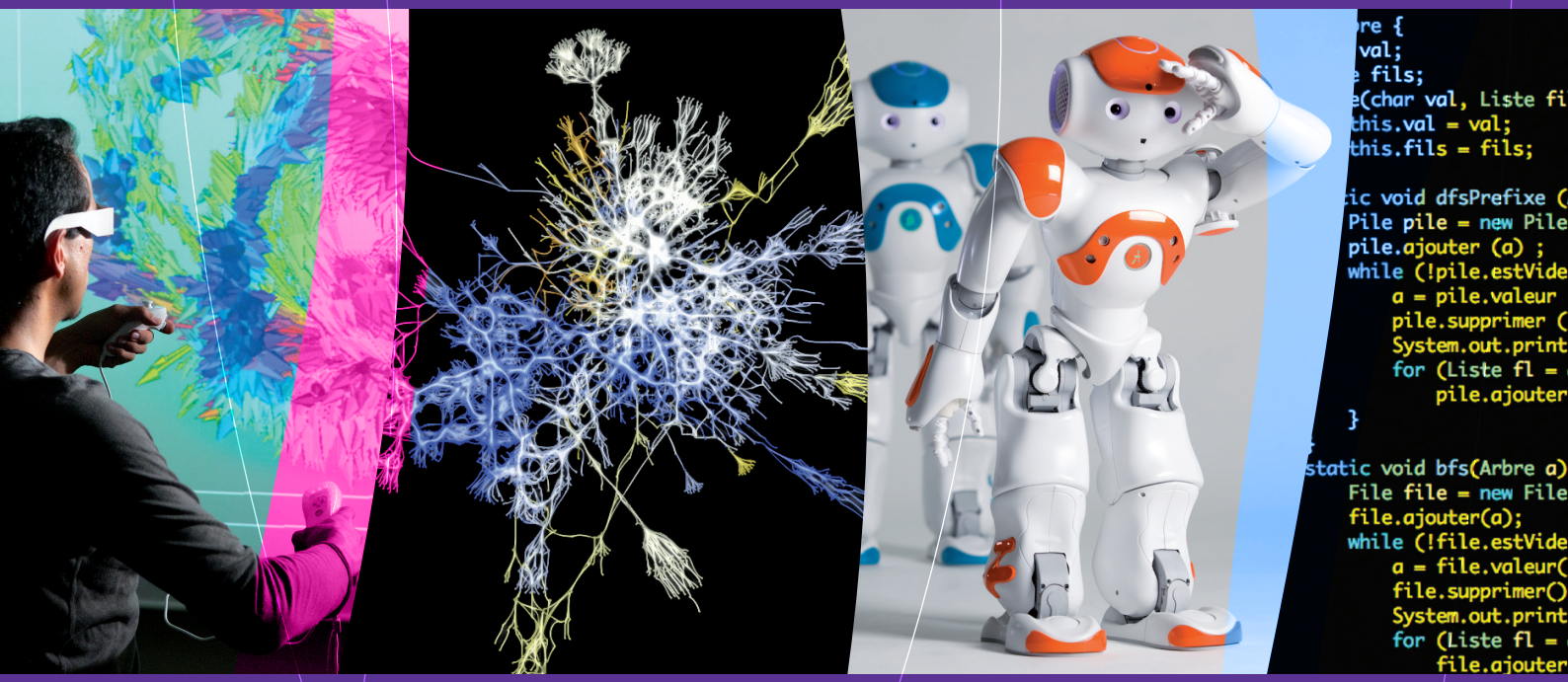
INS2I

Institut des **sciences** de **l'information** et de **leurs interactions**



Sélection

Faits marquants 2015

www.cnrs.fr

Sommaire

14/04/15 – PPS – CNRS le Journal, billet par Roberto Di Cosmo

Reprenons le contrôle de nos données

Nos téléphones portables, ordinateurs, cartes bancaires ou de fidélité collectent chaque jour de nombreuses informations qui en disent long sur nous. Comment éviter les utilisations abusives et garder le contrôle de nos données personnelles ? Spécialiste du logiciel libre, Roberto Di Cosmo nous livre son analyse et invite la communauté scientifique à s'emparer de la question.

Les technologies liées à l'informatique évoluent à une vitesse vertigineuse : la taille de la mémoire et de l'espace disque disponible, la puissance de calcul et la vitesse d'échange des informations ont gagné chacune deux ordres de grandeur en seulement dix ans. Nous avons produit, stocké, élaboré, échangé et exploité plus de données cette dernière année que dans toute l'histoire de l'humanité.

Nous nous sommes habitués au fait que, en termes d'information, l'échange et l'accès priment sur la possession : la mise en réseau d'un nombre croissant de services, chaque jour plus riches, et notre hyperconnectivité font en sorte que nous utilisons les moteurs de recherche, les sites Web, les services en ligne et les réseaux sociaux comme une extension naturelle de nos capacités intellectuelles. Nous profitons d'une mise à jour constante des informations, qui rendrait rapidement obsolète toute copie, même complète, qu'on pourrait réaliser à un moment donné.

En contrepartie, une partie grandissante de nos informations personnelles se retrouve elle aussi numérisée, mise en ligne, et rendue disponible. Certaines informations sont entre les mains de l'État, comme notre dossier fiscal, judiciaire et d'état civil, mais d'autres sont collectées par des acteurs privés avec notre participation active, quoique souvent non informée : notre profil de consommation, nos goûts culturels, nos préférences politiques et notre réseau de connaissance sont facilement identifiables par l'analyse des très nombreuses traces que nous laissons chaque jour derrière nous, via les cartes de fidélité, les cartes bancaires, les abonnements de transport, les mots clés dans les moteurs de recherche, les messages sur les réseaux sociaux, les documents partagés en ligne, les échanges de courriels et les communications téléphoniques.

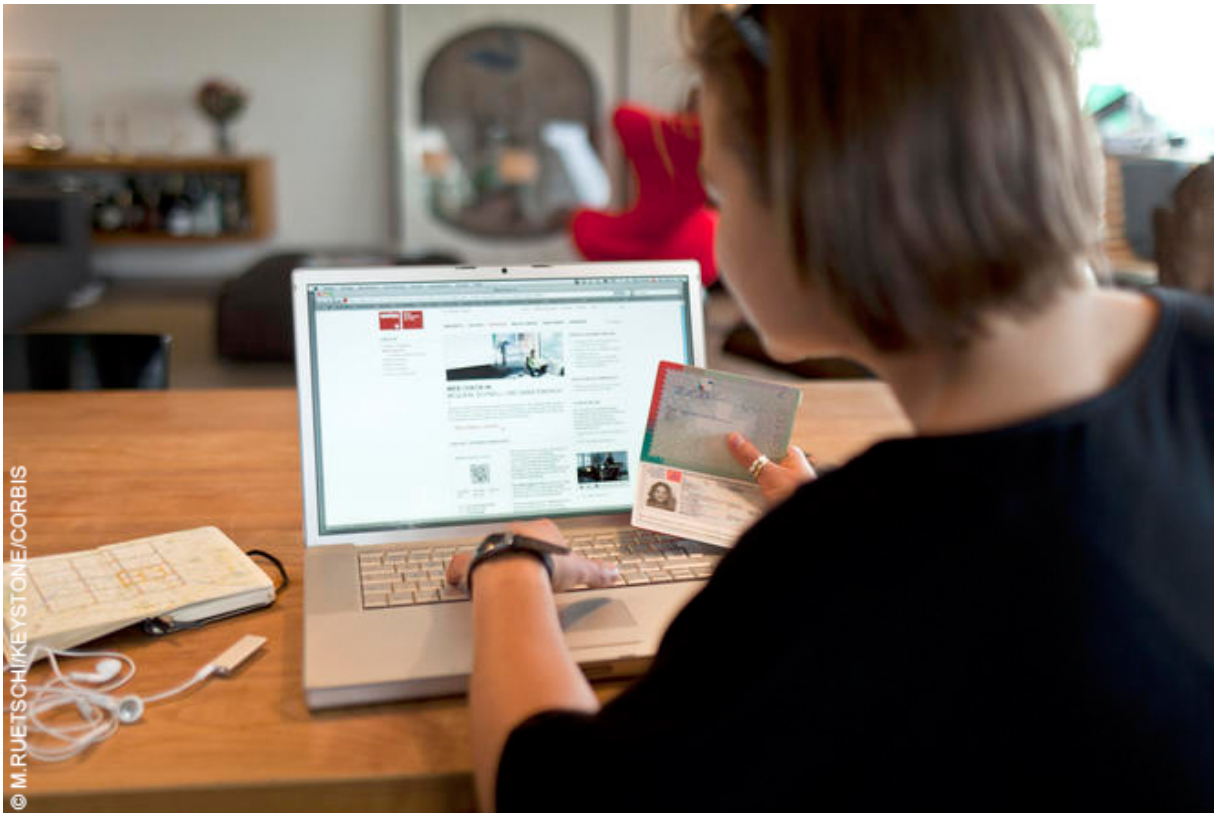
Une invasion sans précédent de la vie privée

La concentration de toutes ces informations dématérialisées dans des infrastructures centralisées disposant de moyens de calcul énormes rend possibles à la fois l'émergence de services de grande utilité sociale et une invasion sans précédent de notre vie privée : en analysant les requêtes des internautes, Google peut suivre l'avancée d'une épidémie de grippe ; en collectant des informations précises de localisation depuis les téléphones connectés, il sait tracer une carte fidèle du trafic, nous indiquer les bouchons et fluidifier ainsi les transports routiers.

Mais ces mêmes données peuvent être utilisées pour dresser un profil de santé très précis d'un individu et suivre tous ses déplacements : les usages de ces informations individuelles sont bien plus inquiétants. En 2012, le fait que la chaîne de supermarché Target, en exploitant les données collectées via les cartes de fidélité, pouvait identifier les femmes enceintes avant que leur famille n'en soit mise au courant avait fait scandale aux États-Unis ; les révélations de Snowden nous apprennent que la NSA connaît notre réseau de relations mieux que nous-mêmes.

On a déjà connu de par le passé des régimes totalitaires qui cherchaient à contrôler chaque aspect de la vie et de la pensée des individus, mais cela coûtait très cher et engendrait de la méfiance. Le changement majeur permis par l'évolution technologique à laquelle nous assistons, et contribuons, est que ce contrôle peut être poussé beaucoup plus loin, pour bien moins cher, et sans susciter de méfiance, parce que la collecte des données nécessaires s'accompagne presque toujours d'une offre de service utile, pratique et à première vue gratuite. Derrière la gratuité monétaire pour les utilisateurs des services se cache en effet très souvent un modèle économique basé sur la connaissance fine des profils de ces utilisateurs, qui sont ensuite exploités de différentes formes. Comme le disait déjà bien Bruce Schneier en 2010, à propos de la politique de confidentialité de Facebook, *« If you dont pay for the product, you are the product »*.

Avec la généralisation des objets connectés, montres, balances, podomètres et autres bracelets et senseurs, l'étendue des données personnelles susceptibles d'être captées s'élargit à perte de vue, et les aspects les plus intimes de notre vie privée, comme notre santé, commencent déjà à être percés à jour.



Renforcer la protection des données personnelles

Plusieurs initiatives essayent de limiter ou d'encadrer la concentration des données et mieux protéger nos informations personnelles, mais il y a encore beaucoup de naïveté, que nous nous devons de dépasser, sur différents sujets :

Le pouvoir limité des lois

Un cadre légal est essentiel et doit affirmer les principes qui séparent ce qui est acceptable de ce qui ne l'est pas, et la directive européenne sur la protection des données est un bon point de départ. Mais une loi n'est pas en soi un rempart suffisant : les acteurs, publics ou privés, qui collectent nos données peuvent être forcés à les fournir par des pressions de diverse nature, se les faire dérober par des cybercriminels, ou tout simplement les dévoiler au grand jour par des erreurs humaines. Et pour les données personnelles critiques, il suffit de les

exposer une fois pour que leur confidentialité soit perdue pour toujours. Pouvons-nous développer des technologies qui nous assurent que les principes établis dans les lois soient effectivement respectés dans les faits ?

L'illusion de l'anonymat

Divers groupes d'intérêts font pression pour qu'on rende disponibles un grand nombre de données collectées par les différents opérateurs publics afin de faciliter l'essor de jeunes pousses dans le domaine du Big Data. Pour éviter de porter atteinte à la vie privée, on nous dit qu'il suffirait de les anonymiser. Mais la nature unique de l'expérience de chacun d'entre nous rend une véritable anonymisation des données très difficile à réaliser : selon une étude récente (link is external), pour identifier complètement la trace GSM d'une personne dans une base de données anonymisée, il suffit juste de la localiser, avec une certaine précision, quatre fois dans le courant d'une année. Pouvons-nous développer des outils théoriques et pratiques qui nous permettent de connaître exactement quelles informations personnelles on peut extraire en combinant une base de données anonymisée avec plusieurs autres sources externes ?

