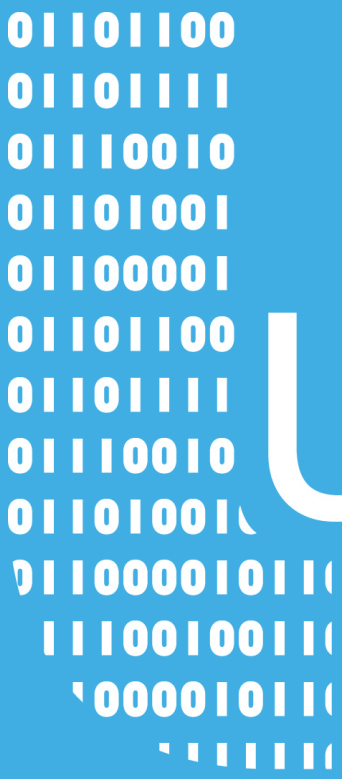
REVUE DE PRESSE

2019



Loria

cnrs Inria UNIVERSITÉ DE LORRAINE

16.01.2019 / France Culture

Qu'appelle-t-on bot et à quoi les différents types de bots servent-ils ? Y a-t-il plus de robots que d'humains sur internet aujourd'hui ? Qu'est-ce qu'un botnet ? Que peut-il infecter et dans quel(s) objectif(s) ?

"Un botnet, c'est la mise en réseau de logiciels a priori malveillants qui se connectent à un système de commande et de contrôle, en général un serveur sur internet, ou des réseaux de pair à pair". Eric Freyssinet • *Crédits : Bloomberg - Getty*

Depuis quelques mois, voire quelques années, selon les études, il y aurait sur internet plus de robots que d'êtres humains. Des programmes ou des algorithmes qui parcourent la toile, certains avec des intentions louables – comme la recension des sites pour les moteurs de recherches, d'autres beaucoup moins. Ces myriades de robots, ou botnets, peuvent être cachés dans des ordinateurs, dans des serveurs infectés mais aussi dans vos objets connectés, frigidaire, aspirateur, caméra et se réveiller, à la manière d'une armée de zombies, pour effectuer des attaques informatiques de grande ampleur, ou des campagnes de spam, ou de fake news. Les botnets sont, de facto, la première espèce indigène du cyberespace.

Internet : l'ère des robots : c'est le programme malveillant qui est celui de La Méthode scientifique pour l'heure qui vient.

Et pour nous accompagner dans cette plongée dans cet univers d'élevage de robots et de fausses identités virtuelles, nous avons le plaisir de recevoir aujourd'hui **Eric Freyssinet**, chef de mission numérique de la Gendarmerie Nationale, docteur en informatique et **Jean-Yves Marion**, professeur à l'Université de Lorraine, membre de l'Institut Universitaire de France.

Écouter l'émission sur le site de France Culture.

17.01.2019 / L'Usine Nouvelle

Détecteur de code malveillant

JEAN-YVES MARION 52 ANS

Directeur du Loria, Nancy (54)

Alors que les antivirus classiques ne protègent que des codes malveillants connus, qui ont infecté suffisamment de machines pour être ainsi répertoriés, Jean-Yves Marion a développé une autre approche de la sécurité informatique : comprendre ce qu'est un code malveillant. Fondateur du premier Laboratoire de haute sécurité (LHS) en informatique, à la tête du Laboratoire lorrain de recherche en informatique et ses applications (Loria) depuis 2013, ce professeur à l'université de Lorraine a mis au point la technique d'analyse morphologique qui permet de scanner la structure du code d'un programme informatique afin d'identifier des fonctions suspectes. Des recherches aujourd'hui reprises par la spin-off Cyber-detect, créée en mai 2017. **M. G.**

22.01.2019 / L'Est Républicain

PERFORMANCE Mardi 22 janvier

Les C.G.U des GAFA

Cette performance interroge notre pratique quotidienne du web.

« Vous utilisez Google ? Vous utilisez Amazon ? Vous utilisez Facebook ? Vous utilisez Apple ? Vous utilisez Netflix, Twitter, Instagram, Microsoft... ? Avez-vous lu leurs Conditions générales d'utilisation avant de les accepter ? »
La performance C.G.U, à la croisée du NetArt et du théâtre, est une tentative absurde de lire au public les Conditions générales d'utilisation des GAFA dans leur intégralité ! Et même de les rendre sexy et passionnantes. Utilisation éhontée de Gif, enfermement des performers dans des cartons, mindmappings pseudo-intelligents, séquestration du public... La fin justifie les moyens.
« À travers cette performance, c'est notre pratique quotidienne du web que nous interrogeons, et sans prôner la déconnexion, nous pointons simplement du doigt les conséquences de notre pacte avec les GAFA. Pacte avec le diable ou pas ? », interrogent Raphaël

Gouisset et Benjamin Villemagne.

Mardi 22 janvier à 19 h. Théâtre de La Manufacture - Nancy. Entrée libre sur réservation. Performance suivie d'une rencontre-débat avec Samuel Nowakowski, Maître de conférences HDR à l'Université de Lorraine, chercheur au Loria.

24.01.2019 / L'Est Républicain

[Lien de la vidéo sur mosaik-cristal.tv]

03.02.2019 / L'Est Républicain

SARREGUEMINES *Festival Sciences en Lumière*

Quand la machine remplace l'homme

Organisé par le CNRS de l'université de Lorraine, le festival *Sciences en lumière* s'est invité au Casino des Faïenceries. Les élèves du lycée Jean-de-Pange ont pu débattre sur le thème de l'intelligence artificielle avec un chercheur.

L'intelligence artificielle va-t-elle nous dépasser ? C'est le titre du film produit par Arte et projeté devant une centaine d'élèves du lycée Jean-de-Pange au Casino des Faïenceries. Une rencontre qui a été organisée par le CNRS, Centre national de la recherche scientifique, de l'université de Lorraine dans le cadre du festival *Sciences en lumière*.

Le thème de cette année est celui de l'intelligence artificielle. « Tout le monde est concerné par les intelligences artificielles, indique Christine Schmal, enseignante en mathématiques. C'est surtout un moment de questions et d'échanges pour les futurs bacheliers, qui pourront préciser leurs projets d'avenir. »

Suite au visionnage du film un débat avec les élèves des classes de seconde à la terminale a eu lieu pendant une heure. Celui-ci a été animé par Samuel Nowakowski, enseignant chercheur en humanité numérique à l'université de Nancy. Une projection qui permet donc de soulever plusieurs problématiques. L'importance grandissante de l'intelligence artificielle dans plusieurs disciplines : médecine, psychiatrie, automobile et publicité. Mais aussi la question de l'automatisation de nombreux secteurs d'activité qui pourrait amener au remplacement de l'homme par la machine. En somme, un film un peu trop « sensationnaliste » d'après le chercheur de Nancy.

> « L'intelligence artificielle est un sujet qui soulève des questions sociales et philosophiques. »
> **Samuel Nowakowski**

« Les machines ne sont pas intelligentes »

Selon lui, le terme « intelligence » n'est pas tout à fait exact pour qualifier l'algorithme de fonctionnement d'une machine. « Les machines sont extrêmes performantes, mais dans un domaine spécifique. »

Les lycéens ont joué le jeu et posé quelques questions au conférencier. Sur les métiers concernés par cette automatisation et sur la dangerosité des intelligences artificielles, notamment en politique. Une dernière question très percutante : « L'intelligence artificielle pourrait-elle impacter la démocratie ? », s'interroge une élève. Samuel Nowakowski rappelle donc le rôle jouer par les algorithmes dans l'élection de Donald Trump en 2016. Les GAFA, Google, Amazon, Facebook et Apple, ont une influence considérable sur les États et leur politique. Il fait alors référence à l'ouvrage de John Brumer, *Tous à Zanzibar*, dans lequel une entreprise du numérique rachète un pays…

Samuel Nowakowski (à droite), enseignant chercheur à l'université de Nancy, s'est adressé aux élèves du lycée Jean-de-Pange dans le cadre d'un débat sur l'intelligence artificielle au Casino des Faïenceries. Photo Thierry NICOLAS

ÉPINAL *Numérique*

Youtube au centre des attentions

L'Espace Cours a été, ce mercredi, au cœur de la réflexion numérique. Des chercheurs, un youtubeur se sont retrouvés à Épinal, sous l'impulsion de Canopé 88 pour parler du savoir et de l'apprentissage à l'heure des nouveaux médias.

Tout le monde a déjà vu le logo rouge de Youtube, dans lequel s'inscrit une petite flèche blanche (un clin d'œil au bouton "play", des ancêtres de la plateforme, magnétoscopes, baladeurs CD et autres chaînes hi-fi). C'est justement de la plateforme de vidéos dont il était question, ce mercredi à l'Espace Cours, sous l'impulsion de l'Atelier Canopé 88. Après une présentation réalisée par Sandrine Philippe, professeur documentaliste et doctorante au Crem (laboratoire de l'Université de Lorraine), dont la thèse concerne les pratiques adolescentes sur Youtube, plusieurs intervenants ont pris la parole sur le thème « apprendre aujourd'hui à l'heure des nouveaux médias ». Si la plateforme vidéo de Google a pignon sur rue, notamment chez les collégiens et lycéens, il y a « une panique morale, pour Annabelle Soudière, directrice de l'Atelier Canopé 88. Quelle est la place des professeurs par rapport à Youtube ? »

« Le parascolaire est le marché de l'angoisse parentale » **Laurent Petit,** professeur à la Sorbonne

Le manque d'esprit critique, un problème global

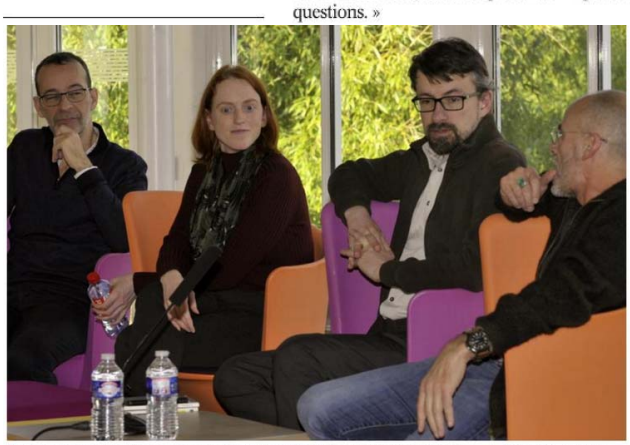
Pour Samuel Nowakowski, enseignant-chercheur à l'Université de Lorraine, « Youtube est une ressource. L'enseignant est encore plus nécessaire pour faire de la médiation des savoirs. Il doit y avoir une dimension pédagogique. À titre personnel, je ne pense pas que Youtube va remplacer l'enseignant. » Ce qui est important, cependant, dans la pratique des nouveaux réseaux, est d'amener les élèves à avoir un regard critique, comme le constate Sandrine Philippe. « Il faut pouvoir évaluer les contenus et ce d'une manière dynamique, pas à partir d'une grille de lecture, comme on a appris à le faire. » Pour elle, ce n'est pas uniquement le public jeune qui est touché par un manque d'esprit critique, mais également « les plus de 65 ans, qui partagent des contenus sans vérification, sans se poser de questions. »

S'est également posée la question de l'utilisation des contenus sur Youtube pour une classe. « Ce n'est pas un problème, constate Thomas Durand, auteur de la chaîne Youtube La Tronche en Biais. Plus un youtubeur est petit, plus il aura tendance à approuver l'utilisation de ses vidéos. Il se peut même qu'il intervienne en classe. Il ne faut pas hésiter à demander. » Tout cela rentre dans un marché parallèle de l'éducation, où les élèves visionnent des vidéos pour avoir des compléments par rapport aux cours. « C'est dans la continuité du programme, estime Laurent Petit, professeur de sciences de l'information et de la communication à la Sorbonne, comme un prof particulier, avec un suivi en parallèle. Il y a quelques années, le parascolaire était le marché de l'angoisse parentale. Maintenant, les enfants s'en emparent d'eux-mêmes. »

Dans la salle, un participant, ancien professeur de lettres, s'inquiète : « On sait que les écrans attirent plus que les livres, qu'ils peuvent provoquer des addictions. Et il est également plus facile de développer une pensée en 500 pages qu'en 10 minutes de vidéo. »

Se pose alors une nouvelle question : les vidéos peuvent-elles remplacer les livres ?

Lucas HUEBER



Quatre intervenants ont pris part au débat organisé par l'Atelier Canopé des Vosges, ce mercredi, dont le thème portait sur l'apprentissage à l'heure des nouveaux médias.

4,6

C'est, en milliards, le nombre de vidéos vues sur Youtube dans le monde entre 8 h et 16 h 40 ce mercredi, d'après Samuel Nowakowski.

« Il faut évaluer les contenus de manière dynamique. »
Sandrine Philippe
Doctorante à l'Université de Lorraine

09.02.2019 / L'Est Républicain

Musée des beaux-arts : une application pour des visites sur mesure en un clic

Thématique, chronologique, exhaustive, ludique et surtout personnalisée… grâce à une application pour tablette ou smartphone, toutes les visites du Musée des beaux-arts sont désormais possibles d'un clic !

Par Lysiane GANOUSSE - 09 févr. 2019 à 11:59 | mis à jour à 12:08 - Temps de lecture : 3 min

01 / 03 On peut choisir sa visite en privilégiant les chefs-d'œuvre, remonter le temps, se focaliser sur une époque, se mettre à hauteur d'enfants, etc. et ainsi transformer totalement notre vision du musée ! Photo Frédéric MERCENIER

L'audioguide, c'est fini. Il a fait son temps. Et d'ailleurs avec succès. Mais l'heure est venue d'entrer dans le XXIe siècle. À l'image de la plupart des grands musées, le MBAN opte pour la souplesse et la richesse de l'écran, autrement dit une application smartphone, grâce à laquelle le visiteur pourra singulièrement varier les plaisirs de son exploration.

« Avec, et ce n'est pas la moindre des choses, l'ajout de l'image là où l'audioguide se contentait du son », signale en préambule Charles Villeneuve de Janti, directeur des musées de Nancy.

Une base, et des briques

Une petite révolution en effet, qui permet de découvrir toutes les informations utiles à la compréhension d'une œuvre en regard de sa photo. Au moins peut-on s'assurer de ne pas s'être trompé de sculpture, ou de tableau…

Mais les bonus à ce changement sont bien plus substantiels. « En fait, on peut se voir suggérer une visite quasi sur-mesure ! »

C'est à la jeune start-up parisienne smArtapps, spécialisée dans les applications à vocation culturelle (et déjà sollicitée par divers musées de la ville de Paris), que Nancy a confié le soin de concevoir ce nouvel outil. Lequel a la vertu de fonctionner par « briques ».

Le principe : une visite de base est proposée aussitôt que l'application téléchargée, à laquelle il est possible d'ajouter des compléments (les briques…) au gré de ses envies.

Fort de ce nouvel outil, on peut aussitôt configurer sa visite, opter pour une remontée artistique du temps, ou filer dans les couloirs en privilégiant telle ou telle thématique (Les femmes de l'art, Art décoratif et design, Parlez-moi d'amour, Prenez les clefs des champs, etc.).

Jeux pour petits et grands

On est libre par ailleurs de décider du temps consacré à notre visite. Si nous ne disposons que d'une demi-heure, l'application nous guidera ainsi vers les dix chefs-d'œuvre à ne pas manquer, de Rubens à Caravage en passant par Delacroix. Autre option également ouverte : bénéficier de la visite guidée par la voix (et par les choix !) de l'écrivain Philippe Claudel.

Mais poussons plus loin encore. En fonction de nos besoins et de notre profil, on peut ajouter un volet supplémentaire à nos critères. Et ainsi télécharger la « brique » consacrée aux enfants. Celle-ci attire l'attention du petit visiteur sur le plus grand tableau du musée, sur l'amour tel que se le représente Picasso, ou sur un soleil couchant immortalisé à Étretat par Monet. En usant bien sûr d'un niveau de langage approprié.

Une autre « brique » est proposée aux personnes à mobilité réduite, qui ouvre par exemple l'accès à une visite en langue des signes, téléchargeable en un clic.

Des plans, des infos pratiques, un système de géolocalisation, et même des jeux sont compris, la dimension ludique étant désormais très prisée par toutes les générations. Ce qui n'exempte pas, bien sûr, de la fonction éminemment pédagogique. Retenons seulement que l'ennui n'est pas compris dans le prix. D'ailleurs, c'est gratuit !

À noter que le musée de l'Ecole de Nancy devrait lui aussi bénéficier prochainement de ce dispositif.

Tout en souplesse

Le nouveau système adopté par le MBAN pour un budget de 55.000 € se singularise par sa « souplesse ». Il est gratuit si on le télécharge sur son propre smartphone, mais pour qui veut, des appareils prêts à l'emploi sont disponibles à l'accueil. Une borne wifi est installée à l'entrée, une seconde borne prévue sur le parcours de sorte de changer la configuration de sa visite à son gré.En outre, le musée pourra à l'avenir enrichir le dispositif de « briques » supplémentaires et introduire lui-même les changements nécessaires en cas de déplacements des œuvres, prêts ou nouvelles acquisitions. Bien sûr, des versions en anglais et allemand sont prévues. Enfin des stations de chargement des batteries sont disponibles, très prisées en particulier des touristes.

Par Samuel Nowakowski
paru en février 2018
L'Elephant N° 19

Dans la jungle du cyberespace

En mai 2017, le piratage à l'échelle mondiale réalisé par le groupe de pirates Shadow Brokers a rappelé la fragilité de notre exposition numérique.

Par Samuel Nowakowski, maître de conférences HDR, université de Lorraine, LORIA UMR 7503

Avant de commencer, remontons d'un cran avec un petit extrait d'un roman culte écrit en 1984 par un auteur qui ne l'est pas moins, William Gibson. Ce roman, *Neuromancien*, donnera naissance aux mouvements cyberpunks. Y apparaît pour la première fois le cyberespace dans lequel évoluent des pirates, des hackers connectés. « Le cyberspace. Une hallucination consensuelle vécue quotidiennement en toute légalité par des dizaines de millions d'opérateurs, dans tous les pays, par des gosses auxquels on enseigne les concepts mathématiques… Une représentation graphique de données extraites des mémoires de tous les ordinateurs du système humain. Une complexité impensable.… » Le cyberespace est pour la première fois décrit comme une dimension supplémentaire du monde dans laquelle on évolue par l'intermédiaire d'interfaces connectées, et où les quêtes sont l'affaire de pirates ou de hackers. Mais aujourd'hui, qui est à l'œuvre ?

Les rançongiciels ou ransomwares

Les rançongiciels ou ransomwares[1] s'immiscent partout et peuvent infecter aussi bien un système bancaire qu'un téléviseur connecté, un ordinateur personnel ou un smartphone. Ils sont apparus dans les années 1990 sous la forme d'une fenêtre invitant à acheter un logiciel antivirus. Transmis par courriel sous forme d'un lien ou d'une pièce jointe contenant le virus[2], ils sont responsables de millions d'attaques et portent de jolis petits noms comme Petya, Locy ou Cerber. Selon Karsperky Lab, au troisième trimestre 2016, à l'échelle de la planète, une entreprise était touchée toutes les quarante secondes. Sur le deuxième trimestre 2016, on a dénombré plus d'une soixantaine de familles inédites de logiciels malveillants et, selon certains, plus de 7 millions d'exemplaires seraient en circulation. Les plus répandus, ces logiciels malveillants sont aussi, selon Cisco, « les plus rentables de l'histoire de la cybercriminalité ».

En décembre 2016, la Malware Hunter Team[3], qui rassemble des chercheurs du monde entier en cybersécurité, a révélé l'existence d'un rançongiciel d'un genre nouveau : Popcorn Time. Il prolifère sur la base d'un double chantage : payer un *bitcoin* (une monnaie électronique) de rançon ou transmettre le lien infecté à au moins deux internautes de son entourage, la victime ne récupérant ses données qu'à condition que les deux autres paient dans le délai imposé.

Enfin, les réseaux sociaux, les mobiles et le *cloud* font désormais partie des cibles. Par exemple sur Facebook, avec la présence de faux onglets *like* qui amènent l'utilisateur directement vers un *malware* (logiciel malveillant, développé dans le but de nuire à un système informatique). Les smartphones ne sont pas immunisés. Les systèmes iOS ou Android présentent des points de vulnérabilité exploités par les pirates. Et, bien sûr, le *cloud* est une cible de choix. En effet, installer un logiciel malveillant dans un serveur permet de récolter une multitude d'informations sensibles.

Dans l'attaque de mai dernier, le rançongiciel incriminé s'appelle WannaCrypt (ou Wcry, WanaCry, WanaCrypt, Wanna Decryptor). Il exploite une faille de Windows corrigée en mars. Cette faille a été exploitée un temps par la NSA par un outil de son arsenal EternalBlue et divulguée dans des documents piratés de l'agence. Comme souvent, il n'aura pas fallu longtemps pour que certains l'utilisent à leur profit. Dans la pratique, le premier vecteur utilisé est une très large campagne de diffusion par email. Les machines infectées se retrouvent avec leurs données chiffrées, une rançon d'au moins 300 dollars étant demandée pour les restaurer. Donc soyez vigilant dans l'ouverture des fichiers reçus et faites les mises à jour de vos ordinateurs !

Un autre exemple bien connu est le *phishing* (hameçonnage). Il consiste à soutirer des renseignements personnels en faisant croire à la victime qu'elle s'adresse à un tiers de confiance. En général, cela se présente sous forme d'un courriel urgent dans lequel figure une demande de cliquer sur un lien pour actualiser des informations personnelles. Ce lien donne accès ensuite à un faux site web semblable au site authentique, où l'on vous demande de saisir vos codes, vos mots de passe… Autre exemple, la technique du trou d'eau, ou *watering hole*, consiste à identifier les goûts des cadres et chefs d'entreprise en matière de visites sur Internet. Le pirate se poste ensuite sur un de ces sites populaires et y attend sa proie patiemment. Enfin, petit dernier, le *malware* Narilam a été employé contre l'Iran. Ce programme endommage les données d'une entreprise en les désordonnant avec comme finalité la perturbation de la chaîne de distribution et de gestion des stocks.

Pour mettre hors service une entreprise, un objectif peut être atteint de manière plus radicale : les cyber-attaques de type Déni de service (DoS) et Déni de service distribué (DDoS), employées par exemple par les Anonymous dans leurs opérations. Comment cela fonctionne-t-il ? Si une seule personne n'est pas dangereuse pour un serveur visé, lorsque des milliers d'internautes font la même action en même temps, cela peut vite devenir ingérable… La technique consiste à louer quelques serveurs web puissants ; la mise en place se fait par l'intermédiaire d'un *malware*, un cheval de Troie, diffusé sur le Net *via* ces serveurs afin d'infecter le plus possible de machines sans être détecté. Ces machines vont submerger de requêtes de tous types un serveur cible. Celui-ci ne pourra plus répondre et s'arrêtera. Les attaques DDoS sont prisées des cybercriminels parce qu'elles sont quasiment impossibles à bloquer, sauf à coups de moyens financiers et matériels astronomiques (voir les premiers épisodes de la série *Mr. Robot*).

Mais comment s'en sort-on ?

Chaque internaute doit avoir toujours conscience de ce qu'il fait et de pourquoi il le fait. Cela passe par de la formation et surtout par une nécessaire citoyenneté en numérique et une forme d'humanisme numérique.

La lutte sur le terrain se joue dans les laboratoires comme le LORIA[4] (Laboratoire lorrain de recherche en informatique et ses applications) et son Laboratoire de haute sécurité (LHS). Le LHS est une forteresse dans laquelle sont confinés six millions de virus informatiques, une collection de méchants capturés sur la Toile par les chercheurs. Collectionner ces virus permet de les analyser en profondeur et ainsi de concevoir des outils permettant de les détecter même après une mutation, afin de proposer des solutions pour garantir la sécurité informatique et celle des citoyens.

1. *Ransomware* ou rançongiciel : logiciel malveillant qui prend en otage des données personnelles en les chiffrant ou bloque l'accès d'un utilisateur à une machine. Seul le paiement d'une rançon permet de déchiffrer les données.

2. Virus : programme capable d'infecter un autre logiciel. Les virus sont aujourd'hui souvent porteurs de code malveillant et peuvent perturber plus ou moins gravement le fonctionnement de l'ordinateur infecté. Ils se répandent *via* les réseaux informatiques ou des dispositifs périphériques comme les clés USB.

3. https://malwarehunterteam.com.

4. www.loria.fr

07.02.2019 / Actu IA

Actualité

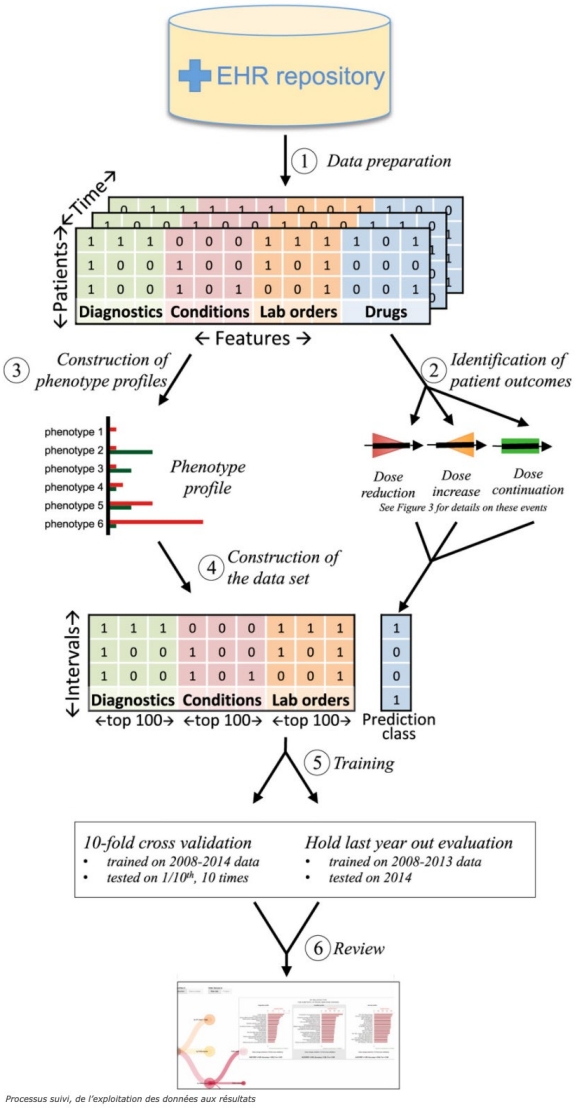
Ajustement à l'aide de l'intelligence artificielle du dosage des chimiothérapies

Par ActuIA - 9 février 2019

Des chercheurs proposent un algorithme destiné à ajuster les dosages de chimiothérapies. Les résultats de la recherche menée par Adrien Coulet, Nicolas Jay (Université de Lorraine, Inria, LORIA), Michel Dumontier (Université de Maastricht) en collaboration avec le Service d'Evaluation et d'Information Médicales du CHRU de Nancy et l'Université de Stanford mettent en avant l'efficacité de l'intelligence artificielle dans l'adaptation du dosage des médicaments aux patients.

La prescription de doses médicamenteuses non adaptées aux patients engendrerait à elle seule 280 000 admissions annuelles par an aux Etats-Unis. Au-delà de l'inconfort et de la souffrance générés par les effets secondaires, elles peuvent notamment engendrer des dysfonctions du système rénal, des intéractions médicamenteuses indésirables réduisant l'efficacité du traitement ou le rendant toxique.

Les chercheurs ont exploité des données anonymisées issues des hôpitaux universitaires de Stanford qui sont informatisées depuis des années et constituent donc une précieuse base de données d'informations pour la recherche médicale.



