Monday, September 1st

08:30 - 09:00	Registration
09:00 - 09:15	Opening Remarks
09:15 - 10:15	Invited Talk: Guido Marco BERTONI, Permutation-based encryption for lightweight
10:15 - 10:30	Coffee Break
Session I: Efficient Implementations and designs	
10:30 - 11:00	Douglas Shors, Louis Wingers, Ray Beaulieu, Stefan Treatman-Clark, Bryan Weeks and Jason Smith. Implementation and Performance of the SIMON and SPECK Lightweight Block Ciphers on AVR 8-bit Microcontrollers.
11:00 - 11:30	Meltem Sonmez Turan and Rene Peralta. The Multiplicative Complexity of Boolean Functions on Four and Five Variables.
11:30 - 12:00	Coffee Break
12:00 - 12:30	Ege Gulcan, Aydin Aysu and Patrick Schaumont. A Flexible and Compact Hardware Architecture for the SIMON Block Cipher.
12:30 - 13:00	Mitsuru Matsui and Yumiko Murakami. AES Smaller Than S-box - Minimalism in Software Design on Low End Microcontrollers.
13:00 - 14:00	Lunch
14:00 - 15:00	Invited Talk: Tolga ACAR, Selecting and Deploying Elliptic Curves in Security Protocols
15:00 - 15:30	Coffee Break
Session II: Attacks	
15:30 - 16:00	Cihangir Tezcan and Ferruh Özbudak. Differential Factors: Improved Attacks on SERPENT.
16:00 - 16:30	Fabrizio De Santis, Oscar M. Guillen, Ermin Sakic and Georg Sigl. Ciphertext-Only Fault Attacks on PRESENT.
17:00 - 19:00	Bosphorus tour. Boat will pick us up from the dock close to the venue building.
19:30 - 22:00	Dinner at Cemile Sultan Korusu.
22:30	Water taxi will pick up guests from Kandilli and drop them off at Eminönü

Tuesday, September 2nd

9:00 - 10:00	Invited Talk: Johann Heyszl, High-Resolution Magnetic Field Side-Channels and their Affect on Cryptographic Implementations.
10:00 - 10:15	Coffee Break
Session III: Attacks (Continued)	
10:15 - 10:45	Rusydi H. Makarim and Cihangir Tezcan. Relating Undisturbed Bits to Other Properties of Substitution Boxes.
10:45 - 11:15	Riham Altawy and Amr Youssef. Differential sieving for 2-step matching meet-in-the-middle attack with application to LBlock.
11:15 - 11:45	Coffee Break
11:45 - 12:15	Ling Song, Lei Hu, Bingke Ma and Danping Shi. Match Box Meet-in-the-Middle Attacks on the SIMON Family of Block Ciphers.
Session IV: Protocols	
12:15 - 12:45	Daisuke Moriyama. A Provably Secure Offline RFID Yoking-Proof Protocol with Anonymity.
12:45 - 13:00	Closing Remarks
13:00 - 14:00	Lunch