1 Synthèse

PASCAL LAFOURCADE
MCF HDR Hors Classe Section 27
https://sancy.iut-clermont.uca.fr/~lafourcade/
LIMOS, Campus des Cézeaux
63170 Aubière

Né le 26/04/1977, à Toulouse
Marié, nationalité française
Téléphone : 06.83.54.90.70.
pascal.lafourcade@uca.fr

Parcours

2016- Maître de conférences Hors Classe à l'Université Clermont Auvergne, IUT d'Aubière département Informatique, Laboratoire d'Informatique, de Modélisation et d'Optimisation des Systèmes LIMOS (UMR 6158), Axe 2 SIC, thème Réseaux et Sécurité.

2013-16 Chaire industrielle confiance numérique Université d'Auvergne, LIMOS, UMR 6158, Équipe Réseaux et Protocoles, IUT d'Aubière département R&T.

2007-13 Maître de conférences à l'UJF, UFR IM2AG, Laboratoire VERIMAG UMR 5104.

2006-07 Bourse post-doctorale DGA, ETH Zürich.

2003-06 Bourse doctorale, ENS Cachan.

Diplômes

- *6 novembre 2012*, **Habilitation à diriger des recherches** de l'Université de Grenoble, « *Computer-Aided Security for Encryption Schemes, Voting protocols and Wireless Sensor Networks* », soutenue devant le jury : David POINTCHEVAL (Président), Gilles BARTHE (Rapporteur), Pr. Hubert COMON-LUNDH (Rapporteur), Pr. Ralf KÜSTERS (Rapporteur), Pr. David BASIN (Examinateur), Pr. Yassine LAKHNECH (Garant), Pr. Peter RYAN (Examinateur).
- *25 septembre 2006*, **Doctorat d'informatique** de l'École Normale Supérieure de Cachan, mention *très honorable*, intitulé « *Vérification de protocoles cryptographiques en présence de théories équationnelles* », obtenue devant le jury : Claude KIRCHNER (Président), Pr. Yassine LAKHNECH (Rapporteur), Pr. Lucas VIGANÓ (Rapporteur), Pr. Denis LUGIEZ (co-directeur), Pr. Ralf TREINEN (co-directeur), Dr. Yannick CHEVALIER (examinateur).
- **Diplôme Universitaire ACTA** (Analyse Cognitive des Techniques d'Apprentissage) de l'ENS Cachan obtenu le 29 septembre 2006, mention *assez-bien*.
- **DEA**, mention bien, Représentation de la Connaissance et Formalisation du Raisonnement, UPS Toulouse III, *juin 2003*.
- **Maîtrise d'informatique fondamentale**, mention assez-bien, UPS Toulouse III, *juin 2002*.
- **Maîtrise de mathématiques fondamentale**, UPS Toulouse III, *juin 2001*.

2 Investissement pédagogique

2.1 Synthèse

De 2007 à 2013, j'étais maître de conférences (MCF) à l'Université Joseph Fourier (UJF) à Grenoble avec une décharge les 2 premières années, j'ai principalement enseigné la **logique** [DLL12a], la **programmation fonctionnelle** [CLM14] et la **sécurité informatique** [DLR15]. De 2013 à 2016, j'étais titulaire de la Chaire de confiance numérique avec un service maximum de 64h à l'Université d'Auvergne (UDA). En 2016 j'ai été recruté comme MCF au département Informatique à l'IUT d'Aubière à l'Université Clermont Auvergne (UCA). J'enseigne dans le cadre du BUT et DUT les **bases de données, la méthodologie d'apprentissage, et les mathématiques**. Je participe également aux soutenances et suivis des stagiaires et alternants du département (au minimum 30 par an). En Licence professionnelle à l'IUT, j'enseigne la **sécurité Web**.

À l'Institut d'Informatique de l'UCA, j'enseigne en anglais à l'ISIMA et au Master international la Sécurité des systèmes d'information et les modèles de sécurité. J'enseigne aussi la blockchain à l'ESC de Clermont (École Supérieure de Commerce) et la sécurité pour la Data Science à SIGMA Clermont.

Universités	Années	Cours	TD	TP	Total EqTD
UCA	21-22	64	115	135	346.0
	20-21	41	117	130	308.5
	19-20	37	125.5	140	321.0
	18-19	34	120	113	284.0
	17-18	36	108	103	265.0
	16-17	13	196.5	102	318.0
UDA	15-16	22	12	20	65.0
	14-15	22	12	20	65.0
	13-14	22	12	20	65.0
UJF	12-13	132	48	15	261.0
	11-12	127	48	15	253.5
	10-11	132	20	15	233.0
	09-10	110	24	12	201.0
	08-09	74	32	18	161.0
	07-08	74	32	18	161.0
Total	15 ans	940.0	1022.0	876.0	**3308.0**

Pour mes enseignements, j'ai mis en place des dispositifs pédagogiques innovants.

— En Licence professionnelle, j'ai réalisé une « *mission cryptographique* » [1]. Il s'agit d'un **escape game en ligne** qui permet de découvrir la cryptographie. Cette idée a donné lieu à un ouvrage « *25 énigmes ludiques pour s'initier à la cryptographie* » chez Dunod co-écrit avec Malika More [LM21a].

1. https://sancy.iut-clermont.uca.fr/~lafourcade/mission-crypto.html

— Dans les **cours de méthodologie**, nous mettons en situation via des exercices pratiques et ludiques les étudiants pour qu'ils découvrent quelles sont les techniques d'apprentissage qui leur correspondent le mieux. Cet enseignement se base sur l'ouvrage co-écrit avec Isabelle Lebrun [LL15].
— Dans les cours de sécurité à l'Institut d'Informatique, mais aussi en Licence professionnelle, je demande aux étudiants de se mettre en groupes de 4 ou 5 et de construire un exposé de 30 minutes ainsi qu'une séance de TP sur une faille ou une attaque en sécurité informatique. Cette **pédagogie active** est largement appréciée par les apprenants. Ces cours se basent sur les ouvrages en sécurité que j'ai co-écrits [DLR+22, DLTV18, DLR15, DL20].
— En base de données, dans le cadre du BUT, j'ai proposé deux SAÉ (Situations d'Apprentissage et d'Évaluation) originales qui donnent aux étudiants une grande **liberté pour apprendre**. Ces SAÉ font appel à des compétences de inter-disciplines : éco, math, anglais.
    1. Le premier sujet consiste à ce que chaque groupe de 4 ou 5 étudiants imagine la société de leurs rêves et réalise la BD pour la gestion de leurs stocks. Une partie analyse économique de l'entreprise est aussi demandée.
    2. Le second sujet consiste à ce que les étudiants choisissent des données ouvertes pour les structurer dans une BD. Ils doivent ensuite utiliser des outils de visualisation à l'aide des outils mathématiques pour décider si les données sont exploitables pour monter une entreprise. Une présentation de leur visualisation est réalisée en anglais.
— En mathématiques à l'IUT, je fais travailler les étudiants en **autonomie en groupe**, cette **pédagogie inversée** est fortement appréciée des étudiants.
— Pour les cours à l'ESC et à SIGMA, j'ai mis en place une **évaluation par projet libre**. Les étudiants doivent réaliser un document sur la mise en place du RGPD (Règlement Général sur la Protection des Données) pour l'entreprise de leurs rêves. Cette approche concrète permet à des non spécialistes d'appréhender les enjeux de la sécurité dans leur cadre professionnel.

2.2 Présentation des enseignements

Je présente les enseignements que j'ai créé de puis 2013 à l'UCA, je ne présente pas les cours crées à Grenoble qui ont donné lieu à deux ouvrages [CLM14, DLL12a] en plus des polys de cours et exercices réalisés durant mes 6 premières années de maître de conférences. Le détail de mes enseignements est disponible en Annexe A, le nombre d'étudiants correspond au nombre de personnes inscrites au cours et le volume horaire indiqué est pour 1 groupe de TD suivant le cours, sachant que j'ai souvent plusieurs groupes. Je commence par les enseignements à l'IUT où les séances d'enseignement font 2h.

— **DUT 2A, FI, 5 TD + 5 TP, 140 étudiants, 60h EQTD. Programmation et administration des bases de données**. J'ai repris ce cours en seconde année en écrivant un polycopié et en changeant totalement la méthode d'enseignement. En effet, au début de chaque séance les étudiants passent un contrôle de connaissances. Ensuite l'évaluation et la correction sont effectuées de manière anonyme par d'autres étudiants. Ce dispositif leur permet d'évaluer chaque semaine ce qu'ils ont appris d'une séance à l'autre. Cela leur permet aussi de se rendre compte comment l'évaluation s'effectue, ce qui est très formateur et leur apprend

donc à mieux rédiger leurs copies.

— **Licence Professionnelle, 7 CM + 7 TP, FI/FC, 30 étudiants, 48h EQTD. Sécurité Web**. Lors de mon recrutement au département Informatique de l'IUT, j'ai créé ce cours qui est très pratique car il comporte 50% de TP. De plus, je suis une pédagogie active dans ce cours : les étudiants font des présentations par groupes de 4 sur les principales attaques en sécurité Web. Chaque groupe crée un mini-TP qui est réalisé par l'ensemble de la classe. J'ai aussi réalisé une "*Mission Cryptographie*" en ligne (il s'agit d'une sorte d'escape game) pour les initier de manière ludique aux notions de cryptographie [DLR15, DLR+22, DLTV18, LM21a] [2].

— **BUT 1A, 1 CM + 5 TD, 140 étudiants, 12 EQTD. Séances de méthodologie**. J'ai conçu ces 6 séances pour les primo entrants du département informatique grâce au livre [LL15] co-écrit avec Isabelle Lebrun. Une séance en amphi montre les fondements de l'apprentissage. Nous abordons en TD la mémorisation, l'attention, la résolution de problèmes, la gestion des émotions, et la motivation. Ces séances sont pour les étudiants une réélle prise de conscience des différences de rythme et de volume travail entre le lycée et l'IUT.

— **BUT 1A, 4 CM + 10 TD + 5 TP, 140 étudiants, 48 EQTD. Base des mathématiques**. Dans ce nouvel enseignement du BUT, j'ai proposé d'enseigner les mathématiques qui servent aux informaticiens, avec pour chaque notion une application en informatique concrète. J'ai conçu les séances de TP et participer à l'élaboration des TD et cours. Ce cours couvre la numération, la théorie des ensembles, l'algèbre de Boole, la logique propositionnelle, l'arithmétique modulaire, les dénombrements.

— **Licence Professionnelle RT, 8 CM, 40 étudiants, 8 EQTD. Introduction à la sécurité**. Pendant la chaire de confiance numérique de 2013 et 2016 j'ai créé ce cours pour donner les bases en cryptographie afin qu'ils puissent comprendre les termes qui seront utilisés dans le reste de la formation. Cet enseignement est actuellement dispensé par mes doctorants.

À l'institut d'Informatique, lors de la refonte des Masters, j'ai créé les deux cours suivants en anglais pour les parcours M2 GLIA, SIAD et ICS :

— **M2, 6 CM + 6 TD + 1 TP, 40 étudiants, 26 EQTD. Sécurité des Systèmes d'Information**. Cet enseignement donne les bases de la sécurité pour les systèmes d'information. Les principales primitives cryptographiques sont présentées ainsi que les attaques les plus connues.

— **M2, 6 CM + 6 TD + 1 TP, 15 étudiants, 24 EQTD. Modèles pour la sécurité**. Dans ce cours les notions élémentaires pour modéliser la sécurité des protocoles et primitives cryptographiques sont présentées. Nous abordons aussi les fondements des preuves de sécurité.

Dans d'autres composantes :

— **M2, 4 CM + 1 TD, 20 étudiants, 10 EQTD. Introduction à la sécurité pour Data scientist (SIGMA)**. J'ai créé ce cours pour l'école d'ingénieur SIGMA Clermont. Le RGPD et la sécurisation des données sont les deux principaux axes développés dans ce cours de sensibilisation à la sécurité des données.

— **M2, 6 CM, 20 étudiants, 12 EQTD. Introduction à la technologie blockchain (ESC Clermont).** J'ai créé ce cours d'introduction à la blockchain pour donner les connaissances essentielles pour mieux comprendre la transformation numérique de notre société aux étudiants en commerce.

2. https://sancy.iut-clermont.uca.fr/~lafourcade/mission-crypto.html

2.3 Responsabilité pédagogique

Je suis responsable des cours que je donne, cela consiste à réaliser les supports de cours, les sujets de TD, TP, et examens, mais aussi à recruter les vacataires car à l'IUT nous avons 10 groupes de TP et 5 groupes de TD par année.

Je suis membre élu du conseil du département depuis 2017 et membre de de la Commission Technique et Informatique du département, cette commission gère les choix pour les infrastructures et logiciels du département qui comptent un parc de plusieurs centaines de machines.

Je suis membre actif de l'Institut de Recherche des Enseignements des Mathématiques (IREM) de Clermont-Ferrand où je suis :

- **Responsable du groupe Informatique au lycée**. Ce groupe réunit des enseignants du lycée de l'académie et réfléchit comment développer des ressources pour la mise en place des nouveaux programmes avec l'apparition de l'informatique au lycée. Je suis intervenu sur les parties sécurité et codage de l'information au Diplôme Universitaire spécialité Numérique et Sciences Informatiques (NSI) de l'UCA. Nous avons conçu des activités et projets pour le lycée à dispositions des enseignants (un livret de plus de 200 pages est en cours de finalisation sortie prévue fin 2022).
- **Membre du groupe Informatique au collège**, nous réfléchissons comment mettre en œuvre l'introduction de l'informatique au collège. Dans ce cadre nous avons réalisé plus de 20 journées de formation à Scratch lors de la réforme du collège.
- **Membre du groupe Informatique Sans Ordinateur**, nous concevons de nombreuses activités, et effectuons des interventions dans plusieurs classes de primaire, collège et lycée pour présenter ces activités débranchées [3].

Avec des collègues du département informatique, nous avons mis en place des **grilles critériées pour l'évaluation des rapports et soutenances de stages et de projets**. Ce travail nous permet une évaluation plus claire et transparente pour les étudiants en leur donnant les compétences à atteindre. Cela facilite l'harmonisation des notes entre les différents jurys.

Ouvrages J'ai co-écrit 9 ouvrages en lien direct avec mes ensignements et ma pédagogie :

- 3 sur la sécurité informatique : un sur la Blockchain [DLTV18] un sur les NFT et un sur les PKI [DLR15].
- 1 sur des énigmes ludiques pour s'initier à la cryptographie [LM21a].
- 1 sur les méthodes d'apprentissage, comment s'exercer à apprendre ? [LL15].
- 1 sur la programmation fonctionnelle [CLM14].
- 1 sur la logique [DLL12a].
- 1 ouvrage collectif sur l'Informatique Sans Ordinateur [Col17].
- 1 ouvrage collectif sur les défis en cybersécurité [DL20].

3. http://www.irem.univ-bpclermont.fr/Informatique-sans-ordinateur-IREM

2.4 Diffusion, rayonnement, activités internationales

Diffusion. Je suis très attaché à la diffusion des savoirs, à la médiation scientifique et à la pédagogie [LM21b, JLMP20, Laf17, DDFLM18, HBB+15, HDB+12, Laf11b, Laf11a, DP10, DGL07]. C'est naturellement que je suis un des co-fondateurs du groupe informel national sur l'Informatique Sans Ordinateur, dans lequel nous créons des activités pour faire de la médiation scientifique. Nous avons co-écrit un numéro spécial de Tangente [Col17]. De plus avec le groupe de Clermontois nous avons publié un article sur un tour de magie [DDFLM18].

En juin 2018 lors de l'école de médiation de la SIF (Société Informatique de France) à Toulouse, avec 3 collègues, nous avons formé pendant 3 jours une trentaine d'enseignants et doctorants à la conception d'action de méditation scientifique. Nous avons co-construit des ateliers avec les participants dont un a donné lieu à une publication internationale [JLM+20].

J'ai également co-animé une journée de la médiation à Paris organisée par la SIF, 60 participants, formation d'enseignants aux activités d'informatique sans ordinateur (juin 2019).

J'ai aussi animé une journée de formation à la médiation scientifique organisée par l'INRIA à Bordeaux en le 18 décembre 2019. Cette formation a permis de sensibiliser plus de 50 personnes. Lors de cette formation Emmanuelle Saillard a pu concevoir une activité sur le parallélisme [4].

En 2021, j'ai co-écrit avec Malika More un article dans le magazine informatique « Programmez » pour expliquer la récursivité.

Médiation. Je réalise régulièrement des activités de médiation scientifiques :

— Chaque année, je propose des activités autour de la cryptographie à la **fête de la science** au sein de l'UCA. Nous accueillons en moyenne 120 jeunes (4 classes de 30 élèves).

— Je réalise des interventions dans des établissements en 2021 en visio classe de première dans un lycée à Toulouse, en 2022 en présentiel au collège à Massiac et au lycée à Montluçon dans le respect des contraintes sanitaires.

— Membre actif de l'association « Les maths en scène » [5], depuis 2019 je participe à l'organisation du **festival annuel** qui accueille plus de 1000 personnes.

Enfin, je participe aux journées « **Filles et maths** » initiées par les associations « Femmes et mathématiques » et Animath sont destinées aux lycéennes afin de les sensibiliser aux études scientifiques. Cela peut être une démarche individuelle ou de groupe, menée par un enseignant du secondaire. Participer à l'organisation de telles journées me semble important afin de changer les mentalités et d'attirer plus de filles dans les filières informatiques. Dans ce cadre je suis intervenant dans les RJM [6] organisées par l'association Filles et Maths en novembre 2020, 2021 et 2022 sur le campus des Cézeaux. Pendant trois journées des jeunes lycéennes de première et terminale vont découvrir les métiers possibles en mathématiques et informatique.

