Marine MINIER

Section 27 Informatique

Equipe INRIA Privatics - Laboratoire CITI
Département Informatique - INSA de Lyon

Table des matières

1 Résumé de mes Activités **1**
État Civil . . . 1
Parcours . . . 1
Diplômes . . . 1
Synthèse des Activités de Recherche . . . 2
Synthèse des Activités d'Enseignement . . . 6
Responsabilités Collectives . . . 7

2 Détails des Activités d'Enseignement **9**
Création de Nouveaux Enseignements . . . 9
Révision d'Enseignements . . . 10
Responsabilités d'Enseignements . . . 10
Activités d'Enseignement avant mon Arrivée à l'INSA de Lyon . . . 11

3 Détails des Activités de Recherche **12**
Résumé des Activités Scientifiques Doctorales . . . 12
Résumé des Activités Scientifiques depuis 2004 . . . 12

4 Liste Complète de mes Publications **15**

5 Liste de mes Co-auteurs par Ordre Alphabétique **21**

1 Résumé de mes Activités

État Civil

Marine Minier
23, rue D'Aguesseau
69007 LYON
Tél : 06 87 10 68 58

marine.minier@insa-lyon.fr
perso.citi.insa-lyon.fr/mminier/

Née le 28 Janvier 1976, à Limoges
Mariée, 1 enfant (14/10/2011)
Nationalité Française

Parcours

Position actuelle depuis 2005	Positions antérieures
Maître de conférences à l'INSA de Lyon Enseignement au département Informatique Laboratoire CITI (EA3720), équipe INRIA Privatics Responsable de l'axe transversal Sécurité au laboratoire CITI (2005-2012)	2009-10, Délégation INRIA, EPI SWING, laboratoire CITI 2004-05, Ingénieur Expert, INRIA Rocquencourt, Projet CODES 2003-04, ATER mi-temps, Université Paris 8, UMR LAGA 2002-03, Bourse post-doctorale INRIA, DTU (Danemark), Département de Mathématiques 1999-02, Allocatrice CIFRE, France Télécom R&D, Issy-Les-Moulineaux

Qualification PR 27, obtenue en 2013, numéro : 13127135146.
Prime d'Excellence Scientifique obtenue pour la première fois en 2011.

Diplômes

- **Habilitation à diriger des recherches** de l'Université Lyon 1 et INSA de Lyon, intitulée "*Quelques résultats en cryptographie symétrique, pour les modèles de confiance dans les réseaux ambiants et la sécurité dans les réseaux de capteurs sans fil*", soutenue le *31 Mai 2012*, devant le jury : Pr. I. Guérin-Lassous (Présidente), Pr. W.Meier (Rapporteur), Pr. R. Molva (Rapporteur), Pr. F.-X. Standaert (Rapporteur), Pr. T. Berger (Examinateur), DR A. Canteaut (Examinateur), HDR H. Gilbert (Examinateur), Pr. T. Risset (Directeur).

- **Doctorat de mathématiques** de l'Université de Limoges, intitulé "*Preuves d'Analyse et de Sécurité en Cryptologie à clé secrète*", obtenue le *30 septembre 2002* devant le jury : Pr. J.-P. Borel (Président), DR P. Charpin (Rapporteure), Pr. J. Patarin (Rapporteur), Pr. T. Berger (co-directeur), Dr. H. Gilbert (co-directeur), Dr. F. Arnault (Examinateur), Dr. A. Canteaut (Examinateur), Pr. B. Preneel (Examinateur).

- **DEA**, Cryptographie, Codage et Calcul Mathématique, Université de Limoges, *Juin 1999*. Sujet de Stage : cryptanalyse de l'algoritme CRYPTON encadré par Henri Gilbert.

Synthèse des Activités de Recherche

Thèmes de Recherche

Mes thématiques de recherche s'articulent autour de trois grands domaines : tout d'abord **la cryptographie symétrique et l'étude des algorithmes de ce domaine** (algorithmes de chiffrement à flot, algorithmes de chiffrement par blocs, fonctions de hachage et codes d'authentification de messages) ; et également **la sécurité dans les réseaux de capteurs sans fil** où nous cherchons des mécanismes algorithmiques ou cryptographiques efficaces permettant de lutter contre des attaques particulières (attaque *wormhole*, attaque par *selective forwarding*, attaques par pollution, etc.) ; Finalement, depuis 2012 et mon intégration dans l'équipe centre INRIA Privatics, je m'intéresse également à la **protection des données personnelles**.

Synthèse de la Production Scientifique

Types	Nombre
Chapitres de livre	3
Revues Internationales	12
Brevets internationaux	1
Conférences internationales avec comité de lecture et actes	40
Workshops internationaux avec comité de lecture et actes	11
Rapports techniques et de recherche	7
Conférences francophones avec comité de lecture et actes	5

Membre de Comités de Programme

- Membre des comités de programme de conférences internationales : **WCC 2015**, **FSE 2011**, **Indocrypt 2009**, **ISPA 2007**, **WCC 2007**. Et aussi : **C2SI 2015**, **CIS 2014**, **CIS 2013**, **CIS 2012**, **CIS 2011**, **TOOLS 2010**, **MEDES 2010**, **CIS 2010**, **CIS 2009**, **IEEE ICDIM 2009**, **ICDIM 2008**, **MWNSW 2008**.
- Membre des comités de programme de conférences nationales : **Journées GDR C2 2011**, **Journées GDR C2 2005**.
- relectrice pour les journaux Journal of Cryptology ; IEEE-IT ; IEEE-TC ; Design, Codes and Cryptography ; Information Processing Letters ; Computer Communications ; Performance Evaluation ; Discrete Mathematics & Theoretical Computer Science ; Telecommunication Systems.

Collaborations internationales et Visites

- Séjour invité en Aout 2015 (15 jours) à Aalto University (Finlande), collaboration avec Céline Blondeau (post-doctorante).
- Crypto Group, Université de Louvain-La-Neuve, pour l'encadrement de la thèse de Baudoin Collard (2 séjours de 15 jours en 2009 et 2010).
- Information Security Group, Université de Louvain-La-Neuve (2008-2010), collaboration avec Cédric Lauradoux (post-doctorant).
- Loughborough University (Angleterre) et Multimedia University (Cyberjaya, Malaysia), collaboration avec Raphaël Phan (Professor).
- Coding and Cryptography Research Group, Nanyang University, Singapore, collaboration avec Thomas Peyrin (Assistant Professor).
- Visite à l'Université de Shangai Jiao-Tong en Mai 2010 (Chine).

Encadrement de Thèses

2014-2017 Je co-encadre la thèse de **Célestin MATTE** comme HDR à 50 % avec M. Cunche.
Sujet : Système d'observation des flux humains via Wi-Fi respectueux de la vie privée. Bourse Région Rhône-Alpes. INSA de Lyon.

2011-2015 Je co-encadre à 50 % la thèse de **Gaël THOMAS** avec Thierry Berger (Université de Limoges).
Sujet : Design et preuves de sécurité des algorithmes de chiffrement par blocs. Financement ANR BLOC.

2009-2013 J'ai co-encadré à 70 % la thèse de **Ochirkhand ERDENE-OCHIR** avec Fabrice Valois (INSA de Lyon).
Sujet : Protocoles de communication sécurisés résilients aux attaques pour les réseaux de capteurs. Thèse soutenue le 5 Juillet 2013 à l'INSA de Lyon.
Bourse CIFRE entre le Laboratoire CITI et Orange Labs Grenoble (représenté par Mr Apostolos Kountouris). Actuellement en post-doctorat au Qatar.

2007-2010 J'ai co-encadré à 90 % la thèse de **Wassim ZNAIDI** avec Stéphane Ubéda (INSA de Lyon).
Sujet : Quelques propositions de solutions pour la sécurité des réseaux de capteurs sans fil. Thèse soutenue le 15 octobre 2010 à l'INSA de Lyon.
Jury : Claude Castelluccia (rapporteur), Refik Molva (rapporteur), Riadh Robbana, Maryline Laurent, Jean-Philippe Babau, Marine Minier (directrice), Stéphane Ubéda (directeur). Actuellement en post-doctorat au Qatar.

2007-2010 J'ai co-encadré à 50 % la thèse de **Benjamin POUSSE** avec Thierry Berger (Université de Limoges).
Sujet : étude des chiffrements à flot à rétroaction non-linéaire. Thèse soutenue le 2 décembre 2010 à l'Université de Limoges.
Jury : François Arnault, Thierry Berger (directeur), Anne Canteaut (rapporteur), Henri Gilbert (rapporteur), Louis Goubin, Marine Minier (directrice). Actuellement développeur dans une société informatique à Toulouse.

