

INSTITUT DES HAUTES ETUDES

POUR LE DEVELOPPEMENT DE LA CULTURE, DE LA SCIENCE ET DE LA TECHNOLOGIE EN BULGARIE

CryptoBG*2008

International Symposium

**Recent Developments in Cryptography
and Information Security**

PROGRAM

September 11-13, 2008

National Institute of Education, Oriahovitzza, Bulgaria

Organized and sponsored by
Minu Balkanski Foundation

PRELIMINARY PROGRAM

Wednesday (10 September 2008) - after 16:00 h & Thursday (11 September 2008) – 09:30-11:30 h
 Registration, National Institute of Education, Oriahovitza, Bulgaria

Thursday (11 September 2008)

12:00 – 13:00 Official Opening

[Lunch]

14:00 – 18:00 **Session 1: Public Key Crypto & Cryptanalysis**

Dr. Yacov Yacobi (Microsoft Research) - SDH Vs. CDH

Dr. Ramarathnam Venkatesan (Microsoft Research) - A Snapshot of Cryptanalysis

Tutorial on elliptic curves: Part 1

Dr. Mladen Dimitrov (Université Paris Diderot, France)

Dr. Dimitar Jetchev (University of California at Berkeley, USA) - Bit Security of Elliptic Curve Diffie-Hellman Secret Keys

Friday (12 September 2008)

09:00 – 10:30 **Session 2: Hashing**

Dr. Mehmet Kivanc (Microsoft Research) - Robust signal hashing

Elena Andreeva (Katholieke Universiteit Leuven, Belgium) - Hash Functions: Past, Present and Future

11:00 – 13:00 **Tutorial on elliptic curves: Part 2**

Dr. Mladen Dimitrov (Université Paris Diderot, France)

Dr. Dimitar Jetchev (University of California at Berkeley, USA)

[Lunch]

14:00 – 16:00 **Session 5: Workshop on *Machine Learning and Intelligent Systems***

introduction and moderation by Dr. Preslav Nakov (IPP, Bulgarian Academy of Sciences)

Ekaterina Mihaylova, Ekaterina Stambolieva - POS-Tagging Bulgarian Text using CRF

Ivelina Nikolova - Employing Language Technologies for Computer Aided Design of Multiple-choice

Questions

Georgi Georgiev - A Study of Using Surface and Domain-specific Features, Lexicons and Part-of-speech Information in a CRF-based Named Entity Recognizer for Bulgarian

16:15 – 18:45 **Tutorial: Smart cards programming** (Nikolay Nedyalkov, ISECA, tbc)

[Concert and exhibition in Nova Zagora]

Saturday (13 September 2008)

09:00 – 11:00 **Session 4: Privacy**

Dr. Preslav Nakov (IPP, Bulgarian Academy of Sciences) - Privacy on the Internet?

Dr. Apostol Vassilev (NetIDSys, Austin, TX, USA) - Title: You say to-mah-to, I say to-mae-to: why isn't there a single solution to Information Security Assurance?

Mariana Raykova (Columbia University, NY, USA) - PAR: Payment for Anonymous Routing

Dr. Dimitar Jetchev (University of California at Berkeley, USA) - Japan & Mobile payments

11:30 – 13:30 **Round table: Security and privacy of mobile payments**

13:30 Closing

[Lunch] [Excursion] [18:00 – Departure]

Speakers and abstracts