Comment construire l'obfuscation indistinguable à l'aide d'un chiffrement homomorphe

Pour construire l'obfuscation indistinguable, on commence par inverser le rôle du programme P et du message m. Le programme P est chiffré, et on évalue de manière homomorphique une entrée m pour obtenir un chiffré de la valeur de sortie P(m). Comment alors récupérer la valeur de P(m) ? En principe, il faudrait avoir une clé secrète capable d'ouvrir tous les chiffrés. Toutefois, l'obfuscation d'un programme ne peut pas contenir cette clé, sans quoi le programme deviendrait complètement lisible. Autrement dit, il faut disposer d'un mécanisme permettant de révéler la valeur de sortie P(m) sans révéler entièrement le programme P. Un tel mécanisme comprend des clés de chiffrement restreintes, chacune d'elles est associée au message m et permet de déchiffrer uniquement le Chiffré(P(m)). Cela révèle la sortie P(m) mais aucune autre information sur le programme P. En résumé, l'obfuscation d'un programme P contient le chiffré homomorphique de P ainsi que les clés restreintes pour tous les messages m possibles. Pour que le programme obfusqué reste de taille raisonnable, il faut donner ces clés sous une forme compressée, c'est-à-dire compacte, dont la taille est plus petite que le nombre total de messages possibles. Réaliser cette compression est le défi technique majeur auquel font face les récentes constructions d'obfuscation. R. G.

concret. Car, quelles que soient les constructions d'obfuscation, elles sont inefficaces, les temps de calcul impliqués étant trop longs. Pour autant, nul doute que ces avancées vont aiguillonner les recherches, car les applications potentielles sont innombrables (lire l'encadré p. 108). Nous sommes en quelque sorte au stade où se trouvait le chiffrement homomorphe il y a une dizaine d'années : il s'agissait d'une très belle réalisation théorique, mais impraticable. Aujourd'hui, des entreprises commencent à proposer du chiffrement homomorphe pour diverses applications.

Toutefois, l'obfuscation iO est tellement universelle qu'il paraît improbable de bâtir toutes les primitives cryptographiques efficacement avec elle. Même si elle devient efficace – et on en est très loin –, elle ne constituera sans doute pas le moyen le plus pratique de construire des primitives classiques simples, comme le chiffrement à clé publique. Ce type d'obfuscation est plutôt comme une baguette magique : si l'on veut savoir si une nouvelle primitive imaginée dans un cerveau créatif d'informaticien fonctionne, on se demandera si on peut la construire avec l'iO ; et si la réponse est oui, on saura que c'est possible. Des constructions plus directes et plus efficaces viendront sûrement ensuite. Dans cet univers foisonnant de la recherche en informatique, il est toujours rassurant de savoir que ce sur quoi on travaille aboutira. En somme, l'obfuscation indistinguable permet d'unifier le vaste domaine de la cryptographie, et même d'en repousser les frontières. ■

(1) B. Barak *et al.*, *in Advances in Cryptology - Crypto 2001*, Springer Verlag, 2139, 1, 2001.

(2) C. Gentry, *STOC'09 : Proceedings of the Forty-First Annual ACM Symposium on Theory of Computing*, 169, 2009.

(3) E. Klarreich, « Computer Scientists Achieve "Crown Jewel" of Cryptography », *Quanta Magazine*, 10 novembre 2020.

(4) A. Jain *et al.*, *STOC 2021*, doi:10.1145/3406325.3451093, 2021.

(5) Ph. Pajot, « Cinq pistes pour la cryptographie du futur », *La Recherche*, *541*, novembre 2018.

(6) Z. Brakerski *et al.*, *in Advances in Cryptology - Eurocrypt 2020*, Springer Verlag, 79, 2020.

(7) R. Gay et R. Pass, *STOC 2021*, doi :10.1145/3406325.3451070, 2021 ; H. Wee et D. Wichs, *in Advances in Cryptology - Eurocrypt 2021*, Springer Verlag, 127, 2021 ; Z. Brakerski *et al.*, ia.cr/2020/1024, 2021.

Édito

De fortes ambitions et des moyens pour développer l'innovation, la recherche et l'enseignement supérieur en Région Grand-Est

La Stratégie régionale enseignement supérieur, recherche, innovation 2020-2030 (SRESRI) fixe de grandes ambitions à la Région pour transformer son économie.

