SOUTH EAST ASIAN MATHEMATICAL SOCIETY

SEAMS SCHOOL PROPOSAL

Number Theory and Applications
in Cryptography and Coding Theory

Ho Chi Minh City, Vietnam
August 31 – September 08, 2015

Organized by

University of Science, Vietnam National University-HCMC
2015

SEAMS SCHOOL PROPOSAL

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

Title of the SEAMS School	:	Number Theory and Applications in Cryptography and Coding Theory.
Place	:	University of Science, Vietnam National University-HCMC 227 Nguyen Van Cu, District 5, Ho Chi Minh, Vietnam
Dates	:	August 31 – September 08, 2015

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

1. Name	:	Thuc Nguyen-Dinh
Institution	:	University of Science, Vietnam National University-HCMC
Email and Phone	:	NDTHUC@FIT.HCMUS.EDU.VN +848 903 33 99 44
2. Name	:	Khuong An Nguyen
Institution	:	University of Technology, Vietnam National University-HCMC
Email and Phone	:	NAKHUONG@GMAIL.COM +84 973734678
3. Name	:	Ha Tran
Institution	:	University of Rome "Tor Vergata", Italy
Email and Phone	:	HATRAN1104@GMAIL.COM +393928484759
4. Name	:	Dung H. Duong
Institution	:	University of Bielefeld, Germany
Email and Phone	:	DHOANG@MATH.UNI-BIELEFELD.DE +49 176 763 141 83

3. Short Description of the Scientific Content (max 100 words)

This school is meant to introduce fundamental notions of Number Theory, Cryptography and Coding Theory. Is is addressed to advanced undergraduate and graduate students and young researchers from south east Asian countries. It will provide 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 has been proposed and, if accepted, will be held in Ho Chi Minh during the summer of 2016. The program of each single course has been discussed with the organisers of the 2016 event.

4. The speakers of the school (names, address, emails): 1/8 female speakers.

1. Dung H. Duong, University of Bielefeld, DHOANG@MATH.UNI-BIELEFELD.DE
2. Francesco Parpalardi, University of Rome Tre, PAPPA@MAT.UNIROMA3.IT

3. Ha Tran, University of Rome "Tor Vergata", HATRAN1104@GMAIL.COM
4. Michel Watdschmidt, University P.et M. Curie Paris 6, MICHEL.WALDSCHMIDT@IMJ-PRG.FR
5. Khuong A. Nguyen, Ho Chi Minh University of Technology, NAKHUONG@GMAIL.COM
6. Thuc D. Nguyen, Ho Chi Minh University of Science, NDTHUC@FIT.HCMUS.EDU.VN
7. Thu D. Tran, Ho Chi Minh University of Science, TDTHU@FIT.HCMUS.EDU.VN
8. Long D. Tran, Ho Chi Minh University of Science, TRANDINHLONG1963@YAHOO.COM.VN

5. Describe in a few lines the local institution related to this school, including the main academic program and its strength. Give also the Internet site of the local institutions.

University of Science, Vietnam National University-HCMC is a research university located in District 5, Ho Chi Minh, Vietnam. The University was found as the Southern College of Science in 1941 and renamed as Sai Gon University of Science in 1957. In 1977, it was incorporated in Combined University but it splitted and joined Vietnam National University Ho Chi Minh City. This university is one of 6 leading research university in Vietnam. The university is offering 52 undergraduate programs and 31 postgraduate programs. It has over 9 departments including department of mathematics and department of computer science. Every year, there are 2400 bachelors and 300 masters and PhDs graduate. This university has two campuses in District 5 and Thu Duc District, Ho Chi Minh. The website of the university is : http://www.hcmus.edu.vn/en/index.php . The address for temporary website for the school is: http://www.math.uni-bielefeld.de/~dhoang/seams15/

6. Provide information about the expected participants. The number and the distribution of expected participants.

We expect around 30 undergraduate and master students including 10 participants from other Southeast Asian countries and at least 40% female students.

7. Describe the objectives and the program of the proposed school, including the courses, speakers, abstracts (8 lines each) and tentative schedules for each course.

