Rapport sur l'École de Recherche CIMPA
Cryptographie
Oujda (Maroc)
du 18 au 29 mai 2009

Michel Waldschmidt

Une école de recherche CIMPA a été organisée à Oujda du 18 au 29 mai 2009. Le programme prévu est rappelé en annexe. Le principal organisateur était Abdelmalek Azizi (Professeur à l'Université Mohammed Premier, Oujda). La première semaine, les cours ont été donnés comme prévu par Abdelmalek Azizi, Alexis Bonnecaze, Johannes Buchmann, Gerhard Frey, Abderrhamane Nitaj et Robert Rolland. Le programme de la seconde semaine a été modifié en raison du forfait de Jean-Jacques Quisquater. En plus du cours prévu de Juan Tena, les autres cours ont été donnés par Mostafa Azizi (cryptographie quantique), M. El Maraki (Cryptographie et groupes de tresses), Ayoub Otmani (cryptographie et codes correcteurs) et Pascal Veron (cryptographie appliquée).

Le premier jour, il y a eu plus de 80 participants, la séance d'ouverture ayant lieu dans un amphithéâtre de l'Université. La seconde semaine, le nombre de participants a oscillé entre 30 et 40.

Une quarantaine de candidats extérieurs au Maroc ont demandé à participer à cette école ; 19 candidats ont été sélectionnés, 12 sont venus: 6 participants venaient d'Algérie, 2 de Tunisie, 2 du Sénégal et 2 de Mauritanie. Parmi ces 12 participants, il y avait 3 femmes. Plusieurs candidats sélectionnés et financés se sont désistés. Aucun des candidats ayant été admis sans financement n'est venu.

Sur les 29 participants marocains ayant rempli une fiche, il y en avait 14 d'Oujda, 5 de Fes, 3 de Rabat, 3 de Meknes, 1 de Taza, 1 d'Errachidia, 1 de Nador et 1 de Tétouan. La répartition géographique est satisfaisante, cette école aura un bon impact local.

L'essentiel des activités a eu lieu dans l'hôtel Isly Golf qui offre de bonnes conditions pour ce genre de rencontres, c'est un hôtel de bonne qualité sans être trop cher. L'hôtel plus simple mais convenable au centre ville, où j'avais été logé il y a 3 ans pour un colloque de théorie des nombres, n'accepte plus d'héberger des colloques de l'Université, car quand celle-ci honore ses factures, elle le fait avec un délai trop important. Deux séances de cours la première semaine et une séance de TD sur ordinateurs la seconde ont eu lieu à l'Université.

La connexion internet de l'hôtel était de bonne qualité. L'hôtel possède un générateur en cas de panne de courant. Il n'y a eu qu'une coupure d'eau un matin de la seconde semaine. La salle de conférence est bien équipée pour une vidéo projection, mais le tableau blanc qui peut servir comme complément est nettement insuffisant, comme c'est presque toujours le cas dans ce genre de situation.

Le niveau des cours a semblé bien adapté aux étudiants, d'après les retours que j'ai eus. Je n'ai pu être présent que la seconde semaine, j'ai assisté à tous les cours qui m'ont personnellement intéressé. J'ai appris beaucoup de choses sur les liens entre d'une part la cryptographie et d'autre part les tresses, les courbes elliptiques ou les codes correcteurs d'erreurs, ainsi que sur la sécurité des cartes électroniques. La fatigue s'est un peu fait sentir chez les participants, après deux semaines de 5 jours avec 4 cours quotidiens d'une heure et demie quotidiennement; le programme des derniers jours a été allégé.

Une seule séance sur ordinateurs était programmée, la seconde semaine, à l'Université, organisée par Pascal Véron. Les ordinateurs en état de fonctionner n'étaient pas suffisamment nombreux. Malgré l'intérêt évident de ce genre de complément aux cours théoriques, les difficultés matérielles justifient qu'il n'y ait pas eu plus de séances pratiques.

De la documentation a été fournie aux étudiants au début, mais seulement sous forme de CD, qu'ils ne pouvaient pas exploiter sur place. Les intervenants n'avaient pas fourni à temps le matériel nécessaire pour être photocopié et distribué. Distribuer des photocopies à chaque participant aurait aussi induit un surcoût, et le budget de l'école était très serré. Un second CD était prévu en fin d'école, mais là encore les enseignants n'ont pas tous donné leurs textes – ils seront disponibles sur internet, soit sur le site de l'école

<http://sciences1.univ-oujda.ac.ma/CIMPA/index.htm>

soit sur celui du CIMPA

<http://www.cimpa-icpam.org/spip.php?article142>

L'organisation de cette école de recherche a demandé énormément de dévouement et d'inventivité de la part de l'organisateur local. C'est Abdelmalek Azizi qui a fait tout le travail jusqu'à un mois avant la tenue de l'école. Pour le dernier mois et pendant la durée de cette école, il a été aidé par un bon nombre de ses collègues de l'Université d'Oujda.

Budget de l'école

Pour parvenir à équilibrer le budget, l'organisateur a dû dépenser une énergie incroyable et solliciter un grand nombre d'organismes, avec un succès étonnant. Par exemple, il est parvenu à loger gratuitement un bon nombre de participants dans un centre sportif, d'autres à l'Université. Il a sollicité de nombreux organismes pour obtenir des financements, il a négocié fermement avec l'hôtel pour obtenir des conditions acceptables dans la limite de son budget.

