Théorie Algébrique des nombres et applications notamment à la cryptographie

Ecole CIMPA-ICTP, Abidjan 2017

Dates : du 10 avril au samedi 22 avril 2017

Lieu : UFR MI - Université Félix Houphouët Boigny

Planning de l'école

Première semaine (Lieu UFRMI sauf mention contraire).

Lundi 10 avril.

Cérémonie d'ouverture

10:00 - 10:20	Accueil et mise en place des invités et des participants.
10:20 - 10:30	Mot de bienvenue et de remerciements du Président du Comité d'organisation : Dr. François TANOE.
10:30 - 10:40	Allocution de M. le Directeur du Laboratoire de Mathématiques Fondamentales: Pr. Edmond FEDIDA.
10:40 - 10:50	Allocution du représentant de l'ICTP : Pr. Francesco Pappalardi.
10:50 - 11:00	Allocution du représentant du CIMPA, porte-parole des conférenciers extérieurs : Pr. Sylvain Duquesne.
11:00 - 11:10	Allocution de Monsieur le Doyen de l'UFRMI : Pr. ADJE Assohoun.
11:10 - 11:20	Allocution de M. BEUGRE MAMBE, Gouverneur du District d'Abidjan.
11:20 - 11:30	Allocution de Son Excellence, Monsieur le Ministre Auprès du Président de la République, Chargé de la Défense : M. Alain Richard DONWAHI.
11:30 - 11:40	Allocution de Monsieur le Président de l'Université Félix Houphouet Boigny : Pr. KARAMOKO Abou.
11:40 - 11:50	Allocution, suivie de l'ouverture de l'Ecole de Recherche du CIMPA-ICTP Abidjan 2017, par Son Excellence, Madame la Ministre de l'Enseignement Supérieur et de la Recherche Scientifique : Pr. Bakayoko-Ly Ramata
11:50 - 12:00	**Cocktail**
11:50 - 12:20	**Conférence : « Les besoins actuels en cryptographie » par le Colonel Lucien Blegban N'GUESSAN**

12:20 - 14:00	**Pause déjeuner**	
14:00 - 14:50	Alain Togbe	Application of the elementary number theory to cryptography
14:50 - 15:20	Pause café	
15:20 - 16:10	Francesco Pappalardi	Elementary approach to elliptic curves
16:10 - 17:00	François Tanoé	Décomposition cyclotomiques sur les corps finis

Mardi 11 avril

9:00 - 9:50	Alain Togbe	Application of the elementary number theory to cryptography
10h00 - 10:50	Francesco Pappalardi	Elementary approach to elliptic curves
10:50 - 11:20	Pause café	
11:20 - 12:10	François Tanoé	Décomposition cyclotomiques sur les corps finis
12:10 - 14:00	**Pause déjeuner**	
14:00 - 14:50	Alain Togbe	Application of the elementary number theory to cryptography
14:50 - 15:20	Pause café	
15:20 - 16:10	Francesco Pappalardi	Elementary approach to elliptic curves
16:10 - 17:00	François Tanoé	Décomposition cyclotomiques sur les corps finis

Mercredi 12 avril

9:00 - 9:50	Alain Togbe	Application of the elementary number theory to cryptography
10h00 - 10:50	Francesco Pappalardi	Elementary approach to elliptic curves

10:50 - 11:20	Pause café	
11:20 - 12:10	François Tanoé	Décomposition cyclotomiques sur les corps finis
12:10 - 14:00	**Pause déjeuner**	
14:00 - 17:00		**Visite ESATIC**
14h30 - 15:20	Conférence 2 : Prosper Kouadio KIMOU	Cryptographie et sécurité du signal et/ou de l'information
15:20 - 15:30	Pause café	

Jeudi 13 avril

9:00 - 9:50	Alain Togbe	Application of the elementary number theory to cryptography
10h00 - 10:50	Francesco Pappalardi	Elementary approach to elliptic curves
10:50 - 11:20	Pause café	
11:20 - 12:10	François Tanoé	Décomposition cyclotomiques sur les corps finis
12:10 - 14:00	**Pause déjeuner**	
14:00 - 14:50	Alain Togbe	Application of the elementary number theory to cryptography
14:50 - 15:20	Pause café	
15:20 - 16:10	Francesco Pappalardi	Elementary approach to elliptic curves
16:10 - 17:00	François Tanoé	Décomposition cyclotomiques sur les corps finis