Bourse Erasmus Mundus. De 2014 à 2017, j'ai bénéficié d'une bourse Erasmus Mundus avec l'Université de Monastir en Tunisie. J'ai effectué plusieurs séjours chaque année pour donner des

4. https://pixees.fr/une-histoire-de-macons-et-de-parallelisme/
5. lesmathsenscene.fr
6. Rendez-vous des Jeunes Mathématiciennes, https://filles-et-maths.fr/rendez-vous-des-jeunes-mathematiciennes/

cours en anglais sur la sécurité informatique. J'ai également participé au montage de la maquette pédagogique de leur Master afin d'avoir une offre de formation cohérente avec le corps enseignant. Cette collaboration a également donné lieu à deux productions scientifiques [BLGR18, BLGR17].

Écoles d'été internationales.

1. École d'été de cybersécurité à Nice, 17 juin 2019, 4h00 de cours sur la blockchain, 40 étudiants en thèse plus des industriels et enseignants.
2. École d'été *Mathinfoly 2019*, du 24 août 2019 au 31 août 2019, à Lyon, 50 étudiants de L1 à M1 pendant 1 semaine. Cours d'introduction à la logique, introduction à la cryptographie, introduction à la blockchain et réalisation de 10 projets par groupe de 5 pour résoudre des jeux logiques en utilisant un SAT solveur.

3 Activité scientifique

3.1 Synthèse

Ma recherche s'articule autour de la sécurité assistée par ordinateur. Je m'intéresse à formaliser les propriétés de sécurité des protocoles de communication et développer des techniques de vérification automatique pour ces protocoles. Je conçois aussi des méthodes de preuves assistées par ordinateur pour prouver la sécurité des primitives cryptographiques. Mes recherches s'articulent autour des thématiques suivantes :

— Modélisation et analyse de protocoles cryptographiques d'e-vote, d'e-vente aux enchères, d'e-examen, d'e-cash, de calculs distribués dans le cloud et pour la Blockchain [DLTV18]. Projets BPI D4N [7] (2021-2024) et ANR SEVERITAS [8] (2021-2025).
— Analyse de primitives cryptographiques sécurisées (ANR DECRYPT 2019-2023 [9]).
— Protocoles de communication sécurisés pour la 5G (ANR MOBIS5 2019-2023 [10]) et les capteurs sans fils.
— Réseaux de capteurs, communications des véhicules connectés (C-ITS [11]), respect de la vie privée (*privacy*) des communications sans fil (Projets européens C-ROADS [12] et INDID [13]).

*M*ots clefs : Vérification formelle, sécurité, cryptographie, privacy, protocoles cryptographiques, réseaux de capteurs, sécurité de la 5G, communications sans fils, blockchain, calculs distribués sécurisés dans le cloud.

7. https://limos.fr/news_project/271
8. https://severitas.univ-grenoble-alpes.fr/
9. https://decrypt.limos.fr/
10. https://mobis5.limos.fr
11. Cooperative Intelligent Transport Systems
12. https://www.c-roads.eu/
13. Infrastructure Digitale de Demain

3.2 Publications et productions scientifiques

Titulaire de la PEDR/PES/PEDR depuis 2008. D'après `Google Scholar` [14], j'ai un h-index [15] de 26, un i10-index [16] de 68, un nombre de citations maximum pour une publication est de 222 et un nombre total de citations est de 2375. Le tableau ci-dessous classe par type mes publications [17], entre parenthèses celles pour la **période 2013-2022** depuis mon arrivée au LIMOS.

Revues Internationales	Conférences Internationales	Livres en français
38 (**32**)	109 (**94**)	9 (**7**)

Présentation des 5 publications : Parmi mes 147 publications internationales avec comité de lecture, j'ai choisi de présenter 5 publications récentes de rang A : 3 dans des journaux internationaux de rang A et 2 dans des conférences de rang A. Ces publications illustrent, dans la mesure du possible, les différents domaines de mes travaux de recherche.

Dans les revues internationales de rang A :

1. [ASNK+21] (IEEE Transactions on Dependable and Secure Computing (TDSC 2021)) Nous avons proposé un système qui construit des preuves de localisation respectueuses de la vie privée de usagers. Ces preuves peuvent servir pour attester que l'on est bien allé à un endroit tout en respectant notre vie privée. Une preuve de concept a été réalisée sur smartphone Android.
2. [GLMS20] (Artificial Intelligence (AI [18] 2020)) Nous avons trouvé des attaques différentielles sur le chiffrement symétrique AES en utilisant la programmation par contraintes. Cette approche est plus rapide que les approches existantes jusqu'à lors et a permis de trouver une attaque optimale de manière automatique et reproductible.
3. [CLMS22] [19], (Journal of Artificial Intelligence Research (JAIR 2022)), nous avons proposé une approche générique pour sécuriser des algorithmes qui maximisent les récompenses en fonction d'un budget dans le contexte de bandits manchots et dans un contexte de ressources distribuées et fédérées.

Dans les conférences internationales de rang A :

1. [BDF+21] (Computer Security Foundations Symposium 2021 (CSF 2021)) Nous avons étudié la sécurité des protocoles de communications sans fils des cartes Master pour les paiements. Nous avons proposé un nouveau modèle de sécurité et trouvé des failles de sécurité grâce à l'outil de vérification automatique Easycrypt.
2. [BBLPK21] (Financial Cryptography and Data Security 2021 (FC 2021)) Nous avons proposé une construction générique pour obtenir des preuves à divulgation nulle de connaissances pour des tests d'égalité et d'inégalité.

14. https://scholar.google.fr/citations?user=Wnz50YUAAAAJ
15. Le *h-index* est le nombre de publications h le plus élevé qui ont eu au moins h citations chacune.
16. Le *i10-index* correspond au nombre de publications avec au moins 10 citations.
17. Le déséquilibre entre conférences et revues s'explique car dans la communauté les conférences sont plus considérées que les revues. Par exemple d'après DBPL le 10 avril 2022 : D. Pointcheval médaille d'argent du CNRS (2021) a 19 revues pour 148 conférences ; V. Cortier médaille d'argent du CNRS (2022) a 26 revues pour 80 conférences.
18. revue de rang A* d'après CORE.
19. https://github.com/gamarcad/paper-samba-code

Rang	Revues 18 A et 17 B	Conférences 17 A et 69 B
A*/A	TDSC [CDLS22, ASNK+21] JAIR [CLMS22] Information Sciences [BCF+21] TCS [LMM+21, BDDL20, DELL16] AI [GLMS20] CS [DLP+18, DLOP17] FMSD [KFL17] JAR [GLLSN16, CDE+10] DC [BLM+16] IC [LLT07, DLLT08] Journal of Computer Security [DDL15, CDL06]	ICDE (Demo) [MCL+22] CP [LDLS21] SoCG [FLLM22, CdFG+21] CSF [BDF+21] FC[BBLPK21, BL19] ISWC Demo[CL20a] TrustCom [CLLS20] COCOON[DLM+19b] LCN [KLL14c, MCL14b] ESORICS [GLL13, DLL12c] CCS [CDE+08a] ICALP [DLLT06] RTA [LLT05]
B	Journal of Computer Security [DDLR21, CLLS22, DLM+19a] CC [RMLM21] CC [CYLR21] CC [RML+21] IPL [LL20, GLMS18] WMBUCDA [NRLSL21] CCIS [AYBGL19] ICTMCS [AGLM17] WN [ADJL16] JSAN[MCL15, MCL14a] CCIS[DGK+15a] DAM[GADL14] AUMCS [KL07]	PKC [CLPK22, BLL+19] ICDCN [BDL21] SAC [BFJ+22] CiE [MLMR21] SSS [LMMR20, BDD+18] FUN [BDD+22, BDL20a, MTS+20, BDDL18, BDDL16, DJL14] SECRYPT [LRS21, LRS20a, CKY+19a, CGLY19a, CGLY19b, CGLY18, DLM+17, BLGR17, DPP+17, GABL17, BBL16b, DLOP16, DKL15, DGK+14, JL14b] DBSec [CL20b] SAC [FJL+22] ARES [ELLR20, BCGL17, BL16b] NETYS [BDL20b, RBD+21] IWSEC [DLF+19] PROVSEC [CDLS20, BDG+17] WISE [JLM+20, LMNS19] ICTAC [CKY+19b] SIRCOCCO [BDL19, ADGL12] EMMECIS [CYLR18] RICS [BDG+18] AsiaCCS [ABG+17] FSE [SGL+17] CANS [BL17] WiSec [BGLO17, BGG+16] IndoCrypt [GL16] IFIP SEC [BL16a] ISPEC [LMM+19, CLLS19, DGK+15b] SAFECOMP [PPL16] AdHocNets [AGLM15] RV [KFL15] ADHOCNOW [MRC+14] AsiaCCS [DJL13] DCOSS [ADJL13b] AfricaCrypt [DDL13, FLA11] FOSSACS [DELL13] POST [DLL13] ICC [DLL12b] IIHMSP [TWE+10] ASIAN [GLLS09a] FAST[LTV09]

Ranking d'après Scimago et Core, en fonction des années, certains classement changent.

Code open source. Certains de mes articles ont donné lieu à du code open source, pour permettre aux chercheurs de reproduire les résultats expérimentaux de nos articles. Je présente ci-dessous des liens vers des dépôts Git publics, les articles pertinents pour chaque code.

— [CLLS22, CLLS20] https://github.com/radu1/secure-ucb
— [MCL+22] https://github.com/gamarcad/samba-demo
— [CLMS22] https://github.com/gamarcad/paper-samba-code
— [CDLS22] https://github.com/anatole33/SR-secure
— [CL20b, CL20a] https://github.com/radu1/goose
— [CDLS20] https://github.com/anatole33/LinUCB-secure
— [CLLS19]
https://gitlab-sds.insa-cvl.fr/vciucanu/secure-bai-in-mab-public-code

3.3 Encadrement doctoral et scientifique

Depuis mon arrivée au LIMOS, j'ai encadré les 6 thèses soutenues :

— (2014-2018) 100% Xavier Bultel financé par la chaire de confiance numérique, actuellement MCF au LIFO. [BBLPK21, BL19, BLL+19, BDLM17, BCG+18, BDDL18, BDG+18, BDD+18, BCGL17, BL17, ABG+17, BDG+17, BL16b, BBL16a, BDDL16, BL16a, BBL16b, BGG+16]
— (2015-2018))100% David Gérault financé par un projet DIS4 de la Région Auvergne, actuellement chercheur à Abou Dabi [GLMS20, GLMS18, SGL+17, ABG+17, BDG+17, BGLO17, GL16, BGG+16].
— (2016-2019) 50 % Matthieu Giraud financé par un projet DIS4 de la Région Auvergne, actuellemnt chez CryptoNext [BDG+18, BDG+17, BCGL17, CGLY19a, CGLY19b, CGLY18, BCG+18, BLGR17].
— (2017-2020) 30 % Marwa Chaieb financé par un collaboration avec la Tunisie, actuellement enseignante à Tunis [CKY+19b, CKY+19a, CYLR18].
— (2018 -2021) 50 % Mirko Koscina financé par un bourse Cifre avec Be-Ys, CTO de Be-Pay [CKY+19b, CKY+19a].
— (2018 - 2021) 50 % Marius Lombard-Platet financé par un bourse Cifre avec Be-Ys, actuellement Post-Doc au Luxembourg [CLLS19, LPL19, LL20, CLLS20, CLLS22, NRLSL21].

J'ai encadré 17 Masters 2 et 11 thèses soutenues. J'encadre actuellement 5 doctorants (*cf.* Annexe C). J'ai aussi encadré 3 post-doctorants dont 1 au LIMOS : Luc Libralesso en 2020-2021 projet ANR DECRYPT. Malgré la pandémie, nous avons obtenu d'excellents résultats avec 3 conférences de rang A [LDLS21, CdFG+21, FLLM22] et 1 journal de rang A [RML+21].

3.4 Diffusion et rayonnement

— Membre du **comité ANR CES** 38 cybersécurité, appel à projet 2016 et 2017. Évaluation de plus de 70 demandes de financement.
— En 2017 membre de 5 **comités de sélection de MCF** à Lyon Limoges et Grenoble (en 2017), en 2021 à Toulouse (en 2021), à Paris Créteil (en 2022).
— Organisateur du **séminaire Confiance Numérique** d'octobre 2013 à juin 2017. Dans le cadre de la chaire de confiance numérique, j'ai organisé un séminaire mensuel à Clermont-Ferrand. A chaque mois, 2 orateurs sont venus parler au séminaire, pour un total de plus de

60 intervenants. Tous les exposés sont filmés et disponibles en ligne [20].

J'ai été membre du jury d'HDR de Gérard Chalhoub (le 22 juin 2016 à l'Université d'Auvergne), Radu Ciucanu (le 9 juin 2021 à l'Université d'Orléans) et Cristina Onete (le 23 mars 2022 à l'Université de Limoges) et j'ai été 17 fois rapporteurs et 5 fois membres du jury de thèses en plus des thèses dirigées.

17 fois rapporteur de thèse

1. Thèse de Georgia Tsaloli, "*Secure and Privacy-Preserving Cloud-Assisted Computing*", le 15 juin 2022 à l'Université de Chamlers (Suède).
2. Thèse de Mohamed Traoré, "*Analyse des biais de RNG pour les mécanismes cryptographiques et applications industrielles*", le 23 mai 2022 à l'Université Grenoble Alpes.
3. Thèse de Neals Fournaise, "*Protocoles cryptographiques pour le respect de la vie privée*", le 4 janvier 2022 à l'Université de Limoges
4. Thèse de Rolland Kromes, "*Conception d'une architecture spécifique Low Power pour les accès Blockchain et Smart Contracts des plateformes IoT*", le 8 décembre 2021 à l'Univ de Côte d'Azur.
5. Thèse de Dang Truong Mac, "*Certain Types of Code-Based Signatures*", le 30 novembre 2021 à l'Université de Limoges
6. Thèse d'Alexandre Gonzalvez, "*Affiner la déobfuscation symbolique et concrète de programmes protégés par des prédicats opaques*", le 2 juin 2020 à Rennes IMT Atlantique.
7. Thèse de Laura Brouilhet, "*Généralisation des protocoles en cas multi-utilisateur*", le 15 décembre 2020 à l'Université de Limoges.
8. Thèse de Sophie Dramé-Maigné, "*Blockchain et contrôle d'accès : Vers un Internet des Objets plus sécurisé*", le 12 novembre 2019 à Telecom SudParis.
9. Thèse de Dimitrios Vasilopoulos, "*Reconciling Cloud Storage Functionalities with Security : Proofs of Storage with Data Reliability and Secure Deduplication*", le 23 juillet 2019 à Eurecom.
10. Thèse de Robert Reimann, "*Towards trustworthy online voting : distributed aggregation of confidential data*", le 18 décembre 2017 à l'Université de Lyon.
11. Thèse de Levent Demir, "*Module de confiance pour l'externalisation de données dans le Cloud*", le 7 décembre 2017 à l'Université Grenoble Alpes.
12. Thèse de Jessye Dos Santos, "*Réseaux de capteurs et vie privée*, le 28 août 2017 à l'Université Grenoble Alpes.
13. Thèse de José Manuel Rubio Hernan, "*Detection of Attacks against Cyber-Physical Industrial Systems*, le 18 juillet 2017 à Telecom Sud Paris.
14. Thèse de Worachet Uttha, "*Étude des politiques de sécurité pour les applications distribuées : le problème des dépendances transitives*", le 26 septembre 2016 à l'Université Aix-Marseille.
15. Thèse d'Olivier Levillain, "*A study of the TLS ecosystem*", le 23 septembre 2016 à Telecom Sud Paris.
16. Thèse de Naipeng Dong, "The formalisation of enforced privacy notions in applied pi calculus", à l'Université de Luxembourg le 18 novembre 2013.
17. Thèse d'Ismail Mansour, "Contribution à la sécurité des communications des réseaux de capteurs sans fil", à l'Université d'Auvergne le 03 juillet 2013.

5 fois examinateurs

1. Thèse de Jean-Baptiste Orphila,"*Évaluation de la confiance dans les architectures de sécurité*", le 3 juillet 2018 à l'Université Grenoble Alpes.
2. Thèse de Cédric Van-Rompay, "*Protocoles Multi-Utilisateurs de Recherche sur Bases de Données*

20. http://confiance-numerique.clermont-universite.fr/

Chiffrées Multi-User Searchable Encryption", le 25 février 2016 à Eurecom.

3. Thèse de Anis Bkakria, "Specification and deployment of integrated Security Policy for Outsourced Data", à l'Université de Rennes, le 30 novembre 2015.
4. Thèse d'Abdourhamane Idrissa, "Traçabilité sécurisée embarquée", à l'Université de Saint-Etienne le 20 septembre 2012.
5. Thèse de Jean Lancrenon, "Authentification d'objets à distance", le 22 juin 2011 à l'Université Joseph Fourier Grenoble.

Co-Organisation de conférences Pour l'ensemble des conférences, j'ai géré les inscriptions, les sallles, les transports, le social event, le repas et le programme.

1. FPS'09 à Grenoble, 40 personnes
2. VETO'09 à Grenoble, 30 personnes.
3. SSS'11 à Grenoble, 50 personnes.
4. SDTA'14 à Clermont-Ferrand sur 2 jours (1er Colloque sur la Confiance Numérique en Auvergne) présence de plus de 100 personnes venant du monde académique et industriel [21]
5. FPS'15 à Clermont-Ferrand, 50 personnes.
6. Journées GdT C2 Codage et Cryptographie en mars 2014 au Sept-Laux, 60 personnes.
7. École de printemps Codage et Cryptographie en mars 2014 à Grenoble, 50 personnes.
8. RESSI'20 en ligne, 70 personnes.
9. RESSI'22 à Chambon sur Lac, 90 personnes.
10. SSS'222 à Clermont-Ferrand, 50 personnes.

Depuis 2016, organisation de REDOCS [22] chaque année.

Depuis sa création, je participe au comité de programme de la conférence GreHack [23].

Comité de rédaction :

— depuis janvier 2021, pour la revue internationale Frontiers in Computer Science.
— depuis janvier 2020, pour la revue internationale Annals of Telecommunications.
— depuis janvier 2013, pour la revue Techniques et Sciences Informatiques (TSI), édition Hermès, Lavoisier.

