

Thanks from the program chairs  
and best paper awards

Carlos Cid and Christian Rechberger

# Basic stats

- 99 submissions
- 31 accepted papers

# Thanks to the Committee

- Martin Albrecht
- Elena Andreeva
- Kazumaro Aoki
- Frederik Armknecht
- Daniel J. Bernstein
- John Black
- Anne Canteaut
- Joan Daemen
- Christophe De Cannière
- Orr Dunkelman
- Martin Hell
- Dmitry Khovratovich
- Gregor Leander
- Subhamoy Maitra
- Mitsuru Matsui
- Florian Mendel
- Svetla Nikova
- Elisabeth Oswald
- Thomas Peyrin
- Josef Pieprzyk
- Martijn Stam
- François-Xavier Standaert
- Serge Vaudenay
- Hongbo Yu

# Thanks to the subreviewers

- Hoda A. Alkhzaimi
- Gilles Van Assche
- Jean-Philippe Aumasson
- Subhadeep Banik
- Harry Bartlett
- Asli Bay
- Guido Bertoni
- Begul Bilgin
- Andrey Bogdanov
- Sonia Bogos
- Christina Boura
- Daniel Cabarcas
- Claude Carlet
- Anupam Chattopadhyay
- Alexandre Duc
- François Durvaux
- Maria Eichlseder
- Sebastian Faust
- Vincent Grosso
- Sourav Sen Gupta
- Jialin Huang
- Andreas Hülsing
- Takanori Isobe
- Tetsu Iwata
- Guo Jian
- Philipp Jovanovic
- Angela Jäschke
- Pierre Karpman
- Elif Kavun
- Nathan Keller
- Stéphanie Kerckhof
- Lars Knudsen
- Matthias Krause
- Stefan Kölbl
- Martin M. Lauridsen
- Gaëtan Leurent
- Zhiqiang Liu
- Atul Luykx
- Daniel Martin
- Bart Mennink
- Vasily Mikhalev
- Paweł Morawiecki
- Nicky Mouha
- Tomislav Nad
- Mridul Nandi
- Ivica Nikolic
- Kaisa Nyberg
- Kenny Paterson
- Michaël Peeters
- Ludovic Perret
- Christiane Peters
- Romain Poussier
- Santos Merino Del Pozo
- Francesco Regazzoni
- Francesco Regazzoni
- Reza Reyhanitabar
- Vincent Rijmen
- Phillip Rogaway
- Santanu Sarkar
- Martin Schläffer
- Peter Schwabe
- Takeshi Shimoyama
- Paul Stankovski
- Ron Steinfeld
- Petr Sušil
- Seth Terashima
- Tyge Tiessen
- Kerem Varici
- Vesselin Velichkov
- Huaxiong Wang
- Lei Wang
- Meiqin Wang
- Quingju Wang
- Gaven Watson
- Tolga Yalcin
- Yusi (James) Zhang

# Two best paper awards

- Differential-Linear Cryptanalysis Revisited  
*Céline Blondeau, Gregor Leander and Kaisa Nyberg*
- Direct Construction of Recursive MDS  
Diffusion Layers using Shortened BCH Codes  
*Daniel Augot and Matthieu Finiasz*