorie des ensembles : le problème est indépendant, on ne peut ni le prouver ni l'infirmer, point. Rivest, Shamir et Andleman eux ont ouvert des perspectives vertigineuses et créé une nouvelle discipline. Dès 1981 un congrès annuel est établi à UCSB, en Californie, qui a commencé à réunir tous les spécialistes de cryptologie. C'est toujours une des deux grandes conférences avec Eurocrypt côté européen. C'est là que l'on voit la différence entre les États-Unis et l'Europe : le congrès américain a lieu tous les ans au même endroit et à la même date, tandis qu'Eurocrypt change tous les ans de lieu et de date.

V. S. : *Vous êtes le premier en France à vous intéresser à la cryptologie ?*

J. S. : C'est toujours très difficile de dire qu'on est le premier, mais j'ai fait l'effort de réunir les gens qui s'intéressaient au sujet et de le structurer en une discipline académique. Bien sûr la cryptologie existait avant, c'est une science ancienne, déjà connue dans l'antiquité. Il y avait des experts, mais je parle ici seulement du monde académique et de ce qui s'est passé à partir des travaux de Diffie et Hellman puis Rivest, Shamir et Adleman.

V. S. : *Vous avez évoqué Arpanet, vous vous intéressez alors aux réseaux ?*

J. S. : Non, pas à l'époque, mais à l'informatique oui, en tant que mécanisation de l'abstraction.

V. S. : *En 1986 vous quittez Caen pour Paris 7.*

J. S. : En effet, je suis nommé professeur de mathématiques à l'université Denis Diderot. Et je retrouve aussi l'École normale supérieure, car des collègues, Michel Broué, directeur du département de mathématiques et Claude Puech, son adjoint en charge de l'informatique (les deux disciplines ne formaient qu'un seul département) me demandent de venir les rejoindre au moins à temps partiel, pour réaliser une sorte d'interface mathématiques/informatique en enseignant la logique. Dans les années qui suivent je viens à temps plein à l'École normale et là il se passe quelque chose qui n'aurait sans doute pas pu se passer ailleurs... Je mets en place un enseignement de DEA en cryptologie et cet enseignement attire de nombreux étudiants extrêmement brillants, de l'École normale, de l'École polytechnique et d'autres universités et écoles. Je réunis ainsi dans un domaine encore largement vierge des jeunes brillants et on entame un vrai dialogue. Eux veulent entrer dans ce domaine nouveau, moi je suis plus âgé mais j'y suis rentré récemment, donc une émulation mutuelle se fait, qui ne pouvait se créer qu'ici. Certains disent que je suis en France le « père de la cryptologie », cela n'aurait pas été possible sans enfants !

V. S. : *Vous créez alors une équipe.*

J. S. : Oui, mes premiers élèves sont aujourd'hui mes collègues. Certains sont professeurs dans de grandes universités françaises, d'autres directeurs de recherche au CNRS ou à l'INRIA, l'un d'eux est professeur à l'EPFL et j'ai même parmi mes anciens élèves le directeur général de l'Agence nationale de sécurité des systèmes d'information (ANSSI). Fonder cette équipe a été une très grande source de joie et de créativité ; on avançait très vite.

V. S. : *En 1992 vous êtes détaché par le CNRS ?*

J. S. : Oui, je suis pour un an directeur de recherche détaché, ce qui me permet de consacrer plus de temps à la recherche au sein du Laboratoire d'informatique de l'École normale, qui est alors une unité mixte CNRS/ENS, créée par Claude Puech. Quand je deviens directeur du département informatique ensuite, à partir de 1999, je choisis d'y associer aussi l'INRIA. Mais, pour revenir au CNRS, je veux souligner le soutien qu'il m'a apporté, en me nommant à un moment crucial pour la poursuite de ce que j'avais commencé ou encore en attribuant ensuite des postes de chargés de recherche pour renforcer l'équipe. Pour que je puisse réussir, il ne fallait pas seulement l'ENS et les étudiants, mais aussi l'appui du CNRS.