2004-2007 J'ai co-encadré à 70 % la thèse de **Samuel GALICE** avec Stéphane Ubéda (INSA de Lyon).
Sujet : Modèle dynamique de sécurité pour réseaux spontanés. Financement de la thèse ACI KAA. Thèse soutenue le 29 octobre 2007 à l'INSA de Lyon.
Jury : Khaldoun Al Agha (rapporteur), Valérie Issarny (rapporteur), Isabelle Chrisment, Daniel Le Métayer, Stéphane Ubéda (directeur), Marine Minier (directrice). Actuellement aux Etats-Unis.

Encadrements de Post-doctorat (1), MASTER2 Recherche (11), Stages doctoraux (3), Projets de fin d'étude ingénieur (7)

- **Encadrement de post-doctorant :** Yuan Yuan ZHANG, Université de Shangai Jiao-Tong, (01/11/2010-01/04/2012). Thème de recherche : sécurité du codage réseau. Financement : sur fond propre via la FFCSA (Fondation Franco-Chinoise pour la Science et ses Applications).

- **Encadrement de stages doctoraux :** Adil BENSLETEN (Université de Rabat), 3 mois en 2006 et 6 mois en 2007 et Yves-Jonathan NDJE (3 mois en 2012).

- **Encadrement de stages de MASTER2 (11) :**
  - Khaoula DHIFALLAH (02/2015-07/2015). **Sujet :** Resilient RPL.
  - David GERAULT (02/2015-07/2015). **Sujet :** Utilisation de la programmation par contraintes pour la résolution de problème en cryptographie symétrique.
  - Pierre BRUNISHOLZ (02/2014-09/2014). **Sujet :** Apport du codage réseau dans le routage pour réseaux de capteurs sans fil multi-saut. Poursuite en thèse à Grenoble.
  - Emmanuel PERRIER (03/2014-07/2014). **Sujet :** Le K-anonymat en pratique : le cas des systèmes de traçage Wi-Fi. Poursuite en thèse à Grenoble.
  - Chloé CAHUET (02/2013-07/2013). **Sujet :** Application des attaques à clés liées de A. Biryukov et I. Nikolic à l'algorithme de chiffrement par blocs Rijndael. Emploi dans le privé.
  - Medhi DIOURI (02/2010-06/2010). **Sujet :** Proposition d'un mécanisme de lutte contre les attaques Sybille dans les réseaux de capteurs sans fil. Poursuite en thèse à l'ENS Lyon.
  - Cherifa BOUCETTA (02/2010-06/2010). **Sujet :** La sécurité des systèmes de coordonnées dans les réseaux de capteurs sans fil. Poursuite en thèse en Tunisie.
  - Ochirkhand ERDENE-OCHIR (02/2009-09/2009). **Sujet :** Résilience des protocoles de routage dans les réseaux de capteurs sans fil. Poursuite en thèse au laboratoire CITI. Poursuite en thèse au laboratoire CITI. Publication lié au stage : [36, 37].
  - Paul FERRAND (02/2009-06/2009). **Sujet :** propriétés linéaires de l'AES et distingueurs à clés connus : applications aux fonctions de hachage. Poursuite en thèse au laboratoire CITI.
  - Bilel ROMDHANI (02/2008-06/2008). **Sujet :** Sécurisation d'un protocole de communication pour réseau de capteurs sans fil. Poursuite en thèse au laboratoire CITI.
  - Martin BOULANGER (02/2007-06/2007). **Sujet :** Sécurisation d'un protocole de communication pour réseaux hybrides. Emploi dans le privé.

- **Encadrement de stages de fin d'étude ingénieur en relation avec la recherche (7) :** Javier LALLANA (02/2015-09/2015), Pierre BRUNISHOLZ(02/2014-09/2014), Medhi DIOURI (06/2010-09/2010), Paul FERRAND (02/2009-06/2009), Dimitar DELOV (02/2009-06/2009), Tian-Qi ZHANG 02/2009-06/2009), Martin BOULANGER (06/2007-09/2007).

- **Stage 4ème année (1) :** Julia REBOUL (06/2014-09/2014).
- **Stage de 3ème année (3) :** Sylvain GOURGEON (06/2013-09/2013), Mickaël CAZORLA (06/2012-09/2012, publication : [24]), Bertrand MANDRIN (06/2008-08/2008).

Colloques et séminaires invités (hors présentations à des conférences)

- **Présentations invitées :**
  - Journées RAIM 2012 (Juin 2012, Dijon). *"l'AES, 10 ans après".*
  - Séminaire CCA 2011 (Janvier 2011, Paris). *"Quelques propriétés intégrales de Rijndael, LANE et Groestl".*
  - Workshop MITACS 2009 (Juin 2009, Grenoble). *"Some integral properties of Rijndael".*
  - Tutoriel invité des Journées Codage et Cryptographie (Février 2005, Aussois). *"LILI-128 et ses attaques".*
  - Conférence YACC (Yacc is "Another" Conference on Cryptography) (Juin 2002, Porquerolles). *"Cryptanalysis of Round-Reduced Versions of Rijndael".*

- **Séminaires invités :**
  - Universités Françaises : Université de Rennes et Université de Bordeaux (Mai 2013), ENS Lyon (Juin 2011), Université de Grenoble (Décembre 2010 et Janvier 2011), Université de Montpellier (Juillet 2010, Juillet 2007), Journées CLUSTER Région Rhône-Alpes (Septembre 2007), Université de Limoges (Avril 2007), Insa de Lyon (Juillet 2005), Université Paris 8 (Avril 2004), Université de Rouen (Mai 2004), Université de Caen (Mai 2004).
  - Universités Etrangères : Aalto Université, Finlande (Août 2014), Shanghai Jiao Tong Université, Chine (Avril 2009), Université de Louvain-La-Neuve, Belgique (Avril 2009, Février 2005)

Synthèse des Activités d'Enseignements

Depuis mon recrutement à l'INSA de Lyon, j'effectue mes heures d'enseignements au département IF (informatique, 120 étudiants pour chacune des trois années du département) et dans le MASTER MASTRIA, MASTER commun à l'INSA de Lyon et à l'Université Lyon 1. Sur une année, la synthèse de mes activités d'enseignements peut être découpée comme suit :

Nature	**Effectif**	**Niveau**	**H EQTD**	**Intitulé**	Ressources
CM	120	L3	12h	Théorie de l'Information, Cryptographie	Cours/TD/TP
TD	120	L3	10h TD	Théorie de l'Information, Cryptographie	TD
TD	120	L3	30h TD	Probabilités	TD
TP	120	L3	40h TD	Probabilités	TP
TP	120	L3	40h	Architecture Matérielle	TP
TP	120	L3/M1	40h	Réseaux	TP
TP	60	L3	20h	Analyse Numérique	TP
TP	60	L3	20h	Traitement du Signal	TP
Cours	15	M2	24h	Sécurité des réseaux sans fil	Cours

Détails des Activités d'Enseignements

- Depuis 2005, je suis **responsables des cours** de théorie de l'information, de cryptographie (L3, 1 enseignant) et de probabilités (L3, 5 enseignants, 2005-2009 et 2013).
- Je fais partie des **équipes pédagogiques** : mathématiques et outils de modélisation, architecture des ordinateurs et réseaux.
- Je participe à tous les **jurys du département**.
- J'ai rédigé et corrigé les sujets de **devoirs surveillés** pour les matières suivantes : probabilités, arithmétique pour la cryptographie et théorie de l'information.
- **Encadrement de stages** : j'encadre chaque année environ 4 stages L3, 4 stages M1 et 2 projets de fin d'étude ingénieur.

Mise en Place de Nouveaux Enseignements

- **Cours Magistraux (L3, 20h de Cours)** : introduction à la théorie de l'information (64 transparents), arithmétique pour la cryptographie (64 transparents), probabilités (58 transparents) ;
- **TP de probabilités (40h TP, L3)** : Avec Irène Gannaz, nous avons monté un TP de probabilités qui concerne les tests statistiques sur la qualité des séquences produites par différents générateurs pseudo-aléatoire et les files d'attente.
- **TP d'architecture matérielle (60h TP et 20h TD, L3)** : Avec Christian Wolf et Guillaume Beslon, nous avons monté un TP micromachine permettant aux étudiants de concevoir l'ALU et l'UC d'une micromachine [1] ; Les TPs pour cette lanière ont été changés cette année.
- **TP d'administration réseaux (60h TP, M1, 2005-2010)** : Avec Yves Boutemy, nous avons mis en place un TP d'administration système sous Windows Server ;
- **Cours de cryptographie et sécurité (24h, Cours, M2)** : j'enseigne la cryptographie pour les réseaux sans fil pour le MASTER MASTRIA et l'option transversale "Sécurité" de 5ème année (250 transparents).
- **Cours de sécurité des réseaux (26h, Cours/TD/TP, L3)** : cette année, en tant que vacataire à l'IUT d'informatique de l'université Lyon 1, j'enseigne sous forme de Cours/TP/Projets la sécurité des réseaux (200 transparents).

