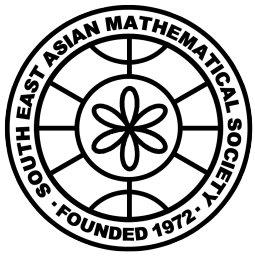

SOUTH EAST ASIAN MATHEMATICAL SOCIETY

SEAMS SCHOOL PROPOSAL

Cryptography : Foundations and New Directions

Hanoi, Vietnam

November 24 – December 02, 2016

Organized by

Vietnam Institute for Advanced Study in Mathematics (VIASM)

and

Hanoi University of Science, Vietnam National University (VNU-HUS)

2016

SEAMS SCHOOL PROPOSAL

1. The proposed title, place and dates of the SEAMS School

Title of the SEAMS School	:	Cryptography: Foundations and New Directions
Place	:	Vietnam Institute for Advanced Study in Mathematics
Dates	:	November 24 – December 02, 2016

2. Organizers (write the names, place of work, and email address, if you have more than two then add the necessary lines)

1. Name		**Nguyen Huu Du**
Institution		VIASM, Vietnam
Email and Phone		NHDU@VIASM.EDU.VN +84 4 36 23 15 30
2. Name	:	**Phan Duong Hieu**
Institution	:	University of Limonges, France
Email and Phone	:	DUONG-HIEU.PHAN@UNILIM.FR +33 587506803
3. Name	:	**Le Minh Ha**
Institution	:	Hanoi University of Science, VNU-Hanoi, Vietnam
Email and Phone	:	MINHHA@VNU.EDU.VN +84 4 38581135
4. Name		**Duong Hoang Dung**
Institution		Kyushu University, Japan
Email and Phone		DUONG@MATH.KYUSHU-U.AC.JP +81 92 802 4425
5. Name		**Ha Tran**
Institution		Aalto University, Finland
Email and Phone		HATRAN1104@GMAIL.COM +358504316172

3. Short Description of the **Scientific Content**, the **Aim** of the proposed school and the potential **Impact** to the local academic system and/or society. (max 100 words)

Cryptography is a young but very active field which has important applications in practice and raise interesting open problems in mathematics and computer science. In 2016, we will organize ASIACRYP - the most important conference in cryptology in Asia and it will be an opportunity to promote research for the local people. It will be thus primordial to prepare solid background for the local people to attend and discuss research with world-class researchers. For this aim, we would like to organize this SEAMS School right before the AsiaCrypt with the lectures will be given by leading experts in relevant topics of cryptography. The school is addressed to advanced undergraduate and master students in Southeast Asia Countries.

4. The speakers of the school (name, address, email, male/female). Give the percentage of female speakers.

There are 6 **confirmed** speakers including 2 female speakers which is overall 33.33% of total.

1. **Phan Thi Ha Duong**, Vietnam Institute of Mathematics, PHANHADUONG@MATH.AC.VN, female
2. **David Pointcheval**, École Normale Supérieure, Paris, France, DAVID.POINTCHEVAL@ENS.FR, male
3. **Tanja Lange**, Eindhoven University of Technology, The Netherlands, TANJA@HYPERELLIPTIC.ORG , female
4. **Daniel J. Bernstein**, Eindhoven University of Technology, The Netherlands, DJB@CR.YP.TO, male
5. **Phong Q. Nguyen**, Japanese-French Laboratory for Informatics, Japan, PHONG.NGUYEN@ENS.FR , male
6. **Neal Koblitz**, University of Washington, Seattle, USA, KOBLITZ@MATH.WASHINGTON.EDU, male

5. Describe in a few lines the local institution related to this school, including the main academic program and its strengths in teaching program and research. Give also the internet site of the local institutions. Do you plan to have a website of this SEAMS school?

1. VIASM: Vietnam Institute for Advanced Study in Mathematics

VIASM is the main institution in implementing the National Program for the Development of Mathematics from 2010 to 2020 (NPDM). This program is responsible for encouraging young students to learn mathematics, improving the quality of teaching and learning mathematics at school and university level as well as dissemination of scientific knowledge to the public.

The main activity of the Institute is organizing research groups to conduct research programs and projects of high quality. Scientists in the same field will gather and work

together at the Institute in short-term basis. It aims to attract Vietnamese mathematicians from abroad and international mathematicians to Vietnam and participate in research and training with their colleagues in Vietnam. This activity will strengthen the research branches which have taken root in Vietnam and will incubate the formation of new branches of Mathematics.