V. S. : *À quoi travaille alors l'équipe ? Quelles sont ses spécialités ?*

J. S. : En cryptologie on travaille de manière générale à garantir l'authenticité, l'intégrité et la confidentialité des communications, mais cette science s'appuie sur différentes méthodes. Prenons l'exemple des travaux sur le RSA : ils sont des descendants très directs de résultats obtenus par le célèbre mathématicien suisse Euler dans la seconde moitié du XVIII^{e} siècle. Beaucoup de travaux sont, quant à eux, à analyser à la lumière de la théorie de la complexité et donc descendant de Turing. D'autres encore mettent en jeu des méthodes probabilistes. Cette multiplicité de sources d'inspiration en cryptologie fait que les différentes branches ne requièrent pas forcément les mêmes goûts, les mêmes aptitudes mathématiques et nous avons essayé de couvrir au plus large le champ. Il fallait construire une école, j'ai essayé de représenter tous les domaines.

Dans notre équipe, nous avons une double marque de fabrique : d'une part, une expertise dans le domaine de la cryptanalyse, cette partie de la cryptologie qui vise à tester la solidité des protections proposées et notamment à recouvrer le contenu d'un message chiffré sans connaître les conventions secrètes qui ont permis de le créer. D'autre part, dans la partie de la discipline qui relève de la conception d'algorithmes cryptographiques, de nombreuses contributions à l'élaboration d'une sécurité [4] prouvée par une méthodologie qui vient de la théorie de la complexité et qui a pour but de démontrer la solidité, sinon de manière absolue mais au moins à partir de conjectures mathématiques communément admises. C'est en somme le contraire de la cryptanalyse.

[…] Ainsi, un algorithme de chiffrement transforme-t-il un texte en langage clair en un texte incompréhensible et un algorithme de déchiffrement fait-il l'opération inverse. Ce que je fais, c'est donc concevoir de nouveaux algorithmes, mais aussi les évaluer.

Cette activité d'évaluation repose sur la cryptanalyse, c'est-à-dire la tentative de mettre en défaut la confidentialité que l'algorithme est censé garantir. La défense et l'attaque en somme, auxquelles s'ajoute toutefois ce qui est une spécificité des recherches que j'ai menées, la preuve qu'un algorithme est capable de résister aux attaques des cryptanalystes. C'est un peu le retour à mes premiers travaux, montrer des résultats d'impossibilité, mais dans un cadre à la fois moins absolu et plus quotidien que celui ouvert par Gödel : moins absolu, car la cryptographie ne protège que compte tenu de limites prescrites à la puissance de calcul de l'adversaire ; plus quotidien, car ce sont les secrets et les transactions de tout un chacun qu'il s'agit de protéger […].

4. Voir notamment David Pointcheval, Jacques Stern, Security Arguments for Digital Signatures et Blind Signatures. *Journal of Cryptology*, vol. 13, n^{o} 3, 361-396, ou David Pointcheval, Jacques Stern, Security proofs for signature schemes, *Eurocrypt 96*, Lecture Notes in Computer Science 1070, 387-398.

Discours prononcé par Jacques Stern le 13 décembre 2006
lors de la remise de la médaille d'or du CNRS
http://www.di.ens.fr/users/stern/data/discours-or-1312.pdf

V. S. : *En 1996 vous devenez directeur du laboratoire d'informatique puis en 1999 directeur du département d'informatique de l'ENS.*

