



RÉPUBLIQUE
FRANÇAISE

*Liberté
Égalité
Fraternité*

● CHERCHEURS ● EN CYBERSÉCURITÉ À L'UBS



Yves GROHENS
Vice Président
Innovation

La capacité de l'UBS à dynamiser le territoire au sein duquel elle s'est déployée repose en premier lieu sur la qualité de sa recherche qui est aujourd'hui reconnue au niveau national et international dans des domaines clairement identifiés.

Résolument pluridisciplinaire, elle s'appuie pour cela sur la richesse de ses ressources humaines ainsi que sur des unités de recherche performantes.

La mise en œuvre d'une politique de Recherche et Innovation, tournée vers les forces socio-économiques de son territoire, suppose de la part de l'UBS une connaissance et une maîtrise des écosystèmes dans lesquels se déploient sa dynamique et son expertise scientifique.

Ainsi, l'UBS a fait, très tôt, le choix de se placer en lançant, en 2013, la première formation d'ingénieurs en apprentissage (ENSIBS) en cyberdéfense en France. L'enjeu en Recherche et Innovation est important dans ce domaine et, dans les années qui viennent, l'UBS poursuivra le développement de ses compétences et de son offre en cybersécurité.



Mathias TRANCHANT
Vice Président
Recherche,
Formation doctorale
et Numérique

SOMMAIRE

Édito..... p5

Une recherche de haut niveau p6

LES CHERCHEURS

- par laboratoire -

► IRISA
(Institut de recherche en informatique et systèmes aléatoires)..... p10

► Lab-STICC
(Laboratoire des Sciences et Technologies de l'Information,
de la Communication et de la Connaissance)..... p26

► LMBA
(Laboratoire de Mathématiques de Bretagne Atlantique) p48

► Lab-LEX
(Laboratoire de recherche en droit) p52

► LEGO
(Laboratoire d'Économie et de Gestion de l'Ouest) p56

Des talents diversifiés d'horizons divers en accompagnement
de la dynamique des laboratoires..... p62

Thèses cyber à l'UBS depuis 2014 p75

Zoom sur les doctorant.e.s en cybersécurité à l'UBS p78

Université
Bretagne Sud
ubs:



Université entrepreneuriale et engagée, l'UBS développe 4 grandes priorités : Cyber & Intelligence des données ; Environnement, Santé & Handicap ; Mer & Littoraux et Industrie du futur. À taille humaine, l'Université Bretagne Sud compte 3 campus : Lorient, Vannes et Pontivy. Elle s'appuie sur la compétence de ses 900 personnels dont 500 enseignants et enseignants-chercheurs pour former chaque année plus de 10 000 étudiants.



VIDEO
La recherche à l'UBS

● **Université agile de territoire, l'UBS a fait le choix, dès l'origine, de se focaliser sur des thématiques à la pointe de l'innovation. En y consacrant toute son énergie, elle produit des résultats répondant pleinement aux attentes du monde de la recherche et de l'entreprise.**

Au sein de cet effort collectif, la recherche en cybersécurité à l'UBS repose sur deux principes :

- **« Secure by design » - La sécurité dès la conception avec comme visée la prévention**
Il s'agit de considérer la sécurité comme une propriété intrinsèque d'un système et non uniquement comme une de ses fonctionnalités. Cette propriété doit être définie et vérifiée à sa conception puis préservée lors de son exécution.
- **La transdisciplinarité**
Les problèmes de cybersécurité sont naturellement transdisciplinaires et ne peuvent être résolus - efficacement - en traitant les différents éléments de manière séparée. Notre effort consiste dans la mise sur pied d'un projet global autour de la cybersécurité comme méta-discipline : technique mais également juridique, éthique, géopolitique, communication, etc. Ainsi, aux experts en informatique et électronique, se sont progressivement ralliés des chercheurs venant de domaines divers tels que le génie industriel, le droit, les sciences humaines ou encore l'économie et à l'avenir bien d'autres disciplines.

Nous abordons donc la sécurité numérique de façon intégrée et systémique, car elle conjugue facteurs humains, installations, objets connectés, etc.

● UNE RECHERCHE ● DE HAUT NIVEAU

Une approche globale

Notre perspective combine du logiciel, des composants électroniques, des automates et des processus, conçus et utilisés par et pour des humains - il y a donc un triptyque logiciel - matériel - humain sur lequel poser les bases de la réflexion cyber-sécuritaire.

L'expertise scientifique de 5 laboratoires - une recherche universitaire pour se hisser au meilleur niveau

La dynamique d'ensemble est soutenue par la fédération de plusieurs laboratoires à l'expertise reconnue, allant de l'étude des facteurs comportementaux à la sécurisation des crypto-processeurs :

- Lab-STICC - Laboratoire des Sciences et Techniques de l'Information et de la Communication et de la Connaissance à Lorient
- IRISA - Institut de Recherche en Informatique et Systèmes Aléatoires à Vannes
- LMBA - Laboratoire de Mathématiques de Bretagne Atlantique à Vannes
- LEGO - Laboratoire d'Économie et de Gestion de l'Ouest à Vannes
- LABLEX - Laboratoire de recherche en droit à Vannes

Six axes principaux de recherche

Les axes de recherches de l'UBS sont diversifiés et complémentaires :

- Systèmes embarqués et IoT (Internet of Things)
- Cybersécurité industrielle
- Systèmes de systèmes socio-techniques
- Big data et détection d'intrusions dans des flux massifs de données
- Cybersécurité et la personne
- Cyberdéfense

Des équipes dédiées

Une quarantaine de chercheurs et doctorants travaillent dans le domaine de la cybersécurité à l'UBS.

VIDEO
La recherche cybersécurité
à l'UBS



● UNE RECHERCHE ● DE HAUT NIVEAU

Une Chaire novatrice,
dans le domaine de la
cybersécurité des grands
événements publics
(CGEP)



« La cybercriminalité est une activité bien organisée avec des intentions qui peuvent être financières, économiques, politiques ou revendicatrices. Les grands événements tels que les Jeux Olympiques ou la Coupe du Monde de football constituent un terrain idéal pour de tels desseins.

L'objectif de notre chaire est de protéger les grands événements de ce type d'activités criminelles. Notre approche est centrée sur la sécurité par la conception, avec une philosophie de traitement transdisciplinaire. En effet, les problèmes de cybersécurité étant transdisciplinaires, nos équipes le sont également. »

Salah SADOU,
titulaire de la Chaire Cybersécurité des
Grands Événements Publics

La chaire : un maillon essentiel - une recherche appliquée tournée vers l'entreprise

Les travaux de recherche, proposés dans le cadre de la chaire, sont conçus pour être fertiles et facilement exploitables. Ils permettent d'aller au-delà des résultats actuels de recherche en cybersécurité et sont immédiatement profitables aux entreprises et organisations.

Un enjeu crucial

La digitalisation massive de toutes les grandes manifestations nationales et internationales accueillant du public engendre des vulnérabilités nouvelles, potentiellement exploitables par des pirates informatiques. Les risques concernent l'intégrité physique des acteurs et les pertes financières.

Un domaine peu exploré - une approche novatrice et originale

Au sein de cette thématique, l'axe directeur du projet est de considérer ces événements comme des « systèmes de systèmes sociaux-techniques » car ils conjuguent facteurs humains, installations, objets connectés, etc.

GICAT



CHAIRE
CYBERSÉCURITÉ
DES GRANDS ÉVÈNEMENTS
PUBLICS

REJOIGNEZ-NOUS !



UMR 6074
INSTITUT DE RECHERCHE EN
INFORMATIQUE ET SYSTÈMES
ALÉATOIRES
IRISA

Plus de **850** membres

L'IRISA (Institut de recherche en informatique et systèmes aléatoires), créée en 1975, est une unité mixte de recherche (UMR) en informatique, automatique, traitement du signal et des images et en robotique. Sur la conjonction de ces thématiques, l'IRISA se positionne comme le grand laboratoire de recherche en Bretagne avec une présence affirmée sur les campus de Rennes, Vannes et Lannion.

L'IRISA sur le site de l'UBS développe des activités dans plusieurs domaines de l'informatique :

- l'architecture logicielle
- la synthèse et l'analyse d'images
- le traitement d'images complexes
- l'interaction gestuelle
- la fouille de données
- l'informatique mobile
- l'informatique décisionnelle
- la cybersécurité

Les chercheurs de l'UBS participent à quatre des équipes de l'UMR IRISA :

- ARCHWARE (architectures logicielles)
- CASA (communication et services dans les réseaux à connectivité intermittente)
- EXPRESSION (fouille, analyse, synthèse de données complexes multimédia et interaction)
- OBELIX (observation de l'environnement par imagerie complexe)

DOMAINES SCIENTIFIQUES

Bio-informatique, sécurité des systèmes, nouvelles architectures logicielles (manycorés, Cloud computing), réalité virtuelle, intelligence artificielle.

COLLABORATIONS INDUSTRIELLES

L'IRISA s'est engagé sur de nombreuses opérations de partenariat industriel dans les domaines des télécommunications, de la défense, de l'informatique et le multimédia, de l'instrumentation médicale et des transports.

France : EADS, Orange, EDF, Nexter System, Renault, ST Microelectronics, Thales, Technicolor, Alcatel...

International : Texas Instruments, IBM, Google, Intel...

VALORISATION

Les résultats de recherche sont investis dans de nombreuses collaborations avec des partenaires industriels. Plusieurs start-up sont issues des recherches de l'IRISA.

LIEN
Vers le site de l'IRISA





Jamal EL HACHEM

Maître de Conférences
Informatique

“
*La recherche scientifique est l'une
des professions les plus
passionnantes et les plus
gratifiantes*
”

Par Frederick Sanger

BIO

Jamal EL HACHEM est Maître de Conférences à l'ENSIBS Vannes, Université de Bretagne Sud (depuis le 1^{er} septembre 2019). Ses activités de recherche se concentrent sur l'étude de solutions basées sur l'ingénierie dirigée par les modèles pour l'ingénierie de la cybersécurité et de la cyberdéfense dans un environnement de systèmes de systèmes. Elle a obtenu son doctorat à l'Université de Pau en décembre 2017, soutenant sa thèse intitulée «Une méthode dirigée par les modèles pour la conception et l'analyse des architectures sécurisées des Systèmes-de-Systèmes. Application à la prédiction des attaques en cascade dans les bâtiments intelligents ». Elle a ensuite travaillé deux ans comme Attachée Temporaire d'Enseignement et de Recherche à l'Université de Pau. Elle a collaboré autour des projets de cybersécurité avec des laboratoires de recherche nationaux et internationaux.

Données essentielles

Doctorant.e.s : 3

Prix/Bourses :

- Bourse de thèse du conseil départemental des Landes, Mont-de-Marsan, 2014-2017, montant : 84000 €.
- Merit-based Award of SIGSOFT CAPS (montant : US\$ 350) pour la participation à ICSE, Italie, 2015.
- Bourses de l'Université d'Adelaïde, Australie (montant : AU\$ 5400) et l'UPPA (montant: 900€) pour une visite de recherche internationale, Février - Avril 2017.

Collaborations internationales :

- CREST team, University of Adelaide, Australia.
- School of Innovation design and Engineering-Mälardalen University, Sweden.
- Information Systems Engineering Research Group, KU Leuven, Belgium.
- ESL Global Cybersecurity Institute-Rochester Institute of Technology, NY.

100% de l'activité du chercheur
dédiée à la cybersécurité

Focus :
Recherche
Domaine applicatif

Axe(s) de recherche

Étude des approches basées sur l'IDM et axées sur l'architecture et la cybersécurité afin de guider la modélisation et d'automatiser l'analyse de la cybersécurité des systèmes.

Champs d'expertise

Modélisation, analyse et simulation de la cybersécurité.
Modélisation et évaluation des vulnérabilités.
Prédiction/découverte des attaques de sécurité.
Techniques de l'Ingénierie Dirigée par les Modèles (IDM).
Définition des langages de Modélisation Spécifiques au Domaine (DSML).

Exemples d'applications

Sécurité dans différents types de systèmes tels que les Systèmes-des-Systèmes, les systèmes à logiciel prépondérants, les systèmes multi-agents.
Sécurité dans différents domaines tels que les bâtiments intelligents, les véhicules autonomes, les réseaux électriques intelligents, Internet des objets, défense, systèmes médicaux, etc.

Responsabilités

Responsable de la mission mixité pour le master européen CYBERUS.
Responsable de la classe préparatoire intégrée STI2D (PEI STI2D ENSIBS).
Membre du Conseil de Laboratoire de l'IRISA.