Les logiciels libres et le Cloud

Le logiciel libre, avec l'accès aux sources, nous aide à comprendre ce qu'on fait de nos données, mais, comme le notait très justement Ken Thompson il y a déjà trente ans[1], on ne peut imaginer faire confiance à un logiciel que s'il est exécuté sur nos propres machines et dans un environnement dont on a la maîtrise totale. Mais du logiciel libre qui tourne hors de notre contrôle ne nous offre aucune protection : la plupart des acteurs dominants d'aujourd'hui, comme Google, Facebook, Amazon et Apple, utilisent massivement du logiciel libre dans leurs serveurs, et nos données ne s'en trouvent pas mieux protégées pour autant. Il est très naïf de penser que la solution à nos problèmes serait de remplacer une connaissance centralisée chez un de ces géants par une connaissance centralisée chez d'autres géants, et encore plus chez de petits hébergeurs, moins armés face aux cyberattaques.

Le difficile équilibre entre l'intérêt général et l'intérêt privé

Pouvons-nous trouver les moyens scientifiques et technologiques pour que nous puissions marier les avantages des infrastructures centralisées tout en gardant le contrôle sur l'usage qui peut être fait de nos données privées ? Pour résumer, aujourd'hui plus que jamais, il est important de savoir qui possède nos données, et lesquelles ; qui peut utiliser ces données, et dans quels buts ; qui contrôle les logiciels qui collectent, transmettent et analysent ces données, et par quels moyens.

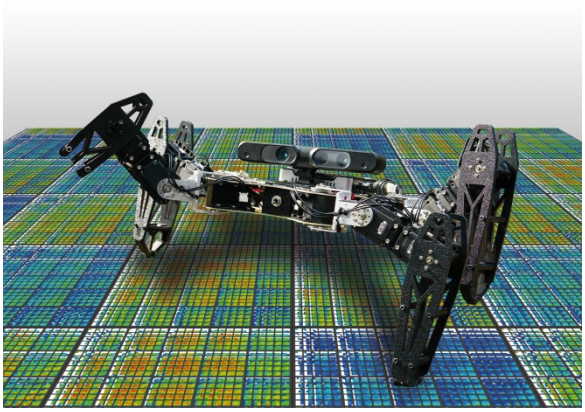
Il est important de donner aux individus les moyens nécessaires pour qu'ils puissent décider, de façon informée, quelles sont les informations qu'ils souhaitent partager, avec qui et pour quels usages. Et il est important de développer les connaissances et la technologie nécessaires pour permettre à chaque individu de s'assurer que ses décisions sont effectivement respectées, sans qu'il soit obligé de faire confiance à des tiers.

Pour tout cela, notre société a besoin de l'aide de la communauté scientifique, et nous pose un défi qui est à la fois noble et stimulant : développer les connaissances scientifiques, technologiques et sociologiques nécessaires pour trouver, et réaliser efficacement, le juste équilibre entre l'usage agrégé de nos données personnelles, qui peut servir l'intérêt général, et la protection de notre vie privée contre les intrusions de plus en plus généralisées qu'elle subit.

[1] *"Reflections on Trusting Trust"*, Ken Thompson, *Communication of the ACM*, août 1984, vol. 27 (8) : 761-763.

28/05/15 – ISIR – Communiqué de presse

Des robots qui s'adaptent aux dommages en quelques minutes



Les robots pourraient aider notre société dans de nombreuses situations, par exemple pour chercher des survivants après des catastrophes naturelles ou pour alerter les pompiers en cas de feu de forêt. Néanmoins, ils resteront cantonnés aux laboratoires de recherche tant qu'ils ne seront pas capables de continuer à fonctionner lorsqu'ils sont endommagés. Des chercheurs de l'Institut des systèmes intelligents et de robotique (CNRS/UPMC) et du Laboratoire lorrain de recherche en informatique et ses applications (CNRS/Inria/Université de Lorraine) montrent comment des robots peuvent automatiquement s'adapter aux dommages en moins de deux minutes. Leurs résultats sont publiés dans *Nature*[2] le 28 mai 2015.

Contrairement aux robots actuels, les êtres vivants ont une impressionnante capacité d'adaptation aux blessures. Ainsi, la plupart des chiens amputés d'une patte sont capables de jouer, sauter, et courir ; et un enfant avec une cheville foulée n'a besoin que de quelques minutes pour trouver une manière de boiter. Les chercheurs se sont inspirés de ces exemples. *« Quand les animaux sont blessés, ils ne partent pas de zéro pour s'en sortir »*, explique Jean-Baptiste Mouret. *« Au contraire, ils ont de bonnes intuitions sur les différentes manières de réagir. Ces intuitions leur permettent de choisir intelligemment quelques comportements à essayer et, après quelques tests, ils arrivent à en trouver un qui fonctionne malgré la blessure. Nos robots font la même chose. »*

Avant d'être envoyé en mission, le robot utilise une simulation de son corps pour créer une « carte » détaillée des milliers de manières différentes de réaliser sa tâche : cette carte représente les intuitions du robot concernant les comportements intéressants et leur potentiel. Si le robot est endommagé, il utilise ses intuitions pour guider un algorithme d'apprentissage qui réalise des expériences afin de découvrir rapidement un comportement de compensation. Le nouvel algorithme a été baptisé *« Intelligent Trial and Error »* (essai-erreur intelligent).

« S'il est endommagé, notre robot se comporte comme un scientifique », explique Antoine Cully. *« Il a des a priori à propos des différentes actions qui pourraient fonctionner et il commence par les tester. Cependant, ces à priori viennent de la simulation du robot intact. Il doit donc trouver celles qui fonctionnent non seulement en réalité mais aussi avec le/les dommages. Chaque action qu'il essaie est comme une expérience qui confirme ou infirme ses hypothèses. Si une action ne fonctionne pas, l'algorithme élimine de manière intelligente des catégories entières d'action pour essayer des choses complètement différentes.*

Par exemple, si marcher en s'appuyant essentiellement sur les pattes arrières ne fonctionne pas correctement, le robot essaiera alors de marcher en mettant son poids sur les pattes avant. Ce qui est surprenant, c'est la rapidité avec laquelle le robot découvre une nouvelle manière de marcher : malgré une patte coupée en deux, il ne faut que deux minutes au robot pour trouver une manière efficace de boiter ! »

[2] Cully, A., Clune, J. Tarapore, D. and Mouret, J.-B. *Robots that can adapt like animals*. Nature, 2015. (article de couverture)

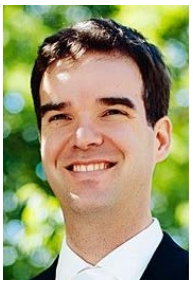
Jeff Clune explique que *« techniquement, l'algorithme est divisé en deux étapes : (1) créer la carte de l'espace comportement performance, et (2) l'adaptation à la nouvelle situation »*. La carte de la première étape est créée avec un nouveau type d'algorithme évolutionniste appelé MAP-Elites. Ce type d'algorithme s'inspire de l'évolution darwinienne et de la « survie du plus apte » pour chercher des solutions performantes. L'adaptation dans la seconde partie s'appuie sur un algorithme d'optimisation « bayesienne », qui exploite les connaissances a priori fournies par la carte pour trouver rapidement un nouveau comportement. *« Nous avons effectué des expériences qui montrent que le point clé est dans la création et l'exploitation des a priori »*, continue Jeff Clune. Cette nouvelle technique pourra contribuer à développer des robots autonomes plus robustes et plus efficaces. Danesh Tarapore donne quelques exemples. *« Cela pourrait permettre la création de robots qui peuvent aider des secouristes sans nécessiter leur attention en permanence »*, dit-il. *« Cela pourrait aussi faciliter la création d'assistants robotiques personnels qui peuvent continuer à être utiles même quand une pièce est cassée. »*

Ce travail a reçu l'aide de l'Agence Nationale pour la Recherche (Creadapt, ANR-12-JS03-0009), de l'*European Research Commission* (ResiBots, grant agreement No 637972), et de la Direction Générale de l'Armement (thèse de A. Cully).

Pour en savoir plus, une vidéo illustrant ce travail : Un robot à 6 pattes réapprend à marcher avec une patte abîmée et une patte manquante. L'expérience est répétée avec un bras robot apprenant à correctement placer un objet malgré plusieurs moteurs coincés.

30/07/15 – CRIStAL – cnrs.fr/ins2i

Une avancée en équivalence de requêtes pour interroger les données sur le web distinguée à IJCAI 2015



Utiliser le champ « recherche » d'un site web fait appel à des mécaniques complexes insoupçonnées. En particulier, l'ordinateur doit trouver les bonnes informations à travers un très grand nombre de données. Pour vous donner une réponse rapidement, l'ordinateur recherche souvent une requête équivalente à la vôtre, mais moins gourmande en calcul. La publication *« Reasonable Highly Expressive Query Languages »* de Pierre Bourhis (en photo) du Centre de Recherche en Informatique, Signal et Automatique de Lille (CRIStAL - CNRS/Université des Sciences et Techniques Lille 1), Markus Krötzsch et Sebastian Rudolph de l'Université de Dresde apporte de nouveaux résultats sur le calcul d'équivalences dans le langage de requête Datalog. Ce travail a été distingué par un *Honorable Mention* lors de l'*International Joint Conference on Artificial Intelligence* (IJCAI), conférence de référence dans le domaine de l'Intelligence Artificielle.

Depuis les années 80, les systèmes de gestion de bases de données relationnelles se sont imposés comme la technologie et paradigme principaux pour la gestion de données. Mais les besoins face aux masses de données désormais accessibles font émerger de nouvelles problématiques : il faut pouvoir y accéder facilement. Jusque-là, quand vous interrogiez un site web, votre requête était généralement évaluée sur une base de données relationnelle ce qui permettait d'identifier les informations que vous souhaitiez obtenir. Ce type de requêtes est principalement exprimé dans le langage SQL, le standard pour interroger des données relationnelles. Mais cette technologie, qui est aujourd'hui bien maîtrisée, ne permet pas de gérer certains types de données qui ont émergé récemment, en particulier les vastes graphes comme le graphe du web ou le réseau social de Facebook ou Twitter. En effet, le langage SQL a un pouvoir d'expression limité qui ne convient pas à l'interrogation moderne des données : par exemple, il n'est pas possible de rechercher un motif intéressant qui se répète ou analyser la propagation d'opinions dans un réseau.

Ces nouveaux besoins ont conduit les chercheurs à étudier d'autres langages comme SPARQL, populaire dans le web sémantique, ou Datalog, un langage de requête récursif développé dans les années 90. En raison de l'expressivité de ces langages, un requête peut prendre plusieurs minutes voir des heures à être calculer. Dès lors, le grand défi est de retourner en temps raisonnable la réponse à votre requête. Or, suivant la façon dont vous exprimez votre requête, le calcul engendré sur les données peut être très différent. Donc plutôt que d'évaluer directement la requête que vous posez, l'ordinateur va chercher à découvrir une requête équivalente optimale, c'est-à-dire qui calcule la même chose mais en prenant le minimum de temps. Malheureusement, cette optimisation de requêtes est un problème indécidable pour SQL et Datalog, c'est-à-dire qu'il n'existe pas de méthode de résolution générale.

Dans l'article *« Reasonable Highly Expressive Query Languages »*, les chercheurs prouvent qu'il est possible de déterminer si deux requêtes calculent la même chose pour une classe très expressive de requêtes Datalog appelés *Guarded Queries*. Les chercheurs se sont intéressés à Datalog, langage à la fois simple, élégant et très expressif, qui connaît un regain d'intérêt depuis quelques années aussi bien dans la recherche que dans l'industrie, car il permet de répondre à certains besoins d'interrogation actuels.

Il est essentiel de circonscrire des classes de requêtes restreintes pour lesquelles il est possible de décider l'équivalence, pour pouvoir optimiser efficacement les requêtes. Le résultat présenté dans cet article constitue donc une avancée dans ce qui constitue un défi considérable : trouver une classe de requêtes assez large pour couvrir les besoins applicatifs mais suffisamment restreinte pour que l'optimisation reste possible. En effet, la classe de *Guarded Queries* étudiée dans cette publication généralise des fragments importants SPARQL et Datalog connus pour avoir leur problème d'équivalence décidable.

03/08/15 – LSIS – cnrs.fr/ins2i

Les spécificités des cerveaux de nouveaux-nés prématurés révélées par la 3D

Les médecins savent depuis longtemps que les bébés prématurés ont sur certains aspects une morphologie particulière. Pour la première fois, une étude vient d'être menée pour comparer des IRM de cerveaux de grands prématurés avec des cerveaux de fœtus du même âge encore dans le ventre de leur mère. Des informaticiens, chercheurs en traitement des images et neurobiologistes se sont réunis autour de ce projet original dont l'article vient de paraître dans *Cerebral Cortex*, journal réputé en neurosciences.

