Program of DIAC 2016

Sunday, September 25, 2016

17:30-20:00 Registration (4F, Oh-en Room)

18:00-20:00 Welcome reception (light meal and drink)
(4F, Oh-en Room)

Monday, September 26, 2016

9:00- Registration (4F, Sakura Room)

9:25- 9:30 Opening remarks (4F, Sakura Room)

9:30-10:45 Session 1 (25min * 3 talks, 1h 15min) (4F, Sakura Room)

10:45-11:15 Break

11:15-12:35 Session 2 (20min * 4 talks, 1h 20min) (4F, Sakura Room)

12:40-14:00 Lunch (2F, Brasserie The Terrace)

14:00-15:15 Session 3 (25min * 3 talks, 1h 15min) (4F, Sakura Room)

15:15-15:45 Break

15:45-16:45 Session 4 (20min * 3 talks, 1h) (4F, Sakura Room)

Tuesday, September 27, 2016

9:00- Registration (4F, Sakura Room)

9:30-10:45 Session 5 (25min * 3 talks, 1h 15min) (4F, Sakura Room)

10:45-11:15 Break

11:15-12:35 Session 6 (20min * 4 talks, 1h 20min) (4F, Sakura Room)

12:40-14:00 Lunch (1F, The Gallery)

14:00-15:15 Session 7 (25min * 3 talks, 1h 15min) (4F, Sakura Room)

15:15-15:45 Break

15:45-16:35 Session 8 (discussion, 50min) (4F, Sakura Room)

_*_*_*_*_

Sunday, September 25, 2016

17:30-20:00 Registration

18:00-20:00 Welcome reception (light meal and drink)

_*_*_*_*_

Monday, September 26, 2016

9:00- Registration

9:25- 9:30 Opening remarks

Session 1 - CAESAR Candidates Analysis (Chair: Carlos Cid)

- 9:30-9:55 More on the Automatic Search for Differential Trails in NORX
  Vesselin Velichkov
- 9:55-10:20 Fault Based Almost Universal Forgeries on CLOC and SILC
  Debapriya Basu Roy, Avik Chakraborti, Donghoon Chang, S V Dilip Kumar, Debdeep Mukhopadhyay, and Mridul Nandi
- 10:20-10:45 Authenticated Encryption with Variable Stretch
  Reza Reyhanitabar, Serge Vaudenay, and Damian Vizár

10:45-11:15 Break

Session 2 - CAESAR Round 3 Candidates I (Chair: Yu Sasaki)

- 11:15-11:35 Ascon
  Christoph Dobraunig, Maria Eichlseder, Florian Mendel, and Martin Schlaffer
- 11:35-11:55 On Tiaoxin-346
  Ivica Nikolić
- 11:55-12:15 Third round updates of AEGIS
  Hongjun Wu and Bart Preneel (talk by Tao Huang)
- 12:15-12:35 Third round updates of MORUS
  Hongjun Wu and Tao Huang

12:40-14:00 Lunch

Session 3 - Hardware Implementation (Chair: Tanja Lange)

- 14:00-14:25 Toward Fair and Comprehensive Benchmarking of CAESAR

Candidates in Hardware: Standard API, High-Speed Implementations in VHDL/Verilog, and Benchmarking Using FPGAs

Ekawat Homsirikamol, William Diehl, Ahmed Ferozpuri, Farnoud Farahmand, Michael X. Lyons, Panasayya Yalla, and Kris Gaj

- 14:25-14:50 Enhancing CAESAR Hardware API Support for Lightweight Architectures

  Panasayya Yalla, Jens-Peter Kaps, Fabrizio De Santis, and Michael Tempelmeier

- 14:50-15:15 An Alternative Approach to Hardware Benchmarking of CAESAR Candidates Based on the Use of High-Level Synthesis Tools

  Ekawat Homsirikamol and Kris Gaj

15:15-15:45 Break

Session 4 - CAESAR Round 3 Candidates II (Chair: Serge Vaudenay)

- 15:45-16:05 Third round updates of ACORN

  Hongjun Wu (talk by Tao Huang)

- 16:05-16:25 Third round updates of JAMBU

  Hongjun Wu and Tao Huang

- 16:25-16:45 Updates on CLOC and SILC Version 3

  Tetsu Iwata, Kazuhiko Minematsu, Jian Guo, Sumio Morioka, and Eita Kobayashi

-*-*-*-*-

Tuesday, September 27, 2016

9:00- Registration

Session 5 - Software Implementation and Analysis of Ciphers (Chair: Ivica Nikolić)

- 9:30-9:55 Software Benchmarking of the 2nd round CAESAR Candidates

  Ralph Ankele and Robin Ankele

- 9:55-10:20 A New Improved Key-Scheduling for Khudra

  Rajat Sadhukhan, Souvik Kolay, Shashank Srivastava, and Debdeep Mukhopadhyay

- 10:20-10:45 Exact Security Analysis of Hash-then-Mask Type Probabilistic

MAC Constructions

Avijit Dutta, Ashwin Jha, and Mridul Nandi

10:45-11:15 Break

Session 6 - CAESAR Round 3 Candidates III (Chair: Kris Gaj)

- 11:15-11:35 AES-OTR v3

  Kazuhiko Minematsu

- 11:35-11:55 Deoxys

  Jérémy Jean, Ivica Nikolić, Thomas Peyrin, and Yannick Seurin

- 11:55-12:15 COLM

  Elena Andreeva, Andrey Bogdanov, Atul Luykx, Bart Mennink, Elmar Tischhauser, Kan Yasuda, Nilanjan Datta, and Mridul Nandi

- 12:15-12:35 Update on AEZ v4

  Phillip Rogaway

12:40-14:00 Lunch

Session 7 – Proposals (Chair: Shoichi Hirose)

- 14:00-14:25 An Online Authenticated Encryption scheme with an Optimal Single-Keyed Inverse-Free Construction

  Ritam Bhaumik and Mridul Nandi

- 14:25-14:50 Blockcipher-based Authenticated Encryption: How Small Can We Go?

  Avik Chakraborti, Tetsu Iwata, Kazuhiko Minematsu, and Mridul Nandi

- 14:50-15:15 A New Look at Counters: Don't Run Like Marathon in a Hundred Meter Race

  Avijit Dutta, Ashwin Jha, and Mridul Nandi

15:15-15:45 Break

Session 8 – Discussion (Chair: Daniel J. Bernstein)

15:45-16:35