Ainsi, la Région s'est fixé comme ambitions à l'horizon 2030 de doubler son faible taux de Dépense Intérieure de Recherche et Développement des Entreprises (DIRDE) régionale, pour atteindre 1,5 % du PIB. La deuxième région industrielle de France a choisi d'orienter ses financements à 80 % vers les enjeux liés aux transitions environnementale, industrielle et numérique ainsi que vers le transfert technologique. La Région conduira la mobilisation de 1,4 milliard d'euros en dix ans de fonds publics régionaux, nationaux et européens, pour un investissement global sur le territoire en faveur de l'enseignement supérieur, de la recherche et de l'innovation.

Dans un contexte de baisse tendancielle de la population jeune, l'enseignement supérieur est au cœur des ambitions. La Région veut accroître de 50 % la proportion des jeunes atteignant un diplôme de l'enseignement supérieur afin que 60 % des 30-34 ans en disposent contre 40,2 % en 2016 et atteindre 250 000 étudiants contre 210 000 en 2019.

En matière de recherche, la Région compte 11 000 chercheurs issus de la recherche publique et privée, 4 prix Nobel en activité et 180 laboratoires. Les thématiques qui font la réputation de la Région sont la chimie, la biologie, les matériaux, la santé-biotech. Ces domaines d'excellence sont le cœur de la politique d'investissement de la Région puisque le SRESRI désigne trois secteurs stratégiques d'innovation : l'industrie, la santé et la bioéconomie afin de garantir l'efficacité des investissements. ■

Dossier réalisé par **DUOMEDIAS.**
Gilles Baron 06 82 84 11 02 – gbaron@duomedias.fr – Rédaction : Guillemette de Bayser – Maquette : Sylvie Bisson

LORIA

Une recherche de pointe en informatique, tournée vers la société

Jean-Yves Marion, directeur du Laboratoire lorrain de recherche en informatique et ses applications (LORIA, UMR CNRS, Inria, Université de Lorraine) nous a parlé des recherches de ses équipes.

© Inria / Photo D. Betzinger

Des méthodes formelles aux aspects théoriques de l'intelligence artificielle, en passant par l'algorithmique, la géométrie et l'informatique quantique, le Loria développe une recherche fondamentale, nécessaire pour anticiper et accompagner les évolutions technologiques. Cette recherche nourrit un vaste champ d'applications à la croisée des disciplines comme la santé, le traitement automatique des langues, les neurosciences et l'e-éducation.

Un laboratoire d'excellence en cybersécurité

Nous développons une forte activité en sécurité informatique grâce à des partenariats européens et industriels. En cryptanalyse, nos chercheurs battent des records de cassage de clés de chiffrement ; Belenios, notre plateforme de vote électronique, est en plein essor : ce système permet la confidentialité du vote et sa vérifiabilité.

Nos équipes scrutent le *Dark Web* grâce au laboratoire de haute sécurité (LHS). Placé dans un environnement clos, il héberge 35 millions de *malwares* dont nous analysons les propriétés. Trois start-up sont nées de nos travaux en cybersécurité : Cyber-Detect, Scuba et Lybero.net.

Des plateformes de recherche à la rencontre de l'innovation et de l'enseignement

Le Creativ'Lab Systèmes Cyber-Physiques et robotique, créé en lien étroit avec le CNRS, Inria et l'Université de Lorraine, accueille chercheurs, étudiants et entreprises pour mener des travaux en synergie. Ils peuvent y naviguer entre plusieurs espaces : une volière pour les drones, un espace robot à câbles pour l'étude du vol des insectes, une salle dédiée à l'impression 3D ou encore une salle d'expérimentation sur les interfaces cerveau-machine. ■

ITI QMat

Les sciences quantiques appliquées aux matériaux

À Strasbourg, l'Institut thématique interdisciplinaire (ITI) Sciences quantiques et Nanomatériaux (QMat) associe recherche et enseignements de pointe. Questions à J. Léonard et G. Weick, membres du comité de pilotage de l'ITI QMat.

