

Colloque du
Département d'informatique et de recherche opérationnelle

Alain Tapp

Département IRO, Université de Montréal

Les mathématiques de la vie privée

Résumé : Une quantité impressionnante d'informations nous concernant s'accumule sur de multiples serveurs. Je parle ici de courriels, de publications sur des réseaux sociaux, d'informations financières, de transactions, de diplômes, de permis, de l'impôt, d'information médicale, de vidéos de surveillance, etc. Une entité comme « big brother » ayant accès à toute cette information est une perspective terrifiante. Paradoxalement, cette information pourrait dans bien des cas être utilisée pour l'avancement de l'humanité, la science et la recherche, notre santé, notre sécurité, la planification urbaine et sociale et notre bien-être général. Un des buts avoués de la cryptographie est de produire des protocoles qui simulent « big brother » dans des contextes utiles, en le remplaçant par un être virtuel honnête et bienveillant. Je vais aborder dans ma conférence certains aspects particulièrement surprenants de cette science complexe.



Le jeudi 21 mars 2013, 15h30, pavillon André-Aisenstadt, salle 3195

Information : Gilles Brassard, brassard@iro.umontreal.ca