Invitations :

— En 2013, j'ai effectué un séjour d'un mois en tant que chercheur invité à l'Université de Monastir (Tunisie). Bourse ERASMUS MUNDUS.
— En 2013, j'ai été invité une semaine à l'University College of London pour collaborer avec Gareth Peters.
— En avril 2015, invité à la conférence Franco-Japonnaise sur la sécurité, à l'ambassade française à Tokyo, avril 2015.
— En 2016, invitation à l'ambassade française d'Atlanta (USA), en octobre 2016 pour une rencontre entre chercheurs français et américains sur la cybersécurité.

21. http://confiance-numerique.clermont-universite.fr/SDTA-2014/
22. https://gdr-securite.irisa.fr/redocs/
23. https://grehack.fr/2021/cfp#pc

Relecteur de revues internationales : Journal of Information and Communication (IC), Journal of Automated Reasoning (JAR), ACM Transactional on Computational Logic (ToCL), Transactions on Dependable and Secure Computing (TDSC), Elsevier Computer Science Review (CSR), Formal Methods in System Design (FMSD), IET Information Security, Computational Intelligence (CI), Information Sciences Journal, Techniques et Sciences Informatiques (TSI).

Membre de comités de programme des conférences internationales suivantes : SETOP'11, CSS'14, FPS'14, DPM'14, ICNAS'15, ATC'16, FPS'16, Grehack'16, GraMSec'16, ISSEP'16, NTMS'16, FPS'17, PST'17, Grehack'17, ICNAS'17, Algotel'17, ATC'17, FPS'18, Grehack'18, PST'18, Algotel'18, ATC'19, APKC'19, FPS'19, Grehack'19, ICISC'19, Algotel'20, APKC'20, Tokenomics'20, WTSC'20, Algotel'20, Grehack'20, FPS'20, Algotel 21, FPS'21, WTSC'21, Grehack'21, WTSC'22, FPS'22.

Relecteur pour les conférences suivantes : ICDCN'21, CCGrid'21, CANDAR'21, ICDCIT2021, OPODIS'19, Computer Network 2019, TPDS19, FEDCISS'18, JLAMP'18, PST'18, Algotel'18, ATC'18, Security and Privacy'17, ISSEP'16, CANDAR'16, ALGOTEL'16, CI'16, EUROPAR'16, GRAMSEC'16, NETSYS'16, TIFS'16, TMC2016, ASIACRYPT'15, CCS'15, FPS'15, ICNAS'15, TACAS'14, FPS'14, CSS'14, DPM'14, CCS'14, SAC'13, ICNAS'13, CARDIS 2013, IC'13, JAR'13, TOCL'13, Algotel'13, CSR'13, CADE'13, ACNS'13, APDCM'13, AFRICACRYPT'12, FPS'12, ICALP'11, CCS'11, RTA'11, FPS'11, SETOP'11, ICDNS'11, FAST'10, VECOS'10, FMSD'10, FROCOS'09, CAV'09, VMCAI'09, VETO'09, FPS'09, FMSE'08, TOCL'08, ESORICS'08, SICS'08, ICALP'07, ESORICS'07, ICTAC'07, RTA'06, CADE'05.

Exposés invités pour plus de 50 séminaires (*cf.* Annexe C.1 pour une liste détaillée).

3.5 Responsabilités scientifiques

Porteurs de 9 projets et participation à 8 autres projets depuis mon arrivée en 2013 au LIMOS pour un budget total de plus de 3 millions d'euros.

— **En tant que porteur** (rédaction du projet, des délivrables et administration) :

1. 2022-2024 : Plan de relance avec la société MyBus, montant : 30 K€.
2. 2020-2024 : Partenariat avec le CEA, *analyse de la sécurité des systèmes SCADA* Grenoble sur 4 ans, montant : 40 K€
3. 2016-2019 : Projet Franco-Indien dans le cadre du ICST CEFIPRA/CNRS. *Study of Privacy, Accountability and Ownership in IoT* avec le Security Group de DA-IICT, montant : 41 K€.
4. 2015-2018 : Projet Région DIS-4 : *Confiance dans les usages numérique*, en partenariat avec le LIMOS, le LAPSCO, Almerys, Coffré, Qualiac, Acquest, Openium : 2 PhDs et 1 Post-doc, montant : 683 K€.
5. 2016-2019 : Projet Région DIS-4 : *Enrichissement sémantique et gestion sécurisée des documents dématérialisés*, en partenariat avec le LIMOS, le LAPSCO : 2 PhDs et 1 Post-doc, montant : 774 K€.
6. 2016-2017 : Projet ASSI *Analyse de Sécurité de Systèmes Industriels* PEPS INS2I Collaboration avec Grenoble UGA et Nancy LORIA, montant : 28 K€.
7. 2017-2019 : Partenariat avec l'entreprise Domraider pour la réalisation d'un *protocole de vente aux enchères électronique dans la blockchain*, montant : 18 K€.

8. 2018-2019 : Partenariat avec l'entreprise Coffreo, montant : 10 K€.
9. 2019-2020 : Partenariat avec l'entreprise Almerys, montant : 30 K€.

— **En tant que responsable pour le LIMOS** (rédaction de la proposition du projet pour les parties, des délivrables et des parties administratives du LIMOS) :

1. 2021-2024 : BPI D4N, *Data Lake for Nuclear*, 1 PhD, montant 140 K€.
2. 2020-2024 : ANR SEVERITAS, *Secure and Verifiable Test and Assessment Systems*, 3 PhDs et 1 Post-doc, montant 340 K€.
3. 2019-2023 : ANR Decrypt, *DEclarative approach for symmetric CRYPTography*, 3 PhDs et 1 Post-doc, réalisation du site web, montant : 86 K€.
4. 2019-2023 : ANR MobiS5 *La sécurité et la protection de la vie privée dans les réseaux mobiles*, 3 PhDs et 1 Post-doc, réalisation du site web, montant : 185 K€.
5. 2017-2018 : PEPS OCAA CHARIOT : *Chiffrement Authentifié pour Renforcer l'IoT*, entre Grenoble (LIG) et Nancy (LORIA) 1 ingénieur de 9 mois, montant : 18.000€ + salaire.

— **En tant que membre et responsable de tâches au LIMOS**

1. 2016-2021 : Projet européen C-ROAD, *European Initiative for testing and implementing C-ITS*, 1 PhD et 3 Masters, montant : 281 K€,
2. 2019-2023 : Projet européen Indid, *Infrastructure Digitale de Demain*, 1 PhD et 2 Masters, montant : 197 K€.
3. 2017-2020 : Projet Région Vasoc : *Vers l'Audit de Sécurité des Objets connectés* 1 PhD, montant : 181 K€.

4 Responsabilités collectives et d'intérêt général

4.1 Synthèse

Membre élu du CNU 27 entre 2017 et 2019.
Membre du bureau du GDR Sécurité Informatique depuis sa création en 2016.
Responsable du séminaire confiance numérique.

4.2 Responsabilités administratives

Les responsabilités administratives listées sur la trame fournie, nécessitent un grand investissement. Il faut un temps pour tout et chacun doit trouver son équilibre et sa place dans le système universitaire. J'ai pour le moment privilégié la recherche et l'enseignement aux responsabilités administratives.

Cela s'explique par ma mobilité géographique et le fait qu'en tant que titulaire de la Chaire de Confiance numérique de 2013 à 2016, je n'étais pas en poste à l'UCA ce qui ne me permettait pas d'occuper ces responsabilités. De plus, il faut un certain temps avant de pouvoir accéder à ces fonctions et ces opportunités ne se sont pas présentées au département informatique de l'IUT car certains collègues enseignants souhaitent occuper ces responsabilités.

4.3 Responsabilités et mandats locaux ou régionaux

Élu au conseil du laboratoire LIMOS de 2017 à 2021.

Élu au conseil du département Informatique de l'IUT depuis 2017.

Responsable de la commission communication du LIMOS depuis 2017 : Réalisation de la page web du laboratoire, du logo et de la charte graphique.

Présidents du jury du Baccalauréat au Lycée de Montélimar en 2012 et au lycée Blaise Pascal à Clermont-Ferrand en 2018.

4.4 Responsabilités et mandats (internationaux, nationaux)

Je me suis investi, depuis sa création en 2016, dans le GDR Sécurité Informatique.

— Depuis 2016, membre du bureau du GDR Sécurité Informatique, réunions mensuelles et participation à l'organisation des activités du GDR.

— Responsable des Rencontres Entreprises DOCtorants en Sécurité (REDOCS [24]), pendant une semaine 15 doctorants sélectionnés travaillent par équipes de 5 et cherchent à résoudre les problèmes proposés par des industriels. Pour cela il faut en amont avoir trouver les entreprises, établir avec elles les sujets, et organiser la semaine en pension complète pour les doctorants.

— Depuis 2021, président du jury du Prix de thèse du GDR Sécurité Informatique. Ce prix de 1500 euros récompense la meilleure thèse dans les domaines du GDR. Il faut sélectionner les membres du jury, mettre en place le site de soumission des candidatures, rédiger les règlements et PV des commissions et étudier en deux phases les dossiers des candidats. Cet exercice est difficile car les dossiers sont excellents et il n'est pas facile de comparer les différentes thèses dans les différents domaines du GDR.

5 Autres informations

Mes passions en plus de l'enseignement et de la recherche sont la montgolfière (titulaire du brevet de pilote) et le Basket-ball. Je pratique ce sport collectif depuis mes 6 ans. Grâce à mon Certificat de Qualification Professionnelle de Technicien Sportif de Basketball, je coach des équipes jeunes et séniores en compétition. Pour moi, l'esprit d'équipe se retrouve clairement dans ma conception de l'animation de la recherche et de l'enseignement. J'ai ainsi pu dans les différentes collaborations aussi bien en recherche qu'en enseignement mettre en place de nombreuses collaborations fructueuses et vertueuses. Cet esprit collectif et de partage se traduit par mes 168 co-auteurs. En Annexe C.2, je liste l'ensemble de mes co-auteurs et j'ai mis en gras les 27 collaborateurs membres du LIMOS. Enfin être pilote de montgolfière dès mes 18 ans m'a permis d'avoir le sens des responsabilités, de développer mes capacités d'adaptation ainsi que la rigueur nécessaire pour la pratique de ce sport aérien exigeant.

24. https://gdr-securite.irisa.fr/redocs/

ANNEXES

A Détails des enseignements

2016 - : Le tableau [25] ci-dessous résume mes activités d'enseignements par an à l'UCA depuis 2016.

Nature	Effectif	Niveau	Eqtd	Intitulé	Ressources
TD/TP	**140**	**2A**	**60h**	**Administration des BD**	**Poly/TP**
CM/TD/TP	**30**	**LP Web**	**38h**	**Sécurité Web**	**TD/TP**
CM/TD	**140**	**1A**	**8h**	**Méthodologie**	**CM/TD/TP**
TD/TP	36	1A	35h	Base de données avancées	TD/TP
Projet	10	2A	8h	Projets 2A	Projet
Projet	24	LP Mobile	8h	Projets sur plateforme mobile	Projet
Soutenance	30	Tous	30h	Soutenances de projets	Soutenance
CM	**20**	**M2 Alt**	**24h**	**Modèles pour la Sécurité**	**[DLR15]**
CM	**40**	**M2 Alt**	**22h**	**Sécurité des systèmes d'information**	**[DLR15]**
CM/TD	**15**	**M2**	**10h**	**Sécurité pour la Data Science**	**[DLTV18]**
IREM	50	-	30h	Animations et formations à l'IREM	Animation
TOTAL			253		

2013 - 2016 : Titulaire de la chaire industrielle Confiance Numérique de l'Université d'Auvergne (UdA), dans ce cadre, j'ai effectué un service réduit de 64h. J'ai proposé de nouveaux enseignements liés à mes thématiques de recherche autour de la sécurité à l'ISIMA et au département R&T de l'IUT de l'UdA.

- 32h : cours en Master international à l'ISIMA : Security models.
- 16h : cours en Licence Pro à l'IUT R&T d'Aubière : Introduction à la sécurité.
- 11h : TD en 1ère année d'IUT R&T d'Aubière : Méthodes de travail.
- 5h : Cours et TD en 1ère année d'IUT INFO de Méthodes de travail.

2007 - 2013 : Maître de conférences à l'Université Joseph Fourier à Grenoble, j'ai enseigné plus de 192h par an à l'UFR IM2AG, à l'ENSIMAG et à Polytech Grenoble. Mes enseignements et les ressources réalisées sont présentés dans le tableau suivant :

25. Les lignes en gras signifient que je suis responsable de l'UE et CM_A que l'UE est aussi dispensée en anglais.

Nature	Effectif	Niveau	Eqtd	Intitulé	Ressources
CM$_A$	**120**	**L1**	**27h**	**Introduction à la programmation Fonctionnelle**	**[CLM14]**
CM$_A$	**60**	**L2**	**27h**	**Introduction à la Logique**	**[DLL12a]**
CM	**40**	**L2**	**16h**	**Magistére pluridisciplinaire**	**Animation**
CM	**40**	**L3**	**27h**	**Algorithmique et programmation Fonctionnelle**	**Poly TD/TP**
CM	**10**	**L3**	**20h**	**Magistére Informatique**	**Animation**
CM	50	M2	9h	Modèles pour la Sécurité (Ensimag)	[DLR15]
CM$_A$	**20**	**M2 R/P**	**27h**	**Modèles pour la Sécurité**	**Poly TD**
CM	**10**	**M2 Alt**	**30h**	**Complexité et Modèles pour la Sécurité**	**Poly TD**
IREM	**15**	**-**	**32h**	**Responsable groupe Algorithmique**	**Animation**
TOTAL			**213**		

B Liste de mes publications

Comme demandé les noms des étudiants encadrés en thèse sont soulignés et mon nom est mis en gras. Mes publications sont accessibles aux addresses suivantes :

Home page : https://sancy.iut-clermont.uca.fr/~lafourcade/recherche.html

HAL : https://cv.archives-ouvertes.fr/pascalafourcade

DBLP : http://dblp.uni-trier.de/pers/hd/l/Lafourcade_0001:Pascal

9 Livres

— 2022 —

[DLR+22] J.-G. Dumas, **P. Lafourcade**, E. Roudeix, A. Tichit, and S. Varrette. *Les NFT en 40 questions, Comprendre les jetons Non Fungible*. Dunod, 2022.

— 2021 —

[LM21a] **P. Lafourcade** and M. More. *25 énigmes ludiques pour s'initier à la cryptographie*. Dunod, 2021.

— 2020 —

[DL20] J.-G. Dumas and **P. Lafourcade**. *13 défis de la cybersécurité : bitcoins et la blockchain*. CNRS, 2020. Ouvrage collectif sous la direction de Gildas Avoine, Marc-Olivier Killijian.

— 2018 —

[DLTV18] J.-G. Dumas, **P. Lafourcade**, A. Tichit, and S. Varette. *Les blockchains en 50 Questions, comprendre le fonctionnement et les enjeux de cette technologie innovante*. Dunod, 2ème édition en 2020 edition, 2018.

— 2017 —

[Col17] Collectif. *L'informatique débranchée*. Number 42-43. POLE Tangente Éducation, 2017. pages 94.

— 2015 —

[DLR15] J.-G. Dumas, **P. Lafourcade**, and P. Redon. *Architectures de sécurité pour Internet, Protocoles, standards et déploiement*. Dunod, 2ème édition en 2020 edition, 2015.

[LL15] **P. Lafourcade** and I. Lebrun. *S'exercer à apprendre*. De Boeck, 2015.

— 2014 —

[CLM14] F. Carrier, **P. Lafourcade**, and L. Mounier. *Exercices de programmation fonctionnelle en Ocaml une approche pédagogique par l'algorithmique, la preuve et la complexité*. Ellipses, 2014.

— 2012 —

[DLL12a] S. Devismes, **P. Lafourcade**, and M. Lévy. *Informatique théorique : Logique et démonstration automatique, Introduction à la logique propositionnelle et à la logique du premier ordre*. Ellipses, 2012.

4 Chapitres de livre

— 2019 —

[ABG+19] G. Avoine, I. Boureanu, D. Gérault, G. P. Hancke, **P. Lafourcade**, and C. Onete. *Security of Ubiquitous Computing Systems Selected Topics, Cryptacus*, chapter From Relay Attacks to Distance-bounding Protocols. Springer-Verlag, 2019.

[DL19] J.-G. Dumas and **P. Lafourcade**. *Treize défis de la cybersécurité : relectures croisées*, chapter La sécurité de Bitcoin et des Blockchains. CNRS, 2019.

— 2016 —

[DL16] J.-G. Dumas and **P. Lafourcade**. *Les Big Data à l'échelle de la société*, chapter Les cryptomonnaies, une réalité virtuelle ? édition CNRS, 2016.

— 2012 —

[JL12] R. Jamet and **P. Lafourcade**. *Formal Model for (k)-Neighborhood Discovery Protocols*, chapter in Advances in Network Analysis and its Applications. Springer, 2012.

1 Magazine

— 2008 —

[PPS+08] P. Papadimitratos, M. Poturalski, P. Schaller, **P. Lafourcade**, D. Basin, S. Čapkun, and J.-P. Hubaux. Secure Neighborhood Discovery : A Fundamental Element for Mobile Ad Hoc Networking. *IEEE Communications Magazine*, 46(2) :132–139, February 2008.

Thèse et Habilitation à diriger des recherches

— 2012 —

[Laf12] **P. Lafourcade**. *Computer-Aider Security for : Cryptographic Primitives, Voting Protocols and Wireless Sensor Networks*. Habilitation à diriger des recherches, Verimag, Grenoble, France, 11 2012. 192 pages.

— 2006 —

[Laf06] **P. Lafourcade**. *Vérification des protocoles cryptographiques en présence de théories équationnelles*. Thèse de doctorat, Laboratoire Spécification et Vérification, ENS Cachan, France, September 2006. 209 pages.