Il est connu que le cerveau humain acquière ses circonvolutions, c'est-à-dire ses plissements caractéristiques, au cours du stade fœtal et plus exactement entre les 20ème et 40ème semaines de développement. Mais le mécanisme sous-jacent reste encore inconnu. Pour comprendre l'origine de ces plissements, et voir si ces circonvolutions peuvent être la signature d'autres phénomènes sous-jacents, des images de cerveaux obtenues par Imagerie par Résonance Magnétique (IRM) ont été collectées dans un contexte de diagnostic anténatal. L'étude *« Are Developmental Trajectories of Cortical Folding Comparable Between Cross-sectional Datasets of Fetuses and Preterm Newborns ? »*[3] réalisée dans le cadre du projet ANR MoDeGy et coordonnée par Julien Lefèvre du Laboratoire des Sciences de l'Information et des Systèmes (LSIS – CNRS/Université Aix-Marseille, Université de Toulon) et de l'Institut des Neurosciences de la Timone a permis une avancée dans cette exploration. Les chercheurs ont comparé pour la première fois, en utilisant des analyses aussi proches que possible, les cerveaux dans un groupe de fœtus et un groupe de grands prématurés (près de 3 mois avant terme) d'âge comparables. Les chercheurs ont ainsi pu mettre en parallèle les trajectoires de développement de cerveaux humains *in* et *ex utero*.

Pour arriver à ce résultat, plusieurs étapes ont été nécessaires. Tout d'abord un travail important a été réalisé sur la qualité des images d'IRM en elles-mêmes : en effet, les mouvements non contrôlables du fœtus demandaient des corrections d'artefacts sur ces images, en utilisant la résolution d'un problème inverse. Une fois les images reconstruites et « nettoyées », le logiciel Brainvisa segmentait de façon précise les différents tissus biologiques (matière grise, future matière blanche, liquide céphalo-rachidien). Le modèle numérique de la surface du cortex est alors construit. Ce modèle 3D permet d'obtenir un certain nombre de mesures quantitatives, qu'elles soient globales (volume ou aire totale) ou plus locales (courbures). Pour comparer deux modèles 3D entre eux, des recherches en modélisation géométrique ont été menées pour proposer des descripteurs locaux de la géométrie du cerveau, à l'aide de deux indices : l'indice de forme (*shape index* en anglais) et l'intensité de courbure (*curvedness* en anglais), obtenus à partir des deux courbures principales orthogonales qui définissent le plissement à chaque point.

[3] Julien Lefèvre, David Germanaud, Jessica Dubois, François Rousseau, Ines de Macedo Santos, Hugo Angleys, Jean-François Mangin, Petra S. Hüppi, Nadine Girard, et François De Guio

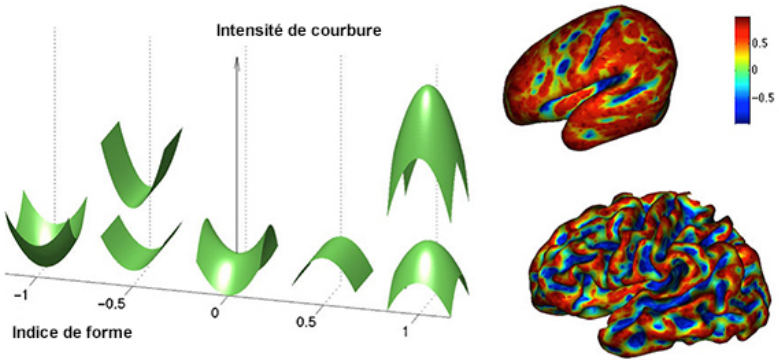


Figure 1 : Représentations schématiques des intensités de courbure et indices de forme appliqués à deux cerveaux de prématurés de 26,7 semaines de gestation et 35,7 semaines de gestation.

Il ressort des indices descriptifs que les nouveaux-nés prématurés ont un cerveau nettement plus plissé que celui des fœtus du même âge ce qui corrobore l'expertise des radiologues (voir figure 2). Néanmoins les vagues d'apparition des plis ne semblent pas différer d'un groupe à l'autre. Les résultats de cette étude suggèrent donc que la différence de milieux (in versus ex utero) pourraient être à l'origine de ces différences morphologiques observées. Ces résultats ont déjà été présentés au congrès européen de résonance magnétique nucléaire.

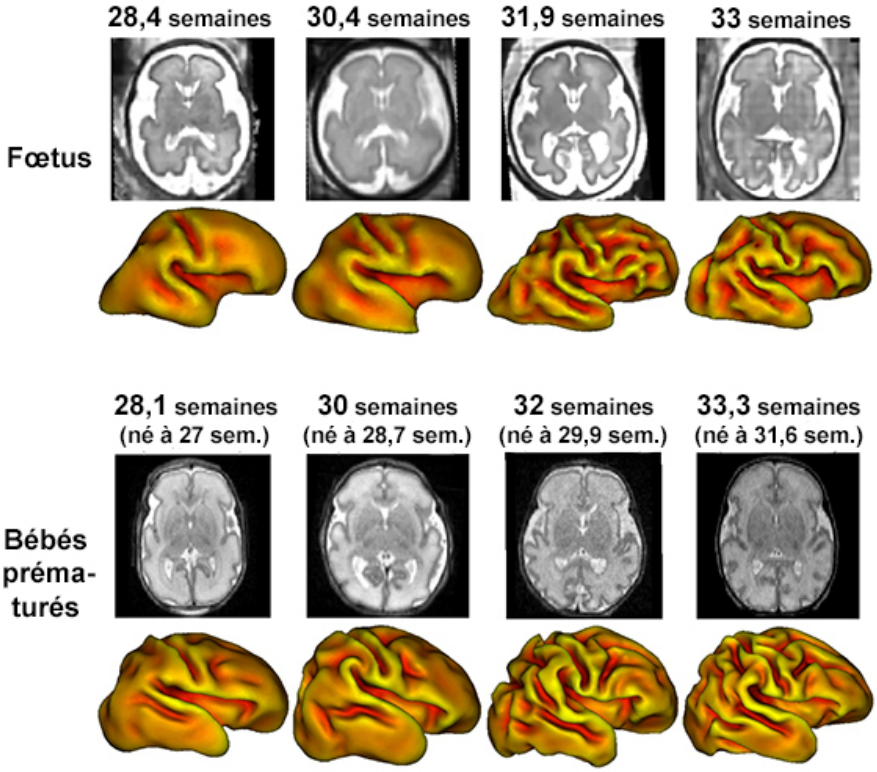


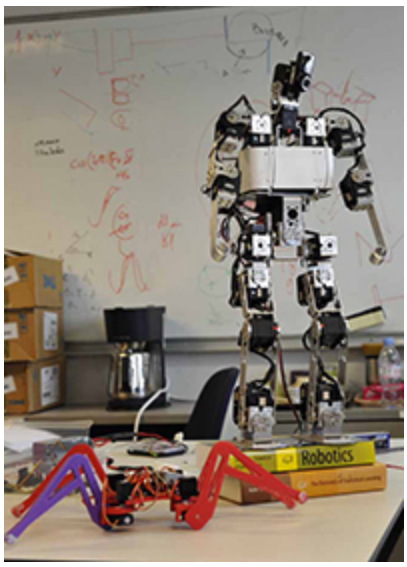
Figure 2 : IRM et reconstruction du modèle 3D de cerveaux pour des fœtus en haut et des prématurés d'âge de conception équivalents en bas.

Après ce travail important sur la création et la comparaison de ces modèles 3D, l'équipe de chercheurs souhaiterait mieux comprendre l'origine des différences observées. Plusieurs observations sont en effet flagrantes, comme par exemple le fait qu'il y ait beaucoup plus de liquide céphalo-rachidien (partie blanche des IRM de la figure 2) chez les fœtus que chez les prématurés. Travailler sur des IRM d'un même enfant juste avant sa naissance et juste après permettrait également de mettre en lumière les conséquences physiologiques de l'accouchement.

05/08/15 – LaBRI – cnrs.fr/ins2i

Jouer au foot, un concentré de problématiques robotiques

La RoboCup, coupe du monde de robotique, regroupe chaque année plusieurs milliers de roboticiens venant du monde entier. Les équipes conçoivent et fabriquent des robots qui concourent lors de divers challenges, le plus emblématique étant un match de football opposant deux équipes de robots humanoïdes autonomes. L'équipe Rhoban du Laboratoire Bordelais de Recherche en Informatique (LaBRI - CNRS/Université de Bordeaux/Bordeaux INP) est arrivée 3ème dans la ligue historique et très compétitive kid-size humanoid. Une démonstration des avancées en recherche de l'équipe sur la motricité et la robotique autonome.



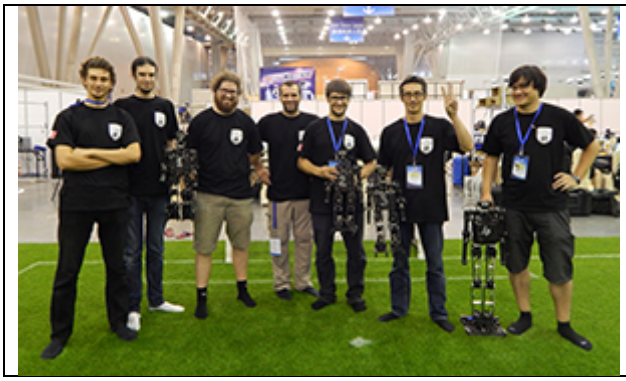
Sous son caractère ludique, la RoboCup constitue avant tout une plateforme d'échange unique dans le monde de la robotique, où se confrontent de façon concrète les concepts robotiques émergents. Le match de football en est l'épreuve centrale. Celle-ci requiert principalement deux aspects de la robotique : la motricité et la robotique autonome.

Au niveau de ses déplacements, le robot doit marcher en locomotion bipède, se relever après une chute, frapper le ballon, et ce sur un sol constitué d'herbe artificielle, donc irrégulier et mou. L'épreuve offre ainsi un cadre clair et concret de développement sur cette question de recherche encore largement ouverte. En effet, la question de la locomotion porte des enjeux scientifiques et technologiques très importants : la compréhension de cette problématique est à la base de la conception de prothèses robotiques ou encore d'exosquelettes. Le projet Rhoban travaille, par exemple, à la conception d'appareillages destinés aux personnes présentant des déficiences musculaires dans la jambe, comme à la suite d'un AVC.

Autre aspect de recherche nécessaire pour l'épreuve de football : la robotique autonome, proche de l'intelligence artificielle. Le joueur robot est en effet totalement autonome sur le terrain, il doit se géolocaliser sur la base de capteurs similaires à ceux de l'Homme (centrale inertielle, caméra embarquée, etc.), jouer en équipe et marquer des buts. La robotique autonome est elle aussi une question importante du point de vue des enjeux avec des applications diverses. L'agriculture de précision s'appuie par exemple sur des techniques de prise de décision sous information partielle très similaires à celles que les robots de Rhoban utilisent pour se positionner sur le terrain.

Le match de football de la RoboCup offre ainsi chaque année un cadre d'expérimentation des dernières avancées en robotique humanoïde et en robotique autonome, les deux thèmes principaux de recherche de l'équipe Rhoban. Le but à terme pour l'ensemble des compétiteurs est de réussir à créer une équipe de football robotisée capable de battre l'équipe de football humaine championne du monde, d'ici à 2050. La RoboCup suit pour cela un programme de développement à long terme en faisant évoluer les règles d'années en années vers des conditions de plus en plus réalistes.

D’autres épreuves sont également disputées lors de la compétition. Dans la ligue “Rescue”, un robot autonome ou téléopéré doit porter secours à des blessés dans un site de catastrophe reproduit dans l’un des hangars de la RoboCup. La ligue “Robot@home”, quant à elle, demande au robot d’effectuer de façon autonome diverses tâches de la maison (ménage, manipulation d’objets, aménagement).



Rhoban Football Club

Le Rhoban Football Club dépasse le cadre de la recherche. Il intègre un volet pédagogique important, ainsi qu’un volet associatif. L’équipe intègre un certain nombre d’étudiants qui participent concrètement à l’événement sous forme de stages ou bien de projets d’études. Le caractère pluri-disciplinaire apporte une richesse de problématiques très formatrice, la robotique offrant en plus une forte motivation intrinsèque.

31/08/2015 – LIMSI – CNRS Le Journal

Un logiciel qui décrypte la politique

Spécialiste du traitement automatique des langues, Xavier Tannier développe un outil qui permet d'analyser, à partir d'articles de presse et de tweets, les opinions des différents courants politiques et de leurs membres. Il nous explique comment cela fonctionne.

Vous venez de recevoir un Google Award pour votre projet *« Event thread extraction for viewpoint analysis »*, une application capable de détecter, analyser et représenter graphiquement les opinions des différents courants politiques et de leurs membres sur des thèmes de société précis. Pouvez-vous nous expliquer ce qu'est le traitement automatique des langues ?