1. `http://intranet-if.insa-lyon.fr/micromachine/`

Responsabilités d'Enseignements

- *2012-... :* **Responsable du MASTER MASTRIA**, spécialité "Systèmes Informatiques et Réseaux", co-habilité par l'Université Lyon 1 et l'INSA de Lyon.
- *2005-2007 :* Responsable de la **gestion des stages de 3ème et 4ème année** au département IF.
- *2008-2009 :* Organisation de la **visite du Data Center de IBM-Montpellier** pour un groupe d'étudiants de 5ème année.

Diffusion des Savoirs

- Rédaction d'un article avec Anne Canteaut "De l'espérance de vie d'un algorithme symétrique (ou l'AES dix ans après)" pour le **Hors Série Numéro 5 du magazine MISC**.
- Participation au **site web de vulgarisation scientifique** picsi : `http://www.picsi.org`. Rédaction de toute la partie concernant les chiffrements par blocs.

Responsabilités Collectives

Responsabilités Administratives

2012-	**Membre nommée suppléante au CHSCT** de l'INSA de Lyon
2012-	Participation à la rédaction du projet de création de l'équipe INRIA Privatics. **Membre élue du conseil du laboratoire CITI.**
2008-2010	Responsable de l'animation scientifique du laboratoire CITI (organisation des séminaires internes et externes).
2009-2011	Participation à la rédaction du projet de création de l'équipe INRIA SWING. Responsable de l'axe transversal Sécurité.
2005-2012	Responsable de l'axe transversal Sécurité au laboratoire CITI.

Comités de Sélection

2015-	Membre du **Comité des Emplois Scientifiques** de l'INRIA Rhône-Alpes.
2011	Membre des comités de sélection du poste 63MC141 (Saint-Etienne) et du poste 27MC1064 (Nice).
2010	Membre du comité de sélection du poste 63MC0511 (Saint-Etienne).
2009	Membre des comités de sélection du poste 63MC0497 (Saint-Etienne) et du poste 27MC0226 (Limoges). Membre du comité de sélection des postes de CR1 et CR2 de l'UR INRIA Rhône-Alpes.

Membre de Jurys de Thèse

- **Rapporteure** de la thèse de Raphaël Jamet, Université de Grenoble, Octobre 2014.
- **Rapporteure** de la thèse de Abdourhamane Idrissa, Université Jean Monnet - Saint-Etienne, Septembre 2012.
- **Rapporteure** de la thèse de Kaoutar Elkhiyaoui, Eurecomm - Télécom ParisTech, Septembre 2012.
- **Membre du jury** de la thèse de Baudoin Collard, soutenue le 24 janvier 2011 à l'Université de Louvain-La-Neuve, Belgique.

Participation à des Projets

2011-2015 **BLOC** (ANR INS 2011, montant global : 643 K€) : Cette ANR-SETIN a pour objet le design et les attaques des chiffrements par blocs dédiés aux environnements contraints. Je suis **coordinatrice** de ce projet. (`http://bloc.project.citi-lab.fr/`). Partenaires : CITI Lab, XLIM, EPI INRIA Rocquencourt SECRET, CryptoExperts.

2010-2013 **ARESA2** (ANR Verso, montant global : 1,5 M€) : Avancées en Réseaux de capteurs Efficaces, Sécurisés et Auto-Adaptatifs. L'INRIA via les équipes SWING et PLANETE est leader des Workpackages 3 et 4. Je suis responsable de la rédaction de deux livrables (`http://aresa2.minalogic.net/`). Partenaires : CEA-LETI, ELSTER SAS, France Telecom R&D, LIG, TELECOM BRETAGNE, VERIMAG.

2009-2012 **CRE** (Contrat de Recherche Externalisée, montant : 27 K€) avec Orange Labs pour financer l'encadrement de la thèse de Ochirkhand ERDENE-OCHIR sur les méthodes de routage résilientes dans les réseaux de capteurs sans fil. Ce CRE a permis de financer le post-doctorat de Y. ZHANG.

2007-2010 **RAPIDE** (ANR Setin 2006, montant global : 428 K€) : Cette ANR-SETIN avait pour objet la conception et l'analyse de chiffrements à flot efficaces pour les environnements contraints. Je suis responsable du Workpackage Construction de MACs. (`http://rapide-anr2006.gforge.inria.fr/`). Partenaires : CITI Lab, XLIM, EPI INRIA Rocquencourt SECRET.

2008 **Projet IXXI** (financé par l'IXXI, montant : 5000 euros) : évaluation expérimentale d'un modèle de confiance pour les communautés ouvertes.

2007-2008 **PRIAM (Privacy Issues and AMbient intelligence)** (ARC INRIA, Action de Recherche Coopérative) : le but de ce projet était de créer une interaction durable entre des juristes et des informaticiens afin de définir les défis de la privacy au sein de l'intelligence ambiante.

2007-2008 **Malisse (Malicious sensors Context)** (ARC INRIA, Action de Recherche Coopérative) : le but de ce projet était d'étudier les réseaux de capteurs et leurs applications en tenant compte de la présence de noeuds malicieux.

2004-2007 **KAA, Knowledge Authentication Ambient** (ACI "Securité Informatique" 2003) : Cette ACI multi-disciplinaire avait pour objet la construction de schémas de gestion de la confiance socialement acceptables et informatiquement réalisables. (`http://kaa.citi.insa-lyon.fr/`). A mon arrivée à Lyon en 2005, j'ai pris la responsabilité de cette ACI. Partenaires : CITI Lab, LIP, Laboratoire d'économie des transports, CREDRID, le centre de sociologie des organisations, MAPPLY.

2004-2005 **Projet RNRT X-CRYPT** : Outils cryptographiques adaptés aux réseaux de télécommunications à haut débit et aux réseaux sans fil émergents (2003-2006). J'ai été ingénieur expert financé par ce projet sur l'année universitaire 2004-2005.

2 Détails des Activités d'Enseignement

Depuis Septembre 2005, je suis maître de conférences au département Informatique de l'INSA de Lyon. Dans cette partie, je détaille l'ensemble des enseignements que j'ai effectués et dont je suis responsable depuis mon arrivée à l'INSA de Lyon, notamment les enseignements en sécurité puis mes responsabilités en termes d'enseignement et finalement mes activités d'enseignement avant l'obtention de mon poste à l'INSA de Lyon.

Création de Nouveaux Enseignements

- À mon arrivée à Lyon, j'ai eu la chance de pouvoir créer un cours de M2 dans le cadre du MASTER RTS sur la sécurité dans les réseaux sans fil [2]. Ce cours présente les primitives de base en cryptographie tant symétrique qu'asymétrique et ensuite comment ces primitives sont agencées pour créer des protocoles dédiés aux réseaux sans fils. Nous étudions comme cas d'application, la sécurité du WiFi, la sécurité du GSM et de la 3G. Finalement, la deuxième partie de ce cours porte sur des aspects plus orientés recherche et s'intéresse aux propositions de sécurité dans les réseaux ad hoc et les réseaux de capteurs sans fil.
  Ce cours de 8 séances de 2h fait partie du tronc commun du MASTER2 recherche RTS et est dispensé chaque année pour une quinzaine d'étudiants. Une partie de cet enseignement est également repris dans le séminaire pour les étudiants ingénieurs de 5ème année du département informatique de 2005 à 2009 et à présent pour les étudiants ingénieurs de 5ème année suivant l'option transversale "Sécurité". Une partie de cet enseignement sert également de base au cours que je donne à la licence pro RESIR de l'IUT d'Informatique de l'Université Lyon 1.
- Avec Stéphane Coulondre (MCF, INSA de Lyon), nous avons également mis en place en 2007 un TP de sécurité pratique à partir du projet SERBER, projet de 2 ans financé par la région Rhône-Alpes dédié à la mise en place de jeux de rôle de sécurité. Le but de ce TP qui fait à présent partie intégrante de l'option transversale "Sécurité" de 5ème année est l'apprentissage des techniques de base du *hacking*. Ainsi, chaque étudiant joue le rôle du pirate informatique qui doit récupérer sur une machine distante un document confidentiel en utilisant un exploit particulier. Ce TP a été remplacé l'an dernier.
- Avec Christian Wolf (MCF, INSA de Lyon) et Guillaume Beslon (Professeur, INSA de Lyon), nous avons mis en place un TP d'architecture matérielle pour les étudiants de 3ème année du département informatique. Ce TP nommé micromachine [3] a pour but la compréhension d'une architecture matérielle dédiée où les étudiants construisent deux éléments de base de l'architecture à savoir l'ALU et l'UC. Pour chaque étudiant, cet enseignement correspond à 12h de TP et 4h de TD en face à face pédagogique. Ce TP est évalué par un QCM. Depuis cette année, ce TP a été remplacé par une série de TPs mise en place par toute l'équipe pédagogique. La première partie de ces nouveaux TPs consiste à modéliser à l'aide du logiciel LogiSim des bascules et des registres. La deuxième partie de ces TPs concerne la programmation vhdl d'un microprocesseur, les buts pédagogiques restant clairement les mêmes.
- Avec Yves Boutemy (PAST, INSA de Lyon), entre 2005 et 2010, nous avons mis en place pour les étudiants de 4ème année du département informatique un TP d'administration serveur sous Windows Server 2003 afin de les familiariser avec les notions d'administration utilisées par Windows. Pour cela, nous avons utilisé un serveur d'ordinateurs virtuels permettant de