Processus suivi, de l'exploitation des données aux résultats

En mettant en oeuvre une méthode d'apprentissage de type Random Forest (forêt d'arbres aléatoires) sur des données de différentes natures (résultats d'analyses, notes et ordonnances..), les chercheurs ont pu prédire les ajustements nécessaires avec une fiabilité (AUC) allant de 0.70 à 0.95 pour 23 médicaments de 22 classes. La prédiction s'est révélée efficace dès la première prescription.

Les chercheurs souhaitent désormais pouvoir adapter cette méthode à l'environnement scientifique, social et légal des hôpitaux français.

Le détail de la recherche, publiée dans Nature Scientific Reports est disponible sur : https://www.nature.com/articles/s41598-018-33980-0

THÉMATIQUES Recherche en intelligence artificielle

LIRE PLUS D'ACTUS IA SUR Adrien Coulet CHRU de Nancy CNRS INRIA LORIA Michel Dumontier Nicolas Jay Université de Lorraine Université de Stanford

07.03.2019 / L'Informaticien - Dossier

Christophe Guillemin / jeudi 7 mars 2019 / Thèmes: Doss

5G et sécurité

Des enjeux bien supérieurs à la 4G

Des faiblesses subsistent dans certains protocoles hérités de la 4G et même de la 3G. Le niveau de sécurité de la 5G sera-t-il à la hauteur des enjeux ? Quelques éléments de réponse ici.

Les débits de la 5G seront au moins 10 fois supérieurs à ceux de la 4G, mais ils augmentent aussi la puissance des attaques DDoS.

La téléphonie de cinquième génération est une technologie de rupture, dont l'ambition est de couvrir des usages bien plus larges que ceux de la 3G et de la 4G. À la convergence des communications mobile et fixe, elle pourra aussi bien servir à connecter un smartphone ou un véhicule en mode nomade, qu'un bâtiment ou encore des capteurs IoT en mode sédentaire. Selon ses principaux promoteurs, la 5G favoriserait ainsi l'émergence d'un monde où la connexion sans-fil serait la norme, et le filaire une exception. De quoi rebattre les cartes de la sécurité informatique, qui va devoir se concentrer de plus en plus sur la protection des communications radio, que ce soit en entreprise comme dans la vie quotidienne.

« *Les enjeux de sécurité liés à la 5G vont bien au-delà de la téléphonie mobile. Ils sont proportionnels aux multiples usages attendus pour cette technologie* », résume ainsi Viktor Arvidsson, directeur stratégie et innovation d'Ericsson France. Un avis partagé par Gwenael Rouillec, directeur cybersécurité de Huawei France : « *La sécurité de la 5G est un enjeu global, touchant des domaines aussi variés que les transports, le bâtiment, la médecine ou l'industrie. La 5G a vocation à être omniprésente, la question de sa sécurité le sera tout autant.* » Pour Zscaler, éditeur spécialisé en solutions de sécurité pour le Cloud : « *La 5G pourrait s'imposer comme une connectivité unique, assurant les communications au bureau, à la maison, dans les transports... Cette démultiplication des usages, entraîne une démultiplication des risques de sécurité* », estime Yogi Chandiramani, directeur technique EMEA.

Les premières expérimentations 5G en conditions réelles, qui débutent cette année dans près d'une vingtaine de collectivités françaises, laissent en effet présager des applications extrêmement larges. Les équipementiers évoquent les usages classiques de la téléphonie mobile, qui prennent cependant « une nouvelle dimension » grâce la 5G.

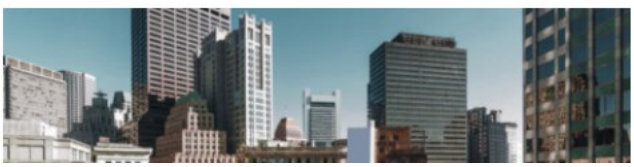
Côté téléphonie, les solutions de VoIP devraient ainsi largement se développer, prenant le pas sur les communications mobiles classiques. Côté data, l'accès à des services cloud devrait se généraliser en mode nomade, grâce aux débits de la 5G, au moins 10 fois supérieur à ceux de la 4G.

IoT et véhicules autonomes

Mais au-delà des connexions des personnes, la 5G devrait largement assurer la connexion de temps réel de machines ou « objets ». L'Internet of Things (IoT) est en effet un des grands domaines d'application prévus pour la 5G. Il s'agira de connecter des capteurs (mesures de qualité de l'air, télérelevé des compteurs d'eau, de gaz ou d'électricité...), mais aussi des caméras de vidéosurveillance ou même du mobilier urbain tels que les panneaux d'affichage dynamiques. Ceci grâce à la capacité d'accueillir jusqu'à 1 million d'objets connectés par km2 que prévoient les réseaux 5G.

Autre grand domaine d'application de la 5G : les transports. Il s'agira notamment de connecter des bus, afin de disposer d'un accès internet haut débit à bord. La 5G est également pressentie pour connecter les futures navettes et voitures autonomes. L'IA embarquée doit en effet accéder à des données hébergées dans le Cloud pour piloter le véhicule. Et en cas de problème, un superviseur pourrait reprendre le contrôle du véhicule à distance. Ceci grâce à la très faible latence de la 5G, de l'ordre de la milliseconde, soit 10 fois moins qu'en 4G (lire L'Informaticien n°170).

Parmi les autres applications évoquées pour la 5G : l'Industrie 4.0 (connexion des robots et autres équipements dans l'usine du futur), la télémédecine (assistance à distance pour certains actes, notamment les premiers secours), la connexion fixe des bâtiments en zone rurale (alternative à la fibre optique) ou encore le télépilotage de drones sur de très longues distances.



Avec la 5G, il faudra multiplier au moins par 4 le nombre d'antennes et même par 20 en zone urbaine ! Cela augmente d'autant le volume de cellules à sécuriser.

Des failles permettant de localiser un équipement 5G

Face à ces larges usages, le niveau de sécurité de la 5G a été sensiblement renforcé par rapport aux précédentes générations de technologies mobiles. « *Dès le début, la 5G a été pensée avec un niveau de sécurité supérieur à ceux de la 3G ou de la 4G* », assure ainsi Viktor Arvidsson d'Ericsson France. Mais si les améliorations ne font pas débat, des failles subsistent selon certains experts en sécurité. C'est la position de Jannik Dreier, maître de conférences à l'Université de Lorraine, enseignant à Télécom Nancy et chercheur au Loria (CNRS, Inria, Université de Lorraine), qui a mené des travaux avec l'ETH Zurich (Suisse) et l'Université de Dundee (Écosse). « *Nous avons étudié le protocole AKA (Authentification and Key Agreement). Il existe déjà en 3G et 4G, et a été décliné pour la 5G. Il s'agit d'une des principales briques de sécurité de la 5G car ce protocole sert à authentifier la connexion entre un équipement et le réseau mobile. Il sert également à générer la clé de chiffrement des communications* », explique le chercheur. « *Nos analyses ont montré que le protocole AKA 5G offre des améliorations sensibles par rapport aux normes précédentes 3G et 4G. Mais des failles persistent. Il se révèle en tout cas insuffisant pour atteindre tous les objectifs de sécurité critiques avec les hypothèses énoncées dans le standard.* »

Dans le détail, le protocole AKA 5G corrige des failles de sa version 3G et 4G en ce qui concerne les écoutes « passives » d'échanges de données réseau. Il ne s'agit pas d'écouter des conversations, mais d'identifier que tel équipement se connecte à tel endroit, à tel moment. Avec l'AKA 3G ou 4G, une partie du processus d'authentification reste en clair. Cette faiblesse peut être exploitée par une personne malveillante, grâce à un équipement appelé intercepteur IMSI (International Mobile Suscriber Identity). Il permet de surveiller en temps réel les données d'authentification sur le réseau mobile. « *Une personne malveillante peut savoir où est un téléphone et en déduire où est son propriétaire. Cela pose des problèmes de respect de la vie privée, mais aussi de sécurité. Savoir qu'une personne est éloignée de son domicile peut servir à préparer un cambriolage* », souligne Jannik Dreier.

Revoir en profondeur le protocole AKA ?

Avec l'AKA 5G, l'ensemble du processus d'authentification est chiffré. « *Cela élimine donc les risques d'écoutes passives. Mais il reste possible de lancer des attaques actives.* » Concrètement, l'attaquant pourrait intercepter un message d'authentification à un instant T, puis le renvoyer ultérieurement sur le réseau. Ce décalage entraînerait une erreur d'authentification, qui va générer des messages d'erreur. En interprétant ces messages d'erreurs, l'attaquant pourrait en déduire quel combiné est connecté au réseau et même le localiser. « *Cela ne serait pas si complexe à réaliser* », assure Jannik Dreier. Le chercheur indique avoir transmis toutes les informations nécessaires au 3GPP pour corriger la faille. « *Mais cela nécessite de revoir en profondeur le protocole AKA. Je ne suis pas certain que cela sera possible pour le lancement des premiers services commerciaux attendus pour 2020 en France. Nous espérons, en revanche, que ce sera le cas pour la seconde vague de déploiement de la 5G, prévue à l'horizon 2025.* »

D'autres observations, plus mineures, ont été faites par cette équipe internationale de chercheurs. Il subsiste notamment une imprécision dans la norme 5G au niveau de la connexion simultanée de deux objets sur une même cellule. « C'est une faille potentielle dans l'échange d'informations entre l'antenne et les serveurs réseau de l'opérateur. Elle pourrait entraîner un mélange ponctuel des identifications des téléphones, et facturer par exemple un appareil pour un service utilisé par un autre. » Une faiblesse qui reste cependant relativement facile à corriger sur les réseaux des opérateurs, en ajoutant par exemple des valeurs dans les messages d'authentification, indique le chercheur.

L'héritage des failles des protocoles de signalisation SS7 et Diameter

L'agence européenne chargée de la sécurité des réseaux et de l'information (Enisa) a également mené des travaux sur la sécurité de la 5G. Dans un rapport paru en 20181, elle pointe les faiblesses des protocoles de signalisation SS7 et Diameter. Le premier sert à superviser l'interconnexion des appels ou l'envoi de SMS sur le réseau mobile – d'où vient un appel, vers quel numéro doit-il être envoyé, la ligne est-elle disponible… Le second est utilisé pour l'interconnexion des équipements du cœur de réseau. Ces protocoles, déjà utilisés sur les réseaux 2G, 3G et 4G, se retrouvent également dans la norme 5G. Or, ils ne sont pas exempts de failles, souligne l'Enisa. « *L'opérateur O2 en Allemagne a confirmé que certains clients avaient eu leurs comptes piratés par des attaquants utilisant SS7 pour intercepter et rediriger des SMS contenants des numéros de transaction mobile (mTAN)* », indique l'agence européenne. Ces mTAN servent notamment à envoyer des codes de validation pour des transactions bancaires. Concernant Diameter, ce protocole a été exploité pour lancer des attaques DDoS (déni de service) sur des équipements connectés au réseau 4G ; des attaques par saturation qui seraient encore plus puissantes avec les débits de la 5G. « *Plusieurs propositions visant à sécuriser SS7 et Diameter n'ont jamais été adoptées par l'industrie – MAPsec, TCAPsec, Diameter over IPsec, Diameter over SCTP/DTLS* », conclut l'agence européenne. Elle recommande aux industriels des télécoms de reconsidérer ces solutions et de prévoir un renforcement global de la sécurité de SS7 et Diameter, notamment via des pare-feu spécifiques.

Au moins quatre fois plus d'antennes à sécuriser

La 5G pose d'autres problématiques de sécurité, un peu moins techniques, mais tout aussi importantes. La première est la multiplication des acteurs qui seront impliqués dans l'exploitation de cette technologie. Au-delà des opérateurs et équipementiers télécoms, des start-up IoT, des industriels du transport et des fournisseurs de services cloud 5G, pourraient intégrer la chaîne de valeur. « *Or, plus il y a de partenaires, plus il y a de risques de sécurité. Il faudra donc que les acteurs de la filière 5G collaborent davantage autour des questions de sécurité. Car, en face, les hackers s'échangent régulièrement des informations sur les failles et leur exploitation* », a déclaré Jonas Halldin, CISO (Chief Information Security Officer) de Zacco, cabinet de consultants danois spécialisé dans la protection de la propriété intellectuelle des entreprises. Il s'exprimait lors d'une table ronde organisée par Ericsson en 20182. « *Nous allons en effet devoir travailler davantage en écosystème* », confirme Gwenael Rouillec, chez Huawei. Autre problématique : la densification des réseaux 5G. Pour atteindre ses très hauts débits et sa faible latence, la 5G mise sur une multiplication du nombre d'antennes. Les opérateurs prévoient au moins 4 fois plus d'antennes en moyenne. Un ratio qui pourrait grimper à x20 dans des zones urbaines denses, comme à Paris. La 5G va donc nécessiter davantage de protections pour ces équipements, y compris des protections physiques pour empêcher l'accès aux installations et d'éventuelles dégradations. « *Une des solutions sur lesquelles nous travaillons est d'intégrer, de manière invisible, les antennes 5G dans du mobilier urbain, comme les luminaires, les feux rouges ou les abribus* », explique-t-on chez Huawei France. Notons que Nokia travaille également avec Signify (ex-Philips Lighting) autour de l'intégration d'antennes 5G dans le réseau d'éclairage public. Une expérimentation est prévue à Paris en 2019 Enfin, tous les acteurs s'accordent sur un point : avec la 5G, le chiffrement des communications devra être quasi-systématique. « *Il va falloir généraliser les sessions chiffrées entre les clients, les applications et les serveurs. Les outils VPN vont également devoir évoluer pour être plus largement utilisés, notamment grâce à l'authentification automatique* », estime Yogi Chandiramani, chez Zscaler. Même son de cloches chez Ericsson et Huawei, pour qui le chiffrement devient incontournable avec la 5G.

Une question qui reste ouverte

Au final, la sécurité de la 5G serat-elle à la hauteur des enjeux ? Les industriels se veulent bien entendu rassurants. « *Il faut éviter le catastrophisme. La sécurité ne sera pas un point bloquant du déploiement de la 5G* », assure ainsi Viktor Arvidsson. Contactés par notre rédaction, les principaux opérateurs mobiles français n'ont cependant pas souhaité s'exprimer sur cette question de la sécurité de la 5G, manifestement encore sensible. Ils indiquent préférer poursuivre leurs développements techniques et leurs expérimentations avant de communiquer sur le sujet. La sécurité de la 5G devrait encore faire débat d'ici les premiers déploiements en 2020. Et lorsqu'ils seront massifs, elle pourrait même s'imposer comme un sujet prépondérant de la sécurité informatique. ❍

1 Rapport de l'Enisa : « Signalling Security in Telecom SS7/Diameter/5G. EU level a ssessment of the current situation », 30 pages – paru en mars 2018
2 « Ringside Session 2 », table ronde organisée à Londres par Ericsson en juin 2018

Huawei accusé d'espionnage

En 2018, plusieurs pays ont fait part de leurs vives inquiétudes quant à l'utilisation de produits Huawei pour le déploiement de la 5G. Aux États-Unis, en Australie, en Nouvelle-Zélande, au Japon comme au Royaume-Uni, les équipements du géant chinois ne sont plus les bienvenus. Outre-Atlantique, un décret de Donald Trump pourrait même être déposé en ce début 2019 pour interdire aux entreprises américaines de se fournir auprès de « *groupes télécoms étrangers présentant d'importants risques pour la sécurité nationale* ». À l'origine de cette mise au ban, des suspicions d'espionnage et même de cyberattaques via l'intégration de portes dérobées dans les équipements Huawei. Des accusations démenties par le groupe de Pékin, qui pointe la guerre commerciale qui lui livre les États-Unis. « *Nous invitons tous les acteurs qui le souhaitent à venir vérifier qu'il n'y a pas de backdoor dans nos produits* », indique Gwenael Rouillec. La France, via l'Anssi, n'a quant à elle pas évoqué de mesures concernant l'équipementier chinois.

23.02.2019 / L'Est Républicain

NANCY *Transports*

Padam gagne le marché francilien

L'entreprise nancéienne Padam, alliée au groupe Setec Its, a été sélectionnée pour déployer la centrale régionale de transport à la demande (TAD) en Île-de-France.

Bonne nouvelle pour Padam. Créée en 2014 par trois jeunes ingénieurs de l'école Polytechnique de Paris et des Ponts & Chaussées, cette entreprise installée au sein de l'accélérateur de start-up Paddock French Tech de Nancy vient de remporter un gros marché.

L'organisation Île-de-France Mobilités présidée par Valérie Pécresse vient de la sélectionner avec une filiale du groupe Setec pour développer les transports à la demande en région francilienne.

Du transport sur-mesure

« On est très contents, notamment parce que cela valide nos hypothèses de travail », se félicite Thibault Lécuyer, directeur marketing de Padam. Le concept : apporter des solutions de transport sur-mesure aux personnes qui résident dans les territoires les moins bien desservis. « On a toujours pensé qu'il devait être aussi simple de commander un bus qu'un VTC », explique le directeur marketing. Son entreprise aura pour mission de développer l'application smartphone ainsi que les algorithmes de simplification de trajet. « On garde l'idée du bus, mais on supprime celle de la ligne, qui est remplacée par des points », fixés en fonction de la demande des usagers.

Le résultat d'un programme du LORIA

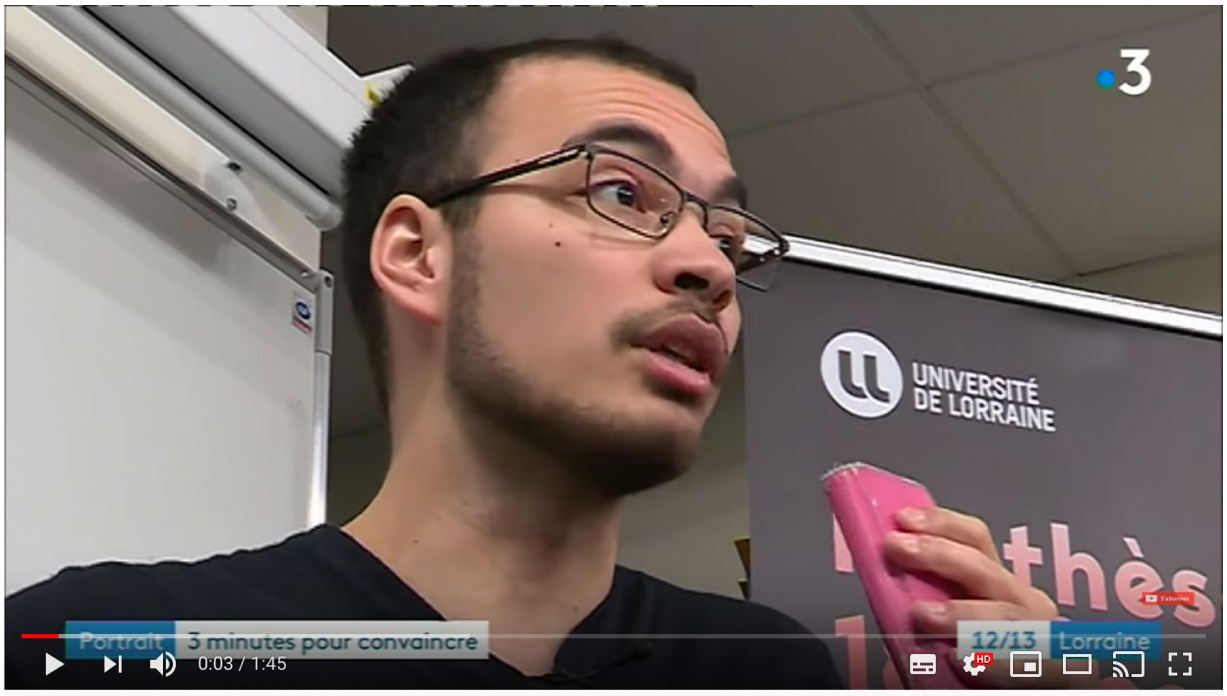
L'attribution de ce marché est le résultat d'un « travail de longue haleine ». Il s'est appuyé sur le programme de recherche d'une institution elle aussi nancéienne : le LORIA (Laboratoire lorrain de recherche en informatique et ses applications).

Padam a désormais du pain sur la planche : « Nous devons développer la centrale dans 4 territoires d'ici mai 2019 », précise Thibault Lécuyer ? « Puis 10 pour 2019 et enfin 33 sur 4 ans », soit la quasi-totalité de la région francilienne. Du travail qui va permettre à l'entreprise de grandir, mais aussi d'« évangéliser » les collectivités territoriales au transport à la demande dynamique. Car ce système permettrait de rendre les transports à la fois plus efficaces et moins chers selon les conclusions de recherches de Padam. Un mode de transport renforcé par l'intelligence artificielle qui conviendrait particulièrement aux territoires les plus ruraux. Le concept pourrait-il un jour arriver à Nancy ? « C'est une des idées qui sont en discussion avec Keolis depuis qu'ils ont repris la délégation de service public », confie le directeur marketing.

Le transport à la demande répond aux besoins des habitants des zones les moins denses. Photo AFP

Élie GUCKERT

15.03.2019 / France 3 Lorraine



Ma thèse en 180 secondes : Portrait d'Itsaka Rakotonirina

[Lien vers la vidéo sur YouTube.]

25.02.2019 / L'Est Républicain

INNOVATION > *Intelligence artificielle*

Chimiothérapie mieux ajustée

Un chercheur nancéien a créé un algorithme à partir de données médicales qui permet de prédire si les patients ont besoin d'une dose plus faible de médicaments que la norme standard. Notamment en chimiothérapie.

Adrien Coulet : « Pouvoir s'appuyer sur un nombre conséquent de données de patients permet de contribuer à ce qu'on appelle aujourd'hui la médecine de précision. » Photo DR

L'intelligence artificielle (IA) au service de la prescription médicale : cette innovation algorithmique permet d'ajuster le dosage au besoin du patient, en suggérant, par exemple, une dose plus faible, particulièrement en chimiothérapie. En réduisant aussi le temps nécessaire pour définir la dose optimale, et ainsi prévenir les effets indésirables, parfois lourds, supportés par les malades. Ce qui contribue aussi à la médecine dite de précision.

C'est un chercheur nancéien en informatique, Adrien Coulet, membre de l'équipe des Orpailleurs, équipe commune à l'Inria (Institut national de recherche en informatique et automatique) et au Loria (Laboratoire lorrain de recherche en informatique et ses applications), qui est à l'origine de cette découverte.

La dénomination de l'équipe de recherche ne doit rien au hasard. « On cherche l'or dans les masses de données professionnelles », sourit Adrien Coulet. Et c'est précisément cette quête approfondie qui fait toute l'originalité du nouvel algorithme.

De multiples applications

Actuellement en résidence à la prestigieuse université américaine de Stanford, au cœur de la Silicon Valley, cet informaticien a commencé ses recherches à Nancy, en particulier en collaboration avec le professeur Nicolas Lejay, chef du service d'évaluation et d'information médicales du CHRU et membre du Loria. L'équipe américaine associée, dirigée par Nigam H.Shah, spécialiste de l'analyse prédictive appliquées aux données médicales, a pu s'appuyer sur un historique plus que conséquent : « Près d'un million de dossiers de patients sur 5 à 10 ans de données », souligne Adrien Coulet (lire ci-dessous). Un corpus qui a permis de définir des typologies pertinentes de patients et donc de nourrir le plus finement possible « un ensemble d'arborescences », composées d'arbres dits « de décision », constituant une aide précieuse à la prescription. Ces travaux viennent de faire l'objet d'une publication dans la revue de référence *ScientificReports*.

L'application de l'algorithme ne se limite pas à la cancérologie. Les chercheurs ont démontré qu'il fonctionnait bien aussi avec les immunodépresseurs après une greffe, ou avec les anticoagulants.

Philippe RIVET

Protection des données et éthique

L'intelligence artificielle suscite des craintes, perçue comme intrusive, à l'insu des personnes. Adrien Coulet se veut rassurant, et souligne l'utilité de l'IA dans le domaine de la santé. « Ceux qui font peur avec l'IA cherchent à se faire de la pub. Le problème tient plutôt à l'accès aux données, il faut savoir lesquelles on choisit. À Stanford, les patients donnent volontiers leur consentement, car le caractère universitaire de l'hôpital lui confère une réputation sérieuse. Le consentement se manifeste plus fortement quand il s'agit non plus de recherche fondamentale mais d'application visant à améliorer les soins. Toutes les données sont anonymisées. Notre recherche se déroule dans un cadre bien défini : les études sont présentées à un comité d'éthique qui valide le protocole. »

Selon Adrien Coulet, l'algorithme mis au point à Stanford pourrait fonctionner dans les hôpitaux français « à partir d'une base de quelques milliers de patients avec au moins un historique d'un an ». Sous réserve de dossiers médicaux informatisés et partagés, et du consentement des patients. Qui ne peuvent être que sensibles à un traitement plus individualisé.

La 5G en mal de sécurité

NUMÉRIQUE

Informatique. Avec un débit dix fois supérieur à celui de la 4G, la 5G fait rêver. Mais avant que ce bolide ne débarque dans nos mobiles en 2020, il reste un point crucial à améliorer : la sécurité.

PAR MARTIN KOPPE

Avec des pointes prévues à 20 gigabits par seconde, la tempête 5G devrait atteindre nos téléphones en 2020. Les utilisateurs se réjouissent de l'approche de cette cinquième génération de standard de télécommunication mobile qui, avec des débits jusqu'à dix fois plus rapides que la 4G, promet de s'adapter à des usages nomades toujours plus gourmands en données.

Alors que ce standard est encore en cours de conception au 3GPP[1], organisme qui regroupe des représentants d'industriels et d'opérateurs téléphoniques, différentes équipes de recherche profitent de cette phase d'élaboration pour tester et renforcer la future norme.

Ainsi, au Laboratoire lorrain de recherche en informatique et ses applications (Loria)[2], Jannik Dreier et ses collègues proposent différentes pistes d'amélioration. « *Le 3GPP met surtout en avant la hausse du débit,* explique ce maître de conférences à Télécom Nancy, *mais les protocoles changent aussi à chaque nouvelle génération, notamment en matière de sécurité.* »

Des failles anciennes

En collaboration avec les chercheurs de l'École polytechnique fédérale de Zurich et de l'université de Dundee en Écosse, Jannik Dreier a souligné la survivance de failles de sécurité dans la nouvelle norme 5G, lors de la conférence CCS[3] de Toronto, en octobre 2018. « *La téléphonie mobile a hérité de points faibles qui remontent à son tout premier protocole d'identification,* déplore-t-il. *Toute la sécurité repose sur les cartes SIM, où sont stockées les clés d'identifications partagées avec les réseaux.* » Les problèmes de sécurité sont inhérents aux technologies sans fil car, contrairement à un transport de données confiné dans un câble, rien ne protège les informations quand elles transitent par la voie des airs.

Utilisateur suivi à la trace

La sécurité passe donc par la capacité du téléphone et du réseau à s'identifier et à s'authentifier lors de la connexion. Dans le même temps, toutes les informations personnelles et les données du détenteur de la ligne téléphonique doivent être préservées. Mais le système n'est pas parfait. Jannik Dreier pointe ainsi les risques de traçabilité de l'utilisateur lorsqu'on peut identifier puis suivre le téléphone. Une opération encore aujourd'hui aisément réalisable avec la 4G, grâce à des appareils comme les intercepteurs Imsi[4] qui scrutent les échanges entre le téléphone mobile et les antennes-relais du réseau pour pister leur cible.