Vendredi 14 avril

9:00 - 9:50	Alain Togbe	Application of the elementary number theory to cryptography
10h00 - 10:50	Francesco Pappalardi	Elementary approach to elliptic curves
10:50 - 11:20	Pause café	
11:20 - 12:10	Sylvain Duquesne	Calcul d'indice sur les corps finis et applications aux couplages pour la cryptographie
12:10 - 14:00	**Pause déjeuner**	
14:00 - 14:50	Adriana Salerno	Lattices and cryptography
14:50 - 15:20	Pause café	
15:20 - 16:10	Christophe Delaunay	TD PARI/GP
16:10 - 17:00	Christophe Delaunay	TD PARI/GP

samedi 15 avril

9:00 - 17:00	**Excursion à Yamoussoukro 11h30 – 12h15 Conférence : « *Introduction à la Cryptographie* » par Christophe Delaunay, Université de Franche-Comté (Besançon, France)**

Deuxième semaine (Lieu UFRMI sauf mention contraire).

Lundi 17 avril.

9:00 - 9:50		
10h00 - 10:50	Abé Sézare Gnagne	Décomposition des Fractions Egyptienne et tests de Primalité
10:50 - 11:20	Pause café	
11:20 - 12:10	Conférence 1 : Kolo Fousseni SORO	Tableaux de Young et Cryptographie
12:10 - 14:00	**Pause déjeuner**	
14:00 - 14:50	Michel Waldschmidt	Application of the elementary number theory to cryptography
14:50 - 15:20	Pause café	
15:20 - 16:10	Adriana Salerno	Lattices and cryptography
16:10 - 17:00	Michel Waldschmidt	Application of the elementary number theory to cryptography

Mardi 18 avril

9:00 - 9:50	Michel Waldschmidt	Introduction to topics of algebraic number theory related to cryptography
10h00 - 10:50	Adriana Salerno	Lattices and cryptography
10:50 - 11:20	Pause café	
11:20 - 12:10	Michel Waldschmidt	Introduction to topics of algebraic number theory related to cryptography
12:10 - 14:00	**Pause déjeuner**	
14:00 - 14:50	Adriana Salerno	Lattices and cryptography
14:50 - 15:20	Pause café	
15:20 - 16:10	Christophe Delaunay	TD PARI/GP
16:10 - 17:00	Christophe Delaunay	TD PARI/GP

Mercredi 19 avril

9:00 - 9:50	Michel Waldschmidt	Introduction to topics of algebraic number theory related to cryptography
10:00 - 10:50	Adriana Salerno	Lattices and cryptography
10:50 - 11:20	Pause café	
11:20 - 12:10	Michel Waldschmidt	Introduction to topics of algebraic number theory related to cryptography
12:10 - 14:00	**Pause déjeuner**	
14:00 - 14:20	O. I. Bado	Démonstration du théorème de Sophie Germain
14:30 - 14:50	S. T. Atamewoue	Hyperstructures and applications to the theory of codes
15:00 - 15:20	K.F. Soro	Tableaux de Young et cryptographie
15:30 - 15:50	S. Varadharajan	Factoring RSA modulus using binary decision diagrams
16:00 - 16:20	H. A. Moufek	Les codes convolutionnels et applications à la cryptographie
16:30 - 16:50	P. S. Sanon	New vector spaces

Jeudi 20 avril

9:00 - 9:20	A. Dossavi-Yoyo	L'extension du *D(±k)-triplet {k ∓1,k,4k ∓1}*
9:30 - 9:50	S. E. Rihane	Les ensembles diophantiens et les nombres de Fibonacci
10:00 - 10:20	J. Odjoumani	Pell factoriangular numbers
10:30 - 10:50	A. Maiga	Fast computation of norm on unramified extension of $\boldsymbol{Q}_p$
10:50 - 11:20	Pause café	
11:20 - 11:40	B. Faye	Extracting a uniform random bit-string over Jacobian of hyperellipic curves of genus 2
11:50 - 12:10	I. Jerrari	On the 2-class field towers of some imaginary quartic number fields of type *(2,2,2)*
12:10 - 14:00	**Pause déjeuner**	
14:00 - 14:50	Christophe Delaunay	TD PARI/GP
14:50 - 15:20	Pause café	
15:20 - 16:10	Christophe Delaunay	TD PARI/GP
16:10 - 17:00	Christophe Delaunay	TD PARI/GP

Vendredi 21 avril

9:00 - 9:50	Adriana Salerno	Lattices and cryptography
10h00 - 10:50	Michel Waldschmidt	Application of the elementary number theory to cryptography
10:50 - 11:20	Pause café	
11:20 - 12:10	Adriana Salerno	Lattices and cryptography
12:10 - 14:00	**Pause déjeuner**	
14:00 - 16:00	**Cérémonie de clôture**	

Samedi 22 avril

9:00 - 12:10	**Retour**
12:10 - 14:00	**Pause déjeuner**
14:00 - 17:00	**Retour**