2. `http://perso.citi.insa-lyon.fr/mminier/images/MASTER_part1.pdf` et `http://perso.citi.insa-lyon.fr/mminier/images/MASTER_part2.pdf`, 300 transparents

3. `http://intranet-if.insa-lyon.fr/micromachine/`, polycopié de 70 pages décrivant le fonctionnement de la micromachine

construire un réseau complet et permettant aux étudiants d'administrer ce réseau. Cet enseignement correspondait à 12h de TP en face à face pédagogique.

Révision d'Enseignements

- A mon arrivée à l'INSA de Lyon, j'ai pris la responsabilité du cours d'*introduction à la cryptographie* (3 séances de cours de 2h en L3). Les objectifs pédagogiques de ce cours sont d'introduire les concepts d'arithmétique de base nécessaires pour comprendre les cryptosystèmes à clé publique RSA et El Gamal. Suite au départ en 2006 d'Olivier Mazet, j'ai pris la responsabilité du cours de probabilités (5 séances de cours de 2h et 8 séances de TD de 2h en L3) jusqu'en 2009 et l'an dernier. Ce cours présente les notions de base en probabilités : combinatoire, variables et vecteurs aléatoires, théorèmes limites et chaînes de Markov. Depuis 2011, je suis également responsable du cours de théorie de l'information (3 séances de cours de 2h en L3) où sont abordées les notions de codage de source, codage de canal, d'entropie et de codes correcteurs d'erreurs. Depuis 2011, nous avons rassemblé en un seul module les cours de théorie de l'information et d'introduction à la cryptographie afin de dégager une séance de TD de 2h et d'y associer un DS.
- Suite au départ à la retraite de Robert Badard, nous avons, avec Irène Gannaz, monté un nouveau TP de L3 correspondant à 8h de face à face pédagogique où les étudiants doivent implémenter tout d'abord des tests sur des générateurs pseudo-aléatoires puis modéliser les processus classiques de files d'attentes. Les buts pédagogiques de ce TP sont l'acquisition de connaissances en matière de qualité statistique d'une suite pseduo-aléatoire et l'acquisition de compétences en matière de modélisation de files d'attentes.
- Je participe également aux TPs d'analyse numérique (12h de face à face pédagogique, niveau L3) et traitement du signal (8h de face à face pédagogique, niveau L3). Le premier TP permet aux étudiants d'implémenter les méthodes de résolution de grands systèmes linéaires et d'appliquer ces méthodes afin qu'ils acquièrent des compétences en matière de résolution de systèmes. Le but du deuxième TP est de familiariser les étudiants avec les calculs de base du traitement du signal (calcul de transformée de Fourier, aliasing, modulation de fréquence ou d'amplitude, filtres passe-bas, filtre de Wiener). Ce dernier TP permet aux étudiants de mettre en pratique les connaissances acquises durant les cours et TDs de traitement du signal.
- Je participe également à un TP réseau (12h de face à face pédagogique, niveau L3) où les étudiants doivent programmer un serveur envoyant des vidéos en utilisant les protocoles réseaux classiques (UDP, TCP-pull, TCP-push, Multicast). Le but pédagogique de ce TP est l'acquisition de compétences en matière de programmation de sockets.

Responsabilités d'Enseignements

- Depuis 2012, je suis **responsable du MASTER M2 recherche** Réseaux, Télécom et Services (RTS) cohabilité par l'INSA de Lyon et l'Université Lyon 1. Ce MASTER diplôme entre 10 et 15 étudiants chaque année, notamment des double-diplômes ingénieur INSA/MASTER. Il s'agit ici de la gestion complète du MASTER : sélection des dossiers de candidature, mise en place de l'emploi du temps, gestion des stages, participation aux jurys communs avec les autres M2 de Lyon 1, rédaction des évaluations et des habilitations/certifications.
- De 2005 à 2007, j'ai également été responsable avec Anne Legait de la gestion des stages de 3ème et 4ème année au département informatique. En 2007, nous avons finalement opté pour une gestion décentralisée rendant caduc le besoin de responsable pour cette tâche.
- De 2005 à 2009, j'ai été responsable du lien entre le département informatique de l'INSA de Lyon et IBM-Montpellier. Dans ce cadre, j'ai organisé durant 2 ans la visite du Data Center d'IBM pour un groupe d'une trentaine d'étudiants de 5ème année.

Activités d'Enseignement avant mon Arrivée à l'INSA de Lyon

J'ai effectué successivement les enseignements suivants :

- 2004 - 2005 :
  - Lors de mon année d'ingénieur expert dans l'Equipe Projet CODES de l'INRIA Rocquencourt, j'ai effectué des vacations d'enseignement à l'école privée d'ingénieur EFREI à Villejuif. J'ai enseigné des TPs de programmation en langage C à hauteur de 80 heures EQTD au niveau L1 et j'ai participé à l'évaluation finale du module de programmation en C. J'ai également enseigné des TPs de programmation en langage C à hauteur de 37,5 heures EQTD au niveau L1 à l'Université Paris 8.
- 2003 - 2004 : Demi ATER en mathématiques à l'Université Paris 8 :
  - Cours et TD, introduction aux probabilités, Université Paris 8 (48 heures EQTD, niveau L2).
  - Cours et TD, suites et séries de fonctions, Université Paris 8 (48 heures EQTD, niveau L2).
- 2002-2003 : Durant mon post-doctorat à l'Université Technique du Danemark (DTU, Lyngby), j'ai effectué les enseignements suivants :
  - Travaux Dirigés de cryptographie (20 heures EQTD, niveau L3).
  - Cours de cryptographie symétrique et cryptanalyse (12 heures EQTD, niveau M1).

3 Détails des Activités de Recherche

Résumé des Activités Scientifiques Doctorales

Durant ma thèse ainsi que pendant les deux années qui ont suivi (2002-2004), mon thème de recherche principal a été l'étude des algorithmes de chiffrement par blocs utilisés en cryptographie symétrique.

Rappelons tout d'abord qu'en cryptographie symétrique, pour que deux individus communiquent entre eux sur un canal non sécurisé, il faut qu'ils partagent une même clé k servant à la fois au chiffrement et au déchiffrement. L'une des meilleures méthodes en matière de rapidité et de sécurité pour chiffrer des messages en clé secrète est l'utilisation d'algorithmes de chiffrement par blocs. Ces algorithmes prennent en entrée/sortie des blocs de taille n bits et sont composés de r étages. À chaque étage, une même fonction paramétrée par une sous-clé k_i est itérée. Les sous-clés sont différentes à chaque étage et générées à partir de la clé secrète k et d'un algorithme de génération de clés.

L'essentiel de mes travaux doctoraux a porté sur l'étude de ces algorithmes du point de vue de l'attaquant. Nous avons monté deux attaques particulières contre les candidats AES (compétition qui s'est déroulée de 1997 à 2000) Crypton et Rijndael (le futur AES) [57, 58]. L'attaque contre l'AES reste encore l'une des meilleures connues et fait l'objet d'un cours de troisième cycle à l'université de Louvain. Nous avons également proposé une attaque [55] contre un schéma de signature à clé publique nommé SFLASH utilisant les principes de la cryptographie multivariable. Cette attaque qui exploite une propriété particulière des espaces d'entrée/sortie a obligé les concepteurs de l'algorithme à modifier ce dernier.

Parallèlement, je me suis intéressée aux notions de pseudo-aléatoirité et de super-pseudo-aléatoirité servant de base au modèle de sécurité des algorithmes de chiffrement par blocs [56].

Résumé des Activités Scientifiques depuis 2004

Cette partie décrit mes activités de recherche effectuées durant mon poste d'ingénieur expert à l'INRIA Rocquencourt (2004-2005) et mes années comme maître de conférences au laboratoire CITI (depuis 2005).

