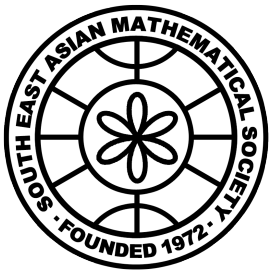

SOUTH EAST ASIAN MATHEMATICAL SOCIETY

FINAL REPORT

Number Theory and Applications in Cryptography and Coding Theory

University of Science, 227 Nguyen Van Cu,
District 5, Ho Chi Minh, Vietnam
August 31 - September 08, 2015

Organized by

University of Science, Vietnam National University-HCMC

with the support of

SEAMS, CIMPA, IMU, HO CHI MINH CITY UNIVERSITY OF SCIENCE, ICTP, CONSULATE GENERAL OF ITALY IN HO CHI MINH CITY , ISP

2015

Number Theory and Applications in Cryptography and Coding Theory

August 31 - September 08, 2015,
University of Science, 227 Nguyen Van Cu,
District 5, Ho Chi Minh, Vietnam

I. Summary

The SEAMS School "Number Theory and Applications in Cryptography and Coding Theory" is organized by University of Science (HCMUS), Vietnam National University at Ho Chi Minh City (VNU-HCMC) and the Southeast Asian Mathematical Society (SEAMS). It was held at University of Science, VNU-HCMC from August 31 to September 08 of 2015.

There are six Vietnamese lecturers (one from Hue, three from Ho Chi Minh, one from Germany and one from Finland) and two European speakers, one from France and one from Italy. There are 74 participants including 32 Vietnamese (2 from Da Lat, 2 from Dong Nai, 11 from Hanoi and 17 from Ho Chi Minh) and 34 international participants from Nepal (11), Thailand (7), Indonesia (6), Philippine (5), Cambodia (3) and Malaysia (2).

The School obtained generous supports from SEAMS-CIMPA, HCMUS, International Mathematical Union (IMU), International Centre for Theoretical Physics (ICTP), Number Theory Foundation (NTF), Consulate General of Italy in Ho Chi Minh and International Science Programme (ISP).

The school started on August 31. The opening ceremony took place on the morning of the second day including speeches given by the General Consul of France in HCMC, Emmanuel Ly-Batallan, and by the Consul General of Italy in HCMC, Carlotta Colli. There is a small symposium on the second Monday afternoon in which there are ten contributed talks from participants. The School ended on September 08 with a short closing ceremony and participants were given the certificates of attendance.

II. Scientific Objectives and Rationale for the School

The SEAMS School “Number Theory and Applications in Cryptography and Coding Theory” introduces fundamental notions of Number Theory, Cryptography and Coding Theory. It is addressed to advanced undergraduate and graduate students and young researchers from south east Asian countries. It provides them with some of the knowledge necessary to further study and research. Another important aim of the school is to provide a good preparation for the future CIMPA school in Lattices and Applications in Cryptography and Coding Theory which will be held in Ho Chi Minh during the summer of 2016. The program of each single course has been discussed with the organizers of the 2016 event.

The School was held at University of Science, VNU-HCMC, at Ho Chi Minh City from August 31 to September 8 of 2015.

III. Organizers and Lecturers

Lecturers

- Dung H. Duong, University of Bielefeld, Germany.
- Khuong A. Nguyen, Ho Chi Minh city University of Technology, Vietnam.
- Thuc D. Nguyen, Ho Chi Minh city University of Science, Vietnam.
- Francesco Pappalardi, University of Roma Tre, Italy.
- Ha Tran, Aalto University School of Science, Finland.
- Long D. Tran, Ho Chi Minh city University of Science, Vietnam.
- Thu D. Tran, Ho Chi Minh city University of Science, Vietnam.
- Michel Waldschmidt, University of Paris 6, France.