Qu'est-ce que cet ITI mis en place par l'université ?
L'ITI QMat est aux interfaces de la physique, de la chimie, des sciences des matériaux. Son volet Formation est incarné par une EUR (Programme d'Investissements d'Avenir) fondée en 2018 tandis que son volet Recherche constitue la suite des programmes d'excellence. Son objectif : la transition des sciences quantiques fondamentales vers l'innovation.

Pourquoi allier sciences quantiques et nanomatériaux dans vos recherches ?
Les progrès des technologies de l'information et la miniaturisation croissante nécessitent un meilleur contrôle de la nature quantique de la matière qui devient dominante à l'échelle nano. En exploitant les effets quantiques, tels que la cohérence et l'intrication, nous pouvons créer des dispositifs et des matériaux nouveaux, innovants et intelligents qui façonneront l'avenir de la technologie et seront utiles à la société.

Que proposez-vous aux étudiants ?
Notre modèle est « l'enseignement par et pour la recherche ». L'EUR combine cursus Master et Doctorat comme les *Graduate Schools* et s'appuie sur le magistère de physique fondamentale de la Faculté de physique & ingénierie ainsi que sur les laboratoires de recherche associés à l'ITI. Les enseignements en physique sont renforcés et nous recrutons des étudiants de haut niveau, ayant un projet professionnel lié à la physique fondamentale. Des bourses et des stages sont proposés aux étudiants de Master puis des contrats doctoraux. ■

ITES

Faire interagir des géophysiciens et géologues de la Terre solide avec des hydrologues et des géochimistes de l'Environnement

L'Institut de physique du globe et le Laboratoire d'hydrologie et de géochimie ont fusionné et formé en janvier 2021 l'Institut Terre et Environnement de Strasbourg (ITES). Entretien avec Renaud Toussaint, directeur.

Institut **Terre & Environnement** de **Strasbourg** | ITES | UMR 7063 de l'**Université** de Strasbourg & **CNRS** & **ENGEES**

Qu'est-ce que l'ITES ?
C'est une UMR de 210 membres sous tutelle du CNRS (INSU), de l'Université de Strasbourg et de l'École Nationale du Génie de l'Eau et de l'Environnement de Strasbourg (ENGEES). L'ITES se positionne sur une recherche pluridisciplinaire autour de l'étude de la Terre et de son environnement de surface. Il s'appuie sur quatre piliers disciplinaires : l'hydrologie, la géochimie, la géologie et la géophysique. Le pôle se structure autour de l'interdisciplinarité de la recherche et la mise en commun des outils numériques et analytiques.

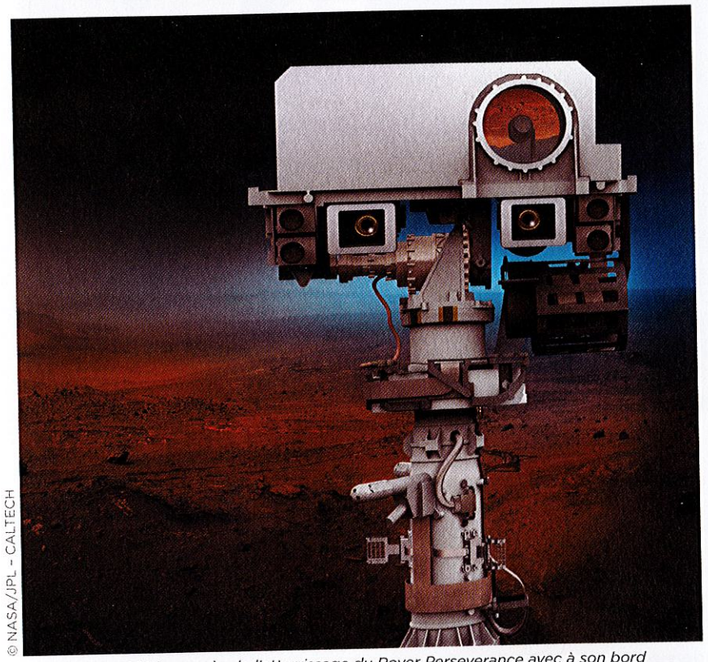
Pourquoi cette interdisciplinarité ?
Nos sujets interdisciplinaires sont notamment liés à la transition énergétique et étudient l'impact du changement climatique sur la surface de la Terre. Nous étudions par exemple : la dynamique et la structure interne de la Terre, la déformation lithosphérique et les risques telluriques, la gestion quantitative et qualitative de la ressource en eau, les processus de transferts en hydrologie et biogéochimie dans les bassins versants.