Domaine

Sécurité par la conception

Mots clés

Sécurité par conception
Vulnérabilités logicielles
Sécurité des Systèmes-de-Systèmes
Ingénierie dirigée par les modèles (IDM)

Contact

jamal.el-hachem@univ-ubs.fr



Mawloud OMAR

Professeur des Universités
Informatique

“
*La recherche scientifique stimule
la veille et l'anticipation. Saisissons
l'opportunité tant qu'on a le choix :
mieux vaut se sécuriser
que se défendre*”

BIO

Mawloud Omar est Professeur des Universités à l'ENSIBS - Université de Bretagne Sud et membre de l'équipe CASA à l'IRISA. Il a obtenu son doctorat et habilitation à diriger des recherches respectivement en 2011 et 2022. Il a exercé en qualité de maître de conférences pendant deux ans à ESIEE Paris - Université Gustave Eiffel. Auparavant, il était chercheur senior à l'IRT SystemX et a travaillé pendant plusieurs années en tant qu'enseignant-chercheur à l'Université de Technologie de Compiègne et à l'Université de Bejaia. Ses activités de recherche se focalisent principalement autour de la cybersécurité. Il s'intéresse aux défis majeurs en relation avec la protection des réseaux émergents et des systèmes à fortes contraintes.



Lien vers la biographie complète

Données essentielles

Doctorant.e.s : 10

Publications/journaux : 43 - IEEE Transactions on ITS, IEEE Transactions on TVT, JNCA, CS, etc.

Conférences : 35 - IEEE ICC, IEEE LCN, IEEE CAMAD, etc.

Collaborations internationales :

École de Technologie Supérieure (Université du Québec, Canada), Université du Québec Outaouais (Canada), Université de Oregon State (Etats-Unis), etc.

Axe(s) de recherche

Sécurité des systèmes à très large échelle.
Sécurité des systèmes hautement dynamiques.
Sécurité des systèmes à faibles ressources.

Champs d'expertise

Confiance et gestion de clés.
Authentification, authentification biométrique et contrôle d'accès.
Vie privée et anonymat.
Robustesse et détection des intrusions.

Exemples d'applications

Internet des objets.
Véhicules connectés.
Applications médicales.

Responsabilités

Responsable de la filière « Sécurité des systèmes d'informations » de l'ENSIBS (2022-*).
Plusieurs responsabilités dans le passé (directeur de département, responsable d'équipes de recherche, etc.).

Domaine

Sécurité des systèmes
à fortes contraintes

Mots clés

Sécurité
Sûreté
Fiabilité

Contact

mawloud.omar@univ-ubs.fr
+33 (0) 2 97 01 72 29



Salah SADOU

Professeur des Universités
Informatique

“

La transdisciplinarité enrichit la science, mais aussi le scientifique

”

BIO

Salah Sadou est le porteur de la chaire cybersécurité des grands événements publics et responsable de la spécialité Informatique et Cybersécurité de l'Ecole Nationale d'Ingénieurs de Bretagne Sud (ENSIBS). Par ailleurs, Salah Sadou est responsable d'une équipe de recherche en cybersécurité de l'IRISA. Il a obtenu un doctorat en janvier 1992 à l'Ecole Centrale de Lyon et a environ 30 ans d'expérience dans la recherche et l'enseignement en génie logiciel. Ses intérêts de recherche antérieurs étaient centrés sur les langages, les processus, les outils de conception et d'ingénierie de systèmes, où l'évolution agit comme une entité de première classe. Il a également été engagé dans la recherche concernant les langages de description architecturale avec les propriétés non fonctionnelles comme entités de première classe, la restructuration de logiciels (orientée objet vers orientée composant), les langages de description orientés composants et la qualité du logiciel. Ses intérêts de recherche actuels portent principalement sur la conception de systèmes sécurisés, appliqués au systèmes de systèmes et de systèmes sociotechniques.



Lien vers la biographie complète

Données essentielles

Doctorant.e.s : 20

Post-doctorant.e.s : 3

Journaux : 20 - JSS, Future Gener. Comput. Syst, Automated Soft. Eng., etc.

Conférences : 70 - WICSA, ECSA, ASE, CBSE, ICECCS, Middleware, etc.

Livre(s) : Evolution du logiciel, Hermes-Lavoisier.

Prix : ACM SIGSOFT Distinguished Paper Award (2011), plusieurs meilleurs papiers.

Collaborations internationales : Université de Montréal (Canada), UQAM (Canada), Université Libre de Bruxelles (Belgique), Université du Luxembourg (Luxembourg), Université du Qatar (Qatar), Politecnico di Milano (Italie), etc.

100% de l'activité du chercheur
dédiée à la cybersécurité

Focus :
Recherche
Domaine applicatif

Axe(s) de recherche

Sécurité des systèmes de systèmes.

Champs d'expertise

Identification de vulnérabilités dans le code.
Identification de vulnérabilités conceptuelles.
Estimation de la vulnérabilité humaine dans un système.
Evaluation de l'impact de la vulnérabilité d'un élément sur le système.
Proposition de bonnes pratiques pour le développement de logiciels sécurisés.

Exemples d'applications

Organisation de grands événements sécurisés.
Identification et correction de failles dans des systèmes logiciels existants.

Responsabilités

Responsable de la filière Cybersécurité du logiciel de l'ENSIBS.
Responsable scientifique de la chaire Cybersécurité des Grands Evènements Publics.
Co-responsable du groupe de travail RIMEL du GDR GPL du CNRS (2006-2014).
Responsable de l'équipe de recherche SE (Valoria, UBS, 2004-2012).

Domaine

Sécurité logicielle

Mots clés

Sécurité par conception
Vulnérabilités logicielles
Sécurité des systèmes de systèmes socio-techniques
Modélisation orientée sécurité
Spécification orientée sécurité

Contact

salah.sadou@univ-ubs.fr
+33698899263



Nicolas BELLOIR

Maître de Conférences
Informatique

“

Il est important de franchir les limites de notre discipline pour s'enrichir des autres domaines

”

BIO

Après un DEA à l'Université Paul Sabatier (Toulouse) et un passage dans l'industrie aéronautique, Nicolas Belloir soutient une thèse sur la composition logicielle à l'Université de Pau et des Pays de l'Adour en 2004. Il y est maître de conférences et se concentre sur les langages d'ingénierie pour les systèmes complexes. En 2016, il rejoint l'Université Bretagne Sud, affecté à l'Académie militaire de St-Cyr Coëtquidan. Les enjeux en vue de la création d'une véritable force cyber sont considérables et ses recherches, souvent menées conjointement pour la société civile et militaire, mettent en perspective la détection des vulnérabilités, et plus récemment la lutte informatique d'influence. Via une approche pluridisciplinaire, la robustesse des systèmes est pensée pour contrer les vulnérabilités des systèmes qui peuvent être physiques, logiciels ou humains.



Lien vers la biographie complète

Données essentielles

Doctorant.e.s : 7

Publications : 5 - Systems Engineering, JSS, etc.

Conférences : 40 - Conceptual Modelly, Trustcom, SoSE.

Collaborations internationales : Université Polytechnique de Valencia (Espagne).

Axe(s) de recherche

Ingénierie de la sécurité des systèmes de systèmes, prise en compte de l'humain dans les processus de sécurité par conception, lutte informatique d'influence.

Champs d'expertise

Détection de vulnérabilités lors des phases de conception.
Amélioration de la communication entre ingénieur logiciel (ou système) et experts en sécurité.
Langage de modélisation.

Exemples d'applications

Logiciel d'analyse de vulnérabilité pour les systèmes de systèmes socio-techniques.
Définition d'une méthode d'analyse des menaces outillée.
Définition d'un modèle conceptuel de Fake News.

Responsabilités

Titulaire de la Chaire « Cyberdéfense-cybersécurité » Saint-Cyr Thales.
Directeur adjoint du mastère spécialisé Cyberdéfense et champs immatériels de l'ARSCC.
Divers projets en recherche duale civile et militaire (DGA / Naval Group) sur la détection des vulnérabilités logicielles ou des systèmes de systèmes socio-techniques.

Domaine

Sécurité par la conception
Lutte informatique d'influence

Mots clés

Conception
Ingénierie
Sécurité de systèmes de systèmes
Analyse de vulnérabilité système et humaine
Fake News

Contact

nicolas.belloir@univ-ubs.fr
+33 (0) 2 97 01 72 17



Isabelle BORNE

Professeur des Universités
Informatique

“
*La sécurité informatique n'est pas
qu'une affaire de spécialistes et
sans les femmes il n'y aurait pas
d'Internet : pour mémoire, le
premier «bug» a été découvert
grâce à Grace Hopper !*
”

BIO

Après avoir obtenu sa thèse à l'Université Pierre-et-Marie Curie (Paris-6), Isabelle Borne a passé deux années de post-doc à Montréal, à l'Université de Montréal et à l'Université McGill au Canada. Puis elle a passé 10 ans à l'Université René Descartes (Paris 5) et ensuite 7 ans à l'Ecole des Mines de Nantes. En 1994 elle a été invitée à l'Institute of Educational Technology de l'Open University à Milton Keynes (UK) et à l'Université de Manchester où elle a travaillé sur les environnements de programmation par objets. Finalement elle rejoint l'Université Bretagne Sud en 2001 où elle s'intéresse actuellement à la sécurité des systèmes de systèmes, et plus spécifiquement à l'utilisation de patrons de sécurité et de métriques pour garantir un niveau de sécurité des architectures logicielles de systèmes de systèmes.



Lien vers la biographie complète

Données essentielles

Doctorant.e.s : 7

Publications : 11 - JSS, Future Generation Computer, etc.

Conférences : 46 - CSMR, ECSA, SoSE, ISPEC, etc.

Collaborations internationales : Université de Montréal (Canada), Universidad de los Andes (Colombie), etc.

Axe(s) de recherche

Sécurité des architectures de systèmes de systèmes.

Champs d'expertise

Modélisation et méta-modélisation des architectures de systèmes de systèmes.
Refactoring avec des patrons de sécurité.
Métriques de sécurité logicielle.

Exemples d'applications

Simulation d'un système de systèmes de gestion des secours.
Évaluation du niveau de sécurité d'une architecture logicielle.
Sécuriser l'architecture d'un smart building.

Responsabilités

Directrice adjointe de l'Ecole Doctorale MathSTIC.
Membre de l'équipe de direction de l'UBS.
Co-responsable de l'action IDM des GDR GPL et ASR (2012-2015).
Co-responsable du GT sécurité dans le développement logiciel du GDR GPL.

Domaine

Génie logiciel

Mots clés

Ingénierie des modèles
Architecture logicielle
sécurisée
Secure by design
Patrons de sécurité

Contact

Isabelle.Borne@univ-ubs.fr



Pierre-François MARTEAU

Professeur des Universités
Informatique

“ *L’anormalité est l’anomalie de la normalité, à moins que cela soit l’inverse. L’identification de l’anomalie est souvent le préambule à des découvertes disruptives* ”

BIO

Après avoir obtenu un diplôme d'ingénieur en informatique à l'École Nationale Supérieure d'Electronique et d'Informatique de Bordeaux (ENSEIRB-MATMECA), puis un doctorat à l'Institut national polytechnique de Grenoble en 1988, Pierre-François Marteau a occupé un poste de post-doctorant à l'Université de Genève, puis à l'INLS de l'Université de Californie (San Diego). A la suite d'un passage à l'Institut des Hautes Etudes Scientifiques, il est consultant chez Bertin Technologies, avant de rejoindre l'Université de Bretagne Sud en 1999. Ses travaux portent sur les approches algorithmiques de l'intelligence artificielle pour la reconnaissance des formes dans les données temporelles et séquentielles. Il développe des applications dans les domaines du traitement des flux d'information, notamment dans un contexte de sécurité informatique ou du traitement de données issus de capteurs multi-modaux et de fouille de textes collectés sur le web et les réseaux sociaux.



Lien vers la biographie complète

Axe(s) de recherche

Détection d'anomalie et d'intrusion.
Traitement de données en flux et séries temporelles
(classification, régression, clustering).
Analyse de mouvements et reconnaissance de gestes.
Fouille de données textuelles.

Champs d'expertise

Algorithmes et complexité.
Traitement de signal et reconnaissance de formes.
Traitement du langage naturel.

Exemples d'applications

Plusieurs algorithmes pour la détection d'intrusions et efficacité algorithmique :
DiFF-RF (surveillance trafic réseau), STree4CS (séquentialité d'événements pour
détection d'attaques), PSS-Phase Shape Separation (authentification de signature
manuscrite par analyse des patterns temporels et de forme).