« *La 5G va régler le problème face à un intercepteur passif, qui ne fait qu'écouter,* détaille Jannik Dreier. *Mais si quelqu'un injecte des messages dans la communication entre le téléphone et l'antenne du réseau, ce qui est relativement facile, alors il peut à nouveau tracer le mobile et son utilisateur.* »

Là encore, c'est l'architecture historique des téléphones mobiles qui est en cause. Comme les premières cartes SIM ne pouvaient pas

© M. BENITEZ/GETTY IMAGES EUROPE/GETTY IMAGES/AFP

L'année dernière, au Congrès mondial du mobile, à Barcelone, la 5G était à l'honneur.

1. Pour *3rd Generation Partnership Project,* « Projet de partenariat de troisième génération ». 2. Unité CNRS/Université de Lorraine/Inria. 3. Pour *Computer and Communications Security,* « Sécurité des ordinateurs et des communications ». 4. Pour *International Mobile Subscriber Identity,* « Identifiant international de client mobile ». 5. Pour *Center for It-Security, Privacy & Accountability,* « Centre pour la sécurité, la vie privée et la responsabilité informatiques ». 6. Pour *Authentication and Key Agreement,* « Accord sur les clés d'authentification. »


© O. BERG/DPA/DPA PICTURE-ALLIANCE/AFP

◢ Des antennes-relais permettent de tester la 5G en conditions réelles, comme ici en Allemagne.

générer de valeurs aléatoires, tout reposait et repose toujours sur un système de compteur. Conçu pour ne pas recevoir plusieurs fois un même message, celui-ci réagit quand il est sollicité.

« Pourtant, les cartes d'aujourd'hui pourraient s'en passer, car elles peuvent générer des valeurs aléatoires, déplore le chercheur, *mais apparemment les décideurs n'ont pas voulu changer le standard aussi profondément. Les outils exploitant la traçabilité sont notamment utilisés par la police et les services de renseignement. Ils leur permettent de savoir qui était à proximité d'une scène de crime, mais aussi d'une manifestation. C'est très pratique pour eux, mais engendre un risque de surveillance de masse »,* poursuit-il. Difficile en effet de ne pas craindre de dérives, sans même compter le détournement par des criminels, quand les deux tiers de la population mondiale utilisent un téléphone portable.

Appels facturés à autrui

Conçu en partenariat avec l'École polytechnique de Zurich, le Loria et le Cispa[5] de Sarrebruck, l'outil de modélisation Tamarin permet d'analyser la fiabilité d'un protocole donné. Jannik Dreier et ses collègues ont ainsi testé la version adaptée à la 5G d'AKA[6], le protocole de sécurité implémenté depuis la 3G que le 3GPP veut continuer d'améliorer. *« On ne fait pas que dénicher des failles et nous ne cherchons pas qu'à casser,* souligne Jannik Dreier. *Nous procédons à des vérifications formelles afin d'améliorer la sécurité. »*

Si le protocole ne contient pas de faille, Tamarin établit alors une preuve mathématique de sa sécurité. En revanche, en cas de problème, l'outil génère une description de l'attaque identifiée. Les chercheurs ont ainsi découvert un défaut pouvant amener à une situation où les appels sont facturés à quelqu'un d'autre, si deux téléphones sont utilisés en même temps et à proximité.

Logiciel à améliorer

« Même si cette faille est probablement difficile à exploiter en pratique, elle n'est pas exclue par le standard. Nous avons envoyé ces résultats au 3GPP et ils nous ont fait un premier retour assez bref, précise le chercheur. *Le processus prend en effet du temps, car il passe par des réunions physiques, des propositions, puis, enfin, un vote. Nous ne faisons pas partie de ces instances, cela reste leur choix de modifier ou non le protocole. »*

Malgré l'approche de l'échéance de 2020 et l'arrivée officielle de la 5G, de nombreuses améliorations peuvent encore être apportées, surtout au niveau logiciel. Les chercheurs du Loria travaillent d'ailleurs à adapter des outils tels que Tamarin, afin que les ingénieurs puissent s'en servir dès la conception.

La partie matériel et équipement est en revanche très difficile à changer une fois celui-ci produit et déployé. *« Les problèmes de traçabilité ne vont malheureusement pas être réglés uniquement avec ce genre de petits changements,* insiste Jannik Dreier. *Il faudrait tout simplement arrêter d'utiliser un compteur dans les cartes SIM, mais cela exigerait une refonte totale du protocole... »* ||

Lire l'intégralité de l'article sur **lejournal.cnrs.fr**

En bref

LE BILAN SOCIAL ET PARITÉ 2017

L'édition 2017 du Bilan social et parité du CNRS est en ligne. Ce document, téléchargeable sur le site du CNRS[1] mais aussi consultable sur tablettes et Smartphones au format (Epub)[2], présente l'essentiel des informations relatives aux personnes titulaires et contractuelles employées par le CNRS en 2017. Le Bilan social et parité offre une information statistique **complète sur l'ensemble des personnels rémunérés par le CNRS, chercheurs comme ingénieurs et techniciens, permanents comme contractuels.**

1. http://www.cnrs.fr/fr/documentation. 2. Pour Electronic Publication.

DEUX ACCORDS AVEC LA BIBLIOTHECA ALEXANDRINA

Le 28 janvier, deux accords ont été signés entre le CNRS, la Bibliotheca Alexandrina, à Alexandrie, en Égypte, et le ministère français de l'Europe et des Affaires étrangères. **Ces accords portent sur le programme des archives de presse du Centre d'études et de documentation économiques, juridiques** et sociales (Cedej) (CNRS/ministère des Affaires étrangères) et sur la numérisation **d'une partie de sa bibliothèque. Le Cedej fait partie du réseau des unités mixtes des instituts français de recherche à l'étranger (Umifre).**

LA PLATEFORME TEMPOS INAUGURÉE

C'est une plateforme unique de microscopie électronique, baptisée Tempos[3], qui a été inaugurée le 18 décembre 2018, à Orsay. Financé dans le cadre d'un Équipex (Équipement d'excellence), ce projet est porté par l'Université Paris-Sud, le CNRS, l'École polytechnique et le CEA. Les industriels Saint-Gobain et Thales sont également impliqués, à travers leurs départements R&D. Cette plateforme permettra d'étudier les propriétés des nanomatériaux : de leurs **mécanismes de croissance à leurs propriétés physiques aux échelles les plus locales. Pour cela, elle se compose de deux équipements dédiés à l'étude de la croissance et de la physique des nano-objets, Chromatem et Nanomax, complétés par une installation de microscopie électronique, Nanotem.**

3. Pour Transmission Electron Microscopy.


© C. FRESILLON/CNRS PHOTOTHÈQUE

03.03.2019 / Pixes

RESSOURCES

ON UTILISE DES RESSOURCES CLÉS EN MAIN QUI ONT FAIT LEURS PREUVES SUR LE TERRAIN

RESSOURCE 2019, 03 MARS . NOMS PROPRES . HISTOIRE DE L'INFORMATIQUE . CULTURE GÉNÉRALE . JEU . *HISTOIRE DU NUMÉRIQUE* . *JEU CARTES*

JEU DES 7 FAMILLES DE L'INFORMATIQUE : UNE HISTOIRE DU NUMÉRIQUE EN JOUANT AUX CARTES !

L'informatique est une science diverse ! Ce jeu est l'occasion de présenter des figures importantes qui ont travaillé et travaillent à façonner la discipline et à la faire évoluer au cours du temps.

Le format « jeu de 7 familles » permet de mettre en lumière 42 (+1) personnalités, et de montrer que l'Histoire de l'informatique ne se résume pas à celle des ordinateurs.

L'informatique se développe à travers une communauté scientifique qui fait vivre la discipline et interagit avec d'autres. Nous proposons dans ce jeu de découvrir 7 de ses grandes thématiques : Algorithmes & programmation, Mathématiques & informatique, Sécurité & confidentialité, Systèmes & réseaux, Machines & Composants, Intelligence Artificielle, Interaction Homme-Machine

Vous pouvez consulter l'intégralité du dossier sur le site Interstices.

En complément :

Le projet a été initié par l'équipe du site interstices.info, dans la dynamique de la fondation Blaise Pascal. Il a reçu le soutien financier de cette fondation, ainsi que d'Inria, de l'Université de Lorraine et de la Société Informatique de France (SIF).

Le projet a été porté par Maxime Amblard, maître de conférences en informatique à l'Université de Lorraine (Loria), responsable scientifique adjoint d'interstices.info. Si l'informatique est une science qui se construit par le travail d'une large communauté, il en est de même pour ce jeu qui a été conçu par un groupe de travail d'une dizaine de personnes, scientifiques et professionnels de la médiation.

Et maintenant si on jouait ?

COMMENT UTILISER LE JEU DE 7 FAMILLES : VOICI QUELQUES IDÉES D'UTILISATION.

- avec les personnalités : présenter une carte et ouvrir la discussion sur la problématique de la personnalité en partant de la description dans la notice, ou faites un quiz à la carte ou sur le mode « Questions pour un champion » faire deviner une personnalité à travers une série d'affirmations…
- avec les familles : ouvrir une discussion, faire un quiz, proposer de faire des recherches et rédiger des mini-biographies…
- avec les objets : proposer d'associer les objets et les personnalités….
- avec les « brefs » : mélanger toutes les phrases et essayer de les rassembler par famille…
- avec la chronologie : faire un Timeline…
- avec les cartes : réaliser des activités débranchées…

Voici les idées en partage…

- des propositions d'activités
- questions de quiz classées par famille
- « qui suis-je?

N'hésitez pas à partager aussi les vôtres !

21.03.2019 / Le Journal de la Haute Marne

L'intelligence artificielle, pourquoi, comment ?

L'enseignant-chercheur Nazim Fatès était au lycée Saint-Exupéry cette semaine, pour un échange passionnant sur le thème de l'intelligence artificielle.

21.03.2019 / France 3 Lorraine

Les chercheurs du Loria scrutent les visiteurs du musée des Beaux-Arts de Nancy à la loupe

Lien vers la vidéo sur YouTube.

29.04.2019 / Les Tablettes Lorraines

NTIC - INRIA

Consortium pour assistant vocal sain

Développer un assistant vocal plus respectueux de la vie privée d'ici trois ans ! Objectif affiché des scientifiques du projet Comprise (Cost-effective, Multilingual, Privacy-driven-voice-enabled services), une action recherche et innovation financée par le programme Horizon 2020 de l'Union européenne. Ce projet est coordonné par Emmanuel Vincent, chercheurs à l'Inria Nancy - Grand Est. Les outils et technologies d'interaction vocale ont récemment essaimé, de l'assistant Alexa d'Amazon aux radios et TV contrôlées vocalement, la voix est en passe de remplacer le toucher ou le texte comme principal vecteur d'interaction avec les objets du quotidien. «*Le projet Comprise vise à accompagner, et même devancer, cette expansion en fournissant les outils et les méthodologies nécessaires pour rendre les interactions vocales plus sûres, économiques, et inclusives dans différentes langues*», assurent les membres du consortium. Le tout avec une forte volonté de voir se développer ce type d'outil notamment au sein des PME «*leur permettant de proposer de nouveaux services et de se développer.*»

MOBILITÉ

Loria - Padam : le transport augmenté

L'ACTUELLE COLLABORATION ENTRE LE LABORATOIRE LORRAIN DE RECHERCHE EN INFORMATIQUE ET SES APPLICATIONS ET LA START-UP PARISIENNE PADAM A VOCATION À DÉPLOYER UN SERVICE DE TRANSPORTS EN COMMUN À LA DEMANDE, RÉPONDANT AUX ÉVOLUTIONS SOCIÉTALES. AU CŒUR DE L'ÉCOMOBILITÉ, CETTE TECHNOLOGIE EST EN COURS D'ÉLABORATION AU LORIA.

© Freepik

Penser les transports différemment.

Transport scolaire plus flexible, prise en charge des personnes à mobilité réduite facilitée, optimisation des flottes de bus en temps réel, en complémentarité des lignes régulières et des trains… La finalité est trouvée : faire du citoyen, non plus un consommateur lambda, mais bien un acteur de ses déplacements. Créée en 2014 par trois jeunes ingénieurs de l'école Polytechnique de Paris et des Ponts & Chaussées, la start-up Padam s'appuie sur l'intelligence artificielle pour transformer l'organisation des transports en commun et proposer un service à la demande, plus adapté aux besoins des usagers. Les solutions logicielles de Padam aident ainsi les opérateurs de transport par bus, publics et privés. En filigrane : optimiser en temps réel leurs flottes de véhicules avec une meilleure rentabilité économique. Déjà adoptée à Orléans ou à Lille, à l'international à Bristol et Padoue, Padam a été choisie par Île-de-France Mobilités, autorité organisatrice de l'ensemble des mobilités durables en région parisienne. Une centrale de réservation et de gestion des services de transport à la demande au niveau régional va se déployer ces mois prochains, avec une extension progressive d'ici quatre ans sur la totalité de la couronne francilienne. Ambitionnant d'étendre leur technologie à d'autres régions, les gérants de Padam regardent le Grand Est, le Luxembourg, le Belgique, l'Allemagne.

RÉPONSE SUR MESURE AUX ZONES LES MOINS DENSES

Accélérée par le Paddock French Tech de Nancy, Padam a noué une collaboration avec les compétences et l'expertise du Loria. Référent du partenariat inclus dans le programme de recherche du laboratoire lorrain et ses coopérations nationales et mondiales : Ammar Oulamara, professeur à l'Université de Lorraine, chercheur et responsable de l'équipe Optimist au Loria, par ailleurs enseignant à la Faculté des Sciences et de Technologies. Pour rappel, le Laboratoire lorrain de Recherche en Informatique et ses Applications, membre de la Fédération Charles Hermite (groupant les trois principaux laboratoires de recherche en mathématiques et sciences et technologies de l'information régionales) et du pôle scientifique Automatique, Mathématiques, Informatique et Interactions, est une unité mixte commune au CNRS, à l'Inria et à l'Université de Lorraine. Depuis 1997, sa mission est la recherche fondamentale et appliquée en sciences informatiques. Le Loria, ce sont 28 équipes en 5 départements, dont 15 sont communes avec l'Inria. Soit plus de 400 personnes. Pour l'heure, le projet Padam à l'échelle Grand Est en est aux phases d'études de potentialités et de faisabilité. Il s'agit d'adapter un produit dessiné à sa genèse pour les réalités parisiennes, à celles propres à des métropoles comme Nancy ou Metz par exemple. Avant de valider la version du logiciel, il faut en définir l'algorithme. La technologie finalisée et opérationnelle, viendra le temps de la mettre sur le marché des appels d'offres pour œuvrer avec les collectivités territoriales intéressées. Le système Padam va dans une logique refonte de la conceptualisation des transports en commun en milieux urbain et rural. Aux côtés des horaires fixes d'un tram ou d'un bus, la flexibilité et la réactivité vont s'immiscer. À l'heure où le tout-voiture cherche ses solutions alternatives, Padam entend contribuer au développement et à l'attractivité des territoires.

Laurent SIATKA

> *« Optimiser les flottes de transports urbains. »*

À propos d'écomobilité

Elle repose sur le développement des modes déplacements alternatifs et doux, comme la marche à pied, le vélo, les transports en commun. Afin de réduire les émissions de polluants et de gaz à effet de serre. En France, 50 % des déplacements en voiture en ville sont inférieurs à 3 km. 15 % d'entre eux sont inférieurs à 500 mètres.

Savoir partager l'espace urbain.

05.2019 / L'Est Républicain

COUP DE PROJECTEUR

La start-up nancéienne Cyber-Detect au salon VivaTech !

Organisée du 16 au 18 mai Portes de Versailles à Paris, la 4e édition du salon VivaTech est le rendez-vous annuel des innovations technologiques et des start-ups. Hébergée à Mines Nancy sur le campus Artem à Nancy, la start-up Cyber-Detect sera présente sur le stand du groupe Thalès. Proposant des solutions innovantes en cyberdéfense et en cybersécurité, Cyber-Detect est le fruit de dix années de recherche au Loria. Elle travaille notamment sur l'analyse morphologique des virus pour mieux les éradiquer.

03.05.2019 / L'Est Républicain

Le CNRS au cœur des relais pour ses 80 ans

Otelo, CRGP, ATILF, INIST, IJL2, Géoressources, LORIA, EMlex….Dans ce paysage des acronymes propres aux laboratoires nancéiens rattachés au CNRS, solution et résolution font souvent bon ménage. Alors lorsque se lève l'idée d'effectuer la course Ekiden pour fêter les 80 ans du CNRS, douze équipes sortent des labos sur l'initiative de Laurent Gobert, rattaché EMlex. « Ici c'est du hors-contexte, les gens se voient avec un autre regard. Lorsque j'ai lancé une petite devinette sur le chrono de leur collègue Polo lorsqu'il était plus jeune, dans les années 80 (NLdr : Paul Allé, rattaché hier à l'équipe de Cristallographie). Il était tout étonné sur 10 km, on m'a dit Paul Allé ? 28'47 ? non ! »

Et avis unanimes, sur ce marathon en relais, la thermochromie, le système de cyberphysique, ou autre la Cristallographie ne leur ont été d'aucun recours, " C'est aussi l'occasion de casser le mythe de la barbe et la blouse blanche mais aussi d'échanger entre nous. Entre labo, on ne se connaît pas nécessairement « reprenait Virginie Galtier, runneuse occasionnelle, qui avait mis les systèmes de cyberphysiques en aparté. D'autres avait effectué pendant deux mois une réathlétisation et y on pris goût : » Après ceci, je suis d'abord fière, mais je compte aussi réinvestir et continuer « savourait rougie d'effort Cécilia Klespert (Otelo) au terme du troisième relais où sa collègue Catherine Pierson savourait cet effort commun : » J'ai fait ce que j'ai pu avec mon genou, mais pour l'ambiance cela restera un souvenir ". A 80 ans cette année, le CNRS promet d'en servir quelques autres.

Casquette noire et sentiment du devoir accompli. Pour ses 80 ans, le CNRS est venu en nombre avec 12 équipes.
Photo ER/Maxime SCHLERET

15.05.2019 / L'Est Républicain

NANCY Festival

Pint of science : les chercheurs vous donnent rendez-vous au bar

Et de trois : l'opération « Pint of science » revient à l'affiche du 20 au 22 mai. En France, des bars de 54 villes accueilleront plus de 800 chercheurs qui viendront discuter avec le public. A Nancy, la taverne de l'Irlandais, le Barami, les Seigneurs seront de la partie.

En 2013, deux chercheurs londoniens décidaient de sortir des murs de leur labo pour aller discuter science, sans filtre ni protocole, avec le grand public dans un pub. Bref, rien à voir avec le côté un peu strict de la conférence. Cinq ans plus tard, « Pint of science », c'était devenu 318 soirées dans 41 villes et 12.000 participants. Et ça continue.

L'édition 2019 du festival qui se déroulera simultanément dans une vingtaine de pays mobilisera quelque 800 chercheurs en France dans des bars de 54 villes.

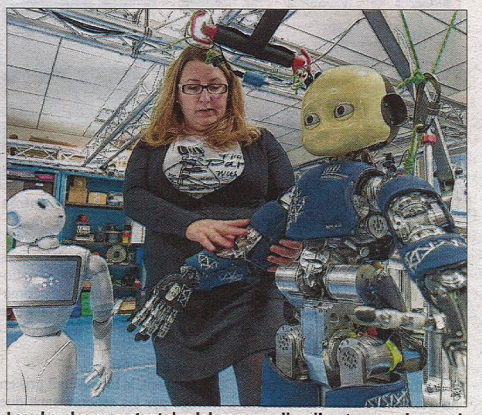
L'université de Lorraine et des unités mixte CNRS seront évidemment « accoudées au comptoir ». 36 chercheurs et doctorants seront de la partie dans six bars de Nancy, Metz ou encore Saint-Dié : « Le but ? Présenter, échanger et partager autour de sujets de recherche en lien avec l'actualité. »

Informatique, forêt, cancer...

Dans la cité ducale, on pourra prendre une pinte de science au Barami, situé Grande Rue. Le lundi 20 mai, on y causera « contre-attaque des plantes », de leur vulnérabilité, de leur défense avec le Laboratoire Agronomie et Environnement (INRA, Université de Lorraine). Le mardi 21, le thème qui se fera mousser : paysages industriels, entre rejets et fascination, avec le LOTERR – Centre de recherche en géographie. Le 22 ce sera robots en détresse avec le Laboratoire Lorrain de Recherche en Informatique et ses Applications - Loria-Inria.

À la Taverne de l'Irlandais, rue Mazagran, on parlera des molécules pour soigner le cancer, le lundi 20 mai avec le Laboratoire Réactions et Génie des Procédés et le Laboratoire Lorrain de Chimie Moléculaire. Mardi 21, même endroit : acheter sous influences avec le Centre Européen de Recherche en Économie. Mercredi 22 : Sylvestre, prends ton tricycle ou mieux comprendre le fonctionnement de la forêt avec l'Unité de recherche Biogéochimie des Écosystèmes Forestiers – BEF (INRA).

A noter aussi une séance enfants au Barami le mercredi 22 mai à 15 h 30 avec le Loria. Thème : l'informatique débranchée (à partir de 6 ans).



Les chercheurs sortent des labos pour aller discuter avec le grand public sur le thème, par exemple, des robots. Photo d'illustration ER/Patrice SAUCOURT

Pour tous ces rendez-vous, réservation obligatoire (2 € la soirée) sur pintofscience.fr

G.U.

16.05.2019 / L'Est Républicain

TOMBLAINE Pédagogie

Escape game pédagogique au collège Jean-Moulin

Messages cachés, code binaire, cadenas, algorithmique, cryptex, les élèves de 4e du collège Jean-Moulin ont agité leurs neurones pour contrer un virus malveillant et une armée de robots destructeurs des data centers. Ou quand l'apprentissage des mathématiques devient ludique.

Un bel exercice de stimulation collective mis en place par des étudiantes en sciences cognitives.

Les élèves du collège Jean-Moulin sont les derniers remparts contre un virus informatique. Tel est le scénario catastrophe d'un escape game pédagogique sur les mathématiques et l'informatique coordonné par Coralie Beller, professeur de mathématiques. Conduit dans le cadre d'un projet tutoré et encadré par Marie Duflot-Kremer, chercheuse au Loria, ce jeu d'évasion imaginé par Aurore Dupuy, Enora Gabory et Célia Kessassi, trois étudiantes en master 1 de sciences cognitives de la fac de Nancy, a débuté par un briefing et un test de positionnement.

Une mise en valeur des compétences

Les élèves avaient alors 60 minutes pour résoudre les neuf énigmes préparées par les étudiantes et sauver la planète de la disparition de l'informatique. Une mise en condition qui a fait mouche. Images et encodage, architecture d'un ordinateur, cryptographie, bases de données, cartes perforées, arbre binaire de recherche, algorithmique, portes logiques, adresses IP et routage, les collégiens ont phosphoré durant une heure, tout en abordant sans s'en rendre compte des compétences transversales dans le cadre de la démarche scientifique.

« C'est une pédagogie différente du cadre habituel qui permet de travailler divers champs d'étude, entre logique, lecture de consignes, écoute, entraide, communication, échanges et rigueur » explique Coralie Beller. « Cet exercice est très formateur car les élèves doivent s'organiser en autonomie, partager leurs compétences, mettre au service des autres leur perspicacité, surmonter ensemble les obstacles, et faire des essais pour réussir à ouvrir les cadenas qui entourent le coffre » S'ils pataugeaient trop, les étudiantes intervenaient subtilement pour les aiguiller vers une solution possible et leur permettre, après une heure d'intenses recherches, d'ouvrir le cadenas du coffre rempli de bonbons. Mission réussie !

21.05.2019 / L'Est Républicain

NANCY Éducation

Le collège Jean-Lamour inaugure son fablab

Le collège Jean Lamour est officiellement devenu l'un des établissements pilotes du programme « La Main à la pâte » ce lundi 20 mai. À cette occasion, le personnel enseignant et les élèves ont inauguré un fablab et présenté leurs travaux scientifiques.

Ce lundi après-midi, au collège Jean-Lamour, ce sont les élèves eux-mêmes qui font visiter leur établissement et qui présentent leurs travaux. Le 20 mai, l'établissement est officiellement devenu l'un des pilotes du programme « Les Mains à la pâte ».

Ouvrir aux sciences

« C'est un projet qui est soutenu par les Maisons pour la science », explique Mme Delon, la principale de Jean-Lamour.

« L'idée c'est d'ouvrir les enfants au monde de la recherche, des sciences et de la technologie ». Un travail réalisé en partenariat avec le Conseil départemental et l'Université de Lorraine, la marraine scientifique du collège, Anne Boyer, étant d'ailleurs chercheuse au LORIA et spécialisée dans l'intelligence artificielle.

La labellisation « Main à la pâte » a aussi été l'occasion pour le collège d'inaugurer son propre fablab. Depuis janvier, il dispose d'une imprimante 3D, d'une découpeuse laser et d'un robot d'usinage et sera accessible à toutes les écoles du secteur. « On y vient 2 heures par semaine depuis octobre », raconte Hafsah, 15 ans, en classe de troisième qui est en train de modéliser un plan en 3D sur le logiciel du constructeur automobile Renault.

Medhi, 15 ans, a travaillé sur une machine connectée pour présenter une voiture miniature. Photo ER/Élie GUCKERT

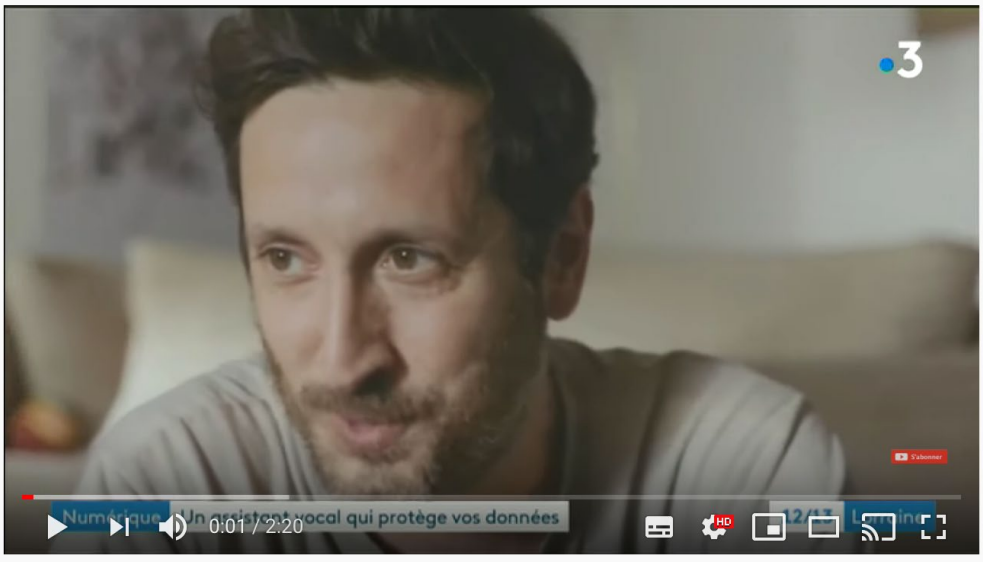
« L'informatique, ce n'était pas vraiment mon truc au début », avoue-t-elle. « Mais plus ça allait plus j'avais l'impression d'apprendre des choses et ça me donnait envie de continuer. »

« Je veux faire ça plus tard »

Medhi, 15 ans et lui aussi en classe de troisième était en revanche déjà féru d'ordinateurs auparavant. « Je bricolais déjà des trucs chez moi. Mais je ne pouvais pas faire tout, tout seul. Quand on a commencé les cours au fablab j'ai accroché direct ! » Le jeune garçon maîtrise désormais les rudiments de la programmation et a même participé à la réalisation d'une machine connectée permettant de faire tourner une voiture miniature. « Je veux faire ça plus tard ! », affirme-t-il.

