LES JEUDIS DE LA RECHERCHE DE L'X

12 JANVIER 2017

DÉFI SÉCURITAIRE

Renforcer la confiance dans les technologies numériques

ÉCOLE
POLYTECHNIQUE
UNIVERSITÉ PARIS-SACLAY

LA RECHERCHE À L'X

Frank Pacard, directeur de l'enseignement et de la recherche

L'École polytechnique s'appuie sur un Centre de recherche de pointe qui rassemble 22 laboratoires, dont 21 unités mixtes de recherche avec le CNRS.

Un Centre de recherche dynamique et reconnu

Regroupant 1600 personnels de recherche, le Centre de recherche de l'X allie l'approfondissement des aspects les plus fondamentaux de la recherche pour le progrès des connaissances au développement de grands domaines plus appliqués qui répondront aux enjeux scientifiques, technologiques et sociétaux du 21e siècle.

Une stratégie de recherche organisée autour de 8 thématiques

L'École polytechnique a défini 8 thématiques dans sa stratégie de recherche. Ces thématiques de recherche répondent à des enjeux sociétaux et technologiques par le biais de projets transverses et multidisciplinaires, auxquels sont associés les laboratoires de l'École :

- Bio-ingénierie, biologie et santé
- Concepts et méthodes pour la société numérique
- Énergies, transports et environnement
- Modélisation et optimisation des systèmes complexes
- Marchés, innovation et relations science et société
- Matière et lumière en conditions extrêmes
- Nanosciences, matériaux innovants et procédés efficaces
- Structures et lois universelles

Les défis pour la société de demain : cette année, les « Jeudis de la Recherche » exploreront quatre grands défis sociétaux : les défis climatiques, sécuritaires, économiques et sanitaires.

Après le défi climatique exposé en octobre 2016, le défi sécuritaire est abordé aujourd'hui sous l'angle du numérique, suivant la thématique :

« Défi sécuritaire : renforcer la confiance dans les technologies numériques ».

La cryptographie est utilisée depuis l'Antiquité pour protéger des messages et a été démocratisée au siècle dernier avec l'apparition de l'informatique. Aujourd'hui, que ce soit par l'arrivée de nouvelles technologies, la modernisation de nos quotidiens, la création d'Internet et de l'Internet des objets, la cryptographie devient omniprésente. Et elle est appelée à jouer un rôle encore plus important dans un futur proche, non seulement dans les nouvelles technologies, mais aussi dans la vie privée et publique. En effet, le vote électronique, les télécommunications ou encore le paiement électronique (et notamment les monnaies telles que le bitcoin) sont amenés à se développer de façon importante, et les moyens cryptographiques devront suivre cette évolution. Il est donc d'une importance capitale de construire des systèmes cryptographiques apportant de fortes garanties, importance reconnue par les grands groupes de télécommunications qui sont de plus en plus demandeurs de tels systèmes.

Le Laboratoire d'Informatique de l'X (LIX) est un laboratoire en cotutelle entre l'École polytechnique et le CNRS, en collaboration avec Inria. Les chercheurs de ce laboratoire sont tout particulièrement impliqués dans le développement de la sécurité informatique et dans la cryptologie, la science qui conçoit et analyse les systèmes cryptographiques. Ils mettent ainsi à profit leurs compétences en associant mathématiques, informatique et ingénierie qui font partie des spécialités du Centre de recherche de l'École polytechnique.

Les exposés de Benjamin Smith, Pierre-Yves Strub et Ulrich Fahrenberg vous permettront de découvrir différents outils et méthodes qui sont actuellement développés par les chercheurs du LIX pour nous permettre de communiquer librement, tout en garantissant une sécurisation optimale.

Nous espérons que ce nouveau « Jeudi de la recherche de l'X » vous permettra de renforcer votre confiance dans les technologies du numérique de demain grâce aux scientifiques de notre Centre de recherche, véritable moteur de l'École polytechnique.

Frank Pacard,
Directeur de l'enseignement et de la recherche

Benjamin Smith

Après une thèse en mathématiques pures à l'Université de Sydney en 2005, Benjamin Smith s'est intéressé à la recherche en cryptologie lors d'un post-doctorat à la Royal Holloway (Université de Londres) en 2006-2007. Il rejoint Inria en 2007 et intègre alors le LIX. Depuis 2009, il est également chargé d'enseignement au département d'informatique de l'École polytechnique.

Ses recherches portent sur le chiffrement asymétrique utilisé pour établir des communications sécurisées et authentifier des entités en ligne (matériels, individuels, entreprises). Benjamin Smith s'intéresse plus particulièrement aux systèmes de chiffrement basés sur des courbes elliptiques et leur généralisation. Ses recherches font appel à la théorie algorithmique des nombres et à la géométrie algébrique dans le double objectif d'améliorer les algorithmes de chiffrement asymétrique et d'en analyser la sécurité.