Domaine

Informatique,
mathématiques discrètes

Mots clés

Intelligence artificielle
Apprentissage statistique
Data Mining
Reconnaissance des formes
Détection d'anomalie
Analyse de séries temporelles
Traitement données textuelles

Contact

pierre-francois.marteau@univ-ubs.fr
+33 (0) 2 97 01 72 99



Nicolas COURTY

Professeur des Universités
Informatique

“

*On peut tromper une fois mille
algorithmes d'IA, mais pas mille
fois un algorithme d'IA*

”

BIO

Après une thèse portée sur la vision active (INSA Rennes, 2002), Nicolas Courty s'est spécialisé dans la simulation de foules dès son séjour post-doctoral au Brésil. Il rejoint l'Université Bretagne Sud en 2004 où il poursuit par l'analyse de modèles de simulation de foule et langage signe. Il est invité huit mois à Beijing en 2012, puis deux mois à l'EPFL Lausanne en 2014. Dès 2012 il développe des méthodologies pour l'apprentissage automatique et la télédétection. Ses activités de recherche au sein de l'équipe Obélix (IRISA) qu'il dirige depuis 2020, portent sur l'apprentissage statistique, le transport optimal et l'apprentissage profond. Dans un contexte de cybersécurité, il aborde essentiellement la sécurité et les vulnérabilités des algorithmes d'IA. Relecteur d'articles pour plusieurs revues et conférences en IA, il est également titulaire d'une chaire en Intelligence Artificielle de l'ANR, portant un projet autour du transport optimal et de la télédétection.



Lien vers la biographie complète

Données essentielles

Doctorant.e.s : 16

Post-doctorant.e.s : 3

Publications : 38 - IEEE PAMI, IEEE TGRS, Machine Learning, etc.

Conférences : 63 - NeurIPS, ICML, ICLR, AISTATS, etc.

Livre(s) : 4 chapitres - Deep learning for earth science, Wiley 2020.

Prix : U.V. Helava Award 2015 ; 4 Best Paper Awards (conférences internationales).

Brevet(s) : 1 - Procédé de dénombrement d'individus dans une foule, 2014 (Thalès / CNRS).

Collaborations internationales : Kyoto University (Japon), Wageningen University (NL), Université des Iles Baléares (ES). Invité à Beijing (2012 - financé par l'académie des Sciences Chinoise) puis à l'EPFL Lausanne (Suisse - 2014).

25% de l'activité du chercheur
dédiée à la cybersécurité

Focus :
Recherche
Domaine applicatif

Axe(s) de recherche

Théorie de l'IA.
Télédétection.
Vision par ordinateur.

Champs d'expertise

Apprentissage statistique.
Apprentissage profond (machine learning).

Exemples d'applications

Segmentation sémantique d'images satellites dans un contexte de labels bruités.
Sécurité des algorithmes d'IA en télédétection.
Apprentissage de données structurées de type graphes.

Responsabilités

- Responsable de l'équipe Obelix (depuis 2020).
- Membre de ELLIS, laboratoire européen de promotion de l'Intelligence Artificielle (depuis 2020).
- Responsable du projet ANR OATMIL - liens entre la théorie du transport optimal et du machine learning.
- Responsable du projet Labex COMINLABS Dynalearn - liens entre apprentissage profond et modèles physiques.
- Animateur du pôle Science des données de l'UBS.
- Directeur d'études du Cursus Master Ingénierie Science des données de l'UBS.
- Expertises IA pour l'ANR à l'international.

Domaine

Intelligence Artificielle

Mots clés

Transport optimal
Réseaux de neurones
Machine à noyaux

Contact

nicolas.courty@univ-ubs.fr
+33 (0) 2 97 01 72 13



UMR 6285

**LABORATOIRE DE SCIENCES
ET TECHNIQUES
DE L'INFORMATION,
DE LA COMMUNICATION
ET DE LA CONNAISSANCE**

LAB-STICC

560 membres

Le slogan de l'Unité « Des capteurs à la connaissance : communiquer et décider » soulignait initialement la volonté de donner du « sens » au « signe », en terme d'interprétations et de valeur augmentée vis à vis des traitements adossés à un signal sous toutes ses formes. Ce slogan s'avère aujourd'hui plus conforté encore face à l'importance de la donnée, qui devient le vecteur de l'innovation technologique et scientifique, dopée indéniablement par les progrès majeurs de la science dans le domaine de la cognition et de l'intelligence artificielle.

Le Lab-STICC, fort de son double rattachement aux instituts INS2I et INSIS du CNRS, est une unité de recherche historiquement reconnue en Bretagne Océane et en France dans le domaine des STIC. Elle affiche une capacité avérée de couvrir un large spectre scientifique autour des sciences du numérique, et avec en particulier cette faculté d'adresser des champs disciplinaires variés (Théorie de l'Information, Ondes & Matériaux, Electronique et Informatique embarquées, Sciences des données, Communication et détection de signaux, Interfaces Homme-Machines,..) suivant des thématiques/secteurs applicatifs multiples : l'environnement maritime, les objets communicants, la défense, le spatial, la santé, la sécurité, la robotique...

560 scientifiques en moyenne (permanents et non-permanents) portent ainsi les activités du Lab-STICC en couvrant des thématiques scientifiques fortes, bien identifiées, différenciantes. L'innovation reste au coeur des préoccupations de nos chercheurs, et les actions transversales de grande ampleur lancées dans le contexte du quinquennat 2017-2021 (autour de la cybersécurité, de l'IA, des drones et systèmes embarqués, de la robotique, de la réalité virtuelle ou augmentée,..) ont conduit à la consolidation des pôles scientifiques d'une part, mais également à l'émergence de nouveaux outils structurants (chaires de recherche, contribution à la création d'un laboratoire International (IRL Crossing), Plateformes technologiques, start-up, EuR).

LIEN
Vers le site du Lab-STICC





Guy GOGNIAT

Professeur des Universités
Électronique et informatique embarquée

“

*La recherche collaborative
est une richesse qu'il faut
cultiver avec passion*

”

BIO

Après avoir obtenu sa thèse à l'Université de Nice Sophia-Antipolis en 1997, Guy Gogniat rejoint l'Université Bretagne Sud en 1998. En 2004-2005, il est invité à l'Université du Massachusetts aux Etats-Unis, où il travaille sur la sécurité des architectures reconfigurables. Depuis 2003, ses activités de recherche concernent la sécurité des systèmes embarqués face aux attaques logicielles et matérielles.

Ses recherches bénéficient de programmes de financements nationaux et européens.



Lien vers la biographie complète

Données essentielles

Doctorant.e.s : 31

Post-doctorant.e.s : 5

Publications : 40 - IEEE TVLSI, IEEE TC, ACM TODAES, ACM TECS, etc.

Conférences : 130 - DATE, FPL, FCCM, FPGA, FPT, ReCoSoC, DSD, etc.

Livre(s) : Security Trends for FPGAs - Springer.

Prix : Best Paper Award (ReCoSoC 2015), IFIP SEC 2020, CYBER2020).

Brevet(s) : Procédé de reconfiguration d'un ensemble de composants d'un circuit électronique (2008).

Collaborations internationales : Ruhr-Universität Bochum (Allemagne), University of Massachusetts (USA), Université Libre de Bruxelles (Belgique), Université Technique de Munich (Allemagne), Information Technology University (Pakistan), Politecnico di Milano (Italie), etc.

100% de l'activité du chercheur
dédiée à la cybersécurité

Focus :
Recherche
Domaine applicatif

Axe(s) de recherche

Sécurité des systèmes embarqués.

Champs d'expertise

Protection des architectures de systèmes embarqués.
Protection des architectures de processeurs.
Systèmes de détection d'intrusion.
Développement de crypto-processeurs.

Exemples d'applications

Protection des données de santé et des applications multimédia.
Protection des systèmes d'exploitation.

Responsabilités

- Vice-doyen de la Faculté Sciences et Sciences de l'Ingénieur (2022 -*).
- Co-directeur du département Sciences et Techniques de la Faculté Sciences et Sciences de l'Ingénieur (2020 - 2023).
- Vice-président recherche UBS (2016-2020).
- Comité d'évaluation ANR sécurité globale et cybersécurité (2017-2020).
- Directeur adjoint laboratoire Lab-STICC (2010-2016).
- Co-responsable du groupe disciplinaire Math-STIC de l'ED SICMA (2010-2016).
- Conseil Scientifique du CNRS INS2I (2015-2018).
- Co-responsable du thème C du GdR ISIS (2009-2015).
- Co-responsable du thème sécurité numérique du GDR SoC-SiP (2009-2013).

Domaine

Sécurité matérielle

Mots clés

Cryptographie
Cryptoprocasseur
Attaques matérielles
et logicielles
FPGA
NoC
Offuscation de code

Contact

guy.gogniat@univ-ubs.fr
+33612849229



Vianney LAPÔTRE

Maître de Conférences
Électronique et informatique embarquée

“

*Nos recherches d'aujourd'hui
sont les bases des technologies
de demain*

”

BIO

Après l'obtention de sa thèse en 2013 sur les architectures reconfigurables multi-cœurs appliquées aux problématiques des télécoms, Vianney Lapôtre revient à l'UBS en 2014. Il y travaille sur la sécurité des systèmes embarqués. L'année précédente il participait au projet européen Mont-Blanc, alors en post-doc au LIRMN (Montpellier). Les technologies issues des systèmes embarqués y étaient étudiées pour concevoir les supercalculateurs de demain, moins gourmands en énergie. Depuis 2017, ses recherches s'intéressent plus particulièrement à la sécurité des processeurs embarqués. Offrir des processeurs sécurisés est pour lui une priorité afin de permettre au plus grand nombre de bénéficier de technologies de confiance.



Lien vers la biographie complète

Données essentielles

Doctorant.e.s : 9

Post-doctorant.e.s : 2

Publications : 11 - IEEE TVLSI, IEEE TC, ACM TECS, etc.

Conférences : 37 - FPL, FPT, ISCAS, ASP-DAC, ISVLSI, etc.

Collaborations internationales : Ruhr-Universität Bochum (Allemagne), Information Technology University (Pakistan).

Axe(s) de recherche

Sécurité des systèmes embarqués.

Champs d'expertise

Protection des architectures de processeurs embarqués.
Protection des architectures de systèmes embarqués.

Exemples d'applications

Protection des objets connectés.
Protection des données sensibles.

Projets collaboratifs

CominLabs SCRATCHS (projet Labex CominLabs2021-2024) avec IRISA, Inria.
HardBlare (projet CominLabs 2015-2019) avec IRISA, Inria, IETR Rennes.
TSUNAMY (projet ANR 2013-2017) avec le laboratoire Hubert Curien (St Etienne),
le Lip6 (Paris), et le CEA Saclay.

Domaine

Sécurité matérielle

Mots clés

Attaques matérielles
et logicielles
Processeurs embarqués
FPGA

Contact

vianney.lapotre@univ-ubs.fr
+33 (0)2 97 87 45 68



Philippe TANGUY

Maître de Conférences
Electronique et informatique embarquée

“
*La sécurité des objets
communicants doit se faire à la
conception, tout en pensant leur
consommation et durabilité*
”

BIO

Dès son doctorat (INSA Rennes 2012), Philippe Tanguy s'est intéressé à la communication pour les systèmes embarqués. En postdoctorat à Telecom Bretagne au sein d'une équipe pluridisciplinaire (IHSEV, Lab-STICC, IMT Atlantique) il se penche sur les protocoles de communication de l'IoT, des robots compagnons, des services de santé et de bien-être (projet européen FP7 PRECIOUS). Il est enseignant-chercheur pendant deux ans à l'INSA Rennes avant de rejoindre l'Université Bretagne Sud en 2018. Ses travaux traitent conjointement chaîne de communication et matériel. En concevant des objets fonctionnant avec de faibles ressources, son objectif est de bien connecter les villes, les industries et les transports pour les rendre plus intelligents et économes. Ceci passe en priorité par la sécurisation de ces objets et en partie par les communications afin d'être plus robustes aux attaques issues du réseau.



Lien vers la biographie complète

Données essentielles

Doctorant.e.s : 2

Publications : 5 - JCM, JECE, JISYS, KI - Künstliche Intelligenz, EAI endorsed transactions on pervasive health and technology.

Conférences : 14 - WSPLC, ATC, ITST, EAI, etc.

Livre(s) : 2 chapitres - Vehicular Technologies (2011), CMOS Emerging Technologies (2012).

Prix : Best Paper Award (ICSNC 2014).

Axe(s) de recherche

Sécurité des systèmes embarqués.

Champs d'expertise

Protection des architectures de systèmes embarqués communicants.
Radio logicielle.

Exemples d'applications

Conception de villes intelligentes, transports intelligents, industrie du futur, santé.

Projets collaboratifs & Implications

- Directeur d'étude du parcours CSSE (Cyber Sécurité des Systèmes Embarqués) du Master Ingénierie des Systèmes Complexes (2020-*).
- POLYPHEME (Contrat CNRS 2017-2018) pour INEO Défense.
- PRECIOUS FP7 n°611366 (Projet européen) - Création d'outils numériques santé et bien-être.
- CIFAER (Projet ANR 2008-2012) - Communication intra-véhicule flexible et architecture embarquée reconfigurable.
- TRUSTGW (Projet ANR 21-CE39-0005) « Protection de gateway IoT contre des menaces logicielles et sur les communications ».