Élie GUCKERT

07.06.2019 / France 3 Lorraine



Un assistant vocal qui protège les données

[Lien vers la vidéo sur YouTube.]

07.06.2019 / Le Monde Binaire

Claude Pair, pionnier de l'informatique

L'informatique avance vite, trop vite pour certains. C'est pourquoi le domaine mérite de temps en temps un regard dans le rétroviseur. C'est ce que nous allons faire avec Pierre Lescanne, Professeur à l'ENS de Lyon, un chercheur français en logique et informatique théorique. Pierre Lescanne nous parle d'un des grands pionniers de l'informatique, Claude Pair. Il nous ramène à cette époque où tout était à inventer, et en particulier l'enseignement de l'informatique. C'est d'ailleurs un peu un paradoxe de parler de coup d'oeil dans le rétroviseur au sujet de Claude Pair, un visionnaire qui a participé à faire sortir des limbes le monde numérique. ***Serge Abiteboul***

Claude Pair, site d'Interstice

Le 14 juin, ses amis et ses anciens élèves célébreront les 85 ans de Claude Pair, un pionnier de l'informatique [1]. En 1962, Claude Pair, ancien élève de l'École normale supérieure, est professeur de classe préparatoire au lycée de Nancy. Il a découvert la programmation pendant son service militaire comme scientifique du contingent. Mais c'est lorsqu'il rejoint Nancy que sa carrière de chercheur en informatique débute quand, ayant appris qu'un langage de programmation révolutionnaire venait d'être décrit par un groupe international, sous le nom d'Algol, il lance une équipe de doctorants dans la réalisation d'un compilateur pour ce langage, c'est-à-dire d'un traducteur, vers la machine à laquelle l'équipe a accès à l'époque, un IBM 1620, qui est mis à leur disposition, la nuit, par le constructeur et qui se trouve à Metz à 60 km, sans autoroute. A l'époque de telles machines ne se programment qu'en langage machine (même pas en assembleur) et les programmes sont saisis grâce à des cartes perforées. Algol est un langage dont les descendants contemporains sont Python, Pascal ou Java. Pour les chercheurs de l'époque, le traduire en code exécutable par la machine est un casse-tête, car aucune des méthodologies qui font partie du bagage d'un informaticien d'aujourd'hui n'existe. Il faut tout créer, tout inventer et les jeunes chercheurs sous la conduite d'un des leurs s'en sortent. Le compilateur commence à fonctionner, mais finalement IBM coupe l'accès à son ordinateur, or c'est le seul dans leur environnement. Cela n'empêche pas les thèses d'être soutenues.

L'émergence de nouveaux concepts

IBM 1620, Wiki Common

Cette recherche empirique a cependant ouvert des horizons à Claude Pair qui a l'intuition que la technologie naissante est plus qu'une ingénierie et que l'« informatique » dont le nom vient d'être inventé est une véritable science, dont les concepts de base sont à inventer. Parmi ceux-ci, il découvre la *pile*, concept omniprésent, entre autres dans l'*analyse syntaxique* (l'analyse des programmes qui permet d'en découvrir la structure et de pouvoir les traduire). Pour cette analyse syntaxique, il invente une structure mathématique : le binoïde. En effet, il comprend qu'il faut attaquer l'informatique avec la culture qui est la sienne, celle des mathématiques. A l'époque les calculateurs servent surtout aux physiciens et aux mécaniciens et sont pour eux des outils. Ils sont peu intéressés par la conceptualisation du calcul et de ce qui lui est lié. La notion de binoïde n'a pas survécu, en tout cas pas sous ce nom, mais il est l'une des premières structures mathématiques dont la définition est *récursive* (on peut *calculer* sur elle) et c'est cela qui est intéressant. Ses travaux attirent l'attention d'une chercheuse hongroise, Rósza Péter, pionnière des fonctions récursives (ou fonctions calculables) dont elle a dégagé les bases dans les années 30. Il entretient avec elle une correspondance épistolaire en 1968-1969. Dès 1966, il comprend aussi comment une démarche algébrique, associée à l'utilisation d'une « pile », permet de concevoir des algorithmes de cheminement dans un graphe : existence d'un chemin , calcul du plus long chemin, calcul du plus court chemin, calcul de tous les chemins, etc. Le même algorithme abstrait s'instancie dans des algorithmes qui résolvent des problèmes différents. Cette approche innovante sera « redécouverte » de multiples fois, après lui. Mais il est encore insatisfait sur deux points : savons-nous ce qu'est un programme et comment enseigner la programmation ?

Comment enseigner la programmation ?

Avant tout, que réalise un *programme* ? En fait, un programme décrit un *calcul* dont le but est de résoudre un *problème*. Ce qui conduit à deux nouvelles questions. Qu'est-ce qu'un problème (informatique) ? Qu'est-ce qu'un calcul ? Avec son équipe nancéienne, il est l'un des premiers à se poser ces questions. Il comprend que les réponses se trouvent du côté de l'algèbre et de la logique, à l'époque peu diffusée en France.

Quand vous demandez à un débutant d'écrire un programme résolvant un problème, il ne sait pas par quel bout prendre la question. Claude Pair, que ce dilemme préoccupe, met au point une méthodologie qu'il appelle la *méthode déductive de programmation* qui propose une approche, rigoureuse et raisonnée, pour aborder la programmation et son initiation. Cette méthode repose sur un principe : « il faut partir du résultat ». Il faut ensuite définir quand ils se posent des sous-problèmes à résoudre, le tout étant associé à une disposition rigoureuse et standardisée pour définir et présenter les identificateurs et les notions que l'on introduit, tandis que le programme s'élabore par étapes.

Un chef de projet et un meneur d'hommes

Dès la réalisation du premier compilateur pour Algol, Claude Pair s'est révélé un leader incomparable, mais il ne s'arrête pas là ! Il dirige de nombreux doctorants (32 thèses sous sa direction et à ce jour, plus de 120 « descendants » docteurs). Il crée à Nancy ce qui est devenu l'un des meilleurs laboratoires français et européen du domaine. Il préside une université. En 1981, qui marque la fin de sa carrière de chercheur, il est appelé comme Directeur des lycées au Ministère de l'Éducation nationale, puis il devient recteur. Dès 1971, sentant que les nouveaux enseignants maîtrisent difficilement les tout nouveaux concepts qui émergent, il crée une école d'été annuelle. En 1985, il participe à la création de SPECIF, dont il est le premier président, et qui se transformera en la *Société informatique de France*. Il est actuellement impliqué dans la lutte contre l'inégalité des chances dans l'éducation.

En fêtant Claude Pair, nous revivons ainsi la naissance de l'informatique en France dont il est un des très grands acteurs.

Pierre Lescanne, Professeur à l'ENS de Lyon

[1] Colloque en l'honneur de Claude Pair, Nancy, 14 juin 2019, http://claudepair.fr/

27.08.2019 / L'Usine Nouvelle

UN CHERCHEUR DU CNRS DÉCOUVRE UNE FAILLE DANS LE VOTE EN LIGNE RUSSE

Gaetan R 27 août 2019 Sécurité Ecrire un commentaire

Dans un communiqué de presse, le CNRS explique que l'un de ses chercheurs a découvert une faille de sécurité dans le système de vote en ligne du parlement à Moscou.

Le 8 septembre, les Moscovites éliront le nouveau parlement de la capitale russe. Ils auront accès au vote électronique. Conscientes des risques en termes de cybersécurité, les autorités locales ont lancé un concours. Elles publient chaque jour des données chiffrées correspondant à des votes factices et une clé publique. Ainsi, les hackers et les spécialistes peuvent tester la qualité du chiffrement.

Dans un communiqué de presse, l'université de Lorraine et le CNRS ont assuré qu'un cryptographe français, Pierrick Gaudry, chercheur du CNRS au sein du Laboratoire lorrain de recherche en informatique et ses applications, a découvert une faille de sécurité dans ce système de vote.

Selon le spécialiste du CNRS, l'objectif était de déchiffrer les données en moins de 12 heures, le temps que durera l'élection en septembre prochain. Pour protéger les bulletins électroniques, les autorités moscovites ont utilisé une variante du cryptosystème ElGamal associée à une blockchain inspirée de l'Ethereum.

Le chercheur du CNRS pirate le système de vote en ligne en 20 minutes

Pierrick Gaudry estime que les clés de chiffrement employées, d'une longueur de 256 bits, sont trop petites. Selon lui, il suffit de 20 minutes à l'aide d'un ordinateur classique et d'un logiciel libre pour venir à bout de la clé privée. Le chercheur affirme qu'un hacker pourrait le faire en 10 minutes seulement. De la sorte, un pirate informatique "aurait été en mesure de suivre les résultats de l'élection russe en direct", selon le communiqué de presse du CNRS. Le compte de vote en direct est illégal. Il faut attendre la fin de l'élection.

Avant de publier la conclusion de ses recherches le 8 août dernier, le cryptographe a prévenu les responsables du concours. Les autorités moscovites l'ont contacté pour lui indiquer qu'il recevra une récompense de 13 500 euros pour ses travaux. **Elles ont reconnu que les clés de chiffrement publiques étaient trop courtes et les ont mises à jour en 1024 bits.**

Un système qui a subit trop de changements pour être sécuriser à la date butoire

Cela ne suffirait pas selon Pierrick Gaudry. Le système développé par le Département des technologies de l'information de Moscou aurait besoin de clés d'une longueur d'au moins 2048 bits pour être protégé. De plus, le 22 août dernier, le chercheur affirme que le déchiffrement ne repose plus sur un contrat intelligent opéré dans la blockchain. **Le 24 août, Alexander Golovnev, cryptographe à l'université d'Harvard, a publié un article expliquant que le système reste vulnérable puisqu'il a trouvé une nouvelle faille dans ce dernier.**

Le spécialiste lorrain considère qu'il y a eu trop de changement dans le code à quelques semaines des élections. **Il conseille tout simplement de ne pas utiliser le vote électronique dans sa version actuelle.**

26.08.2019 / Le Quotidien Luxembourgeois

Un chercheur lorrain détecte une faille dans le système de vote électronique russe

Dans Grande Région Mis à jour le 26/08/19 17:33 | Publié le 26/08/19 17:32

Grâce à cette faille, le chercheur aurait "été en mesure de suivre les résultats de l'élection russe en direct". (illustration AFP)

Un chercheur lorrain a mis en évidence une faille dans le système de vote électronique qui doit être utilisé le 8 septembre pour les élections locales à Moscou, ont annoncé lundi l'université de Lorraine et le CNRS.

"Moins d'un mois avant que Moscou ne s'essaye au vote en ligne lors de l'élection du nouveau parlement de la ville, un cryptographe français vient de mettre en évidence une faille de sécurité du protocole testé dernièrement", selon un communiqué diffusé par l'université et le CNRS.

Pierrick Gaudry, cryptographe du Laboratoire lorrain de recherche en informatique et ses applications, a relevé le défi lancé par les autorités moscovites, qui publient chaque jour "des données cryptées correspondant à des votes factices et une clé publique" pour que les internautes éprouvent la qualité du chiffrement. "Pierrick Gaudry a montré qu'avec un ordinateur standard et des logiciels libres accessibles à tous, il arrivait à obtenir la clé privée en 20 minutes environ. Selon lui, un pirate informatique aurait pu obtenir cette clé privée en 10 minutes seulement", poursuit le communiqué.

Il recevra 13 500 euros

Grâce à cette faille reposant sur la petite taille de la clé publique qui rendait le calcul de la clé privée très simple, le chercheur aurait "été en mesure de suivre les résultats de l'élection russe en direct", affirme le communiqué. Depuis la publication de ces travaux le 14 août, pour lesquels la ville de Moscou doit verser 13 500 euros au chercheur, "les derniers tests ont proposé un nouveau protocole avec une clé publique plus longue", conclut le communiqué.

A Moscou, la campagne électorale a été marquée par plusieurs manifestations non autorisées pour exiger des élections libres, qui ont débouché sur des milliers d'arrestations ces dernières semaines. Le mouvement de contestation électorale a éclaté mi-juillet après le rejet, officiellement pour des vices de forme, de l'enregistrement de candidats à l'élection. Il s'agit du plus important mouvement de contestation depuis le retour de Vladimir Poutine au Kremlin en 2012.

LQ/AFP

Comment un Français a trouvé une faille dans le vote électronique prévu à Moscou

Publié le : 27/08/2019 - 18:55 Modifié le : 28/08/2019 - 18:41

Un bureau de vote à Moscou, pour la présidentielle en mars 2018. Sergei Karpukhin, Reuters

Texte par : Sébastian SEIBT Suivre

Le système de vote électronique prévu pour l'élection du Parlement de Moscou, le 7 septembre, est vulnérable à une attaque, a découvert un spécialiste français de cryptographie. Et il ne faut pas plus de 20 minutes pour y parvenir.

Les élections au Parlement de Moscou du 7 septembre ne sont pas seulement contestées dans la rue. Alors que des dizaines de milliers de Moscovites ont manifesté en juillet contre le caractère jugé peu démocratique de la sélection des candidats, la fiabilité de l'une des principales innovations de ce scrutin - le vote électronique - a été remise en cause. Et c'est un spécialiste français de cryptographie, Pierrick Gaudry du Laboratoire lorrain de recherche en informatique et ses applications (Loria), qui en a, le premier, démontré les limites.

C'est la première fois que la Russie propose de choisir entre le bureau de vote traditionnel et la possibilité de voter par Internet pour une élection à fort enjeu politique. L'initiative viserait à enrayer le faible taux de participation aux élections locales dans la capitale russe (21 % en 2014) en misant, notamment, sur l'attrait de l'e-vote pour les jeunes électeurs, explique au site dédié à l'actualité russe Riddle, Julia Krivonosova, spécialiste des questions de gouvernance numérique à l'Université de Tallinn (Estonie). Le vote électronique serait également une manière de prouver que les autorités locales prennent au sérieux la lutte contre la fraude électorale, tant elles ont insisté sur la sécurité du processus.

Blockchain et clés de chiffrement

Le système mis en place par Moscou repose sur la blockchain, c'est-à-dire la même technologie qui permet de garantir la fiabilité des transactions en cryptomonnaies tels que le bitcoin ou l'Ethereum. "Une propriété intéressante d'une blockchain est qu'une fois que l'information y a été stockée, il est essentiellement impossible de l'effacer. Dans le contexte du vote électronique, cela peut servir à garantir qu'aucun bulletin n'est retiré de l'urne avant le dépouillement", explique Pierrick Gaudry, contacté par France 24. Il n'a pas connaissance d'autre expérience de vote électronique qui s'appuie ainsi sur la blockchain.

Mais la vulnérabilité découverte et rendue publique le 14 août par le chercheur français se situe au moment où les Moscovites soumettent le vote électronique. Ils utilisent une clé de chiffrement qui agit comme un bulletin virtuel et garantit, en théorie, le secret du vote. Pour l'ouvrir, les organisateurs du scrutin doivent appliquer une clé de déchiffrement.

Pour tester la fiabilité du système, Alexeï Venediktov, rédacteur en chef de la radio d'opposition Echos de Moscou et directeur d'une organisation de surveillance des élections, a lancé un défi [et non les autorités russes, comme annoncé par erreur par le CNRS]. Chaque jour, "des données cryptées correspondant à des votes factices et une clé publique" étaient publiées pour que les internautes éprouvent la qualité du chiffrement. Pierrick Gaudry a sauté sur l'occasion. "J'ai téléchargé le code source du logiciel de vote publié par Moscou et je l'ai parcouru en me concentrant sur ce qui relève de la cryptographie, ma spécialité", raconte-t-il.

Il ne lui a pas fallu longtemps pour découvrir le hic : les clés de chiffrement fournies étaient trop petites. "On peut comparer ça à un antivol de vélo : moins il y a chiffres à découvrir, plus c'est facile à décoder", explique-t-il. En l'occurrence, les bulletins virtuels de vote des Moscovites allaient être protégés par des clés à chiffrement de 256 bits, ce qui est insuffisant pour des informations aussi sensibles. La preuve : Pierrick Gaudry a réussi à décrypter le code en 20 minutes grâce à un logiciel développé par son laboratoire. De quoi donner des sueurs froides aux autorités moscovites, qui avaient mis les experts au défi de trouver des vulnérabilités en moins de 12 heures, soit le temps du scrutin. "C'est vraiment étonnant, et je ne m'explique pas pourquoi ils ont fait une telle erreur", reconnaît le chercheur français.

Conséquence potentiellement dramatique

Les bulletins secrets soumis par vote électronique risquent donc de ne pas être si secrets que ça. Les conséquences, en théorie, peuvent être dramatiques pour l'intégrité d'un scrutin. Ainsi, lorsque l'électeur remet son bulletin dans l'urne virtuelle, il envoie, en pratique, son vote crypté à un serveur où des personnes humaines - des administrateurs - le réceptionnent. Ils agissent, en général, un peu à la manière d'un assesseur dans un bureau de vote pour s'assurer que c'est bien la bonne personne qui vote ou qu'elle n'a pas voté plusieurs fois. Ils sont les seuls à savoir de qui provient chaque bulletin car le lien entre le vote électronique et l'électeur est ensuite coupé. Si ces personnes utilisent la même méthode que Pierrick Gaudry pour décrypter la clé de chiffrement ou qu'un pirate informatique s'infiltre sur le serveur, "l'attaque devient dévastatrice, puisque le secret du vote n'est plus garanti et l'on sait pour qui chacun a voté", prévient le spécialiste français.

Mais ce n'est pas le seul danger. La possibilité de décoder rapidement et facilement ces clés de cryptage peut permettre à un attaquant "de connaître les résultats partiels tout au long du scrutin", assure Pierrick Gaudry. En cas de tendance de vote défavorable, des organisateurs peu scrupuleux pourraient, par exemple, être tentés de bourrer les urnes traditionnelles pour améliorer les chances de leur champion.

Ces risques sont théoriques et dans le cas du vote à Moscou le chercheur français n'a "actuellement pas les moyens de confirmer ou d'infirmer ces scénarios". Il lui faudrait la documentation détaillant comment est organisé, par exemple, la vérification de l'identité de chaque e-votant ou, encore, à quel moment le lien entre le bulletin électronique et l'électeur est coupé. "Je l'ai demandé à plusieurs reprises, mais je n'ai jamais eu de réponse de Moscou", regrette Pierrick Gaudry.

Les autorités l'ont, en revanche, remercié avec un chèque de 13 500 euros pour avoir découvert cette faille, et ont amélioré le niveau de complexité de la clé de chiffrement. Tout est bien qui finit bien ? Pas franchement. Un autre chercheur, de l'université de Harvard, a découvert une nouvelle vulnérabilité dans le système.

Le système russe "n'est pas mûr"

La conséquence pour Pierrick Gaudry est claire : Moscou ferait bien de renoncer au vote électronique pour ce scrutin "car leur système n'est pas mûr". Pour lui, les autorités ont trop tardé à le soumettre aux experts. "La conception d'un système de vote électronique est très compliqué. De ce point de vue, le test effectué, avec publication du code source, était une excellente chose. Mais cela arrive bien trop tard par rapport à la date du scrutin, et il aurait fallu en plus fournir une documentation complète afin de réaliser une vraie évaluation de sécurité", affirme-t-il.

Au-delà du cas moscovite, cette expérience démontre les limites du vote électronique à l'heure actuelle. "Malheureusement, il n'y a pas encore de système de vote par Internet qui apporte autant de garanties qu'un vote à l'urne traditionnel", assure Pierrick Gaudry. La nécessité de prendre en compte à la fois des considérations de transparence – s'assurer que le vote n'est pas fait sous la contrainte, qu'un électeur ne vote pas plusieurs fois, etc. – et de secret de l'isoloir virtuel n'est pas une mince affaire, surtout lorsque l'enjeu politique est fort.

Pour autant, ce spécialiste estime que le vote électronique sera de plus en plus utilisé dans des "contextes nonpolitiques, à enjeu modéré", comme les élections en entreprises ou au sein d'associations. "Un vote électronique peut permettre de réduire les coûts, d'allonger la durée du scrutin (et donc potentiellement d'augmenter la participation), et d'éviter la fastidieuse surveillance de l'urne", détaille Pierrick Gaudry. Il préfère aussi le vote électronique au vote par correspondance pour les expatriés ou les militaires en mission. "Je considère que s'il est bien fait, il apporte plus de garanties" que le vote par courrier. Mais pour ce qui est d'élire Vladimir Poutine, ou simplement les parlementaires moscovites, le vote électronique apporte plus de problèmes que de solutions.

RUSSIE ÉLECTIONS INTERNET CYBERSÉCURITÉ

Un Lorrain détecte la faille du vote électronique russe

Un chercheur lorrain a mis en évidence une faille dans le système de vote électronique qui doit être utilisé le 8 septembre, pour les élections locales à Moscou.

Le chercheur lorrain aurait «été en mesure de suivre les résultats de l'élection russe en direct», selon le communiqué. (photo: AFP/Alexander Nemenov)

«Moins d'un mois avant que Moscou ne s'essaye au vote en ligne lors de l'élection du nouveau Parlement de la ville, un cryptographe français vient de mettre en évidence une faille de sécurité du protocole testé dernièrement», selon un communiqué diffusé par l'université de Lorraine et le CNRS, lundi.

Pierrick Gaudry, cryptographe du Laboratoire lorrain de recherche en informatique et ses applications, a relevé le défi lancé par les autorités moscovites, qui publient chaque jour «des données cryptées correspondant à des votes factices et une clé publique» pour que les internautes éprouvent la qualité du chiffrement.

Moscou doit verser 13 500 euros au lorrain

«Pierrick Gaudry a montré qu'avec un ordinateur standard et des logiciels libres accessibles à tous, il arrivait à obtenir la clé privée en 20 minutes environ. Selon lui, un pirate informatique aurait pu obtenir cette clé privée en 10 minutes seulement», poursuit le communiqué.

Grâce à cette faille reposant sur la petite taille de la clé publique qui rendait le calcul de la clé privée très simple, le chercheur aurait «été en mesure de suivre les résultats de l'élection russe en direct», affirme le communiqué. Depuis la publication de ces travaux le 14 août, pour lesquels la ville de Moscou doit verser 13 500 euros à M. Gaudry, «les derniers tests ont proposé un nouveau protocole avec une clé publique plus longue», conclut le communiqué.

Les Moscovites exigent des élections libres

À Moscou, la campagne électorale a été marquée par plusieurs manifestations non autorisées pour exiger des élections libres, qui ont débouché sur des milliers d'arrestations ces dernières semaines. Le mouvement de contestation électorale a éclaté mi-juillet après le rejet, officiellement pour des vices de forme, de l'enregistrement de candidats à l'élection.

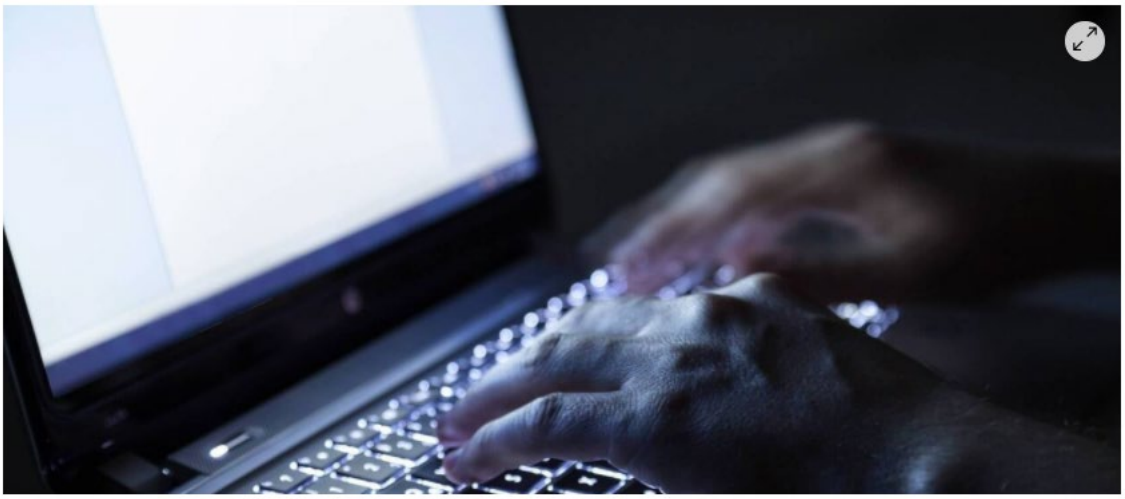
Il s'agit du plus important mouvement de contestation depuis le retour de Vladimir Poutine, au Kremlin, en 2012.

(L'essentiel/afp)

26.08.2019 / Ouest France

Un chercheur lorrain détecte une faille dans le système de vote électronique russe

Le cryptographe a relevé le défi lancé par les autorités moscovites, qui publient des données factices chaque jour pour en éprouver la sécurité en vue des élections de septembre prochain. Il a réussi à détecter et exploiter la faille en vingt minutes.



Le chercheur a réussi à détecter et exploiter la faille en quelques minutes. (Photo d'illustration) | FOTOLIA

Un chercheur lorrain a mis en évidence une faille dans le système de vote électronique qui doit être utilisé le 8 septembre pour les élections locales à Moscou, ont annoncé l'université de Lorraine et le CNRS lundi 26 août.
« Moins d'un mois avant que Moscou ne s'essaye au vote en ligne lors de l'élection du nouveau parlement de la ville, un cryptographe français vient de mettre en évidence une faille de sécurité du protocole testé dernièrement », selon un communiqué diffusé par l'université et le CNRS.

13 500 € de récompense

Pierrick Gaudry, cryptographe du Laboratoire lorrain de recherche en informatique et ses applications, a relevé le défi lancé par les autorités moscovites, qui publient chaque jour **« des données cryptées correspondant à des votes factices et une clé publique »** pour que les internautes éprouvent la qualité du chiffrement.

« Pierrick Gaudry a montré qu'avec un ordinateur standard et des logiciels libres accessibles à tous, il arrivait à obtenir la clé privée en 20 minutes environ. Selon lui, un pirate informatique aurait pu obtenir cette clé privée en 10 minutes seulement », poursuit le communiqué.

Grâce à cette faille reposant sur la petite taille de la clé publique qui rendait le calcul de la clé privée très simple, le chercheur aurait **« été en mesure de suivre les résultats de l'élection russe en direct »**, affirme le communiqué.

Depuis la publication de ces travaux le 14 août, pour lesquels la ville de Moscou doit verser 13 500 € à Pierrick Gaudry, **« les derniers tests ont proposé un nouveau protocole avec une clé publique plus longue »**, conclut le communiqué.

Des manifestations pour des élections libres

À Moscou, la campagne électorale a été marquée par plusieurs manifestations non autorisées pour exiger des élections libres, qui ont débouché sur des milliers d'arrestations ces dernières semaines.

Le mouvement de contestation électorale a éclaté mi-juillet après le rejet, officiellement pour des vices de forme, de l'enregistrement de candidats à l'élection.

Il s'agit du plus important mouvement de contestation depuis le retour de Vladimir Poutine au Kremlin en 2012.

#High Tech #Sciences #Russie #Grand Est #Actualité en continu #Régions #Nancy

27.08.2019 / L'Est Républicain

Une faille du vote électronique russe détectée par un Nancéien

Pierrick Gaudry, chercheur du CNRS au sein du Laboratoire lorrain de recherche en informatique et ses applications a mis en évidence la vulnérabilité du système de sécurité du vote électronique qui devait être utilisé le 8 septembre pour les élections du Parlement de Moscou, en Russie.