38 Revues internationales

— 2022 —

[CDLS22] R. Ciucanu, A. Delabrouille, **P. Lafourcade**, and M. Soare. Secure protocols for best arm identification in federated stochastic multi-armed bandits. In *Transactions on Dependable and Secure Computing*, 2022.

[CLLS22] R. Ciucanu, **P. Lafourcade**, M. Lombard-Platet, and M. Soare. Secure protocols for cumulative reward maximization in stochastic multi-armed bandits. *Journal of Computer Security*, 2022.

[CLMS22] R. Ciucanu, **P. Lafourcade**, G. Marcadet, and M. Soare. SAMBA : A generic framework for secure federated multi-armed bandits. *Journal of Artificial Intelligence Research (JAIR)*, 73, 2022. https://github.com/gamarcad/paper-samba-code.

[RMLM21] L. Robert, D. Miyahara, **P. Lafourcade**, and T. Mizuki. Interactive physical zkp for connectivity : Applications to nurikabe and hitori. In L. De Mol, A. Weiermann, F. Manea, and D. Fernández-Duque, editors, *Connecting with Computability*, pages 373–384, Cham, 2021. Springer International Publishing.

— 2021 —

[ASNK+21] M. Akand, R. Safavi-Naini, M. Kneppers, M. Giraud, and **P. Lafourcade**. Privacy-preserving proof-of-location with security against geo-tampering. *IEEE Transactions on Dependable and Secure Computing*, 2021.

[BCF+21] V. Bellot, M. Cautrès, J.-M. Favreau, M. Gonzalez-Thauvin, **P. Lafourcade**, K. LeCornec, B. Mosnier, and S. Rivière-Wekstein. How to generate perfect mazes ? *Information Sciences, Informatics and Computer Science Intelligent Systems Applications, Elsevier*, 2021.

[CYLR21] M. Chaieb, S. Yousfi, **P. Lafourcade**, and R. Robbana. Design and practical implementation of verify-your-vote protocol. *Concurrency and Computation : Practice and Experience*, 2021.

[DDLR21] J. Dreier, J.-G. Dumas, **P. Lafourcade**, and L. Robert. Optimal threshold padlock systems. In *Journal of Computer Security*, 2021.

[LMM+21] **P. Lafourcade**, D. Miyahara, T. Mizuki, L. Robert, T. Sasaki, and H. Sone. How to construct physical zero-knowledge proofs for puzzles with a "single loop" condition. *Theor. Comput. Sci.*, 888 :41–55, 2021.

[NRLSL21] C. Negri-Ribalta, M. Lombard-Platet, C. Salinesi, and **P. Lafourcade**. Blockchain mirage or silver bullet ? A requirements-driven comparative analysis of business and developers' perceptions in the accountancy domain. *J. Wirel. Mob. Networks Ubiquitous Comput. Dependable Appl.*, 12(1) :85–110, 2021.

[RML+21] L. Robert, D. Miyahara, **P. Lafourcade**, L. Libralesso, and T. Mizuki. Physical zero-knowledge proof and np-completeness proof of Suguru puzzle. *Information and Computation*, page 104858, 2021.

— 2020 —

[BDDL20] X. Bultel, J. Dreier, J.-G. Dumas, and **P. Lafourcade**. A faster cryptographer's conspiracy santa ? *Theoretical Computer Science*, 2020.

[GLMS20] D. Gerault, **P. Lafourcade**, M. Minier, and C. Solnon. Computing AES related-key differential characteristics with constraint programming. *Artificial Intellgence*, 278, 2020.

[LL20] M. Lombard-Platet and **P. Lafourcade**. About blockchain interoperability. In *Information Processing Letters, (IPL)*, 2020.

— 2019 —

[AYBGL19] A. Anzala-Yamajako, O. Bernard, M. Giraud, and **P. Lafourcade**. No Such Thing As A Small Leak : Leakage-Abuse Attacks Against Symmetric Searchable Encryption. *Communications in Computer and Information Science, Springer*, 2019.

[DLM+19a] J.-G. Dumas, **P. Lafourcade**, F. Melemedjian, J.-B. Orfila, and P. Thoniel. LocalPKI : An Interoperable and IoT Friendly PKI. *Communications in Computer and Information Science, Springer*, 2019.

— 2018 —

[BLGR18] M. Berrima, **P. Lafourcade**, M. Giraud, and N. B. Rajeb. Formal Analysis of a Private Access Control Protocol to a Cloud Storage. *International of Innovative Computing and Applications*, 2018.

[DLP+18] J. Dreier, **P. Lafourcade**, M.-L. Potet, M. Puys, and J.-L. Roch. Formally and Practically Verifying Flow Integrityf Properties in Industrial Systems. *Computer & Security (Elsevier)*, 2018.

[GLMS18] D. Gérault, **P. Lafourcade**, M. Minier, and C. Solnon. Revisiting aes related-key differential attacks with constraint programming. *Information Processing Letters, Elsevier, In press*, 139 :24–29, 2018.

— 2017 —

[ADJL16] K. Altisen, S. Devismes, R. Jamet, and **P. Lafourcade**. SR3 : secure resilient reputation-based routing. *Wireless Networks*, pages 1–23, 2016.

[AGLM17] A. T. Aby, A. Guitton, **P. Lafourcade**, and M. Misson. History-based MAC Protocol for Low Duty-Cycle Wireless Sensor Networks : the SLACK-MAC Protocol. *ICST Trans. Mobile Communications Applications*, 3(8) :e5, 2017.

[BDLM17] X. Bultel, J. Dreier, **P. Lafourcade**, and M. More. How to explain modern security concepts to your children. *Cryptologia*, pages 1–26, 2017.

[DLOP17] J. Dumas, **P. Lafourcade**, J. Orfila, and M. Puys. Dual protocols for private multi-party matrix multiplication and trust computations. *Computers & Security*, 71 :51–70, 2017.

[KFL17] A. Kassem, Y. Falcone, and **P. Lafourcade**. Formal analysis and offline monitoring of electronic exams. *Formal Methods in System Design*, 51(1) :117–153, 2017.

— 2016 —

[BLM+16] B. Bérard, **P. Lafourcade**, L. Millet, M. Potop-Butucaru, Y. Thierry-Mieg, and S. Tixeuil. Formal verification of mobile robot protocols. *Distributed Computing*, 29(6) :459–487, 2016.

[DELL16] J. Dreier, C. Ene, **P. Lafourcade**, and Y. Lakhnech. On the existence and decidability of unique decompositions of processes in the applied pi-calculus. *Theoretical Computer Science*, 612 :102 – 125, 2016.

[GLLSN16] M. Gagné, **P. Lafourcade**, Y. Lakhnech, and R. Safavi-Naini. Automated Proofs of Block Cipher Modes of Operation. *Journal of Automatic Reasoning*, 56(1) :49–94, 2016.

— 2015 —

[DDL15] J. Dreier, J.-G. Dumas, and **P. Lafourcade**. Brandt's Fully Private Auction Protocol Revisited. *Journal of Computer Security Special Issue on Security and High Performance Computing Systems*, 2015.

[DGK+15a] J. Dreier, R. Giustolisi, A. Kassem, **P. Lafourcade**, G. Lenzin, and P. Y. Ryan. Formal security analysis of traditional and electronic exams. In *Communications in Computer and Information Science*, volume Springer-Verlag, LNCS of *CCIS*, 2015.

[MCL15] I. Mansour, G. Chalhoub, and **P. Lafourcade**. Key Management in Wireless Sensor Networks. *J. Sensor and Actuator Networks*, 4(3) :251–273, 2015.

— 2014 —

[GADL14] A. Gerbaud, K. Altisen, S. Devismes, and **P. Lafourcade**. Comparison of mean hitting times for a degree-biased random walk. *Discrete Applied Mathematics*, 170 :104–109, 2014.

[MCL14a] I. Mansour, G. Chalhoub, and **P. Lafourcade**. Evaluation of Secure Multi-Hop Node Authentication and Key Establishment Mechanisms for Wireless Sensor Networks. *Journal of Sensor Actuator Networks*, 3(3) :224–244, 2014.

— 2011 —

[CDE+10] J. Courant, M. Daubignard, C. Ene, **P. Lafourcade**, and Y. Lakhnech. Automated Proofs for Asymmetric Encryption. *Journal of Automated Reasoning*, 46(3-4) :261–291, 2010.

— 2008 —

[DLLT08] S. Delaune, **P. Lafourcade**, D. Lugiez, and R. Treinen. Symbolic Protocol Analysis for Monoidal Equational Theories. *Information and Computation*, 205 :581–623, 2008.

— 2007 —

[KL07] B. Ksiezopolski and **P. Lafourcade**. Attack and Revison of an Electronic Auction Protocol using OFMC. *Annales UMCS, Informatica*, 6(1) :171–183, 2007.

[Laf07b] **P. Lafourcade**. Intruder Deduction for the Equational Theory of Exclusive-or with Commutative and Distributive Encryption. *Electr. Notes Theor. Comput. Sci.*, 171(4) :37–57, 2007.

[LLT07] **P. Lafourcade**, D. Lugiez, and R. Treinen. Intruder Deduction for the Equational Theory of Abelian Groups with Distributive Encryption. *Information and Computation*, 205(4) :581–623, April 2007.

— 2006 —

[CDL06] V. Cortier, S. Delaune, and **P. Lafourcade**. A Survey of Algebraic Properties Used in Cryptographic Protocols. *Journal of Computer Security*, 14(1) :1–43, 2006.

109 Conférences internationales

— 2022 —

[BDD+22] Q. Bramas, A. Durand, S. Devismes, **P. Lafourcade**, and A. Lamani. Beedroid : How luminous autonomous swarms of uav can save the world ? In *11th International Conference on Fun with Algorithms (FUN 2022)*, 2022.

[BFJ+22] O. Blazy, P.-A. Fouque, T. Jacques, C. Onete, **P. Lafourcade**, and L. Robert. MARSHAL : Messaging with Asynchronous Ratchets and Signatures for faster HeALing. In *The 37th ACM/SIGAPP Symposium on Applied Computing (SAC, Security Track)*, 2022.

[CLPK22] A. Connolly, **P. Lafourcade**, and O. Perez-Kempner. Improved constructions of anonymous credentials from structure-preserving signatures on equivalence classes. In *The International Conference on Practice and Theory of Public-Key Cryptography (PKC)*, 2022.

[FJL+22] P. A. Fouque, T. Jacques, **P. Lafourcade**, A. Nedelcu, C. Onete, and L. Robert. A cryptographic view of deep-attestation, or how to do provably-secure layer-linking. In *International Conference on Applied Cryptography and Network Security ACNS*, Rome, 2022.

[FLLM22] F. Fontan, **P. Lafourcade**, L. Libralesso, and B. Momège. Local search with weighting schemes for the cg :shop 2022 competition. In *38th International Computational Geometry Week In the CG :SHOP Challenge 2022, SoCG*, 2022.

[MCL+22] G. Marcadet, R. Ciucanu, **P. Lafourcade**, M. Soare, and S. Amer-Yahia. SAMBA : A system for secure federated multi-armed bandits. In *IEEE International Conference on Data Engineering (ICDE) – Demo*, 2022.

— 2021 —

[BBLPK21] O. Blazy, X. Bultel, **P. Lafourcade**, and O. Perez-Kempner. Generic plaintext equality and inequality proofs. In *The Twenty-Fifth International Conference, Financial Crypto And Data Security 2021 (FC 2021)*, 2021.

[BDF+21] I. Boureanu, F. Dupressoir, C. C. Fragan, D. Gérault, and **P. Lafourcade**. Precise models and mechanised proofs for distance-bounding. In *34th IEEE Computer Security Foundations Symposium June 21-25, CSF 2021 Virtual Conference*, 2021.

[BDL21] Q. Bramas, S. Devismes, and **P. Lafourcade**. Optimal exclusive perpetual grid exploration by luminous myopic opaque robots with common chirality. In *The 22nd International Conference on Distributed Computing and Networking ICDCN 2021*, 2021.

[CdFG+21] L. Crombez, G. D. da Fonseca, Y. Gerard, A. Gonzalez-Lorenzo, **P. Lafourcade**, and L. Libralesso. Shadoks approach to low-makespan coordinated motion planning. In *Computational Geometry : Solving Hard Optimization Problems Geometric Optimization Challenges*, 2021.

[LDLS21] L. Libralesso, F. Delobel, **P. Lafourcade**, and C. Solnon. Automatic generation of declarative models for differential cryptanalysis. In *27th International Conference on Principles and Practice of Constraint Programming, CP 2021*, 2021.

[LRS21] **P. Lafourcade**, L. Robert, and D. Sow. Fast Cramer-Shoup Cryptosystem. In *18th Internationa Conference on Security and Cryptography, SECRYPT*, 2021.

[MLMR21] D. Miyahara, **P. Lafourcade**, T. Mizuki, and L. Robert. Interactive physical zero-knowledge proof for continuity, applications to Nurikabe and Hitori. In *Computability in Europe Conference 2021, 5 – 9 July 2021*, 2021.

[OARBL21] C. Olivier-Anclin, L. Robert, X. Bultel, and **P. Lafourcade**. Generic construction for identity-based proxy blind signature. In *The 14th International Symposium on Foundations & Practice of Security, FPS*, Paris, 2021.

[RBD+21] A. Rauch, Q. Bramas, S. Devismes, **P. Lafourcade**, and A. Lamani. Optimal exclusive perpetual grid exploration by luminous myopic robots without common chirality. In *9th International Conference on Networked Systems NETYS 2021.*, 2021.

— 2020 —

[BDL20a] Q. Bramas, S. Devismes, and **P. Lafourcade**. Finding water on Poleless using melomaniac myopic chameleon robots. In *10th International Conference on Fun with Algorithms (FUN 2020)*, volume 157. LIPIcs, 2020.

[BDL20b] Q. Bramas, S. Devismes, and **P. Lafourcade**. Infinite grid exploration by disoriented robots. In *The 8th Edition of the International Conference on NETworked and sYStems, NETYS 2020*. LNCS, June 2020.

[CDLS20] R. Ciucanu, A. Delabrouille, **P. Lafourcade**, and M. Soare. Secure cumulative reward maximization in linear stochastic bandits. In *The 14th International Conference on the theme of Provable and Practical Security, ProvSec*, Singapore, November 2020. LNCS, Springer.

[CL20a] R. Ciucanu and **P. Lafourcade**. Demonstration of GOOSE : A Secure Framework for Graph Outsourcing and SPARQL Evaluation. In *International Semantic Web Conference (ISWC) – Demo Track*, 2020. http://ceur-ws.org/Vol-2721/paper476.pdf.

[CL20b] R. Ciucanu and **P. Lafourcade**. Goose a secure framework for graph outsourcing and sparql evaluation. In *34th Annual IFIP WG 11.3 Conference on Data and Applications Security and Privacy (DBSec'20)*, Regensburg, Germany, June 2020.

[CLLS20] R. Ciucanu, **P. Lafourcade**, M. Lombard-Platet, and M. Soare. Secure outsourcing of multi-armed bandits in an honest-but-curious cloud. In *The 19th IEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom 2020)*, 2020.

[ELLR20] R. Esmander, **P. Lafourcade**, M. Lombard-Platet, and C. N. Ribalta. A silver bullet ? : a comparison of accountants and developers mental models in the raise of blockchain. In M. Volkamer and C. Wressnegger, editors, *ARES 2020 : The 15th International Conference on Availability, Reliability and Security, Virtual Event, Ireland, August 25-28, 2020*, pages 83 :1–83 :10. ACM, 2020.

[GLTT20] P.-M. Grollemund, **P. Lafourcade**, K. Thiry-Atighehchi, and A. Tichit. Proof of behaviours. In *The 2nd Tokenomics Conference on Blockchain Economics, Security and Protocols*, Toulouse, 2020.

[JLM+20] M. Journault, **P. Lafourcade**, M. More, R. Poulain, and L. Robert. How to teach the undecidability of malware detection problem and halting problem. In *WG 11.8 - 13th World Conference on Information Security Education, WISE*, Maribor, Slovenia, september 2020.

[LMMR20] **P. Lafourcade**, T. Mizuki, D. Miyahara, and L. Robert. Physical zero-knowledge proof for suguru puzzle. In *2nd International Symposium on Stabilization, Safety, and Security of Distributed Systems (SSS'20)*, Austin, Texas, USA, November 18-21 2020. LNCS, Springer.

[LRS20a] **P. Lafourcade**, L. Robert, and D. Sow. Fast linear Elgamal. In *The 17th International Conference on Security and Cryptography (SECRYPT 2020)*, Lieusant, Paris, July 2020.

[LRS20b] **P. Lafourcade**, L. Robert, and D. Sow. Fast short (linear) Cramer Shoup. In *The 13th International Symposium on Foundations & Practice of Security 1, 2 and 3 December 2020, Montreal, Canada, FPS*, 2020.

[MTS+20] D. Miyahara, S. Takeshige, K. Shinagawa, A. Nagao, **P. Lafourcade**, T. Mizuki, L. Robert, and H. Sone. Card-based ZKP protocols for Takuzu and Juosan. In *10th International Conference on Fun with Algorithms (FUN 2020)*, volume 157. LIPIcs, 2020.

— 2019 —

[BDL19] Q. Bramas, S. Devismes, and **P. Lafourcade**. Infinite grid exploration by disoriented robots. In K. Censor-Hillel and M. Flammini, editors, *Structural Information and Communication Complexity - 26th International Colloquium, SIROCCO 2019, L'Aquila, Italy, July 1-4, 2019, Proceedings*, volume 11639 of *Lecture Notes in Computer Science*, pages 340–344. Springer, 2019.

[BL19] X. Bultel and **P. Lafourcade**. Secure trick-taking game protocols how to play online spades with cheaters. In *Twenty-Third International Conference Financial Crypptography and Data Security 2019*, February 2019.

[BLL+19] X. Bultel, **P. Lafourcade**, R. W. F. Lai, G. Malavolta, D. Schröder, and S. A. K. Thyagarajan. Efficient invisible and unlinkable sanitizable signatures. In D. Lin and K. Sako, editors, *Public-Key Cryptography - PKC 2019 - 22nd IACR International Conference on Practice and Theory of Public-Key Cryptography, Beijing, China, April 14-17, 2019, Proceedings, Part I*, volume 11442 of *Lecture Notes in Computer Science*, pages 159–189. Springer, 2019.