Domaine

Sécurité matérielle

Mots clés

Attaques matérielles
et logicielles
Attaques réseaux
FGPA
IDS/IPS

Contact

philippe.tanguy@univ-ubs.fr
+33 (0)2 97 87 45 67



CAMILLE MONIÈRE

Maître de Conférences
Electronique et informatique embarquée

“ *Les enjeux climatiques et sociaux
d'aujourd'hui requièrent de penser
conjointement la sécurité,
l'efficacité et la durabilité
des systèmes numériques* ”

BIO

Les travaux de thèse de Camille Monière portaient sur le développement d'implémentations logicielles et matérielles efficaces en énergie et en ressources de systèmes communicants (Projet ANR QCSP). Au cours du prolongement de ses recherches durant un ATER au sein du Lab-STICC et de l'Université Bretagne Sud, il a pu constater que les aspects sécurité et efficacité des systèmes sont souvent explorés indépendamment. Pourtant, ces deux aspects s'influencent l'un l'autre ; les fonctions de sécurité peuvent entraîner des augmentations de consommation et l'accroissement de l'efficacité peut s'accompagner de celle de la surface d'attaque. En tant que maître de conférence à l'UBS, son objectif est d'essayer de concilier les deux approches, notamment en pensant dès la conception des systèmes sur puces, voire en les intégrant dans les protocoles de communications.

Données essentielles

Publications : 1 - Elsevier JSA.

Conférences : 4 - DASIP, SiPS, EuCNC, COMPAS.

Prix : Best Paper Award (DASIP 2022).

Axe(s) de recherche

Sécurité des systèmes embarqués.

Champs d'expertise

Conception d'architecture matérielle et logicielle efficace.
Radio logicielle.

Exemples d'applications

Industrie du futur, systèmes de communications numériques sécurisés, économique et écologique, santé.

Projets collaboratifs & Implications

- Directeur d'étude de la 1^{ère} et 2^{ème} année de la mention SNIO (Sciences Numériques, Internet et Objets connectés) de la licence science des systèmes communicants (2023 - *)
- QCSP (Projet ANR 2019 - 2023) - Développement, conception et implémentation efficace d'un protocole de communication basse consommation, longue portée et haute fiabilité de nouvelle génération pour l'Internet des objets et les réseaux de capteurs.

Domaine

Sécurité et efficacité
matérielle

Mots clés

Synthèse de Haut-Niveau
Architectures matérielles
et logicielles
Efficacité énergétique
Adéquation algorithme-
architecture

Contact

camille.moniere@univ-ubs.fr
+33 (0)2 97 87 45 67



Laurent GUILLET

Maître de Conférences
Psychologie sociale de la santé

“ *La technologie, l'innovation
technologique et leurs utilisations
doivent s'accompagner de l'étude
des facteurs humains pour être
efficaces* ”

BIO

Laurent Guillet, arrivé à l'Université Bretagne Sud en 2004, s'intéresse aux facteurs humains. Ses premiers travaux ont porté sur les processus cognitifs impliqués dans l'évaluation du stress avec l'obtention de sa thèse en 2002 (Université de Nantes). A l'ouverture d'un cycle de formation en cybersécurité à l'UBS, ses recherches ont rejoint immédiatement les problématiques rencontrées, spécifiquement l'étude du comportement humain. Le « Cyber Range » (plateforme technique de simulation d'attaques cyber) de l'ENSIBS lui permet d'étudier comment les individus réagissent et interagissent en situation de crise : gestion du stress, charge mentale, phénomènes de coopération, leadership, modèles mentaux partagés pour gagner en efficacité... Ceci à l'aide de différents dispositifs de mesure de l'activité (eye-tracking, cardiofréquence-mètre, mesure de l'activité cérébrale, analyses des communications). Les problématiques des vulnérabilités orientent ses recherches sur la perception et la prévention des risques cyber. L'objectif est de rendre les utilisateurs d'outils informatiques et numériques véritablement acteurs de cette prévention par l'adoption de comportements sécurés.



Lien vers la biographie complète

Données essentielles

Doctorant.e.s : 2

Post-doctorant.e.s : 1

Publications : 14 - Stress & Health, Risk Analysis, CTW, PUR.

Conférences : 20 - HFES, SFP, ADRIPS, AIPTLF, AFPSA, SELF, ARPEGE.

Livre(s) : Le stress, 2012.

Collaborations internationales : Washington (USA).

35% de l'activité du chercheur
dédiée à la cybersécurité

Focus :
Recherche
Domaine applicatif

Domaine

Facteurs humains /
psychologie de la santé

Mots clés

Gestion de crise
Stress
Charge mentale
Soutien social
Management
Capacité d'adaptation
Prévention et Perception
des risques

Contact

laurent.guillet@univ-ubs.fr
+33668402262

Axe(s) de recherche

Modélisation du comportement.

Champs d'expertise

Gestion de crise.
Perception des risques.
Management des individus.
Animation d'équipe.
Acceptabilité.

Exemples d'applications

Gestion de crise au sein d'un centre opérationnel de sécurité.
Prévention et perception des risques de cybersécurité.

Responsabilités

Chef de Département BUT QLIO (Bachelor Universitaire de Technologie - Qualité,
Logistique Industrielle et Organisation) - IUT de Lorient.



Salwa ALEM

Laboratoire des Sciences et Techniques de l'Information de la Communication et de la Connaissance
Enseignante-chercheuse en cybersécurité industrielle

“

*La science ne doit plus être
exclusive mais faire partie
intégrante de la culture*

”

BIO

Ses études d'ingénieur télécom l'ont conduit à une thèse sur la détection d'intrusion pour l'Industrie du Futur menée en 2018 à l'UBS. Salwa Alem poursuit avec un post-doc sur la détection d'anomalies dans l'agroalimentaire, avant d'être recrutée en tant qu'enseignante-chercheuse à l'ENSIBS où elle partage ses connaissances en sécurité industrielle, logicielle, réseaux et virtualisation. Elle rejoint l'équipe IRIS du Lab-STICC en 2023 avec laquelle elle intervient notamment sur la détection d'intrusion et d'anomalies industrielles. Avec le projet Cyber Food, elle met ces détections au profit de la réduction du gaspillage alimentaire, de la dégradation nutritionnelle et du coût énergétique. Elle encadre un post-doc financé par l'AUB (association universitaire de Bretagne) sur cette même thématique. Salwa Alem travaille aussi en partenariat avec l'INERIS en intégrant facteurs humains et cybersécurité.



Lien vers la biographie complète

30% de l'activité du chercheur
dédiée à la cybersécurité

Focus :
Recherche
Domaine applicatif

Données essentielles

Post-doctorant.e.s : 1

Publications : 5, Cybersécurité industrielle

Conférences : AICCSA Abu D'habi 2019, CRISIS 2020 Paris, IFAC 2023 Japon, etc.

Collaborations internationales : Université d'Antananarivo (Madagascar), ENSA de Kenitra (Maroc).

Axe(s) de recherche

Détection d'intrusions.
Sécurité et la sureté des systèmes cyber-physiques.
Facteur humain et cybersécurité.

Champs d'expertise

Les systèmes cyber physiques (CPS).
La cybersécurité industrielle.
Les réseaux de neurones.

Exemples d'applications

L'industrie conventionnelle.
L'industrie 4.0.
Le secteur de l'agro-alimentaire.
Les systèmes d'information conventionnels.

Projets collaboratifs & Implications

CyberFood - Détection d'anomalies et d'intrusions dans l'industrie agro-alimentaire (équipe IRIS du Lab-STICC).
Cybersécurité et le facteur humain : l'analyse technique, opérationnelle et organisationnelle des pratiques et du comportement humain pouvant être une source de vulnérabilités dans l'industrie.

Domaine

Détection d'intrusion
et cybersécurité industrielle

Mots clés

Industrie 4.0
Systèmes de détection
d'intrusion (IDS)
Intelligence artificielle
Réseaux de neurones

Contact

salwa.alem@univ-ubs.fr
+33 (0)7 67 81 01 09



Pascal BERRUET

Professeur des Universités
Automatisme et génie industriel

“

*L'innovation passe par une
approche globale aux interfaces
entre les domaines*

”

BIO

Pascal Berruet rejoint l'Université Bretagne Sud en 1999 après avoir obtenu une thèse sur la reconfiguration des systèmes de production en 1998 à l'Ecole Centrale de Lille. Si ses objets de recherche sont restés sensiblement les mêmes (modélisation, système à évènement discret), il ouvre ses domaines applicatifs pour répondre aux limites des supports d'aide à la personne (handicap, domotique...). Plus globalement, dans une approche pluridisciplinaire, il intègre les problématiques du pilotage des systèmes socio-techniques complexes. En associant facteurs humains et automatismes, il s'intéresse à la coopération homme-machine pour aller au-delà d'une garantie de robustesse face aux pannes et aux attaques. Il propose également de sensibiliser le monde industriel aux attaques cyber et à l'apport des systèmes reconfigurables.

Données essentielles

Doctorant.e.s : 18

Post-doctorant.e.s : 2

Publications : 16 - JIM, H&T, SIMULATION, Computers in Industry, Applied Ergonomics, STH, etc.

Conférences : 90 - MOSIM, IEEE SMC, IFAC, IMACS, HMS, MSR, etc.

Livre(s) : 5 - "Advanced Manufacturing", Springer 2019 ; "Techniques de l'ingénieur", 2007, 2010 ; Productique Traité IC2, 2002.

Prix : prix de la meilleure thèse IFRATH 2013.

Brevet(s) : 1 - Dépôt logiciel : Appli conso (2016).

25% de l'activité du chercheur
dédiée à la cybersécurité

Focus :
Recherche
Domaine applicatif

Axe(s) de recherche

Pilotage des systèmes socio-techniques complexes.
Conception de systèmes socio-techniques sûrs et reconfigurables.
Optimisation de la coopération humain-machine.

Champs d'expertise

Systèmes à évènements discrets reconfigurables.
Surveillance supervision commande des systèmes.
Génération du contrôle commande.
Modélisation / simulation.

Exemples d'applications

Sécurisation au niveau capteurs/actionneurs des systèmes industriels.

Responsabilités

- Chef du département IUT QLIO (2018-2020).
- Vice-Président des relations socio-économiques et industrielles à l'Université Bretagne Sud (2012-2016).
- Responsable Master Gestion pilotage de la production en alternance (1999-2008).
- Pilote et coordinateur du projet SOLENN -12 partenaires 900 expérimentateurs autour de la maîtrise et sécurisation énergétique (2014-2018).
- ASIM (Projet e-santé) assistant pour la santé et la gestion des habitats domotisés (2012-2014).
- Diverses collaborations CIFRE autour de conception de la commande et des interfaces de supervision à partir de modèles métiers.

Domaine

Sureté des systèmes
complexes

Mots clés

Détection-réaction
aux attaques
Simulation conjointe
Systèmes socio-techniques

Contact

pascal.berruet@univ-ubs.fr
+33 (0) 6 66 94 97 15



Christine CHAUVIN

Professeur des Universités
Ergonomie cognitive

“ Les transitions rapides auxquelles sont confrontées les sociétés modernes génèrent de nouveaux défis qui ne peuvent être abordés que dans le cadre d’approches systémiques et interdisciplinaires ”

BIO

Titulaire d'un doctorat en ergonomie cognitive (obtenu en 1996 à l'Université René Descartes), Christine Chauvin a été recrutée à l'UBS en tant que Maître de Conférences en 1997. Habilitée à Diriger les Recherches en 2008, elle est Professeur des Universités depuis 2010. Ses travaux de recherche portent sur la prise de décision en situation dynamique, la gestion des risques et la coopération humain-machine dans des systèmes fortement automatisés. Ils sont principalement appliqués au domaine des transports (conduite de navire, véhicules autonomes, aviation) ainsi qu'à la gestion de crise. Ils visent à améliorer la performance, l'efficacité et la résilience des systèmes sociotechniques complexes. Ils s'inscrivent dans une réflexion plus générale sur l'impact des transitions numériques et industrielles sur les activités humaines et les organisations et dans un cadre interdisciplinaire, à la frontière entre sciences humaines et sociales et sciences de l'ingénieur.



Lien vers la biographie complète

Données essentielles

Doctorant.e.s : 15

Post-doctorant.e.s : 2

Publications : 37

Conférences : 75

Distinction(s) : Membre d'honneur de l'Association ARPEGE (Association pour la Recherche en Psychologie Ergonomique et Ergonomie).

Collaborations internationales : Université Memorial de Terre-Neuve (Canada), Université Sherbrooke (Canada), University of South Australia (UniSA), Feuerwehr Ludwigshaven (Allemagne).

25% de l'activité du chercheur dédiée à la cybersécurité

Focus :
Recherche
Domaine applicatif

Axe(s) de recherche

Fiabilité des systèmes sociotechniques.

Champs d'expertise

Modélisation des activités cognitives dans des situations dynamiques et complexes.
Identification des stratégies cognitives des opérateurs.
Identification des modes de contrôle cognitif.
Mesure de l'efficacité des opérateurs et des équipes.
Conception et évaluation d'Interfaces Humain-Machine.
Analyse des accidents.

