Algebra, Arithmetic and Applications

Ecole Normale Supérieure, Libreville

march 13 - 28, 2020

Organizing Committee

- Obame Nguema Maurice Saint-Clair (chair of the organizing committee),
  Ecole Normale Supérieure de Libreville, Gabon
  Head of the Department of mathematics
  obame_maurice@yahoo.fr

- Tony Ezome
  Université de Sciences et Techniques de Masuku, Franceville, Gabon
  latonyo2000@yahoo.fr

- Christian Maire
  Université de Franche-Comté, France
  christian.maire@univ-fcomte.fr

https://www.prema-a.org/agenta/

African Senior Mathematicians Support

Professor Basile Guy Richard Bossoto
Université Marien Ngouabi de Brazzaville, Congo
Doyen de la Faculté des Sciences

Professor Celestin Nkuimi Celestion
Université Yaoundé 1, Cameroun

Professor Idrissa Kabore
Université Nazi Boni
Directeur Général de la Recherche et des Innovations du Burkina Faso

Professor Philibert Nang
ENS Libreville, Gabon

Professor Achile Ntyam
Université de Ngaoundere, Cameroun

Professor Djiby Sow
Université Cheikh Anta Diop de Dakar, Sénégal

Professor Ralph Twum
University of Ghana Legon

International day of maths - March 14, 2020

https://www.idm314.org/

The two days will take place in the *Institut Français au Gabon*, Amphitheater J.-L. Barrault, https://www.institutfrancais-gabon.com/

—— Friday, March 13 2020 ——

9am - 9:20	Welcome
9:20 - 09:30	Open Session by Pr. Guy Martial NKIET
	Coffee Break
10:00 - 10:30	Pr. Guy Martial NKIET
10:30 - 11:00	Pr. Philibert NANG
11:00 - 11:30	Pr. Octave MOUTSINGA
11:30 - 11:45	Dr. Neil-Yohan MUSADJI
11:45 - 12:00	M. Henri BOUITYVOUBOU

—— Saturday, March 14 2020 ——

9:00 - 9:20	Pr. Ousmane KONFE
9:20 - 9:40	Pr. Armel ANDAMI OVONO
9:40 - 10:00	Dr. Marthe BETOUE
	Coffee Break
10:20 - 10:40	Dr. Mohamed Ali IPOPA
10:40 - 11:00	Dr. Brice DOUMBE
11:00 - 11:20	Dr. Saint-Clair OBAME
11:20 - 11: 40	
11:40 - 12:10	Pr. Christian MAIRE
12:10 - 12:30	Movie about mathematics
12:30	Final Session by Pr. Guy Martial NKIET

Schedule

day	9-10:15am	10:45-12am	2-3:15pm	3:45-5pm
march 17	Pr. Nang	CM1	MBE	discussions
march 18	CM1	TE	MBE	discussions
march 19	CM1	TE	MBE	discussions
march 20	CM1	TE	MBE	discussions
march 21	CM1	TE	–	–
march 22	–	–	–	–
march 23	CM2	AQM	YRL	YRL
march 24	CM2	AQM	PR	PR
march 25	CM2	AQM	PR	PR
march 26	CM2	AQM	AQM	PR
march 27	CM2	AQM	CM2	AQM

A PREMA women in Maths meeting will take place on March 22.

MBE: Marthe Betoue Etoughe, Ecole Normale Supérieure, Libreville, Gabon
Advanced course in complex analysis

TE: Tony Ezome, University of Masuku Franceville, Gabon
Geometry of tangents to cubics and their parameterizations

CM1: Christian Maire, University of Franche-Comté, France
Linear representations of finite groups

CM2: Christian Maire
Introduction to class field theory

AQM: Anne Quéguiner Mathieu, University Paris 13, France
Algebraic theory of quadratic forms - Towards Milnor's conjecture

PR: projects

YRL: young researchers lectures

Participants

BARRY Demba, Univ. des Sci. Techniques et des Technologies de Bamako, Mali
barry.demba@gmail.com

BETOUE ETOUGH Marthe, Ecole Normale Supérieure, Libreville, Gabon

BOUNDOU Fruit, Ecole Normale Supérieure, Libreville, Gabon
fruithorne@gmail.com

DIOP Soda, University Cheikh Anta Diop de Dakar, Sénégal
sodettes@gmail.com

EZOME Tony, University of Masuku, Franceville, Gabon
tony.ezome@gmail.com

IBARA NGIZA MFUMU Roslan, University Marien Ngouabi, Brazaville, Congo
roslancello7@gmail.com

MAIRE Christian, University of Franche-Comté, France
christian.maire@univ-fcomte.fr

MEMIAGHE LENGA Fermi Adrien, Ecole Normale Supérieure, Libreville, Gabon
fermiadrien@gmail.com

MIAYOKA Brice, University Marien Ngouabi, Brazaville, Congo
bricemiayoka@gmail.com