Every year, VIASM offers some Postdoctoral fellowships. These fellowships are intended for mathematicians with Ph.D.s awarded within 5 years. Postdoctoral Fellows must hold a Ph.D. at the time of their proposed residency. The fellowship is for one year and can be extended up to three years. The VIASM will organize conferences, workshops, seminars on topics associated with research groups working at the institute in order to implement their research projects as well as attract new students to do research.

In cooperation with NPDM, the Institute will hold summer schools for math students, short-term training courses for mathematics teachers and organize other activities to disseminate scientific knowledge to the public.

The address of the institution is the following:

The 7th floor, Ta Quang Buu Library, University of Science and Technology, 1 Dai Co Viet Street, Ha Noi, Viet Nam.
Tel: +84 4 3623 1542 - Fax: +84 4 3623 1543
Email: VIASM@VIASM.EDU.VN
Website: HTTP://VIASM.EDU.VN/?LANG=EN

2. Hanoi University of Science, VNU-HUS

VNU University of Science, an integral part of Vietnam National University, Hanoi, ranks among a few universities in Vietnam with long-standing tradition.

VNU University of Science is dedicated to conducting research in basic science and applied. The University is committed to initiating, propagating and promoting science knowledge; providing the society with a constant supply of high-qualified intellectual workers as well as high-quality scientific and technological products; actively contributing to the basic science development of the country.

The Faculty of Mathematics, Mechanics and Informatics offers bachelor, master and PhD programs in mathematics, mechanics and informatics. There are seven departments including Mechanics, Algebra-Geometry-Topology, Analysis, Informatics, Bio-Math, Computational and Applied Mathematics, Probability and Statistics. At the moment, there are 5 professors, 12 associate professors and 36 PhDs.

The address is as the following:

334 Nguyen Trai, Thanh Xuan District, Hanoi, Vietnam
Tel : +84 4 38 58 11 35
Website: HTTP://HUS.VNU.EDU.VN/EN

We will soon set up a website for the School.

6. Provide information on the number and distribution of expected participants. Give the percentage of female participants who will attend the school.

We expect 50 participants of which 30 are from Vietnam and 20 are from other Southeast Asian Countries. We expect at least 30% female participants.

7. Describe the objectives and the program of the proposed school, including the courses (max 5 courses), speakers (in each course), abstracts (8 lines for each course) and tentative schedule of the whole proposed school.

The aim of this Seams School is to introduce some mathematical background of cryptography and some trends in cryptography. This is also a preparation for the follow-up AsiaCrypt 2016 which is held in the same place in the week right after this Seams school.

There are four courses in the school. The titles and abstracts are as the following.

Course M1: Mathematical foundations of cryptography
Lecturers: Phan Thi Ha Duong, Vietnam Institute of Mathematics-Vietnam
Phong Q. Nguyen, Japanese-French Laboratory for Informatics-Japan
Neal Koblitz, University of Washington, Seatle, USA
Abstract : The course is divided into three parts. In the first part, we will introduce some basic of complexity theory such as time, P versus NP, polynomial hierarchy, complexity of counting problems, the average-case and worst-case complexity of problems. In the second part, we will introduce lattices and algorithms on lattices as well as some applications of lattices in cryptography. The last part of the course is devoted for elliptic curve cryptography. In this part, we will short survey some basic of elliptic curves and some results as well as trends in elliptic curve cryptography.

Course M2 : Provable Security for Public-Key Schemes
Lecturer : David Pointcheval
Abstract: In this first lecture, we will explain what provable security means for cryptographic schemes, with concrete simple illustrations on
public-key encryption (one-wayness and semantic security, with RSA and
ElGamal) and signature (unforgeability with RSA). We will also have to
present the computational assumptions that are usually admitted to
hold (Fact, RSA, DL, DH). Then, we will describe the game-based methodology to conduct a security proof, again with simple examples in signature and encryption. Basic security notions for encryption are not enough in some specific applications. We will thus define stronger security notions (IND-CCA), and present some encryption schemes that achieve these security goals, together with formal security proofs (Cramer-Shoup and OAEP). The same holds for signatures. Stronger security notions (EUF-CMA) are required. We will present them together with the forking lemma, that allows to prove the security of a large class of signature schemes.