Xavier Tannier : Il s'agit d'une discipline de l'intelligence artificielle à mi-chemin entre l'informatique et la linguistique, qui a pour but d'analyser le langage humain, et dans ce cas, le texte. Des exemples d'applications sont la traduction automatique, la correction orthographique, le résumé automatique, l'extraction d'information, la fouille de texte. Mon laboratoire, le Limsi[4], travaille sur presque tous ces domaines, ainsi que sur le traitement du langage parlé. Mon travail est plutôt tourné vers l'extraction d'information et la fouille de texte. Je m'attache à l'analyse de grandes quantités de documents textuels (typiquement, plusieurs millions) pour en extraire des informations pertinentes pour une situation donnée. On parle d'intelligence artificielle dès qu'on essaie de faire faire par la machine une tâche qui nécessitait de l'intelligence humaine auparavant, et qui n'est pas du calcul pur. Dans le traitement automatique des langues (TAL), on essaie de simuler les compétences langagières d'un humain, que ce soit en termes de production, de traduction ou de compréhension. C'est le cas de cet outil qui permet d'organiser des textes écrits de façon à mieux décrypter les opinions et les rapports de force dans le monde politique.

Comment est née l'idée de ce projet *« Event thread extraction for viewpoint analysis »* ?

X. T. : Il s'agit d'une collaboration avec Ioana Manolescu, de l'Inria de Saclay, et l'équipe des Décodeurs du journal *Le Monde*, dirigée par Samuel Laurent, qui se consacre au *fact checking*. Cette pratique aujourd'hui très répandue dans les journaux consiste à vérifier, parfois en temps réel, la véracité des déclarations factuelles d'un homme politique par exemple. Il peut s'agir d'une information chiffrée – baisse du chômage ou dépenses engagées sur un budget – dont on vérifie l'exactitude, ou encore des affirmations qui peuvent contredire des déclarations précédentes.

L'équipe travaille également sur de la visualisation de données, essentiellement pour le site Web du journal. Le traitement automatique des langues est particulièrement adapté à l'analyse des articles de presse. Je travaille par exemple sur la notion d'événement et j'essaye, à partir d'une grande masse de textes, de construire une chronologie d'événements importants qui se sont déroulés sur un thème précis. Par exemple, si l'utilisateur veut la liste des événements importants sur le Printemps arabe, sur les événements en Irak ou sur une personne, le système va chercher automatiquement les articles de journaux et va essayer de déterminer ce qui est le plus important sur ces questions et va fournir une chronologie à l'utilisateur (projet ANR Chronolines).

[4] Laboratoire d'informatique pour la mécanique et les sciences de l'ingénieur du CNRS

Quel est le progrès par rapport à un simple moteur de recherche ?

X. T. : Il y a une hiérarchisation de l'importance de l'article cité, effectué grâce à un grand nombre de données et d'articles. Pour prendre l'exemple d'une thématique telle que « la laïcité », nous allons disposer d'une base de données très importante, avec les dix ou quinze événements marquants sur le domaine, où les informations temporelles ont une grande importance. Nous allons attribuer des coefficients d'importance en prenant en compte les aspects liés aux rumeurs ou aux tendances politiques. Deux critères principaux sont divisés ensuite en sous-critères : la redondance, c'est-à-dire le nombre d'article reprenant un événement, et l'analyse temporelle, qui estime que si l'on en parle encore longtemps après, c'est un événement important. L'écriture journalistique est très appréciée parce que les contenus sont nombreux et parce que ce n'est pas du tout-venant comme sur les blogs : il n'y aura pas de fautes d'orthographe, les phrases seront bien construites, etc. Cela nous pose un problème de moins à résoudre. On travaille sur l'ensemble du Web, mais on privilégie surtout les sites de presse pour traiter les données compliquées avec moins d'éléments disparates.

Quel type d'informations traitez-vous ?

X. T. : Nous collectons un maximum de données pour étudier ces phénomènes parmi des articles de presse, des déclarations des hommes politiques, ainsi que leurs sites Web et leurs comptes Twitter. On va se concentrer sur la politique parce que c'est ce qui intéresse le plus les gens du *Monde* : par exemple, ils visent les régionales qui approchent, ou encore les primaires à droite ou plus tard les présidentielles. Le but étant, soit sur un événement précis, soit sur un sujet donné, de collecter les déclarations politiques et de les répartir sur l'échiquier politique : de l'extrême-gauche, gauche, centre, droite, jusqu'à l'extrême-droite et de disposer d'une visualisation qui permette de décoder assez rapidement quel est le vocabulaire utilisé et l'opinion portée par chacun de ces partis. Ainsi nous allons distinguer des tics de langage ou des postures sans vrai contenu politique. Il y a de nombreux partis politiques en France et en leur sein est diffusée l'opinion portée par le parti ou au contraire par des gens qui s'en éloignent un petit peu. Nous allons nous concentrer sur les éléments de langage, ou sur les commentaires et réactions des partis qui sont assez diserts sur les événements sensibles, et repérer ainsi ceux qui s'écartent du discours imposé à des fins de stratégie politique. Souvent, on a un courant principal affiché par un parti politique et finalement deux ou trois personnalités qui vont tenir un langage complètement différent au sein de ce même parti. Sur le sujet de la laïcité par exemple, on peut le mesurer, et c'est encore plus visible sur des sujets tels que le mariage pour tous. C'est ce que nous avons dénommé des « expressions dissonantes ».

Votre matériel de départ est toutefois très formaté et déjà homogène ?

X. T. : En effet, même si certains tweets s'en éloignent un petit peu ; mais nous ne prenons pas en compte tous les tweets, seulement ceux qui restent liés aux comptes des personnalités politiques. Le vocabulaire y est un tout petit peu plus débridé, mais cela reste relativement contrôlé. On pourrait imaginer que ce type d'outil participe à l'uniformisation de la pensée, mais on constate déjà que le *fact checking* pratiqué depuis quelques années empêche les politiques de transmettre des chiffres erronés. Ils sont alors obligés de mentir de manière plus fine. Le but de cette application est d'aider les journalistes et les citoyens à comprendre comment et pourquoi les hommes politiques ne disent pas ce qu'ils pensent, mais répètent ce qui est formaté selon chaque

parti. Le but n'est pas prédictif : il s'agit uniquement de décoder le discours politique et d'aider à le visualiser. Typiquement, ce projet permettra de remarquer, par exemple sur une question européenne, comment des partis que tout oppose en apparence adoptent en fait la même ligne.

Quel est l'état d'avancement du projet et sera-t-il commercialisé ?

X. T. : Le Google Award, contrairement à ce que le nom semble indiquer, n'est pas une récompense pour un travail achevé, mais un soutien financier sur un an pour un travail en cours (avec l'Inria et *Le Monde*). Nous n'en sommes encore qu'à la phase de collecte de fonds, qui commence plutôt bien puisque l'Agence Nationale de la Recherche (ANR) vient d'accepter de financer ce programme (projet ANR ContentCheck) (link is external). Les travaux que nous avons effectués sont préalables : notre travail sur les « chronolines », les chronologies journalistiques que nous étudions depuis quelques mois sur les dépêches de l'AFP[5], est à présent terminé. Mais le projet récompensé en tant que tel n'existe pas encore. Je pense que l'application sera gratuite, elle n'a pas vocation à être commercialisée dans l'immédiat, car il s'agit pour l'instant d'un travail de recherche, et Google ne s'ingère pas dans nos travaux, mais collecte plutôt des idées. Symboliquement, ce prix est très important pour nous, mais nettement moins que l'ANR en termes de retombées financières. Il nous permet juste de financer un ingénieur pendant un an.

[5] Agence France Presse

02/09/15 – LaBRI – CNRS Le Journal

Les IRM cérébrales ont leur traducteur automatique


Le professeur Jose Vincente Manjón Herrera devant une interface de la plateforme volBrain. © IPV

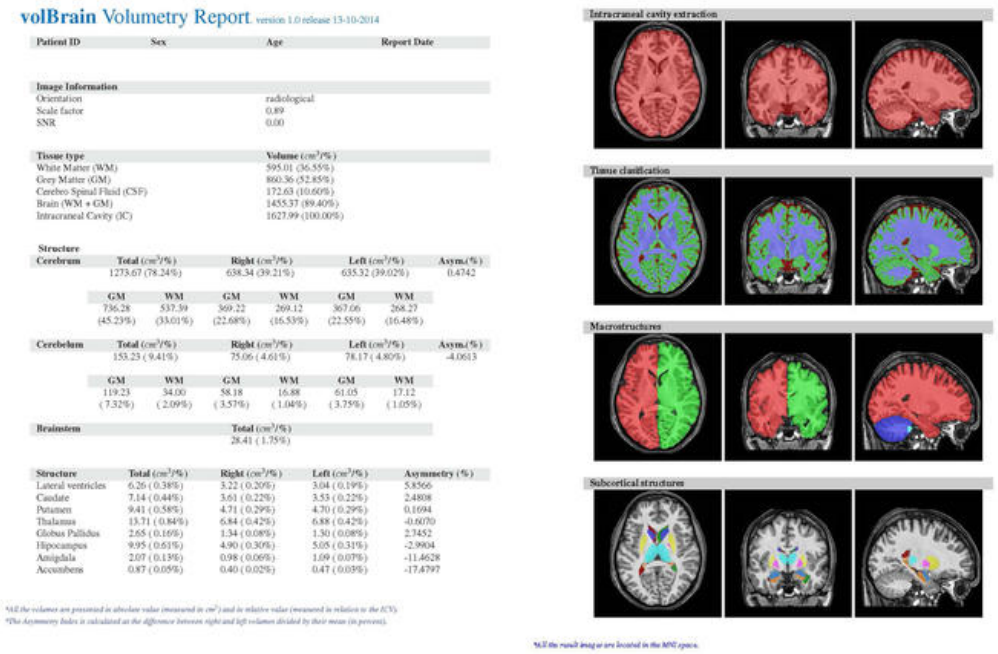
C'est une petite révolution pour l'étude des pathologies neurodégénératives : alors que les images du cerveau sont longues à décrypter manuellement, la plateforme en ligne volBrain, développée par des chercheurs français et espagnols, analyse en quinze minutes des IRM envoyées du monde entier.

Du partage de vidéos à l'enseignement des langues en passant par les coachs en ligne, on ne compte plus les nouveaux services offerts par les plateformes interactives du Web. C'est dans ce contexte qu'une équipe franco-espagnole de chercheurs a décidé de s'attaquer à l'analyse de données un peu particulière : les IRM 3D du cerveau. Ces derniers ont développé volBrain, une plateforme gratuite sur laquelle les chercheurs peuvent déposer les fichiers d'une IRM structurelle et obtenir en un temps record une analyse automatisée du volume des structures cérébrales scannées.

Quatre années de développement

Cette première mondiale a nécessité quatre années de collaboration entre Jose Vicente Manjón Herrera, professeur à l'université polytechnique de Valence en Espagne, et Pierrick Coupé, du Laboratoire bordelais de recherche en informatique[6]. Concrètement, VolBrain commence par améliorer la qualité de l'image puis segmente les structures sous-corticales. Ces régions du cerveau situées sous le cortex, comme l'hippocampe ou l'amygdale, sont extraites automatiquement et peuvent être observées et manipulées en 3D. *« volBrain mesure le volume des structures sous-corticales, puis les compare à des valeurs moyennes estimées sur une population de sujets contrôles*, explique Pierrick Coupé. *La plateforme indique au chercheur si une des structures a un volume anormal. Par exemple, une réduction de l'hippocampe peut être un biomarqueur précoce de la maladie d'Alzheimer ou d'une sclérose en plaques. volBrain reste aujourd'hui un outil de recherche, et non pas d'aide au diagnostic. »* Le processus d'homologation pour une utilisation en milieu hospitalier est en effet cher, long et coûteux.