La cryptologie pour sécuriser les communications dans un monde connecté

Benjamin Smith

Le 21 octobre 2016, plusieurs grands sites internet tels que Amazon, Twitter, Paypal ou encore Spotify ont disparu pendant quelques heures des accès internet. Cette disparition a été causée par une attaque sur un fournisseur majeur de l'infrastructure sous-terraine d'Internet, Dyn, qui permet d'accéder aux différents sites du web.

L'originalité de cette attaque, c'est d'avoir été déclenchée par l'intervention massive d'objets connectés : des webcams, des caméras de surveillance, mais aussi des objets du quotidien tels que des grille-pains se sont connectés tous en même temps à Dyn et ont saturé son accès. Cela pose la question de la sécurisation d'objets de plus en plus nombreux et diversifiés, qui n'ont pas forcement la capacité d'intégrer des systèmes complexes de sécurisation.

Comment sécuriser ces objets ? La science qui étudie ces problèmes, la cryptologie, cherche à assurer des communications authentifiées, fiables, et sûres, ne permettant pas à une unité malveillante, un « adversaire », d'interférer dans l'accès aux données, aux comptes informatiques et aux ressources physiques des machines piratées.

Les chercheurs en cryptologie de l'équipe de Benjamin Smith au LIX travaillent sur de nouvelles méthodes de sécurisation des communications. Pour ce faire, les deux parties communicantes ont besoin de partager un code secret, une « clé » permettant de chiffrer et de déchiffrer les informations échangées. Mais comment se mettre d'accord sur cette clé sans avoir établi une communication sécurisée auparavant, ce qui est loin d'être le cas avec Internet ? La méthode consiste à cacher les clés secrètes dans la solution de problèmes mathématiques très difficiles : les énoncés de ces problèmes peuvent alors être transmis ouvertement, et la sécurité de la communication repose alors sur la difficulté à les résoudre par un adversaire extérieur.

L'objectif de ces problèmes est donc d'être faciles à construire et à vérifier, compacts à énoncer pour être intégrés aux objets, et pratiquement impossibles à résoudre. Depuis les années 1970, des problèmes d'arithmétique étaient utilisés pour assurer la sécurité, mais aujourd'hui, la cryptologie se base sur de nouveaux types de problèmes pour lesquels le LIX possède une grande expertise. Ces nouveaux énoncés mathématiques utilisent des courbes elliptiques dont les points ont une algèbre propre, donnant ainsi des problèmes très concis mais extrêmement difficiles à résoudre.

Le travail de Benjamin Smith consiste à anticiper et à étudier des problèmes qui seront utilisés demain pour chiffrer les communications, par exemple en passant de l'utilisation de courbes à l'utilisation de surfaces (voir illustration) permettant de créer des crypto-systèmes très efficaces avec des clés cryptographiques compactes et sécurisées.

Pierre-Yves Strub

Pierre-Yves Strub a soutenu sa thèse en informatique à l'École polytechnique en 2008. Après un post-doctorat au sein du Centre de Recherche commun Microsolft-Inria (Microsoft Research-Inria Joint Centre) à Paris, et au LIAMA institute à Pékin, il a poursuivi sa carrière de recherche en intégrant le IMDEA Software Institute à Madrid en 2013. Depuis septembre 2016, il a rejoint le LIX en tant que Maître de conférences.

Ses recherches portent sur les preuves formelles, les assistants à la démonstration, la théorie des types qui leur est rattachée, mais aussi la certification d'algorithmes cryptologiques, la vérification de programmes et la programmation web sécurisée.

La logique pour vérifier les algorithmes de sécurité de manière autonome et sûre

Pierre-Yves Strub

Au cours des dernières décennies, le domaine de la cryptographie a considérablement évolué. Dans les premiers temps, il s'agissait de définir des « primitives » cryptographiques : des algorithmes de base utilisés pour chiffrer un message ou authentifier son émetteur. Aujourd'hui, elle fait appel à la conception de nouveaux types de protocoles par exemple dits « à divulgation nulle de connaissance ».

C'est dans cette optique que la cryptographie moderne s'attache à produire de nouvelles primitives, apportant des fonctionnalités de plus en plus complexes. Cette complexification des algorithmes rend la preuve de leur sécurité plus longue à démontrer et susceptible de contenir des erreurs de raisonnement difficilement décelables.

La vérification des protocoles de chiffrement est d'autant plus délicate qu'il existe une fragmentation de la communauté cryptographique, entre, d'un côté, les théoriciens définissant des primitives cryptographiques et d'un autre, les praticiens qui les intègrent à des systèmes utilisables. Ainsi, certaines des utilisations de primitives cryptographiques les plus répandues ont présenté, à plusieurs reprises, des faiblesses de sécurité. Ces failles peuvent provenir de plusieurs sources différentes, que ce soit des erreurs de programmation, des attaques par canaux cachés, des erreurs logiques, voire des portes dérobées volontairement introduites dans les standards.

Ces différents problèmes ont été clairement identifiés par la communauté cryptographique qui a préconisé, en 2005, l'utilisation de méthodes formelles couplées à la vérification assistée par ordinateur déjà utilisée dans de nombreux domaines (conception de matériel, systèmes embarqués, systèmes d'exploitation, compilateurs).