Par Jean-Christophe VINCENT - 27 août 2019 à 05:02 | mis à jour à 07:32 - Temps de lecture : 3 min

1 | | Vu 5438 fois

Pierrick Gaudry, cryptographe au CNRS, a relevé le défi proposé par les autorités moscovites. Photo ER /Jean-Christophe VINCENT

Le défi lancé par les autorités moscovites était d'éprouver la qualité du chiffrement des données censées protéger le système de vote en ligne devant être utilisé ce 8 septembre, pour les élections du Parlement de Moscou. Et ceci en moins de 12 heures. Le Nancéien Pierrick Gaudry, chercheur du CNRS au sein du Laboratoire lorrain de recherche en informatique et ses applications (CNRS/Inria/Université de Lorraine), a relevé le défi avec succès, début août.

> « Un pirate informatique aurait pu obtenir le code de déchiffrement en 10 minutes »

« Les autorités moscovites publient chaque jour des données cryptées correspondant à des votes factices et une clé publique pour que les internautes éprouvent la qualité du chiffrement », explique Pierrick Gaudry. « Comme le vote électronique fait partie de mes recherches, j'ai décidé de relever le challenge. Avec un ordinateur standard et un logiciel libre qui implante un algorithme appelé crible algébrique, que nous développons depuis dix ans, j'ai trouvé la clé privée, c'est-à-dire le code de déchiffrement nécessaire pour décrypter les votes, en 20 minutes environ. Et, selon moi, un pirate informatique aurait pu obtenir cette clé privée en 10 minutes seulement ! Cela veut dire qu'il aurait été en mesure de suivre les résultats de l'élection russe en direct, avec la possibilité de révéler le scrutin partiel tout au long du vote. » Le cryptographe nancéien a prévenu les autorités moscovites qu'il avait réussi le test, avant de rendre la chose publique sur son site web le 8 août, puis de publier le 14 août un article sur la plateforme de la communauté scientifique arXiv. « Cette faille reposait sur la petite taille de la clé publique, c'est-à-dire le code de chiffrement, qui rendait le calcul de la clé privée très simple », détaille ce spécialiste.

Récompense de 13.500 €

Depuis la publication de son article sur la plateforme arXiv, les concepteurs moscovites ont revu le système, en proposant un nouveau protocole avec une clé publique plus longue. Quant à la mairie de Moscou, elle a contacté le chercheur nancéien pour l'informer qu'il recevrait prochainement une récompense de 13.500 euros pour ses travaux. « Les autorités moscovites étaient très contentes que je puisse les aider à améliorer leur système de vote électronique. Le résultat du test donne de la visibilité à nos recherches. Mais, à mon avis, faire autant de changements dans un système de vote électronique avec des échéances électorales aussi proches, c'est risqué. Je pense que les autorités moscovites devraient annuler tout simplement le vote électronique pour cette élection du 8 septembre. D'ailleurs, vendredi dernier, un chercheur de Harvard (États-Unis) a trouvé une nouvelle faille dans le code de chiffrement de la nouvelle version. »

À Moscou, la campagne électorale a déjà été marquée par plusieurs manifestations non autorisées et des milliers d'arrestations, après le rejet, officiellement pour des vices de forme, de l'enregistrement de certains candidats à l'élection.

Edition Nancy et agglomération | Région Lorraine +

26.08.2019 / Mobile Payements Today

French researcher cracks Moscow's blockchain voting system

Aug. 23, 2019

Pierrick Gaudry, a French researcher at Lorraine University, has uncovered a vulnerability in a blockchain-based voting system that Russian officials plan to use for the 2019 Moscow City Duma election on Sept. 14. Gaudry was able to compute the voting system's private keys based on its public keys, according to a **report** by ZDNet.

The Moscow Department of Information Technology built the voting system on the Ethereum blockchain. Residents would be able to vote via phone or computer and their votes would be cryptographically recorded on the Ethereum blockchain.

Gaudry claimed the weakness in the system was the ElGamal encryption scheme that used encryption keys that were too small to be secure.

"It can be broken in about 20 minutes using a standard personal computer, and using only free software that is publicly available," Gaudry said in a report.

Moscow Department of IT officials claim they will fix the issue by providing a stronger key.

"We absolutely agree that 256x3 private key length is not secure enough," a spokesperson said in an online response. "This implementation was used only in a trial period. In few days the key's length will be changed to 1024."

26.08.2019 / 20 Minutes

Russie : Un chercheur lorrain détecte une faille dans le système de vote électronique

ELECTIONS Un cryptographe français a relevé le défi lancé par la Russie de tester la qualité du chiffrement du système de vote électronique mis en place pour les élections locales

Vladimir Poutine, le 17 décembre 2017 au Kremlin. — *Alexey DRUZHININ / SPUTNIK / AFP*

Une faille dans le système de vote électronique russe, qui doit être utilisé le 8 septembre pour les élections locales à Moscou, a été mise en évidence par un chercheur lorrain, ont annoncé l'université de Lorraine et le CNRS, ce lundi.

« Moins d'un mois avant que Moscou ne s'essaye au vote en ligne lors de l'élection du nouveau parlement de la ville, un cryptographe français vient de mettre en évidence une faille de sécurité du protocole testé dernièrement », ont expliqué les deux institutions.

« Un pirate informatique aurait pu obtenir cette clé privée en 10 minutes seulement »

Pierrick Gaudry, cryptographe du Laboratoire lorrain de recherche en informatique et ses applications, a relevé le défi lancé par les autorités moscovites, qui publient chaque jour « des données cryptées correspondant à des votes factices et une clé publique » pour que les internautes éprouvent la qualité du chiffrement.

« Pierrick Gaudry a montré qu'avec un ordinateur standard et des logiciels libres accessibles à tous, il arrivait à obtenir la clé privée en 20 minutes environ. Selon lui, un pirate informatique aurait pu obtenir cette clé privée en 10 minutes seulement », poursuit le communiqué. Grâce à cette faille reposant sur la petite taille de la clé publique qui rendait le calcul de la clé privée très simple, le chercheur aurait « été en mesure de suivre les résultats de l'élection russe en direct », affirme le communiqué.

La ville de Moscou doit verser 13.500 euros à Pierrick Gaudry

Depuis la publication de ces travaux le 14 août, pour lesquels la ville de Moscou doit verser 13.500 euros à Pierrick Gaudry, « les derniers tests ont proposé un nouveau protocole avec une clé publique plus longue », conclut le communiqué.

A Moscou, la campagne électorale a été marquée par plusieurs manifestations non autorisées pour exiger des élections libres, qui ont débouché sur des milliers d'arrestations ces dernières semaines. Le mouvement de contestation électorale a éclaté mi-juillet après le rejet, officiellement pour des vices de forme, de l'enregistrement de candidats à l'élection. Il s'agit du plus important mouvement de contestation depuis le retour de Vladimir Poutine au Kremlin en 2012.

26.08.2019 / Bitfinance.news

Blockchain security system of upcoming Moscow elections is violated

A French security researcher broke the encryption scheme of the voting system, based on blockchain technology, which will be used in the upcoming Moscow 2019 elections

Last updated Aug 21, 2019

Share

Pierrick Gaudry, a professor at the University of Lorraine and a member of the French Research Institute INRIA, achieved a vulnerability in the voting system based on ethereum crypto technology that will be implemented in the next elections in Moscow.

According to the investigation presented, only 20 minutes were enough for Gaudry to calculate the private keys of the voting system based on the public keys. These keys are used to encrypt the votes of the users during the elections, in order to avoid their identity being known.

It is worth emphasizing that Gaudry points out that due to the implementation of the encryption scheme "ELGAMAL" with short encryption keys, the system becomes insecure, which allows to unlock the keys in just 20 minutes.

The researcher explains: "It can be broken in about 20 minutes using a standard personal computer and using only free software that is publicly available. Once these private keys are known, any encrypted information can be decrypted as quickly as it is created."

At the moment, the extent of the privacy violation is unknown. In the worst case, the votes of all voters using this system will be revealed to anyone as soon as they are issued.

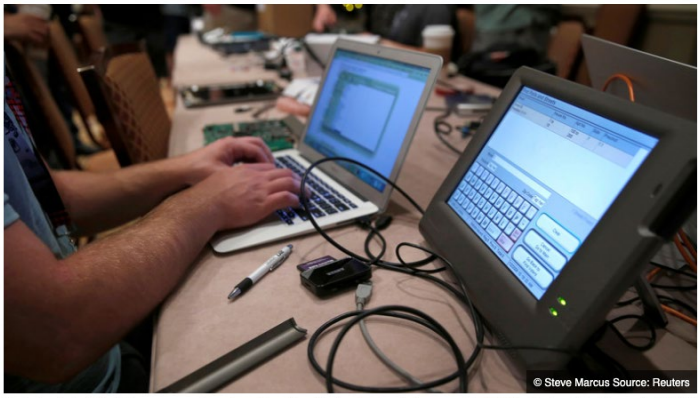
L. Sáenz

Source: Tekcrispy

17.08.2019 / RT France

Russie : les failles du système de vote en ligne révélées avec l'aide d'un expert français

17 août 2019, 13:23



Un hacker tentant de pirater un appareil contenant des listes électorales, lors de la convention Def Con Hacker à Las Vegas, le 29 juillet 2017, dans le Nevada (image d'illustration).

Pierrick Gaudry, expert français en chiffrement informatique, pourrait bénéficier d'une importante récompense pour avoir révélé des faiblesses dans le système de vote par Internet qui sera utilisé à Moscou lors des prochaines élections.

D'après des informations de l'agence de presse publique TASS datées du 16 août, un expert français en chiffrement informatique, Pierrick Gaudry, spécialisé dans l'analyse algorithmique appliquée à la cryptologie, devrait recevoir une récompense pécuniaire pour avoir mis en lumière des points faibles dans le système de vote en ligne prévu pour les élections locales de la ville de Moscou, qui se tiendront le 8 septembre prochain.

«Je pense que M. Gaudry peut être éligible pour bénéficier de la plus grande partie de la récompense, bien qu'il n'y ait pas eu de piratage informatique en réalité. Cependant, il a été d'une grande aide, soulignant un maillon faible dans la longueur de la clé. Lundi [19 août], au quartier général, nous en discuterons avec le personnel informatique. Pour ma part, je serais favorable à ce que Pierrick Gaudry remporte la plus grande part de la récompense», a indiqué Alexeï Venediktov, chef de l'organisme chargé de surveiller et de contrôler les élections, toujours auprès de TASS.

Lire aussi

Pour avoir piraté Facebook, un hacker russe a reçu 40 000 dollars

En effet, afin d'améliorer son système de cryptage, la ville avait lancé un appel à des experts en cybersécurité et offrait deux millions de roubles (27 061 euros) aux personnes ayant réussi à déjouer le système de vote par Internet. «Nous sommes fiers qu'un expert en cryptage tel que Pierrick Gaudry se soit intéressé à l'expérience et nous ait montré comment améliorer le cryptage», a indiqué Alexeï Venediktov à l'agence de presse.

Le service de presse du département des technologies de l'information, rattaché au ministère de l'Intérieur, a pour sa part noté que les clés de chiffrement des données pour le vote en ligne n'étaient pas assez puissantes et qu'il était prévu de les améliorer avant le jour du scrutin. Au cours de celui-ci, une expérience de vote sur Internet sera menée dans trois districts. Le processus sera surveillé depuis un centre de contrôle situé au sein de l'administration.

17.08.2019 / Israël Defense

Moscow Blockchain Voting System Hacked in 20 Minutes

A recent report by a French security researcher revealed that a blockchain-based voting system to be used in Moscow's upcoming municipal elections is "completely insecure"

Ami Rojkes Dombe | 21/08/2019

Send to printer | Send to a friend | Size | Share on | Share on

By Mos.ru, CC BY 4.0, https://commons.wikimedia.org/w/index.php?curid=52646657

A French security researcher has found a critical vulnerability in the blockchain-based voting system that will be used next month for the 2019 Moscow City Duma (parliament) election.

Pierrick Gaudry, a researcher for INRIA, the French research institute for digital sciences, and CNRS, The French National Center for Scientific Research, found that he could compute the voting system's private keys based on its public keys. This private keys are used together with the public keys to encrypt user votes cast in the election.

Gaudry blamed the issue on Russian officials using a variant of the ElGamal encryption scheme that used encryption key sizes that were too small to be secure. This meant that modern computers could break the encryption scheme within minutes.

"It can be broken in about 20 minutes using a standard personal computer, and using only free software that is publicly available," Gaudry said in a report published earlier this month.

Moscow's blockchain voting system is a first of its kind. It was developed in-house by the Moscow Department of Information Technology, and works as a "smart contract" on top of the Ethereum blockchain platform.

Un francais dévoile une faille sécurité dans un système de vote en ligne Russe

Sécurité : *Un chercheur français dans le domaine de la sécurité a découvert une vulnérabilité critique dans un système de vote basé sur la blockchain mis au point en Russie. Les responsables russes prévoient d'utiliser cet outil de vote le mois prochain pour les élections à la Douma municipale de Moscou en 2019.*

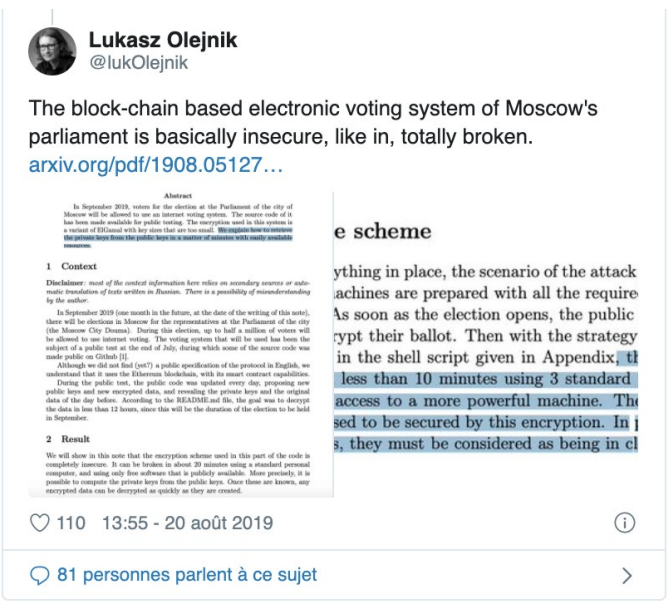
Pierrick Gaudry, universitaire lorrain et chercheur à l'INRIA, a découvert qu'il pouvait calculer les clés privées d'un système de vote basé sur la blockchain à partir des clés publiques. Ces clés privées sont utilisées conjointement avec les clés publiques pour chiffrer les votes des utilisateurs lors de l'élection.

Gaudry reproche aux responsables russes d'avoir utilisé une variante du système de chiffrement ElGamal qui utilisait des clés de chiffrement de taille trop petite pour être sécurisées. Cela signifiait que les ordinateurs modernes pouvaient briser le chiffrement en quelques minutes.

"Il peut être cassé en environ 20 minutes à l'aide d'un ordinateur personnel standard, et en utilisant uniquement des logiciels libres accessibles au public ", a déclaré M. Gaudry dans un rapport publié plus tôt ce mois-ci. Ce qu'un attaquant peut faire avec ces clés de chiffrement n'est pas très clair : les protocoles du système de vote sont uniquement disponibles en Russe, Gaudry n'a donc pas pu enquêter davantage.

"Sans avoir lu le protocole, il est difficile de prévoir précisément les conséquences. Nous pensons que ce système de chiffrement insuffisant est utilisé pour chiffrer les bulletins de vote mais il est difficile d'estimer à quel point il serait facile pour un attaquant d'avoir la correspondance entre les bulletins et les électeurs," a déclaré le chercheur français.

"Dans le pire des scenarios, les votes de tous les électeurs utilisant ce système pourraient être révélés à un tiers après avoir été transmis."



Une première dans le domaine

Le système de vote par blockchain de Moscou est une première dans son genre. Il a été développé en interne par le Département des technologies de l'information de Moscou et fonctionne comme un "smart contract" sur la plateforme de la blockchain Ethereum.

Le système de vote sera mis en service le 8 septembre et fonctionnera pendant 12 heures, en même temps que la séance de vote officielle. Une fois déployé le jour du scrutin, il permettra aux habitants de Moscou de voter par Internet, par téléphone ou sur leur ordinateur personnel, et de faire enregistrer de manière cryptographique sur la blockchain Ethereum.

Ce système de vote par Internet ne se limite pas uniquement aux personnes qui voyagent à l'étranger ou aux personnes handicapées. Tous ceux qui s'inscrivent à l'avance peuvent l'utiliser, ce qui signifie qu'il a le potentiel d'attirer des gens qui se seraient normalement abstenus.

Lorsqu'il sera déployé le mois prochain, le système de vote par Internet de Moscou deviendra le premier système basé sur une blockchain utilisé lors d'élections juridiquement contraignantes, et pas seulement lors de tests limités.

Une promesse de correctif

L'universitaire français a pu tester le système de vote car les responsables ont publié son code source sur GitHub en juillet, et ont demandé aux chercheurs en sécurité de trouver les failles.

Après la découverte de Gaudry, le Département des technologies de l'information de Moscou a promis de régler le problème signalé, en l'occurrence l'utilisation d'une clé privée faible.

"Nous sommes tout à fait d'accord pour dire que la longueur de clé privée de 256x3 n'est pas suffisante", a déclaré un porte-parole dans une réponse en ligne. "Cette implémentation n'a été utilisée que pendant une période d'essai. Dans quelques jours, la longueur de la clé passera à 1024."

Gaudry, qui a découvert que les autorités de Moscou avaient modifié le système de chiffrement ElGamal pour utiliser trois clés privées plus faibles au lieu d'une, n'a pas pu expliquer pourquoi le département informatique avait choisi cette approche. "C'est un mystère ", a déclaré le chercheur français.

Cependant, une clé publique d'une longueur de 1024 bits pourrait ne pas suffire, selon Gaudry, qui estime que les fonctionnaires devraient plutôt utiliser un des 2048 bits au moins. Ce choix de conception a également déconcerté Chris Roberts, stratège en chef de la sécurité chez Attivo Networks.

"Pourquoi les développeurs de la plate-forme choisiraient-ils une longueur faible en premier lieu est évidemment une question. Est-ce un manque de connaissance et de compréhension ? Ou simplement chercher à maximiser la vitesse et l'efficacité ou autre chose ", a dit M. Roberts.

1 million de roubles comme récompense

En outre, les responsables de Moscou ont également approuvé une récompense monétaire pour Gaudry. Selon le site de nouvelles russes Meduza, la récompense monterait à un million de roubles russes, ce qui represente un peu plus de 15.000 $.

"Le système américain pourrait apprendre beaucoup avec la Russie sur ce sujet ", a dit M. Roberts, faisant référence à la pléthore de difficultés que les États-Unis ont rencontré en essayant de sécuriser leurs machines de vote électronique. Ces difficultés viennent principalement des vendeurs de machines de vote, qui refusent de s'engager avec la communauté de la cybersécurité, ce que le gouvernement de Moscou n'a pas eu de problème à faire.

Cette nature fermée des machines de vote électronique et des systèmes électoraux utilisés aux États-Unis est la raison pour laquelle Microsoft a récemment annoncé son intention d'ouvrir le code source d'une nouvelle technologie pour sécuriser les machines de vote électronique sur GitHub.

Source : Moscow's blockchain voting system cracked a month before election

A lire aussi :
Le gouvernement suisse dépose une plainte pénale dans l'affaire Crypto AG
Les services de renseignements américains et allemands auraient délibérément mis en place des portes dérobées dans les...

Sujet: *Chiffrement* *Cybersécurité* *Piratage* *Blockchain*

Suivre via:

21.08.2019 / Meduza

STORIES

Prominent journalist Alexey Venediktov has accused 'Meduza' of cheating to prove Moscow's online voting system is hackable. He's wrong.

17:28, 21 августа 2019 · Источник: Meduza

Sergey Savostyanov / TASS / Sipa USA / Vida Press

This September's elections for the Moscow City Duma have already gained renown for inspiring regular mass protests, but they are also remarkable for another reason: In three of the Russian capital's districts, voters will be able to use an online system to select their new representatives. Moscow's Information Technology Department held intrusion tests on GitHub in late July to verify the integrity of the system: Officials gave programmers several opportunities to attempt to decrypt mock voting data, and each round of data was subsequently published so that it could be compared to the results of those hacking attempts. On August 16, *Meduza* reported on French cryptographer Pierrick Gaudry's successful attempt to break through the system's encryption. To confirm that the encryption keys used in the system are too weak, we also implemented Gaudry's program ourselves. City Hall officials responded to the successful hackings by refusing to post its private keys and data, thereby preventing outsiders from confirming that the system had indeed been hacked. Instead, *Ekho Moskvy* Editor-in-Chief Alexey Venediktov, who is also leading the citizens' board responsible for the elections, accused *Meduza* of abusing the testing process. Here's why he's wrong.

The claim

On August 21, during the latest round of testing for Moscow's online voting system, Alexey Venediktov said the following:

"It's all very simple. This is what Gaudry explained to me. How did *Meduza* abuse the system when they said they hacked it? They took the private key that our technical group put out, and then they cracked the code! We won't publish that key — I've forbidden it — until all the votes are counted. So they can't say they hacked us. If you want to hack us, hack us! Who's stopping you? They say they hacked us. But they took the private key our technical group put out. It's just dishonest. And Mr. Gaudry explained all this to me. Because that's exactly what he did himself."

GET THE BACKSTORY

After hackers break Moscow's prototype Internet voting, city officials stop sharing contest results on GitHub

What Gaudry did and *Meduza* replicated

Contrary to Venediktov's arguments, neither Gaudry nor *Meduza* "cracked the code" using a "private key" that was already "put out." First and foremost, that's because Venediktov's version of events makes no sense in the context of cryptography: If you already have a private key, you can decrypt data that has been encrypted using that key's public pair right away. In other words, if we really did have a "private key" from the start, we wouldn't have had to "crack" anything.

In fact, what both Gaudry and *Meduza* did was simply complete the testing challenge Moscow City Hall issued to check the strength of its encryption system. Here's how that challenge was set up:

1. City Hall creates a mock dataset.
2. The dataset is encrypted using a public key.
3. The public key and encrypted data are both posted online.
4. City Hall gives the public time to try to hack the system and decrypt the data.
5. City Hall posts the "answers" to the challenge — that is, the private key and the initial data.

Because the keys Moscow officials used were too weak (and too short), both Gaudry and *Meduza* were able to decrypt the test dataset in only 20 minutes. In actual election conditions, that would theoretically allow hackers to track voting results almost in real time well before polls officially close.

Does *Meduza* have a secret key to Moscow's elections now?

No. The challenge Moscow officials posted on GitHub was a test that used its own mock data and its own test keys. The results *Meduza* and Gaudry obtained have no bearing on the actual elections or even the new round of testing that began on August 21. Hacking those datasets was never the goal. Instead, the goal of this exercise was to demonstrate that the Moscow government's voting encryption system itself was weak and should be strengthened.

So what did Venediktov stop the city from posting until all votes are counted?

We don't know for sure, but it seems that he was talking about the "solution" to the testing challenge. Every time City Hall posts a new challenge, it simultaneously publishes the "solution" (that is, the private key and the initial data) for the previous challenge. Posting the private key and the dataset for the testing round Gaudry and *Meduza* solved would enable other journalists and the general public to verify that the city's encryption really was successfully hacked.

When City Hall posted the materials for a new round of testing on August 18, however, it did not publish the "solution" to the round that was posted on August 7 (i.e., the round *Meduza* solved). In other words, City Hall refused to publish data that had nothing to do with Moscow's actual elections but would have enabled the public to confirm that the city's online voting system is eminently hackable.

Artyom Kostyrko, the second-in-command at Moscow's Information Technology Department, explained on August 21 that "there was a problem in there on [August] 7th" but promised that the private key from the challenge would be published as usual. Immediately after Kostyrko made that announcement, Venediktov, who was sitting directly to his left, declared that the key would not, in fact, be published.

Footage from the discussion clearly shows Kostyrko deliberating about whether or not to interrupt Venediktov's subsequent arguments:

Did Moscow change its online voting system after the system was hacked?

Yes. The latest round of testing for the system features a longer and more secure encryption key. This modified encryption system will not be possible to hack in the span of 20 minutes. In other words, Moscow City Hall practically acknowledged that there was a vulnerability in its voting system and implemented changes to eliminate that vulnerability.

Update: After this fact check was published in Russian, Alexey Venediktov said on *Ekho Moskvy*, the radio station he leads and co-owns, that "nothing was hacked" but that Pierrick Gaudry "prevented [the online voting system] from being hacked" and may therefore receive up to $15,000 from the funds set aside as rewards for hackers in the testing process. Venediktov also argued that "some of my colleagues have sworn that our system is hackable in 20 minutes" but that its encryption has in fact never been successfully broken. He was apparently referring to the August 16 report by *Meduza* in which the system was indeed hacked. However, the encryption system for Moscow's online voting has been strengthened since that report was published, and tests for the newly strengthened system are currently ongoing.

Report by **Mikhail Zelenskiy**

Translation by **Hilah Kohen**

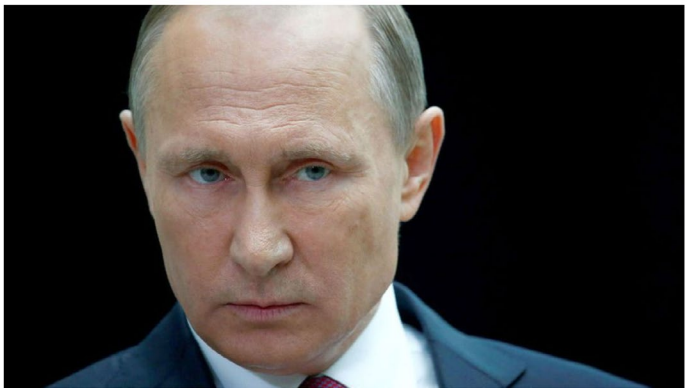
22.08.2019 / BFM TV

[Lien vers l'interview d'Arnaud Laprevote]

02.09.2019 / Le Parisien

Un Lorrain réussit à déjouer la sécurité russe

En un temps record, Pierrick Gaudry, basé à Vandœuvre-lès-Nancy (Meurthe-et-Moselle), a trouvé une faille dans le système de vote électronique russe.



Par **Doris Henry**

Le 2 septembre 2019 à 10h43

Il avait 12 heures pour relever le défi, il l'a fait en seulement 20 minutes ! Pierrick Gaudry, chercheur au Loria, le laboratoire lorrain de recherche en informatique et ses applications de Vandœuvre-lès-Nancy (Meurthe-et-Moselle) – affilié au CNRS – a réussi à déjouer le système de sécurité du vote électronique russe.

Il s'est prêté au jeu lancé par l'organisation de surveillance des élections du Parlement de Moscou prévues dimanche prochain. Il s'agissait de tester la fiabilité du système, qui s'est donc révélée très friable. Le quadragénaire est parvenu à le décoder en un temps record. « J'aurais même pu réussir en moins de 10 minutes, voire seulement en deux ou trois minutes avec un ordinateur plus puissant que le mien », explique-t-il.

Il va recevoir une récompense de 13 500 euros

Sur le principe d'un problème de mathématiques, les Moscovites ont posé l'énoncé, à savoir un bulletin chiffré qu'il fallait décoder. Pour Pierrick Gaudry, la solution était toute trouvée « comme pour un antivol de vélo, les clés de chiffrements étaient trop petites, moins il y a de chiffres, plus c'est facile. »

En clair, si le système de vote électronique était resté tel quel, un pirate informatique aurait pu suivre en temps réel les résultats. Les Russes n'ont pas tardé à féliciter l'expert en lui offrant une récompense de 13 500 euros.

02.09.2019 / Actu 17

Un Français déjoue la sécurité du système de vote électronique russe en 20 minutes

Y.C. -
2 septembre 2019, 15h26 | MAJ : 2 septembre 2019, 15h31

Vladimir Poutine. (Alexey Nikolsky / Sputnik/KREM/EFE/Newscom/MaxPPP)

Un chercheur le laboratoire lorrain de recherche en informatique et ses applications (LORIA) a fait très fort.

