Programme

of Indo-Russian conference on Algebra, Number Theory, Discrete Mathematics and their Applications

October 15, 2014, Wednesday, room 16-24

9.30–10.00 Registration

10.00–10.30 Opening ceremony (V.N. Chubarikov, B. Roy, Yu.V. Nesterenko, V.N. Latyshev, O.M. Kasim-Zade, A.V. Mikhalev, V.B. Kudryavcev, V.A. Artamonov)

Chairman A.V.Mikhalev

10.30–11.00 V.N. Chubarikov (The dean of Mech.-Math. Faculty Moscow Univ.). Arithmetics and polynomials

11.10–11.40 B. Roy. (ISI, Kolkata) Uniform Combinatorial Batch Codes (Indian statistical Institute, Discrete Math). [*View/download presentation*]

11.40–12.10 Break

Chairman B. Roy

12.10–12.40 Yu.V. Nesterenko (Moscow University). Primality testing in algebraic number fields (after AKS)

12.45–13.15 Santanu Sarkar. Cryptanalysis of an RSA variant (Chennai Mathematical Institute, Number Theory)

13.15–14.30 Lunch

Room 12-25

Chairman Santanu Sarkar

14.30–15.00 Sandip Das. The Erdos-Sekeres Theorem; upper bounds and related results (Indian Statitical Insisute, Discrete Math)

15.05–15.35 A.V. Gribov, V.T. Markov, A.V. Mikhalev, A.A. Nechaev (Moscow University) Non-commutative and non-associative structures in coding and cryptography [*View/download presentation*]

15.40–16.00 P.A. Panteleev. Computer modelling of logical processes

16.00–16.20 Break

Chairman A. Yushunsky

16.20–16.40 I. Popovyan (Moscow University). Factoring RSA-180 and RSA-190.

16.40–17.10 Sushmita Ruj. Key management in sensor networks (R C Bose Center for Cryptology and Security, Discrete Math)

17.15–17.35 M.A. Goltvanica. Bit sequences of twist linear recurrent sequences.

18.30–22.00 Conference dinner

October 16, 2014, Thursday, room 16-24

Chairman

9.00–9.30 A.V.Galatenko, D.E.Aleksandrov (Moscow University). Automata-theory models in information security.

9.35–10.05 Ashish Choudhury. Asynchronous MPC with a strict honest majority using non-equivocation (International institute of information technology, Bangalor, Cryptography) [*View/download presentation*]

10.10–10.40 Arpita Patra. A simple and efficient framework for secure multi-party computation (Department of computer science an automation, Indian institute of sciences, Bangalor, Cryptography)

10.45–11.15 Mridul Nandi. Minimum number of multiplication to compute a Delta-Universal hash function (Indian Statistical Institute, Cryptography)

11.15–11.30 Break

Chairman

11.30–12.00 A.L. Kanunnikov (Moscow University), E.A. Vasileva (France). A recurrence formula for Jack connection coefficients.

12.05–12.35 V.Arvind. The Alon-Roichman Theorem and derandomied construction of expanding generator sets for finite groups (The Institute of Mathematical Sciences, Chennai, Algebra)

12.40–13.10 A.I. Bufetov (Steklov Instutute). Quasi-Symmetries of Determinantal Point Processes

13.15–13.45 Alexey Yu. Nesterenko. A construction of endomorphisms of elliptic curves over finite fields.

13.45–15.00 Lunch

Room 13-11

Chairman

15.00–15.30 R.M. Kolpakov (Moscow University), Djamal Belazzougui (Department of Computer Science, FI-00014 University of Helsinki, Finland), Mathieu Raffinot, (LIAFA, Université Paris Diderot–Paris 7, France). Indexing and querying character sets in one- and two-dimensional words. [*View/download presentation*]

15.30–16.00 Sourav Sen Gupta. (Non-)random sequences from (non-)random permutations (Indian Statistical Institute, Discrete Math). [*View/download presentation*]

16.05–16.25 Yu. Tarannikov (Moscow University). A new approach to the constructing of m-resilient functions with maximal nonlinearity and auxiliary mathematical problems. [*View/download presentation*]

16.25–16.55 A.V. Chashkin (Moscow University). Linear hashing

17.00–17.30 V.V. Kochergin (Moscow University). On the Bellman and Knuth problems and their generalizations. [*View/download presentation*]

17.30–17.50 Break

Chairman Yu.V. Nesterenko

17.50–18.10 M. Zelenova (Moscow University). Solving of polynomial equations over integers

18.10–18.30 A. Kochergin (Keldysh Institute for Applied Mathematics, Russian Acad. of Sci.). On the depth of functions of k-valued logics over arbitrary bases.

18.30–18.50 Yu.A. Kombarov (Moscow University). Complexity and structure of circuits for parity functions. [*View/download presentation*]

October 17, 2014, Friday, room 16-24

Chairman A.V. Mikhalev

9.00–9.30 V.N. Latyshev (Moscow University). Algebraic simplification and cryptographic motives

9.35–10.05 V.A. Artamonov, S. Chakrabarti, S. Gangopadhyay and S.K. Pal. On Latin squares of polynomially complete quasigroups and their application in cryptography. [*View/download presentation*]

10.10–11.40 Sucheta Chakrabarti. Algebraic Structures of combinatorial designs and their application to Cryptography (SAG, DRDO, Algebra)

10.45–11.15 V.A. Nosov, A.E. Pankratiev (Moscow University). Using Boolean functions to construct Latin squares

11.20–11.50 S. Gangopadhyay. Generalized Bent Functions (DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING, Algebra). [*View/download presentation*]

11.50–12.20 Kishan Gupta. Cryptographically significant MDS matrices (Indian statitical Insitute, Discrete Math) [*View/download presentation*]

Chairman V.N. Latyshev

12.20–12.40 Shweta Agrawal. Expensive encryption systems for modern computing needs (Indian Statistical Institute,Cryptography) [*View/download presentation*]

12.45–13.05 Maryana Kovalenko (Moscow University). Linear codes generated by the affine geometries over a 4-element field and their properties. [*View/download presentation*]

13.10–13.30 M.V. Budrevich, A.E. Guterman. Permanent Polya problem.

13.35–14.05 P.B. Tarasov (Moscow University). Conditions of parallelizability in multi-valued logics.

14.05–15.00 Lunch

Room 13-11

Chairman Sandip Das

15.00–15.20 A. Klyachko (Moscow University). The identities of additive binary arithmetics

15.20–15.40 Olga Podolskaya (Moscow University). Tight lower bounds on the circuit complexity of parity and majority functions. [*View/download presentation*]

15.40–16.00 Kirill Popkov (Moscow University). Single tests for contacts. [*View/download presentation*]

16.00–16.20 Alexey Yashunsky (Keldysh Institute for Applied Mathematics, Russian Acad. of Sci.). Generating probability distributions over finite fields. [*View/download presentation*]

16.20–16.40 Igor Cherednik. Non-negative bases of integer lattices

16.40-17.00 Serafim Chekalkin (Moscow University). Polynomials quality estimation for NFS.

17.00 Closing ceremony.