RUHR-UNIVERSITÄT BOCHUM

Thanks and Best Paper Award

Gregor Leander, PC-Chair

Horst Görtz Institut für IT-Sicherheit

Basic Statistics

- 76 submissions received
- 28 accepted
- 3 reviews per paper
- 5 for PC-member papers

Program Committee

- Elena Andreeva
- Kazumaro Aoki
- Daniel Bernstein
- Celine Blondeau
- Andrey Bogdanov
- Anne Canteaut
- Joan Daemen
- Itai Dinur
- Orr Dunkelman
- Tetsu Iwata
- Orhun Kara
- Dmitry Khovratovich
- Gaetan Leurent
- Stefan Lucks
- Amir Moradi
- Maria Naya-Plasencia
- Svetla Nikova
- Thomas Peyrin
- Vincent Rijmen
- Martin Schlaeffer
- Tom Shrimpton
- Martijn Stam
- Francois-Xavier Standaert
- Vesselin Velichkov
- Tolga Yalcin

Thank you very much for all your work!

External Reviewers

- Farzaneh Abed
- Zahra Ahmadian
- Sedat Akleylek
- Tomer Ashur
- Gilles Van Assche
- Guido Bertoni
- Begul Bilgin
- Christina Boura
- Cagdas Calik
- Claude Carlet
- Mustafa Copan
- Hueseyin Demirci
- Christoph Dobraunig
- Maria Eichlseder
- Oguzhan Ersoy
- Muhammed Fethullah Esgin
- Matthieu Finiasz
- Christian Forler
- Benedikt Gierlichs
- Vincent Grosso
- Benoit Gerard
- Mehmet Emin Goenen
- Takanori Isobe
- Arpan Jati
- Jeremy Jean
- Anthony Journault
- Ferhat Karakoc
- Nathan Keller
- Thomas Korak
- Virgnie Lallemand
- Martin M. Lauridsen
- Wang Lei
- Eik List
- Atul Luykx
- Florian Mendel
- Bart Menning
- Bart Mennink
- Hristina Mihajloska
- Kazuhiko Minematsu
- Nicky Mouha
- Ivica Nikolic
- Ventzislav Nikov
- David Oswald
- Leo Perrin
- Thomas Pornin
- Santos Merino del Pozo
- Francesco Regazzoni
- Tolga Sakalli
- Somitra Sanadhya
- Yu Sasaki
- Falk Schellenberg
- Tobias Schneider
- Peter Schwabe
- Yannick Seurin
- Kyoji Shibutani
- Raphael Spreitzer
- Valentin Suder
- Fatih Sulak
- Ruggero Susella
- Junko Takahashi
- R. Seth Terashima
- Cihangir Tezcan
- Praveen Vadnala
- Kerem Varici
- Srinivas Vivek Venkatesh
- Qingju Wang
- Dai Watanabe
- Erich Wenger
- Jakob Wenzel
- Kan Yasuda
- Hirotaka Yoshida

Thank you very much for all your work!

General Chair

Endless

- **queries**
- **questions**
- **suggestions**

from me to Hüseyin DEMIRCI

Thank you very for your effort and patience

Invited Talks @ FSE 2015

hgi Horst Görtz Institut für IT-Sicherheit
RUB

Thanks to

Meltem Turan Sönmez

and

Jacob Applebaum

Best Paper FSE 2015

Based on a PC-vote

Two papers solicited to the JoC

Best Paper FSE 2015

Based on a PC-vote

Two papers solicited to the JoC

Rotational Cryptanalysis of ARX Revisited

Dmitry Khovratovich, Ivica Nikolic, Josef Pieprzyk, Przemyslaw Sokolowski, Ron Steinfeld

Meet-in-the-Middle Attacks and Structural Analysis of Round-Reduced PRINCE

Patrick Derbez and Léo Perrin

Best Paper FSE 2015

Based on a PC-vote

hgi Horst Görtz Institut für IT-Sicherheit
RUB

Best Paper FSE 2015

Based on a PC-vote

Best Paper Award
FSE 2015

The program committee of FSE 2015 is glad to present
the best paper award of the conference to

Yuichi Niwa, Keisuke Ohashi,
Kazuhiko Minematsu, and **Tetsu Iwata**

for their contribution entitled

GCM Security Bounds Reconsidered

Istanbul, March 2015

Gregor Leander, Program Chair