Financement par le CIMPA : 8836 Euros, à savoir

- Nuits d'hôtel de 10 participants : 2900 Euros
- Repas pour 13 participants : 2976 Euros
- Voyages pour 8 participants : 2960 Euros

Budget total de l'école : 31 026 Euros.

Sources de financement autres que le CIMPA : FSO, UMP, Labo ACSA, Ambassade de France, Tempus, ICTP, IMU, Académie Hassan II, CNRST, Département de Mathématiques, Agence Orientale.

Merci

À Abdelmalek Azizi qui a été le maître d'œuvre de cette école et qui peut légitimement être fier du succès.

A ses collègues de la Faculté des Sciences d'Oujda et à tous les membres du comité d'organisation qui ont permis que cette école se déroule dans d'excellentes conditions.

A l'Ambassade de France qui a contribué au financement de cette école, notamment en remboursant ma propre mission.

Aux partenaires du CIMPA qui ont apporté leur soutien financier : le CIMPA n'a pas les moyens à lui seul d'organiser une telle école de recherche, les partenaires jouent un rôle irremplaçable.

Aux intervenants qui ont donné des cours très appréciés par les participants. On demande beaucoup aux collègues qui acceptent de donner des cours : ils doivent les préparer, les rédiger et distribuer leurs notes aux étudiants, on leur demande aussi dans la mesure du possible de trouver des financements pour leurs missions. Et on ne leur donne pas

de compensation, autre que la joie de transmettre leurs connaissances. Seules des personnes motivées et désintéressées peuvent accepter de telles conditions !

Je termine en adressant tous mes vœux de meilleure santé à Günther Frei, membre du comité scientifique.

Annexe : présentation selon le site du CIMPA (avant la tenue de l'école)

<http://www.cimpa-icpam.org/spip.php?article142>

Objectifs :

Depuis longtemps, l'Arithmétique, la Géométrie et l'Algèbre ont joué et jouent encore un grand rôle dans notre vie courante. Le développement économique, social et culturel des différentes civilisations a été réalisé, entre autres, grâce au développement de ces trois disciplines de Mathématiques. Actuellement, le commerce électronique, les transmissions, les transactions bancaires, la sécurité des réseaux, la sécurité des fichiers et des bases de données, etc., se basent essentiellement sur ces trois disciplines à travers la cryptographie.

La cryptographie est un domaine de recherche très diversifié et possède des applications industrielles très importantes (cartes à puces, cartes d'identité, passeport biométrique...). C'est un domaine, parmi tant d'autres, d'application de la Théorie des Nombres, la Géométrie et l'Algèbre.

Pour cela, il est intéressant d'orienter une partie des activités de recherche théorique des Laboratoires d'Algèbre, de Théorie des Nombres et de Géométrie, des pays voisins du Maroc vers une recherche qui a des applications industrielles comme celle de la Cryptographie.

Organisateurs :

A. Azizi (Université Mohammed Premier, FSO Oujda - Maroc), M. Azizi (Université Mohammed Premier, ESTO Oujda - Maroc), M. C. Ismaili (Université Mohammed Premier Oujda - Maroc), C. Levesque (Université Laval, Québec-Canada)

Comité scientifique :

A. Azizi (Oujda, Maroc), J. Buchmann (Darmstadt, Germany), Gerhard Frey (Duisburg-Essen, Germany), Gunther Frei (Université Laval, Canada), Jean-Jacques Quisquater (Bruxelles, Belgique), R. Rolland (Marseille, France), A. Nitaj (Caen, France), Juan Gabriel Tena Ayuso (Valladolid, Spain).

Comité local d'organisation :

M. Ayadi, A. Azizi, M. Azizi, M, Ziane, Mr. Chellali, M.C. Ismaili, A. Lidouh, A. Addou, E. Idrissi, M. Amrani, M. Zaoui.

Langue de travail :

Anglais, Français

Date et lieu :

18-30 mai 2009, Faculté des Sciences, Université Mohammed premier, Oujda (Maroc)

Programme scientifique :

- *Histoire de la cryptographie au Maroc* par Abdelmalek Azizi (Université Mohammed Premier, Oujda)
- *L'organisation de la cryptographie moderne* par Robert Rolland (IML, Marseille, France)
- *La cryptanalyse du cryptosystème RSA* par A. Nitaj (Université de Caen, France)

- *Arithmétique et cryptographie* par Robert Rolland et Alexis Bonnecaze (IML, Marseille, France)
- *Cryptographie appliquée* par Jean-Jacques Quisquater (Université de Louvain-la-Neuve, Bruxelles, Belgique).
- *Methods of Arithmetic Geometry applied to Public Key Cryptography* by Gerhard Frey (IEM, Essen, Allemagne)
- *Elliptic Curve Cryptography : some cryptographical protocols* by Juan Gabriel Tena Ayuso (Univ. of Valladolid, Spain).
- *Quantum Immune Cryptography* by Johannes Buchmann (Darmstadt, Germany)

Prérequis :
Pour la plupart des cours, les prérequis sont les connaissances de base en Arithmétique, Algèbre et Géométrie. Les stagiaires seront choisis parmi les doctorants, les chercheurs et les enseignants chercheurs.

Mise à jour: 03/06/2009

Ce texte est disponible sur le site
<http://people.math.jussieu.fr/~miw/cooperations.html>