## December 9

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

## December 10

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

## December 11

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

