Pierre-Louis CAYREL

18 rue du Prof. Benoît Lauras
42000 Saint-Etienne
Tél : 04.77.91.57.87

pierre.louis.cayrel@univ-st-etienne.fr

www.cayrel.net

Né le 07 Août 1981, à Limoges
Marié
Nationalité Française

Position actuelle depuis 2011	Positions antérieures
Maître de conférences à l'UJM à Saint-Étienne	2009-2011 Post-doc à CASED à Darmstadt
Enseignement au département GEII à l'IUT	2008-2009 ATER, Université Paris 8
Laboratoire Hubert Curien (UMR CNRS 5516)	Bourse de thèse, Université de Limoges

Diplômes

• **Doctorat de mathématiques et applications**, intitulée *"Construction et optimisation des cryptosystèmes"*, soutenue le 2 octobre 2008 (mention très honorable)

• **Master II Recherche**, *"Mathématiques Cryptographie Codage Calcul"*, Université de Limoges. mention Bien (rang : 2ème), juin 2005.

Activités de recherche

h-index : 12 et i10-index : 15 avec 446 citations (en juillet 2014)

Thèmes de recherche

Cryptographie asymétrique : basée sur les codes correcteurs d'erreurs et sur les réseaux
Attaques par canaux cachés de protocoles de chiffrement
Conception d'algorithmes d'identification et de signature à propriétés spéciales
Implantations efficaces d'algorithmes post-quantiques

Synthèse de la production scientifique

2 chapitres de livre ; 4 revues internationales ; 37 conférences internationales ; 8 conférences nationales.

Encadrement d'étudiants

• 1 thèse en cours : T. Richmond (Implantation sécurisée de McEliece, Université Jean Monnet)
• 3 thèses soutenues : R. Niebuhr (06/2012), M. Meziani (06/2013), M. ElYousfi (06/2013).
• 3 stages de Master ; 11 stages de Licence/Bachelor.

Membre de comités de programme

Conférences internationales : MoCrySEn 2013, Journées codes et stéganographie 2011 Conférences nationales : MAJECSTIC 2007

Exposés invités

Conférences internationales : TATACRYPT 2012, CryptArchi 2012, PQSM Workshop 2010
Audiences nationales : Journées GDR SoC SiP 2011, une quarantaine de séminaires nationaux.

Activités d'enseignement

Depuis mon recrutement à l'IUT de Saint-Etienne, j'effectue mes heures d'enseignements au département GEII, à l'ISTP ainsi qu'à Télécom Saint-Étienne.

Nature	Niveau	Effectif	Nb heures	Contenu
TP	L1	60	54	Outils logiciels
Cours/TD	L3	60	52	Mathématiques générales
Cours/TD	L2	60	48	Suites, séries de Fourier
Cours/TD/TP	L1	50	63	Informatique industrielle
Cours/TD	M1	20	42	Cryptographie et théorie des codes

Depuis 2011, je suis responsable du cours de cryptographie et de codes correcteurs d'erreurs.

Responsabilités collectives

Jury de thèse

• Rapporteur de la thèse de Mohammed Meziani (Université de Darmstadt - CASED, Juin 2013)
• Rapporteur de la thèse de Mohamed ElYousfi (Université de Darmstadt - CASED, Juin 2013)
• Rapporteur de la thèse de Robert Niebuhr (Université de Darmstadt - CASED, Juin 2012)

Responsable des séminaires : PI2C (2006-2008) et CASED (2009-2011)

Participation à des projets

2014-2017, Projet OTAN SfP
2005-2008, ANR XCODES