The school will introduce 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 is requested to 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 theis 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 and 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. Introduction to Algebraic Number Theory and Lattices, Ha Tran. Dung H. Duong, Khuong A. Nguyen.
Abstract : We will cover some basic notions from algebraic number theory such as ring of integers of a number field, ideals and factorisations, class number and class group, lattices and Minkowski's theorem. We also introduce some algorithmic lattice theory such as the LLL algorithms and its applications.

The school will start from Monday, August 31, 2015 till Tuesday, September 08, 2015. The school includes 38.5 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 18:00 in the afternoon. The tentative schedules are the following.

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

HOUR	FRI SEP 06	SAT SEP 07	SUN SEP 08	MON SEP 09	TUE SEP 10
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	BREAK
16:30 – 18:00	GROUP DISCUSSION			GROUP DISCUSSION	GROUP DISCUSSION

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

Provisional Budget:

DESCRIPTION	CURRENCY	AMOUNT
EXPENSE FOR LECTURERS	EURO	3600
AIRLINE TICKETS FOR PARTICIPANTS FORM SOUTHEAST ASIAN COUNTRIES	EURO	3000
LODGING AND LIVING EXPENSES FOR INTERNATIONAL STUDENTS AND VIETNAMESE STUDENTS NON RESIDENT IN HO CHI MINH	EURO	4400
MISCELLANEA : SUPPLIES (PROGRAM, SCHOOL KITS, HANDOUTS, FACILITIES, EQUIPMENT, SECRETARIAT AND LOCAL COMMITTEE EXPENSES.	EURO	1500
TOTAL	EURO	12500

Provisional Expected Funding:

DESCRIPTION	CURRENCY	AMOUNT
SEAMS-CIMPA	EURO	5000
UNIVERSITY OF SCIENCE	EURO	2000
NATIONAL FOUNDATION OF SCIENCE AND TECHNOLOGY	EURO	3000
IMU	EURO	1000
ICTP	EURO	1500

9. Provide CVs for the organizers.

DUNG H. DUONG

CONTACT INFORMATION

Faculty of Mathematics
Bielefeld University
Postfach 100131, 33615 Bielefeld
Germany

+49 521 106 5234
dhoang@math.uni-bielefeld.de
dhdung1309@gmail.com

RESEARCH INTERESTS

Group Theory, Representation Theory and Number Theory.

Division rings, Coding Theory and Computational Algebra.

EMPLOYMENT

Universität Bielefeld, Postdoctoral Fellow, September 2013 - present.

EDUCATION

Leiden Universiteit, The Netherlands. Ph.D. in Mathematics, May 2013.
Supervisors: Hendrik W. Lenstra and Andrea Lucchini.

Leiden Universiteit, The Netherlands. Master in Mathematics, July 2010.
Supervisor: Jan Draisma.

Ho Chi Minh University of Pedagogy, Vietnam, Bachelor in Mathematics, July 2007.

PUBLICATIONS

Recognizing $\mathrm{PSL}(2,p)$ *in the non-Frattini chief factors of finite groups*, in preparation.

Analytic properties of representation zeta functions of finitely generated nilpotent groups, joint work with Christopher Voll, preprint.

Finiteness of profinite groups with a rational probabilistic zeta function, preprint.

On normal subgroups of division rings which are radical over a proper division subring, joint work with Mai Hoang Bien, Studia Sci. Math. Hungar. 51 (2), 231–242 (2014).

Rationality of the probabilistic zeta function of finitely generated profinite groups, joint work with Andrea Lucchini, J. Group Theory 17 (2014), 317–335.

A finiteness condition on the coefficients of the probabilistic zeta function, joint work with Andrea Lucchini, Int. J. Group Theory, Vol. 2 No. 1 (2013), 167–174.

INVITED TALKS

Rationality of the probabilistic zeta function of profinite groups, Workshop on Zeta functions of groups and related algebraic structures, Padova, Italy. (September 2013)

Zeta functions of groups, an introduction, Mathematical Conference: "Summer Meeting 2013", Ho Chi Minh, Vietnam. (July 2013)

The Dirichlet Series of a Profinite Group, Graz, Austria (January 2013), Eindhoven, The Netherlands (December 2012), Geneve, Switzerland (November 2012).