Il disposait de 12 heures pour tenter de parvenir à déjouer la sécurité du système de vote informatique russe. Il a réussi… en vingt minutes.

Pierrick Gaudry est un chercheur au LORIA de Vandœuvre-lès-Nancy en Meurthe-et-Moselle, un laboratoire affilié au CNRS. Il a participé à un « *bug bounty* » mis en place par l'organisation de surveillance des élections du Parlement de Moscou prévues dimanche prochain.

Une récompense de 13 500 €

Un *bug bounty* est un programme proposé par le responsable d'une application informatique qui promet aux internautes une récompense en cas de découverte de bugs ou de vulnérabilités. Ce genre de programme participatif permet à l'éditeur d'un logiciel d'en améliorer la sécurité.

Le chercheur français, âgé d'une quarantaine d'années, n'a pas mis longtemps à déchiffrer le système. Il a affirmé que seules deux ou trois minutes auraient été nécessaires s'il avait eu un ordinateur plus puissant, relate *Le Parisien*.

Un bulletin électronique à déchiffrer

Moscou demandait aux participants d'essayer de déchiffrer un bulletin de vote électronique. C'est ce qu'est parvenu à faire Pierrick Gaudry, qui a expliqué que les « *clés de chiffrement étaient trop petites* ».

Ainsi, si le système de vote électronique était mis en oeuvre tel quel le 8 septembre prochain, un pirate informatique pourrait suivre en temps réel les résultats.

25.09.2019 / France 3 Lorraine

Urbanloop plateau France 3 24092019

Lien vers la vidéo sur YouTube.

Le jeu de 7 familles de l'informatique

Maxime Amblard nous présente un projet porté par interstices.info, avec le soutien d'Inria, de la fondation Blaise Pascal, de la SIF et de l'Université de Lorraine : un jeu de 7 familles pour entrer dans les sciences de l'informatique.
Tamara Rezk

Construire une histoire de l'informatique n'est pas chose aisée. Si certaines figures comme Alan Turing se sont médiatiquement imposées ces dernières années, d'autres personnalités marquantes ont plus de difficulté à se faire connaître du grand public. On pense par exemple à Claude Shannon qui avait pourtant une pensée suffisamment originale pour accrocher tout un chacun. Quoi de plus amusant que de se lancer dans l'explication de la machine dont la seule fonction est d'appuyer sur le bouton qui l'éteint.

Une discipline scientifique, même jeune, a besoin de poser des jalons que sont ces grandes figures afin de se définir. Il suffit de demander aux spécialistes d'expliquer ce qu'est l'informatique pour constater que chacun parle depuis un point de vue très singulier. Et cela se complexifie si on intègre la question des relations entre informatique, numérique, mathématiques, ingénierie…

Et pourtant l'informatique c'est bien tout cela.

Nous avons rassemblé 42 grandes figures de la science sous la forme d'un jeu de sept familles. Le jeu est évidemment un prétexte pour appréhender de manière ludique l'histoire de l'informatique. Le principe a été de susciter des discussions dans un groupe d'une dizaine de personnes afin de trouver un équilibre pour former une photographie générale d'une vision de l'informatique. Bien évidemment, les 42 cartes ne permettent pas d'intégrer toutes les thématiques majeures, ni de faire la place à tous les grands noms. Nous nous sommes donc imposés des contraintes d'équilibre, entre les grands anciens et les modernes, la représentation des femmes (sans qu'elle ne soit artificielle), la diversité des thématiques (en les limitant à 7), ancrer une école française dans un panorama international (ne se limitant pas aux États-Unis). Bref, après de nombreuses heures de discussions, nous avons constitué cette proposition.

Chaque famille reprend une thématique particulière, des algorithmes et la programmation à l'intelligence artificielle, en passant par les composants et les machines. Ce jeu a été pensé comme une porte pour entrer dans la complexité de l'informatique qui s'inscrit comme une science. De nombreux éléments sont disséminés pour servir de passerelle tant pour la découverte du binaire, que la spécificité de chaque personnalité au travers d'un objet qui l'accompagne. Vous penserez qu'il n'est pas donné à tout le monde de connaître tous ces scientifiques, ce qui est vrai. Nous avons accompagné le jeu d'une notice reprenant de manière accessible (nous l'espérons) et condensée les faits marquants de chacune des personnalités afin de comprendre pourquoi elle a été introduite dans le jeu.

Le projet a été porté par interstices.info, avec le soutien d'Inria, de la fondation Blaise Pascal, de la SIF et de l'Université de Lorraine. Le graphisme a été réalisé par un tout jeune dessinateur (Triton Mosquito) qui a eu à cœur de rendre hommage à chaque personnalité. Une première impression a été diffusée auprès des enseignants du secondaire volontaires.

Ce jeu de 7 familles est donc un support pour entrer dans les sciences de l'informatique, tant au travers de son évolution dans le temps qu'en fouillant une thématique particulière. Il est tout aussi bien utilisable en primaire (expérience à faire) qu'au lycée (n'hésitez pas à utiliser les cartes pour réaliser le fameux tour de magie de Marie Duflot).

Alors pour animer vos soirées et vous préparer aux nouveaux programmes sur l'informatique au lycée, n'hésitez pas, découvrez le jeu de 7 familles de l'informatique !

Et si vous êtes vraiment joueurs, découvrez notre quizz sur les personnalités du jeu

Maxime Amblard
Université de Lorraine

Lien vers la vidéo sur YouTube

25.09.2019 / La Tribune

Comment Google doit prouver la s quantique

Par François Manens | 30/09/2019, 17:59 | 1069 mots

Depuis la fuite de l'article scientifique sur la suprématie quantique, Google n'a pas commenté son contenu et s'expose donc à des critiques. (Crédits : Arnd Wiegmann)

La semaine dernière, la Nasa laissait fuiter un article scientifique de Google sur son site, avant de le retirer. Les chercheurs de l'entreprise américaine y annonçaient la suprématie quantique, le point où l'ordinateur quantique va au-delà des capacités de l'ordinateur classique. Depuis, Google n'a pas commenté cette affirmation, et s'expose aux critiques. Nous avons demandé à Simon Perdrix, chargé de recherche au CNRS, comment le géant peut s'y prendre pour démontrer le dépassement de la suprématie quantique.

FRANÇOIS MANENS

DU MÊME AUTEUR

AVC ou crise de panique ? Le danger des biais dans la santé

Avec l'Oculus Quest, Facebook peut-il faire de la réalité virtuel...

La startup de la semaine : comment Defymed va révolutionner le qu...

Abonnez-vous

Comment prouver quelque chose jamais observé ? Voilà le casse-tête qu'ont dû se poser les équipes de Google, avant d'affirmer avoir atteint la suprématie quantique, dans un article. Cette avancée, même si elle ne porte que sur un calcul très précis, signifierait que les chercheurs sont parvenus à dépasser un stade essentiel pour le futur de l'informatique quantique.

Cependant, les conditions chaotiques de la diffusion de l'article ont gâché l'effet d'annonce. L'article a été publié par la Nasa puis retiré, mais le Financial Times l'avait déjà repéré. Depuis, l'équipe de chercheurs de Google ne s'est pas exprimée sur le sujet. Elle n'a pas pu répondre aux critiques formulées sur son travail, notamment par Dario Gil, directeur de la recherche chez IBM, un des principaux concurrents dans la course à l'informatique quantique.

Il n'est pas rare que Google - comme d'autres - fasse part de ses découvertes avant leur parution dans des revues scientifiques. Le processus de publication dans une revue scientifique est contraignant et il prend facilement plus de six mois. En revanche, il a des avantages certains : des correcteurs indépendants vont vérifier le sérieux de la démarche et remonter leurs interrogations. Si l'article est publié, il confirme la qualité de la recherche, même si certains doutes peuvent subsister.

Pour comprendre comment Google peut confirmer son annonce, nous avons posé des questions à Simon Perdrix, directeur du Groupe de Travail Informatique Quantique du CNRS. Ce chargé de recherche au Loria (laboratoire lorrain de recherche en informatique et ses applications) travaille sur les couches logicielles de l'informatique quantique. Concrètement, il développe à la fois des modèles de calcul quantique qui feront tourner les machines, mais aussi des techniques pour utiliser l'ordinateur quantique.

LA TRIBUNE : Quel est votre avis sur cet article de Google ?

SIMON PERDRIX - C'est un résultat sérieux, mais il a été mis en ligne par erreur. Nous pouvons imaginer que Google va bientôt publier un nouvel article dans une revue scientifique de renom, avec les relectures nécessaires. Nous y verrons alors plus clair.

Comment les chercheurs peuvent-il démontrer la suprématie quantique sur leur calcul ?

La suprématie quantique n'est pas simple à démontrer. Il faut d'abord prouver que l'ordinateur classique ne peut pas faire le calcul. C'est déjà un premier obstacle, car établir un résultat d'impossibilité s'avère très souvent laborieux. Ensuite, il faut aussi prouver que l'ordinateur quantique a bien résolu le problème.

Concrètement, comment faut-il s'y prendre ?

Pour cette expérience, Google a utilisé un calculateur quantique à 53 qubits [unité de puissance d'un calculateur quantique, ndlr]. Aujourd'hui, nous considérons que la puissance nécessaire pour qu'un ordinateur quantique dépasse un ordinateur classique se situe autour de 50 qubits. L'ordinateur de Google est très proche de la limite, donc. D'un côté, c'est un problème, car les qubits peuvent être imparfaits ou avoir beaucoup de bruit [insérer de nombreuses erreurs dans leurs calculs, ndlr], et l'ordinateur se situerait alors en dessous de cette limite théorique. Mais d'un autre côté, pour prouver que l'ordinateur quantique est capable d'obtenir ce résultat, cette proximité avec la frontière s'avère intéressante. Dans tous les cas, fabriquer un ordinateur quantique avec 53 qubits de bonne qualité est déjà une prouesse.

En quoi utiliser un calculateur quantique relativement peu puissant a-t-il aidé les chercheurs de Google ?

Pour prouver que les résultats sont bons, les chercheurs vont prendre le même problème sur des machines avec moins de qubits, et comparer ses résultats à ceux d'un ordinateur classique. Si les deux correspondent, ils vont reproduire l'expérience sur des machines avec davantage de qubits. Ils augmentent ainsi la puissance du calculateur quantique jusqu'à ce que la comparaison avec l'ordinateur classique ne soit plus possible.

Les chercheurs affirment qu'il faudrait 10.000 ans au plus gros superordinateur classique pour parvenir au même résultat. Comment expliquer que l'ordinateur classique accuse un tel retard quand l'ordinateur quantique dépasse le palier des 50 qubits ?

Si nous mettons de côté la variable de temps, il n'y a pas de différence entre les capacités des deux machines. Par exemple les deux peuvent résoudre des problème de la factorisation, puisque c'est une opération que nous savons même faire à la main. Sauf que quand le nombre à factoriser est grand, le calculateur quantique peut ne prendre que quelques minutes là où il faudrait des milliers d'années à un ordinateur normal.

La suprématie quantique abordée dans l'article porte sur un calcul unique, très précis. Pourriez-vous le vulgariser ?

Dans leur expérience, les chercheurs ont choisi, au hasard, un circuit quantique qu'ils ont exécuté plusieurs fois. Ensuite, ils ont mesuré les résultats qu'ils obtenaient, et ils en ont tiré des probabilités. Ils affirment avoir atteint la suprématie quantique car la distribution des probabilités issues de ces résultats est extrêmement difficile à obtenir de façon classique.

Certaines critiques relèvent le côté inutile de ce calcul, qui réduirait l'ampleur du terme "suprématie quantique". Qu'en pensez-vous ?

Côté application, ce qu'ils ont découvert pourrait devenir un protocole pour certifier de l'aléatoire. Concrètement, nous pourrions nous en servir comme d'une bonne source d'aléatoire dans plusieurs domaines, notamment en cryptographie [discipline qui porte sur la protection des messages, ndlr].

Mais il faut aussi comprendre que démonter la suprématie quantique n'équivaut pas à résoudre un problème utile. Nous pouvons imaginer que dans le futur, nous répondrons à des problèmes utiles grâce aux calculateurs quantiques : d'ailleurs nous y travaillons déjà avec les machines quantiques disponibles actuellement. Mais quand nous y parviendrons, il n'est même pas sûr que nous ayons les moyens de prouver la suprématie quantique sur ces tâches. Et pour cause : il sera toujours difficile de prouver qu'un ordinateur classique ne peut pas résoudre les même problèmes efficacement. ■

SUR LE MÊME SUJET

Google a-t-il oui ou non atteint la suprématie quantique ?

Antitrust : 50 Etats américains vont enquêter sur Google

En donnant raison à Google, la CJUE enterre la vision française d...

Pourquoi l'arrivée de Google dans le jeu vidéo est un vrai séisme

Le futur de la robotique se dessine peut-être à Vittel

Les journées nationales de la recherche en robotique (JNRR) se tiennent à Vittel depuis mardi. Jusqu'à ce jeudi matin, environ 180 chercheurs sont réunis au palais des congrès pour partager le fruit de leurs recherches et échanger sur les futures innovations.

Par Maya DIAB - 17 oct. 2019 à 05:03 - Temps de lecture : 4 min

Des entreprises étaient présentes au palais des congrès pour présenter les dernières innovations, comme ce bras articulé ou cette imprimante 3D. Photo VM /Maya DIAB

« L'idée est de rassembler toute la communauté de la recherche en robotique pour échanger sur les dernières avancées dans tous les domaines », explique Philippe Fraisse, directeur du groupe de recherche en robotique au CNRS (Centre national de la recherche scientifique). « Les robots sont des systèmes qui vont générer du mouvement. Par exemple, les voitures autonomes, les drones, les bras industriels sont des robots. »

Moins d'erreurs que les humains

Ces journées nationales de la recherche en robotique sont un moyen d'entrapercevoir ce que sera le futur. « Par exemple, il y a une vingtaine d'années, alors que je préparais ma thèse, on parlait déjà de voitures autonomes », un sujet désormais d'actualité.

La robotique est présente dans de nombreux domaines, les chercheurs s'attendent à ce que sa présence soit de plus en plus prégnante dans notre société. « C'est indéniable », assure Philippe Fraisse. « Dans le transport par exemple, il y aura de grandes mutations, même s'il est difficile de prévoir exactement de quoi il en retournera demain. »

Les scientifiques imaginent qu'il n'y aura peut-être plus de chauffeurs routiers. « Ils se projettent déjà plutôt dans l'idée qu'il y aura quelqu'un à bord du camion, mais qui fera autre chose que conduire, comme de la logistique, de la gestion etc. », détaille Olivier Simonin, co-organisateur de l'événement. « Il y a un aspect sécuritaire également », renchérit François Charpillet, également organisateur. « Avec les véhicules autonomes, il y a l'espoir que le robot commette moins d'erreurs que les humains et qu'il y ait donc moins d'accidents. »

01 / 04 De gauche à droite : Olivier Simonin, François Charpillet et Philippe Fraisse. Photo VM /Maya DIAB

Étudier aussi l'humain

Les robots sont aussi présents dans le domaine de la santé et de l'environnement, avec le développement de robots en chirurgie ou pour la dépollution comme le désamiantage. Les chercheurs se penchent également sur la cobotique, des robots collaboratifs qui travaillent avec l'humain en effectuant les tâches les plus pénibles ou répétitives. Cela permet, entre autres, de réduire les risques de troubles musculosquelettiques. « On a également fait des tests en rééducation en gériatrie avec des robots. C'est passionnant, cela nous fait étudier aussi l'humain, notamment avec des psychologues, sur l'acceptabilité du robot », s'enthousiasme François Charpillet.

Justement, le robot est-il accepté dans notre société où il est souvent le personnage principal de films ou de séries dystopiques ? « Tant que les innovations ne sont pas dans le domaine public, l'art s'en empare, notamment au sujet de l'intelligence artificielle. C'est cela qui alimente le fantasme, notamment autour du transhumanisme. Les films comme « Terminator » ou « Blade Runner » en sont des exemples. Les Japonais sont culturellement très demandeurs, en Europe, les gens sont un peu plus méfiants vis-à-vis de la machine. »

Industrie, santé, agriculture, transport... les robots vont-ils remplacer les humains au travail ? Les chercheurs pensent que des emplois vont disparaître, mais que d'autres seront créés. Les robots ne sont donc pas (encore) prêts à envahir le monde.

« Être au plus près des innovations »

Dans le hall d'accueil du palais des congrès, trois entreprises sont présentes et exposent les dernières innovations en matière de robotique. « La plupart des participants ici ont des projets d'études, ils ont parfois besoin d'investir dans du matériel », explique Sébastien Manigot, ingénieur des ventes chez SBG Systems, une entreprise qui fabrique des centrales inertielles, permettant, entre autres, la navigation autonome pour une voiture ou encore un bateau.

« En étant là pour ces journées nationales, on est au plus près des innovations, en contact direct avec les experts », ajoute Christophe Arnould, de chez RS Components. Sur sa table de présentation, trônent une imprimante 3D, un bras articulé et des oscilloscopes. En face de lui, Alexis Michel, stagiaire chez Génération Robots, présente quelques équipements, dont une caméra capable de reconnaître les objets et les êtres humains. « On doit se tenir au courant de ce qu'il se passe au niveau de la recherche », affirme-t-il.

2020, année de la robotique

Selon François Charpillet, 2020 sera l'année de la robotique en France. « Tout d'abord, notre pays va accueillir l'une des deux grandes conférences internationales de robotique, appelée ICRA (International Conference on Robotics and Automation). » L'événement aura lieu au palais des congrès de Paris du 31 mai au 4 juin 2020. « Il y aura des chercheurs du monde entier. »

Quelques semaines plus tard, Bordeaux accueillera la Robocup. « C'est une compétition où les robots doivent être capables d'effectuer certaines actions », détaille le chercheur.

Edition La Plaine | Economie | +

08.11.2019 / L'Est Républicain

VILLERS-LÈS-NANCY Citoyenneté

Comment inventer la République du futur

Conférences, tables rondes et expos à l'affiche pour la 5e édition de République en tête(s), sur le thème de la République du futur.

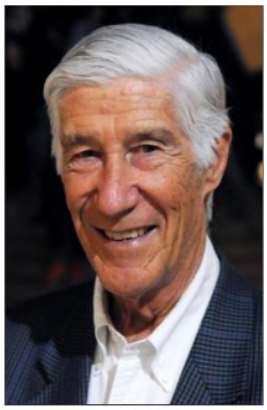
La 5e édition de République en tête(s) se décline jusqu'au 10 novembre sur le thème de la République du futur. « En écho aux attentats qui ont frappé Paris en 2015, République en tête [s] est un événement annuel qui a pour but de permettre à chacun, avec sa propre sensibilité, de revenir sur tous les enjeux que nous questionnons depuis lors : la liberté, les différences, la tolérance » souligne le maire François Werner.

« Face à l'urgence climatique, aux poussées nationalistes et xénophobes, au creusement des inégalités, il paraît primordial de réinventer notre rapport au monde et d'imaginer un futur à notre société et à nos enfants. Comment se départir des visions anxiogènes pour construire un monde meilleur ? »

Les réponses que les intervenants tenteront d'apporter s'adresseront à des publics variés, adultes, professionnels, enseignants, enfants et scolaires. L'entrée est libre.

Le programme

- Exposition Julian Rivière, Maisons/Pluies, jusqu'au 10 novembre, galerie Mme-de-Graffigny.
- Exposition participative : Le kiosque aux 400 coups de main de l'association Michel Dinet - Fraternité en actes, Hôtel de ville, jusqu'au 22 novembre.
- Villes interculturelles, villes résilientes ? Rencontre avec Irena Guidikova, cheffe de la division Programme d'Inclusion et d'anti-discrimination au Conseil de l'Europe, samedi 9 à 10 h 30, salle Jean-Ferrat.
- Atelier culinaire et causerie avec Gérard Verret, samedi 9 à 11 h, 14 h et 15 h au château Mme-de-Graffigny.
- Prospective, perspective, gestion du risque climatique : comment envisager le futur de la planète ? Rencontre avec Bettina Laville, présidente du Comité 21, Olivier Parent, prospectiviste, Yvette Veyret, géographe, Jean-Pierre Schmitt, Atmo Grand Est, Romain Grandjean, The Shift Project, samedi 9 à 14 h 30, salle Jean-Ferrat.
- Demain, un pour tous et tous pour un ? Intelligence collective, interconnexion, démocratie contributive, des concepts novateurs ? Rencontre-débat avec Vincent Beillard, maire de Saillans, Nicolas D'Ascenzio, coordinateur du Shadock/la Coop, Samuel Nowakowski, chercheur Infocomm, Loria, Philippe Sessiecq, directeur adjoint des Mines Nancy, Louis Ollagnon, carto-débat, samedi 9 à 16 h, château Mme-de-Graffigny.
- Artistes et visionnaires, la force de l'imagination. Table ronde avec Yves Blanc, journaliste, Susana Gállego Cuesta, directrice du Musée des Beaux-Arts de Nancy, Veronika Petit, collectif Kinorev, théâtre d'anticipation, samedi 9 à 17 h 30, galerie Mme-de-Graffigny.
- L'Homme et le robot. Faut-il avoir peur de l'Intelligence artificielle et du transhumanisme ? Rencontre avec Joël de Rosnay, scientifique, samedi 9 à 20 h 30, salle Jean-Ferrat.



Rencontre avec Joël de Rosnay samedi 9 à 20 h 30.

Doctorat en Lorraine : 8 thèses à l'honneur !

21 novembre 2019 - 14:00 par Infodujour

La cérémonie de remise des diplômes de doctorat et des prix de thèse 2019 de l'Université de Lorraine aura lieu le vendredi 22 novembre à l'Amphi Le Moigne sur le Campus du Saulcy à Metz.

Désormais, les doctorants doivent aussi apprendre à vulgariser leurs recherches. (Ici à l'Education University of Hong-Kong) Lisa Jeanson, Author provided

Impact psychologique de l'épisiotomie, traitement alternatif à la chirurgie pour les cancers de la tête et du cou, analyse autour du débat sur l'énergie nucléaire en Lorraine, prise en compte des paramètres agronomiques des sols dans le développement urbain, valorisation du hêtre et développement d'un outil de biotechnologie pour sonder la durabilité de certains bois, etc.
Tous ces travaux de thèse seront récompensés le vendredi 22 novembre 2019 lors de la cérémonie de remises des diplômes de doctorat et des prix de thèses 2019.

Christophe Clesse – SLTC (sociétés, langages, temps, connaissances)

Ses recherches ont permis d'évaluer avec précision l'impact psychologique que pouvait engendrer une épisiotomie. Après une série d'entretiens avec des femmes enceintes, il a pu comparer les conséquences des différents modes d'accouchement (césarienne, épisiotomie, déchirure...) en se centrant plus précisément sur l'épisiotomie.
Christophe Clesse a réalisé sa thèse en parallèle d'un travail de psychologue à plein temps. Depuis l'obtention de son doctorat, il a continué à exercer tout en ayant pu bénéficier d'un contrat d'ingénieur de recherche à temps partiel au sein de son laboratoire de rattachement (INTERPSY). Actuellement, il est en partance pour Londres dans le but d'obtenir un post-doc au sein d'une université anglo-saxonne ou encore intégrer un projet de recherche dans les domaines qui le passionnent : périnatalité et parentalité, féminité et masculinité, neuropsychanalyse ou encore psychologie communautaire.

Doctorant à l'université de Lorraine

Marie Millard – BioSE (biologie, santé, environnement)

Ses travaux de recherche ont porté sur la thérapie photodynamique (traitement alternatif à la chirurgie pour les cancers de la tête et du cou) et plus précisément sur comment limiter les effets secondaires tout en améliorant l'efficacité thérapeutique.
Actuellement, Marie Millard est en post-doctorat au sein du laboratoire de nanomédecine régénérative (Inserm/Université de Strasbourg). Elle travaille sur la mise en place d'un modèle tridimensionnel vascularisée, à partir de biopsie de patients, permettant de recréer au plus proche une micro tumeur de poumons dans le but de tester des médicaments anticancéreux.

Vincent Carlino – HN-FB (humanités Nouvelles – Fernand Braudel)

Ses travaux de recherche ont consisté en l'analyse des formes actuelles et passées du débat sur l'énergie nucléaire en Lorraine.
Actuellement, Vincent Carlino est en postdoc à l'Académie du journalisme et des médias de l'Université de Neuchâtel (Suisse) où il contribue à un projet de recherche sur les fake news, les publics et le journalisme.

Anne Blanchart – SIReNa (science et ingénierie des ressources naturelles)

Ses travaux de recherche portent sur la prise en compte des paramètres agronomiques des sols dans le développement urbain pour adapter l'usage du foncier aux caractéristiques agronomiques des sols et optimiser les bienfaits que peut fournir cette ressource pour le développement d'une ville durable. Depuis juillet 2019, Anne Blanchart a créé son propre bureau d'études spécialisé en agronomie, en pédologie, en écologie des sols et en urbanisme « Sol & co » où elle travaille en collaboration avec Quentin Vincent, un ancien doctorant de l'Université de Lorraine.

Mathieu Schwartz – C2MP (chimie, mécanique, matériaux, physique)

Ses travaux de recherche ont permis de développer un outil de biotechnologie pour sonder la durabilité de certains bois.
Actuellement, Mathieu Schwartz est chargé de recherche au Centre des Sciences du Goût et de l'Alimentation à l'INRA de Dijon. Il travaille sur le rôle de protéines salivaires dans la métabolisation et le transport des arômes, influençant la perception de la flaveur.

Charlotte Grosse – SIMPPÉ (science et ingénierie des molécules, des procédés, des produits et de l'énergie)

Ses travaux de recherchent portent sur la valorisation du hêtre et le développement de matériaux de construction bio-sourcés performants. Grâce à un traitement thermique, elle a pu améliorer considérablement les propriétés du hêtre, le rendant utilisable en extérieur.

Actuellement, Charlotte Grosse a rejoint l'entreprise Luxembourgoise Leko (www.lekolabs.com) où elle se consacre à l'étude de ce matériau au sein de leur laboratoire.

Loïc Malfettes – SJPEG (sciences juridiques, politiques économiques et de gestion)

Ses travaux de recherche ont permis de faire la lumière sur ce qui se présentait comme une « crise » des sources, en particulier en droit du travail.
Actuellement, Loïc Malfettes est juriste et poursuit ses recherches dans le champ du droit social au sein de l'Institut François Geny de l'Université de Lorraine.

Simon Abélard – IAEM Lorraine (informatique, automatique, électronique-électrotechnique, mathématiques et sciences de l'architecture)

Ses travaux de recherche portent sur le calcul du nombre de solutions de certaines équations en cryptographie (protection et authentification de données) et en théorie des nombres. Il propose une analyse de nouveaux algorithmes plus efficaces.
Actuellement, Simon Abélard entame un second postdoc au LIX (laboratoire d'informatique de l'École Polytechnique) toujours sur des problèmes liés aux courbes algébriques. Les applications qui en découlent concernent les codes correcteurs d'erreurs, outils essentiels au stockage et à la transmission de données.

UL : 60.000 étudiants

Le doctorat est le plus haut diplôme de l'enseignement supérieur (8 années d'études après le baccalauréat). Il se prépare au sein d'une école doctorale, après obtention d'un diplôme conférant le grade de master ou d'un niveau équivalent. Après validation d'une soutenance de thèse, cette formation permet d'obtenir le grade de docteur. La recherche répond aux grands enjeux sociétaux à venir. Les études doctorales représentent donc un enjeu majeur qui intéresse le monde scientifique et la société tout entière grâce au recrutement par les entreprises privées et publiques tournées vers la recherche et l'innovation.
Source : site du ministère de l'enseignement supérieur, de la recherche et de l'innovation

L'Université de Lorraine est un établissement public d'enseignement supérieur composé de 10 pôles scientifiques rassemblant 60 laboratoires et de 9 collégiums réunissant 43 composantes de formation dont 11 écoles d'ingénieurs. Elle compte près de 7 000 personnels et accueille chaque année plus de 60 000 étudiants.