Et la formation à l'ITES ?
Nous accueillons des étudiants de master ou en école d'ingénieurs, des doctorants. Leur formation s'appuie sur nos travaux et dispositifs de recherche, avec par exemple des stages de terrain sur des sites instrumentés par des membres de l'ITES et des travaux pratiques sur les dispositifs expérimentaux et/ou dans les unités analytiques du laboratoire. ■

INSTITUT DE SCIENCE DES MATÉRIAUX DE MULHOUSE (IS2M)

Les matériaux sous toutes leurs coutures

Sous tutelle de l'université de Haute-Alsace et du CNRS, membre de l'Institut Carnot MICA, de la Fédération des Matériaux et Nanosciences du Grand-Est et partenaire du réseau RS2E, l'Institut de Science des Matériaux de Mulhouse (IS2M) tient l'équilibre entre recherche fondamentale et appliquée, une force mise au service de la connaissance scientifique, de l'industrie et de la formation. Rencontre avec Vincent Roucoules, son directeur.



© NASA/JPL – CALTECH

Mission Mars 2020 : succès de l'atterrissage du Rover Perseverance avec à son bord l'instrument français.

Pouvez-vous nous présenter l'IS2M ?
96 chercheurs, enseignants-chercheurs et ingénieurs y travaillent avec une approche pluridisciplinaire dans le domaine des matériaux, science frontière entre la physique, la chimie, la mécanique, le génie des procédés sans oublier la biologie.
Nous sommes reconnus sur 5 volets, cœur de nos recherches quotidiennes : procédés et processus innovants de synthèse et de mise en forme de ces matériaux ; fonctionnalisation et bio-fonctionnalisation ; méthodes de caractérisation spécifiques des matériaux et sur-mesure ; interactions entre la surface du matériau et l'environnement ; corrélations des propriétés aux différentes échelles.

Quelles sont vos forces ?
C'est résolument notre forte activité contractuelle qui permet que nos activités de recherche fondamentale irriguent nos activités industrielles et réciproquement. Ce sont ainsi 195 projets formalisés qui ont été menés depuis 2018 avec des laboratoires français et étrangers dont 8 projets européens, 35 projets ANR et 80 projets industriels. Nous publions chaque année environ 170 articles.
Ensuite, c'est la présence de 11 plateformes de caractérisation des matériaux certifiées ISO 9001. Elles nous accompagnent avec une grande efficacité dans nos recherches puisque chacune est gérée par un ingénieur spécialisé.

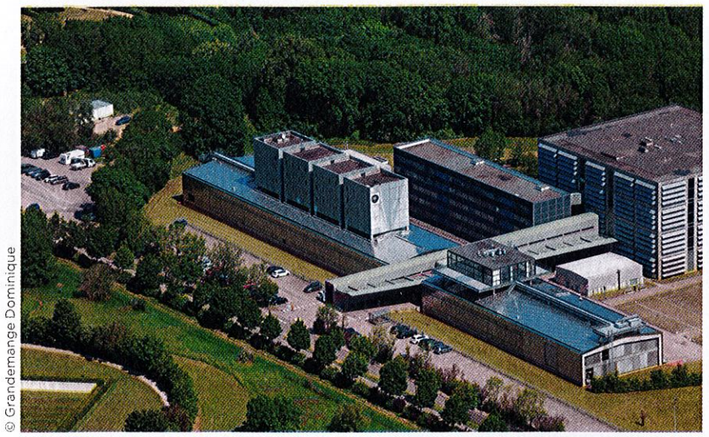
Pouvez-vous nous parler de vos objets de recherche et de leurs applications ?
Nous fonctionnons selon 8 axes thématiques. En voici le détail : Ingénierie des polymères fonctionnels. Nous cherchons par exemple à dépolymériser un matériau grâce à la lumière, pour trouver une alternative au recyclage mécanique du plastique. Matériaux à porosité contrôlée. Concrètement ici des matériaux vont nous servir à capter des molécules comme des polluants. Ces matériaux sont aujourd'hui sur Mars, dans la SuperCam du Robot Perseverance. Carbone et matériaux hybrides, pour les batteries du futur par exemple. Molécules, nano-, microstructures : élaboration, fonctionnalités. Il s'agit ici de structurer la matière comme dans l'impression 3D et 4D. Transferts, réactivité, matériaux pour les procédés propres. L'idée ici est par exemple de stocker dans divers matériaux de la chaleur et de la restituer au moment opportun. Physique des systèmes de basse fonctionnalité. Il s'agit là de physique fondamentale, notamment toute l'activité liée au graphène. Biomatériaux-Biointerfaces. Sont étudiées ici les interactions d'une protéine, d'une bactérie ou d'une cellule avec une surface. Par exemple, c'est de mieux comprendre le comportement d'une cellule cancéreuse et mieux la combattre. Simulations numériques multi-échelles. Il s'agit ici de modéliser l'interaction d'une molécule sur une surface.

