September 28 Wednesday

9:30 – 10:45	Invited Talk (ES033) Yosuke Todo *Nonlinear Invariant Attack* Ivica Nikolić *On the Meet-in-the-Middle Attack*
10:45 – 11:15	Coffee Break (ES Building, 3rd Floor)
11:15 – 12:30	Invited Talk (ES033) Mridul Nandi *On the Exact Security of Iterated Random Function* Damian Vizár *Online Authenticated-Encryption and its Nonce-Reuse Misuse-Resistance*
12:30 – 14:00	Lunch (Restaurant Hananoki (Japanese))
14:00 – 16:00	Group Discussion Group 1: ES031, Group 2: ES032, Group 3: ES035, Group 4: ES033, Group 5: NIC209, Group 6: NIC 211, Group 7: NIC212
16:00 – 16:30	Coffee Break (ES Building, 3rd Floor)
16:30 – 18:00	Group Discussion Group 1: ES031, Group 2: ES032, Group 3: IB908, Group 4: ES033, Group 5: NIC209, Group 6: NIC 211, Group 7: NIC212

September 29 Thursday

9:30 – 10:45	Invited Talk (ES033) Meicheng Liu *Algebraic Cryptanalysis of Round-Reduced Keccak* Florian Mendel *Statistical Fault Attacks on Nonce-Based Authenticated Encryption Schemes*
10:45 – 11:15	Coffee Break (ES Building, 3rd Floor)
11:15 – 12:30	Invited Talk (ES033) Lei Wang *How to Build Fully Secure Tweakable Blockciphers from Classical Blockciphers* Jooyoung Lee *Wegman-Carter Style MACs from Tweakable Block Ciphers*
12:30 – 14:00	Lunch (Restaurant GRAN PIATTO (Pizza and Pasta))
14:00 – 16:00	Group Discussion Group 1: ES031, Group 2: ES032, Group 3: ES035, Group 4: ES033, Group 5: NIC209, Group 6: NIC 211, Group 7: NIC212
16:00 – 16:30	Coffee Break (ES Building, 3rd Floor)
16:30 – 18:00	Group Discussion Group 1: ES031, Group 2: ES032, Group 3: ES035, Group 4: ES033, Group 5: NIC209, Group 6: NIC 211, Group 7: NIC212

September 30 Friday

9:30 – 10:45	Invited Talk (ES033) Subhadeep Banik *A Compact Implementation of the AES Ecnryption/Decryption Core* Thomas Peyrin *The Skinny Family of Tweakable Block Ciphers*
10:45 – 11:15	Coffee Break (ES Building, 3rd Floor)
11:15 – 12:30	Invited Talk (ES033) Shoichi Hirose *Pseudorandom-Function Modes of a Compression Function* Atul Luykx *Understanding Multi-Key Security Degradation*
12:30 – 14:00	Lunch (Restaurant UNIVERSAL CLUB (meat or fish))
14:00 – 15:30	Group Discussion Group 1: ES031, Group 2: ES032, Group 3: ES035, Group 4: ES033, Group 5: NIC209, Group 6: NIC 211, Group 7: NIC212
15:30 – 16:00	Coffee Break (ES Building, 3rd Floor)
16:00 – 17:00	Group Discussion Group 1: ES031, Group 2: ES032, Group 3: ES035, Group 4: ES033, Group 5: NIC209, Group 6: NIC 211, Group 7: NIC212
17:00 – 18:00	Wrap Up (ES033)