Deux nouveaux records dans le cassage de clés de chiffrement

Au terme de 35 millions d'heures de calcul, une équipe internationale est parvenue à inverser des opérations mathématiques utilisées pour assurer la sécurité informatique.

Par David Larousserie • Publié le 03 décembre 2019 à 14h24 - Mis à jour le 03 décembre 2019 à 14h28

Une équipe de l'Inria à Nancy et du Laboratoire lorrain de recherche en informatique et ses applications (Loria – Inria, CNRS), associée aux universités de Limoges et de San Diego (Californie), a battu simultanément deux records numériques. Ces deux prouesses éprouvent la solidité de la sécurité informatique de systèmes aussi courants que les paiements par carte bancaire ou les communications en ligne. Ces chercheurs ont démontré jusqu'à quel niveau les chaînes de sécurité de tels systèmes pouvaient tenir, comme ils l'ont expliqué lundi 2 décembre à la conférence Elliptic curve cryptography à Bochum (Allemagne). Ces niveaux se mesurent par la taille des nombres, appelés clés, utilisés dans les protocoles de sécurité. Leur réponse est que l'utilisation de tout nombre inférieur à 240 chiffres (ou 795 bits) est dangereuse. C'est-à-dire que le chiffrement qu'il permet pourrait être cassé et les messages déchiffrés.

Les précédents records sur ce type d'exercice dataient de 2009 et 2016 pour des nombres à 768 bits. Ces quelques bits d'écart peuvent sembler faibles, mais les spécialistes estimaient que le « cassage » devait être deux fois et demie plus difficile.

Le logiciel utilisé est désormais en open source

Il aura fallu 35 millions d'heures de calcul (ou 4 000 ans pour un PC doté d'un seul cœur) et trois centres de calcul pour venir à bout des deux records. Le chantier a été lancé il y a plus d'un an et a consisté à améliorer l'algorithme précédent. D'ailleurs, à puissance de machine équivalente, les chercheurs ont mis 25 % de temps en moins pour ce record que pour le précédent. Le logiciel utilisé est désormais en open source, *« là aussi une première »*, souligne Emmanuel Thomé, responsable de cette équipe au Loria.

Deux opérations mathématiques

Les deux records sont liés à deux opérations mathématiques. La première consiste à chercher les deux nombres premiers dont le produit donne la clé de 795 bits. Ces nombres servent ensuite à chiffrer des communications ou des messages. La seconde, appelée problème du logarithme discret, implique des calculs de puissance et sert en général pour protéger la première étape d'un protocole de sécurité. Les deux sont des fonctions mathématiques d'autant plus difficiles à inverser que les nombres impliqués sont grands.

La sécurité des échanges informatiques actuels n'est cependant pas menacée puisque les clés utilisées, ou en tout cas recommandées, sont bien plus grandes, de l'ordre de 2048 bits. *« L'un des intérêts de cette démonstration est d'avoir montré que les deux calculs sont presque aussi difficiles l'un que l'autre, alors que la communauté pensait que le problème du logarithme discret était plus dur »*, note Emmanuel Thomé, qui a tout de même identifié un objet connecté doté d'une clé de 768 bits seulement.

David Larousserie

La difficile mise en place des cours de programmation informatique en primaire

Seule la moitié des professeurs enseigne aujourd'hui le code à l'école, alors que cette discipline figure dans les programmes depuis septembre 2016.

WALLY BORDAS @wallybordas

ÉDUCATION « *Il faut apprendre à coder dès 10 ans.* » En 2016, dans une interview accordée au média *Acteurs publics*, Cédric Villani, la star française des mathématiques, désormais député et candidat à la mairie de Paris, militait pour un apprentissage de la programmation informatique dès l'école primaire. Cet enseignement, déjà expérimenté dans plusieurs établissements depuis 2014, fait désormais partie des programmes de primaire et du collège depuis la rentrée 2016.

En primaire, les élèves apprennent à « programmer les déplacements d'un robot ou d'un personnage sur écran » ou à « construire une figure simple ». Mais la mise en place de ce nouvel enseignement n'est pas aussi facile que prévu. Selon une étude effectuée par plusieurs enseignants-chercheurs auprès de 578 professeurs des écoles en 2018, 45 % d'entre eux n'enseignent pas encore la programmation dans leur classe. En réalité, le chiffre serait même beaucoup plus élevé. « *Il n'y a pas la moitié des instituteurs qui enseigne aujourd'hui le code à leurs élèves* », confie un enseignant ayant travaillé à la mise en place de la réforme. Le ministère, qui affirme ne pas avoir de données officielles, admet à demi-mot que les chiffres évoqués correspondent à peu près à la réalité.

Des professeurs peu formés

Pour Colin de la Higuera, enseignant-chercheur à Nantes et ancien président de la Société informatique de France (SIF), une association qui a œuvré pour que le code soit enseigné aux élèves dès le plus jeune âge, la raison de ces difficultés est évidente : « *Beaucoup trop d'argent a été dépensé pour l'achat de matériel alors que la priorité était la formation des enseignants. Cela ne sert à rien d'avoir des robots dernier cri si les professeurs n'ont pas les prérequis pour en parler aux élèves* », explique-t-il. « *On ne peut pas passer de 0 à 100 % de professeurs formés en trois ans*, se défend Jean-Marc Merriaux, directeur du numérique pour l'éducation (DNE) au ministère de l'Éducation nationale. *Nous avions un certain retard sur les autres pays d'Europe, nous sommes en train de le rattraper.* » Les enseignants, quant à eux, sont très mitigés sur la question. « *Je ne savais même pas que c'était au programme* », répond Marine une jeune enseignante parisienne. « *Je n'ai encore jamais enseigné le code*, avoue de son côté Julie, en poste en Île-de-France. *En réalité, je ne vois pas très bien ce que c'est, il faudrait que je me forme. Mais ce n'est clairement pas ma priorité.* » Erwan, lui, a dû apprendre seul pour pouvoir enseigner la programmation à ses élèves. « *On ne m'a jamais proposé une quelconque formation sur le sujet et, même en cherchant, je n'ai rien trouvé. C'est une collègue qui m'a appris les bases. Je me suis formé assez facilement, mais une personne réfractaire aura beaucoup plus de mal* », admet-il. Le jeune professeur des écoles, qui enseigne le code pour la deuxième année consécutive, se dit en tout cas « *satisfait* » de l'apport de ce nouveau module. « *Les élèves sont très réceptifs car l'interface sur laquelle nous travaillons est ludique*, explique-t-il. *Il faut prendre le temps de leur expliquer quel est le sens de ce qu'ils font pour qu'ils comprennent que ce n'est pas juste un jeu.* »

Des avis mitigés

L'apprentissage du code a ses adeptes. « *La programmation permet de structurer la pensée. Lorsqu'un professeur de maths demande aux élèves de résoudre un problème, ils vont proposer une solution et c'est leur enseignant qui leur dira si leur réponse est bonne. Lorsqu'ils vont essayer de résoudre un problème algorithmique, ils se rendront compte seuls que cela ne fonctionne pas et essaieront eux-mêmes de trouver une alternative* », analyse Marie Duflot-Kremet, maître de conférences en informatique à l'université de Lorraine et chercheuse à l'Inria. « *Apprendre le code permet aux jeunes de faire travailler leur créativité et leur imagination. En écrivant un algorithme, ils inventent une histoire. Cela peut d'ailleurs les aider à progresser dans d'autres matières, comme les mathématiques ou le français* », complète Colin de la Higuera.

Un argument qui n'a pour l'instant pas été prouvé scientifiquement. Une étude effectuée en Italie auprès de 150 enfants de 7 à 9 ans indique même le contraire. Ces élèves ont utilisé Scratch, un logiciel pour apprendre la programmation, au moins 2 heures par jour pendant plusieurs semaines. À l'issue de cette période, leurs résultats scolaires n'ont pas augmenté dans les autres matières. Grégoire Borst, professeur de neurosciences de l'éducation, explique : « *Cela ne signifie pas que l'apprentissage du code n'apporte rien, cela veut juste dire qu'a priori, il ne permet pas de progresser en français, en mathématiques ou dans les autres matières.* »

André Giordan, neurophysiologiste et spécialiste de l'apprentissage du numérique, estime que l'apprentissage du code aux élèves n'est « *absolument pas nécessaire* ». « *Cela ne sert à rien*, tranche-t-il. *On apprend la programmation aux enfants alors même que l'intelligence artificielle est en pleine explosion et qu'ils n'auront donc nullement besoin de la connaître. Si aujourd'hui on a quelque chose à enseigner à l'école, ce n'est sûrement pas ça.* » Quoi qu'il en soit, le gouvernement n'entend pas faire machine arrière sur ce sujet. « *L'apprentissage du code permet d'acculturer les élèves à certains enjeux. C'est le rôle de l'école. Cet enseignement leur permettra de comprendre le monde dans lequel ils vont évoluer afin qu'ils puissent le faire en toute autonomie* », conclut Jean-Marc Merriaux, du ministère de l'Éducation nationale. ■

Mathis, Hamza... et le robot Thymio

CE MATIN, à l'école Pierre-de-Coubertin de Mantes-la-Jolie (Yvelines), située dans le quartier Gassicourt en zone Rep+ (réseau d'éducation prioritaire), dans le nord de la ville, les 23 élèves de CM2 sont tout sourire. Aujourd'hui, pour la première fois, ils vont pouvoir utiliser Thymio, un petit robot qui permet d'apprendre la programmation informatique. Pendant plusieurs séances, ils découvriront les différentes fonctionnalités de la machine, avant d'entrer dans la véritable phase d'apprentissage du code, où ils programmeront sur ordinateur les déplacements du robot.

Thomas Cochin, leur professeur, introduit la séance du jour, qui durera une heure. « *C'est quoi comme robot ?* », interroge Mathis, tout excité par la découverte de cette nouveauté. « *Vous allez voir* », répond l'instituteur en distribuant les appareils. La machine blanche, qui fait peu ou prou le diamètre d'une petite boîte à bijoux, déclenche immédiatement l'euphorie générale. Dès la mise en marche de l'appareil, les questions fusent : « *Pourquoi il change de couleur quand on appuie là ?* », « *Comment on fait pour le faire reculer ?* », « *Pourquoi il avance dans le mauvais sens ?* »

> **« Depuis que j'exerce, j'ai souvent vu des élèves décrocheurs s'ouvrir et prendre confiance grâce au cours de programmation »**
>
> LAURENT TOUCHÉ, CONSEILLER PÉDAGOGIQUE POUR LES USAGES NUMÉRIQUES

Après avoir haussé le ton pour faire revenir le calme, Thomas Cochin explique à ses élèves : « *Chaque lumière correspond à un mode. On va essayer de voir ensemble ce que fait le robot dans chacun de ces modes.* »

Pour l'occasion, Laurent Touché, conseiller pédagogique pour les usages numériques de l'académie de Versailles, est venu assister l'enseignant. « *Sur le bassin de Mantes-la-Jolie, nous sommes deux conseillers à faire le tour des écoles pour aider les enseignants lorsqu'ils enseignent la programmation informatique. La plupart du temps, c'est nous qui amenons le matériel* », explique-t-il. Alors que les élèves expérimentent en groupe la machine, le spécialiste analyse leurs premiers pas : « *Pour la plupart, c'est la première fois de leur vie qu'ils voient un robot et qu'ils peuvent le tester. Ils sont envahis par l'émotion* », décrypte-t-il. C'est en effet ce qui marque le plus lors de cette séance d'initiation au code : la plupart des élèves sont très agités, si bien que leur professeur est obligé d'intervenir à plusieurs reprises.

Cette séance ne ressemble pas vraiment à l'idée que le quidam pourrait se faire d'un cours de « code ». Les enfants s'amusent et rient beaucoup en appuyant sur les différents boutons du robot. À première vue, ils ne retiendront pas une once de base en programmation informatique aujourd'hui. Et pourtant, selon Laurent Touché, c'est tout le contraire : « *Regardez, ces élèves sont en train de construire un labyrinthe avec leurs trousses et leurs cahiers pour voir si le robot peut trouver son chemin. Ils commencent à comprendre la logique et font preuve de créativité* », veut-il croire en désignant un groupe. « *Ils n'ont pas l'impression de travailler mais, en fait, ils apprennent énormément*, insiste-t-il. *Depuis que j'exerce, j'ai souvent vu des élèves décrocheurs s'ouvrir et prendre confiance grâce au cours de programmation.* »

Thomas Cochin, qui a déjà enseigné le code à ses élèves l'année dernière, vante également les mérites du dispositif : « *Nous sommes dans un établissement Rep+ où certains élèves sont parfois en grande difficulté. Les cours de code tels que nous les enseignons leur permettent de sortir du cadre scolaire et leur apportent de la nouveauté* », vante-t-il.

Le cours se poursuit avec une phase de réflexion, durant laquelle les élèves, beaucoup plus calmes, prennent la parole et expliquent à leur instituteur ce qu'ils viennent d'expérimenter. « *Avec la lumière jaune, il bouge en évitant les obstacles* », tente Hamza. « *Exactement !* », félicite Thomas Cochin, en prenant soin de noter chacune des remarques de ses élèves au tableau. Pour finir, le professeur distribue une carte à tous les groupes : sur chacune d'elles, une mission à faire accomplir à leur robot. « *On doit faire marquer un but à Thymio* », se réjouit Djibril, maillot du PSG sur le dos. « *Il faut qu'on dessine quelque chose avec lui, mais il fait que des gribouillis* », déplore de son côté Ayoub. La sonnerie retentit, le cours est terminé. Après la récréation, place aux mathématiques, les vraies. ■ **W. B.**

Des élèves se frottent pour la première fois au code informatique à l'aide du petit robot Thymio *(ci-dessus et ci-contre)*, à l'école Pierre-de-Coubertin, début octobre à Mantes-la-Jolie (Yvelines). JEAN-CHRISTOPHE MARMARA/LE FIGARO

SNALC

> Beaucoup de professeurs des écoles ne s'estiment pas compétents, car ils n'ont pas reçu de formation sur le sujet. Et comme ils ont une éthique professionnelle, ils préfèrent enseigner des choses qu'ils maîtrisent
>
> JEAN-RÉMI GIRARD

« Avant de coder, les élèves ont besoin d'apprendre les fondamentaux »

JEAN-RÉMI Girard est le président du Syndicat national des lycées et collèges (Snalc).

LE FIGARO. – L'apprentissage de la programmation à l'école primaire, est-ce une bonne idée ?
Jean-Rémi GIRARD. – Non, nous avons autre chose à faire. Avant de coder, les élèves ont besoin d'apprendre les fondamentaux : l'écriture, la lecture, l'histoire, les mathématiques, les enseignements artistiques. On a passé des années à taper sur le code grammatical, et là, il faudrait enseigner le code informatique. « *Le code pour tous* » est un slogan stupide. Tout le monde ne va pas s'amuser à coder. Quand on voit les enquêtes sur le niveau de nos élèves, on se dit qu'on a peut-être d'autres priorités avant d'apprendre l'informatique dès le plus jeune âge.

Peu d'instituteurs enseignent le code, alors qu'il fait désormais partie du programme officiel. Pourquoi ?
Apprendre le code aux élèves n'est pas jugé prioritaire par la plupart des collègues. Beaucoup de professeurs des écoles ne s'estiment pas compétents, car ils n'ont pas reçu de formation sur le sujet. Et comme ils ont une éthique professionnelle, ils préfèrent enseigner des choses qu'ils maîtrisent. Puis, globalement, l'école primaire est très mal dotée et servie en termes de matériel. Il y a quelques années, 15 % des écoles primaires n'avaient pas encore de connexion internet. Ce chiffre n'a pas dû changer beaucoup. Nous n'avons ni les postes suffisants, ni les logiciels, ni les bonnes formations pour que les professeurs des écoles s'emparent de ce sujet. Et, surtout, nous n'avons pas le temps : les programmes sont chargés, avec des matières très importantes. Nous n'avons pas la possibilité de papillonner, on ne veut pas que les élèves se retrouvent avec des lacunes qu'ils auront du mal à rattraper par la suite.

Tous les professeurs des écoles peuvent-ils être formés pour enseigner le code ?
Beaucoup n'en ont pas envie, et la plupart n'ont pas le niveau. L'enseignement du code n'est pas du tout évalué au concours de recrutement de professeurs des écoles. Il n'est pas non plus proposé dans la formation continue. Il ne faut donc pas s'étonner que les collègues ne l'enseignent pas ou l'enseignent mal. ■

PROPOS RECUEILLIS PAR **W. B.**

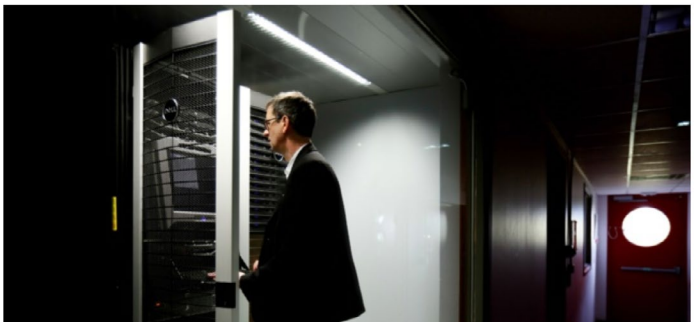
10.12.2019 / We Demain

TECH-SCIENCES

Cybersécurité : ils piègent tous les malwares du monde

Par Clément Le Foll I Publié le 10 Décembre 2019

À Nancy, We Demain a eu accès à un laboratoire ultrasécurisé où l'on capture les programmes informatiques malveillants pour mieux les combattre. Nécessaire alors que les menaces se multiplient. Au printemps, l'un de ces virus a même paralysé une ville américaine pendant plusieurs semaines...



Dans cette unité du Loria, le laboratoire lorrain de recherche en informatique et ses applications, 10 millions de logiciels malveillants ont été capturés par des ordinateurs simulant des failles. Les chercheurs les étudient pour mieux les combattre. (Crédit : Mathieu Cugnot)

Retrouvez le reportage complet dans la revue We Demain n°28, disponible en kiosque et sur notre boutique en ligne.

C'est une pièce enclavée, bercée par le bourdonnement de la climatisation. Pour y accéder, il faut franchir un sas, déverrouillé par un système de reconnaissance des veines du doigt. La petitesse du lieu contraste avec le trésor qu'il renferme. Dans les armoires de refroidissement qui garnissent la salle, 10 millions de malwares, des programmes malveillants conçus pour nuire à un système informatique, sont stockés sur des serveurs.

Nous sommes au sous-sol du laboratoire lorrain de recherche en informatique et ses applications, le Loria. Dans ce bâtiment situé en périphérie de Nancy, 400 chercheurs planchent sur des sujets liés à l'impression 3d, la robotique ou la cryptologie. Né en 1997, le Loria est un laboratoire du CNRS et de l'université de Lorraine. En 2010, il a été le premier en France à se doter d'un laboratoire de haute sécurité (LHS), destiné à une cinquantaine de chercheurs en cybersécurité. Il a été imité, en 2015, par le centre de recherche universitaire de Rennes.

Costume anthracite et lunettes rondes, Jean-Yves Marion, directeur du Loria, nous raconte comment son laboratoire capture les ennemis de nos ordinateurs. *"Nous utilisons des 'pots de miel'. Nous simulons la présence d'ordinateurs défaillants. Le malware repère la vulnérabilité, entre dans le système et, à ce moment, nous le capturons."* Dix milles malwares sont ainsi appâtés chaque jour. un chiffre à tempérer : *"Nous sommes des petits acteurs par rapport à des entreprises comme Kapersky, Symantec ou Google, qui en reçoivent 400 000 par jour."*

LA MENACE RANÇONGICIEL

D'après une étude mondiale d'Accenture, lorsqu'elle frappe une grande entreprise, une cyberattaque lui coûte en moyenne 13 millions d'euros. Face à ces chiffres, une structure comme celle du Loria est indispensable pour assurer notre sécurité numérique et surtout comprendre le fonctionnement et la manière dont se propagent ces programmes.

Le 7 mai, la ville américaine de Baltimore a été victime d'une attaque inédite qui a bloqué nombre de ses services : ordinateurs de la municipalité, paiements en ligne, ventes immobilières ou plateformes de paiement pour les impôts locaux, les factures d'eau et d'électricité. Ironie du sort, EternalBlue, le logiciel malveillant qui aurait été utilisé par les hackers, a été initialement conçu par la NSA, l'agence nationale de sécurité américaine, *"probablement à des fins d'espionnage ou de surveillance"*, précise Jean-Yves Marion.

Le malware qui a frappé Baltimore est de la famille des rançongiciels – *ransomware* en anglais. Son fonctionnement est simple. Lorsque le virus s'exécute, les fichiers de l'ordinateur sont chiffrés, comme ceux de tous les appareils qui y sont connectés. Seul le pirate possède la clé de déchiffrement et il ne la communique qu'en échange d'une rançon. Jean-Yves Marion connaît parfaitement ces programmes : *"Ce sont les malwares les plus répandus depuis Wannacry."* en 2017, cette cyberattaque mondiale a notamment paralysé une quarantaine d'hôpitaux anglais, obligés de retarder des actes médicaux...

17.12.2019 / France 3 Lorraine

Creativ'Lab au LORIA à Nancy, un outil pour l'avenir

Lien vers la vidéo sur YouTube.

New crypto-cracking record reached, with less help than usual from Moore's Law

795-bit factoring and discrete logarithms achieved using more efficient algorithms.

Researchers have reached a new milestone in the annals of cryptography with the factoring of the largest RSA key size ever computed and a matching computation of the largest-ever integer discrete logarithm. New records of this type occur regularly as the performance of computer hardware increases over time. The records announced on Monday evening are more significant because they were achieved considerably faster than hardware improvements alone would predict, thanks to enhancements in software used and the algorithms it implemented.

Many public-key encryption algorithms rely on extremely large numbers that are the product of two prime numbers. Other encryption algorithms base their security on the difficulty of solving certain discrete logarithm problems. With sufficiently big enough key sizes, there is no known way to crack the encryption they provide. The factoring of the large numbers and the computing of a discrete logarithm defeat the cryptographic assurances for a given key size and force users to ratchet up the number of bits of entropy it uses.

The new records include the factoring of RSA-240, an RSA key that has 240 decimal digits and a size of 795 bits. The same team of researchers also computed a discrete logarithm of the same size. The previous records were the factoring in 2010 of an RSA-768 (which, despite its digit is a smaller RSA key than the RSA-240, with 232 decimal digits and 768 bits) and the computation of a 768-bit prime discrete logarithm in 2016.

The sum of the computation time for both of the new records is about 4,000 core-years using Intel Xeon Gold 6130 CPUs (running at 2.1GHz) as a reference. Like previous records, these ones were accomplished using a complex algorithm called the Number Field Sieve, which can be used to perform both integer factoring and finite field discrete logarithms. A rough breakdown of the time spent in the sieving and matrixing of both the RSA factoring and the computation of the discrete logarithm problem are:

- RSA-240 sieving: 800 physical core-years
- RSA-240 matrix: 100 physical core-years
- DLP-240 sieving: 2400 physical core-years
- DLP-240 matrix: 700 physical core-years

Moore's Law takes a back seat

It's the first time that records for integer factorization and discrete logarithm have been broken together. It's also the first time two records have been set using the same hardware and software. These aren't the only things setting the latest milestones apart from previous ones.

When new records are set, the edicts of Moore's Law inevitably play a major role. Moore's Law is the trend that computer chips generally double the number of transistors they have every 18 months or so. The increase in transistors, in turn, boosts the computing power of computers running them, giving computers increased speed and performance over time.

While Moore's Law was originally an observation made by Intel cofounder Gordon Moore in 1965, it has come to be viewed as almost an inescapable force of nature, like the laws of physics. Given the relentless march of Moore's Law, it would be unusual if records like the one announced on Monday didn't occur regularly.

This one, however, is driven less by Moore's Law than previous milestones and more by improvements made in the software that carries out the Number Field Sieving. To demonstrate the boost in efficiency, the researchers ran their software on hardware that was identical to that used to compute the 768-bit discrete logarithm in 2016. They found that using the old hardware to sieve the record 795-bit size would take 25% less time than it took the same equipment to perform the 768-bit DLP computation.

Another sign of the improved performance: using identical hardware from 2016, the computation on the 795-bit logarithm was 1.33 times faster than it was on the 768-bit one. Estimates that are widely accepted in the field of cryptography predict that the larger size logarithm should be about 2.25 times harder to compute. Taken together, that suggests a three-fold performance increase over what was expected (that is 2.25*1.33=3). Since the hardware was the same for both bit sizes, the performance boost isn't attributable to the availability of ever-faster computers.

"The acceleration can be attributed to various algorithmic improvements that were implemented for these computations," the researchers wrote in Monday night's announcement. Key to those improvements were updates made to the open source software used to implement the Number Field Sieve. Known as CADO-NFS, it comprises 300,000 lines of code written in C and C++.

Emmanuel Thomé, a senior researcher at France's National Institute for Computer Science and Applied Mathematics and the leader of the team that set the record, said it's not easy to describe the optimizations in layperson's terms. The improvements, he wrote in an email, include:

> - we worked on better parallelization and memory usage (but our competitors also did, to be perfectly honest).
> - we took more systematic advantage of asymptotically fast algorithms in some compute-intensive parts of the computation.
> - there's a big part of this crypto record business that calls to the art of "choosing parameters." We did that really well. An important part of the picture is the ability to test many different parameter sets and rank them using accurate simulation tools that we developed.
>
> But it's only slightly less allusive than saying "various improvements."

Other researchers on the team included Fabrice Boudot, of France's Ministry of National Education and the University of Limoges, Pierrick Gaudry of the French National Center for Scientific Research, Aurore Guillevic with France's National Institute for Computer Science and Applied Mathematics, Nadia Heninger with the University of Pennsylvania and the University of California, San Diego, and Paul Zimmermann of France's National Institute for Computer Science and Applied Mathematics.

With so much attention devoted to the coming advent of quantum computers and their ability to easily break today's public key encryption, researchers have been busy developing new schemes that can withstand such attacks.

"In the meantime, researchers have been making progress improving classical algorithms to solve factoring and discrete log, which together with Moore's law results in new key sizes being breakable by computational resources available to academics," Heninger wrote in an email. "The takeaways for practitioners are basically that we hope they have followed advice to move to at least 2048-bit RSA, Diffie-Hellman, or DSA keys as of several years ago, which would keep them safe from any of these improvements."

29.12.2019 / L'Est Républicain

NANCY Recherche

Creativ'Lab : la recherche au service des entreprises

Plate-forme « robotique, intelligence artificielle et impression 3D » des laboratoires Loria et Inria de l'Université de Lorraine, le Creativ'Lab a été inauguré mi-décembre. Un espace d'expérimentation et de conception ouvert aux collaborations avec les entreprises.

De la taille d'un adulte, un robot humanoïde de toute dernière génération vient de faire son entrée à l'espace « arène robotique » du Creativ'Lab, inaugurée mi-décembre à Villers-lès-Nancy (54), une plate-forme « robotique, intelligence artificielle et impression 3D » commune à deux laboratoires de l'Université de Lorraine, le Loria et l'Inria. Ce robot humanoïde, un prototype dont il n'existe que cinq exemplaires dans le monde, ouvre de nouvelles perspectives aux chercheurs qui imaginent ses applications : il pourrait atteindre par exemple des endroits contaminés ou lointains, autrement dit dangereux ou inaccessibles à l'Homme.