Exemples d'applications

Mesure de l'efficacité d'opérateurs dans une situation de cyberattaque.
Analyse de l'efficacité d'équipes de pompiers en situations d'urgence.
Conception d'interface utilisant la Réalité Augmentée pour la supervision de véhicules autonomes.
Conception d'interface « écologique » pour le pilotage de sous-marin.
Analyse des Facteurs Humains et Organisationnels dans la survenue des accidents maritimes.

Responsabilités

- Vice-Présidente Relations Internationales à l'UBS depuis 2016.
- Responsable de l'équipe FHOX (Facteurs Humains et Organisationnels, Automatique et Systèmes Complexes) du laboratoire Lab-STICC de sa création jusqu'en 2020.
- Présidente de l'association nationale ARPEGE (Association pour la Recherche en Psychologie Ergonomique et Ergonomie) de 2012 à 2018.
- Responsable du Groupe Thématique « Prise de décision et gestion des risques en situation dynamique » au sein du GDR « Psycho-Ergo » de 2007 à 2011.

Domaine

Facteurs Humains
et Organisationnels

Mots clés

Prise de décision en situation dynamique,
Représentation mentale,
Gestion des risques,
Coopération Humain-Machine

Contact

christine.chauvin@univ-ubs.fr
+33 (0)2 97 87 45 21
+33 (0)6 86 07 53 36



Philippe COUSSY

Professeur des Universités
Électronique et informatique embarquée

“
*La recherche,
un espace de liberté
fantastique*
”

BIO

Issu de Paris6-Université Pierre et Marie Curie, Philippe Coussy obtient sa thèse sur la synthèse de haut niveau à l'Université Bretagne Sud en 2003. Il y est Maître de conférences en 2004, Habilité à diriger des recherches (HdR) en 2011, et Professeur des Universités en 2014. Ses activités de recherche se concentrent autour des architectures matérielles et des outils logiciels associés : synthèse de haut niveau d'accélérateurs matériels non programmables, génération automatique d'entrelaceurs mémoire sans conflit, architectures reconfigurables gros grains et outils de compilation associés, architectures de réseaux de neurones sur silicium, conception matérielle et logicielle. Depuis 2015 ses travaux s'ouvrent à la sécurité des systèmes embarqués. Ses recherches bénéficient de financements régionaux, nationaux et internationaux.



Lien vers la biographie complète

Données essentielles

Doctorant.e.s : 21

Post-doctorant.e.s : 6

Publications : 15 - IEEE (TCAD, D&T, TNNLS, TSP), ACM (JETCS, TECS), etc.

Conférences : 70 - DATE, ASP-DAC, ICCAD, FPL, ISCAS, ICASSP, SIPS, etc.

Livre(s) : 2 - "High-Level Synthesis: From Algorithm to Digital Circuit", 2008 Springer ; "Advanced hardware design for error correcting codes", 2008 Springer. Editeur associé IEEE Transactions on Computer Aided Design of Integrated Circuits and Systems (TCAD), IEEE Signal Processing Letters (SPL).

Distinction(s) : IEEE senior Member, membre du réseau d'excellence HiPEAC.

Brevet(s) : 6 - Procédé d'entrelacement, procédé d'architecture de réseaux de neurones, dispositif de tolérance aux fautes, cache active...

Collaborations internationales : Université de Bologne (Italie), ETH Zurich (Suisse), Université Polytechnique de Milan (Italie), Université de Californie à Los Angeles (USA), Université de Californie à San Diego (USA), Université McGill (Canada), Université de Brown (USA), Université de Palakkad (Inde)...

25% de l'activité du chercheur
dédiée à la cybersécurité

Focus :
Recherche
Domaine applicatif

Axe(s) de recherche

Architectures matérielles et outils logiciels associés.

Champs d'expertise

Synthèse de haut niveau - Conception électronique assistée par ordinateur (EDA Electronic Design Automation en anglais).

Exemples d'applications

Outil open-source de synthèse de haut niveau GAUT.

Responsabilités

- Directeur adjoint laboratoire Lab-STICC (depuis juin 2020).
- Directeur Adjoint Ed MathSTIC (2017-2020).
- Directeur du Master STIC puis Ingénierie des Systèmes Complexes (2015-2020).
- Responsable du pôle Communications, Architectures, Circuits et Systèmes (CACS) du Lab-STICC (2016-2020).
- Membre du comité scientifique du laboratoire commun LATERAL Thales/Lab-STICC (2018-).
- Membre élu au comité technique international IEEE Signal Processing Society, Design and Implementation of Signal Processing Systems (DISPS) (2011 à 2013, 2015 à 2021).
- Membre du comité d'évaluation ANR INS (2012-2014), ANR Micro-Nano CES 24 (2015-2017).
- Co-responsable du groupe disciplinaire Math-STIC de l'ED SICMA (2016-2017).
- Responsable du thème « Logiciels Embarqués et Architectures Matérielles » du GDR Soc-SIP (2011-2016).

Domaine

Méthode de conception
de composants
électroniques

Mots clés

Synthèse de haut-niveau
Architectures reconfigurables
gros grain et outil associé
Génération automatique
d'entrelaceurs mémoire
sans conflit
Architectures de réseaux
de neurones sur silicium

Contact

philippe.coussy@univ-ubs.fr
+33 (0) 2 97 87 45 65



Philippe RAUFFET

Maître de conférences
Automatique / Systèmes Humain-Machine

“ Pour faire face aux situations dynamiques et critiques, il faut penser les technologies et les nouveaux systèmes, non plus comme de simples outils, mais comme des co-équipiers interdépendants avec les opérateurs humains ”

BIO

Avec un diplôme d'ingénieur en Génie Industriel en poche en 2007, puis un doctorat en 2010 en Génie Informatique à l'Ecole Centrale Nantes, Philippe Rauffet rejoint l'Université Bretagne Sud, où il est Maître de Conférences depuis 2012 et habilité à diriger des recherches (HDR) depuis 2021. Il effectue une mobilité d'un an en Australie (2021-2022) - délégation CNRS - pour travailler sur des sujets de coopération hommes-machines. Ses travaux, combinant automatique, analyse du signal et sciences cognitives, s'inscrivent dans le paradigme Human-Autonomy Teaming (HAT) et visent à améliorer le fonctionnement d'équipes hybrides, dans lesquelles des opérateurs humains coopèrent avec des agents artificiels autonomes. Ses recherches sont réalisées dans le cadre de projets nationaux et collaborations industrielles internationales, principalement appliquées aux domaines de l'Industrie 4.0 et des transports. Depuis 2017, il a investigué le champ de la cyberdéfense pour analyser les processus de coopération humain-système et les mécanismes d'adaptation des opérateurs aux situations critiques et au stress.



Lien vers la biographie complète

Données essentielles

Doctorant.e.s : 6

Post-doctorant.e.s : 5

Publications : 14 - Cognition Technology and Work, Computers In Industry, Frontiers in Psychology, Le Travail Humain, International Journal of Technology Management, etc.

Conférences : 44 - IFAC Human-Machine Systems, IEEE on Systems, Man and Cybernetics, H-Workload, HFES European Chapter, IFAC World Congress.

Livre(s) : 6 chapitres - Human Mental Workload: Models and Applications, Springer, 2019, CCIS series, Springer, 2022.

Prix : Best papers à la 4e conférence internationale CHIRA (2020) et à la 13e conférence internationale IFAC HMS (2016).

Collaborations internationales : université d'Adélaïde (Australie), University of South Australia (Australie), IRL CNRS CROSSING (Australie), université d'Ariel (Israël), université de Stellenbosch (Afrique du Sud).

20% de l'activité du chercheur dédiée à la cybersécurité

Focus :
Recherche
Domaine applicatif

Axe(s) de recherche

Développement de méthodes pour la classification et le suivi des états cognitifs de l'opérateur.

Modélisation et conception de mécanismes d'adaptation des systèmes humains-machines au niveau de la répartition du travail et du dialogue.

Champs d'expertise

Modélisation et évaluation des mécanismes d'adaptation, au niveau individuel (mode de contrôle cognitifs) et au niveau collectif (allocation dynamique des fonctions, processus de gestion d'équipe).

Analyse et classification de signaux neurophysiologiques (fNIRS, ECG, Eyetracking).
Conception d'interfaces écologiques et transparentes.

Exemples d'applications

Détection de niveau élevé de charge mentale chez les opérateurs de drones et les pilotes de Rafale.

Reconfiguration dynamique d'interfaces de supervision pour réduire la charge mentale ou pour améliorer la confiance dans des systèmes de maintenance prédictive maritime.

Responsabilités

Responsable de l'équipe FHOOX (Facteurs Humains et Organisationnels, automatique et systèmes complexes) (2020 - *).

Responsable du pôle SHM (Systèmes Humains-Machines) du laboratoire Lab-STICC (2022- *).

Responsable de la Licence Professionnelle LOGIQ (2015 -*).

Nombreuses collaborations dans les domaines de l'Industrie 4.0 (ANR HUMANISM, ANR RODIC, ADEME SEANATIC) et des transports (ANR TAPAS, collaboration avec Renault, Airbus, Dassault Aviation et Thalès).

Soc-SIP (2011-2016).

Domaine

Human-Autonomy Teaming /
Systèmes Humains-Machines

Mots clés

Modélisation des systèmes
sociotechniques
Analyse et traitement
des données
neurophysiologiques
Automatisation et dialogue
humain-machine adaptatif

Contact

philippe.rauffet@univ-ubs.fr
+33 (0)6 71 61 14 08



UMR 6205

**LABORATOIRE DE
MATHÉMATIQUES
DE BRETAGNE ATLANTIQUE**

LMBA

105 membres dont :
60 Chercheurs (20 UBS)
25 Doctorants (13 UBS)

Le LMBA regroupe la majorité des mathématiciens dans l'Ouest Bretagne. Les thèmes de recherche représentés, couvrent une large partie des domaines mathématique, depuis les aspects théoriques jusqu'aux plus appliqués, tels que la géométrie algébrique et différentielle, la physique mathématique, la topologie et les groupes ; les systèmes dynamiques, les probabilités et la statistique ; le contrôle, les jeux différentiels, l'analyse numérique et le traitement de l'image.

3 grands thèmes sont organisés autour d'équipes et de séminaires :

- Géométrie et topologie ;
- Systèmes dynamiques, probabilités et statistique ;
- Analyse, phénomènes stochastiques et applications.

COLLABORATIONS SCIENTIFIQUES

France : 11 équipes de recherche (mathématiques, TIC, optique).

International : Nombreuses équipes de recherche (Allemagne, Canada, Grande-Bretagne, États-Unis, Chine, Colombie, Pérou, Brésil, Algérie, Vietnam, Japon, Russie, Espagne, Norvège).

Projets européens : Breuds (échange entre l'Europe et le Brésil) et Portonovo.

COLLABORATIONS INDUSTRIELLES

En France : plusieurs entreprises dans des domaines variés (énergie, défense, télécommunications, biostatistique, environnement).

LIEN
Vers le site du LMBA





Gilles DURRIEU

Professeur des Universités
Mathématiques Appliquées et Statistique

“
*De l'observation
à la prédiction*
”

BIO

Gilles Durrieu obtient son doctorat de mathématiques appliquées en 1997 à l'Université de Bordeaux, puis effectue un post-doctorat dans le cadre d'un contrat européen. Il est Maître de Conférences pendant 11 ans à l'Université de Bordeaux avant de rejoindre l'Université Bretagne Sud comme Professeur des Universités en 2010. La pluridisciplinarité et les collaborations à l'international teintent ses recherches dans les domaines des statistiques multidimensionnelles et de la modélisation de systèmes complexes. Ses travaux se penchent sur des questions liées à l'écologie (réchauffement global, biodiversité), mais aussi au médical avec des recherches sur le génome humain et la localisation de gènes responsables de pathologies complexes. Sa recherche concerne aussi le développement de modèles associés aux sciences des données et à l'intelligence artificielle pour la prédiction et la gestion des attaques cyber. Depuis novembre 2022 il est le doyen de la faculté des Sciences et Sciences de l'Ingénieur.



Lien vers la biographie complète

Données essentielles

Doctorant.e.s : 8

Post-doctorant.e.s : 3

Publications : 50 - Journal of Applied Statistics, Open Journal of Statistics, Statistical Inference for Stochastic Processes, Extremes, Journal of American Statistical Association, Environmetrics, etc.

Conférences : 105 (dont 45 invités) - SERA Brisbane (Australie), Journées de Statistique (Montpellier, Lille, Rennes, Bruxelles, Toulouse), French Mathematical Society (Vietnam), 20th International Conference on Computational Statistics (Chypre), Université de Toronto, 23rd International Biometric Conference, Genetic Analysis Workshop GAW15 (USA), etc.

Livre(s) : Handbook of Quantile Regression (Chapman & Hall /CRC Handbooks of Modern Statistical Methods 2017).

Prix : Primes d'excellence scientifique (PES) et primes d'encadrement doctoral et de recherche (PEDR) - depuis 2006.