OTHER TALKS

Clifford Theory, Seminar in Representation Theory, Bielefeld, Germany (June 2014).

Induced Representations, Seminar in Representation Theory, Bielefeld, Germany (May 2014).

The Probabilistic Zeta Function, Seminario Dottorato, Padova, Italy (January 2013).

Profinite groups with a rational probabilistic zeta function, Lausanne, Switzerland (June 2012).

The probabilistic zeta function of groups, an introduction, Summer Meeting in Mathematics, Ho Chi Minh, Vietnam (July 2011).

Equivariant Groebner Bases, Eindhoven Discrete Math Seminar, Eindhoven, The Netherlands (June 2010).

The Probabilistic Zeta Function of a Finitely Generated Profinite Group, Leiden, The Netherlands (May 2010).

On Casas-Alvero Conjecture, Leiden, The Netherlands (April 2010).

Finiteness of Symmetric Ideals, Leiden, The Netherlands (February 2010).

Teaching Experience

Fall	2014	Algebra 1, Bielefeld University.
Fall	2011	Algebraic Number Theory, University of Padua.

Supervision

Tram Ngo, Bachelor Honors Thesis, September 2014– present
Project : *Computing Igusa's local zeta functions by Newton polyhedron method.*

Vinh Hoang Nguyen, Undergraduate Research, September 2014– present
Project : *The Eulerian function of a finite group.*

Honors and Awards

05/2013	First Algant-Doc graduate, Algant-Doc Erasmus Program.
2010–2013	Algant Erasmus PhD Fellowship Leiden University and University of Padova
2008–2010	Algant Erasmus Master Scholarship Leiden University and University of Padova
2003–2007	University Monthly Scholarship for Excellent Students Ho Chi Minh University of Pedagogy
06/2007	Third Price in Competition on Solving Math by Calculator
09/2005	The Student Union Award for Excellent Union Official
09/2004	The Youth Union Award for Excellent Union Official
04/2003	Fourth Prize in Math Competition Dong Nai Province, Vietnam.
04/2003	Third Prize in Competition on Solving Math by Calculator Dong Nai Province, Vietnam.
04/2002	Fourth Prize in Math Competition Dong Nai Province, Vietnam.

Professional service

Reviewer of Mathematical Reviews.

Other Service	07–08/2016	Local co-organizer of CIMPA summer school in Lattices and Applications, Ho Chi Minh University of Pedagogy, Vietnam.
	08/2015	Local co-organizer of SEAMS summer school in Number Theory and Applications, Ho Chi Minh University of Pedagogy, Vietnam.
	08/2014	Co-organizer of Summer Mathematical Meetings, Ho Chi Minh City University of Sciences.
	03–05/2012	Organizer for Vietnamese Reading Course on Representation Theory, University of Padova.
	07/2011	Organizer of Students Summer Meeting in Algebra, University of Natural Sciences, Ho Chi Minh City.
	2004–2005	Vice President of Math Department Student Union, University of Pedagogy, Ho Chi Minh City.
	2003-2004	Manager member of Math Department Youth Union, University of Pedagogy, Ho Chi Minh City.
Languages	Vietnamese	Mother tongue
	English	Fluent
	German	Basic
References	Available upon request.	

HA TRAN

CONTACT INFORMATION

Faculty of Mathematics
Tor Vergata University
Via della Ricerca Scientifica 1, 00133, Roma, Italy

+39 392 848 4759
hatran1104@gmail.com
tran@axp.mat.uniroma2.it

RESEARCH INTERESTS

Algebraic Number Theory, Computational Number Theory.

Lattices, Coding Theory and Cryptography.

EMPLOYMENT

National Center for Theoretical Sciences (NCTS), Research Assistant at Division of Mathematics, National Tsing Hua University, Taiwan R.O.C, from July 2014 to December 2014.

Ho Chi Minh University of Economics and Finances, Lecturer in Mathematics, from 2009–2012.