[6] Unité CNRS/Univ. de Bordeaux/Bordeaux INP



volBrain Volumetry Report version 1.0 release 13-10-2014

Patient ID	Sex	Age	Report Date

Image Information	
Orientation	radiological
Scale factor	0.89
SNR	0.00

Tissue type	Volume (cm^3/%)
White Matter (WM)	595.01 (36.55%)
Grey Matter (GM)	860.36 (52.85%)
Cerebro Spinal Fluid (CSF)	172.63 (10.60%)
Brain (WM + GM)	1455.37 (89.40%)
Intracraneal Cavity (IC)	1627.99 (100.00%)

Structure

Cerebrum	Total (cm^3/%)		Right (cm^3/%)		Left (cm^3/%)		Asym.(%)
	1273.67 (78.24%)		638.34 (39.21%)		635.32 (39.02%)		0.4742
	GM	WM	GM	WM	GM	WM	
	736.28 (45.23%)	537.39 (33.01%)	369.22 (22.68%)	269.12 (16.53%)	367.06 (22.55%)	268.27 (16.48%)	

Cerebellum	Total (cm^3/%)		Right (cm^3/%)		Left (cm^3/%)		Asym.(%)
	153.23 (9.41%)		75.06 (4.61%)		78.17 (4.80%)		-4.0613
	GM	WM	GM	WM	GM	WM	
	119.23 (7.32%)	34.00 (2.09%)	58.18 (3.57%)	16.88 (1.04%)	61.05 (3.75%)	17.12 (1.05%)	

Brainstem	Total (cm^3/%)
	28.41 (1.75%)

Structure	Total (cm^3/%)	Right (cm^3/%)	Left (cm^3/%)	Asymmetry (%)
Lateral ventricles	6.26 (0.38%)	3.22 (0.20%)	3.04 (0.19%)	5.8566
Caudate	7.14 (0.44%)	3.61 (0.22%)	3.53 (0.22%)	2.4808
Putamen	9.41 (0.58%)	4.71 (0.29%)	4.70 (0.29%)	0.1694
Thalamus	13.71 (0.84%)	6.84 (0.42%)	6.88 (0.42%)	-0.6070
Globus Pallidus	2.65 (0.16%)	1.34 (0.08%)	1.30 (0.08%)	2.7452
Hipocampus	9.95 (0.61%)	4.90 (0.30%)	5.05 (0.31%)	-2.9904
Amigdala	2.07 (0.13%)	0.98 (0.06%)	1.09 (0.07%)	-11.4628
Accumbens	0.87 (0.05%)	0.40 (0.02%)	0.47 (0.03%)	-17.4797

*All the volumes are presented in absolute value (measured in cm^3) and in relative value (measured in relation to the IC).
*The Asymmetry Index is calculated as the difference between right and left volumes divided by their mean (in percent).

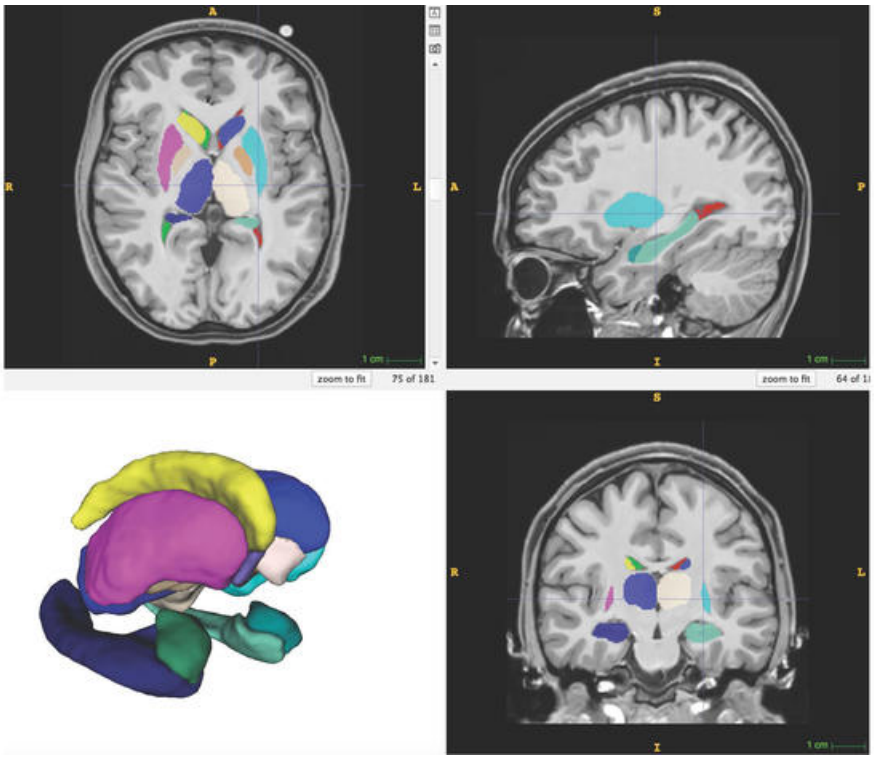
*All the result images are located in the MNI space.

Exemple de rapport automatique produit par la plateforme volBrain.
La première page fournit les volumes des différentes structures extraites de l'IRM envoyée par l'utilisateur.
La seconde page propose des captures d'écran permettant un contrôle qualité rapide.

La plateforme traite les fichiers IRM en environ quinze minutes et envoie directement le résultat dans la boîte e-mail du chercheur. Les serveurs du site, installés à Valence, peuvent traiter jusqu'à 500 IRM par jour ! Si l'inscription est libre pour tous les utilisateurs, les hôpitaux et les centres de recherche constituent le gros des utilisateurs. Pas moins de 124 institutions issues de six continents ont accepté d'apparaître officiellement sur le site, mais il existe en réalité davantage d'inscrits.

Un outil statistique

La plateforme, qui n'accepte que des données anonymisées, permet aux chercheurs de réaliser des études statistiques sur le cerveau. Thomas Tourdias, neuroradiologue et enseignant-chercheur au Neurocentre Magendie de Bordeaux, utilise justement volBrain dans le cadre de ses travaux sur la sclérose en plaques. Cette maladie, surtout connue pour les handicaps moteurs qu'elle engendre, provoque également des troubles cognitifs longtemps négligés. Elle touche entre autres l'hippocampe, qui constitue un des centres de la mémoire.



Résultat de la segmentation automatique des structures sous-corticales offerte par volBrain. En bas, à gauche, représentation 3D des structures sous-corticales extraites par volBrain.

Cela peut prendre plusieurs heures pour délimiter à la main l'hippocampe droit et gauche.

« Il n'existe pas d'autres moyens que l'imagerie pour « observer » l'intérieur du cerveau d'un patient de manière non invasive, explique Thomas Tourdias. *Mais, même avec une IRM, délimiter à la main un hippocampe pour en connaître le volume reste extrêmement fastidieux et dépendant de l'opérateur. Cela peut prendre plusieurs heures pour délimiter l'hippocampe droit et gauche. volBrain permet une extraction rapide, standardisée et reproductible de cette structure cérébrale. »*

Vers une standardisation de l'analyse d'IRM

Les frontières de certaines aires cérébrales ne font en effet pas consensus et des chercheurs différents risquent d'obtenir des volumes différents. volBrain suit toujours les mêmes standards et donne des résultats normalisés en fonction du volume de la cavité intercrânienne. Cela permet de prendre en compte la variabilité interindividuelle de la taille du cerveau. Ces étapes rendent possible l'établissement de statistiques cérébrales sur des populations importantes, une analyse difficile sans cette standardisation.

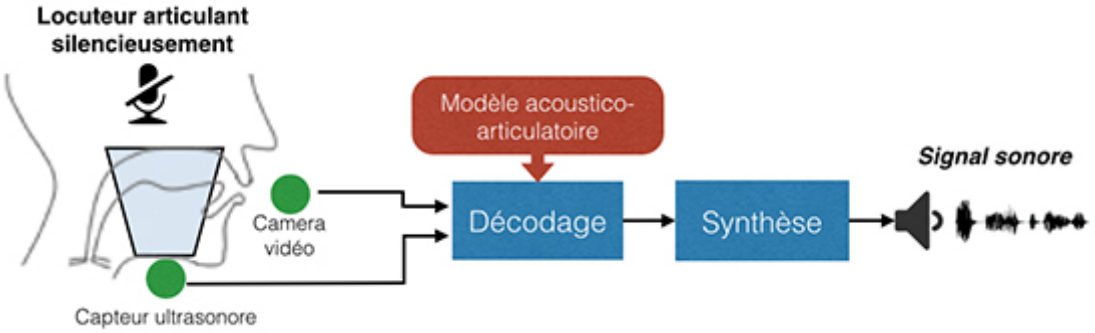
Pierrick Coupé et Jose Vicente Manjón Herrera souhaitent préserver la gratuité de cet outil pour la recherche académique et continuent de l'améliorer. Le passage à une analyse effectuée entièrement sur le *cloud* fait partie de leurs objectifs, afin de se préparer à l'accroissement du trafic et des données. Une plateforme similaire, dédiée aux IRM révélant la microstructure du cerveau, comme les fibres de matière blanche, est également en cours de développement sous le nom de dtiBrain. L'utilisation de volBrain et de dtiBrain permettra d'analyser conjointement la macro et la microstructure du cerveau. En attendant, la communauté des utilisateurs de volBrain ne cesse d'augmenter.

28/09/15 – GIPSA-Lab – cnrs.fr/ins2i

La parole silencieuse

Permettre à une personne de parler sans qu'aucun son ne sorte de sa bouche. C'est le défi auquel tente de répondre Thomas Hueber, chargé de recherche CNRS au laboratoire Grenoble Image, Parole, Signal, Automatique (GIPSA-lab - CNRS/Grenoble INP/Université Joseph Fourier/Université Stendhal). Son objectif est de concevoir une « interface de communication en parole silencieuse » (*silent speech interfaces*), un dispositif permettant de communiquer oralement dans des situations où le silence est nécessaire, ou au contraire dans des environnements bruyants. Une application médicale dans le cadre de certaines pathologies du larynx est également envisagée.

Les travaux de recherche de Thomas Hueber portent sur le développement de nouvelles technologies vocales. Il travaille notamment sur un dispositif permettant à une personne de communiquer oralement, mais sans nécessité de vocaliser. En parole silencieuse, un locuteur bouge normalement ses lèvres, sa langue, sa mâchoire, mais il ne produit aucun son. L'objectif du système est de capturer un ensemble de signaux physiologiques liés à cette « articulation silencieuse », et de les convertir en temps réel en une voix de synthèse. Ces signaux peuvent par exemple être l'activité électrique des muscles impliqués dans les mouvements articulatoires, ou bien directement les mouvements eux-mêmes, que l'on peut visualiser avec des capteurs spécifiques. C'est notamment cette seconde approche que Thomas Hueber poursuit avec son collègue Bruce Denby (UPMC/Institut Langevin). Pour cela, ils utilisent un capteur ultrasonore placé sous la mâchoire du locuteur, et une caméra vidéo positionnée à proximité de la bouche. Cette association permet de suivre simultanément les mouvements des articulateurs internes (comme la langue) et externe (comme les lèvres).

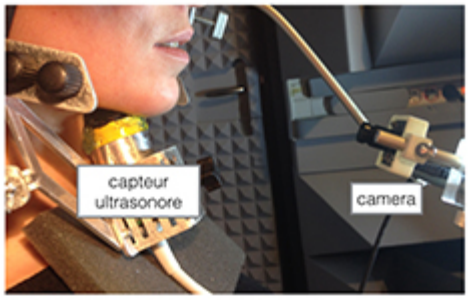


Pour décoder ces signaux et les convertir en une voix de synthèse, les chercheurs s'appuient sur différentes techniques « d'apprentissage artificiel » (*machine learning* en anglais). Cette discipline regroupe un ensemble de méthodes mathématiques permettant de créer un modèle de façon automatique, à partir de l'analyse de données expérimentales. Les paramètres de ce modèle sont estimés sur un ensemble de phrases prononcées « normalement » (c'est-à-dire non-silencieusement) par l'utilisateur au moment de la calibration du système. Cette base d'apprentissage permet de mettre en regard les « causes » du son, à savoir l'activité articulatoire, avec ses « effets », à savoir le son. Si cette phase d'apprentissage réussit, alors le modèle devient capable de « prédire » l'effet, uniquement en observant la cause, ce qui est le but recherché ici.

Cependant, il est important de souligner que le problème du décodage de la parole silencieuse est un problème « mal posé », au sens mathématique du terme, c'est-à-dire un problème qui n'a pas de solution unique. En effet, la parole silencieuse étant caractérisée par l'absence de vibration des cordes vocales, il est *a priori* impossible de distinguer certains sons (phonèmes) comme [k] vs. [g] (comme vs. gomme). Une des solutions

proposées pour tenter de lever ces ambiguïtés, est d'introduire dans la conversion des informations linguistiques a priori. Ces dernières prendront la forme d'une limitation sur le vocabulaire autorisé, et d'un « modèle de langage probabiliste », c'est-à-dire un modèle renseignant sur la probabilité d'occurrence d'une suite de mots dans une langue donnée. Par exemple, après la suite de mots « je mange une », le mot « pomme » est plus probable que le mot « table ».

Dispositif expérimental « de laboratoire »



À terme, les différents capteurs ainsi que les algorithmes de décodage et de reconstruction de la parole ont vocation à être embarqués sur un *smartphone*. Cela permettrait notamment de communiquer dans des lieux ou circonstances nécessitant de la discrétion (transports en commun, lieux publics, réunions), de la confidentialité (saisie d'informations bancaires, opérations de sécurité), ou au contraire dans des environnements extrêmement bruyants, dans lesquels l'exploitation d'une voix enregistrée à l'aide d'un microphone est très difficile (concerts, hélicoptères, hall de gare). Les chercheurs envisagent à terme également une application médicale, comme complément aux différentes voix de substitution aujourd'hui mises en place après l'ablation du larynx dans le cadre du traitement du cancer (laryngectomie).