Collaborations internationales : Université de Toronto (Canada), Université de la Nouvelle Calédonie, Université de Pittsburgh, Université de Rochester (USA), Universités Rockefeller et Columbia - New-York (USA), Université Santiago (Chili), etc.

25% de l'activité du chercheur
dédiée à la cybersécurité

Focus :
Recherche
Domaine applicatif

Axe(s) de recherche

Mathématiques appliquées.

Champs d'expertise

Apprentissage statistique, estimation non paramétrique, processus stochastique, régression fonctionnelle, théorie des valeurs extrêmes, modèles prédictifs.

Exemples d'applications

Suivi et qualité des eaux à partir du comportement animal.
Développement d'indicateurs mathématiques de restauration écologique de sites miniers de nickel (Nouvelle Calédonie).
Modélisation de stratégies de défense suite à une attaque cyber.

Responsabilités

- Doyen de la faculté des Sciences et Sciences de l'Ingénieur (depuis novembre 2022).
 - Directeur du LMBA-UBS (2015-2016).
- Directeur du département Mathématiques, Informatique et Statistique (2012-2016).
- Directeur du pôle Mathématiques et Statistique (2015-2017 et 2020 - 2022).
- Responsable de l'équipe Systèmes Dynamiques, Probabilités et Statistique du LMBA (2012-2015 et 2022-*).
- Responsable de formations (Licence, Master et CMI) depuis 2010.
- Responsable de l'axe de recherche Science de Données du LMBA (2019 -*).
- Membre élu du conseil d'administration de l'UBS et de l'Université de la Nouvelle Calédonie (2017-2019).
- Membre élu commission de la recherche (2012-2016) / formation et vie universitaire (depuis 2020) de l'UBS.
- Projet Ambition EcoDep - Paris Seine initiative d'Excellence (2020-2024).
- Responsable de la partie modélisation de projet RecoSynth (projet CNRT 2015-2017).

Domaine

Statistique

Mots clés

Science des données
Analyse de données
Modélisation
Valeurs extrêmes
Prédiction

Contact

gilles.durrieu@univ-ubs.fr
+33 (0) 2 97 01 71 78



EA 7480

**LABORATOIRE DE RECHERCHE
EN DROIT**

LAB-LEX

55 membres dont :
49 Chercheurs (18 UBS)
36 Doctorants (11 UBS)

Le laboratoire Lab-LEX concentre ses recherches sur 3 thématiques majeures :

- **La vulnérabilité** : l'appréhension de la notion de vulnérabilité appliquée aux personnes physiques, aux personnes morales, aux structures et aux espaces, et des instruments juridiques de la vulnérabilité dans les différents champs du droit privé, du droit public, du droit européen et des droits fondamentaux ;
- **La gouvernance** : analyse des différentes significations du terme de gouvernance des territoires (littoral, décentralisation et déconcentration), gouvernance européenne, gouvernance des entreprises (associations, coopératives, fondations), évolution de l'emploi dans les secteurs public et privé ;
- **Le contentieux** : recherches sur le renouvellement de l'office du juge (à travers les stratégies contentieuses, les politiques juridictionnelles, les modalités d'action en justice, la compréhension et l'exécution des décisions juridictionnelles) ; la notion de risque, la prévention et le traitement amiable des risques ; les modes alternatifs de règlement des conflits.

COLLABORATIONS SCIENTIFIQUES

France : notamment la Maison des Sciences de l'Homme en Bretagne (MSHB).

International : plusieurs universités (Italie, Espagne, Canada, Vietnam, Mexique, Colombie, Brésil, Costa-Rica, Canada).

PARTENARIATS AVEC LE MONDE PROFESSIONNEL

Entreprises, collectivités territoriales et administrations, hôpitaux, milieux associatifs, tribunaux et magistrature, barreau, notariat, gestionnaire de patrimoine...

LIEN
Vers le site du LAB-LEX





Michel SEJEAN

Professeur des Universités
Droit privé et sciences criminelles

“

*Le juriste doit contribuer à ce que
notre société se développe grâce à
des technologies qui sécurisent la
liberté au lieu de la surveiller*

”

BIO

Diplômé de l'Institut Supérieur d'Interprétation et de Traduction (ISIT, Paris), Michel Séjean a poursuivi, en parallèle, des études de droit et a choisi l'Université Bretagne Sud en 2013 à l'issue du concours d'agrégation en droit privé et sciences criminelles. Il développe des recherches en droit civil comparé et participe à plusieurs traductions de codes civils et de commerce, en France et aux États-Unis. En 2018, il entreprend de se former à la cybersécurité, une discipline peu connue des juristes. Il obtient une certification à HarvardX ainsi que le grade d'auditeur de l'Institut des Hautes Études de Défense Nationale (IHEDN) sur la souveraineté numérique et la cybersécurité. Il est membre des bureaux de Cyber : UBS ainsi que de la Chaire CYBER de l'IHEDN.

Membre associé du Lab-LEX, il est aujourd'hui professeur à l'Université Sorbonne Paris Nord.



Lien vers la biographie complète

Données essentielles

Doctorant.e.s : 7

Publications : 27- La Gazette du Palais, Trans Europe Experts, Recueil Dalloz, Revue Lamy Droit civil, Bulletin Joly Sociétés, La Semaine juridique, Sécurité&Défense, Revue internationale de droit comparé, etc.

Livre(s) : 4 - Le Code de la cybersécurité, 1^{ère} éd. 2022, Dalloz (directeur scientifique) ; Le Code civil trilingue français-anglais-arabe, LexisNexis 2020 ; L'Europe de la cybersécurité, Trans Europe Experts 2019 ; L'index de la sécurité juridique/ The Index of Legal Certainty, Dalloz 2018.

Collaborations internationales : Louisiana State University, Baton Rouge - 2021 (USA).

Domaine

Droit du numérique

Mots clés

Assurance de risques cyber
Cybersécurité des territoires
Identité numérique
Confidentialité numérique
Souveraineté numérique

Contact

michel.sejean@univ-paris13.fr
+33 (0)6 62 84 47 45

Axe(s) de recherche

Droit de la sécurité des systèmes d'information.
Droit de la lutte contre la cybercriminalité.
Droit de la cyberdéfense nationale.

Champs d'expertise

Législation interne, européenne et internationale de la cybersécurité.

Responsabilités

Membre du bureau de Cyber : UBS.



EA 2652

**LABORATOIRE D'ÉCONOMIE
ET DE GESTION DE L'OUEST**

LEGO

125 membres dont :
100 Chercheurs (34 UBS)
25 Doctorants (7 UBS)

Le Laboratoire d'Économie et de Gestion de l'Ouest est composé d'une équipe de chercheurs pluridisciplinaires spécialisés en sciences économiques et en sciences de gestion dont la vocation est d'aider à créer, développer et diffuser la connaissance.

COLLABORATIONS INDUSTRIELLES

Collaboration avec **Enedis** : projet SOLENN (Solidarité, Énergies, Innovation).

CONTRATS DE RECHERCHE

- **ALIMDURABLE** : développement des pratiques alimentaires durables au sein d'un territoire ;
- **COAGUL** : COmmunautés, Activité, réGULations
- **COMPNUM** : compétences numériques et employabilité subjective des stagiaires et alternants issus de l'enseignement supérieur en fin de cycle.
- **NUTRICHIC** : alimentation des personnes âgées au Centre Hospitalier de Cornouaille (Quimper)
- **SESAME** : étude autour de l'outil « Sésame Relationnel ».
- **TEXSENS** : perception, sens et utilisation de la texture des aliments par le consommateur.

GROUPEMENT DE RECHERCHE SCIENTIFIQUE

M@rsouin (Môle Armoricain de Recherche sur la SOciété de l'information et les Usages d'INternet).

LIEN
Vers le site du LMBA





Christine PETR

Professeur des Universités
Marketing et usages numériques

“

*Celui qui a la prétention
de chercher ne doit jamais
cesser d'apprendre*

”

BIO

Depuis sa thèse soutenue en 1998 à l'Université Rennes 1, Christine Petr interroge les comportements des usagers des mondes du tourisme, de l'art et de la culture. Dès 2005 elle s'associe au GIS Marsouin sur la question des usages du numérique, et s'intéresse particulièrement au e-tourisme. En tant qu'enseignante-chercheur, Christine Petr est intervenue dans différentes institutions (IUT Saint Briec, IAE Rennes, IAE Tours, SciencesPo Rennes), avant de rejoindre l'Université Bretagne Sud en 2015. Elle consacre ses recherches aux effets et évolutions des comportements de l'individu dans l'usage d'outils numériques. Depuis 2018, ses thématiques de recherches restent consacrées aux secteurs de l'art et du tourisme, mais se concentrent plus spécifiquement sur le lien entre sensibilité à la protection des données personnelles et hygiène du numérique, ce qui implique la cybersécurité.



Link to full biography

Données essentielles

Doctorant.e.s : 9

Post-doctorant.e.s : 2

Publications : 32 - IJAM, Management & Avenir, JMT, Tourism Management, Arts Marketing, RAM, DM, etc.

Conférences : 113 - IMTC, AFM, HTSF, AIMAC, etc.

Livre(s) : 7 ouvrages, 29 chapitres - L'Urgence de l'hygiène numérique: le monde d'après les données (PUR à paraître), Théories et Pratiques du marketing de la culture et du tourisme dans un monde d'innovation (2022) ; Le marketing du Tourisme (Dunod, 2010.2015), L'Accueil international: concepts et cas de management (De Boeck, 2011), 10 cas de Communication (Dunod, 2015.2020), etc.

Prix : Prix du meilleur article JTTM 2009.

Vidéographie : Experiencing Contemporary Arts : a Reexamination of Fun, Feeling and Fantasy, 2015.

Collaborations internationales : Université Udayana - Bali (Indonésie), Université La Sagesse - Beyrouth (Liban).

 25% de l'activité du chercheur dédiée à la cybersécurité

Focus :
Recherche
Domaine applicatif

Axe(s) de recherche

Analyses des usages numériques.

Champs d'expertise

Types et degrés de pratique du numérique.
Transformation numérique.
Sensibilité perçue des données individuelles.
Empowerment des utilisateurs.

Exemples d'applications

Sensibilisation des utilisateurs à la protection de leurs données personnelles
Implication des utilisateurs dans le système de partage des données au profit du collectif.

Responsabilités

- Responsable Pédagogique de la Licence L3, Option Marketing Vente (depuis 2019).
- Membres de différentes commissions de l'UBS depuis 2015 (Recherche, CAC, CFVU...).
- Membre du Comité Scientifique de l'Institut Archipel, Institut de Recherche de l'Université Bretagne Sud sur la Mer et le Littoral (depuis 2019).
- Directrice du Laboratoire IREA-Lego Vannes (2015-2018).
- Responsable de projets de recherche sur les usages du numérique (depuis 2005).
- Conseil scientifique du GIS Marsouin - www.marsouin.org
- Reviewer revues et congrès internationaux.
- Co-porteur du GIT AFM - Innovations et Marketing de la Culture et du Tourisme.

Domaine

Utilisateurs

Mots clés

Utilisations
Impacts
Appropriation
Addictions
Déviations
Empowerment
Confiance
Information marketing

Contact

christine.petr@univ-ubs.fr



Vanessa SERRET

Professeur des Universités
Sciences de gestion - finance organisationnelle & gouvernance d'entreprise

“
La cybersécurité ne saurait se limiter à ses aspects techniques. Il est important d'avoir une approche multidisciplinaire (politique, économique, managériale, juridique et technologique) de la cybersécurité en général
”

BIO

Vanessa Serret rejoint l'Université Bretagne Sud en tant que Maître de Conférences après une thèse en gestion de portefeuille soutenue à l'Institut d'Administration des Entreprises (Université d'Aix-Marseille, 2002). Entre 2000 et 2017 elle est invitée à plusieurs reprises à l'Université de Sherbrooke au Canada où ses recherches portent sur la démocratie actionnariale, puis à HEC Montréal en 2017 pour travailler sur le fonctionnement des conseils d'administration des sociétés. Ses travaux sur la gouvernance et la responsabilité sociétale des organisations lui permettent d'aborder le champ de la cybersécurité du point de vue du management et de la structuration des organisations. Pour prévenir les attaques et leurs conséquences, elle invite à construire une culture organisationnelle performante et à se livrer à une analyse sensible du coût des attaques cyber. En septembre 2020, elle est Professeur des Universités à l'IAE school of management de Metz, au sein de l'Université de Lorraine.



Lien vers la biographie complète

Données essentielles

Doctorant.e.s : 5

Publications : 40 - Management international, Revue Française de Gestion, Finance Contrôle Stratégie, Revue de Gestion des Ressources Humaines, Corporate Social Responsibility and Environmental Management, International Journal of Business and Management, Revue Française de Gouvernance d'Entreprise, Ressources policy, RIBAF, etc.