[CGLY19a] R. Ciucanu, M. Giraud, **P. Lafourcade**, and L. Ye. Secure intersection with mapreduce. In M. S. Obaidat and P. Samarati, editors, *Proceedings of the 16th International Joint Conference on e-Business and Telecommunications, ICETE 2019 - Volume 2 : SECRYPT, Prague, Czech Republic, July 26-28, 2019.*, pages 236–243. SciTePress, 2019.

[CGLY19b] R. Ciucanu, M. Giraud, **P. Lafourcade**, and L. Ye. Secure strassen-winograd matrix multiplication with mapreduce. In M. S. Obaidat and P. Samarati, editors, *Proceedings of the 16th International Joint Conference on e-Business and Telecommunications, ICETE 2019 - Volume 2 : SECRYPT, Prague, Czech Republic, July 26-28, 2019.*, pages 220–227. SciTePress, 2019.

[CKY+19a] M. Chaieb, M. Koscina, S. Yousfi, **P. Lafourcade**, and R. Robbana. Dabsters : a privacy preserving e-voting protocol for permissioned blockchain. In *ICTAC 2019, the 16th International Colloquium on Theoretical Aspects of Computing*, 2019.

[CKY+19b] M. Chaieb, M. Koscina, S. Yousfi, **P. Lafourcade**, and R. Robbana. DABSTERS : distributed authorities using blind signature to effect robust security in e-voting. In M. S. Obaidat and P. Samarati, editors, *Proceedings of the 16th International Joint Conference on e-Business and Telecommunications, ICETE 2019 - Volume 2 : SECRYPT, Prague, Czech Republic, July 26-28, 2019.*, pages 228–235. SciTePress, 2019.

[CLLS19] R. Ciucanu, **P. Lafourcade**, M. Lombard-Platet, and M. Soare. Secure best arm identification in multi-armed bandits. In S. Heng and J. López, editors, *Information Security Practice and Experience - 15th International Conference, ISPEC 2019, Kuala Lumpur, Malaysia, November 26-28, 2019, Proceedings*, volume 11879 of *Lecture Notes in Computer Science*, pages 152–171. Springer, 2019.

[DGG+19] M. L. Das, H. Gajera, D. Gérault, M. Giraud, and **P. Lafourcade**. Private oblivious polynomial evaluation. In *International Conference on Information Security Theory and Practice, WISTP'19*, 2019.

[DLF+19] J. Dumas, **P. Lafourcade**, J. L. Fenner, D. Lucas, J. Orfila, C. Pernet, and M. Puys. Secure multiparty matrix multiplication based on strassen-winograd algorithm. In N. Attrapadung and T. Yagi, editors, *Advances in Information and Computer Security - 14th International Workshop on Security, IWSEC 2019, Tokyo, Japan, August 28-30, 2019, Proceedings*, volume 11689 of *Lecture Notes in Computer Science*, pages 67–88. Springer, 2019.

[DLM+19b] J. Dumas, **P. Lafourcade**, D. Miyahara, T. Mizuki, T. Sasaki, and H. Sone. Interactive physical zero-knowledge proof for norinori. In D. Du, Z. Duan, and C. Tian, editors, *Computing and Combinatorics - 25th International Conference, COCOON 2019, Xi'an, China, July 29-31, 2019, Proceedings*, volume 11653 of *Lecture Notes in Computer Science*, pages 166–177. Springer, 2019.

[GL19] D. Gérault and **P. Lafourcade**. Towards secure tmis protocols. In *Foundations and Practice of Security - 12th International Symposium, FPS 2019, Toulouse, France, 2019, Revised Selected Papers*, Lecture Notes in Computer Science. Springer, 2019.

[LMM+19] **P. Lafourcade**, D. Miyahara, T. Mizuki, T. Sasaki, and H. Sone. A physical ZKP for slitherlink : How to perform physical topology-preserving computation. In S. Heng and J. López, editors, *Information Security Practice and Experience - 15th International Conference, ISPEC 2019, Kuala Lumpur, Malaysia, November 26-28, 2019, Proceedings*, volume 11879 of *Lecture Notes in Computer Science*, pages 135–151. Springer, 2019.

[LMNS19] **P. Lafourcade**, T. Mizuki, A. Nagao, and K. Shinagawa. Light cryptography. In L. Drevin and M. Theocharidou, editors, *Information Security Education. Education in Proactive Information Security - 12th IFIP WG 11.8 World Conference WISE 12, Lisbon, Portugal, June 25-27, 2019, Proceedings*, volume 557 of *IFIP Advances in Information and Communication Technology*, pages 89–101. Springer, 2019.

[LNP+19] **P. Lafourcade**, M. Nopere, J. Picot, D. Pizzuti, and E. Roudeix. Security analysis of auctionity : a blockchain based e-auction. In *Foundations and Practice of Security - 12th International Symposium, FPS 2019, Toulouse, France, 2019, Revised Selected Papers*, Lecture Notes in Computer Science. Springer, 2019.

[LPL19] M. Lombard-Platet and **P. Lafourcade**. Get-your-id : Decentralized proof of identity. In *Foundations and Practice of Security - 12th International Symposium, FPS 2019, Toulouse, France, 2019, Revised Selected Papers*, Lecture Notes in Computer Science. Springer, 2019.

— 2018 —

[BCG+18] X. Bultel, R. Ciucanu, M. Giraud, **P. Lafourcade**, and L. Ye. Secure Joins with MapReduce. In *FPS'18, Montréal, Canada.*, 2018.

[BDD+18] X. Bultel, J. Dreier, J. Dumas, **P. Lafourcade**, D. Miyahara, T. Mizuki, A. Nagao, T. Sasaki, K. Shinagawa, and H. Sone. Physical zero-knowledge proof for makaro. In T. Izumi and P. Kuznetsov, editors, *Stabilization, Safety, and Security of Distributed Systems - 20th International Symposium, SSS 2018, Tokyo, Japan, November 4-7, 2018, Proceedings*, volume 11201 of *Lecture Notes in Computer Science*, pages 111–125. Springer, 2018.

[BDDL18] X. Bultel, J. Dreier, J.-G. Dumas, and **P. Lafourcade**. A Cryptographer's Conspiracy Santa. In H. Ito and S. Leonardi, editors, *9th International Conference on Fun with Algorithms (FUN 2018)*, LIPIcs, La Maddalena, Maddalena Islands, Italy,, June 2018. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik.

[BDG+18] X. Bultel, J. Dreier, M. Giraud, M. Izaute, T. Kheyrkhah, **P. Lafourcade**, D. Lakhzoum, V. Marlin, and L. Moták. Security Analysis and Psychological Study of Authentication Methods with PIN Codes. In *IEEE Twelfth International Conference on Research Challenges in Information Science, May 29-31, 2018, Nantes, France*, 2018.

[CGLY18] R. Ciucanu, M. Giraud, **P. Lafourcade**, and L. Ye. Secure grouping and aggregation with mapreduce. In P. Samarati and M. S. Obaidat, editors, *Proceedings of the 15th International Joint Conference on e-Business and Telecommunications, ICETE 2018 - Volume 2 : SECRYPT, Porto, Portugal, July 26-28, 2018.*, pages 514–521. SciTePress, 2018.

[CYLR18] M. Chaieb, S. Yousfi, **P. Lafourcade**, and R. Robbana. Verify-Your-Vote : A Verifiable Blockchain-based Online Voting Protocol. In *15th European Mediterranean and Middle Eastern Conference on Information Systems 2018, Cyprus*, 2018.

— 2017 —

[ABG+17] G. Avoine, X. Bultel, S. Gambs, D. Gérault, **P. Lafourcade**, C. Onete, and J. Robert. A Terrorist-fraud Resistant and Extractor-free Anonymous Distance-bounding Protocol. In R. Karri, O. Sinanoglu, A. Sadeghi, and X. Yi, editors, *Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security, AsiaCCS 2017, Abu Dhabi, United Arab Emirates, April 2-6, 2017*, pages 800–814. ACM, 2017.

[BCGL17] X. Bultel, R. Ciucanu, M. Giraud, and **P. Lafourcade**. Secure Matrix Multiplication with MapReduce. In *Proceedings of the 12th International Conference on Availability, Reliability and Security, ARES'17, Reggio Calabria, Italy, August 29 - September 01, 2017*, pages 11 :1–11 :10. ACM, 2017.

[BDG+17] X. Bultel, M. L. Das, H. Gajera, D. Gérault, M. Giraud, and **P. Lafourcade**. Verifiable Private Polynomial Evaluation. In T. Okamoto, Y. Yu, M. H. Au, and Y. Li, editors, *Provable Security - 11th International Conference, ProvSec 2017, Xi'an, China, October 23-25, 2017, Proceedings*, volume 10592 of *Lecture Notes in Computer Science*, pages 487–506. Springer, 2017.

[BDL17] E. Blot, J. Dreier, and **P. Lafourcade**. Formal Analysis of Combinations of Secure Protocols. In A. Imine, J. M. Fernandez, J. Marion, L. Logrippo, and J. García-Alfaro, editors, *Foundations and Practice of Security - 10th International Symposium, FPS 2017, Nancy, France, October 23-25, 2017, Revised Selected Papers*, volume 10723 of *Lecture Notes in Computer Science*, pages 53–67. Springer, 2017.

[BGLO17] I. Boureanu, D. Gérault, **P. Lafourcade**, and C. Onete. Breaking and fixing the HB+DB protocol. In G. Noubir, M. Conti, and S. K. Kasera, editors, *Proceedings of the 10th ACM Conference on Security and Privacy in Wireless and Mobile Networks, WiSec 2017, Boston, MA, USA, July 18-20, 2017*, pages 241–246. ACM, 2017.

[BL17] X. Bultel and **P. Lafourcade**. Unlinkable and Strongly Accountable Sanitizable Signatures from Verifiable Ring Signatures. In *16th International Conference on Cryptology and Network Security, CANS'17*, Hong Kong, Hong Kong, 2017.

[BLGR17] M. Berrima, **P. Lafourcade**, M. Giraud, and N. B. Rajeb. Formal Analyze of a Private Access Control Protocol to a Cloud Storage. In P. Samarati, M. S. Obaidat, and E. Cabello, editors, *Proceedings of the 14th International Joint Conference on e-Business and Telecommunications (ICETE 2017) - Volume 4 : SECRYPT, Madrid, Spain, July 24-26, 2017.*, pages 495–500. SciTePress, 2017.

[DLM+17] J. Dumas, **P. Lafourcade**, F. Melemedjian, J. Orfila, and P. Thoniel. LOCALPKI : A User-Centric Formally Proven Alternative to PKIX. In P. Samarati, M. S. Obaidat, and E. Cabello, editors, *Proceedings of the 14th International Joint Conference on e-Business and Telecommunications (ICETE 2017) - Volume 4 : SECRYPT, Madrid, Spain, July 24-26, 2017.*, pages 187–199. SciTePress, 2017.

[DPP+17] J. Dreier, M. Puys, M. Potet, **P. Lafourcade**, and J. Roch. Formally Verifying Flow Properties in Industrial Systems. In P. Samarati, M. S. Obaidat, and E. Cabello, editors, *Proceedings of the 14th International Joint Conference on e-Business and Telecommunications (ICETE 2017) - Volume 4 : SECRYPT, Madrid, Spain, July 24-26, 2017.*, pages 55–66. SciTePress, 2017.

[GABL17] M. Giraud, A. Anzala-Yamajako, O. Bernard, and **P. Lafourcade**. Practical Passive Leakage-abuse Attacks Against Symmetric Searchable Encryption. In P. Samarati, M. S. Obaidat, and E. Cabello, editors, *Proceedings of the 14th International Joint Conference on e-Business and Telecommunications (ICETE 2017) - Volume 4 : SECRYPT, Madrid, Spain, July 24-26, 2017.*, pages 200–211. SciTePress, 2017.

[KLL17] A. Kumar, C. Lauradoux, and **P. Lafourcade**. Duck Attack on Accountable Distributed Systems. In *14th EAI International Conference on Mobile and Ubiquitous Systems : Computing, Networking and Services, Mobiquitous'17*, Melbourne, Australia, November 7-10 2017.

[SGL+17] S. Sun, D. Gérault, **P. Lafourcade**, Q. Yang, Y. Todo, K. Qiao, and L. Hu. Analysis of AES, SKINNY, and Others with Constraint Programming. *IACR Trans. Symmetric Cryptol.*, 2017(1) :281–306, 2017.

— 2016 —

[BBL16a] O. Blazy, X. Bultel, and **P. Lafourcade**. Anonymizable Ring Signature Without Pairing. In *9th International Symposium on Foundations & Practice of Security (FPS 2016), Québec city, QC, Canada, 24-25-26 October*, 2016.

[BBL16b] O. Blazy, X. Bultel, and **P. Lafourcade**. Two Secure Anonymous Proxy-based Data Storages. In C. Callegari, M. van Sinderen, P. G. Sarigiannidis, P. Samarati, E. Cabello, P. Lorenz, and M. S. Obaidat, editors, *Proceedings of the 13th International Joint Conference on e-Business and Telecommunications (ICETE 2016) - Volume 4 : SECRYPT, Lisbon, Portugal, July 26-28, 2016.*, pages 251–258. SciTePress, 2016.

[BDDL16] X. Bultel, J. Dreier, J. Dumas, and **P. Lafourcade**. Physical Zero-Knowledge Proofs for Akari, Takuzu, Kakuro and KenKen. In E. D. Demaine and F. Grandoni, editors, *8th International Conference on Fun with Algorithms, FUN 2016, June 8-10, 2016, La Maddalena, Italy*, volume 49 of *LIPIcs*, pages 8 :1–8 :20. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, 2016.

[BGG+16] X. Bultel, S. Gambs, D. Gérault, **P. Lafourcade**, C. Onete, and J. Robert. A Prover-Anonymous and Terrorist-Fraud Resistant Distance-Bounding Protocol. In M. Hollick, P. Papadimitratos, and W. Enck, editors, *Proceedings of the 9th ACM Conference on Security & Privacy in Wireless and Mobile Networks, WISEC 2016, Darmstadt, Germany, July 18-22, 2016*, pages 121–133. ACM, 2016.

[BL16a] X. Bultel and **P. Lafourcade**. A Posteriori Openable Public Key Encryption. In J. Hoepman and S. Katzenbeisser, editors, *ICT Systems Security and Privacy Protection - 31st IFIP TC 11 International Conference, SEC 2016, Ghent, Belgium, May 30 - June 1, 2016, Proceedings*, volume 471 of *IFIP Advances in Information and Communication Technology*, pages 17–31. Springer, 2016.

[BL16b] X. Bultel and **P. Lafourcade**. K-time Full Traceable Ring Signature. In *12th International Conference on Availability, Reliability and Security (ARES 2016), Salzburg, Austria, 29 August 2 September*, 2016.

[DLOP16] J. Dumas, **P. Lafourcade**, J. Orfila, and M. Puys. Private Multi-party Matrix Multiplication and Trust Computations. In C. Callegari, M. van Sinderen, P. G. Sarigiannidis, P. Samarati, E. Cabello, P. Lorenz, and M. S. Obaidat, editors, *Proceedings of the 13th International Joint Conference on e-Business and Telecommunications (ICETE 2016) - Volume 4 : SECRYPT, Lisbon, Portugal, July 26-28, 2016.*, pages 61–72. SciTePress, 2016.

[GL16] D. Gérault and **P. Lafourcade**. Related-Key Cryptanalysis of Midori. In *17th International Conference on Cryptology in India, Indocrypt'16, December 11-14, Kolkata*, 2016.

[KGLR16] N. Kahya, N. Ghoualmi, **P. Lafourcade**, and K. Roumaissa. Formal analysis of key management in mobile wimax. In *The 2nd International Conference on Pattern Analysis and Intelligent Systems (IEEE) PAIS'16*, Khenchela, Algeria, November 2016.

[PPL16] M. Puys, M. Potet, and **P. Lafourcade**. Formal Analysis of Security Properties on the OPC-UA SCADA Protocol. In A. Skavhaug, J. Guiochet, and F. Bitsch, editors, *Computer Safety, Reliability, and Security - 35th International Conference, SAFECOMP 2016, Trondheim, Norway, September 21-23, 2016, Proceedings*, volume 9922 of *Lecture Notes in Computer Science*, pages 67–75. Springer, 2016.

— 2015 —

[AGLM15] A. T. Aby, A. Guitton, **P. Lafourcade**, and M. Misson. SLACK-MAC : Adaptive MAC Protocol for Low Duty-Cycle Wireless Sensor Networks. In N. Mitton, M. Erol-Kantarci, A. Gallais, and S. Papavassiliou, editors, *Ad Hoc Networks - 7th International Conference, AdHocNets 2015, San Remo, Italy, September 1-2, 2015, Proceedings*, volume 155 of *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*, pages 69–81. Springer, 2015.

[BGL15] A. Brelurut, D. Gérault, and **P. Lafourcade**. Survey of Distance Bounding Protocols and threats. In *Foundations and Practice of Security - 8th International Symposium, FPS 2015, Clermont-Ferrand, France, 2015*, Lecture Notes in Computer Science. Springer, 2015.

[DGK+15b] J. Dreier, R. Giustolisi, A. Kassem, **P. Lafourcade**, and G. Lenzini. A framework for analyzing verifiability in traditional and electronic exams. In J. Lopez and Y. Wu, editors, *Information Security Practice and Experience - 11th International Conference, ISPEC 2015, May 5 - 8, 2015. Proceedings*, volume 9065 of *Lecture Notes in Computer Science*, pages 514 – 529. Springer, 2015.

[DKL15] J. Dreier, A. Kassem, and **P. Lafourcade**. Formal analysis of e-cash protocols. In *SECRYPT 2015 - Proceedings of the 12th International Conference on Security and Cryptography, Colmar, Alsace, France, 20-22 July, 2015.*, pages 65–75, 2015.