Résumé des Activités Scientifiques concernant la cryptographie symétrique

Depuis 2004, je continue mon activité de recherche théorique concernant la cryptographie symétrique en m'attachant plus particulièrement aux algorithmes de chiffrement à flot, aux algorithmes de chiffrement par blocs et aux fonctions de hachage (notamment dans le cadre de la compétition du NIST SHA-3, 2007-2012). Durant mon année d'ingénieur expert au projet CODES de l'INRIA Rocquencourt financé par le projet RNRT X-CRYPT, nous avons soumis à la compétition eStream [4] du réseau d'excellence Européen ECRYPT [5] deux propositions d'algorithmes de chiffrement à flot : SOSEMANUK [5] dans la catégorie logicielle et Decim [4] dans la catégorie matérielle. SOSEMANUK a été retenu comme finaliste dans la catégorie logicielle.

Dans le cadre du projet ANR SETIN 2006 RAPIDE (2007-2010) et du co-encadrement de thèse de Benjamin Pousse (laboratoire XLIM, Limoges) financé par ce même projet, nous avons obtenu avec F. Arnault, T. Berger (du laboratoire XLIM, Limoges) et C. Laraudoux (équipe INRIA Privatics) des résultats clés concernant l'utilisation d'une représentation matricielle pour les FCSR (Feedback with Carry Shift Register) et les LFSR (Linear Feedback Shift Register), briques de base fondamentales pour la construction d'algorithmes de chiffrement à flot [16, 17, 39].

4. `http://www.ecrypt.eu.org/stream/index.html`
5. `http://www.ecrypto.eu.org`

En ce qui concerne les algorithmes de chiffrement par blocs, nous avons, avec B. Pousse et R. Phan (Loughborough University), exploité des propriétés intégrales afin de monter des distingueurs dans les nouveaux modèles dits à clés connues et à clés liées connues [12]. Nous avons trouvé le même type de propriétés contre 3 des candidats de la compétition SHA-3. Avec T. Peyrin (Nanyang Technological University, Singapore) et M. Naya-Plasencia (PRISM, Université de Versailles), nous avons monté une attaque par rebond sur le candidat SHA-3 SHAvite-256 afin de générer des collisions sur une version réduite de la fonction de compression [31].

Depuis 2011, je suis coordinatrice du projet ANR 2011 INS BLOC (2011-2015) dont le but est d'étudier le design et les attaques contre les chiffrements par blocs dédiés aux environnements contraints comme les tags RFIDs ou les capteurs. Dans le cadre de ce projet, je co-encadre depuis novembre 2011 la thèse de Gaël Thomas au laboratoire XLIM de Limoges avec T. Berger. Nous travaillons actuellement sur une représentation matricielle des schémas de Feistel [23] et la définition d'un nouvel algorithme de chiffrement par blocs pour environnement contraint. L'un des défis que se propose de relever le projet BLOC concerne la définition de ce que doit être un bon algorithme de génération de clés permettant de construire des preuves de sécurité. Nous avons, dans le cadre du projet BLOC, implémenté une librairie de chiffrements par blocs [24] dédié à un environnement contraint particulier, il s'agit ici du capteur WSN430 utilisé dans les IoT-labs déployés en France [6]. La librairie est disponible en ligne : `http://bloc.project.citi-lab.fr/library.html`.

Résumé des Activités Scientifiques concernant la sécurité dans les réseaux sans fil

A mon arrivée au laboratoire CITI, et afin de m'intégrer à l'équipe INRIA ARES, je me suis intéressée à des domaines de recherche plus pratiques où se posaient des problématiques concrètes de sécurité. Il s'agissait des modèles de confiance dans les réseaux ambiants et de la sécurité des réseaux de capteurs sans fil, domaine d'application privilégié du laboratoire CITI qui lui vaut sa reconnaissance internationale.

S. Ubéda m'a proposé de prendre la responsabilité du projet ANR ACI Sécurité Informatique KAA (2004-2007) et de co-encadrer la thèse de Samuel Galice financée dans le cadre de ce projet. Ce projet multidisciplinaire avait pour objectif l'étude des modèles de confiance dans les réseaux ambiants. Nous avons donc cherché à développer avec l'aide de sociologues, d'économistes et de juristes un modèle de confiance informatique qui soit socialement acceptable et économiquement viable. Nous avons finalement proposé le modèle KAA qui fonde la confiance entre deux entités sur des échanges qui ont eu lieu dans le passé et qui sont cryptographiquement vérifiables [48]. Afin de financer une partie de l'étude relevant de l'économie expérimentale, nous avons, suite à ce premier projet, monté un deuxième projet d'un an financé par l'IXXI (2008) afin de conduire à bien la dernière partie de ce travail.

Parallèlement à ce premier projet, depuis 2007, je m'intéresse à la sécurité dans les réseaux de capteurs sans fil. Dans le cadre de la thèse de Wassim Znaidi financée par la région Rhône-Alpes, nous avons proposé des solutions algorithmiques et cryptographiques permettant de détecter ou de contourner des attaques dédiées à ces réseaux. Nous avons notamment proposé une méthode fondée uniquement sur des informations locales de voisinage permettant de détecter des attaques de type Wormhole [45] ou de type réplication [7]. Nous avons proposé l'utilisation de codes d'authentification de messages homomorphes permettant d'assurer l'authenticité et l'intégrité de données agrégées ou combinées via du codage réseau [13]. C'est aussi sur ce thème et plus précisément sur la sécurité du codage réseau dans les réseaux de capteurs sans fil que travaillait Yuanyuan Zhang (Novembre 2010-Avril 2012), post-doctorante que j'encadrais, financée par une bourse de la fondation franco-chinoise FFCSA. Nous avons notamment étudié des contremesures au problème de l'attaque par inondation dans les réseaux de capteurs sans fil [10]. Nous avons mené une étude théorique afin de savoir comment se propageait un paquet pollué en fonction de la politique du buffer stockant les

6. pour plus de détails voir : `http://www.senslab.info/`

paquets à coder [8].

Dans le cadre du projet ANR VERSO ARESA2 (2010-2013) et d'une collaboration avec Orange Labs Grenoble qui a financé la thèse d'Ochirkhand Erdene-Ochir, avec F. Valois du CITI et A. Kountouris (Orange Labs Grenoble), nous nous sommes intéressés à la résilience des protocoles de routage dans les réseaux de capteurs sans fil. Il s'agit de proposer des protocoles qui vont être intrinsèquement résilients et vont donc continuer à router les paquets de données dans le réseau même en présence d'attaquants [28]. Nous avons également défini une métrique permettant de comparer ces différents protocoles [9]. Avec F. Valois, nous avons continué à travailler dans cette direction en encadrant plsu récemment deux stages de MASTER, celui de Pierre Brunisholz sur la résilience du codage réseau et celui de Khaoula Dhifallah sur la résilience du protocole RPL.

Résumé des Activités Scientifiques concernant la Privacy

Depuis 2012, je fais partie de la nouvelle équipe INRIA Privatics bilocalisée entre Grenoble et Lyon et dont le thème de recherche central est la protection des données de la vie privée. Des résultats tant théoriques en cryptographie que pratiques en sécurité, sont bien sûr des éléments très importants pour garantir la privacy dans les domaines qui représentent les nouveaux paradigmes de l'informatique comme les bases de données, les réseaux ambiants ou les réseaux de capteurs sans fil. Avec Cédric Lauradoux (CR, EPI INRIA Privatics) et Mathieu Cunche (MCF, INSA de Lyon, EPI INRIA Privatics), tous deux membres de l'équipe INRIA Privatics, nous avons dans [25] proposé une architecture de sécurité permettant de garantir d'une part la privacy des données-utilisateurs et leur vérifiabilité dans le contexte du smart metering. Nous souhaitons d'une part continuer cette étude et d'autre part tester sur des données réelles l'applicabilité de méthodes comme le k-anonymat ou la differential privacy.

En tant qu'HDR, je co-encadre depuis Novembre 2014 avec Mathieu Cunche la thèse de Célestin Matte qui porte sur les systèmes d'observation des flux humains via Wi-Fi respectueux de la vie privée. L'idée de cette thèse est d'étudier les différentes politiques d'anonymisation possibles sur les données qui fuitent via le Wi-Fi des téléphones portables dit intelligents et d'étudier selon un certain nombre de métriques classiques comme le suivi d'un utilisateur particulier, le k-anonymat,... ces différentes politiques. Le but est de proposer à la fin de cette thèse un certain nombre de politiques qui respectent l'avis de la CNIL concernant les dispositifs de mesure de fréquentation [7].

7. http://www.cnil.fr/linstitution/actualite/article/article/mesure-de-frequentation-et-analyse-du-comportement-des-consommateurs-dans-les-magasins/

4 Liste Complète de mes Publications

Thèses et Habilitations

[1] Marine Minier : Quelques résultats en cryptographie symétrique, pour les modèles de confiance dans les réseaux ambiants et la sécurité dans les réseaux de capteurs sans fil. Habilitation à Diriger des Recherches, Université Claude Bernard Lyon 1 et INSA de Lyon, France, mai 2012.