Conférences : 60 - CIG, AFC, EURAM, AFFI, ADERSE, RIODD, etc.

Livre(s) : 4 - Finance DSCG 2 (Dunod, 2019) ; Analyse Financière (Hachette, 2011) ; Principes d'Analyse Financière (2009).

Prix : Best Paper Award EURAM 2015.

Collaborations internationales : Université de Sherbrooke (Canada), HEC Montréal (Canada), Université de Georgetown (USA).

20% de l'activité du chercheur dédiée à la cybersécurité

Focus :
Recherche
Domaine applicatif

Axe(s) de recherche

Finance et gouvernance d'organisation.

Champs d'expertise

Activisme actionnarial.
Rémunération des dirigeants.
Démocratie actionnariale.
Fonctionnement des conseils d'administration.
Impact des attaques cyber sur les marchés financiers.

Exemples d'applications

Réponse du conseil d'administration aux actionnaires concernant la gestion du risque cyber.
Evaluation des coûts de destruction de valeur.

Responsabilités

- Responsable de l'équipe Finance Comptabilité Contrôle du laboratoire CEREFIGE (2020 -*).
- Membre élue du conseil du laboratoire CEREFIGE (2022 - *).
- Membre élue du Conseil d'Administration de l'Association Académique Internationale de Gouvernance (2021-2027).
- Présidente du Comité d'Organisation de la Conférence Internationale de Gouvernance 2023.
- Membre élue du conseil de l'école doctorale d'économie & gestion (2017-2020).
- Membre élue à la commission recherche (2017-2020).
- Responsable d'axe du laboratoire IREA (Institut de recherche des entreprises et administrations, 2014-2016).
- Membre du conseil de la maison de la recherche de l'UBS (2007-2010).

Domaine

Gouvernance du risque cyber

Mots clés

Coût des attaques cyber
Gestion du risque cyber

Contact

vanessa.serret@univ-lorraine.fr
+33 (0)6 63 03 88 72



Jack NOEL

Ingénieur innovation cybersécurité

BIO

Jack NOEL est un ancien colonel des forces armées françaises ; au cours de ses 30 ans de service, il a occupé divers postes (en France et à l'étranger) en guerre électronique/cyber, connaissance/anticipation, contre-ingérence (y compris cyber) et relations internationales.

Il rejoint ensuite l'Université Bretagne Sud où il est actuellement ingénieur d'innovation cybersécurité, coordinateur de la communauté Cyber:UBS et animateur avec le professeur Guy GOGNIAT de l'écosystème Cyber et Intelligence de la donnée.

Son travail consiste à faire l'interface entre l'université, les acteurs socio-économiques, les entreprises ou les agences de l'Etat dans les domaines de l'enseignement, la recherche et l'entraînement à la gestion de crise cyber.

Il donne également différents cours et a dirigé la création du premier MOOC de l'UBS en cybersécurité. Il est titulaire de deux masters (relations internationales et politiques de gestion publique), ainsi que de divers diplômes et certificats militaires supérieurs (Ecole de Guerre, Académie du renseignement, etc.).

● **DES TALENTS DIVERSIFIÉS**
● **D'HORIZONS DIVERS**
EN ACCOMPAGNEMENT
DE LA DYNAMIQUE
DES LABORATOIRES



Sébastien GUILLET

Enseignant-chercheur en informatique

“

Je ne dirais pas que ce modèle est faux, je dirais qu'il n'a pas marché.

”

BIO

Sébastien Guillet travaillait dans les méthodes formelles pour la sécurité des systèmes dynamiques à événements discrets lorsqu'il a transité vers l'enseignement. Après une thèse soutenue en 2012 sur la modélisation et le contrôle de la reconfiguration dynamique et partielle des architectures reconfigurables, et deux post-doc appliqués à la domotique pour l'aide au handicap puis à la cybersécurité industrielle, il arrive à l'UBS en 2018 en tant qu'enseignant dans la filière cyberdéfense pour transmettre son savoir en programmation et rétroingénierie. Ses travaux de recherches concernent l'IDM et la théorie du contrôle, mais aussi aujourd'hui les problématiques liées à la collecte de données pour la modélisation et la prise de décision en cyberdéfense.



Lien vers la biographie complète

100% de l'activité du chercheur dédiée à la cybersécurité

Focus :
Recherche
Domaine applicatif

Domaine

Modélisation pour le raisonnement tactique et l'aide à la décision pour la définition numérique en lien avec les systèmes d'information.

Mots clés

TALN
(traitement automatique du langage naturel)
Scrapping
MITRE

Contact

Sebastien.guillet@univ-ubs.fr



Jérémie BUISSON

Maître de Conférences
Informatique

“

*La recherche,
c'est aussi l'humilité intellectuelle
au quotidien*

”

BIO

Jérémie Buisson soutient sa thèse en 2006 à l'INSA de Rennes sur l'autoadaptation des logiciels de calculs scientifiques. En post-doctorat à Telecom Bretagne (IMT Atlantique), il travaille sur l'architecture des logiciels embarqués en satellites et les problématiques de mises à jour en continuité de service (projet ANR). Recruté en 2009 à l'Université Bretagne Sud, il est détaché au ministère des Armées, aux Ecoles de St-Cyr Coëtquidan pour l'Armée de Terre pendant 14 ans. En 2023, il a rejoint l'Ecole de l'air et de l'espace. Depuis 2008 ses travaux de recherche s'intéressent à la reconfiguration dynamique, puis plus particulièrement aux systèmes de systèmes avec une démarche évolutionnaire et à la sécurité par la conception. Il participe à la création de l'équipe Archware de l'IRISA en 2012 autour de ces questions. Les méthodologies de conception et processus d'ingénierie sont aujourd'hui au cœur de ses travaux, que ce soit pour le domaine de la Défense ou de la cybersécurité.



Lien vers la biographie complète

Focus :
Recherche
Domaine applicatif

Données essentielles

Doctorant.e.s : 4

Publications : 3 - JSS, etc.

Conférences : 25 - SoSE, CBSE, etc.

Collaborations internationales : Université de Constantine (Algérie),
Université de Yaoundé (Cameroun).

Axe(s) de recherche

Ingénierie des systèmes de systèmes.
Sécurité par la conception.

Champs d'expertise

Architecture logicielle.
Reconfiguration dynamique.
Ingénierie dirigée par les modèles.

Responsabilités

Directeur adjoint du Mastère spécialisé « Conduite des opérations et gestion des crises en cyberdéfense » (2015 - 2022).

Domaine

Génie logiciel

Mots clés

Systèmes de systèmes
Architecture
Evolution

Contact

jeremy.buisson@irisa.fr



Aurélie JAMMET

Enseignante-chercheuse en Management

“ *Appréhender la cybersécurité en tant que système sociotechnique est la meilleure manière d'aider les organisations à améliorer leur résistance et leur résilience face aux attaques qu'elles subissent* ”

BIO

Après un doctorat en management des organisations et des politiques publiques à Paris Tech, soutenu en 2010 sur la gouvernance des politiques publiques de transports en Bretagne, elle s'est consacrée à l'entrepreneuriat. Aurélie Jammet est arrivée en septembre 2019 à l'ENSIBS en tant qu'enseignante, puis enseignante-chercheuse en 2021. Elle transmet son savoir sur le management et l'entrepreneuriat, et réalise du suivi de projets sur l'hygiène numérique, le risque humain et la résilience organisationnelle. Elle coordonne aussi des séminaires sur les facteurs humains pour les étudiants en cyberdéfense, et les exercices de gestion de crises. Ses recherches se penchent particulièrement sur les risques industriels avec les chercheurs de l'INERIS dans une approche pluridisciplinaire et systémique de la cybersécurité. Son objectif est de rendre les organisations plus fortes pour réduire les vulnérabilités ou limiter l'impact des attaques.



Lien vers la biographie complète

50% de l'activité du chercheur dédiée à la cybersécurité

Focus :
Recherche
Domaine applicatif

Domaine

Vulnérabilités humaines et organisationnelles face aux risques numériques

Mots clés

Management de la cybersécurité
Protection et résilience organisationnelle face aux risques numériques
Hygiène numérique
Gouvernance et analyse des risques
Approche sociotechnique

Contact

aurelie.jammet@univ-ubs.fr



Jean PEETERS

Professeur des Universités
Études anglophones et sociolinguistique de la traduction

“
*Dans un monde de plus en plus
numérique, point de liberté sans
cybersécurité*
”

BIO

Jean Peeters a été président de l'Université Bretagne Sud de 2012 à 2020, période pendant laquelle la cybersécurité est devenu un axe stratégique de développement et de rayonnement de l'UBS. Auditeur diplômé de l'Institut des Hautes Études de Défense Nationale (IHEDN) pour sa session nationale Souveraineté numérique et cybersécurité (2018-2019), il est, depuis septembre 2020, titulaire de la chaire de recherche du même institut intitulée Cyber et souveraineté numérique. Il est aussi responsable du master européen Erasmus Mundus, CYBERUS, porté par l'UBS en collaboration avec l'Université du Luxembourg, l'Université Libre de Bruxelles et TalTech en Estonie.



Lien vers la biographie complète

Focus :
Recherche
Domaine applicatif

Champs d'expertise

Initier, coordonner et piloter des projets en cybersécurité.

Responsabilités

Titulaire de la chaire Cyber et souveraineté numérique de l'IHEDN (2020 -*).
Responsable du master Erasmus Mundus CYBERUS (2021- *).
Président de l'Université Bretagne Sud (2012-2020).

Contact

jean.peeters@univ-ubs.fr
+33 (0)6 75 85 65 69



Julie LASSALLE

Chercheuse indépendante
Psycho-ergonomie

“

*Co-concevoir des instruments
pour le développement du pouvoir
d'agir des individus*

”

BIO

Après une première approche des sciences cognitives sur le sujet de la qualité audiovisuelle et la manière dont les outils pouvaient contraindre l'utilisateur dans le cadre d'une thèse Cifre Orange Labs Lannion en collaboration avec l'IMT et l'UBS, Julie Lassalle a mené un post-doctorat sur la charge mentale des pilotes de chasse. Elle a ensuite étudié l'appropriation des technologies sur les questions de consommations énergétiques et du développement du pouvoir d'agir des individus via les usages développés. La question du pouvoir d'agir peut aussi se transposer à la cybersécurité en transférant les mêmes méthodes de l'ergonomie pour améliorer la sécurité au sein de l'entreprise et répondre aux enjeux contemporains sans ajouter de charge mentale. Chercheuse indépendante, elle travaille en collaboration étroite avec le Lab-STICC et veille à faire redescendre vers les entreprises les constats des études menées pour engager des actions avec différents acteurs et développer des outils adaptés, reconstruire des règles de travail, ramener du sens et étudier la question de la souffrance au travail. Elle s'interroge sur le poids de l'organisation et le pouvoir d'agir pour développer les compétences et l'autonomie des individus en situations professionnelles en participant à la création d'environnements capacitants quel que soit le domaine d'activité.



Lien vers la biographie complète

20% de l'activité du chercheur
dédiée à la cybersécurité

Focus :
Recherche
Domaine applicatif

Données essentielles

Doctorant.e.s : 2

Publications : 4

Conférences : 13

Collaborations internationales : Université de Plymouth, université de Portsmouth.

Axe(s) de recherche

Création d'environnements capacitant à partir de méthodes de co-conception.
Conception de systèmes socio-techniques appropriables.

Champs d'expertise

Étude de l'acceptabilité.
Étude de l'appropriation.
Analyse de l'activité.

Exemples d'applications

Création d'une interface pour la maintenance prédictive maritime.
Favoriser l'acceptabilité d'un filet de pêche biodégradable.
Comprendre et favoriser l'appropriation des technologies smart-grids pour la transition énergétique.
Participation à la création d'une interface pour l'allocation dynamique des tâches humain-système.

Responsabilités / Projets collaboratifs

SEANATIC (projet Ademe) - conception d'une interface de maintenance maritime prédictive.
INDIGO (projet collaboratif européen) - étude de l'acceptabilité d'un filet de pêche biodégradable.
SOLENN (PIA Ademe) - consultation en temps réel de la consommation et développement de la maîtrise utilisateur.