MOUSSAVOU Lydia, Ecole Normale Supérieure, Libreville, Gabon
moussavoulydia945@gmail.com

NANG Philibert, Ecole Normale Supérieure, Libreville, Gabon

PECHA Amina, University of Maroua, Cameroon
Aminap2001@yahoo.fr

PONCHO-KOTEY Ephraim Nii Amon, University of Ghana, Ghana
Ephraim.poncho@aims.ac.rw

QUEGUINER-MATHIEU Anne, University Paris 13, France
queguin@math.univ-paris13.fr

SAINT-CLAIR Obame Nguema Maurice, Ecole Normale Supérieure, Libreville, Gabon
obame_maurice@yahoo.fr

SANKARA Karim, University Nazi Boni, Burkina Faso
sankara86@yahoo.fr

Projects

student	subject	supervisor	local manager
F. Boundou	Théorie de Galois finie et infinie	C. Maire	T. Ezome
R. Ibara	Symboles de Hilbert - Principe de Hasse	C. Maire	Pr. Bossoto Dr. Mialebama
A. Memiaghe Lenga	Quotient de Herbrand - Applications	C. Maire	T. Ezome
B. Miyaoka	Isogeny based cryptography and SEA algorithm	T. Ezome	Pr. Bossoto Dr. Badindamana
L. Moussavou	Produits de groupes et suites exactes	A. Quéguiner	T. Ezome
E. Poncho-Kotey	Complex multiplication for curves with genus g=1,2,3.	T. Ezome	Pr. Twum
K. Sankara	Geometry of flex tangents to a cubic curve	T. Ezome	Pr. Kabore

Local managers

Professor Fouotsa, *emmanuelfouotsa@yahoo.fr*

Doctor Babindamana, *regis.babindamana@yahoo.fr*

Doctor Mialebama, *mialebama@aims.ac.za*

Young researchers lectures

Demba Barry, Univ. des Sci. Techniques et des Technologies de Bamako, Mali
Automorphismes extérieurs et rationalité des groupes adjoints de type **A**

(Cet exposé est basé sur un travail en commun avec J.-P. Tignol.) Soit G un groupe classique de type **D** sur un corps k de caractéristique différente de 2. La première partie de l'exposé consiste Ãă montrer l'existence d'une extension régulière R de k sur laquelle G admet des automorphismes extérieurs. Dans la seconde partie, en utilisant ce résultat et une technique de construction des groupes de type **A** à partir des groupes de type **D**, des nouveaux exemples de groupes de type **A** qui ne sont pas R-triviaux (donc non-rationnels) seront donnés.

Soda Diop, University Cheikh Anta Diop de Dakar, Sénégal
On the computation of minimal free resolutionswith integer coefficients
Supervisor: Pr. Djiby Sow

Let $I = \langle f_1, \ldots, f_s \rangle$ be an ideal of $R = \mathbb{Z}[x_1, \ldots, x_n]$. We introduce the concept of $\mathbb{Z}-$ideal $\mathbb{Z}(I)$ of I which is a proper ideal of R and we propose a technique for computing a weak Gröbner basis for $\mathbb{Z}(I)$. This result is central and leads to the computation of a minimal free resolution for $\mathbb{Z}(I)$ as an $R-$module.

Aminatou Pecha, University of Maroua, Cameroon
Fault injection attacks on Pairing-based Cryptography
Supervisors: Prof. Celestin Nkuimi (Cameroon) and Prof. Nadia El Mrabet (France)

Fault injection attacks are active attacks which focus on deliberately injecting faults and observing the erroneous outputs. These attacks have proved to be a powerful technique allowing to retrieve the secret key with a very small number of experiments. In the literature, many attacks exist against almost all known ciphers like AES, DES, RSA, ECC and Pairing-based cryptography. In this talk, we will restrict our attention to fault injection attacks on pairing based cryptography. Many fault attacks have been developed against Tate-like pairings which their computations require two stages: Miller loop followed by the final exponentiation. Majority of them concentrated upon fault attack on Miller loop. Although the final exponentiation can be considered as an efficient countermeasure against the fault attack on the Miller loop; Lashermes et al. developed a fault attack on Tate pairing in order to reverse the final exponentiation. The aims of this talk is to present work covering fault attacks on pairing especially those that focus on the final exponentiation.

Sponsors

ENS Libreville	
PREMA	http://www.prema-a.org/
CIMPA	https://www.cimpa.info/
ICTP	https://www.ictp.it/
ANR FLAIR Project	http://anrflair.math.cnrs.fr/
SARIMA	http://sarima.edu-math.org/
Institut Français du Gabon	https://www.institutfrancais-gabon.com/
Graduate School EIPHI-BFC	http://gradschool.eiphi.univ-bfc.fr/
USTM	http://univ-masuku.org/
University of Franche-Comté	http://www.univ-fcomte.fr/
FEMTO-ST Institute	https://www.femto-st.fr/fr
LAGA University Paris 13	https://www.math.univ-paris13.fr/laga/

March 10, 2020