[KFL15] A. Kassem, Y. Falcone, and **P. Lafourcade**. Monitoring Electronic Exams. In E. Bartocci and R. Majumdar, editors, *Runtime Verification - 6th International Conference, RV 2015 Vienna, Austria, September 22-25, 2015. Proceedings*, volume 9333 of *Lecture Notes in Computer Science*, pages 118–135. Springer, 2015.

[PL15] M. Puys and **P. Lafourcade**. Performance Evaluations of Cryptographic Protocols : Verification Tools Dealing with Algebraic Properties. In *Foundations and Practice of Security - 8th International Symposium, FPS 2015, Clermont-Ferrand, France, 2015*, Lecture Notes in Computer Science. Springer, 2015.

— 2014 —

[DGK+14] J. Dreier, R. Giustolisi, A. Kassem, **P. Lafourcade**, G. Lenzini, and P. Y. A. Ryan. Formal Analysis of Electronic Exams. In M. S. Obaidat, A. Holzinger, and P. Samarati, editors, *SECRYPT 2014 - Proceedings of the 11th International Conference on Security and Cryptography, Vienna, Austria, 28-30 August, 2014*, pages 101–112. SciTePress, 2014. Best Paper Award.

[DJL14] J. Dreier, H. Jonker, and **P. Lafourcade**. Secure Auctions without Cryptography. In A. Ferro, F. Luccio, and P. Widmayer, editors, *Fun with Algorithms - 7th International Conference, FUN 2014, Lipari Island, Sicily, Italy, July 1-3, 2014. Proceedings*, volume 8496 of *Lecture Notes in Computer Science*, pages 158–170. Springer, 2014.

[JL14b] R. Jamet and **P. Lafourcade**. (In)Corruptibility of Routing Protocols. In *Foundations and Practice of Security - 7th International Symposium, FPS 2014, Montréal, Canada, 2014*, Lecture Notes in Computer Science. Springer, 2014. Best Paper Award.

[KLL14b] A. Kassem, **P. Lafourcade**, and Y. Lakhnech. Formal Verification of e-Reputation Protocols. In *Foundations and Practice of Security - 7th International Symposium, FPS 2014, Montréal, Canada*, Lecture Notes in Computer Science. Springer, 2014.

[KLL14c] A. Kumar, **P. Lafourcade**, and C. Lauradoux. Performances of cryptographic accumulators. In *IEEE 39th Conference on Local Computer Networks, LCN 2014, Edmonton, AB, Canada, 8-11 September, 2014*, pages 366–369. IEEE Computer Society, 2014.

[MCL14b] I. Mansour, G. Chalhoub, and **P. Lafourcade**. Secure Multihop Key Establishment Protocols for Wireless Sensor Networks. In Z. Kotulski, B. Ksiezopolski, and K. Mazur, editors, *Cryptography and Security Systems - Third International Conference, CSS 2014, Lublin, Poland, September 22-24, 2014. Proceedings*, volume 448 of *Communications in Computer and Information Science*, pages 166–177. Springer, 2014.

[MCLD14] I. Mansour, G. Chalhoub, **P. Lafourcade**, and F. Delobel. Secure Key Renewal and Revocation for Wireless Sensor Networks. In *IEEE 39th Conference on Local Computer Networks, LCN 2014, Edmonton, AB, Canada, 8-11 September, 2014*, pages 382–385. IEEE Computer Society, 2014.

[MRC+14] I. Mansour, D. Rusinek, G. Chalhoub, **P. Lafourcade**, and B. Ksiezopolski. Multihop Node Authentication Mechanisms for Wireless Sensor Networks. In S. Guo, J. Lloret, P. Manzoni, and S. Ruehrup, editors, *Ad-hoc, Mobile, and Wireless Networks - 13th International Conference, ADHOC-NOW 2014, Benidorm, Spain, June 22-27, 2014 Proceedings*, volume 8487 of *Lecture Notes in Computer Science*, pages 402–418. Springer, 2014.

— 2013 —

[ADJL13b] K. Altisen, S. Devismes, R. Jamet, and **P. Lafourcade**. SR3 : Secure Resilient Reputation-based Routing. In *IEEE International Conference on Distributed Computing in Sensor Systems, DCOSS 2013, Cambridge, MA, USA, May 20-23, 2013*, pages 258–265. IEEE, 2013.

[DDL13] J. Dreier, J.-G. Dumas, and **P. Lafourcade**. Brandt's Fully Private Auction Protocol Revisited. In A. Youssef, A. Nitaj, and A. E. Hassanien, editors, *Progress in Cryptology - AFRICACRYPT 2013, 6th International Conference on Cryptology in Africa, Cairo, Egypt, June 22-24, 2013. Proceedings*, volume 7918 of *Lecture Notes in Computer Science*, pages 88–106. Springer, 2013.

[DELL13] J. Dreier, C. Ene, **P. Lafourcade**, and Y. Lakhnech. On Unique Decomposition of Processes in the Applied -Calculus. In F. Pfenning, editor, *Foundations of Software Science and Computation Structures - 16th International Conference, FOSSACS 2013, Held as Part of the European Joint Conferences on Theory and Practice of Software, ETAPS 2013, Rome, Italy, March 16-24, 2013. Proceedings*, volume 7794 of *Lecture Notes in Computer Science*, pages 50–64. Springer, 2013.

[DJL13] J. Dreier, H. Jonker, and **P. Lafourcade**. Defining verifiability in e-auction protocols. In K. Chen, Q. Xie, W. Qiu, N. Li, and W.-G. Tzeng, editors, *8th ACM Symposium on Information, Computer and Communications Security, ASIA CCS '13, Hangzhou, China - May 08 - 10, 2013*, pages 547–552. ACM, 2013.

[DLL13] J. Dreier, **P. Lafourcade**, and Y. Lakhnech. Formal Verification of e-Auction Protocols. In D. A. Basin and J. C. Mitchell, editors, *Principles of Security and Trust - Second International Conference, POST 2013, Held as Part of the European Joint Conferences on Theory and Practice of Software, ETAPS 2013, Rome, Italy, March 16-24, 2013. Proceedings*, volume 7796 of *Lecture Notes in Computer Science*, pages 247–266. Springer, 2013.

[GLL13] M. Gagné, **P. Lafourcade**, and Y. Lakhnech. Automated Security Proofs for Almost-Universal Hash for MAC Verification. In J. Crampton, S. Jajodia, and K. Mayes, editors, *Computer Security - ESORICS 2013 - 18th European Symposium on Research in Computer Security, Egham, UK, September 9-13, 2013. Proceedings*, volume 8134 of *Lecture Notes in Computer Science*, pages 291–308. Springer, 2013.

[JL14a] R. Jamet and **P. Lafourcade**. Discovering Flaws in IDS Through Analysis of Their Inputs. In J. L. Danger, M. Debbabi, J.-Y. Marion, J. García-Alfaro, and A. N. Zincir-Heywood, editors, *Foundations and Practice of Security - 6th International Symposium, FPS 2013, La Rochelle, France, October 21-22, 2013, Revised Selected Papers*, volume 8352 of *Lecture Notes in Computer Science*. Springer, 2014.

[KLL14a] A. Kassem, **P. Lafourcade**, and Y. Lakhnech. A More Realistic Model for Verifying Route Validity in Ad-Hoc Networks. In J. L. Danger, M. Debbabi, J.-Y. Marion, J. García-Alfaro, and A. N. Zincir-Heywood, editors, *Foundations and Practice of Security - 6th International Symposium, FPS 2013, La Rochelle, France, October 21-22, 2013, Revised Selected Papers*, volume 8352 of *Lecture Notes in Computer Science*. Springer, 2014.

— 2012 —

[ADGL12] K. Altisen, S. Devismes, A. Gerbaud, and **P. Lafourcade**. Analysis of Random Walks Using Tabu Lists. In G. Even and M. M. Halldórsson, editors, *Structural Information and Communication Complexity - 19th International Colloquium, SIROCCO 2012, Reykjavik, Iceland, June 30-July 2, 2012, Revised Selected Papers*, volume 7355 of *Lecture Notes in Computer Science*, pages 254–266. Springer, 2012.

[DLL12b] J. Dreier, **P. Lafourcade**, and Y. Lakhnech. A Formal Taxonomy of Privacy in Voting Protocols. In *Proceedings of IEEE International Conference on Communications, ICC 2012, Ottawa, ON, Canada, June 10-15, 2012*, pages 6710–6715. IEEE, 2012.

[DLL12c] J. Dreier, **P. Lafourcade**, and Y. Lakhnech. Defining Privacy for Weighted Votes, Single and Multi-voter Coercion. In S. Foresti, M. Yung, and F. Martinelli, editors, *Computer Security - ESORICS 2012 - 17th European Symposium on Research in Computer Security, Pisa, Italy, September 10-12, 2012. Proceedings*, volume 7459 of *Lecture Notes in Computer Science*, pages 451–468. Springer, 2012.

[GKL12] N. Ghoualmi, N. Kahya, and **P. Lafourcade**. Key Management Protocol in WIMAX revisited. In *The Third International Conference on Communications Security and Information Assurance (CSIA 2012)*, Delhi, India, May 2012. Springer.

— 2011 —

[DLL12d] J. Dreier, **P. Lafourcade**, and Y. Lakhnech. Vote-Independence : A Powerful Privacy Notion for Voting Protocols. In J. García-Alfaro and **P. Lafourcade**, editors, *Foundations and Practice of Security - 4th Canada-France MITACS Workshop, FPS 2011, Paris, France, May 12-13, 2011, Revised Selected Papers*, volume 6888 of *Lecture Notes in Computer Science*, pages 164–180. Springer, 2012.

[FLA11] L. Fousse, **P. Lafourcade**, and M. Alnuaimi. Benaloh's Dense Probabilistic Encryption Revisited. In *Progress in Cryptology - AFRICACRYPT 2011 - 4th International Conference on Cryptology in Africa, Dakar, Senegal, July 5-7, 2011. Proceedings*, volume 6737 of *Lecture Notes in Computer Science*, pages 348–362. Springer, 2011.

[GLLSN12] M. Gagné, **P. Lafourcade**, Y. Lakhnech, and R. Safavi-Naini. Automated Verification of Block Cipher Modes of Operation, an Improved Method. In J. García-Alfaro and **P. Lafourcade**, editors, *Foundations and Practice of Security - 4th Canada-France MITACS Workshop, FPS 2011, Paris, France, May 12-13, 2011, Revised Selected Papers*, volume 6888 of *Lecture Notes in Computer Science*, pages 23–31. Springer, 2012.

— 2010 —

[CDE+11] J. Courant, M. Daubignard, C. Ene, **P. Lafourcade**, and Y. Lakhnech. Automated Proofs for Asymmetric Encryption. In D. Dams, U. Hannemann, and M. Steffen, editors, *Concurrency, Compositionality, and Correctness, Essays in Honor of Willem-Paul de Roever*, volume 5930 of *Lecture Notes in Computer Science*, pages 300–321. Springer, 2011.

[TWE+10] J. Tharaud, S. Wohlgemuth, I. Echizen, N. Sonehara, G. Müller, and **P. Lafourcade**. Privacy by Data Provenance with Digital Watermarking - A Proof-of-Concept Implementation for Medical Services with Electronic Health Records. In *Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP 2010), Darmstadt, Germany, 15-17 October, 2010, Proceedings*, pages 510–513. IEEE Computer Society, 2010.

— 2009 —

[CLN09] C. J. Cremers, **P. Lafourcade**, and P. Nadeau. Comparing State Spaces in Automatic Protocol Analysis. *Formal to Practical Security*, 5458/2009 :70–94, 2009.

[GLLS09a] M. Gagne, **P. Lafourcade**, Y. Lakhnech, and R. Safavi-Naini. Automated Proofs for Encryption Modes. In *13th Annual Asian Computing Science Conference Focusing on Information Security and Privacy : Theory and Practice (ASIAN0'9)*, Urumqi, China, oct 2009.

[LTV09] **P. Lafourcade**, V. Terrade, and S. Vigier. Comparison of Cryptographic Verification Tools Dealing with Algebraic Properties. In P. D. Joshua Guttman, editor, *sixth International Workshop on Formal Aspects in Security and Trust, (FAST'09)*, Eindhoven, Netherlands, nov 2009.

— 2008 —

[CDE+08a] J. Courant, M. Daubignard, C. Ene, **P. Lafourcade**, and Y. Lakhnech. Automated Proofs for Asymmetric Encryption. In *15th ACM Computer and Communications Security Conference (CCS'08)*, 2008.

— 2006 —

[DLLT06] S. Delaune, **P. Lafourcade**, D. Lugiez, and R. Treinen. Symbolic Protocol Analysis in Presence of a Homomorphism Operator and *Exclusive Or*. In M. Buglesi, B. Preneel, V. Sassone, and I. Wegener, editors, *Proceedings of the 33rd International Colloquium on Automata, Languages and Programming (ICALP'06) — Part II*, volume 4052 of *Lecture Notes in Computer Science*, pages 132–143, Venice, Italy, July 2006. Springer.

— 2005 —

[LLT05] **P. Lafourcade**, D. Lugiez, and R. Treinen. Intruder Deduction for AC-like Equational Theories with Homomorphisms. In J. Giesl, editor, *Proceedings of the 16th International Conference on Rewriting Techniques and Applications (RTA'05)*, volume 3467 of *Lecture Notes in Computer Science*, pages 308–322, Nara, Japan, April 2005. Springer.

Édition de proceedings

— 2012 —

[GAL12] J. García-Alfaro and **P. Lafourcade**, editors. *Foundations and Practice of Security - 4th Canada-France MITACS Workshop, FPS 2011, Paris, France, May 12-13, 2011, Revised Selected Papers*, volume 6888 of *Lecture Notes in Computer Science*. Springer, 2012.

Workshops

— 2009 —

[GLLS09b] M. Gagne, **P. Lafourcade**, Y. Lakhnech, and R. Safavi-Naini. Automated Proofs for Encryption Modes. In R. Kuesters, editor, *Workshop on Formal and Computational Cryptography, (FCC'09)*, Port Jefferson NY, USA, jul 2009.

[ML09] S. Malladi and **P. Lafourcade**. Prudent engineering practices to prevent type-flaw attacks under algebraic properties. In H. Comon-Lundh and C. Meadows, editors, *Workshop on Security and Rewriting Techniques, (SecReT'09)*, Port Jefferson NY, USA, jul 2009.

— 2008 —

[CDE+08b] J. Courant, M. Daubignard, C. Ene, **P. Lafourcade**, and Y. Lakhnech. Automated Proofs for Asymmetric Encryption. In *Proceedings of the LICS-Affiliated Workshop on Foundations of Computer Security and Automated Reasoning for Security Protocol Analysis*, Pittsburg, USA, 2008.

[Laf08] **P. Lafourcade**. Relation between intruder deduction problem and unification. In *Proceedings of the LICS-Affiliated 3rd International Workshop on Security and Rewriting Techniques (SecReT'08)*, 2008.

— 2006 —

[Laf07a] **P. Lafourcade**. Intruder Deduction for the Equational Theory of *Exclusive-or* with Commutative and Distributive Encryption. In M. Fernández and C. Kirchner, editors, *Proceedings of the 1st International Workshop on Security and Rewriting Techniques (SecReT'06)*, volume 171 of *Electronic Notes in Theoretical Computer Science*, pages 37–57, Venice, Italy, July 2007. Elsevier Science Publishers.

[LLT06] **P. Lafourcade**, D. Lugiez, and R. Treinen. ACUNh : Unification and Disunification Using Automata Theory. In J. Levy, editor, *Proceedings of the 20th International Workshop on Unification (UNIF'06)*, pages 6–20, Seattle, Washington, USA, August 2006.

7 Conférences Françaises

— 2021 —

[DL21] S. Devismes and **P. Lafourcade**. Un jour sans fin. In *ALGOTEL 2021 — 23èmes Rencontres Francophones sur les Aspects Algorithmiques des Télécommunications, Jun 2021, La Rochelle, France*, 2021.

— 2020 —

[BDL20c] Q. Bramas, S. Devismes, and **P. Lafourcade**. Vers l'infini et au delà. In *ALGOTEL 2020 - 22èmes Rencontres Francophones sur les Aspects Algorithmiques des Télécommunications*, Lyon, France, 2020.

— 2017 —

[BGG+17] X. Bultel, S. Gambs, D. Gérault, **P. Lafourcade**, and J.-M. R. Cristina Onete. Spade : un protocole délimiteur de distance anonyme et résistant à la fraude terroriste. In *ALGOTEL 2017 - 19èmes Rencontres Francophones sur les Aspects Algorithmiques des Télécommunications, May 2017, Quiberon, France*, 2017.

— 2014 —

[MLC14a] I. Mansour, **P. Lafourcade**, and G. Chalhoub. Mécanismes d'authentification pour des réseaux de capteurs sans fil multi-sauts. In *16èmes Rencontres Francophones pour les Aspects Algorithmiques des Télécommunications, Algotel'2014, Le-Bois-Plage-en-Ré, France*, 2014.

[MLC14b] I. Mansour, **P. Lafourcade**, and G. Chalhoub. Révocation et renouvellement séecurisées de clés pour les RCSF. In *Journées Nationales de Communications Terrestres, JNCT'14, Blagnac France*, 2014.

— 2013 —

[ADJL13a] K. Altisen, S. Devismes, R. Jamet, and **P. Lafourcade**. Routage sécurisé et résilient pour réseaux de capteurs sans fils. In *15èmes Rencontres Francophones pour les Aspects Algorithmiques des Télécommunications Algotel 2013*, 2013.

— 2011 —

[ADLP11] K. Altisen, S. Devismes, **P. Lafourcade**, and C. Ponsonnet. Routage par marche aléatoire à listes tabous. In *In Proceedings of 13èmes Rencontres Francophones pour les Aspects Algorithmiques des Télécommunications, Algotel'2011. Pages 87-90, May 23-26, 2011. Cap Estérel.*, page 5, 2011.

