# BCS 2018 – Conference Program

September 20 (Thursday)

8:00 - 8:45 Registration

8:45 - 9:00 Welcome

9:00 - 10:00 Invited talk: Marc Fischlin (Darmstadt University of Technology)
*Cryptographic Analysis of TLS 1.3*

10:00 – 10:30 Abdelrahaman Aly and Sara Cleemput
*Efficient and Secure Shortest Path Protocol and its Applications to Combinatorial Auctions*

10:30 - 11:00 Coffee break

11:00 - 11:30 Julian Speith, Tobias Oder, Marcel Kneib and Tim Güneysu :
*A Lattice-based AKE on ARM Cortex-M4*

11:30 - 12:00 Kashi Neupane
*Deniable Authenticated Two-Round Group Key Establishment*

12:00 - 14:00 Lunch

14:00 – 15:00 Invited talk
Ioan Constantin (Orange Romania)
Needles and Haystacks: Using Machine Learning and Threat Intelligence to Detect, Prevent, and Mitigate Advanced Cyber-physical Threats to the Communications Critical Infrastructure of Europe

15:00 - 15:30 Coffee break

15:30 - 16:00 Tomer Ashur and Raluca Posteuca
*On linear hulls in one round of DES*

16:00 - 16:30 Pınar Çomak, Svetla Nikova and Vincent Rijmen
*On Decomposition of Permutations*

16:30 – 17:00 Steering Committee meeting

18:30 - Dinner

September 21 (Friday)

9:00 - 10:00 Tudor Dumitras (University of Maryland)
Measurements, Predictions, and the Puzzle of Machine Learning: what Data from 10 Million Hosts can Teach us about Security

10:00 – 10:30 Octavian Catrina
*Towards Practical Secure Computation with Floating-Point Numbers*

10:30 - 11:00 Coffee break

11:00 - 11:30 Sorina Ionica and Malika Izabachene
*Weak Instances of Composite Order Protocols*

11:30 - 12:00 Katerina Samari, Foteini Baldimtsi and Aggelos Kiayias
*Watermarking Probabilistic Circuits: The Case of Digital Signatures*

12:00 - 13:30 Lunch

13:30 - 14:00 Diana Stefania Maimut and George Teseleanu
*New Configurations of Grain Ciphers: Security against Slide Attacks*

14:00 - 14:30 Alexandre Adomnicai, Jacques Fournier and Laurent Masson
*Masking the Lightweight Authenticated Ciphers ACORN and Ascon in Software*

14:30 - 15:00 Coffee break

15:00 - 16:00 Round table

16:30 – Closing remarks and conclusions