# „Symmetric Cryptography“ 2014

## Thursday, January 9

| Time | Title | Presenter | Duration |
|---|---|---|---|
| - 9:00 | Breakfast | | |
| 9:00 - 10:30 | New Generic Attacks on Hash-based MACs | Gaetan Leurent | 30 mins |
| | Black-box, White-box, and Public-key ASASA schemes | Dmitry Khovratovich | 30 mins |
| | Color Visual Cryptography with Scotch Tape and Polarizers | Alex Biryukov | 20 mins |
| 10:30-11:00 | Coffee | | |
| 11:00 – 12:00 | Incremental Authenticated Encryption | Kan Yasuda | 30 mins |
| | APE: Authenticated Permutation-Based Encryption for Lightweight Cryptography | Bart Mennink | 30 mins |
| 12:15-13:45 | Lunch | | |
| 14:00 - 15:30 | Private Discussions | | |
| 15:30-16:00 | Coffee and Cake | | |
| 16:00 - 18:00 | Block Ciphers for Efficient Masking | Francois-Xavier Standaert | 30 mins |
| | LWE with Small Secrets | Martin Albrecht | 30 mins |
| | Randomness | Tanja Lange | 30 mins |
| 18:00-19:00 | Dinner | | |
| 19:30 | Discussion | | |

## Friday, January 10

| Time | Title | Presenter | Duration |
|---|---|---|---|
| - 9:00 | Breakfast | | |
| 9:30 - 10:30 | Cryptanalysis of a reduced version of Crypt-MT | Greg Rose | 30 mins |
| | An Improvement of Linear Cryptanalysis with Addition Operations with Application to FEAL-NX | Eli Biham | 30 mins |
| 10:30-11:00 | Coffee | | |
| 11:00 – 12:00 | | | 30 mins |
| | | | 30 mins |
| 12:15-13:45 | Lunch | | |