Announcement of a certifiable doctoral training activity

Title of activity

Introduction to lattices and their applications in Computer Science/Cryptography - Seminar

For primary research field:

Computer Science and Computer Engineering

Open for other fields:

no

Activity's type:

Seminar

Course category:

Category 1/2
(Cat. 1 =Scientific competences, related to research topic, Cat. 2 =inter/cross-disciplinary research-competences)

The assignment of a course to categories 1 or 2 depends on the research topic of the PhD candidate. It is proposed by the candidate upon registration in agreement with the supervisor. The final decision on the ECTS validation lies with the Programme Committee after the completion of the course.

Mandatory:	*no*		
Language :	*English*		
Speaker(s)/Teacher(s) :	Rajeev Sahu	**Email-address**	rajeev.sahu@uni.lu
Responsible UL	Rajeev Sahu	**Email-address**	rajeev.sahu@uni.lu
Certifier UL:	Rajeev Sahu	**Email-address**	
Date, time, semester, frequency:	- ***Fr 24 May*** *10:00 - 13:00 (intro session) -* ***Mo 03 June*** *9:00 - 13:00 -* ***Wed 05 June*** *9:00 - 13:00* - ***Fr 07 June*** *9:00 - 13:00 + 14:00 - 16:00 -* ***Wed 12 June*** *9:00 - 13:00 -* ***Fr 14 June*** *9:00 - 13:00 + 14:00 - 16:00*		
Location:	*Campus Belval, Maison du Nombre, room MNO 1.050*		

Description of the course/module:

After an introduction session to lattices, the participants of the seminar will be asked to prepare a 60-90 minutes talk about a concrete problem in computer science/cryptography to which lattices can be applied followed by 20 minutes discussion.
Details: On the 24.05.2019 there will be a 3 hours introduction session about lattices during which we will define lattices, prove their basic properties, develop some algorithms and enumerate some applications and open problems. At the end of the session, the participants will be asked to choose one topic from the given list or another related topic to give a talk about. Then the schedule will be fixed. After the introduction session, the participants have (at least) one week to prepare their talks (depending on the fixed schedule). From the 03.06.2019 to 14.06.2019 the seminar will take place as given above. Each participant has a 2h slot for his/her presentation (60-90 min talk + 20 min questions and comments).

Learning outcomes/ learning objectives:

At the end of the seminar, the participants will know the definition of lattices, their basic theoretical results and they will be able to manipulate them. Furthermore, the participants should have gained a broad knowledge of applications of lattices, as well as how they are used in modern computer science/cryptography. At last, each participant should be able to use the key concepts and lattice reduction method seen in the talks for their own research projects.

Workload:

Each participant needs to prepare a 60-90 minutes talk with a 20 minutes question session at the end.
To prepare the talks, a preparatory workload (off-course workload) of 15 hours will be taken into consideration.

Type of Evaluation:	**Max. number of participants:**
Exam, oral	*12*

Admission criteria: *(if applicable)*

Participants should have a strong knowledge of linear algebra (vector fields, norms, Gram-Schmidt,...). Furthermore, the basic notions of abstract algebra (groups, finite fields, polynomial rings) will be required, as well as the definitions of algorithms and notions of complexity theory. As several talks will rely on cryptographic schemes the participants should be aware of the basic notions of public key encryption.

Remarks:

This seminar can be seen as an introduction to lattices and their applications and might be repeated as an advanced course next semester.

The admission does not require any preliminary knowledge about lattices or any specific problems in computer science/cryptography. In particular, the talks will be targeted to a non-specialized public and will introduce the problems that should be solved using lattices. However, any preliminary knowledge of the topics will be an advantage.

Non-participants of the seminar might attend the talks to widen their knowledge about lattices, their applications and related problems.

This seminar is supported by the Luxembourg National Research Fund through grant PRIDE15/10621687/SPsquared.

Multiple Validation possible: *(for course series)* No [X] Yes, how often: [ ] **times**

Registration: *To guarantee ECTS validation for the course, PhD candidates have to register additionally on Moodle. This registration is independent from any other registration/enrollment procedure.*

The DSSE is validating this doctoral training activity: No [ ] Yes, approv. ECTS: *2*

Additional comments: