December 9

9.00-10:20	**Nicky Mouha** Finding Bugs in Cryptographic Hash Function Implementations **Lei Wang** Towards Minimizing Key-Alternating Feistel Ciphers	Invited Talks No. 3 Building, 3# Room
10:20-10:50	Coffee Break	
10:50-12:10	**Yosuke Todo** Some Improvements of Non-Blackbox Cube Attacks **Ling Song** Conditional Cube Attacks on Keccak-p Based Constructions	Invited Talks No. 3 Building, 3# Room
12:10-14:00	Lunch	
14:00-15:30	Group Discussion Group 1: Room A, 6th Floor, Group 2: Room A, 7th Floor, Group 3: Room B, 7th Floor, Group 4: Room A, 8th Floor, Group 5: Room B, 8th Floor, Group 6: Room A,9th Floor, Group 7: Room B, 9th Floor	
15:30-16:00	Coffee Break	
16:00-17:30	Group Discussion Group 1: Room A, 6th Floor, Group 2: Room A, 7th Floor, Group 3: Room B, 7th Floor, Group 4: Room A, 8th Floor, Group 5: Room B, 8th Floor, Group 6: Room A,9th Floor, Group 7: Room B, 9th Floor	

December 10

9.00-10:20	**Mridul Nandi** Tools for Symmetric Key Provable Security **Tetsu Iwata** ZMAC: Specification, Security Proof, and Instantiation	Invited Talks No. 3 Building, 3# Room
10:20-10:50	Coffee Break	
10:50-12:10	**Yu Sasaki** MILP Modeling for(Large) S-boxes to Optimize Probability of Differential Characteristics **Yunwen Liu** The Phantom of Differential Characteristics	Invited Talks No. 3 Building, 3# Room
12:10-14:00	Lunch	
14:00-15:30	Group Discussion Group 1: Room A, 6th Floor, Group 2: Room A, 7th Floor, Group 3: Room B, 7th Floor, Group 4: Room A, 8th Floor, Group 5: Room B, 8th Floor, Group 6: Room A,9th Floor, Group 7: Room B, 9th Floor	
15:30-16:00	Coffee Break	
16:00-17:30	Group Discussion Group 1: Room A, 6th Floor, Group 2: Room A, 7th Floor, Group 3: Room B, 7th Floor, Group 4: Room A, 8th Floor, Group 5: Room B, 8th Floor, Group 6: Room A,9th Floor, Group 7: Room B, 9th Floor	

December 11

9.00-10:20	**Meiqin Wang** Automatic Search of (Related-Key, Impossible) Differential and (Zero -Correlation) Linear Trails for S-Box Based Ciphers with STP **Patrick Derbez** Yet another attack on whitebox AES implementation	Invited Talks No. 3 Building, 3# Room
10:20-10:50	Coffee Break	
10:50-12:10	**Danping Shi** Programming the Demirci-Selcuk Meet-in-the-Middle Attack with Constraints **Sumanta Sarkar** On the Lightweight Design Choices for Diffusion Layer of Block Ciphers	Invited Talks No. 3 Building, 3# Room
12:10-14:00	Lunch	
14:00-15:30	Group Discussion Group 1: Room A, 6th Floor, Group 2: Room A, 7th Floor, Group 3: Room B, 7th Floor, Group 4: Room A, 8th Floor, Group 5: Room B, 8th Floor, Group 6: Room A,9th Floor, Group 7: Room B, 9th Floor	
15:30-16:00	Coffee Break	
16:00-17:00	Wrap Up(No. 3 Building, 3# Room)	