International Workshop on Boolean Functions and Their Applications

September 2 – September 7

Preliminary Program

September 2, Tuesday

Arrival and registration.
12:00–14:00 Lunch.
19:00–22:00 Dinner.

September 3, Wednesday

07:00–09:00 Breakfast.
09:00–10:00 Claude Carlet ”Boolean plateaued functions, vectorial functions with plateaued components, and their APNness”.
10:00–10:30 Philippe Langevin ”An interesting open question related to an old conjecture of Helleseth”.
10:30–11:00 Coffee break.
11:00–12:00 Kaisa Nyberg ”Links between differential and linear cryptanalysis and Boolean functions”.
12:00–14:00 Lunch.
14:00–14:30 Sihem Mesnager ”Several infinite families of bent functions and their duals”.
14:30–15:30 Patrick Sole ”On self-dual bent functions”.
15:30–16:00 Coffee break.
16:00–16:30 Max Sala ”Boolean functions and trapdoors in block ciphers”.
16:30–17:00 Chunlei Li ”De Bruijn sequences constructed from two classes of LFSRs”.
17:00–17:30 Yin Tan ”More constructions of differentially 4-uniform permutations on GF(2^{2k})”.
19:00–22:00 Dinner.

September 4, Thursday

07:00–09:00 Breakfast.
09:00–10:00 Faruk Gologlu ”Projective polynomials and their applications in cryptography”.
10:00–10:30 Tor Helleseth ”On the proof of Lin’s conjecture”.
10:30–11:00 Coffee break.
11:00–12:00 Robert Coulter ”Commutative semifields and the equivalence problem”.
12:00–14:00 Lunch.

14:00–19:00 Excursion.
19:00–22:00 Dinner.

September 5, Friday

07:00–09:00 Breakfast.
09:00–10:00 Alexander Kholosha "On Niho bent functions".
10:00–10:30 Florian Caullery "Algebraic geometry and Boolean functions".
10:30–11:00 Coffee break.
11:00–11:30 Havard Raddum "Solving systems of Boolean polynomials using binary decision diagrams".
11:30–12:00 Enes Pasalic "A survey on bent functions and related combinatorial and graph theoretic aspects".
12:00–14:00 Lunch.
14:00–15:00 Alexander Pott "Relative difference sets and their component functions".
15:00–15:30 Svetla Nikova "Reversed genetic algorithms for generation of bijective S-boxes with good cryptographic properties".
15:30–16:00 Coffee break.
16:00–16:30 Oleksandr Kazymyrov "Algebraic-differential cryptanalysis and addition modulo 2^n".
16:30–17:00 Yongbo Xia "Some results on cross-correlation distribution between a p-ary m-sequence and its decimated sequences".
19:00–22:00 Dinner.

September 6, Saturday

07:00–09:00 Breakfast.
09:00–10:00 Wilfried Meidl "On quadratic functions from F_{p^n} to F_p".
10:00–10:30 Gaofei Wu "Some results on bent$_4$ functions".
10:30–11:00 Coffee break.
11:00–12:00 Matthew Parker "A survey of the negaHadamard transform in various contexts".
12:00–14:00 Lunch.
14:00–19:00 Excursion.
19:00–22:00 Dinner.

September 7, Sunday

07:00–10:30 Breakfast.
Departure.