EDUCATION

University of Tor Vergata , Ph.D. in Mathematics, from February 2012 to March 2015.
Dissertation: *On reduced Arakelov divisors of a number field*.
Supervisor: **René Schoof**.

University of Leiden, visistor at Mathematisch Institut, Leiden Universiteit, the Netherlands from September 2013 to March 2014.

Ho Chi Minh University of Pedagogy, Master in Mathematics, June 2010.
Thesis: *On Laurent p-adic series*.
Supervisor: **My Vinh Quang**.

Ho Chi Minh University of Pedagogy, B.S. in Mathematics, July 2007.

PUBLICATIONS

On reduced Arakelov divisors of real quadratic fields, preprint.

Computing spaces of effective Arakelov divisors of a number field, preprint.

A generalization of reduced Arakelov divisors, preprint.

INVITED TALKS

Reduced Arakelov divisors and its applications, Midwest Number Theory Conference for Graduate Students and Recent PhDs X, June 3 - 4, 2014, University of Illinois at Urbama-Champaign, Champaign, United State.

Reduced Arakelov divisors of a number field,"Young Researcher conference", university of Seville, Spain, 16th to 20th September, 2013.

Computing Arakelov class groups, Workshop in European University of Rome, Rome, Italy, 6th June, 2013.

Other Talks

On reduced Arakelov divisors of a number field, NCTS seminar, Fall 2014, National Center for Theoretical Sciences Third General Building, National Tsing Hua University, Hsinchu, Taiwan, September, 2014.

Reflex type and the type norm , Seminar on Complex Multiplication, Fall Semester of 2013, University of Leiden, Nethelands.

Chebotarev density theorem, Workshop in Roma 3 University in Rome, Italy.

Teaching Experience

Summer	2016	Lattices and Number Theory, CIMPA Summer School 2016.
Summer	2015	Lattices, SEAMS Summer School 2015.
Spring	2014	Linear Algebra and Geometry, University of Tor Vergata.
2009	2012	Linear Algebra 1 and 2, Analysis, Probability and Statistics, University of Economic and Finance.

Honors and Awards

2011–2014	PhD Fellowship University of Tor Vergata
2007–2010	First rank in master program in Algebraic number theory Ho Chi Minh University of Pedagogy
2003–2007	University Monthly Scholarship for Excellent Students Ho Chi Minh University of Pedagogy
2006	Prize in Math Competition DakLak Province, Vietnam.
2007	Prize in Math Competition DakLak Province, Vietnam.

Service

07–08/2016	Local co-organizer of CIMPA summer school in Lattices and Applications, Ho Chi Minh University of Pedagogy, Vietnam.
08/2015	Local co-organizer of SEAMS summer school in Number Theory and Applications, Ho Chi Minh University of Pedagogy, Vietnam.

Languages

Vietnamese	Mother tongue
English	Fluent
Italian	Basic

References

René Schoof, Univeristy of Tor Vergata, schoof.rene@gmail.com

Hendrik W. Lenstra, Leiden Universiteit, hwl@math.leidenuniv.nl

Winnie Li, Pennsylvania State University, wli@math.psu.edu

My Vinh Quang, Ho Chi Minh University of Pedagogy, quangmv@hcmup.edu.vn

Pareschi Giuseppe, Univeristy of Tor Vergata, pareschi@axp.mat.uniroma2.it

Curriculum Vitae

NGUYEN An Khuong

University of Technology, Vietnam National University-HCMC
Department of Computer Science, Faculty of C.S. and Eng.
268 Ly Thuong Kiet Street, District 10,
Ho Chi Minh City, Vietnam.
Office Tel.: *+84 (8) 865-8689*, Fax: *+84 (8) 864-5137*
Email: nakhuong@gmail.com.