10 Articles en pédagogie

— 2021 —

[LM21b] **P. Lafourcade** and M. More. Des énigmes pour s'initier à la cryptographie. In *AU FIL DES MATHS n° 540, LE BULLETIN DE L'APMEP n° 540, Référence AFDM 540*, 2021.

— 2020 —

[JLMP20] M. Journault, **P. Lafourcade**, M. More, and R. Poulain. Une preuve pour le lycée de l'indécidabilité du problème de l'arrêt. In *Didapro 8, - DidaSTIC L'informatique, objets d'enseignements - enjeux épistémologiques, didactique et de formation*, feb 2020.

— 2018 —

[DDFLM18] B. Drot-Delange, S. Fleury, **P. Lafourcade**, and M. More. Un tour de magie pour introduire la représentation binaire des nombres. In *APMEP Association des Professeurs de Mathé matiques de l'Enseignement Public*, pages 17–34, 2018.

— 2017 —

[Laf17] **P. Lafourcade**. Vérifier la sécurité de nos communications. Interstices, Octobre 2017.

— 2015 —

[HBB+15] C. Hoffmann, A. Briançon, P. Brulard, J.-L. Cracowski, J. Douady, M. Houssay-Holzschuch, **P. Lafourcade**, I. L. Brun, S. Seidelin, and S. Térouanne. Les émulateurs pédagogiques : une source d'innovations qui se construit à l'Université Joseph Fourier de Grenoble. In *8ème édition du colloque Questions de Pédagogie dans l'Enseignement Supérieur, QPES'15*, 2015.

— 2012 —

[HDB+12] C. Hoffmann, J. Douady, M. Billon, M. Bonvalot, F. Courtois, **P. Lafourcade**, I. L. Brun, E. Moraux, C. Rist, and M.-F. Soulage. Deux approches pour une formation opérante des étudiants de l'Université Joseph Fourier (Grenoble, France) aux méthodes de travail universitaire. In *27e Congrès International de Pédagogie Universitaire (Association Internationale de Pédagogie Univeersitaire AIPU)*, Trois-Rivières, Québec, may 2012.

— 2011 —

[Laf11a] **P. Lafourcade**. La génération Y . Colloque Pédagogique National GEII, june 2011. Angoulême, publié dans le journal des IUTs GEII.

[Laf11b] **P. Lafourcade**. Techniques d'apprentissage en liaison avec l'analyse cognitive. Colloque Pédagogique National GEII, june 2011. Angoulême, publié dans le journal des IUTs GEII.

— 2010 —

[DP10] M. Daubignard and L. Pascal. Je veux te dire un secret mais tout le monde m'écoute. Visions Croisées, magazine de vulgarisation scientifique édité par les moniteurs du CIES de l'Académie de Grenoble, march 2010.

— 2007 —

[DGL07] D. Dobrowolski, A. Grabowska, and **P. Lafourcade**. The Concept of Developing E-learnung Repository - Metadata and Group Work. In *ICETA 2007, 5 th International Conference on Emerging e-Learning Technologies and Applications*, pages 217–220, The High Tatra, Slovakia, 2007.

C Encadrements

17 Encadrements de thèses

1. **Encadrant à 50 %** de la thèse de doctorat de Dhekra Mahmoud, sur la sécurité des e-examens. 50% Jannik Dreier (LORIA). Thèse débutée en **mai 2022**.
   — Financement : Bourse ANR SEVERITAS.
2. **Encadrant à 30 %** de la thèse de doctorat de Charles Olivier-Anclin, sur la signature électronqiue. 40% Xavier Bultel (LIFO/INSA Val de Loire), 30% Mirko Koscina (Be-Pay). Thèse débutée en **avril 2022**.
   — Financement : Bourse Cifre.
   — Publications : FPS 2021.
3. **Encadrant à 30 %** de la thèse de doctorat de Gael Marcadet, sur les calculs multi-parties sécurisés. 40% Marta Soare (LIFO/Univ. Orléans), 30% (LIFO/INSA Val de Loire). Thèse débutée en **septembre 2021**.
   — Financement : Bourse Projet D4N.
   — Publications : JAIR 2022, ICDE'22 (Démo).
4. **Encadrant à 30 %** de la thèse de doctorat de Fréderic Hayek, sur la sécurité des blockchains. 40% Ariane Tichit (CERDI/UCA), 30% Mirko Koscina (Be-Pay) . Thèse débutée en **septembre 2021**.
   — Financement : Bourse Chaire industrielle.
5. **Encadrant à 50 %** de la thèse de doctorat de Léo Robert, sur la sécurité des protocoles de communication pour la 5G. 25% Cristina Onete (XLIM Limoges) et 25% Olivier Blazy (XLIM Limoges). Thèse débutée en **octobre 2019**.
   Financement : Projet ANR MOBIS5.
6. **Encadrant à 50 %** de la thèse de doctorat d'Octavio Perez Kempner, sur la sécurité des ZKP. 50% David Naccache (ENS Paris). Thèse débutée en **octobre 2018**.
   — Financement : CIFRE avec Almerys.
7. **Encadrant à 50 %** de la thèse de doctorat de Marius Lombard-Platet, sur la sécurité de la blockchain. 50% David Naccache (ENS Paris). Thèse débutée en **janvier 2018**.
   — Financement : CIFRE avec Almerys.
   — Publications : ISPEC 2019 [CLLS19], FPS 2019 [LPL19], IPL [LL20], TrustCom [CLLS20], Journal of Computer Security [CLLS22], Journal of Wireless Mobile Networks Ubiquitous Computer Dependable Application. [NRLSL21]
8. **Encadrant à 30 %** de la thèse de doctorat de Mirko Koscina, sur la sécurité des mécanismes de consensus. 70% David Naccache (ENS Paris). Thèse débutée en **janvier 2018**.
   — Financement : CIFRE avec Almerys.
   — Actuellement en post-doctorant au Luxembourg avec A. Biryukov.
   — Publications : ICTAC 2019 [CKY+19b], SECRYPT 2019 [CKY+19a],
9. **Encadrant à 30 %** de la thèse de doctorat de Marwa Chaieb, sur le vote électronique et la blockchain. 50% Souheib Yousfi, 20% Riadh Robbana.Marius (Tunis, Tunisie). Thèse débutée en **septembre 2017**.
   — Financement : Bourse tunisienne.
   — Actuellement : Enseignante contractuelle à Tunis.
   — Publications : ICTAC 2019 [CKY+19b], SECRYPT 2019 [CKY+19a], EMMECIS 2018 [CYLR18].

10. **Encadrant à 50 %** de la thèse de doctorat de Matthieu Giraud, "Secure Distributed MapReduce Protocols". Thèse débutée en **octobre 2016**, soutenance le **24 septembre 2019**.
    - Financement : bourse projet région DIS-4.
    - Actuellement en poste d'ingénieur chez Thales puis chez CryptoNext.
    - Publications : WISTP'19 [DGG+19], 2 × SECRYPT'19 [CGLY19a, CGLY19b], FPS'18 [BCG+18], SECRYPT'18 [CGLY18], RCIS'18 [BDG+18], ARES'17 [BCGL17], SECRYPT'17 [BLGR17], ProveSec'17 [BDG+17].
11. **Encadrant à 100 %** de la thèse de doctorat de David Gérault, "Security Analysis of Contactless Communication Protocols". Thèse débutée en **octobre 2015**, soutenance le **27 novembre 2018**.
    - Financement : bourse projet région DIS-4.
    - Actuellement en poste de chercheur à Abudabi.
    - Publications : AI'22 [GLMS20], IPL'18 [GLMS18], FSE'17 [SGL+17], AsiaCCS'17 [ABG+17], ProvSec'17 [BDG+17], Wisec'17 [BGLO17], IndoCrypt'16 [GL16], Wisec'16 [BGG+16].
12. **Encadrant à 100 %** de la thèse de doctorat de Xavier Bultel, "Mécanismes de délégation pour les primitives de cryptographie à clef publique". Thèse débutée en **octobre 2014**, soutenance le **17 mai 2018**.
    - Financement : bourse de la chaire de confiance numérique de la Fondation d'Auvergne.
    - Actuellement maître de conférences à l'INSA Val de Loire, depuis septembre 2019.
    - Publications : Financial Cryptography 19 [BBLPK21, BL19], PKC'19 [BLL+19], Cryptologia 2017 [BDLM17], FPS'18 [BCG+18], FUN'18 [BDDL18], RICS'18 [BDG+18], SSS'18 [BDD+18], ARES'17 [BCGL17], CANS'17 [BL17], AsiaCCS'17 [ABG+17], ProvSec'17 [BDG+17], ARES'16 [BL16b], FPS'16 [BBL16a], FUN'16 [BDDL16], IFIP SEC'16 [BL16a], SECRYPT'16 [BBL16b], WISEC'16 [BGG+16].
13. **Encadrant à 50 %** de la thèse de doctorat d'Amrit Kumar, "Sécurité et protection de la vie privée pour le calcul déporté". 50% Cédric Lauradoux (INRIA Grenoble). Thèse débutée en **novembre 2013**, soutenance le **20 octobre 2016**.
    - Financement : bourse du Labex Persyval.
    - Actuellement à Singapour, Chief Scientific Officer à Zilliqa (une cryptomonnaie).
    - Publications : MobiQuitous 2017 [KLL17].
14. **Encadrant à 90 %** de la thèse de doctorat d'Ali Kassem, sur la vérification de protocoles d'examen. 10% Yassine Lakhnech (Verimag Grenoble). Thèse débutée en **septembre 2012** soutenance le **18 septembre 2015**.
    - Financement : bourse ministérielle.
    - Actuellement post-doc à l'INRIA.
    - Publications : FPS 2013, SECRYPT 2014, FPS 2014, ISPEC 2015, SECRYPT 2015, RV 2015, Communications in Computer and Information Science 2015, Formal Methods in System Design 2017.
15. **Encadrant à 100 %** de la thèse de doctorat de Raphaël Jamet, intitulée « Protocols and Models for the Security of Wireless Ad-Hoc Networks ». Thèse débutée en **octobre 2011** et **soutenue le 3/10/2014**.
    - Financement : bourse ministérielle et contrat de moniteur CIES.

— Actuellement expert sécurité chez Google (Zürich).
— Publications : FPS 2013, Algotel 2013, DCOSS 2013, FPS 2014, Wireless Networks 2016.

16. **Encadrant à 50 %** de la thèse de doctorat de Jannik Dreier, intitulée « *Formal Verification of Voting and Auction Protocols : From Privacy to Fairness and Verifiability* ». 50% Yassine Lakhnech (Verimag Grenoble). Thèse débutée en **octobre 2010** et **soutenue le 25/10/2013**.
    — Financement : Contrat sur projet et contrat de vacataire.
    — Actuellement enseignant chercheur au LORIA.
    — Publications : FPS 2011, ICC 2012, ESORICS 2012, AFRICACRYPT 2013, ASIACCS 2013, FOSSACS 2013, POST 2013, SECRYPT 2014, FUN 2014, ISPEC 2015, SECRYPT 2015, Journal of Computer Security 2015, Communications in Computer and Information Science 2015, FUN 2016, Theoretical Computer Science 2016, Cryptologia 2017, FPS 2017, SECRYPT 2017, SSS 2018, FUN 2018, RCIS 2018, Computer & Security 2018
17. **Encadrant à 50 %** de la thèse de doctorat de Marion Daubignard, intitulée « *Formal Methods for Concrete Security Proofs* ». 50% Yassine Lakhnech (Verimag Grenoble). Thèse débutée en **septembre 2009** et **soutenue le 12/01/2012**.
    — Financement : bourse ministérielle et contrat de moniteur CIES.
    — Actuellement en poste à l'ANSSI.
    — Publications : CCS 2008, LICS-Affiliated Workshop on Founda- tions of Computer Security and Automated Reasoning for Security Protocol Analysis 2008, Journal of Automated Reasoning 2010.

Encadrements post-doctoral

1. **Encadrant à 50%** de Luc Libralesso, en stage post-doctoral au LIMOS d'octobre 2020 à décembre 2021 dans le cadre du projet ANR DECRYPT. (50% François Delobel).
2. **Encadrant à 33%** d'Antoine Gerbaud, en stage post-doctoral à VERIMAG de septembre 2011 à septembre 2012 dans le cadre du projet MSTIC UJF Terra. (33% Karine Altisen ; 33% Stéphane Devismes).
3. **Encadrant à 100%** de Martin Gagné, en stage post-doctoral à VERIMAG de septembre 2010 à septembre 2012 dans le cadre du projet ANR PROSE et ANR.

Encadrements de Master 2 Recherche

1. En 2011, **encadrant à 33%** de Clément Ponsonnet, étudiant en Master 2 MAI (Mathématiques Appliquées et Industrielles) à l'UJF. (33% Karine Altisen ; 33% Stéphane Devismes).
2. En 2011, **encadrant à 100%** de Jean-Pierre Cyndia, étudiante en Master 2 SCCI de l'UJF.
3. En 2011, **encadrant à 100%** de Bashar Saleh, étudiant en Master 2 SCCI de l'UJF.
4. En 2012, **encadrant à 100%** d'Ali Kassem, étudiant en Master 2 SCCI de l'UJF.
5. En 2014, **encadrant à 50%** de Firas Ben Njima, étudiant en Master 2 à l'Université de Monastir (Tunisie) 50% Leila Benabdelghani (Monastir).
6. En 2015, **encadrant à 100%** de Agnès Brelurut, étudiante en Master 2 à l'Université de Bordeaux.
7. En 2016, **encadrant à 100%** d'Elliot Blot, Master 2 de l'Université de Bordeaux, financé par le projet européen C-ROADS. Publications : FPS'17.

8. En 2018, **encadrant à 100%** de Lihua Ye, Master 2 de l'Institut d'informatique de Clermont financé par une bourse de l'Université de Harbin (Chine). Publications : FPS'18, 2 × SECRYPT 19.
9. En 2019, **encadrant à 60%** de Daniela Pizzuti Master 2 de l'Université de Grenoble, financé par Domraider, 40% Etienne Roudeix. Publication : FPS'19.
10. En 2019, **encadrant à 60%** de Laure Bachelet Master 2 de l'Université de Bordeaux, financé par l'entreprise Coffreo, 40% Éric Pagan.
11. En 2020, **encadrant à 33%** d'Anatole Delabrouille Master 2 de l'Université de Bordeaux, financé par le LIMOS, 33% Radu Ciucanu et 33% Marta Soare.
12. En 2021, **encadrant à 33%** de Gael Marcadet, Master 2 de l'Université d'Orléans, financé par le LIFO, 33% Radu Ciucanu et 33% Marta Soare.
13. En 2021, **encadrant à 50%** de Charles Olivier, Master 2 de l'Université de Versailles, financé par Be-Pay, 50% Mirko Koscina.
14. En 2021, **encadrant à 100%** Frédéric Hayek, Master 2 de l'Université de Grenoble, financé par le Chèque Inovation Recherche.
15. En 2021, **encadrant à 50%** d'Ana Margarita Rodriguez Cordero, Master 2 de l'Université de Grenoble, financé par le projet ANR DECRYPT, 50% François Delobel.
16. En 2021, **encadrant à 33%** d'Alexis Vannaire, Master 2 de l'Université Clermont Auvergne, financé par un Chèque Inovation Recherche, 33% Paul-Marie Grollemund et 33% Kévin Atighehchi.
17. En 2022, **encadrant à 50%** de Dhekra Mahmoud, Master 2 de l'Université de Bordeaux, financé par une bourse de Télécom Paris, 50% Mounira Mshali

Autres encadrements orientés Recherche

— Encadrement d'un stage de L3 de l'ENS Lyon, Carine Séraphim (été 2014).
— Encadrement d'un stage de 1ère année d'ISIMA sur le chiffrement ADFGVX, Anne-Lise Michel et Victor Salard (février - mai 2015).
— Encadrement d'un stage de 3e année d'ISIMA sur la cryptographie visuelle en 3D, Jean-Paul Roussel et Quentin Desmestre, (octobre 2014 - mars 2015).
— Encadrement d'un stage de 3e année d'ISIMA sur la sécurité des protocoles de communication sans contact, Damien Tessyer, (octobre 2015 - mars 2016).
— Encadrement d'un stage de 3e année d'ISIMA sur l'authentification par code PIN, Vicent Marlin et Timothée Kheyrkhah, (octobre 2015 - mars 2016).
— Encadrement d'un stage de 3e année d'ISIMA sur l'implémentation de SPADE, un jeu de carte en ligne sécurisé, (octobre 2018 - mars 2019).
— Encadrement d'un stage de 3e année d'ISIMA sur l'ordinateur post-quantique et la cryptographie, Charline Grenier (octobre 2019 - mars 2020).
— Encadrement d'un stage de 3e année d'ISIMA sur l'intégration de PKI sur SCADA, Valentin Ramirez et Grégory Wychowaniec (octobre 2019 - mars 2020).
— Encadrement d'un stage de 3e année d'ISIMA sur l'implémentation de Conspiracy Santa une application de partage de cadeaux, Antoine Sicard et William Masson (octobre 2019 - mars 2020).
— Encadrement d'un stage de 3e année d'ISIMA sur le Reverse Engineering de circuit PCB,

William Legourd (mai 2022 - septembre 2022).

— Encadrement d'un stage de 3e année d'ISIMA sur l' implémentation d'une version améliorée du protocole de la messagerie sécurisée instantanée SIGNAL, Cédric Salette (mai 2022 - septembre 2022).

— Encadrement d'un stage de 3e année d'ISIMA sur l'implementation d'un keyswitching d'AES en FHE, Pierre Hitsch et Davy Million (octobre 2021-mars 2022).

— Encadrement d'un stage de 3e année d'ISIMA sur ;implementation de variantes de SIGNAL, Maxime Audigié etYassine Bengana (octobre 2021-mars 2022)

C.1 Exposés invités

Je ne mentionne pas les exposés effectués lors des présentations en conférence de mes publications.