Organizers

- Dung H. Duong, University of Bielefeld, Germany.
- Khuong A. Nguyen, Ho Chi Minh city University of Technology, Vietnam.
- Thuc D. Nguyen, Ho Chi Minh city University of Science, Vietnam.
- Ha Tran, Aalto University School of Science, Finland.

IV. The Participants

Cambodia

- Mam Mareth, Royal University Of Phnom Penh
- Say Ol, University Of The Philippine Diliman
- Sok Lin, Royal University Of Phnom Penh

Indonesia

- Defita, Bandung Institute Of Technology
- Ni Luh Dewi Sintiari, Ganesha University Of Education
- Ricky Aditya, Bina Nusantara University
- I Gede Adhitya Wisnu Wardhana, Institut Teknologi Bandung
- Intan Nisfulaila, Universitas Islam Negeri Maulana Malik Ibrahim Malang
- Muhammad Zaki Riyanto, Universitas Islam Negeri (UIN) Sunan Kalijaga

Malaysia

- Amizah Malip, University Of Malaya
- Chew Chun Yong, Universiti Tunku Abdul Rahman

Nepal

- Kedar Nath Uprety, Tribhuvan University
- Prakash Muni Bajracharya, Tribhuvan University
- Ajaya Singh, Tribhuvan University
- Bishnu Hari Subedi, Tribhuvan University
- Dhan Kumari Thapa, Tribhuvan University
- Ramesh Gautam, Tribhuvan University
- Bhadra Man Tuladhar, Kathmandu University
- Kanhaiya Jha, Kathmandu University
- Sharada Shrestha, Tribhuvan Univeristy
- Anjana Pokhrel, Tribhuvan University
- Abatar Subedi, Tribhuvan University

Philippines

- Eric Anthony Arances, University Of The Philippines Diliman
- Vonn Kee G. Wong, University Of The Philippines Diliman

- Charles Repizo, Ateneo De Manila University
- Jane D. Palacio, University Of The Philippines Los Baños
- Odessa D. Consorte, University of the Philippines Diliman

Thailand

- Jareena Tharnnukhroh, Silpakorn University
- Atsanon Wadsanthat, Mahidol University
- Fongchan Wannalookkhe, Khonkaen University
- Sawian Jaidee, KhonKaen University
- Siripong Sirisuk, Chulalongkorn University
- Tanadon Chaobankoh, Chiang Mai University
- Arunwan Bonipan, Chulalongkorn University

Vietnam

- Hoang Nguyen Thuy Ngan, DaLat University
- Phạm Minh Quý, DaLat University
- Trương Hữu Dũng, Dong Nai University
- Vo Quoc Bao,, Dong Nai University
- Le Huy Hung, Hanoi University of Science
- Mạc Đăng Trường, Hanoi University of Science
- Nguyen Tuan Anh, Hanoi University of Science
- Nguyen Thi Thanh Yen, Hanoi University of Science
- Trieu Quang Phong, Hanoi University of Science
- Đỗ Xuân Thành, Military Institute of Information Technology
- Nguyen Tien Tai, Hanoi University of Science
- Nguyen Hai Vinh, Hanoi University of Science
- Nguyen Quoc Toan, Institute of Cryptography Science and Technology, Vietnam Government Information Security Commission.

- Vo Tung Linh, Institute of Cryptography Science and Technology, Vietnam Government Information Security Commission.
- Le Minh Ha, Hanoi University of Science
- Võ Lê Quỳnh Như, HCMC University of Science
- Le Thi Thanh Huong, Ernst Thalmann Highschool
- Ngo Thi Bao Tram, HCMC University of Pedagogy
- Tran Tu Trinh, HCMC University of Pedagogy
- Ho Ngoc Tram, HCMC University of Pedagogy
- Trinh Thi Kim Phuong, HCMC University of Pedagogy
- Tran Hieu Nghia, HCMC Pre-University College
- Dang Tuan Thuong, HCMC University of Science
- Trần Quang Huy, HCMC University of Science
- Trương Lê Minh Nhựt, HCMC University of Science
- Trang Trọng Thức, HCMC University of Science
- Nguyễn Phan Mạnh Hùng, HCMC University of Science
- Tran Van Tuan, HCMC University of Pedagogy
- Le Quoc Huy, Ernst Thalmann Highschool
- Nguyễn Anh Tuấn, HCMC University of Science
- Le Van Tan, HCMC University of Pedagogy
- Nguyen Thi Ngoc Thu, HCMC University of Pedagogy

.

