SOUTH EAST ASIAN MATHEMATICAL SOCIETY

FINAL REPORT

CRYPTOGRAPHY: FOUNDATIONS AND NEW DIRECTIONS

Hanoi, Vietnam
November 27 – December 04, 2016

Organized by

Vietnam Institute for Advanced Study in Mathematics (VIASM)
and
University of Science, Vietnam National University in Hanoi (VNU-HUS)

with the support of
CIMPA, SEAMS, IACR, VIASM, HUS and IMU

2016

Cryptography: Foundations and New Directions
Hanoi, November 27 – December 04, 2016

I. Summary

The IACR-SEAMS School "Cryptography: Foundations and New Directions" was organized by Vietnam Institute for Advanced Study in Mathematics (VIASM) and University of Science, Vietnam National University at Hanoi (VNU-HUS). It was held at VIASM from November 27 to December 04, 2016. This is the first joint school between International Association of Cryptology Research (IACR) and South East Asian Mathematical Society (SEAMS).

There were six lecturers: one from Vietnam, one from France, one from United States, one from Japan and two from the Netherlands. There were 83 participants including 35 from Vietnam and 48 international from France (7), Germany (1), India (7), the Netherlands (4), Indonesia (4), Malaysia (4), Hong Kong (1), Australia (1), Italy (1), Japan (2), Korea (1), Canada (1), New Zealand (1), Philippines (3), Sri Lanka (1), Sweden (2), USA (5), Singapore (1).

The School obtained generous supports from CIMPA-SEAMS, IACR, VIASM, HUS and International Mathematical Union (IMU).

The School started on November 27. The opening ceremony took place on the first morning including speeches given by Prof. Nguyen Huu Du, Director of VIASM and President of the Vietnam Mathematical Society, and Prof. Le Tuan Hoa, Director of Vietnam Institute of Mathematics and Presentative of SEAMS in Vietnam. There were two contributed talks on Wednesday and Friday afternoon by participants. The School ended on Sunday, December 04 followed by a public talk of Prof. Adi Shamir.

II. Scientific Objectives and Rationale for the School

The School introduced foundations and some new trends in cryptography. It was addressed to advanced undergraduate and graduate students and young researchers from Southeast Asian Countries and all over the world. It provided them solid background as well as some new trends in cryptography for further study. It prepared background for participants to

attend the ASIACRYPT 2016 organized by VIASM in the following week.

III. Organizers and Lecturers

Organizers:

- Nguyen Huu Du, Vietnam Institute for Advanced Study in Mathematics
- Duong Hoang Dung, Kyushu University, Japan
- Phan Duong Hieu, University of Limoges, France
- Le Minh Ha, University of Science, Vietnam National University at Hanoi
- Tran Nguyen Thanh Ha, University of Calgary, Canada

Lecturers:

- Daniel Bernstein, Technische Universiteit Eindhoven, the Netherlands
- Phan Thi Ha Duong, Vietnam Institute of Mathematics
- Neal Koblitz, University of Washington, Seattle, United States
- Tanja Lange, Technische Universiteit Eindhoven, the Netherlands
- Phong Q. Nguyen, University of Tokyo, Japan
- David Pointcheval, École Normale Supérieure, Paris, France

IV. The Participants

(see the attached file)

V. School Programs

The School introduced foundations and some new trends in cryptography. It prepared solid background for participants to attend the ASIACRYPT 2016 held in the following week.

There are four courses in the school including:

Course 1: Mathematical foundations of cryptography}
Lecturers: Phan Thi Ha Duong, Phong Q. Nguyen and Neal Koblitz
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 2 : 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 3: Cryptanalysis of public-key systems
Lecturer: Tanja Lange
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 4: High-speed cryptography
Lecturer: **Daniel J. Bernstein**
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.USERKEY=PROGRAM. The lecture notes are also updated at HTTP://VIASM.EDU.VN/HDKH/CRYPTOSCHOOL2016?USERKEY=DOCUMENTS

VI. Conclusion

The School started from Sunday, November 27, 2016 to Sunday, December 04, 2016. The school included 35 hours for lectures and 10.5 hours for group discussion. Every day, there were 5 hours for lectures and 1.5 hours for group discussion. The lessons last from 9:00 to 12:00 in the morning and from 14:00 to 16:30 in the afternoon. The schedule is located at here: HTTP://VIASM.EDU.VN/HDKH/CRYPTOSCHOOL2016?

The IACR-SEAMS has been a very good program that prepares background for participants to attend the Asiacrypt 2016 which was held also in Hanoi right after the school. This event attracted attention of not only more students from several regions in Vietnam but also some companies as well as governmental organizations; this will encourage the develop of cryptology research in near future in Vietnam. The school together with two previous schools held in Ho Chi Minh in Summer 2015 (SEAMS School "Number Theory and Applications in Cryptography and Coding Theory") and in Summer 2016 (CIMPA-ICTP School "Lattices and Applications in Cryptography and Coding Theory") have created a network of researchers working in the subjects in the South East Asian Countries. We are planning to have a joint school in Thailand in near future. It is a good sight for promoting research and collaboration in the area.

VII. Financial Report

CIMPA – SEAMS	EURO	5000
VIASM	EURO	5000
HUS	EURO	2500
IMU	EURO	1000
IACR	USD	8000

Contributed talks by participants:

Duong Ngoc Thai (Google): BEAST and other browser-based attacks

Siu-Ming Yiu (Hong Kong): Oblivious RAM