Comment parvenez-vous à attirer les talents à l'Institut ?
Notre positionnement thématique nous rend attractifs aux niveaux national et international. Nous accueillons les jeunes chercheurs de talent en leur donnant immédiatement les moyens de travailler en finançant sur nos fonds propres des projets structurants innovants de haut niveau. ■

INIST

La science ouverte pour mieux gérer l'information scientifique

L'Institut de l'Information Scientifique et Technique (INIST) est le « bras armé » du CNRS pour mettre en œuvre sa stratégie de science ouverte. Claire François, directrice, nous en parle.



© Grandemange Dominique

Pouvez-vous nous présenter l'INIST ?
L'INIST est une unité d'appui à la recherche du CNRS qui dépend de la Direction des Donnés Ouvertes de Recherche. Il compte 160 membres. La mission initiale de l'INIST était de permettre l'accès à l'information scientifique. Avec le virage numérique et l'ouverture des données de recherche, ses missions ont évolué vers la mise en place de services et d'un environnement nécessaire à la gestion, au partage, à la diffusion et à la réutilisation de l'information scientifique, données comprises.

Pouvez-vous nous expliquer les services de l'INIST ?
Premièrement, nous assurons un accès numérique à l'ensemble des publications scientifiques internationales *via* deux portails documentaires BibCNRS (littérature courante) et Istex (archives scientifiques). Pour cela, nous négocions et gérons les abonnements aux différentes revues. Nous accompagnons également les chercheurs pour déposer leurs publications sur l'archive ouverte HAL *via* le nouveau portail HAL-CNRS afin de favoriser l'ouverture de la science au plus grand nombre.

Le deuxième axe est celui de la valorisation des données de la recherche. L'INIST accompagne les scientifiques dans la gestion de leurs données, leur partage, leur interopérabilité et leur réutilisation. Pour cela, l'INIST propose deux plateformes : Doranum (ressources pédagogiques pour se former aux nouvelles pratiques) et Opidor (aide à la rédaction de plans de gestion de données).

Enfin le dernier axe : analyser et fouiller l'information scientifique. Dans un contexte de volume toujours croissant d'informations, cela concerne les analyses de type bibliométrique et de cartographies et également la préparation de corpus des textes scientifiques à partir de la base Istex. Ces corpus permettent une analyse plus approfondie et sont utiles pour le développement des logiciels d'apprentissage *Deep Learning*).

Qu'est-ce que la « science ouverte » ?
Elle est née d'une réflexion sur l'accès aux publications. Les recherches sont financées pour une grande part par les États, les publications sont rédigées et évaluées par les scientifiques, il semblait

plus fondé qu'elles restent disponibles librement pour la recherche.

Par cette démarche, le ministère souhaite rendre l'ensemble des résultats de la recherche (publications et données) accessibles afin d'améliorer le fonctionnement même de la recherche, de préserver l'intégrité scientifique.

Cela nécessite un énorme travail. Si certaines ne peuvent pas être ouvertes, il y a tout un pan de données partageables qui ne le sont pas par manque d'organisation spécifique. Aider les chercheurs à documenter et gérer leurs données permet de lutter contre une perte très importante des données de recherche et rend possible leur éventuelle réutilisation pour de nouvelles recherches.