Education

- 2004 – 2008: ***Ph.D. in Mathematics***, Groningen University, The Netherlands
  Advisors: Prof. Marius van der Put *and* Prof. Jaap Top
- 2003 – 2004: ***Diploma in Mathematics***, The ICTP, Trieste, Italy
  Advisor: Prof. Charles Chidume
- 2001 – 2003: ***M.S. in Mathematical Analysis***, Institute of Mathematics, Ha Noi, Vietnam
  Advisor: Prof. Tran Duc Van
- 1996 – 2000: ***B.S. in Mathematics***, Quy Nhon University, Vietnam
- 1993 – 1996: ***Honor Class in Mathematics***
  Quoc Hoc Quy Nhon High School for the Gifted, Quy Nhon, Binh Dinh, Vietnam

Research Interests

Algorithmic Number Theory; Symbolic Computation; Differential Galois Theory; D-modules

Teaching Experience

History of Mathematics; Advanced Geometry; (Advanced) Linear Algebra; Calculus; Number Theory; Differential Geometry; (Differential) Galois Theory; Lie Algebras; Statistics, (Advanced) Discrete Mathematics

Employment

- 09.2014 – present: ***Lecturer***, Department of Computer Sciences, Faculty of C.S. and Eng.
  University of Technology, Vietnam National University-HCMC, Vietnam
- 2010 – 2014: ***Lecturer***, Department of Mathematics, Faculty of Computer Science
  HCMC University of Technology (HUTECH), Vietnam
- 2009 – 2010: ***Head*** of the Department of Algebra and Geometry, Faculty of Mathematics
  Quy Nhon University, Vietnam
- 2000 – 2009: ***Lecturer***, Faculty of Mathematics, Quy Nhon University, Vietnam

Honors/Awards/Grants

- Third Prize, Binh Dinh Province Competition in Chemistry for High School Students of 12^{nd} Grade, 1995.
- Tien Phong (Vanguard) Newspaper's Scholarship for Outstanding Undergraduate Students, 1997.
- Institute of Mathematics' Prize for Outstanding Graduate Students of the Year, 2002.
- Diploma Scholarship, ICTP, Italy, 2003-2004.
- Ubbo Emmius Ph.D. Scholarships, University of Groningen, 2004-2008.
- Member in the research group ***"Algebra and Number Theory"*** at the Vietnam Institute for Advanced Studies in Mathematics (VIASM), Ha Noi: 8-9/2012, 2-3/2013, 3-5/2015.

Professional Activity

Editor for the ***"Bullletin of Vietnamese Mathematical Society"*** (in Vietnamese), 12/2012 - present

Publications

1. K. H. Karlsen, Tran Duc Van, **Nguyen An Khuong**, Vu Van Bang. Front- tracking method for the Dirichlet problem to scalar conservation laws. *Vietnam J. of Math. Apps.,* 3 (2): 1-13, 2005. (*in Vietnamese*)
2. **Nguyen, K. A.**, van der Put, M. and Top, J. Algebraic Subgroups of $GL_2(\mathbb{C})$. *Indag. Math. (N.S.),* 19 (2): 287-297, 2008.
3. **Nguyen An Khuong.** *A modern perspective on Fano's approach to linear differential equations.* Ph.D. Thesis, University of Groningen, The Netherlands, 10/2008.
4. **Nguyen, An Khuong.** On d-solvability for linear differential equations. *J. of Symbolic Comput.,* 44 (5): 421-434, 2009.
5. **Nguyen, K. A.**, van der Put, M. Solving linear differential equations. *Pure Appl. Math. Q.,* 6 (1): 173-208, 2010.
6. L. X. Chau Ngo, **K. A. Nguyen**, M. van der Put, and J. Top. Equivalence of differential equations of order one. *J. of Symbolic Comput.,* 67 (5), 2015.

Conferences/Schools

- Mini-Programme on "The Algebraic Theory of Differential Equations", 31/07-11/08/2006, Heriot-Watt University, Edinburgh, Scotland.
- International Congress of Mathematicians, 22-30/08/2006, Madrid, Spain.
- Workshop on "Arithmetic and Differential Galois Groups", 13-19/05/2007, Mathematisches Forschungsinstitut Oberwolfach, Germany.
- International Congress of Mathematicians, 19-27/08/2010, Hyderabad, India.

Student Supervisions

- **Master Degree:** Dinh Cong Hung, Tran Van Luu, Hoang Thi Ha My, Ha Duy Nghia, Ha Ngoc Du (*Quy Nhon University*); Nguyen Thai Cuong (*Da Nang University*); Nguyen Phuong Quyet (*Can Tho University*).
- **Undergraduate:** Luong Thi Hong Cam, Le Thi Tra, Nguyen Thi Phuong Thuy (*Quy Nhon University*).