Les travaux de Thomas Hueber et de ses collègues sur ce sujet ont fait l'objet de plusieurs publications dans les revues et conférences internationales sur les technologies vocales[7], ainsi que d'un brevet[8]. En 2011, il a obtenu le Prix international Christian Benoît récompensant un jeune scientifique pour un travail prometteur dans le domaine de la communication parlée. En 2015, un article dont il est le co-auteur se voit décerner le *best paper award* par l'*European Association for Signal Processing* (EURASIP)[9].

[7] Hueber, T., Benaroya, E.L., Chollet, G., Denby, B., Dreyfus, G., Stone, M., (2010) *"Development of a Silent Speech Interface Driven by Ultrasound and Optical Images of the Tongue and Lips"*, Speech Communication, 52(4), pp. 288-300. Hueber, T., Bailly, G. (2015), *"Statistical Conversion of Silent Articulation into Audible Speech using Full-Covariance HMM"*, Computer Speech & Language, ISSN 0885-2308, http://dx.doi.org/10.1016/j.csl.201…

[8] Patent No. WO/2011/032688

[9] Denby, B., Schultz, T., Honda, K., Hueber, T., Gilbert, J.M., Brumberg, J.S. (2010) *"Silent speech interfaces"*, Speech Communication, 52(4), pp. 270-287.

27/10/15 – Maison de la simulation – Communiqué de presse

Le calcul haute performance accélère la transition vers les énergies faiblement carbonées

Le projet EoCoE (*Energy Oriented Center of Excellence*), porté par la Maison de la simulation[10] (CEA, CNRS, Inria, Université Paris Sud et Versailles St Quentin en Yvelines) a été officiellement lancé en octobre 2015. Ce centre d'excellence s'emploiera à utiliser le potentiel prodigieux offert par les infrastructures de calcul, qui ne cessent de grandir, afin de faciliter et d'accélérer la transition énergétique européenne vers l'usage d'énergies fiables et faiblement carbonées.

Avec un budget total de 5,5millions d'euros, EoCoE va accompagner la transition énergétique à travers des soutiens ciblés à quatre secteurs clés – météorologie, matériaux, eau et fusion – chacun d'eux utilisant intensivement la modélisation numérique. Ces quatre piliers s'ancreront dans une solide base transverse et pluridisciplinaire qui fournira une expertise de haut niveau en mathématiques appliquées et en calcul haute performance. Le projet EoCoE travaillera par exemple à la réalisation de simulations météorologiques permettant de prédire la production des champs d'éoliennes ou des centrales solaires afin de les coupler plus efficacement au réseau électrique, ou bien à la mise au point par la simulation de nouveaux matériaux plus performants pour les batteries.

Le projet EoCoE, porté par la Maison de la simulation (Saclay, France), est structuré autour d'un centre franco-allemand (Maison de la simulation et Centre de recherche de Jülich) coordonnant un réseau européen qui comprend au total huit pays et 23 équipes. Ses partenaires sont fortement impliqués dans le calcul haute performance comme dans le domaine de l'énergie.

EoCoE est l'un des huit centres d'excellence en calcul haute performance établis dans le cadre du programme Horizon 2020 de la Commission européenne. L'objectif premier de l'ensemble de ces nouveaux centres d'excellence est de renforcer le leadership européen dans les applications de calcul haute performance en relevant différents défis dans des domaines importants comme les énergies renouvelables, la modélisation et la conception des matériaux, la modélisation moléculaire et atomique, le changement climatique, la science des systèmes globaux, la recherche biomoléculaire et les outils destinés à améliorer les performances de ces applications.

Le projet EoCoE est dirigé par la Maison de la simulation, un laboratoire commun au CEA, au CNRS, à Inria et aux universités de Paris-Sud et de Versailles. La France est fortement impliquée dans le projet avec la participation également d'équipes du CEA, du CNRS, d'Inria, du Cerfacs, d'EDF R&D et de Météo-France.

[10] Créée en 2014, la Maison de la simulation résulte de la volonté de mettre en commun les recherches en simulation dans le cadre de l'université Paris-Saclay, dont l'excellence dans ce domaine se voit ainsi reconnue à l'échelle européenne.

06/11/15 – IRIT – cnrs.fr/ins2i

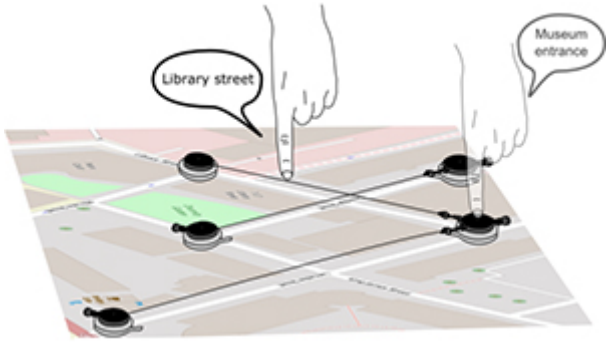
Accessimap, rendre les cartes géographiques accessibles aux déficients visuels

Les cartes géographiques sont de plus en plus présentes sur les sites web, journaux ou applications, mais elles sont inaccessibles aux personnes déficientes visuelles. L'accès à des cartes ou à d'autres représentations graphiques est pourtant essentiel pour être autonome, se déplacer, comprendre des données quantitatives, etc. L'objectif d'Accessimap, développé à l'Institut de recherche en informatique de Toulouse (IRIT - CNRS/Université Toulouse 1 Capitole/Université Toulouse - Jean Jaurès/Université Toulouse III - Paul Sabatier/Institut National Polytechnique de Toulouse) est de concevoir des cartes tactiles augmentées avec des informations sonores, mais aussi de permettre aux déficients visuels d'explorer « dynamiquement » des contenus spatiaux grâce à de nouvelles techniques d'interaction adaptées.

Des cartes tactiles à explorer avec les doigts permettent déjà de rendre une carte géographique accessible à une personne déficiente visuelle. Cependant ces cartes sont créées de manière artisanale et sont loin d'offrir les mêmes fonctionnalités que les cartes destinées aux personnes voyantes : impossible par exemple d'annoter une carte tactile, de zoomer ou de déplacer la carte, de calculer des distances ou des itinéraires, etc.

Les cartes interactives augmentées avec des informations sonores constituent une première amélioration. La carte tactile devient interactive quand elle est posée sur une tablette : les abréviations braille sont remplacées par des sorties sonores, ce qui permet d'augmenter la quantité d'informations mais aussi de modifier facilement les informations associées à chaque élément. Un premier objectif du projet Accessimap est de développer un éditeur de cartes tactiles augmentées qui s'appuiera sur des données géographiques issues de contenus numériques libres de droit (par ex. OpenStreetMap) et facilitera la tâche des transcripteurs, spécialistes de la déficience visuelle, qui créent les documents en relief.

Un deuxième objectif d'Accessimap est de concevoir et d'évaluer un prototype de table collaborative interactive permettant à un déficient visuel d'explorer des cartes géographiques de manière « dynamique » (annotations, zoom, pan, etc.). Julie Ducasse, doctorante à l'IRIT, a pour cela développé un système qui permet à des déficients visuels de construire et d'explorer une carte tangible, c'est-à-dire une carte qui est la représentation physique d'une carte numérique. Grâce à des instructions audio, les utilisateurs sont guidés pas à pas pour placer des objets sur la table – chaque objet représente un point d'intérêt ou un carrefour. Comme chaque objet est muni d'un enrouleur, les utilisateurs peuvent tracer des lignes pour « matérialiser » les rues, fleuves, frontières, etc. Les objets sont détectés grâce à une caméra placée sous la table qui localise des tags placés sous ces objets. Une fois la carte construite, il est possible d'écouter le nom des différents points et lignes en les pointant avec le doigt : un cadre infra-rouge placé autour de la table détecte la position des doigts. Ce système a été évalué avec 8 déficients visuels, qui devaient construire quatre



cartes de complexité croissante. 283 sur 288 objets ont été correctement placés et 27 cartes sur 32 ont été parfaitement reconstruites.

Cette interface tangible permet à des personnes déficientes visuelles de construire des cartes rapidement, et de manière autonome. L'éditeur en cours de développement permettra d'automatiser la simplification des données issues de contenus numériques pour qu'elles soient compatibles avec ce dispositif. La prochaine étape est de permettre aux utilisateurs de choisir le niveau de zoom de la carte qu'ils souhaitent reconstruire : des interactions non-visuelles adaptées seront conçues pour que les utilisateurs maintiennent une représentation mentale cohérente de la carte, quand elle est agrandie ou rétrécie.

Prix Google Anita Borg Memorial Scholarship

Julie Ducasse, doctorante à l'IRIT, a obtenu pour ses travaux le Prix Google Anita Borg Memorial Scholarship qui met en avant des jeunes chercheuses en informatique. Elle est la seule distinguée en France parmi les lauréates 2015. Elle a été invitée au siège de Google à Londres du 21 au 24 juin 2015 pour rencontrer les autres lauréates du prix EMEA et travailler sur un projet par équipe pour encourager les femmes à faire de l'informatique. Elle est encadrée par Christophe Jouffrais et Marc Macé, chargés de recherche au CNRS.

16/11/15 – ISIR – cnrs.fr/ins2i

Prix La Recherche pour Stéphane Régnier

Permettre à des micro-robots de circuler dans nos vaisseaux sanguins pour faire des mesures ou tester la résistance d'organes, c'est le défi relevé par Stéphane Régnier qui vient d'obtenir pour ses travaux, avec Zhou Ye et Metin Sitti de l'Université Carnegie-Mellon, le Prix La Recherche 2015 en technologie.

L'un des domaines d'application phare de la micro-robotique, cette robotique à l'échelle nanométrique, est bien évidemment la médecine, avec cette idée de pouvoir utiliser de petits robots à l'intérieur du corps pour éviter des traitements ou des opérations lourdes. La tête de ces robots pourrait ainsi être munie d'un capteur qui réagirait à certaines protéines, ou pourrait réaliser des opérations de poussée, de caractérisation de toucher pour tester la résistance de tissus…

Stéphane Régnier travaille en amont de ses projets au sein de l'Institut des systèmes intelligents et de robotique (ISIR - CNRS/Université Pierre et Marie Curie). La difficulté pour ces tous petits systèmes est de les faire se déplacer dans des liquides très visqueux, comme le sang. Le robot utilisé jusqu'à présent était constitué d'une tête et d'une hélice pour l'aider à le propulser. À ces dimensions, l'hélice est activée grâce au magnétisme pour permettre le déplacement. Depuis 4 ans, Stéphane Régnier et son équipe cherche comment améliorer ce système de propulsion, pour le rendre le plus efficace et maniable possible. Créer des prototypes à la taille micrométrique était difficile. C'est pourquoi ils ont réalisé leurs essais avec des modèles millimétriques, mais en reproduisant les « conditions réelles » : le nombre de Reynolds, rapport de la force d'inertie sur la force visqueuse, était augmenté pour recréer la viscosité extrême dans laquelle les robots doivent circuler au niveau micrométrique.

Des travaux ont d'abord été faits pour utiliser plusieurs hélices et optimiser la propulsion du petit robot nageur. Mais la meilleure solution a été d'employer plusieurs flagelles reliées à une tête pour faciliter les déplacements, grâce à une ondulation des flagelles grâce à un champ sinusoïdale. Orienter les micro-robots dans l'espace constituait un point délicat dans le contrôle de ces machines, challenge réussi pour la première fois par cette équipe. Plusieurs tests ont été effectués, pour comparer les tailles et longueurs de tête et de flagelles optimales. Les chercheurs n'ont pas été surpris de constater que le ratio « taille de la tête et des flagelles » correspondait à ce que la nature produit dans ces dimensions : les bactéries.

Les recherches en micro-robotique restent très en amont d'une utilisation thérapeutique. Mais la résolution des problématiques de propulsion est encourageante pour la suite. La prochaine étape pour l'équipe est de revenir à l'échelle micrométrique pour affronter des problèmes spécifiques de fabrication et de visibilité.

25/11/15 – LIAFA – cnrs.fr/ins2i

Calculer le diamètre du réseau routier mondial

L'équipe-projet commune Inria Gang du Laboratoire d'Informatique Algorithmique : Fondements et Applications (LIAFA - CNRS/Université Paris-Diderot) a calculé récemment le diamètre du réseau routier mondial. Plus qu'un défi calculatoire, il s'agit d'un pas dans la résolution effective des problèmes de distances dans les grands graphes.

Le diamètre d'un graphe est la distance entre les deux points les plus éloignés du graphe. Dans le réseau routier, la notion de distance qui nous intéresse le plus souvent est le temps de trajet. Trouver le diamètre du réseau routier mondial revient donc à trouver deux points tels que le temps de trajet pour aller de l'un à l'autre est maximal. Une fois ces deux points identifiés, on peut alors calculer le plus court trajet qui va de l'un à l'autre pour obtenir, en quelque sorte, le plus long « road trip » possible au monde. Calculer le diamètre d'un graphe requiert en général de calculer toutes les distances pour toutes paires de nœuds, ce qui est infaisable pour un graphe aussi grand.