Quels sont les objectifs de l'INIST ?
Le ministère définit une politique de science ouverte avec les établissements dont le CNRS. Les services de l'INIST participent à la mise en œuvre opérationnelle de cette politique.

Aussi, nous nous impliquons dans la mise en place de l'entrepôt national des données (recherche.data.gouv).

L'axe « analyser » est aujourd'hui toujours le plus prospectif, il s'agit de mettre en œuvre à terme un service de fouille de texte répondant aux besoins des tutelles et des chercheurs.

Enfin, nos portails documentaires sont très utilisés et plébiscités, leurs évolutions seront définies en fonction de la vitesse de développement du libre accès.

GEORGIA TECH

Un campus technologique au cœur de la Lorraine

L'antenne lorraine de l'université américaine Georgia Tech fête ses 30 ans. Elle pilote désormais un véritable écosystème axé sur de l'innovation à fort enjeu sociétal : le laboratoire international Georgia Tech-CNRS[1] (IRL), coopéré avec le CNRS, qui fête ses 15 ans et l'Institut Lafayette[2]. Questions à Jean-Paul Salvestrini, directeur de l'IRL.

Pouvez-vous nous présenter votre écosystème de recherche ?
Georgia Tech a été la première université américaine à fonder en 1990 un campus en France : Georgia Tech Lorraine à Metz. Y passent chaque année, environ 700 étudiants essentiellement américains en licence, master, doctorat. En 2006, le campus s'est doté, en partenariat avec le CNRS, d'un laboratoire de recherche international (avec une antenne à Atlanta) s'appuyant sur une soixantaine de personnes. Enfin, pour tourner résolument ce campus vers l'innovation, une plateforme de transfert technologique en optoélectronique est née en 2014 : l'Institut Lafayette.

Quels objets de recherche sont particulièrement moteurs pour vous aujourd'hui ?
Nous travaillons sur les matériaux de structure et fonctionnels. Pour ces derniers nous avons mis en place une filière pour le développement de matériaux et composants à base de semiconducteurs de type GaN. Notre innovation dans ce domaine provient de notre maîtrise du nitrure de bore (2D h-BN), sur lequel nous sommes leaders en Europe, et qui nous permet de développer des applications en optoélectronique et électronique flexible telles que, par exemple, des micro-LED flexibles pour l'optogénétique ou des capteurs environnementaux et biologiques.

Le contrôle non destructif est également un axe de recherche important fondé sur deux techniques complémentaires que sont les spectroscopies THz et acoustique. Nous réalisons par exemple une caractérisation qualitative et quantitative des défauts dans des matériaux composites, un contrôle de la corrosion des métaux ou une identification de défaut dans la cornée de l'œil.

Enfin, une troisième thématique majeure actuellement a trait à l'intelligence artificielle, la robotique et la vision.

À ce sujet, pouvez-vous nous parler de votre projet européen ?
Ce projet de 9 millions d'euros que nous pilotons réunit 9 universités et 11 partenaires industriels. Sa problématique concerne tous les ports maritimes du monde : l'inspection et la maintenance de coques de navires. Aujourd'hui cette opération coûte cher et nécessite un temps d'immobilisation très long. Il s'agirait donc de la faire réaliser par une flotte de robots et de créer une interface virtuelle en 3D avec vue globale et en temps réel de l'analyse faite à l'inspection afin qu'un opérateur puisse prendre la décision de l'immobilisation du bateau et des réparations nécessaires. Nous travaillons également sur les questions de normalisation des technologies développées afin qu'à l'issue du projet les résultats puissent être directement exploitables commercialement.

Comment travaillez-vous avec l'industrie ?
Notre part de recherche contractuelle est relativement importante, ce qui nous permet d'être membre de l'Institut Carnot ARTS. Nous développons ainsi des travaux de recherche avec de grands groupes industriels mais également avec des PME surtout locales souvent grâce aux bourses CIFRE. Nous sommes aussi partenaires d'un Open Lab avec le groupe automobile Stellantis, dans lequel nous avons développé par exemple des capteurs de pollution pour pots d'échappement. ■

1. IRL 2958, https://umi2958.gatech.edu/
2. (https://www.institutlafayette.eu/)