Domaine

Psychologie / ergonomie
cognitive

Mots clés

Charge mentale
Acceptabilité
Pouvoir d'agir
Co-construction
Analyse de l'activité
Analyse systémique
Environnement capacitant

Contact

julie.lassalle@univ-ubs.fr



- **THÈSES CYBER**
- **À L'UBS DEPUIS 2014**

Delphine BEAULATON

Détection automatique de vulnérabilités dans les systèmes de systèmes

Maria Teresa MENDEZ REAL

Déploiement sécurisé d'applications sur des architectures many core

Vincent MIGLIORE

Cybersécurité matérielle et conception de composants dédiés au calcul homomorphe

Fatma SBIAA ZAYEN

Modélisation et analyse de la sécurité au niveau système des primitives cryptographiques

Thomas TOUBLANC

Sécurisation matérielle de capteurs/actionneurs distribués sur des réseaux industriels

Raounak BENABIDALLAH

Identification automatique des situations à risques dans les systèmes informatiques : cas des systèmes embarqués

Ghita HARCHA

Introduction d'aléas dans les architectures matérielles pour une contribution à la sécurisation de chiffreurs AES dans un contexte IoT

Maria MUSHTAQ

Prise en compte des attaques par canaux auxiliaires lors de l'allocation des ressources au sein des MPSoC

Salwa ALEM

Cybersécurité des équipements connectés industriels : modélisation, détection et performances temporelles en présence d'intrusions des systèmes cyber-physiques de l'usine 4.0

Hicham LALAOUI HASSANI

Contribution à la sécurisation de la communication M2M par la proposition d'une architecture de sécurité dynamique et hétérogène

Nathalie BOULDOUKIAN

Détection automatique des vulnérabilités de code à l'aide de l'exploration de données graphiques

Valentin DURAND DE GEVIGNEY

Modèles d'apprentissage automatique pour la détection multimodale de comportements anormaux

Nan ZHANG (MESSE)

Cybersécurité des systèmes de systèmes par des méthodes d'ingénierie des exigences dirigées par les modèles

Timo ZIJLSTRA

Accélérateurs matériels sécurisés pour la cryptographie post-quantique

Noura AIT MANSSOUR

Sécurisation matérielle de processeurs embarqués face aux attaques logiques et physiques

Elia Christy FIKANY

Simulation de systèmes de systèmes pour l'identification de vulnérabilités

Monica BUITRAGO RAMIREZ

Mesurer et garantir le niveau de sécurité d'une architecture de systèmes de systèmes

Fabrice LOZACHMEUR

Extensions cryptographiques pour processeurs embarqués (RISC V)

Johann MILON

Étude de vulnérabilités physiques de crypto-systèmes embarqués

Mohamed EL BOUZZATI

Processeur radio logicielle faible consommation pour la flexibilité et la sécurité

Nicolas GAUDIN

Développement et évaluation d'un processeur RISC-V robuste face à des attaques par canaux auxiliaires

William PENSEC

Protection d'un processeur avec DIFT contre des attaques physiques

Philippe CHARTON

Formalisation d'exercices de gestion de crise : une approche dirigée par modèles

Ahmed ELMARKEZ

Security by design pour une conception sécurisée des systèmes industriels SCADA

Tianxu LI

Contribution à la conception de mécanismes de sécurité matérielle pour une passerelle IoT sécurisée contre les attaques sans fil

Qiyang LI

Protection de la vie privée lors d'externalisation des données par des applications mobiles et IoT

Jesus Antonio SANCHEZ-RAMOS

Actifs et menaces dans l'architecture sécurisée d'un système de systèmes

Jeisson Andrés VERGARA VARGAS

L'assurance de la sécurité dans l'évolution architecturale des systèmes logiciels basés sur le Web

Sidbewendin Angélique YAMEOGO

Une démarche XAI pour la caractérisation et la conceptualisation des Fake News

Hongwei ZHAO

Architecture de communication sécurisée d'un SoC vis-à-vis des attaques physiques et logiques

Paul PERROTIN

Analyse de la vulnérabilité humaine dans les systèmes de systèmes socio-techniques

Ayoub BOURHIM

Concevoir pour le développement des pratiques préventives en cybersécurité

ZOOM LES DOCTORANT.E.S EN CYBERSÉCURITÉ À L'UBS



Noura AIT MANSOUR a un parcours d'ingénierie au Maroc. A l'occasion d'un stage de fin d'étude au LIP6 (Sorbonne Université) elle découvre le monde de la recherche et choisit de continuer sur une thèse. Sous la direction d'Arnaud Tisserand, Guy Gogniat et l'encadrement de Vianney Lapôtre, elle se penche sur la protection d'un processeur face aux attaques physiques, notamment les attaques par injection de fautes. A peine soutenue, elle est recrutée par Secure-IC pour œuvrer à la protection et l'évaluation des circuits. Elle aimerait garder cette mobilité entre le travail en entreprise, l'enseignement et la recherche.



Ayoub BOURHIM réalise une thèse sur les facteurs humains dans la cybersécurité avec deux laboratoires de l'UBS, le Lab-STICC et le LEGO. Il est encadré par Christine Petr, Julie Lassalle et Laurent Guillet pour travailler sur la mise en place d'environnements capacitants et la perception du risque cyber. Il apporte la richesse de son parcours en psychologie sociale et dynamiques cognitives pour étudier les facteurs individuels et organisationnels et permettre à terme de co-construire de nouveaux modèles de sécurité. Le doctorant, venu des universités de Nîmes et Montpellier, envisage de poursuivre dans la recherche et l'enseignement.



Monica BUITRAGO a suivi des études d'ingénieurs en télécommunication en Colombie avant de rejoindre l'UBS pour une thèse sur la mesure et la conception d'architectures sécurisées de systèmes. Ses travaux, encadrés par Isabelle Borne et Jérémy Buisson, s'inspirent des « security patterns » afin de quantifier dans quelle mesure l'architecture logicielle est conforme aux patterns comme les points d'entrée protégés d'un sous-système. C'est à la recherche qu'elle souhaite se consacrer.



Philippe CHARTON réalise une thèse sur la formalisation d'exercice de gestion de crise sur une approche dirigée par les modèles, sous la direction de Salah Sadou. Le but est de constituer un ou plusieurs langages pour pouvoir modéliser des exercices, en vue de les automatiser et d'y appliquer des contraintes en fonction des domaines. En parallèle, il est enseignant en cybersécurité à l'école d'ingénieurs ENSIBS. C'est une reprise d'études qu'il effectue, satisfaisant son goût pour la recherche et pour la vulgarisation.



Mohammed El Bouazzati travaille sur un processeur de communication pour les objets connectés, sécurisé et flexible. Cette thèse dirigée par Guy Gogniat et Philippe Tanguy, vise à protéger des failles et attaques venant du réseau. Il travaille à concevoir un mécanisme qui va prendre modèle du comportement légitime du système et comparer les données prélevées en temps réel pour déceler une intrusion. Après un parcours au Maroc alliant systèmes embarqués et télécommunication, il rejoint l'Enseirb-Bordeaux qu'il double avec un master en systèmes électroniques avant de se concentrer sur la cybersécurité. Il donne également des cours de programmation défensive dans le Master européen Cyberus Mundus.



Nicolas GAUDIN est arrivé au Lab-STICC en 2021 pour réaliser sa thèse sur le développement et l'évaluation d'un processeur RISC-V robuste face à des attaques par canaux auxiliaires, sous la direction de Guy Gogniat, Vianney Lapôtre et Pascal Cotret (ENSTA Bretagne Brest). Son objectif est de venir greffer des mécanismes de sécurité sur les architectures matérielles de systèmes embarqués qui vont contre les attaques logicielles. Il envisage un travail en R&D en entreprise.

ZOOM LES DOCTORANT.E.S EN CYBERSÉCURITÉ À L'UBS



Tianxu LI travaille sur la maintenance contre les attaques sans fil pour l'IoT, qu'elles soient matérielles ou logicielles, à travers une thèse encadrée par Guy Gogniat et Philippe Tanguy. Après une licence en Chine, il est arrivé en France pour des études d'ingénieurs sur les systèmes embarqués à Polytech Montpellier. Au cours d'un stage, il s'est penché sur un système de surveillance des patients pour la prise de médicament. La santé fait partie des domaines extrêmement sensibles des objets connectés. Il envisage de poursuivre la recherche et de devenir enseignant pour partager ses connaissances.



Fabrice LOZACHMEUR réalise une thèse Cifre avec Thalès, dirigée par Arnaud Tisserand depuis novembre 2020. Son travail consiste à réaliser des extensions cryptographiques pour des processeurs embarqués. Il veille alors à développer des implémentations matérielles et étudie les chiffrements dans l'objectif d'étendre le jeu d'instruction et de protéger contre les attaques physiques. L'internet des objets en expansion, leur protection devient un enjeu majeur, aussi s'intéresse-t-il beaucoup aux attaques par canaux auxiliaires. Etudiant à Lorient en licence Sciences du numérique, ainsi qu'une licence de mathématique à distance, il valide ensuite un master Cybersécurité des systèmes embarqués dans cette même ville. Après sa thèse, il souhaite se tourner vers l'enseignement.



Nan MESSE a mené une thèse de doctorat financée par la DGA. Initialement tournée sur la sécurisation des systèmes de systèmes en utilisant l'IDM, elle a été amenée à proposer une assistance de sécurité aux architectes de systèmes. Etudiante chinoise, elle arrive en France en 2013 et réalise un Master SeCRéTS (Sécurité des Contenus, des Réseaux, des Télécommunications et des Systèmes) à l'UVSQ (Université Paris-Saclay). A l'UBS, elle enseignait aux licences, à l'IUT et aux écoles de St Cyr Coëtquidan. C'est à la recherche et l'enseignement autour de la sécurité et du génie logiciel qu'elle se destine.



William PENSEC est arrivé à l'UBS en 2021 pour réaliser une thèse sur la protection d'un processeur DIFT contre les attaques physiques. Après un cursus en informatique à Brest, il se concentre aujourd'hui sur les processeurs open source et les IoT. Les cours qu'il dispense depuis sa thèse lui confirment son goût pour la transmission et lui font envisager une carrière d'enseignant-chercheur.



Paul PERROTIN a soutenu sa thèse en 2022 (financement par la Chaire CyberNavals) sur l'analyse de la vulnérabilité humaine dans les systèmes de systèmes socio-techniques. Sous la direction de Salah Sadou, il s'est intéressé aux représentations de la vulnérabilité et à la conception de systèmes plus sécurisés en prenant en compte la vulnérabilité humaine. Il poursuit ses travaux par un post-doc à mi-temps.



Benabidallah RAOUNAK a mené une thèse sur l'identification automatique des situations à risque dans les systèmes logiciels à l'Irisa. Issue d'un master en Intelligence Artificielle de l'Université des sciences et de la technologie Houari Boumediene - Alger, elle utilise les technologies IA au service de la cybersécurité, en orientant les développeurs vers les zones à risques. Si ce type de profil est très recherché dans le monde de l'industrie, c'est à la recherche et à l'enseignement que l'étudiante souhaite se consacrer. En parallèle de ses recherches, elle a enseigné en licence informatique et a encadré des projets.

ZOOM LES DOCTORANT.E.S EN CYBERSÉCURITÉ À L'UBS



Jesus SANCHEZ est arrivé de Colombie où il a suivi un parcours d'ingénieur en télécommunication, il rejoint le laboratoire IRISA en 2023 pour une thèse sur la sécurité de la conception de systèmes de systèmes. Il s'assure que les modèles soient sécurisés et anticipe les mesures de sécurité pour défendre et prévenir les attaques dans différents scénarios réactifs.



Angélique YAMEOGO a démarré une thèse en 2022 au sein de l'IRISA sur une démarche XAI pour la caractérisation et la conceptualisation des Fakes news. Après un master en cybersécurité, elle s'est intéressée à la détection des fake news lors de stages effectués au Burkina Faso et au Luxembourg, en utilisant des techniques d'intelligence artificielle. Elle met ses compétences au service de la cybersécurité pour faciliter l'identification et la compréhension des campagnes de désinformations utilisant des fake news.



Hongwei ZHAO est doctorant au sein de l'équipe de recherche ARCAD du laboratoire Lab-STICC. Après trois ans d'études universitaires en Chine, il rejoint Telecom St Etienne et obtient son diplôme d'ingénieur en 2020. Ses travaux de thèse, portant sur l'étude d'architectures de communication de SoC robustes face à des attaques logiques et physiques, sont dirigés par Vianney Lapôte et Guy Gogniat. Après son doctorat, il envisage de devenir enseignant-chercheur.



Timo ZIJLSTRA
C'est autour de l'implémentation d'accélérateurs matériels sécurisés pour la cryptographie post-quantique que Timo ZIJLSTRA, étudiant néerlandais, a conclu sa thèse. Arrivé en France en 2015, après une licence de mathématiques à l'université de Groningen, son goût pour l'algèbre l'a conduit à la cryptographie via un Master mathématiques et cryptographie à Rennes. Il a ensuite été accueilli au sein du Lab-STICC, laboratoire d'unité mixte de recherche CNRS-UBS, sous la direction d'Arnaud Tisserand, avec une thèse CNRS financée par la Région Bretagne et la DGA. Recruté à Bordeaux, Timo a choisi d'apporter son expertise au monde de l'entreprise.

ILS NOUS SOUTIENNENT



ACTEURS PÉDAGOGIQUES ET DE RECHERCHE



CONTACT

Cyber : UBS

Campus de Tohannic
Rue Yves Mainguy BP 573
56017 VANNES CEDEX
www-cybersecuritycenter.univ-ubs.fr
Tel. +33 (0)2 97 48 50 57
cyber@univ-ubs.fr