C'est un sujet d'actualité qui a donné lieu à de nombreux résultats théoriques montrant la quasi-impossibilité d'un algorithme vraiment efficace sur tous les graphes (temps de calcul proportionnel à la taille de la donnée). Cette impossibilité dépend d'une conjecture SETH (*Strong Exponential Time Hypothesis*) sur la résolution du problème de satisfiabilité (SAT) qui est central en théorie de la complexité.

Cependant, l'équipe a développé une algorithmique basée sur des parcours de graphes qui s'avère très efficace sur de nombreux graphes rencontrés en pratique. Les réseaux routiers avec leurs structures très diversifiées fournissent un ensemble de données de grande taille qui ont permis de tester les algorithmes. Grâce à OpenStreetMap, l'équipe a pu ainsi calculer le diamètre routier du monde (et d'autres parties plus restreintes du réseau routier) et les visualiser. Les algorithmes peuvent être adaptés pour calculer aussi les centres des réseaux, c'est-à-dire les points depuis lesquels on peut atteindre tout autre point en un temps qui soit le plus petit possible. Cependant le calcul des centres s'avère moins efficace que pour le calcul du diamètre de certaines parties du réseau et la prochaine étape consistera donc à l'améliorer. À plus long terme, l'équipe cherche à obtenir des représentations succinctes et algorithmiquement efficaces de toutes les distances dans de tels graphes.

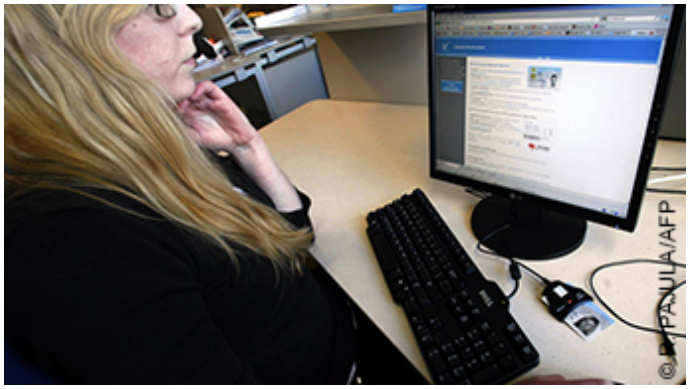
04/12/15 – LORIA – CNRS le Journal

Le vote électronique, pour quelles élections ?

Pour lutter contre l'abstention dans les grandes élections, certains hommes politiques souhaitent que l'on puisse bientôt voter chez soi, par Internet. Mais cette mesure est-elle envisageable. Point avec Véronique Cortier, lauréate du prix Inria – Académie des sciences du jeune chercheur.

L'électeur se cale dans son siège, connecte son ordinateur au site officiel du gouvernement, entre son identifiant et son mot de passe, clique sur le bulletin de vote de son choix et le valide. A voté ! Selon un sondage réalisé fin octobre 2015 par Harris Interactive pour le quotidien Le Parisien, 56 % des Français interrogés souhaiteraient pouvoir voter ainsi, sans avoir à se déplacer jusqu'à leur bureau de vote. Mieux : 58 % des abstentionnistes lors des précédents scrutins déclarent que, s'ils pouvaient voter par Internet, ils le feraient. Et ce nombre grimpe à 79 % chez les 18-25 ans !

À une époque où l'abstention est devenue un problème préoccupant, plusieurs responsables politiques, de droite comme de gauche, ont réagi à ce sondage en estimant urgent de mettre en place un tel système. Mais est-ce techniquement possible ? Le vote en ligne est-il aussi fiable que le vote à l'urne ?



Pour tous les scrutins, les Estoniens -telle cette électrice en février 2011- ont le choix entre le vote à l'urne et le vote à distance.

« Pour le moment, non ! », estime Véronique Cortier, chercheuse au Laboratoire lorrain en recherche informatique et ses applications (Loria)[11]. Récente lauréate du prix Inria-Académie des sciences du jeune chercheur, elle et son équipe, constituée principalement de Stéphane Glondu et de Pierrick Gaudry, travaillent au développement de Belenios, un logiciel de vote par Internet. « *Les problèmes à résoudre sont nombreux, estime-t-elle. Ils tiennent à deux éléments essentiels, mais a priori contradictoires, de tout scrutin politique : le secret du vote, qui interdit de pouvoir établir un lien entre un votant et son bulletin, et la vérifiabilité, qui assure au votant que son bulletin a bel et bien été pris en compte pendant le dépouillement.* »

Belenios, un logiciel libre et ouvert

Lors d'un vote classique, ces deux conditions sont remplies. Dans l'isoloir, l'électeur place le bulletin de son choix dans une enveloppe puis, devant le président du bureau de vote, le glisse dans une urne transparente. Le secret du vote est donc bien respecté. Et la vérifiabilité aussi : le votant peut s'en convaincre, s'il le souhaite, en restant dans la salle jusqu'à la fin du dépouillement.

« Les logiciels développés par les entreprises privées, remarque Véronique Cortier, *se concentrent sur la confidentialité du vote, une condition d'ailleurs exigée par la Commission national de l'informatique et des*

[11] Unité CNRS/Univ. de Lorraine/Inria

libertés. La transparence du scrutin, elle, n'est pas à la hauteur : le fonctionnement de ces systèmes est secret et l'électeur ne peut rien vérifier par lui-même. »

Belenios, le programme développé au Loria, est une amélioration de Helios, un logiciel sous licence libre conçu en 2008 par Ben Adida, de l'université d'Harvard. Ce dernier a été utilisé avec succès en 2009 pour l'élection du président de l'université de Louvain (en Belgique) et, depuis 2010, pour l'élection de l'équipe dirigeante de l'Association internationale pour la recherche en cryptologie. Comme Helios, Belenios est sous licence libre et chacun pourra, s'il le veut et s'il en a la capacité, en connaître le code et le fonctionnement.

Multiplier pour mieux additionner

« Comme pour toute élection, poursuit Véronique Cortier, le scrutin électronique se compose d'une phase de vote, suivie d'une phase de dépouillement. Le votant s'identifie et sélectionne le bulletin de son choix. Ce bulletin est ensuite crypté à l'aide d'une clé publique, puis envoyé à un serveur. Sur l'écran de son ordinateur, l'électeur voit son bulletin tomber dans une urne virtuelle et rejoindre les bulletins cryptés des autres votants. »

Afin de renforcer la confidentialité du dépouillement, le décompte des voix se fait sans que les bulletins soient préalablement déchiffrés. « *Belenios utilise un chiffrement de type El Gamal, qui possède une propriété homomorphique très intéressante : en combinant ensemble les bulletins cryptés, on obtient directement le résultat du vote. Mais ce résultat est crypté, et il faut le déchiffrer avant de pouvoir l'annoncer au public. »*

Pour ce faire, les responsables du scrutin possèdent chacun un fragment d'une clé privée. Il faut la mise en commun des différents fragments pour permettre le déchiffrement du dépouillement. Ainsi, un responsable mal intentionné ne peut pas, avec son seul morceau de clé, avoir accès au résultat du vote et être tenté de le modifier.

Réduire les risques de fraude

Pour réduire au minimum les risques de fraude, l'équipe du Loria a multiplié les systèmes de protection. « *Chaque votant possède un jeton de vote à usage unique*, explique Véronique Cortier. *Le bulletin est signé grâce à ce jeton, et chacun peut vérifier que les bulletins présents dans l'urne sont tous valables. Si quelqu'un attaque le serveur pour bourrer l'urne, cela se verra immédiatement… »*

Imaginons maintenant qu'un hacker parvienne à intercepter un bulletin chiffré avant qu'il n'arrive dans l'urne. Puisque la clé de cryptage est la même pour tous, le hacker pourrait déduire le contenu du bulletin en le comparant avec des bulletins qu'il aurait cryptés sur son ordinateur. Le secret du vote en serait alors brisé. Pour empêcher cela, l'ordinateur de l'électeur génère, avant l'envoi du bulletin, un nombre aléatoire qui est utilisé dans le chiffrement. Ainsi, un même vote, généré à deux instants distincts, produit deux bulletins chiffrés différents.

« Mais le système n'est pas parfait, met en garde Véronique Cortier. *Par exemple, lors d'un scrutin, nul ne doit pouvoir forcer la main d'un électeur. Avec un vote à l'urne, le citoyen est seul dans l'isoloir. Avec Internet, comment être sûr que, chez lui, il n'est pas menacé par quelqu'un ? Et comment s'assurer que son ordinateur n'est pas infesté par un virus capable de modifier le vote avant l'envoi ? »*

Les expériences de vote électronique en France

Ces imperfections empêcheront-elles la mise en œuvre du vote en ligne en France ? En réalité, le vote électronique y a déjà été expérimenté, sous deux formes différentes. En 2003, une loi a fixé les conditions d'agrément de machines à voter électroniques : présentes dans les bureaux de vote, elles remplacent à la fois l'isoloir et l'urne. En 2007, 83 villes les avaient adoptées – Brest, Mulhouse, Le Havre, Courbevoie, Nevers… –, pour un million et demi d'électeurs, soit 3 % du corps électoral. Cependant, cette année-là, le premier tour de l'élection présidentielle a été entaché par plusieurs problèmes techniques et juridiques, comme lorsque deux machines ont été installées dans chaque bureau de vote de Reims pour écourter le temps d'attente[12]. Un moratoire a alors été instauré, interdisant l'adoption de ce système par de nouvelles communes.

En 2007, pour l'élection présidentielle, des machines à voter électroniques avaient été utilisées dans 83 villes, comme ici à Issy-les-Moulineaux.

Autre vote électronique testé lors de scrutins réels : à l'occasion des élections législatives de 2012 et consulaires de 2014, les Français résidant à l'étranger ont pu voter soit à l'urne en se rendant dans leur consulat, soit par correspondance avec un bulletin papier et des enveloppes, soit par Internet. Un votant sur deux s'est exprimé en ligne lors de ces législatives, mais sans effet notable sur le taux de participation, contrairement à ce qui était espéré.

En 2014, dans un rapport sur le vote électronique en France, les sénateurs Alain Anziani et Antoine Lefèvre se sont montrés très réservés à ce sujet. Devant l'opacité du fonctionnement des machines à voter, ils ont demandé le maintien du moratoire sur ces machines. Et, face aux imperfections du vote par Internet, ils se sont déclarés opposés à son extension au territoire métropolitain, mais favorables à son maintien pour les Français de l'étranger (le vote par correspondance, l'autre solution pour ceux qui résident loin du consulat, étant encore moins bien sécurisé que le vote en ligne).

---

[12] Selon le code électoral, il ne peut être mis à la disposition des électeurs qu'une seule urne par bureau de vote, or, comme précisé par le Conseil constitutionnel en 2007, *« une machine à voter étant à la fois assimilable à une urne et à un isoloir, il ne peut y en avoir en principe plus d'une par bureau de vote »*

Le vote en ligne, pour quelles élections ?

Le bilan des expérimentations menées ailleurs en Europe est, selon les deux sénateurs, lui aussi mitigé. Seules la Suisse et l'Estonie continuent à développer le vote par Internet. La seconde, surnommée « e-Estonie », investit beaucoup et depuis longtemps dans les services électroniques mis à la disposition de ses citoyens : e-carte d'identité, e-impôts, e-police, e-services de santé, e-école et, bien sûr, e-élections. Pour tous les scrutins, les Estoniens ont le choix entre le vote à l'urne et le vote à distance. En 2013, 21 % du corps électoral a voté électroniquement.

Partout ailleurs en Europe, le vote électronique stagne ou recule. L'Irlande a abandonné son programme en 2004 en raison d'un manque de fiabilité des machines à voter. En Allemagne, la Cour constitutionnelle fédérale a déclaré les machines contraires à la loi, leur exactitude n'étant pas vérifiable par le citoyen. Aux Pays-Bas, le vote par Internet a été arrêté en 2008 après une rupture de la confiance dans la fiabilité des résultats. Idem au Royaume-Uni, où le vote à distance a été testé lors d'élections locales de 2002 à 2007.

« Si le vote par Internet n'est pas aussi fiable que le vote à l'urne, il est tout de même promis à un bel avenir, mais pas pour les grandes élections politiques », note Véronique Cortier. En novembre 2014, les 268 000 militants de l'UMP ont ainsi été appelés à élire leur président par Internet. En décembre 2014, les élections professionnelles à l'Éducation nationale se sont faites en ligne. En décembre 2015, les étudiants de l'Institut national des langues et civilisations orientales choisiront leurs représentants également en ligne.