1. Exposé invité à l'antenne de Paris-Dauphine à Tunis, le 18 mars 2021, "*Introduction au fonctionnement de Bitcoin et la Blockchain*.
2. Exposé invité au festival "Math en Scène", le 6 mars 2021, "*Les scientifiques dans les séries TV, Mythe ou réalité ?*".
3. Exposé invité au Workshop "Blockchains & Cryptocurrencies, le 5 mars 2021, "*Preuve de comportement : application à une monnaie éco-responsable EcoMobiCoin*" à Grenoble.
4. Exposé invité au festival "Math en Scène", en mars 2020, Castanet Tolosan, "*La révolution Blockchain*".
5. Exposé d'ouverture du département STID option cybersécurité à Aurillac, le 10 septembre 2019, "*Introduction à la sécurité*".
6. Exposés aux journées AUDACES (AUvergne, Développement d'Applications et Calcul en Environnement Scientifique), en mai 2019, "*RGPD*".
7. Exposé à Pint of Science, en mai 2019, "*L'épopée Bitcoin"*.
8. Exposé invité à l'INSA Bourges, en avril 2019, "*Secure Grouping and Aggregation with MapReduce*".
9. Exposé sur bitcoin et la monnaie à l'Université Ouverte de l'Université Clermont Auvergne, en février 2019, "*Comment fonctionne Bitcoin et la Blockchain ?*".
10. Exposé à la journée mobilité durable de l'école Sigma, en janvier 2019, "*Security in connected autonomous vehiculars*".
11. Exposé à la deuxième édition du forum *Génération 2050* organisé par La Tribune, à l'Opéra de Lyon, le 3 décembre 2018. Exposé avec Arian Tichit devant plus de 200 personnes (professionnels, étudiants, chercheurs). "*Les crypto-monnaies, une transformation technologique... et sociale ?*"
12. Exposé à TeDx Salon Clermont-Ferrand, mars 2018, "*La sécurité des Blockchains*".
13. Exposé à Clermont Innovation Week, avril 2018, "*Le RGPD et les Blockchains*".
14. Exposé invité à la journée sur la « Mobilité innovante » du Labex IMOBS3, janvier 2017 à Clermont Ferrand, *Comment borner la distance véhicule-véhicule ou véhicule-infrastructure, peut aider à sécuriser les échanges de données ?*".
15. Journée de formation à l'IRUP de St-Étienne, en mai 2017, "*Apprentissage et émotions*".

16. Exposé invité à la rencontre *Open Source et sécurité pour l'Internet des Objets*, devant plus de 60 personnes, mai 2017, Paris INS2I, "*Distance bounding for Securing IoT*".
17. Exposé invité à à Beijing Chinese Academy of Sciences, en juillet 2017, "*Automatic Proofs for Cryptographic Primitives : Public Encryption, Encryption Modes, MACs*".
18. Exposé à école de droit de l'UCA, octore 2017, "*Cyberguerre informatique une réalité*".
19. Invitation à l'ambassade française d'Atlanta (USA), en octobre 2016 pour une rencontre entre chercheurs français et américains sur la cybersécurité. "*A Posteriori Openable Public Key Encryption*".
20. Orateur invité aux journées annuelles de l'ARC 6 Rhône Alpes, pour plus de 80 doctorants, en novembre 2016, "*Formal Methods and Security*".
21. Invité pour une table ronde aux journées annuelles du centre Jacques Cartier en novembre 2016 à Lyon devant plus de 200 industriels et politiques.
22. Exposé invité aux journées de l'ANSSI et l'OZSSI à Clermont-Ferrand en novembre 2016, "*Proximity Devices Everywhere*".
23. Exposé invité au Lycée Camille Claudel, avril 2016, "*La sécurité, quelle confiance ?*"
24. Invité au séminaire du Labex UCN Eurecom, en février 2016 à Sophia, "*Security Analysis of Electronic Exams*".
25. Exposé sur la cryptographie à l'Université Ouverte de l'Université Blaise Pascal, en février 2016, "*La cryptographie de l'Antiquité à nos jours*".
26. Exposé invité au CEA List, en juin 2016 à Saclay, "*Security Analysis of Electronic Exams*".
27. Exposé invité sur la sécurité de l'Internet des objets, à la maison innovergne, en mars 2016 à Clermont-Ferrand, "*(In)Security of IoT*".
28. Journée de formation à l'IRUP de St-Étienne, en mai 2016, "*Cerveau, apprentissage et motivation*".
29. Exposé aux rencontre France Canada de l'UdA en novembre 2015, "*Security and Formal Proofs*".
30. Exposé invité à Innorobo, janvier 2015 à Lyon, "*Which security for the Factories of the Future*".
31. Exposé invité à la conférence Franco-Japonnaise sur la sécurité, Tokyo, avril 2015, "*Secure Key Renewal and Revocation for Wireless Sensor Networks*".
32. Exposé invité à l'OZSSI, à Clermont-Ferrand, octobre 2015, "*Architectures PKI et communications sécurisées*".
33. Exposé invité au LCIS à Valence en janvier 2015, "*Security and Formal Proofs*".
34. Exposé aux jeudis de la pédagogie, à Clermont-Ferrand, en mai 2015, "*Retours d'expériences pédagogiques au regard des sciences cognitives*".
35. Exposé invité à la journée sur la « Mobilité innovante » du Labex IMOBS3, Clermont Ferrand, janvier 2015, "*Securing data in connected autonomous vehiculars*".
36. Exposé invité à Apsilon, en mai 2014, "*La sécurité numérique et vous ?*"
37. Exposé invité à la conférence CSS'2014, Pologne Lublin, septembre, 2014, "*Secure Multihop Key Establishment Protocols for Wireless Sensor Networks*".
38. Exposé invité à la conférence JNCT'2014, Toulouse, juin, 2014, "*Comment les méthodes formelles peuvent-elles nous aider à sécuriser les RCSF ?*"

39. Exposé d'ouverture de la chaire Confiance Numérique, octobre 2013 [26], "*Comment avoir confiance dans les applications numériques ? Les méthodes formelles à la rescousse*".
40. Exposé invité au LIP6, en juin 2013, "*Formal approaches for analyzing properties of wireless protocols*".
41. Séminaire du LIMOS mai 2013, "*Formal analysis of security properties for e-voting and e-auction protocols*".
42. Séminaire méthodes formelles et sécurité de Rennes mars 2013, "*Automatic security proof of cryptographic primitives : public encryption, symmetric encryption modes, MAC*".
43. Exposé au Citi, avril 2013 à Lyon, "*Formal analysis of security properties for e-voting and e-auction protocols*".
44. Exposé au Groupe de Travail Modélisation et Vérification du LaBRI, avril 2013 Bordeaux, "*Automatic security proof of cryptographic primitives : public encryption, symmetric encryption modes, MAC*".
45. Exposé invité au 3rd Canada-France MITACS Workshop on Foundations & Practice of Security, Toronto, juin 2010, "*Automatic Proofs for Symmetric Encryption Modes*".
46. Exposé au iCIS, séminaire de l'Université de Calgary, février 2009, Calgary, Canada, "*Comparing State Spaces in Automatic Security Protocol Verification*".
47. Exposé invité à la conférence Cryptography and Security Systems CSS'12, Kazimierz Dolny, Pologne septembre 2012, "*Automatic Proofs for Cryptographic Primitives : Public Encryption, Encryption Modes, MACs*".
48. Exposé invité au Third Franco-Japanese Computer Security Workshop decembre 2008, Nancy, "*Comparing State Spaces in Automatic Security Protocol Verification*".
49. Exposé invité au Seventh International Conference on Computer Science - Research and Applications IBIZA'07, Kazimierz Dolny, Pologne, "*Attack and Revison of an Electronic Auction Protocol using OFMC*".
50. Séminaire NQRT à Rennes en juin 2006, "*Vérification formelle de protocoles cryptographiques en présence d'une théorie équationnelle : l'homomorphisme et le "ou exclusif"* ".

C.2 Liste de mes co-auteurs

En gras mes 27 co-auteurs qui étaient affiliés au LIMOS lors de la publication d'au moins un article ensemble.

1. **Thérèse Aby**
2. Mamunur Akand
3. Mohamed Alnuaimi
4. Karine Altisen
5. Sihem Amer-Yahia.
6. Alexandre Anzala-Yamajako
7. Ghada Arfaoui
8. **Kévin Atighehchi**
9. Gildas Avoine
10. David Basin
11. Olivier Blazy
12. Béatrice Bérard
13. Victor Bellot
14. Narjes Ben Rajeb
15. Mouheb Berrima
16. Olivier Bernard
17. Ioana Boureanu
18. Quentin Bramas
19. **Agnés Brelurut**
20. **Xavier Bultel**

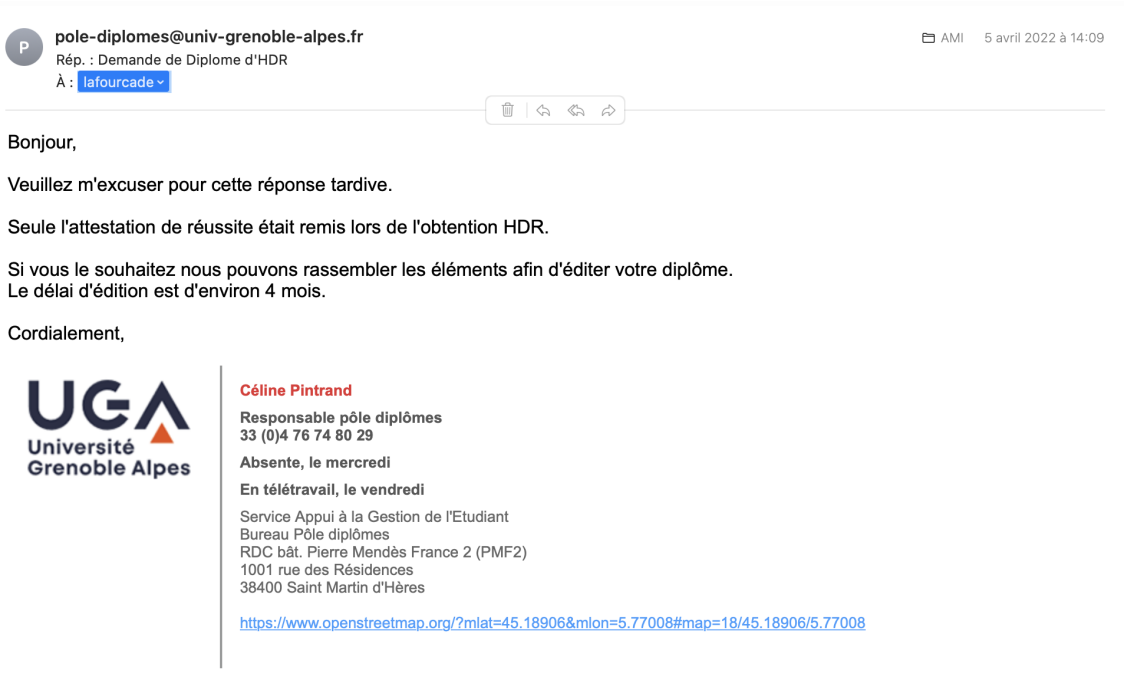
26. http://confiance-numerique.clermont-universite.fr/

21. Srdjan Capkun
22. Fabienne Carrier
23. Maxime Cautrès
24. Marwa Chaieb
25. **Gérard Chalhoub**
26. **Radu Ciucanu**
27. Véronique Cortier
28. Judicaël Courant
29. Cas J. F. Cremers
30. **Loïc Crombez**
31. Marion Daubignard
32. **Anatole Delabrouille**
33. Stéphanie Delaune
34. **François Delobel**
35. Stéphane Devismes
36. Dariusz Dobrowolski
37. Jannik Dreier
38. Béatrice Drot-Delange
39. Jean-Guillaume Dumas
40. **Anaïs Durand**
41. **Axel Durbet**
42. Isao Echizen
43. Rose Esmander
44. Ylés Falcone
45. **Jean-Marie Favreau**
46. Séverine Fleury
47. **Guilherme D. da Fonseca**
48. Florian Fontan
49. Pierre-Alain Fouque
50. Sébastien Gambs
51. Martin Gagné
52. Hardik Gajera
53. Joaquín García
54. Antoine Gerbaud
55. **Yan Gérard**
56. David Gérault
57. Nacira Ghoualmi
58. **Matthieu Giraud**
59. Rosario Giustolisi
60. Aldo Gonzalez-Lorenzo
61. Milan Gonzalez-Thauvin
62. Anna Grabowska
63. **Paul-Marie Grollemund**
64. **Alexandre Guitton**
65. Lei Hu
66. Jean-Pierre Hubaux
67. Marie Izaute
68. Raphael Jamet
69. Thibaut Jacques
70. Hugo Jonker
71. Matthieu Journault
72. Timothée Kheyrkhah
73. Bogdan Ksiezopolski
74. Mirko Koscina
75. Amrit Kumar
76. Ali Kassem
77. Manik Lal Das
78. Russell WF Lai
79. Yassine Lakhnech
80. Dounia Lakhzoum
81. Anissa Lamani
82. Cédric Lauradoux
83. Isabelle Le Brun
84. **Kerghan Le Cornec**
85. Gabriele Lenzini
86. Michel Lévy
87. **Luc Libralesso**
88. Marius Lombard-Platet
89. Julio Ernesto Lopez Fenner
90. David Lucas
91. Denis Lugiez
92. Giulio Malavolta
93. Sreekanth Malladi
94. Ismail Mansour
95. **Gael Marcadet**
96. Vincent Marlin
97. **Vincent Mazenod**
98. Francis Melemedjian
99. Laure Millet
100. Marine Minier
101. **Michel Misson**
102. Daiki Miyahara
103. Takaaki Mizuki
104. Sebastan Mödersheim
105. Mariane Mognos
106. Benjamin Momège
107. **Malika More**
108. Ladislav Motak
109. Bastien Mosnier
110. Laurent Mounier
111. Günter Müller
112. Philippe Nadeau
113. Atsuki Nagao
114. Adina Nedelcu
115. Claudia Negri Ribalta
116. Mike Nopere
117. **Charles Olivier-Anclin**
118. Cristina Onete
119. Jean-Baptiste Orfila
120. Panagiotis Papadimitratos
121. Octavio Perez Kempner
122. Clément Pernet
123. Jérémy Picot
124. **Daniela Pizzuti**
125. Maria Potop-Butucaru
126. Rémy Poulain
127. Marcin Poturalski
128. Marie-Laure Potet
129. **Maxime Puys**
130. Kexin Qiao
131. Arthur Rauch

132. Patrick Redon
133. Samuel Rivière-Wekstein
134. Riadh Robbana
135. Jean-Louis Roch
136. Jean-Marc Robert
137. **Léo Robert**
138. Étienne Roudeix
139. Damian Rusinek
140. Peter Ryan
141. Reihaneh Safavi-Naini
142. Camille Salinesi
143. Tatsuya Sasaki
144. Patrick Schaller
145. Dominique Schröder
146. Kazumasa Shinagawa
147. Marta Soare
148. Christine Solnon
149. Noboru Sonehara
150. Hideaki Sone
151. Demba Sow
152. Siwei Sun
153. So Takeshige
154. Vanessa Terrade
155. Jérémie Tharaud
156. Yann Thierry-Mieg
157. Pascal Thoniel
158. Sri Aravinda Krishnan Thyagarajan
159. Ariane Tichit
160. Sébasien Tixeuil
161. Yosuke Todo
162. Ralf Treinen
163. Sébastien Varrette
164. Sylvain Vigier
165. Sven Wohlgemuth
166. Qianqian Yang
167. Lihua Ye
168. Souheib Yousfi

D Attestation de réussite à l'Habilitationà Diriger des Recherche

J'ai obenu mon HDR [Laf12] en 2012, ceci pendant la fusion des Universités grenobloises. Depuis l'École dcoctorale n'a jamais pu éditer le diplôme. J'en ai fait la demande le 5 avril 2022, car la procédure semble maintenant possible.



pole-diplomes@univ-grenoble-alpes.fr
AMI 5 avril 2022 à 14:09
Rép. : Demande de Diplome d'HDR
À : lafourcade

Bonjour,

Veuillez m'excuser pour cette réponse tardive.

Seule l'attestation de réussite était remis lors de l'obtention HDR.

Si vous le souhaitez nous pouvons rassembler les éléments afin d'éditer votre diplôme.
Le délai d'édition est d'environ 4 mois.

Cordialement,

UGA Université Grenoble Alpes

Céline Pintrand
Responsable pôle diplômes
33 (0)4 76 74 80 29
Absente, le mercredi
En télétravail, le vendredi
Service Appui à la Gestion de l'Etudiant
Bureau Pôle diplômes
RDC bât. Pierre Mendès France 2 (PMF2)
1001 rue des Résidences
38400 Saint Martin d'Hères
https://www.openstreetmap.org/?mlat=45.18906&mlon=5.77008#map=18/45.18906/5.77008

Ci-joint l'attestation de réussite à l'HDR.

UNIVERSITE DE GRENOBLE

ATTESTATION DE REUSSITE AU DIPLOME

L'administrateur provisoire atteste que

l' HABILITATION A DIRIGER DES RECHERCHES Spécialité INFORMATIQUE ET MATHEMATIQUES APPLIQUEES

a été décernée à

Monsieur LAFOURCADE PASCAL

né le 26 avril 1977 à TOULOUSE (031)

au titre de l'année universitaire 2012/2013

Date de soutenance	: 6 novembre 2012
Etablissement soutenance	: UNIVERSITE DE GRENOBLE
Jury	: M. DAVID POINTCHEVAL, Président du jury M. GILLES BARTHE, Rapporteur du jury M. HUBERT COMON-LUNDH, Rapporteur du jury M. RALF KÜSTERS, Rapporteur du jury M. DAVID BASIN, Membre du jury M. YASSINE LAKHNECH, Membre du jury M. PETER RYAN, Membre du jury

Fait à Grenoble, le 13 novembre 2012

Farid OUABDESSELAM

UNIVERSITÉ DE GRENOBLE Collège doctoral

N° étudiant : 21260219

Avis important: Il ne peut être délivré qu'un seul exemplaire de cette attestation. Aucun duplicata ne sera fourni.