# “Symmetric Cryptography” 2016

## Monday, January 11

| Time | Title | Presenter | Duration |
|---|---|---|---|
| 7:30-<br>9:00 | Breakfast | | |
| Session Chair: Frederik Armknecht | | | |
| 9:00<br>-<br>10:30 | Dynamic Cube Attacks Revisited, with Applications to Grain-128a | Willi Meier | 30 min |
| | Another View of the Division Property | Anne Canteaut | 30 min |
| | Invariant Subspace Attack Against Full Midori64 | Yu Sasaki | 30 min |
| 10:30-<br>11:00 | Coffee | | |
| Session Chair: Yu Sasaki | | | |
| 11:00<br>–<br>12:00 | On GCM-SIV | Tetsu Iwata | 30 min |
| | RIV and Resilient Authenticated Encryption | Stefan Lucks | 20 min |
| 12:15-<br>13:45 | Lunch | | |
| Session Chair: Anne Canteaut | | | |
| 14:00<br>-<br>15:30 | Memory Efficient Algorithms for Finding Needles in Haystacks | Adi Shamir | 30 min |
| | Bit Cryptanalysis on Symmetric Ciphers | Xiaoyun Wang | 30 min |
| | The Problem of Estimating the Variance of the Linear Cryptanalysis Test Statistic | Kaisa Nyberg | 30 min |
| 15:30-<br>16:00 | Coffee and Cake | | |
| Session Chair/Moderator: Dan Bernstein | | | |
| 16:00<br>-<br>(17:30) | Separating Modes and Primitives in CAESAR | Joan Daemen | 30 min |
| | Discussion on CAESAR | | |
| 18:00-<br>19:00 | Dinner | | |

## Tuesday, January 12

| Time | Title | Presenter | Duration |
|---|---|---|---|
| 7:30-9:00 | Breakfast | | |
| Session Chair: Jooyoung Lee | | | |
| 9:00 - 10:30 | Key-Alternating PRFs and Provable Security of Stream Ciphers against Time-Memory-Data Tradeoff Attacks | Matthias Krause | 30 min |
| | Improved Masking for Tweakable Blockciphers with Applications to Authenticated Encryption | Bart Mennink | 25 min |
| | Tweaking Even-Mansour Ciphers | Benoît Cogliati | 30 min |
| 10:30-11:00 | Coffee | | |
| Session Chair: Bart Mennink | | | |
| 11:00 – 12:00 | Indifferentiability of Confusion-Diffusion Networks | John Steinberger | 60 min |
| 12:15-13:45 | Lunch | | |
| Moderation: Adi Shamir | | | |
| 14:30-15:30 | Discussion on Attacks | | |
| 15:30-16:00 | Coffee and Cake | | |
| Session Chair: John Steinberger | | | |
| 16:00 - 18:00 | Even-Mansour type ciphers based on involutions | Jooyoung Lee | 20 min |
| | Even-Mansour cipher analysis reduced to the generalized birthday problem | Ivica Nikolic | 25 min |
| | Transitivity aspects of the (iterated) Even-Mansour cipher | Ernst Schulte-Geers | 30 min |
| 18:00-19:00 | Dinner | | |

## Wednesday, January 13

| Time | Title | Presenter | Duration |
|---|---|---|---|
| 7:30-9:00 | Breakfast | | |
| Session Chair: Nicky Mouha | | | |
| 9:00 - 10:30 | Polytopic cryptanalysis | Tyge Tiessen | 20 min |
| | Linear Cryptanalysis: Some bizarre bias distributions | Gregor Leander | 10 min |
| | Universal Multidimensional and Multiple Zero-Correlation Cryptanalysis | Meiqin Wang | 20 min |
| | Key-Recovery Attack on the ASASA Cryptosystem with Expanding S-Boxes | Henri Gilbert | 30 min |
| 10:30-11:00 | Coffee | | |
| Session Chair: Christian Rechberger | | | |
| 11:00 – 12:00 | Low-Energy Block Ciphers | Andrey Bogdanov | 20 min |
| | Some Results on the GOST Block Ciphers | Orr Dunkelman | 20 min |
| 12:15-13:45 | Lunch | | |
| Hike | | | |
| 15:30-16:00 | Coffee and Cake | | |
| Free for discussions | | | |
| 18:00-19:00 | Dinner | | |

## Thursday, January 14

| Time | Title | Presenter | Duration |
|---|---|---|---|
| 7:30-9:00 | Breakfast | | |
| Session Chair/Moderator: Orr Dunkelman | | | |
| 9:00 - 10:30 | S-Box Reverse-Engineering: Recovering Design Criteria, Hidden Structures and New Boolean Function Results | Léo Perrin | 30 min |
| | Simpira | Nicky Mouha | 20 min |
| | Discussion on Secret Agency Crypto Standards | | 40 min |
| 10:30-11:00 | Coffee | | |
| Session Chair: Gregor Leander | | | |
| 11:00 – 12:00 | New Attacks on Hash function Combiners | Itai Dinur | 30 min |
| | Transcipt Collision Attacks against TLS | Gaëtan Leurent | 25 min |
| 12:15-13:45 | Lunch | | |
| Session Chair: | | | |
| 14:00 - 15:30 | Egalitarian computing: how to establish a level playing field with hash functions and NP-hard problems | Dmitry Khovratovich | 30 min |
| | New Publication Model for FSE | Anne Canteaut | 30 min |
| | MAC with low computation overhead | Kazuhiko Minematsu | 30 min |
| 15:30-16:00 | Coffee and Cake | | |
| Session Chair: Bart Preneel | | | |
| 16:00 - 18:00 | Some Application of Symmetric Cryptography in Multi Party Computation | Elena Andreeva | 10 min |
| | A new cryptographic hash function design below 1 cycle per byte for short inputs | Christian Rechberger | 30 min |
| | Revisiting Structure Graph and Its Applications to CBC-MAC and EMAC | Mridul Nandi | 25 min |
| | Second Preimage Attacks against Dithered Hash Functions with Practical Online Memory Complexity | Orr Dunkelman | 25 min |
| 18:00-19:00 | Dinner | | |

## Friday, January 15

| Time | Title | Presenter | Duration |
|---|---|---|---|
| 7:30-9:00 | Breakfast | | |
| Session Chair: Stefan Lucks | | | |
| 9:20 - 10:35 | Provable Security Evaluation of Structures against Impossible Differential Cryptanalysis | Jian Guo | 15 min |
| | On Ciphers that Continuously Access the Non-Volatile Key | Frederik Armknecht | 30 min |
| | Directly Evaluating Multi-collisions and Improving Security Bounds | Kan Yasuda | 30 min |
| 10:35-11:00 | Coffee | | |
| Session Chair: Kan Yasuda | | | |
| 11:00 – 12:00 | Some challenges in heavyweight cipher design | Dan Bernstein | 30 min |
| | Mirror Theory and Cryptography | Jacques Patarin | 30 min |
| 12:15-13:45 | Lunch | | |