J. S. : Oui, en 1996 Claude Puech part à Grenoble et je le remplace comme directeur du Laboratoire, mais c'est un changement un peu anecdotique. En 1999 par contre je propose la séparation d'avec les collègues mathématiciens, ce qui est bien plus structurant. Ça s'était fait partout ailleurs : les priorités et les pratiques scientifiques des deux disciplines ne sont pas les mêmes. Au demeurant, la séparation s'est faite à l'amiable et chacun était conscient qu'on ne pouvait pas indéfiniment rester sous l'aile des mathématiques. L'école mathématique française est parmi les plus réputées au monde et l'École normale supérieure en est un peu le phare. Il nous fallait, quant à nous, gagner notre propre notoriété et on était par ailleurs face à une vraie difficulté, que mes successeurs doivent encore résoudre : trop peu d'élèves choisissent l'informatique à l'ENS, car il n'y a pas beaucoup d'enseignements en informatique dans les lycées et classes préparatoires. Pour y remédier, nous avons introduit une spécialité informatique au concours de l'ENS, l'idée étant de développer au sein de l'École une filière proprement informatique.

V. S. : *Vous parliez de notoriété à gagner au moment de la séparation avec les mathématiques, c'est chose faite ?*

J. S. : Je crois. Un bon indicateur en est notamment l'obtention des bourses ERC par le département : nous sommes au premier rang en France et peut-être même en Europe.

V. S. : *À partir de 2007 votre carrière prend de nouveaux tournants.*

J. S. : Oui, en 2007 je deviens président d'une société anonyme, Ingenico, qui fabrique des terminaux de paiement sécurisés. C'est le leader mondial dans le domaine des transactions bancaires sécurisées. J'ai accepté ce poste – non exécutif toutefois – car cela m'intéressait de voir comment ultimement ce qu'on faisait dans la théorie était utilisé dans la pratique. Je deviens également président de l'ANR en 2007 puis en 2010 conseiller auprès du ministre de la Recherche et de l'Enseignement supérieur sous Valérie Pécresse puis Laurent Wauquiez, au moment du très beau programme des investissements d'avenir. Enfin depuis 2012 je suis membre du collège de l'ARCEP, Autorité de régulation des communications électroniques et des postes. J'ai longtemps été immergé dans la théorie et les applications de l'informatique, je

cherche aujourd'hui à mieux comprendre en quoi la pensée informatique a transformé les réseaux de télécommunications. Après l'interface entre mathématiques et informatique, me voici dans la convergence de l'informatique et des télécoms ! Ce qui ne m'empêche pas de continuer à enseigner la cryptologie et de participer aux grandes conférences de la discipline.

[. . .] Dans le monde de la connaissance, quelle est aujourd'hui la place de la cryptologie ? Elle était intimement liée à l'informatique des commencements, on l'a bien vu. Elle reste présente dans l'agora virtuelle constituée par l'Internet et le web, à tel point qu'on peut véritablement parler d'ubiquité de la cryptologie. Chacun d'entre nous l'utilise – sans le savoir – dans nombre de gestes de la vie quotidienne : en téléphonant avec son portable, en payant avec sa carte bancaire, en faisant des achats sur le Net. À l'heure où sont envisagés la création d'identités numériques et l'archivage massif de nos données personnelles, notamment médicales, elle est aussi appelée à jouer un rôle essentiel pour la protection de nos libertés, afin que ces données ne soient accessibles qu'à ceux qui ont le besoin d'en connaître. Elle n'est plus seulement la science du secret mais aussi la science de la confiance [. . .].

Discours prononcé par Jacques Stern le 13 décembre 2006
lors de la remise de la médaille d'or du CNRS,
`http://www.di.ens.fr/users/stern/data/discours-or-1312.pdf`

V. S. : *Comment voyez-vous l'avenir de la cryptologie française, elle a un bel avenir ?*

J. S. : Pendant longtemps quand je rencontrais un Français en conférence, je le connaissais et il avait été formé dans notre laboratoire à l'École normale supérieure ou à l'INRIA. Aujourd'hui, c'est le signe d'une communauté plus large, je rencontre de plus en plus de Français que je ne connais pas...

Pour aller plus loin voir notamment

Jacques Stern, *Fondements mathématiques de l'informatique*, Paris, Mac Graw Hill, 1990.
Jacques Stern, *La science du secret*, Paris, Odile Jacob, 2004.
Le site personnel de Jacques Stern : `http://www.di.ens.fr/users/stern/`