Course M3: Cryptanalysis of public-key systems
Lecturer: Tanja Lange, Eindhoven University of Technology, The Netherlands

Abstract: All currently used public key cryptography on the Internet and in other applications is related to (one of) two hard problems from number theory: integer factorization and the discrete logarithm problem. To make secure choices for the parameters it is important to understand the strength of attacks and how powerful current computers are. This short course covers the main methods for factorization and
computing discrete logarithms.

Course M4: High-speed cryptography
Lecturer: Daniel J. Bernstein, Eindhoven University of Technology, The Netherlands
Abstract: Large parts of the Internet traffic are still transmitted in clear text, or using cryptosystems that are surprisingly easy to break. The cost of using cryptography at the server and client side (CPU time, latency, power consumption, etc.) is often brought forward as a justification. Is cryptography actually so expensive? Can it be made less expensive? This course will take a close look at cryptographic performance.

The School will start from November 24 to December 02, 2016. The school includes 42 hours for lectures and 10.5 hours for group discussion. Everyday, there will be 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 18:30 in the afternoon. The tentative schedules are the following.

HOUR	THURSDAY NOVEMBER 24	FRIDAY NOVEMBER 25	SATURDAY NOVEMBER 26	SUNDAY NOVEMBER 27	MONDAY NOVEMBER 28
8:30 – 10:00	REGISTRATION	M1			M1
10:00 – 10:15		BREAK			BREAK
10:15 – 11:45	M1	M1			M2
11:45 – 13:30	LUNCH	LUNCH			LUNCH
13:30 – 15:00	M1	M1			M3
15:00 – 15:15	BREAK	BREAK			BREAK
15:15 – 16:45	M1	M1			M4
16:45 – 17:00	BREAK	BREAK			BREAK
17: 00– 18:30	GROUP DISCUSSION	GROUP DISCUSSION			GROUP DISCUSSION

HOUR	TUESDAY NOVEMBER 29	WEDNESDAY NOVEMBER 30	THURSDAY DECEMBER 01	FRIDAY DECEMBER 02
8:30 – 10:00	M1	M1	M1	M1
10:00 – 10:15	BREAK	BREAK	BREAK	BREAK
10:15 – 11:45	M2	M2	M2	M2
11:45 – 13:30	LUNCH	LUNCH	LUNCH	LUNCH

13:30 – 15:00	M3	M3	M3	M3
15:00 – 15:15	BREAK	BREAK	BREAK	BREAK
15:15 – 16:45	M4	M4	M4	M4
16:45 – 17:00	BREAK	BREAK	BREAK	BREAK
17:00 – 18:30	GROUP DISCUSSION	GROUP DISCUSSION	GROUP DISCUSSION	GROUP DISCUSSION

8. Provide information about provisional budget and the expected funding.

Provisional Budget

No	Item	Details	Sources		Total (EUR)
			CIMPA	Others	
1	**Tickets**				**6750**
	Overseas Participants				4750
	Speakers (overseas and local)				2000
2	**Accommodation**				**5500**
	Participants				4500
	Speakers				1000
3	**Food Expenses**				**3180**
4	**Local Transport**				**570**
5	**Supplies and Printings**				**1000**
6	**Living Expenses for overseas participants**				**1000**
7	**Social program (Exursion)**				**1000**
	TOTAL				**19000**

Note: At least 2/3 of **CIMPA support** can be used for travel, accommodation and/or living expenses of young researchers (less than 38 or recent PhD) from neighbouring countries of the activity; at most 1/3 at most can be used for lecturers (economy class travel and/or standard living expenses).
CIMPA support cannot be used for: reimbursements for participants living in developed countries (even if their nationality is from a developing country); registration fees; proceedings; organizational expenses.

Expected Funding

No	Item	Confirmed (Yes/Not Yet)	Total
1	CIMPA	Not yet	5000
2	VIASM	Yes	5000
3	VNU-HUS	Yes	1000
4	IACR: International Association for	Not yet	5000

	Cryptologic Research		
5	NTF: Number Theory Foundation	Not yet	1000
6	IMU: International Mathematical Union	Not yet	1000
7	ICTP: International Center for Theoretical Physics	Not yet	1000
	TOTAL		**19000**

9. Provide CVs for the organizers (**2 pages max** for **each person**, including current publications).