Loubna Ghammam

Curriculum Vitae

32 Rue Mirabeau
35700 Rennes
(+33) 07 55 07 86 17
ghammam.loubna@yahoo.fr

Formation

Septembre 2016–... **Post-Doc**, ENSI Caen, École Nationale Supérieur d'Ingénieurs de Caen.

Sujet: La Cryptographie Homomorphique sur les réseaux

Novembre 2013– Décembre 2016 **Doctorat en mathématiques appliquées**, IRMAR de Rennes-France, Faculté des Sciences de Monastir-Tunisie.
(Thèse en cotutelle)

Sujet: Utilisation des couplages en cryptographie asymétrique pour la micro électronique.

2011–2013 **Master de recherche en mathématiques et applications**, Faculté des Sciences de Monastir - Tunisie, Mention : **AssezBien(Major de promotion)**.

2007–2011 **Licence fondamentale en Mathématiques et applications** , Institut Supèrieure de Mathématique et d'Informatique de Monastir - Tunisie.

Juin 2007 **Baccalauréat-Scientifique**, *Spécialité Mathématiques*, Lycée de Ksour Essef, Tunisie.
Mention : **Bien**

Expériences de Recherches

Septembre 2016–... **Post-Doc**, Laboratoire de GREYC, Le Groupe de Recherche en Informatique, Image, Automatique et Instrumentation de Caen .

Sujet: La Cryptographie Homomorphique sur les réseaux

Encadrants : Patrick Lacharme

Novembre 2013– Novembre 2016 **Doctorante**, Laboratoire de Mathématiques (IRMAR-UMR 6625 du CNRS), IRMAR de Rennes-France.

Laboratoire d'électronique et de micro-électronique FSM de Monastir-Tunisie

Sujet: Utilisation des couplages en cryptographie asymétrique pour la micro électronique

Encadrants : Sylvain Duquesne & Leila Ben Abdelghani

Avril et Novembre 2015 **Stage de Recherche**, Laboratoire de Mathématiques Nicolas Oresme (CNRS UMR 5139), Université de Caen-France.

Collaboration John Boxall & Emmanuel Fouotsa

Octobre 2015 **Stage de Recherche**, Institut de Mathématiques de Toulon, Université de Toulon-France.
Collaboration Nicolas Méloni

Juillet 2016 **Stage de Recherche**, N, Ecole des Mines de Saint Etienne, antenne de Gardanne.
Collaboration Nadia El Mrabet

Février-Octobre 2013 **Stage de Master 2**, *Faculté des Sciences de Monastir-Tunisie* , IRMAR de Rennes-France, Mention : **Très Bien**.

Sujet : Couplages sur les courbes elliptiques.

Encadrant : Leila Ben Abdelghani

Thèmes de Recherche

1 Les Couplages Optimaux pour les différents niveaux de sécurité.

1 Courbes Elliptiques.

2 Implémentation des Couplages dans un environnement restreint.

3 Calcul de produit de n couplages.

4 Les chaînes d'additions.

5 Attaques et contre mesure sur le calcul des couplages.

5 Chiffrement homomorphique sur les réseaux.

5 Chiffrement homomorphique sur les entiers.

Publications

[1] Sylvain Duquesne and Loubna Ghammam(2015). Memory Saving computation of the pairing final exponentiation on BN curves*. groups complexity cryptology- De Gruyter.

[2] Loubna Ghammam. and Emmanuel Fouotsa (2016).On the computation of the Optimal Ate pairing at the 192-security level*. Soumis à Applicable Algebra in Engineering, Communication and Computing

[3] Anissa Sghaier and Loubna Ghammam and . . . (2015). Area efficient Hardware Implementation of Optimal Ate Pairing on BN Curves*. Soumis à Journal of Universal Computer Science

[4] Loubna Ghammam and Emmanuel Fouotsa(2016). Adequate Elliptic Curve for Computing the product of n pairings*. **Soumis**

[5] Loubna Ghammam (2016). On computing the hard part of the final exponentiation of Tate pairing and its derivates. Soumis à WAIFI

[6] Loubna Ghammam and Antti Hakaka and Imed Ben Dhaou . . . (2016). Application Driven Survey on Recent Developments in the Field of Lightweight Cryptography. **En préparation**

[7] Loubna Ghammam, Nicolas Méloni et Nadia Elmrabet (2016). Contre mésure sur les attaques par injection des fautes sur l'algorithme de Miller. **En préparation**

∗ Ces papiers sont publiés dans eprint cryptography archieve.

Congrès & Colloques

- **Séminaire "Université Rennes IRMAR"** Le calcul de l'exponentiation finale du Couplage Optimal Ate sur les courbes BN , Talk, 29 Janvier 2015.
- **Séminaire "Université Caen"** Le gain sur la mémoire dans le calcul des couplages, Talk, 04 Novembre 2015.
- **Réunion d'équipe SIMPATIC "ENS Paris"** Le couplage Optimal Ate sur les BN: du non implémentable à l'implémentable sur une carte à puce, Talk, Avril 2015.
- **Séminaire "Université de Rennes IRMAR"** Le produit de n couplages dans le pratique , Talk, Janvier 2016.
- "**École de Printemps**", 17 - 21 Mars 2014, Grenoble-France.
- **Semaine D'étude Maths – Entreprises SEME**, 20- 24 Janvier 2014, Orléans-France.

Conférences et Posters

- **WorkshopWAIFI** Internation Workshop on Arithmetich on finite Fields Adequate Elliptic Curves for Computing the product of n pairings. 12-15 Juillet 2016 Ghent, Belgique.
- **ConférenceSMT** Couplages sur les courbes elliptiques ,20-24 Mars 2016, Hammamet, Tunisie.
- **Journées de Cryptographie et Codages**. 24 - 28 Mars 2014, Grenoble-France.
- **Journées de Cryptographie et Codages**. Talk, Memory Saving computation of the pairing final exponentiation on BN curves, 04 - 09 Octobre 2015, Toulon-France.
- **Rencontres Crypto'Puces**. Talk, Memory Saving computation of the Optimal Ate pairing, 4 au 8 mai 2015, au village IGESA, sur l'île de Porquerolles.

Expériences d'Enseignement

2014–2015 **Enseignante vacataire au Lycée de Cesson Sévigné** (Rennes-France)

- Cours et TD Probabilité pour les classes Terminals S.
- Cours et TD Probabilité pour les classes de Première ES.
- Cours et TD Probabilité pour la Première S.
- Cours et TD Géométrie dans l'espace pour la classe de Seconde.

Connaissances Informatiques & Linguistiques

- Calcul Mathématique : Sage, Matlab, Magma.
- Programmation : Langage C, Paris/GP.
- Systèmes d'exploitation : MS-Office, Linux, Microsoft Windows.

- Langues :
  - Francais : bilingue.
  - Anglais : Bon niveau.
  - Allemand : Niveau débutant.
  - Arabe : Langue maternelle.

Références

Professeur Sylvain Duquesne
- Professeur à l'Université de Rennes 1.
- E-mail :sylvain.duquesne@univ-rennes1.fr

Leila Ben Abdelghani
- Professeur à la faculté des Sciences de Monastir-Tunisie .
- E-mail :leila.benabdelghani@gmail.com