[2] Marine Minier : *Preuves d'Analyses et de Sécurité en Cryptologie à Clé Secrète*. Thèse de doctorat, Université de Limoges, France, 2002.

Chapitres de Livre d'Audience Internationale

- 2012 -

[3] YuanYuan Zhang, Marine Minier et Wassim Znaidi : Security FOR Network Coding. *In* Khaldoun Al Agha, éditeur : *Network Coding, Chapitre de livre*. ISTE Ltd and Wiley, 2012.

- 2008 -

[4] C. Berbain, O. Billet, A. Canteaut, N. Courtois, B. Debraize, H. Gilbert, L. Goubin, A. Gouget, L. Granboulan, C. Lauradoux, M. Minier, T. Pornin et H. Sibert : Decimv2. *In* M. Robshaw et O. Billet, éditeurs : *New Stream Cipher Designs*, volume 4986 de *Lecture Notes in Computer Science*, pages 140–151. Springer, 2008.

[5] C. Berbain, O. Billet, A. Canteaut, N. Courtois, H. Gilbert, L. Goubin, A. Gouget, L. Granboulan, C. Lauradoux, M. Minier, T. Pornin et H. Sibert : Sosemanuk : a fast oriented software-oriented stream cipher. *In* M. Robshaw et O. Billet, éditeurs : *New Stream Cipher Designs*, volume 4986 de *Lecture Notes in Computer Science*, pages 98–118. Springer, 2008.

Brevets

[6] Apostolos KOUNTOURIS, Ochirkhand ERDENE-OCHIR, Marine MINIER et Fabrice VALOIS : Invention : Méthode résiliente à la présence des noeuds compromis pour la détermination des routes par un protocole de routage dans un réseau. brevet européen Numéro FR-11 58 828, Int. : PCT/FR2012/052143, Septembre 2012.

Revues Internationales

- 2013 -

[7] Wassim Znaidi, Marine Minier et Stéphane Ubéda : Hierarchical Node Replication Attacks Detection in Wireless Sensor Networks. *IJDSN - International Journal of Distributed Sensor Networks*, 2013:12 pages, 2013.

[8] Yuanyuan Zhang and Marine Minier. How network coding system constrains packet pollution attacks in wireless sensor networks. *IJGUC*, 4(2/3) :197–203, 2013.

- 2012 -

[9] Ochirkhand Erdene-Ochir, Apostolos Kountouris, Marine Minier et Fabrice Valois : A New Metric to Quantify Resiliency in Networking. *Communications Letters, IEEE*, 16(10):1699–1702, IEEE, 2012.

[10] YuanYuan Zhang et Marine Minier : Selective Forwarding Attacks Against Data and ACK Flows in Network Coding and Countermeasures. *Journal of Computer Networks and Communications*, (2012), 2012.

[11] Marine Minier et María Naya-Plasencia : A related key impossible differential attack against 22 rounds of the lightweight block cipher LBlock. *Inf. Process. Lett.*, 112(16):624–629, 2012.

[12] Marine Minier, Raphael C.-W. Phan et Benjamin Pousse : On Integral Distinguishers of Rijndael Family of Ciphers. *Cryptologia*, 36(2):104–118, 2012.

[13] Anya Apavatjrut, Wassim Znaidi, Antoine Fraboulet, Claire Goursaud, Katia Jaffrès-Runser, Cédric Lauradoux et Marine Minier : Energy efficient authentication strategies for network coding. *Concurrency and Computation : Practice and Experience*, 24(10):1086–1107, 2012.

[14] Wassim Znaidi et Marine Minier : Key management and access control scheme for WSNs. *Telecommunication Systems Journal*, 50(2):113–125, 2012.

- 2011 -

[15] Ochirkhand Erdene-Ochir, Marine Minier, Fabirce Valois et Apostolos Kountouris : Enhancing Resiliency Against Routing Layer Attacks in Wireless Sensor Networks : Gradient-based Routing in Focus. *IARIA on-line journals, International Journal on Advances in Networks and Services*, 4(1&2):38–54, 2011. disponible en ligne `http://www.iariajournals.org/networks_and_services/`.

[16] François Arnault, Thierry P. Berger, Marine Minier et Benjamin Pousse : Revisiting LFSRs for Cryptographic Applications. *IEEE Transactions on Information Theory*, 57(12):8095–8113, 2011.

- 2008 -

[17] F. Arnault, T. P. Berger et M. Minier : Some Results on FCSR Automata with applications to the security of FCSR-based pseudorandom generators. *IEEE Trans. on Inf. Theory*, 54(2):836–841, 2008.

[18] Samuel Galice, Marine Minier et Stéphane Ubéda : The KAA Framework : A History-Based Trust Establishment in Ambient Networks. *IJICS - International Journal of Intelligent Control and Systems, Special Issue on Information Assurance*, 12(4):331–340, 2007.

Conférences Internationales avec Comité de Lecture et Actes

- 2015 -

[19] Céline Blondeau et Marine Minier : Analysis of Impossible, Integral and Zero-Correlation Attacks on Type-II Generalized Feistel Networks using the Matrix Method. *In Fast Software Encryption - FSE 2015*, volume à paraître de *Lecture Notes in Computer Science*, pages à paraître. Springer, 2015.

[20] Marine Minier : Improving Impossible Differential Attacks against Rijndael-160 and Rijndael-224. *In The Ninth International Workshop on Coding and Cryptography - WCC 2015*, à paraître, 2015.

[21] Ochirkhand Erdene-Ochir, Mohamed Abdallah, Khaled Qaraqe, Marine Minier et Fabrice Valois : Theoretical Framework of Resilience : Biased Random Walk Routing Against Insider Attacks. *In IEEE Wireless Communications and Networking Conference - WCNC 2015*, pages à paraître. IEEE, 2015.

- 2014 -

[22] Ochirkhand Erdene-Ochir, Mohamed Abdallah, Khaled Qaraqe, Marine Minier et Fabrice Valois : Routing Resilience Evaluation for Smart Metering : Definition, Metric and Techniques. *In IEEE PIMRC 2014 - International Symposium on Personal, Indoor and Mobile Radio Communications*, pages 1-6. IEEE, 2014.

- 2013 -

[23] Thierry P. Berger, Marine Minier et Gaël Thomas : Extended Generalized Feistel Networks using Matrix Representation. *In Selected Areas in Cryptography - SAC 2013*, volume à paraître de *Lecture Notes in Computer Science*. Springer, 2013.

[24] Mickaël Cazorla, Kevin Marquet, and Marine Minier. Survey and Benchmark of Lightweight Block Ciphers for Wireless Sensor Networks. In *SECRYPT 2013 - - Proceedings of the International Conference on Security and Cryptography*, volume to appear. SciTePress, 2013.

[25] Mathieu Cunche, Cedric Lauradoux, Marine Minier, and Roksana Boreli. Private and resilient data aggregation. In *38th Annual IEEE Conference on Local Computer Networks - LCN 2013*, pages 1-6. IEEE, 2013.

[26] Marine Minier and Gaël Thomas. Integral Distinguisher on Grøstl-512 v3. In *Progress in Cryptology - INDOCRYPT 2013*, volume 8250 of *Lecture Notes in Computer Science*, pages 50–60. Springer, 2013.

[27] Marine Minier. On the security of *Piccolo* lightweight block cipher against related-key impossible differentials. In *Progress in Cryptology - INDOCRYPT 2013*, volume 8250 of *Lecture Notes in Computer Science*, pages 308–317. Springer, 2013.

- 2012 -

[28] Ochirkhand Erdene-Ochir, Marine Minier, Fabrice Valois et Apostolos A. Kountouris : Resiliency taxonomy of routing protocols in Wireless Sensor Networks. *In 37th Annual IEEE Conference on Local Computer Networks, Clearwater Beach, FL, USA, October 22-25, 2012 - LCN 2012*, pages 324–327. IEEE, 2012.

[29] Thierry P. Berger et Marine Minier : Cryptanalysis of Pseudo-random Generators Based on Vectorial FCSRs. *In Progress in Cryptology - INDOCRYPT 2012*, volume 7668 de *Lecture Notes in Computer Science*, pages 209–224. Springer, 2012.

[30] Thierry P. Berger, Joffrey D'Hayer, Kevin Marquet, Marine Minier et Gaël Thomas : The GLUON Family : A Lightweight Hash Function Family Based on FCSRs. *In Progress in Cryptology - AFRICACRYPT 2012*, volume 7374 de *Lecture Notes in Computer Science*, pages 306–323. Springer, 2012.