« Et courant 2016, nous rendrons Belenios utilisable par tous, conclut Véronique Cortier. *En allant sur un serveur dédié, les associations, les comités d'entreprise, les communes et tous ceux qui souhaitent organiser un scrutin en ligne pourront le faire librement et gratuitement. »* Chacun pourra alors se faire sa propre idée sur les élections version 2.0. En attendant, un jour peut-être, de choisir un président de la République depuis son ordinateur personnel…

09/12/15 – IRISA – cnrs.fr/ins2i

Une reconnaissance 10 ans après la démocratisation de la fabrication des langages informatiques

Pierre-Alain Muller, Franck Fleurey et Jean-Marc Jézéquel ont obtenu à Models 2015 le *« 10 Year Most Influential Paper Award »* pour leur publication *« Weaving Executability into Object-Oriented Meta-Languages »* présenté en 2005. Cet article présentait une idée originale, permettant à tout ingénieur informaticien de facilement créer son propre langage informatique, en se basant sur l'outil Kermeta qu'ils avaient créé. Une petite révolution à l'époque.

Face à la multiplication des langages informatiques, on a du mal aujourd'hui à imaginer que dans les années 1960-1970 seuls quelques génies pouvaient créer à partir de rien un langage informatique. Les outils pour permettre la création de langages plus facilement se sont développés peu à peu par la suite, mais restaient quand-même réservés à des chercheurs experts. Au milieu des années 2000, de plus en plus de personnes ont eu besoin de créer de nouveaux langages, que ce soit pour répondre à différents aspects de problématiques complexes comme de concevoir une voiture ou un avion, ou même plus simplement pour faciliter la conception ou le déploiement d'applications web.

Pierre-Alain Muller, Franck Fleurey et Jean-Marc Jézéquel ont alors la volonté de faciliter encore un peu plus la création de langages informatiques, que ce soit de programmation, de spécification, de configuration, de test… Plutôt que de développer de nouveaux concepts difficiles à appréhender, ils ont l'idée de s'appuyer sur des connaissances communes aux ingénieurs informatiques. Pour créer un outil pour fabriquer des outils pour créer des logiciels (d'où le terme de méta-langage), les chercheurs ont importé les mêmes logiques que dans les langages orientées objet comme Java ou C++, bien connus des ingénieurs. Les chercheurs ont ainsi réellement démocratisé la fabrication de langages. Ce méta-outil, baptisé Kermeta, devient rapidement assez populaire à l'époque et a enregistré plusieurs dizaines de milliers de téléchargement. Et pour cause : il est alors l'un des rares outils open source à réellement fonctionner, et permet une utilisation relativement simple. Pour démonstration de l'efficacité de l'outil, les chercheurs ont par exemple repris un langage des années 1970, Logo, qui permet de simuler le déplacement d'une tortue sur un écran, et ont réussi à faire atteindre le même résultat au bout d'une simple séance de 2h de TP d'étudiants en master d'informatique… L'outil a marqué un tournant et inspiré beaucoup de personnes qui ont développé de nouveaux outils en se basant sur l'idée de s'appuyer sur les environnements déjà connus des utilisateurs.

La reconnaissance par la communauté, avec ce *« 10 Year Most Influential Paper Award »*, est d'autant plus appréciable que la publication *« Weaving Executability into Object-Oriented Meta-Languages »* de 2005 n'avait pas forcément été très bien comprise de tout le monde au début. Pierre-Alain Muller, Franck Fleurey et Jean-Marc Jézéquel étaient en effet plutôt à contre-courant de ce qui se faisait à cette période, où les chercheurs inventaient des solutions très pointues. En se basant sur le principe du *« Less is more »*, ils ont permis de proposer un outil, certes pas le plus puissant de son époque, mais qui répondait à un besoin réel pour permettre l'explosion de la créativité dans les langages informatiques.

22/12/15 – IRISA – CNRS le Journal, billet par Emmanuel Thomé, Pierrick Gaudry et Paul Zimmermann

Logjam : la faille qui met Internet à nu

Des chercheurs mettent en garde contre une faille majeure dans le protocole qui sécurise les connexions Internet et expliquent pourquoi et comment il faut se prémunir contre cette faille.

Au printemps dernier, en collaboration avec des chercheurs de l'Inria Paris-Rocquencourt, de Microsoft Research, et des universités américaines Johns Hopkins, du Michigan et de Pennsylvanie, nous avons mis en évidence une faille importante dans le protocole TLS qui permet de sécuriser les connexions Internet. Cette faille affectait un grand nombre de services Internet (Web, mail, vpn, etc), avec des conséquences allant de l'absence de confidentialité à l'usurpation d'identité de serveurs. Dans cet article, nous souhaitons revenir sur cette attaque et ses implications pratiques.

TLS, un protocole omniprésent sur Internet

Le protocole TLS (pour Transport Layer Security) est le mécanisme qui est mis en œuvre de manière automatique, et souvent transparente pour l'utilisateur, dès que l'on souhaite sécuriser une connexion Internet entre deux machines. Par exemple, la différence entre deux adresses Web de la forme http://fr.wikipedia.org et https://fr.wikipedia.org est que, dans le second cas, les échanges de données entre ma machine et le serveur de Wikipédia seront chiffrés par TLS. Plus précisément, le rôle de TLS dans ce type de connexion est d'abord de garantir la confidentialité : ni mon fournisseur d'accès, ni personne qui écoute sur la ligne ne doit pouvoir connaître le contenu de la communication. Tout au plus, on pourra savoir que je me suis connecté à Wikipédia et connaître la quantité de données qui aura transité sur le réseau.

Une autre fonction de TLS, tout aussi critique, est l'authenticité. Grâce à un système de certificats, véritables cartes d'identité numériques des serveurs Web, je suis certain que les pages que je vois sont bien fournies par Wikipédia, et non par un serveur pirate usurpant son identité.

TLS est un protocole très complexe où de nombreux algorithmes cryptographiques sont combinés, avec pour objectifs la sécurité et la rapidité d'exécution. Au tout début de la connexion, dans une première phase appelée *handshake*, les deux machines (le serveur Web et mon ordinateur personnel, dans l'exemple ci-dessus) s'entendent sur les algorithmes à utiliser. En effet, pour des raisons d'interopérabilité, un serveur se doit de parler de très nombreuses langues cryptographiques, sachant que de nombreux ordinateurs ne sont pas très à jour et ne connaissent que des algorithmes datant d'il y a une dizaine d'années. Ensuite, les deux machines fabriquent et s'échangent ce qu'on appelle une clé de session. Cette clé temporaire va servir à chiffrer les communications durant la connexion.

Assez de chiffres pour chiffrer ?

Au sein de TLS, les calculs permettant aux deux machines de s'entendre sur une clé se font souvent à l'aide de l'algorithme de Diffie-Hellman, dont la sécurité repose sur un problème mathématique complexe : le problème du logarithme discret.

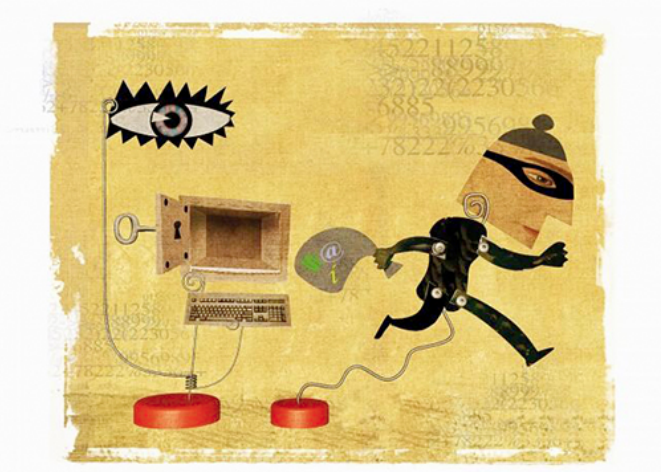
Sans entrer dans les détails, on peut dire que le problème du logarithme discret repose sur l'utilisation de grands nombres premiers, et que plus ces nombres sont grands, plus le système sera sûr, mais plus les calculs seront lourds. Quantifier précisément ce compromis est notre spécialité.

Nous connaissons très bien les algorithmes en jeu et sommes détenteurs du record actuel du plus grand nombre premier pour lequel le problème du logarithme discret a été résolu. Pour fixer les idées, ce record concerne un nombre premier de 180 chiffres, alors que la taille minimale recommandée actuellement est de l'ordre de 600 chiffres. Il y a donc de la marge ! Malheureusement, sur Internet, on trouve encore trop de systèmes protégés par des nombres premiers de seulement 300 chiffres, voire moins. En informatique comme dans d'autres domaines, l'existence d'un compromis entre coût et sécurité est fréquente, et les dérives qui s'ensuivent bien connues…

L'attaque Logjam : un problème de taille

Pour comprendre l'attaque Logjam, il faut se souvenir de la législation américaine à la fin des années 1990. L'export de produits cryptographiques était alors très réglementé. En conséquence, les protocoles de chiffrement prévoyaient explicitement un mode « Export » lors des connexions, limitant la taille des nombres premiers utilisés à 155 chiffres.

Cette « tare génétique » de TLS est encore présente dans les spécifications, et dans bien des logiciels, aussi bien du côté des serveurs que dans les ordinateurs personnels. Ce mode n'est certes pas activé par défaut, mais toujours considéré acceptable si l'une des machines le demande lors du *handshake*. Une petite subtilité dans le protocole (qu'on peut tout à fait qualifier de bug de conception) fait qu'un attaquant malintentionné peut se glisser au milieu de la connexion et faire croire aux deux protagonistes que l'autre désire passer en mode Export. Cela requiert toutefois de résoudre le problème du logarithme discret pour un nombre de 155 chiffres.


© GUIDO ROSA/IKON IMAGES/CORBIS

Un calcul qui, nous l'avons vu, est désormais faisable si l'on dispose de quelques semaines et de moyens de calculs modérés, mais pas durant les quelques secondes que dure le *handshake*… Le souci vient d'une seconde subtilité, bien connue des spécialistes du logarithme discret : quand le nombre premier ne change pas, des précalculs permettent de résoudre chaque instance bien plus rapidement. Ainsi, pour un nombre de 155 chiffres, quelques jours sur un cluster d'un millier de cœurs de processeurs modernes sont nécessaires pour faire ce précalcul, mais ensuite, le cassage du logarithme discret peut être effectué en quelques secondes. En pratique, seule une poignée de nombres premiers différents sont effectivement utilisés. La raison n'est pas théorique (il y a énormément de nombres premiers de la taille voulue), mais uniquement pour faciliter la mise en pratique ; et

de fait, si la taille du nombre premier était suffisante, cela ne poserait pas de problème. Mais avec un nombre limité de nombres de 155 chiffres, au final, l'attaque s'avère très réaliste.

L'importance des preuves de concept

Convaincre qu'une faille de sécurité est réellement exploitable est un art difficile. Dans le cas de l'attaque Logjam, il ne suffit pas de démontrer mathématiquement que le calcul peut s'effectuer pendant le *handshake*. Dans ce contexte, présenter un logiciel qui y parvient avec des moyens modérés est un argument crucial. Or c'est ce que permet notre logiciel CADO-NFS de factorisation d'entiers et de calcul de logarithme discret. Développé depuis huit ans, principalement par les membres de notre équipe nancéienne et diffusé librement, il permet de forcer les vendeurs de solutions de sécurité à se plier aux nouvelles recommandations quant aux tailles des nombres premiers à utiliser.

Ainsi, lors de la publication de la vulnérabilité, celle-ci a été prise particulièrement au sérieux : des milliers de serveurs ont été reconfigurés pour ne plus accepter de passer en mode Export, et les navigateurs des ordinateurs personnels ont également été mis à jour.

Au-delà de l'attaque liée au mode Export, le second intérêt de notre travail a été de donner pour la première fois un ordre de grandeur du temps de cassage du logarithme discret, lorsque les précalculs étaient réalisés. Comme ce temps est finalement très faible, même pour d'assez grands nombres premiers, les questions de la faisabilité et du coût du précalcul deviennent critiques. Surtout quand on sait que ce coût sera amorti par le fait que le même précalcul peut être utilisé pour casser des millions de connexions.

Les regards se tournent alors évidemment vers les agences de renseignement. La paranoïa ambiante vis-à-vis de la NSA à la suite des révélations d'Edward Snowden incite d'autant plus à ne pas jouer avec le feu : augmentons les tailles des nombres premiers ! Il est grand temps de suivre les recommandations et de passer à des premiers d'au moins 600 chiffres ! Mieux encore, la cryptographie moderne se doit de continuer la transition vers des algorithmes de chiffrement plus sûrs qui reposent sur des fonctions plus complexes comme les courbes elliptiques.

Crédits photos : Technique de réalité augmentée en imagerie médicale tridimensionnelle. © CNRS Photothèque - Cyril Frésillon / Visualisation des appels de fonctions dans un programme avec le logiciel Tulip. © David Auber / Robot humanoïde Nao. © Ed Alcock - Aldebaran Robotics / Un arbre en java. © CNRS
Mars 2016