

**Visite du Professeur Jacques Stern :
Programme "Distinguished Lecture",
Fondations Wenner-Gren.
20-22 novembre 2007**

M. Jacques Stern, professeur d'informatique et de cryptologie à l'Ecole Normale Supérieure (ENS) de Paris, et nouveau président de l'ANR (Agence Nationale de la Recherche), fut invité, sur proposition de l'AFSR, par les Fondations Wenner-Gren. Il rencontra ses homologues suédois et donna deux conférences à l'Ecole Royale Polytechnique (KTH) à Stockholm et à l'université de Lund (LTH). Le programme fut élaboré par l'AFSR en concertation avec les interlocuteurs suédois.

Le 21/11, lors de la visite d'Ericsson Research à Kista (Stockholm), M. Jacques Stern rencontra une dizaine de spécialistes représentant différents laboratoires de recherche. Il visita ensuite le Demo Center où les dernières inventions dans le domaine de la téléphonie mobile furent présentées par un spécialiste. Ce dernier montra également les deux futurs bateaux d'Ericsson (encore en construction) qui seront testés pour la Volvo Ocean Race de 2008-2009.

M. D. Delbourg, Ambassadeur de France, offrit ensuite un déjeuner auquel furent invités le professeur J. Håstad (KTH) et M. M. Näslund (Ericsson Research). Le professeur B. Daneholt des Fondations Wenner-Gren avait dû tardivement décliner l'invitation, mais souligna qu'il était sensible à la bonne entente existant entre l'ambassade et l'AFSR.

L'après-midi, à KTH, le professeur Stern donna une conférence intitulée "*Cryptography in Financial Transactions: Current Practice and Future Directions*" à laquelle participèrent 35-40 personnes. Au cours de cette conférence, il retraça brièvement l'histoire de la cryptographie et expliqua comment cette science était devenue un champ de recherche. Il donna ensuite un exemple concret de l'utilisation de la cryptologie pour les comptes bancaires et les paiements. Il décrivit les progrès de la recherche durant ces 30 dernières années et expliqua les questions qu'elle avait dû résoudre pour arriver à des niveaux de sécurité toujours plus hauts. Des discussions suivirent la présentation.

Le soir, M. Stern dîna avec les professeurs E. Sandewall, président de l'AFSR, P. Omling, directeur général du Conseil suédois pour la recherche (VR) et J. Håstad (KTH, VR).

La conversation se déroula dans une ambiance positive et cordiale. M. Stern résuma l'organisation de la recherche en France et souligna que la vocation de l'ANR est de financer des projets de recherche fondamentale, en précisant qu'il n'y a aucune concurrence avec le CNRS. Les représentants suédois résumèrent l'organisation de la recherche en Suède (suite à la réforme de 2001) et parlèrent de leurs nombreux contacts aussi bien avec les représentants de l'ANR qu'avec ceux du CNRS. Les rencontres sont fréquentes au niveau européen.

M. Stern souligna qu'après la période de démarrage, l'ANR a étudié la recherche conduite en Allemagne. A son retour, il va suggérer à Mme J. Lecourtier, Directrice générale, de s'intéresser de plus près aux priorités de la recherche suédoise.

Le deuxième jour, M Jacques Stern se rendit à Lund où il rencontra ses collègues d'Ericsson Mobile Platform (EMP) et ceux de l'université technologique de Lund (LTH). Des discussions informelles eurent lieu avec les chercheurs aussi bien avant qu'après son exposé. Celui-ci porta

sur le même thème qu'à KTH: "*Cryptography in Financial Transactions: Current Practice and Future Directions*". Une cinquantaine de participants (chercheurs, représentants de l'industrie et quelques étudiants) assistèrent à la conférence qui fut suivie d'échanges entre experts.

M. Jacques Stern, qui n'était pas venu en Suède depuis plusieurs années mais qui rencontre des collègues suédois dans plusieurs projets européens, remercia les Fondations Wenner-Gren et l'AFSR pour l'organisation de cette visite. Enfin, en sa qualité de Président de l'ANR, il souhaite développer les contacts avec la Suède dans le domaine de la recherche fondamentale.

COMMENTS

ERICSSON, Kista (Stockholm) / Dr Mats Näslund

Prof. Stern was welcomed to Ericsson (Kista). We had a one hour presentation of Ericsson Research in general and the security / cryptography research in particular. Prof. Stern showed great interest in several of our topics, e.g. usability aspects of security /cryptography. We also proposed some new problems in cryptography of interest to Ericsson, and we hope in the near future to investigate the potential of research collaboration with prof. Stern's group at ENS on these matters.

The visit to Ericsson continued by a live demonstration of the new possibilities with "Mobile Multimedia" over the 3GPP IP Multimedia System and 3G/HSPA radio networks, e.g. IP TV broadcast, Mobile Presence services, etc.

We concluded by an "entertainment" activity in the shape of a presentation of Ericsson's effort (as part of marketing strategy) to build and enter two sail boats to the 2008 Volvo Ocean Race. An overview visit to the boat yard was included.

KTH, Stockholm / Prof. Johan Håstad

Prof. Jacques Stern besökte skolan för datavetenskap och kommunikation på KTH under eftermiddagen 21 november. Han gav ett mycket uppskattat seminarium om kryptografins utveckling när det gäller bankomat- och betalkort. Efter seminariet fördes informella diskussioner på institutionen.

ERICSSON, Lund / Prof. Ben Smeets

Prof. Stern visited Ericsson Mobile Platform (EMP) for two hours. One hour was used to explain the research that is done at Ericsson in Lund and in particular the security areas we are active in. Prof. Stern was explained how boundary conditions for high volume consumer products may turn straightforward cryptographic problems into very challenging ones. We spent the rest of the time on discussing potentials of security processors in mobile phones and the use of the phone in e-payment solutions in particular and NFC based solutions in general. We also discussed DRM solutions and how realistic we can be in hoping they actually can achieve what one wants to achieve.

LTH, Lund / Prof Thomas Johansson

Prof. Stern was picked up at the hotel in Lund. He had a one hour discussion with the crypto group at the department before he continued to visit Ericsson Mobile Platform (EMP).

After lunch Prof Stern gave his seminar. It was attended by about 50 people, researchers, industry representatives as well as some students. After the seminar we had another half hour of discussion, before Prof. Stern continued to the airport.