V. School Programs

The school introduces fundamental notions in Number Theory, Cryptography and Coding Theory. This will be a good preparation for the future CIMPA school on Lattices and Applications in Cryptography and Coding Theory which will be held in Ho Chi Minh in Summer 2016. This school will stimulate a good research atmosphere in Vietnam in general and in South Vietnam in particular where Cryptography and Coding Theory is not yet well studied. This school also provide excellent opportunity for students to meet outstanding researchers/speakers from other countries. This school also introduces new and further research directions as well as provide great chance to create good research network.

There are four courses in the school including Elliptic Curves Cryptography, Introduction to Coding Theory, RSA and its variants, Number Theory and Lattices. The information of courses including lecturers are as the following.

M1. Elliptic Curve Cryptography, Francesco Pappalardi.
Abstract: We will first recall the fundamental aspects of Algorithmic Elementary Number Theory including the notion of complexity and polynomial time algorithms which will be applied to classical algorithms. Then we will cover the basic theory of Finite fields and we will use it to describe the classical cryptosystems based in the difficulty of the discrete logarithm problem. The last part will be devoted to Elliptic curves and some of their applications to cryptography.

M2. Introduction to Coding Theory, Michel Waldschmidt.
Abstract: The theory of error correcting codes is an essential component of the data transmission process. There are plenty of applications in the real life, including the technology of CD's and DVD's and the transmission of data by satellites. We will define and study the Hamming distance among words of a given length on a finite alphabet. We will introduce the main codes and study their properties. Among the most important codes are the linear ones, where the theory of finite fields can be combined with tools from linear algebra. Cyclic codes are related with cyclotomic polynomials over finite fields, the theory of which will be fully explained.

M3. RSA and its variants, Thuc D. Nguyen, Long D. Tran, Thu D. Tran.
Abstract: Since RSA was first introduced in 1978 by Ron Rivest, Adi Shamir, and Leonard Adleman, development RSA variants have been attracted many authors. We will introduce mathematical structure of RSA and its variants. Topics include: Group, Ring, and field ; RSA and cryptanalysis ; variants of RSA on platforms other Zn ; generic RSA scheme.

M4. Lattices and applications, Ha Tran. Dung H. Duong, Khuong A. Nguyen.

Abstract: We introduce basic definitions and properties of lattices and problems on lattices such as shortest vector problem (SVP), closest vector problem (CVP), etc. as well as LLL algorithm and other algorithms for SVP, CVP. We also introduce how to use lattices in the design of cryptographic schemes.

The school starts from Monday, August 31, 2015 untill Tuesday, September 08, 2015. The school includes 31.5 hours for lectures and 10.5 hours for group discussion. Everyday, there are 5.5 hours for lectures and 1.5 hour for group discussion. The lessons will daily last from 8:30 to 11:45 in the morning and 13:30 to 18:00 in the afternoon. The tentative schedules are the following.