- 2011 -

[31] Marine Minier, María Naya-Plasencia et Thomas Peyrin : Analysis of Reduced-SHAvite-3-256 v2. *In Fast Software Encryption - FSE 2011*, volume 6733 de *Lecture Notes in Computer Science*, pages 68–87. Springer, 2011.

[32] Marine Minier et Raphael C.-W. Phan : Energy-Efficient Cryptographic Engineering Paradigm. *In Open Problems in Network Security - IFIP WG 11.4 International Workshop, iNetSec 2011*, volume 7039 de *Lecture Notes in Computer Science*, pages 78–88. Springer, 2011.

[33] Yuanyuan Zhang, Wassim Znaidi, Cédric Lauradoux et Marine Minier : Flooding attacks against network coding and countermeasures. *In 5th International Conference on Network and System Security, NSS 2011*, pages 305–309. IEEE, 2011.

- 2010 -

[34] Marine Minier, Raphael C.-W. Phan et Benjamin Pousse : Integral Distinguishers of Some SHA-3 Candidates. *In Cryptology and Network Security - CANS 2010*, volume 6467 de *Lecture Notes in Computer Science*, pages 106–123. Springer, 2010.

[35] Chérifa Boucetta, Mohamed Ali Kâafar et Marine Minier : How Secure are Secure Localization Protocols in WSNs ? *In Sensor Systems and Software - Second International ICST Conference, S-Cube 2010*, volume 57 de *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*, pages 164–178. Springer, 2010.

[36] Ochirkhand Erdene-Ochir, Marine Minier, Fabrice Valois et Apostolos Kountouris : Resiliency of wireless sensor networks : Definitions and analyses. *In Telecommunications (ICT), 2010 IEEE 17th International Conference on*, pages 828–835. IEEE, april 2010.

[37] Ochirkhand Erdene-Ochir, Marine Minier, Fabrice Valois et Apostolos Kountouris : Toward Resilient Routing in Wireless Sensor Networks : Gradient-Based Routing in Focus. *In Sensor Technologies and Applications (SENSORCOMM), 2010 Fourth International Conference on*, pages 478–483. IEEE, july 2010.

[38] Anya Apavatjrut, Wassim Znaidi, Antoine Fraboulet, Claire Goursaud, Cédric Lauradoux et Marine Minier : Energy Friendly Integrity for Network Coding in Wireless Sensor Networks. *In Fourth International Conference on Network and System Security, NSS 2010*, pages 223–230. IEEE Computer Society, 2010.

- 2009 -

[39] François Arnault, Thierry P. Berger, Cédric Lauradoux, Marine Minier et Benjamin Pousse : A New Approach for FCSRs. *In Selected Areas in Cryptography - SAC 2009*, volume 5867 de *Lecture Notes in Computer Science*, pages 433–448. Springer, 2009.

[40] Thierry Berger, Marine Minier et Benjamin Pousse : Software oriented stream ciphers based upon FCSRs in diversified mode. *In Progress in Cryptology - INDOCRYPT 2009*, volume 5922 de *Lecture Notes in Computer Science*, pages 119–135. Springer, 2009.

[41] Gérald Gavin et Marine Minier : Oblivious Multi-variate Polynomial Evaluation. *In Progress in Cryptology - INDOCRYPT 2009*, volume 5922 de *Lecture Notes in Computer Science*, pages 430–442. Springer, 2009.

[42] Wassim Znaidi, Cédric Lauradoux et Marine Minier : Aggregated authentification (AMAC) using universal hash functions. *In International ICST Conference on Security and Privacy in Communication Networks - SecureComm 2009*, volume 19 de *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*, pages 248–264. Springer, 2009.

[43] Marine Minier, Raphael C.-W. Phan et Benjamin Pousse : Distinguishers for Ciphers and Known Key Attack against Rijndael with Large Blocks. *In Progress in Cryptology - AFRICACRYPT 2009*, volume 5580 de *Lecture Notes in Computer Science*, pages 60–76. Springer, 2009.

[44] Wassim Znaidi, Marine Minier et Stéphane Ubéda : Hierarchical node replication attacks detection in wireless sensors networks. *In Proceedings of the IEEE 20th International Symposium on Personal, Indoor and Mobile Radio Communications, PIMRC 2009*, pages 82–86. IEEE, 2009.

- 2008 -

[45] Wassim Znaidi, Marine Minier et Jean-Philippe Babau : Detecting wormhole attacks in wireless networks using local neighborhood information. *In Proceedings of the IEEE 19th International Symposium on Personal, Indoor and Mobile Radio Communications, PIMRC 2008*, pages 1–5. IEEE, 2008.

[46] Samuel Galice et Marine Minier : Improving Integral Attacks Against Rijndael-256 Up to 9 Rounds. *In Progress in Cryptology - AFRICACRYPT 2008*, volume 5023 de *Lecture Notes in Computer Science*, pages 1–15. Springer, 2008.

- 2007 -

[47] François Arnault, Thierry P. Berger, Cédric Lauradoux et Marine Minier : X-FCSR - A New Software Oriented Stream Cipher Based Upon FCSRs. *In Progress in Cryptology - INDOCRYPT 2007*, volume 4859 de *Lecture Notes in Computer Science*, pages 341–350. Springer, 2007.

[48] Samuel Galice, Marine Minier et Stéphane Ubéda : A trust protocol for community collaboration. *In Joint iTrust and PST Conferences on Privacy, Trust Management and Security - IFIPTM 2007*, volume 238 de *IFIP Advances in Information and Communication Technology*, pages 169–184. Springer, 2007.

[49] Samuel Galice, Marine Minier et Stéphane Ubéda : Gestion de la confiance dans les communautés ouvertes. *In Conférence Internationale sur les NOuvelles TEchnologies de la REpartition - NOTERE 2007*, 2007.

[50] Nicolas Fournel, Marine Minier et Stéphane Ubéda : Survey and Benchmark of Stream Ciphers for Wireless Sensor Networks. *In Information Security Theory and Practices - WISTP 2007*, volume 4462 de *Lecture Notes in Computer Science*, pages 202–214. Springer, 2007.

- 2006 -

[51] Samuel Galice, Véronique Legrand, Marine Minier, John Mullins et Stéphane Ubéda : A History-Based Framework to Build Trust Management Systems. *In Second International Conference on Security and Privacy in Communication Networks and the Workshops - SecureComm 2006*, pages 1–7. IEEE, 2006.

[52] Samuel Galice, Marine Minier, John Mullins et Stéphane Ubéda : Cryptographic Protocol to Establish Trusted History of Interactions. *In Security and Privacy in Ad-Hoc and Sensor Networks - ESAS 2006*, volume 4357 de *Lecture Notes in Computer Science*, pages 136–149. Springer, 2006.

- 2005 -

[53] Thierry P. Berger et Marine Minier : Two Algebraic Attacks Against the F-FCSRs Using the IV Mode. *In Progress in Cryptology - INDOCRYPT 2005*, volume 3797 de *Lecture Notes in Computer Science*, pages 143–154. Springer, 2005.

- 2004 -

[54] Marine Minier : A Three Rounds Property of the AES. *In Advanced Encryption Standard - AES 2004, 4th International Conference*, volume 3373 de *Lecture Notes in Computer Science*, pages 16–26. Springer, 2004.

- 2002 -

[55] Henri Gilbert et Marine Minier : Cryptanalysis of SFLASH. *In Advances in Cryptology - EUROCRYPT 2002*, volume 2332 de *Lecture Notes in Computer Science*, pages 288–298. Springer, 2002.

- 2001 -

[56] Henri Gilbert et Marine Minier : New Results on the Pseudorandomness of Some Blockcipher Constructions. *In Fast Software Encryption - FSE 2001*, volume 2355 de *Lecture Notes in Computer Science*, pages 248–266. Springer, 2002.

- 2000 -

[57] Marine Minier et Henri Gilbert : Stochastic Cryptanalysis of Crypton. *In Fast Software Encryption - FSE 2000*, volume 1978 de *Lecture Notes in Computer Science*, pages 121–133. Springer, 2001.

[58] Henri Gilbert et Marine Minier : A Collision Attack on 7 Rounds of Rijndael. *In AES Candidate Conference*, pages 230–241, 2000.

Workshops Internationaux avec Comité de Lecture et Actes

- 2014 -

[59] Christine Solnon, Marine Minier et Julia Reboul : Solving a Symmetric Key Cryptographic Problem-with Constraint Programming. ModRef 2014, Workshop of the CP 2014 Conference, September 2014. Lyon, France.

- 2011 -

[60] Marine Minier et María Naya-Plasencia : Some Preliminary Studies on the Differential Behavior of the Lightweight Block Cipher LBlock. Workshop on Lightweight Cryptogrpahy 2011, November 2011. Louvain, Belgique.