Repousser les limites de la 3D

Outre cette « arène robotique », le Creativ'Lab se compose d'autres espaces : un espace dédié aux bras robotisés où sont développés des projets collaboratifs avec des industriels sur des problématiques d'amélioration des conditions de travail, un autre où les chercheurs travaillent à repousser les limites de l'impression 3 D en « courbant » les couches par exemple, ou encore un espace prototypage.

La recherche sur les drones

A quelques pas, une volière dédiée à la recherche sur les drones. Là sont menées des collaborations avec de grosses entreprises sur des thématiques de surveillance environnementale en milieu aquatique ou encore de surveillance de lignes électriques aériennes. La start-up Alerion, issue de la recherche lorraine, qui développe des solutions intelligentes par et pour les drones témoignait lors de cette inauguration : « Le Creativ'Lab est un espace de rencontres, d'émulation entre chercheurs. L'accès à la volière est pour nous important, pour effectuer les premiers tests de réglage, pour l'utilisation des imprimantes 3D ».

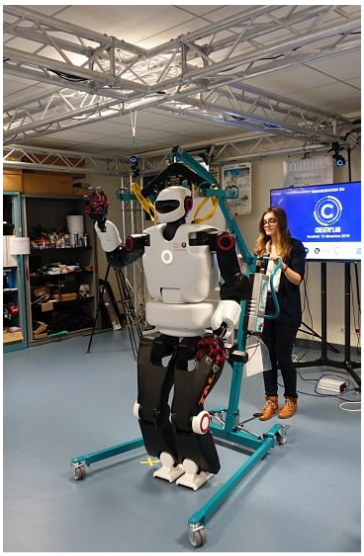
Une zone de bras robotiques est ouverte aux scientifiques et aux industriels pour améliorer les conditions de travail sur des lignes de production par exemple. Photo ER

Le Creativ'Lab fait partie de Robotex, un réseau national de plates-formes expérimentales de robotique dont l'objet est notamment de « favoriser les synergies » entre les équipes travaillant dans le domaine au niveau national et « d'accroître la compétitivité » des entreprises.

Marie-Hélène VERNIER

Robotique et IA : le Loria inaugure le Creativ'Lab à Nancy pour "partager les expertises" et "attirer les jeunes talents"

Le **Loria** (laboratoire commun CNRS, **Inria** et université de Lorraine) a inauguré officiellement le "Creativ'Lab", une nouvelle plate-forme dédiée à la robotique, à l'intelligence artificielle et aux systèmes cyberphysiques, le 13 décembre 2019. Pour la direction du laboratoire et ses tutelles, ces nouveaux espaces de recherche fondamentale et appliquée visent à impliquer les chercheurs, les étudiants et les entreprises, en croisant les expertises.



L'équipe Larsen (commune Inria/Loria) développe des méthodes pour doter les robots de compétences d'interaction. Ici, le nouveau robot Talos. | AEF - P. Marion

Un espace drones avec volière, une salle dédiée à l'impression 3D, un espace de prototypage, etc. : les nouvelles salles d'expérimentation du laboratoire Loria (dites "Creativ'Lab") ont ouvert grand leurs portes, le 13 décembre 2019, pour leur inauguration officielle. "C'est un moment que nous attendions depuis longtemps", souligne Jean-Yves Marion, directeur du laboratoire depuis 2013. "L'idée de construire cette plate-forme m'a été soufflée par l'ancienne directrice Françoise Simonot. Nous pouvons y faire de la recherche sur la robotique, avec en particulier le nouveau robot Talos, financé par le **CPER** et qui est le 5e vendu. Nous faisons aussi des travaux sur les systèmes cyberphysiques [drones], sur la fabrication additive, mais aussi sur la biorobotique, avec une cage pour suivre le vol des papillons."

"AVOIR LES YEUX QUI BRILLENT"

Dans "ce laboratoire tourné vers la société", "je voulais une plate-forme qui soit au carrefour entre la partie formation-enseignement, la recherche, la valorisation, le transfert, les entreprises", explique Jean-Yves Marion.

"Voir des robots, avoir les yeux qui brillent" participe de "l'effort" à accomplir "pour attirer les jeunes talents", souligne le directeur. "Pour deux raisons, au moins : les former aux nouvelles méthodes, et aussi les former à la recherche, pour qu'éventuellement ils fassent de la recherche en entreprise privée ou dans le service public, pour qu'ils fassent des thèses."

En outre, cet espace a aussi été conçu comme "un lieu ouvert, de façon à travailler dans de bonnes conditions avec les entreprises". "Nous sommes capables de travailler avec elles de différentes façons : thèses **Cifre**, contrats de prestation, ingénieurs partagés, codéveloppement de logiciels, etc. (1)".

IA : "ALIGNEMENT DES ÉTOILES"

Cette nouvelle implantation coïncide aussi avec "l'explosion de l'**IA**", avec la présence au sein du Loria "d'experts en deep learning, en modèles prédictifs, en apprentissage automatique, etc..", ajoute Jean-Yves Marion, se réjouissant de l'obtention récente de "trois chaires en IA" en région Grand Est (2).

À cet égard, le directeur d'Inria Nancy-Grand Est Bruno Lévy constate aujourd'hui "un alignement des étoiles, au niveau des acteurs de l'**ESR**, au niveau de nos partenaires du monde politique", "mûs par une ambition commune, celle de répondre à des grandes questions sociétales, environnementales". L'enjeu est de "dépasser les frontières des différents organismes, des différents acteurs", à travers la politique de site autour de l'université de Lorraine, puis "en élargissant le cercle, au niveau de la région Grand Est avec le lancement d'un plan IA (lire sur AEF info), et au niveau transfrontalier, avec l'Allemagne notamment, sur des sujets comme l'intelligence artificielle et la cybersécurité".

UN ESPACE DE COOPÉRATION TRÈS OUVERT

Pour le président de l'université de Lorraine, Pierre Mutzenhardt, "c'est forcément un très beau jour que de voir la création d'une nouvelle plate-forme, mais aussi de la voir dans le domaine du numérique et sous une forme particulière". "Là ou un Fablab est quelque chose de très ouvert au grand public, nous avons avec ce Creativ'Lab [...] un espace de coopération très ouvert à l'ensemble des chercheurs du site, à l'ensemble des doctorants du site". Le président de l'UL y voit aussi "un objet d'interface" avec le monde économique : "sur l'impression 3D, lorsque nous voyons les développements actuels à l'**IJL** [matériaux], il y a ici un formidable espace pour que les chercheurs et les entreprises se retrouvent".

Le Loria (400 personnes au total, (3)) est "un laboratoire phare du monde de l'informatique et de ses applications aux sciences et technologies de l'information, il suffit de mentionner les 10 **ERC** obtenues par ses membres", rappelle Thierry Siméon, chargé de mission robotique à l'**INS2I** (CNRS). "Sa force vient aussi de sa capacité à rassembler des compétences multiples et complémentaires, que ce soit dans l'IA, la robotique, les neurosciences, pour traiter les grands enjeux scientifiques".

Thierry Siméon précise que les travaux du Loria sont "en forte résonance avec les priorités thématiques définies dans le contrat d'objectifs du CNRS, dans le domaine des sciences du numérique : le futur du calcul, les recherches en cybersécurité, les défis des systèmes autonomes et interactifs, etc.". En particulier, "le Loria s'est donné les moyens de faire de la robotique une thématique forte, étant aujourd'hui reconnu comme l'un des principaux acteurs de la recherche française dans ce domaine", dit-il, évoquant l'organisation de conférences nationales et internationales, et l'intégration du Creativ'Lab dans le réseau de plateformes expérimentales Robotex (financé dans le cadre du **PIA**).

"UN ESPACE DE RENCONTRES" INGÉNIEURS-CHERCHEURS

Au sein du Creativ'Lab, les différents activités de recherche (robotique, internet des objets, médecine numérique, etc.) voisinent aisément : "c'est un lieu où l'on fédère les équipes, où l'on partage les expertises", souligne Jean-Yves Marion. "Il y a une porosité thématique très intéressante", confirme Sylvain Lefebvre, directeur de recherche Inria, qui dirige l'équipe MFX (en informatique graphique et fabrication additive). "Juste à côté, se trouvent les autres disciplines spécialisées dans la conception de robots et de drones. Nous, nous fabriquons des pièces en impression 3D, et eux les utilisent pour leurs travaux".

Cet espace, mis en service en début d'année, vise à "stimuler les échanges avec les entreprises, en faisant émerger des partenariats entre chercheurs, étudiants et entreprises", ajoute-t-on au Loria. Preuve en a été donnée, à travers la collaboration avec la start-up Alerion (drones et IA embarquée). Par exemple, "dans le cadre d'un projet financé par la région, nous avons imaginé pour 'Pedon Environnement' un hydradrone au sein du Loria, puis au sein d'Alerion", retrace Anne-Sophie Didelot, sa dirigeante. L'ex-doctorante de l'UL a cofondé cette société en 2015 avec un enseignant-chercheur du Loria, et a travaillé pour plusieurs industries depuis (Thales, Enedis, etc.). "Le Creativ'Lab constitue un espace de rencontres pour mes ingénieurs : le fait de pouvoir discuter avec d'autres scientifiques crée une émulation".

Le coût total des travaux d'infrastructure s'est élevé à plus de 300 K€, dont près de 220 K€ sur les ressources propres du Loria et plus de 85 K€ du Feder. S'y est ajoutée la contribution du CPER pour du matériel.

(1) Le Loria réalisant environ 5 millions d'euros de contrats par an.

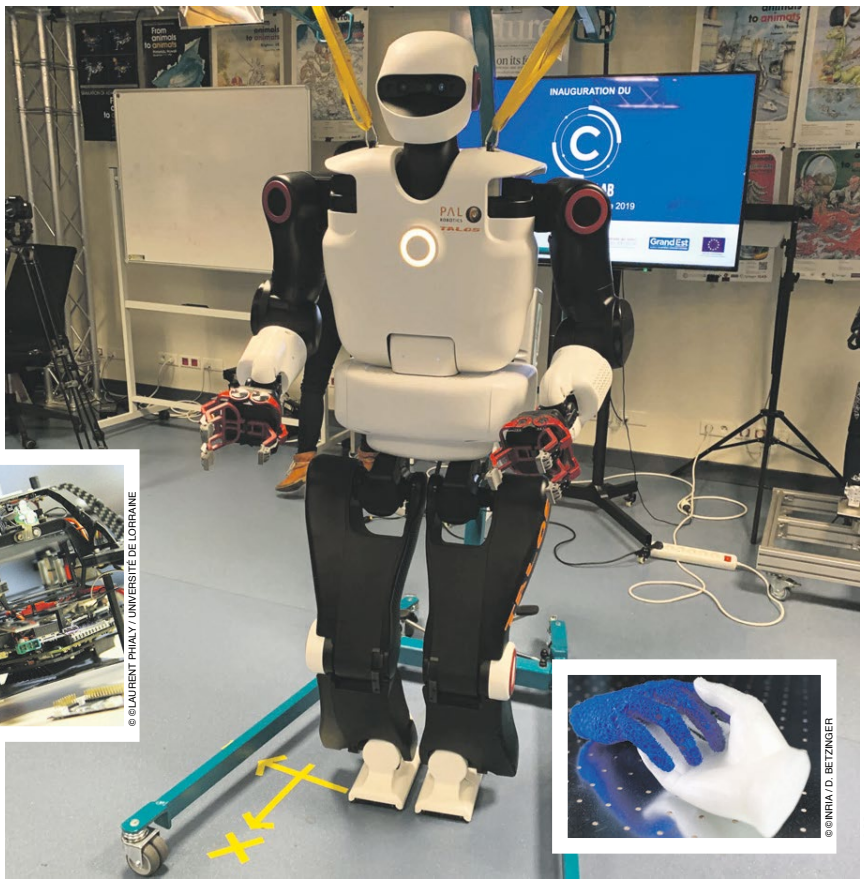
(2) Dont deux, côté Loria : Steve Kremer (directeur de recherche Inria) et Claire Gardent (directrice de recherche CNRS). Les 40 projets de "chaires de recherche et d'enseignement IA" sélectionnés ont été dévoilés ce vendredi (lire sur AEF info).

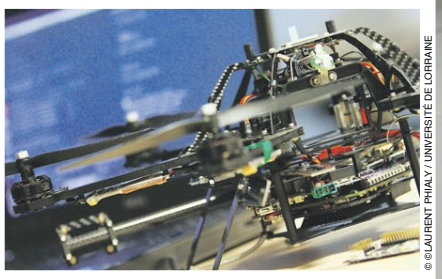
(3) Au sein de 28 équipes, dont 15 communes avec Inria.

Villers-lès-Nancy / INNOVATION

La science des possibles

Développer à la fois une recherche fondamentale et appliquée, répondre aux besoins des entreprises tout en soutenant les **PROJETS DE RECHERCHES DES ÉTUDIANTS**. Voilà pour les missions du Creativ'Lab, plateforme du laboratoire Loria. Imprimantes 3D exceptionnelles, robotique humanoïde et bien d'autres surprises. Immersion.





© ©LAURENT PHILALY / UNIVERSITÉ DE LORRAINE

© ©INRIA / D. BETZINGER

© DR

Pénétrer dans les méandres de la recherche d'un laboratoire, c'est accéder en quelque sorte aux solutions sociétales de demain. Le tout en avant-première bien évidemment. C'est le cas au Creativ-Lab, cette plateforme du laboratoire Loria dédiée à la robotique, à l'intelligence artificielle et aux systèmes cyberphysiques. En partenariat avec l'Inria, le CNRS de Villers-lès-Nancy et l'Université de Lorraine, les équipes s'affairent dans ces nombreux domaines. Parce qu'ils touchent directement aux enjeux sociétaux de demain. Mais aussi parce que les entreprises peuvent s'appuyer sur les compétences de cette plateforme pour faire fructifier leurs projets.

Cet espace d'expérimentation et de conception qu'est le Creativ'Lab vise à faire émerger des partenariats entre chercheurs, étudiants et entreprises. Pour que l'ouverture rime aussi bien avec idée fondatrice que fondations des processus créateurs. A l'image d'Alerion, une startup née des travaux de recherche issus du laboratoire. *« Le gros intérêt pour nous est d'avoir plus facilement accès au chercheur avec qui nous collaborons. Et son équipe pour pouvoir échanger sur nos projets de recherche et discuter des développements. La présence au sein du Creativ'Lab du matériel mais aussi de moyens humains nous permettent d'avancer sur les sujets plus techniques. Le Creativ'Lab nous offre une sorte d'émulation scientifique »*, souligne Anne-Sophie Didelot, présidente de la start-up Alerion.

Panorama des espaces de recherches qui inventent les solutions de demain.

Robotique et environnements intelligents

L'équipe Larsen, commune à Inria et au Loria, développe des méthodes pour doter les robots d'une autonomie à long terme et de compétences d'interaction, en tenant compte des capteurs intégrés ou externes. Ces compétences reposent sur l'interaction physique et sociale, l'apprentissage automatique et la planification tout en prenant en compte les incertitudes. Les expériences, notamment en robotique de service et d'assistance, sont au cœur de la méthodologie de l'équipe. Les techniques développées auront potentiellement un impact sur tous les domaines de la robotique et catalyseront les efforts en cours pour insérer les robots dans la société. Les robots sont déjà dans les usines de production. Pour étendre la robotique en dehors de cette industrie et de ces laboratoires de recherche, il est nécessaire de développer l'autonomie et les compétences d'interaction des robots.

La saisie d'objets à l'aide d'un bras robotique fait aussi partie des travaux étudiés. Dans une pile non organisée, il est compliqué pour la machine de déterminer de quelle manière saisir l'objet visé. Afin d'éviter la casse, le robot avec une caméra intégrée et aidée par un logiciel de reconnaissance, détermine des processus de saisies. Et développe des préférences et reconnaissances de tailles, formes, aspects, etc. Cette application est fortement utile dans le domaine de la robotique nucléaire par exemple.

Au sein de la plateforme, un robot de la taille d'un enfant permet aussi d'étudier les systèmes d'apprentissage. Marcher, échanger avec d'autres, analyser l'environnement avec des capteurs d'efforts, de vision, entre autres.

Un autre robot, de la taille d'un humain cette fois, se déplace. Dénommé Talos, cet avatar humain vient apporter une aide et assistance dans des gestes dynamiques du quotidien. Porter un paquet, ouvrir des portes, marcher dans un couloir. Dans l'espace, lors de catastrophes naturelles ou encore pour manipuler des matières dangereuses. Ces innovations à plusieurs centaines de milliers d'euros sont d'ores et déjà utilisées dans de nombreux chantiers à dimension européenne.

Fabrication additive

L'équipe Matter From Graphics (MFX) se concentre, elle, sur les défis liés à la complexité des formes dans le contexte de l'informatique graphique et de la fabrication additive. L'équipe considère toute la chaîne numérique. De la modélisation 3D interactive au traitement de la géométrie des pièces pour leur visualisation et leur fabrication. Objectifs : changer la structure en lui donnant davantage de flexibilité et aider les concepteurs à créer des géométries complexes répondant à des exigences strictes de fabrication, géométriques et fonctionnelles. La forme générale est toujours pensée par le designer mais la structure est faite par un algorithme. Les recherches de l'équipe sont notamment intégrées dans le logiciel IceSL développé au sein de la plateforme. Pour des rendus avec une précision immense et des couches de matière presque invisibles à l'œil nu. Et comme ce logiciel peut être relié à des imprimantes 3D grand public, il est disponible en accès libre pour tous les chercheurs et les passionnés du sujet.

Systèmes cyberphysiques intelligents et Internet des objets

Ce sont des termes dont on ne saisit pas toujours le sens. Mais quand ils sont décortiqués par des professionnels, cela est toujours mieux. Un système cyberphysique doit posséder une grande capacité d'adaptation ainsi qu'une puissance de calcul et de communication appropriée à son échelle. Ils sont généralement composés de nombreuses entités hétérogènes, mais connectées et interdépendantes. Les scientifiques doivent donc pouvoir simuler et valider expérimentalement des systèmes efficaces en fonction de modèles réels. Les architectures réseau doivent également pouvoir gérer les interactions en temps réel entre les entités. L'équipe Simbiot (SIMulating and Building IOT) du Loria étudie et conçoit de tels systèmes cyberphysiques, notamment en testant et validant leur adaptabilité par co-simulation et expérimentation in-situ. Plusieurs projets de l'équipe concernent l'utilisation de drones. Notamment pour des missions de reconnaissance et d'inspection. Sur des terrains difficilement accessibles, des installations en mer ou encore des mesures environnementales. De grands groupes comme EDF ou Enedis ont fait appel aux services du laboratoire.

Neurosciences et médecine numérique

Les travaux de l'équipe NeuroRhythms visent une meilleure compréhension du fonctionnement et du dysfonctionnement du cerveau. Principalement en lien avec le mouvement et la mémoire. Pour identifier les liens entre le fonctionnement des neurones, des populations de neurones et le comportement, les chercheurs de l'équipe analysent des résultats expérimentaux (électroencéphalogrammes, par exemple). Ou créent des modèles de simulation informatique.

Le travail de l'équipe NeuroRhythms mène doit déboucher sur des applications médicales spécifiques, liées à l'anesthésie par exemple. Mais aussi sur le développement d'interfaces cerveau-ordinateur ou de nouveaux outils de neuro-robotique tels que des robots olfactifs.

Baptiste Zamaron

Grand Nancy. Immersion au Créativ'Lab, le laboratoire des possibles

ABONNÉS | Par Baptiste Zamaron sur 20 décembre 2019 Economie, Nancy et alentours

Exemple d'objets imprimés en 3D par l'équipe MFX avec le remplissage Polyfoam. La main bleue montre le remplissage présent dans la main blanche : grâce à ce remplissage orienté et à un filament flexible, les doigts de ces mains peuvent se plier. Photo Inria / D. Betzinger

Développer à la fois une recherche fondamentale et appliquée, répondre aux besoins des entreprises tout en soutenant les projets de recherches des étudiants. Voilà pour les missions du Creativ'Lab, plateforme du laboratoire Loria. Imprimantes 3D exceptionnelles, robotique humanoïde et bien d'autres surprises. Immersion.

Pénétrer dans les méandres de la recherche d'un laboratoire, c'est accéder en quelque sorte aux solutions sociétales de demain. Le tout en avant-première bien évidemment. C'est le cas au Creativ-Lab, cette plateforme du laboratoire Loria dédiée à la robotique, à l'intelligence artificielle et aux systèmes cyberphysiques. En partenariat avec l'Inria, le CNRS de Villers-lès-Nancy et l'Université de Lorraine, les équipes s'affairent dans ces nombreux domaines. Parce qu'ils touchent directement aux enjeux sociétaux de demain. Mais aussi parce que les entreprises peuvent s'appuyer sur les compétences de cette plateforme pour faire fructifier leurs projets.

Cet espace d'expérimentation et de conception qu'est le Creativ'Lab vise à faire émerger des partenariats entre chercheurs, étudiants et entreprises. Pour que l'ouverture rime aussi bien avec idée fondatrice que fondations des processus créateurs. A l'image d'Alerion, une startup née des travaux de recherche issus du laboratoire. *« Le gros intérêt pour nous est d'avoir plus facilement accès au chercheur avec qui nous collaborons. Et son équipe pour pouvoir échanger sur nos projets de recherche et discuter des développements. La présence au sein du Creativ'Lab du matériel mais aussi de moyens humains nous permettent d'avancer sur les sujets plus techniques. Le Creativ'Lab nous offre une sorte d'émulation scientifique »*, souligne Anne-Sophie Didelot, présidente de la start-up Alerion. Panorama des espaces de recherches qui inventent les solutions de demain.

Robotique et environnements intelligents

L'équipe Larsen, commune à Inria et au Loria, développe des méthodes pour doter les robots d'une autonomie à long terme et de compétences d'interaction, en tenant compte des capteurs intégrés ou externes. Ces compétences reposent sur l'interaction physique et sociale, l'apprentissage automatique et la planification tout en prenant en compte les incertitudes. Les expériences, notamment en robotique de service et d'assistance, sont au cœur de la méthodologie de l'équipe. Les techniques développées auront potentiellement un impact sur tous les domaines de la robotique et catalyseront les efforts en cours pour insérer les robots dans la société. Les robots sont déjà dans les usines de production. Pour étendre la robotique en dehors de cette industrie et de ces laboratoires de recherche, il est nécessaire de développer l'autonomie et les compétences d'interaction des robots.

La saisie d'objets à l'aide d'un bras robotique fait aussi partie des travaux étudiés. Dans une pile non organisée, il est compliqué pour la machine de déterminer de quelle manière saisir l'objet visé. Afin d'éviter la casse, le robot avec une caméra intégrée et aidée par un logiciel de reconnaissance, détermine des processus de saisies. Et développe des préférences et reconnaissances de tailles, formes, aspects, etc. Cette application est fortement utile dans le domaine de la robotique nucléaire par exemple.

Au sein de la plateforme, un robot de la taille d'un enfant permet aussi d'étudier les systèmes d'apprentissage. Marcher, échanger avec d'autres, analyser l'environnement avec des capteurs d'efforts, de vision, entre autres.

Un autre robot, de la taille d'un humain cette fois, se déplace. Dénommé Talos, cet avatar humain vient apporter une aide et assistance dans des gestes dynamiques du quotidien. Porter un paquet, ouvrir des portes, marcher dans un couloir. Dans l'espace, lors de catastrophes naturelles ou encore pour manipuler des matières dangereuses. Ces innovations à plusieurs centaines de milliers d'euros sont d'ores et déjà utilisées dans de nombreux chantiers à dimension européenne.

Fabrication additive

A Lire Aussi
Attractivité : Nancy fait le pari des startups

L'équipe Matter From Graphics (MFX) se concentre, elle, sur les défis liés à la complexité des formes dans le contexte de l'informatique graphique et de la fabrication additive. L'équipe considère toute la chaîne numérique. De la modélisation 3D interactive au traitement de la géométrie des pièces pour leur visualisation et leur fabrication. Objectifs : changer la structure en lui donnant davantage de flexibilité et aider les concepteurs à créer des géométries complexes répondant à des exigences strictes de fabrication, géométriques et fonctionnelles. La forme générale est toujours pensée par le designer mais la structure est faite par un algorithme. Les recherches de l'équipe sont notamment intégrées dans le logiciel IceSL développé au sein de la plateforme. Pour des rendus avec une précision immense et des couches de matière presque invisibles à l'œil nu. Et comme ce logiciel peut être relié à des imprimantes 3D grand public, il est disponible en accès libre pour tous les chercheurs et les passionnés du sujet.

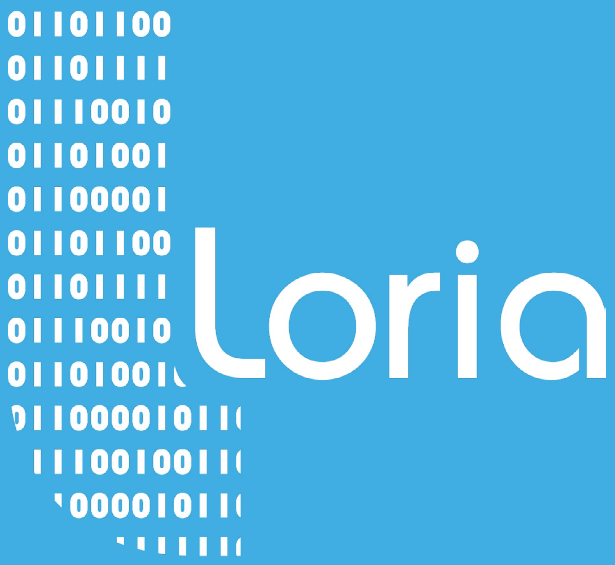
Systèmes cyberphysiques intelligents et Internet des objets

Ce sont des termes dont on ne saisit pas toujours le sens. Mais quand ils sont décortiqués par des professionnels, cela est toujours mieux. Un système cyberphysique doit posséder une grande capacité d'adaptation ainsi qu'une puissance de calcul et de communication appropriée à son échelle. Ils sont généralement composés de nombreuses entités hétérogènes, mais connectées et interdépendantes. Les scientifiques doivent donc pouvoir simuler et valider expérimentalement des systèmes efficaces en fonction de modèles réels. Les architectures réseau doivent également pouvoir gérer les interactions en temps réel entre les entités. L'équipe Simbiot (SIMulating and Building IOT) du Loria étudie et conçoit de tels systèmes cyberphysiques, notamment en testant et validant leur adaptabilité par co-simulation et expérimentation in-situ. Plusieurs projets de l'équipe concernent l'utilisation de drones. Notamment pour des missions de reconnaissance et d'inspection. Sur des terrains difficilement accessibles, des installations en mer ou encore des mesures environnementales. De grands groupes comme EDF ou Enedis ont fait appel aux services du laboratoire.

Neurosciences et médecine numérique

Les travaux de l'équipe NeuroRhythms visent une meilleure compréhension du fonctionnement et du dysfonctionnement du cerveau. Principalement en lien avec le mouvement et la mémoire. Pour identifier les liens entre le fonctionnement des neurones, des populations de neurones et le comportement, les chercheurs de l'équipe analysent des résultats expérimentaux (électroencéphalogrammes, par exemple). Ou créent des modèles de simulation informatique.

Le travail de l'équipe NeuroRhythms mène doit déboucher sur des applications médicales spécifiques, liées à l'anesthésie par exemple. Mais aussi sur le développement d'interfaces cerveau-ordinateur ou de nouveaux outils de neuro-robotique tels que des robots olfactifs.



CONCEPTION SERVICE COMMUNICATION DU LORIA