HOUR	MON AUG 31	TUE SEP 01	WED SEP 02	THU SEP 03
8:30 – 10:00	REGISTRATION	OPENNING CEREMONY	HOLIDAY	M1
10:00 – 10:15				BREAK
10:15 – 11:45	M1	M2		M2
11:45 – 13:30	LUNCH	LUNCH		LUNCH
13:30 – 15:00	M4	M4		M4
15:00 – 15:15	BREAK	BREAK		BREAK
15:15 – 16:15	M3	M3		M3
16:15 – 16:30	BREAK	BREAK		BREAK
16:30 – 18:00	GROUP DISCUSSION	GROUP DISCUSSION		GROUP DISCUSSION

HOUR	FRI SEP 04	SAT SEP 05	SUN SEP 06	MON SEP 07	TUE SEP 08
8:30 – 10:00	M1			M1	M1
10:00 – 10:15	BREAK			BREAK	BREAK
10:15 – 11:45	M2			M2	M2
11:45 – 13:30	LUNCH			LUNCH	LUNCH
13:30 – 15:00	M4			M4	M4
15:00 – 15:15	BREAK			BREAK	BREAK
15:15 – 16:15	M3			M3	M3
16:15 – 16:30	BREAK			BREAK	CLOSING CEREMONY
16:30 – 18:00	GROUP DISCUSSION			GROUP DISCUSSION	

Conclusion

This SEAMS school had several positive side effects:

- This was the first academic school in the area of Mathematics, Cryptography and Coding Theory happening in Ho Chi Minh which introduce and encourage students both in mathematics and computer science to follow this fascinating research areas. It also gave chance for Vietnamese and international participants to make friends and work together in group discussion from which some future collaboration may occur.

- The School is related with support from IMU to 11 Nepalese mathematicians to attend which allow them to regroup and make plans from moving forward, as well as sharing the needs of the Nepalese math community with their colleagues from other countries within the region. This contributed to connect mathematicians from Nepal with mathematicians from Vietnam and neighboring countries and to help them to make plans for support and regional projects after the earthquake that hat hit Nepal recently.

- The School has been the opportunity for Vietnamese Mathematicians and Computer Scientists from Hanoi and Ho Chi Minh to have useful exchanges involving future program of cooperation.

- The School has attracted several young mathematicians working in the area of Algebra in Ho Chi Minh city. They all obtained their Ph.Ds from abroad mostly from European countries. They together with two Vietnamese organizers (Dung H. Duong and Ha Tran) have start up a study group learning about Cryptography (called SaigonCrypt). A weekly seminar is held in HCMUS and there are several master students attending and deciding to do their thesis in this area. This will be the first step for build up a research group working in cryptography in near future.

- A proposal on future SEAMS School “Cryptography: Foundations and New Directions” has been submitted which, if accepted, will be held at Vietnam Institute for Advanced Study in Mathematics (VIASM) in Hanoi from November 24 – December 02 of 2016 which is aimed as a good preparation for AsiaCrypt 2016 happening in the week after in Hanoi.

In conclusion, the School has been happening successfully and we hope this will enable many such events in the area of Mathematical Cryptography and Coding Theory in the region. We would like to thank all supporters for their generous supports and we hope they will continue support us in near future for the development of mathematics in Vietnam and Southeast

Financial Report

SEAMS-CIMPA	EURO	8000
UNIVERSITY OF SCIENCE	EURO	2400
NTF	EURO	909
IMU	EURO	1500
ISP	EURO	545
ICTP	EURO	1000
IMU FOR NEPAL (IMUN)	EURO	10000

Contributed talks by participants

1. Atsanon Wadsanthat, On Dynamics of Quadratic Systems over Finite Fields
2. Arunwan Boripan, Self-Conjugate-Reciprocal Irreducible Monic Polynomials over Finite Fields.
3. Kanhaiya Jha, Robustness Analysis of Zero-Knowledge Proof
4. Say OL, Constructions of Cheating-Immune Secret Sharing Schemes
5. Siripong Sirisuk, M-primary submodules
6. Adhitya Wisnu Wardhana, On almost prime submodules
7. Dang Tuan Thuong, Weil pairings and applications.
8. Charles Repizo, On **k**-Orthogonal Matrices Over Finite Local Rings.
9. Ricky Aditya, Algebraic Geometric Construction of Convolutional Goppa Codes.
10. Zaki Riyanto, Key Exchange Protocols based on non-commutative groups