- 2008 -

[61] Benjamin Pousse et Marine Minier : Construction of FCSR algebraic equations and empirical analysis. SASC 2008 - Stream Ciphers Revisited, February 2008. Special Workshop hosted by the ECRYPT Network of Excellence.

- 2007 -

[62] C. Bryce, M. Dekker, S. Etalle, D. Le Métayer, M. Minier et S. Ubéda : Ubiquitous Privacy Protection. *In Fifth Workshop on Privacy in Ubicomp*, 2007.

[63] François Arnault, Thierry P. Berger et Marine Minier : On the security of FCSR-based pseudorandom generators. SASC 2007 - Stream Ciphers Revisited, February 2007. Special Workshop hosted by the ECRYPT Network of Excellence.

- 2006 -

[64] Samuel Galice, Véronique Legrand et Stéphane Ubéda Marine Minier, John Mullins : Modelization and trust establishment in ambient networks. International Symposium on Intelligent Environment, Cambridge, April 2006. poster, 5 pages.

[65] C. Berbain, O. Billet, A. Canteaut, N. Courtois, B. Debraize, H. Gilbert, L. Goubin, A. Gouget, L. Granboulan, C. Lauradoux, M. Minier, T. Pornin et H. Sibert : Decimv2. SASC 2006 - Stream Ciphers Revisited, February 2006. Special Workshop hosted by the ECRYPT Network of Excellence.

- 2005 -

[66] C. Berbain, O. Billet, A. Canteaut, N. Courtois, B. Debraize, H. Gilbert, L. Goubin, A. Gouget, L. Granboulan, C. Lauradoux, M. Minier, T. Pornin et H. Sibert : Decim : a new stream cipher for hardware applications. `http://www.ecrypt.eu.org/stream/`, 2005. Call for Stream Cipher Primitives, Network of Excellence in Cryptology ECRYPT.

[67] C. Berbain, O. Billet, A. Canteaut, N. Courtois, B. Debraize, H. Gilbert, L. Goubin, A. Gouget, L. Granboulan, C. Lauradoux, M. Minier, T. Pornin et H. Sibert : Decim : a new stream cipher for hardware applications. *In Proceedings of SKEW - Symmetric Key Encryption Workshop, Network of Excellence in Cryptology ECRYPT*, mai 2005. `http://www2.mat.dtu.dk/people/Lars.R.Knudsen/stvl/`.

[68] C. Berbain, O. Billet, A. Canteaut, N. Courtois, H. Gilbert, L. Goubin, A. Gouget, L. Granboulan, C. Lauradoux, M. Minier, T. Pornin et H. Sibert : Sosemanuk : a fast oriented software-oriented stream cipher. `http://www.ecrypt.eu.org/stream/`, 2005. Call for Stream Cipher Primitives, Network of Excellence in Cryptology ECRYPT.

[69] C. Berbain, O. Billet, A. Canteaut, N. Courtois, H. Gilbert, L. Goubin, A. Gouget, L. Granboulan, C. Lauradoux, M. Minier, T. Pornin et H. Sibert : Sosemanuk : a fast oriented software-oriented stream cipher. *In Proceedings of SKEW - Symmetric Key Encryption Workshop, Network of Excellence in Cryptology ECRYPT*, mai 2005. `http://www2.mat.dtu.dk/people/Lars.R.Knudsen/stvl/`.

Rapports Techniques et de Recherche

---

[70] Christina Boura, Marine Minier, María Naya-Plasencia, et Valentin Suder : Improved Impossible Differential Attacks against Round-Reduced LBlock. Cryptology ePrint Archive, Report 2014/279, 2014. `http://eprint.iacr.org/2014/279`.

[71] Pierre Brunisholz, Marine Minier et Fabrice Valois : The Gain of Network Coding in Wireless Sensor Networking. Rapport de Recherche RR-8650, INRIA, 2014.

[72] Ochirkhand Erdene-Ochir, Marine Minier, Fabrice Valois et Apostolos A. Kountouris : Resilient networking in wireless sensor networks. Rapport de Recherche RR-7230, INRIA, 2010.

[73] Cédric Lauradoux et Marine Minier : A Mathematical Analysis of Prophet Dynamic Address Allocation. Rapport de Recherche RR-7085, INRIA, 2009.

[74] Marine Minier et Benjamin Pousse : Improving Integral Cryptanalysis against Rijndael with Large Blocks. Rapport de Recherche RR-00423681, INRIA, 2009.

[75] Wassim Znaidi, Marine Minier et Jean-Philippe Babau : An ontology for attacks in wireless sensor networks. Rapport de Recherche RR-6704, INRIA, 2008.

[76] Samuel Galice, Véronique Legrand, Marine Minier, John Mullins et Stéphane Ubéda : The KAA project : a trust policy point of view. Rapport de Recherche RR-5959, INRIA, 2006.

[77] Marine Minier : A Bottleneck Attack on Crypton. Rapport de Recherche RR-5324, INRIA, 2004. 12 pages.

5 Liste de mes Co-auteurs par Ordre Alphabétique

1. Mohamed Abdallah (Chercheur, Université TEXAS A&M au Qatar, Qatar)
2. Anya Apavatjrut (Doctorante, Laboratoire CITI, France)
3. François Arnault (Maître de conférences, XLIM, Université de Limoges, France)
4. Jean-Philippe Babau (Professeur, Université de Brest, France)
5. Côme Berbain (Doctorant, France Télécom R&D, France)
6. Thierry P. Berger (Professeur, XLIM, Université de Limoges, France)
7. Olivier Billet (Doctorant, France Télécom R&D, France)
8. Roksana Boreli (Chercheuse, NICTA, Australie)
9. Chérifa Boucetta (Stagiaire, Laboratoire CITI, France)
10. Christina Boura (Maître de conférences, PRISM, Université de Versaille, France)
11. Pierre Brunisholz (Doctorant, Laboratoire LIG, Université de Grenoble, France)
12. Anne Canteaut (DR, EPI INRIA SECRET, France)
13. Mickaël Cazorla (Stagiaire, Département Informatique, INSA de Lyon, France)
14. Nicolas Courtois (Professeur, University College London, Angleterre)
15. Mathieu Cunche (Maître de conférences, Laboratoire CITI, France)
16. Blandine Debraize (Doctorante, Université de Versailles, France)
17. Joffrey D'Hayer (Stagiaire, Département Télécom, INSA de Lyon, France)
18. Ochirkhand Erdene-Ochir (Doctorante, Laboratoire CITI, France)
19. Nicolas Fournel (Maître de conférences, Laboratoire TIMA, Grenoble, France)
20. Antoine Fraboulet (Maître de conférences, Laboratoire CITI, France)
21. Samuel Galice (Doctorant, Laboratoire CITI, France)
22. Gérald Gavin (Maître de conférences, Université Lyon 1, France)
23. Henri Gilbert (Expert Senior, ANSSI, France)
24. Louis Goubin (Professeur, Laboratoire PRISM, Université de Versailles, France)
25. Aline Gouget (Experte en cryptographie, Gemalto, France)
26. Claire Goursaud (Maître de conférences, Laboratoire CITI, France)
27. Louis Granboulan (Expert en cryptographie, EADS, France)
28. Katia Jaffrès-Runser (Maître de conférences, , France)
29. Mohamed Ali Kâafar (CR, EPI INRIA Privatics, France)
30. Apostolos A. Kountouris (Ingénieur, Orange Labs Grenoble, France)
31. Cédric Lauradoux (CR, EPI INRIA Privatics, France)
32. Véronique Legrand (Professeur associée, Laboratoire CITI, France)
33. Kevin Marquet (Maître de conférences, Laboratoire CITI, France)
34. John Mullins (Professeur, École Polytechnique de Montréal, Canda)
35. María Naya-Plasencia (CR, EPI INRIA SECRET, France)
36. Thomas Peyrin (Assistant Professor, Nanyang Technological University, Singapour)
37. Raphael Chung-Wei Phan (Professeur, Multimedia University, Malaisie)
38. Thomas Pornin (Ingénieur, Cryptolog International, France)
39. Benjamin Pousse (Doctorant, XLIM, Université de Limoges, France)
40. Khaled Qaraqe (Professeur, Université TEXAS A&M au Qatar, Qatar)
41. Hervé Sibert (Architecte Sécurité, ST-Ericsson, France)
42. Valebtin Suder (Post-doctorant, Université de Waterloo, Canada)
43. Gaël Thomas (Doctorant, XLIM, Université de Limoges, France)
44. Stéphane Ubéda (Professeur, délégation INRIA, France)
45. Fabrice Valois (Professeur, Laboratoire CITI, France)
46. Yuanyuan Zhang (Post-doctorante, Laboratoire CITI, France)
47. Wassim Znaidi (Doctorant, Laboratoire CITI, France)