Languages

- **English:** *Fluent*
- **Vietnamese:** *Mother tongue*

Skills

Maple, R, C^{++}, Python

Curriculum Vitae – Academic

Nguyen Dinh Thuc
Hochiminh City, VIETNAM
Phone: +84-38993636
Cell: +84-903-339944
thuc.nguyen@globdr.com

Title and Specialty

Associate Professor in Mathematics and Computer Science

Education:

Ph.D., Computer Science, University of Science, VNU-HCMC, 2000
Concentrations: Medical Image Processing, Data Analysis
Dissertation: Developing Models for Medical Data and Image Analysis

B.A, Computer Science, University of HCMC, 1990

Experience:

Vice-Dean, 2006 - 2014
School of Information Technology, University of Science, VNU-HCMC
Course: Cryptography 1, Cryptography 2, Database Security

Professor, 2000 - 2014
School of Information Technology, University of Science, VNU-HCMC
Course: Cryptography 1, Cryptography 2, Database Security

Visiting Professor, 2009 - 2010
Faculty of Mathematics and Statistics, Tartu University, ESTONIA
Course: Advanced Cryptography.

Teaching Assistant, 1990 - 2000
University of Science, VNU-HCMC
Courses: Logic Programming

Research Skills:

Extensive knowledge of security information.

Extensive knowledge of statistics and data analysis.

Presentations:

Thuc Dinh Nguyen (2013). Model and Architecture of UoS-Active eLearning System. Paper presented at the ELATE Conference at the University of Pedagogy, HCMC.

Publications:

- Huynh Nguyen Chinh, Nguyen Dinh Thuc, Tan Hanh, *"A distributed architecture and Non-adaptive Group testing approach to fast detect Hot-IPs in ISP networks"*, 2014 International Conference on Green and Human Information Technology (ICGHIT 2014), pp.232-236.
- Huynh Nguyen Chinh, Nguyen Dinh Thuc, Tan Hanh, *"Early detection and limitation Hot-IPs using Non-adaptive group testing and dynamic firewall rules"*, International Conference on Computing, Management and Telecommunications (ComManTel 2014), Vietnam.
- Thang Hoang, Thuc Dinh Nguyen, Chuyen Luong, Son Do, Deokjai Choi: Adaptive Cross-Device Gait Recognition Using a Mobile Accelerometer. JIPS 9(2): 333 (2013)
- Long D. T., Thu D. T., Thucc D. N.: A Bergman Ring Based Cryptosystem Analogue of RSA.2013 International Conference on IT Convergence and Security (ICITCS), 2013.
- Pham Thi Bach Hue, Thuc Dinh Nguyen, Dong Thi Bich Thuy, Isao Echizen, Sven Wohlgemuth: A User Privacy Protection Technique for Executing SQL over Encrypted Data in Database Outsourcing Service. I3E 2013: 25-37
- Thach V. Bui, Binh Q. Nguyen, Thuc Dinh Nguyen, Noboru Sonehara, Isao Echizen: Robust Fingerprinting Codes for Database. ICA3PP (2) 2013: 167-176
- Thuc Dinh Nguyen, Van H. Dang: Quasi-inverse Based Cryptography. ICCSA (4) 2013: 629-642
- Thach V. Bui, Oanh K. Nguyen, Van H. Dang, Nhung T. H. Nguyen, Thuc Dinh Nguyen: A Variant of Non-Adaptive Group Testing and Its Application in Pay-Television via Internet. ICT-EurAsia 2013: 324-330
- Thach V. Bui, Van H. Dang, Isao Echizen, Thuc Dinh Nguyen: How Can We Acquire the Most Common Query Types in Two-Tiered Wireless Sensor Networks? NGMAST 2013: 111-115
- Thang Hoang, Deokjai Choi, Quang Viet Vo, Huy Anh Nguyen, Thuc Dinh Nguyen: A Lightweight Gait Authentication on Mobile Phone Regardless of Installation Error. SEC 2013: 83-101.
- Bui, Thach V., Binh Q. Nguyen, Thuc D. Nguyen, Noboru Sonehara, and Isao Echizen. "Effective Fingerprinting Codes for Database." In *Signal-Image Technology & Internet-Based Systems (SITIS), 2013 International Conference on*, pp. 655-659. IEEE, 2013.
- Thach V. Bui, Binh Q. Nguyen, Thuc Dinh Nguyen, Noboru Sonehara, Isao Echizen: Effective Fingerprinting Codes for Database. SITIS 2013: 655-659
- Huynh Nguyen Chinh, Nguyen Dinh Thuc, Tan Hanh, *"Finding Hot-IPs in network using group testing method – A review"*, The 2012 International Conference On Green Technology And Sustainable Development (GTSD 2012)/Journal of Engineering Technology and Education – Kuas,Taiwan, 2013, pp.374-379.
- Thach V. Bui, Chinh N. Huynh, Thuc D. Nguyen, *"Early detection for networking anomalies using Non-Adaptive Group testing,"* International Conference on ICT Convergence 2013 (ICTC 2013), Korea, 2013. pp. 984-987.
- Nguyen, Binh T., Anh-Duc Luong-Thanh, Nguyen Dinh Thuc, and Bui Van Thach. A divide-and-conquer algorithm for a symmetric tri-block-diagonal matrix. In *Southeastcon, 2012 Proceedings of IEEE*, pp. 1-6. IEEE, 2012.
- Thuc Dinh Nguyen, Thach V. Bui, Van H. Dang, Deokjai Choi: Efficiently Preserving Data Privacy Range Queries in Two-Tiered Wireless Sensor Networks. UIC/ATC 2012: 973-978
- Pham Thi Bach Hue, Thuc Dinh Nguyen, Van H. Dang, Isao Echizen, Dong Thi Bich Thuy: A Mutual and Pseudo Inverse Matrix - Based Authentication Mechanism for Outsourcing Service. ACIIDS (1) 2011: 119-128
- Van H. Dang, Sven Wohlgemuth, Hiroshi Yoshiura, Thuc Dinh Nguyen, Isao Echizen: Approach to Privacy-Preserve Data in Two-Tiered Wireless Sensor Network Based on Linear System and Histogram. FGIT-UNESST 2010: 17-30
- Thuc Dinh Nguyen, Pham Thi Bach Hue, Van H. Dang: An Efficient Pseudo Inverse Matrix - Based Solution for Secure Auditing. RIVF 2010: 1-6.
- Bao Ngoc Tran, Thuc Dinh Nguyen, Tran Dan Thu: A New S-Box Structure Based on Graph Isomorphism. CIS (1) 2009: 463-467.
- Bao Ngoc Tran, Thuc Dinh Nguyen: Modular Matrix Cipher and Its Application in Authentication Protocol. SNPD 2008: 318-323.
- Trung Hau Tran, Cédric Sanza, Yves Duthen, Thuc Dinh Nguyen: XCSF with computed continuous action. GECCO 2007: 1861-1869

Grants and Fellowships:

- KAAD Grant, PostDoc at Ruhr-Universty of Bochom, Germany, 2005 – 2006. (Project: WIFI Security - Defending against Man-in-the-Middle attacks).
- HCMC Department of Science and Technology Research Grant, 2011 – 2013, Project: Secure Hotspot ($15,000 ~ 300 Mil VNĐ).
- Ministry of Science and Technology Research, Project: Grant Designing and Implementing IP Cores for cryptosystems on FPGA, 2011 – 2012 ($30,000).
- VNU-HCMC Key Research Grant, Project: Designing and Implementing Crypto-Processors on FPGA,, 2012 -2014 ($25,000).
- HCMC Department of Science and Technology Research Grant, Project: RSA : algebraic properties and cryptanalysis, 2013 – 2014, ($20000 ~ 400 Mil VNĐ).

Awards and Honors:

- Young Researcher Awards, Hochiminh City, 1990.

Skills and Qualifications:

- Programming ability in C, C++ and PROLOG
- Fluent in French