Les recherches de Pierre-Yves Strub au sein du LIX se focalisent essentiellement sur la conception et l'implémentation de ces outils formels d'aide à la construction et la vérification de preuves de sécurité. Ces outils reposent sur la longue littérature qui existe en conception des langages de programmation et de vérification assistée par ordinateur. Le but à long terme est de fournir les méthodologies nécessaires pour la production certifiée de standards cryptographiques présentant des garanties de sécurités fortes dans des modèles d'attaques malveillantes concrètes.

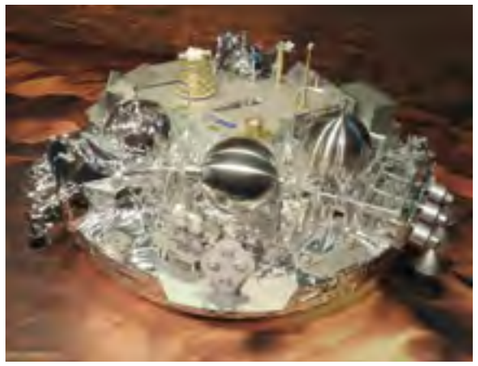
Ulrich Fahrenberg

Ulrich Fahrenberg a soutenu une thèse en mathématiques à l'Université Aalborg au Danemark en 2005, où il a ensuite débuté sa carrière en tant que professeur assistant en informatique. Après un post-doctorat qu'il a effectué à Inria Rennes, il intégre le LIX en 2016 en tant que chercheur.

Ulrich Fahrenberg a travaillé sur la topologie algébrique, la théorie de la concurrence, la vérification temps réel, et la vérification quantitative. Il a ainsi publié plus de 60 articles en informatique et en mathématiques. Membre de nombreux comités de programmation de conférences, il fait partie depuis 2016 des relecteurs pour les publications de l'American Mathematical Society (AMS Mathematical reviews).

La vérification formelle pour assurer la sureté des systèmes embarqués

Ulrich Fahrenberg



Le 19 octobre 2016, Schiaparelli, un engin spatial conçu par l'Agence Spatiale Européenne (ESA) en partenariat avec le Roscosmos russe, a commencé sa descente vers la planète Mars. Cinquante secondes avant l'atterrissage prévu, tout contact avec l'atterrisseur a été perdu, et deux jours plus tard, l'ESA a confirmé que Schiaparelli s'était écrasé.

L'enquête sur l'accident suit encore son court, mais il semble qu'il ait été causé par une défaillance du système de guidage, de navigation et de contrôle automatique. Une mesure défectueuse aurait amené le logiciel à conclure que l'atterrisseur était à une altitude négative, alors que Schiaparelli était encore 3,7 kilomètres au-dessus du niveau du sol de Mars. Le parachute a été largué, les propulseurs ont été arrêtés, faisant ainsi chuter l'engin qui s'est écrasé sur la surface martienne.

Schiaparelli est un exemple d'un système cyber-physique : un système informatique qui s'interface avec son environnement physique et le contrôle. On peut citer de nombreux exemples de systèmes cyber-physique comme les systèmes modernes de contrôle de climatisation, les centrales électriques, les pilotes automatiques d'avion, les réseaux électriques «intelligents», ou encore les véhicules autonomes.

Il est difficile d'assurer le bon fonctionnement des systèmes cyber-physiques, pour éviter les incidents comme le crash de Schiaparelli. Il est possible de vérifier les bugs de logiciel, mais en raison des interactions entre l'unité de calcul et l'environnement extérieur, ce n'est généralement pas suffisant.

Une approche couramment utilisée consiste à construire un modèle mathématique du système et de son environnement. Le modèle mathématique peut alors être simulé afin d'estimer s'il fonctionne correctement. Mais, si les outils de simulation permettent d'explorer une grande quantité de scénarios possibles, l'interaction des systèmes avec l'extérieur ne permet pas forcement d'assurer que tout a été simulé. Pour éviter les lacunes potentielles de la simulation, une autre méthode consiste à utiliser une vérification formelle : des algorithmes avancés permettant de s'assurer que tous les scénarios sont pris en compte et que le modèle se comporte comme prévu.

La vérification formelle est une technique qui a connu un développement rapide au cours des 30 dernières années et qui est maintenant couramment utilisée dans l'industrie même si elle est très coûteuse en termes de calcul. Ulrich Fahrenberg travaille au sein de l'équipe de recherche d'Éric Goubault au LIX pour trouver des méthodes de vérification formelle permettant d'abaisser le temps et la mémoire nécessaires pour assurer la sécurité de ces systèmes.

Contacts

Cécile Mathey
01 69 33 38 70 - 06 30 12 42 41
cecile.mathey@polytechnique.edu

Chloé Aubisse-Daniault
01 69 33 33 40 - 06 76 43 99 97
chloe.aubisse@polytechnique.edu

ÉCOLE POLYTECHNIQUE
91128 PALAISEAU CEDEX
www.polytechnique.edu