# FSE 2019

**Yu Sasaki** (NTT Secure Platform Laboratories)

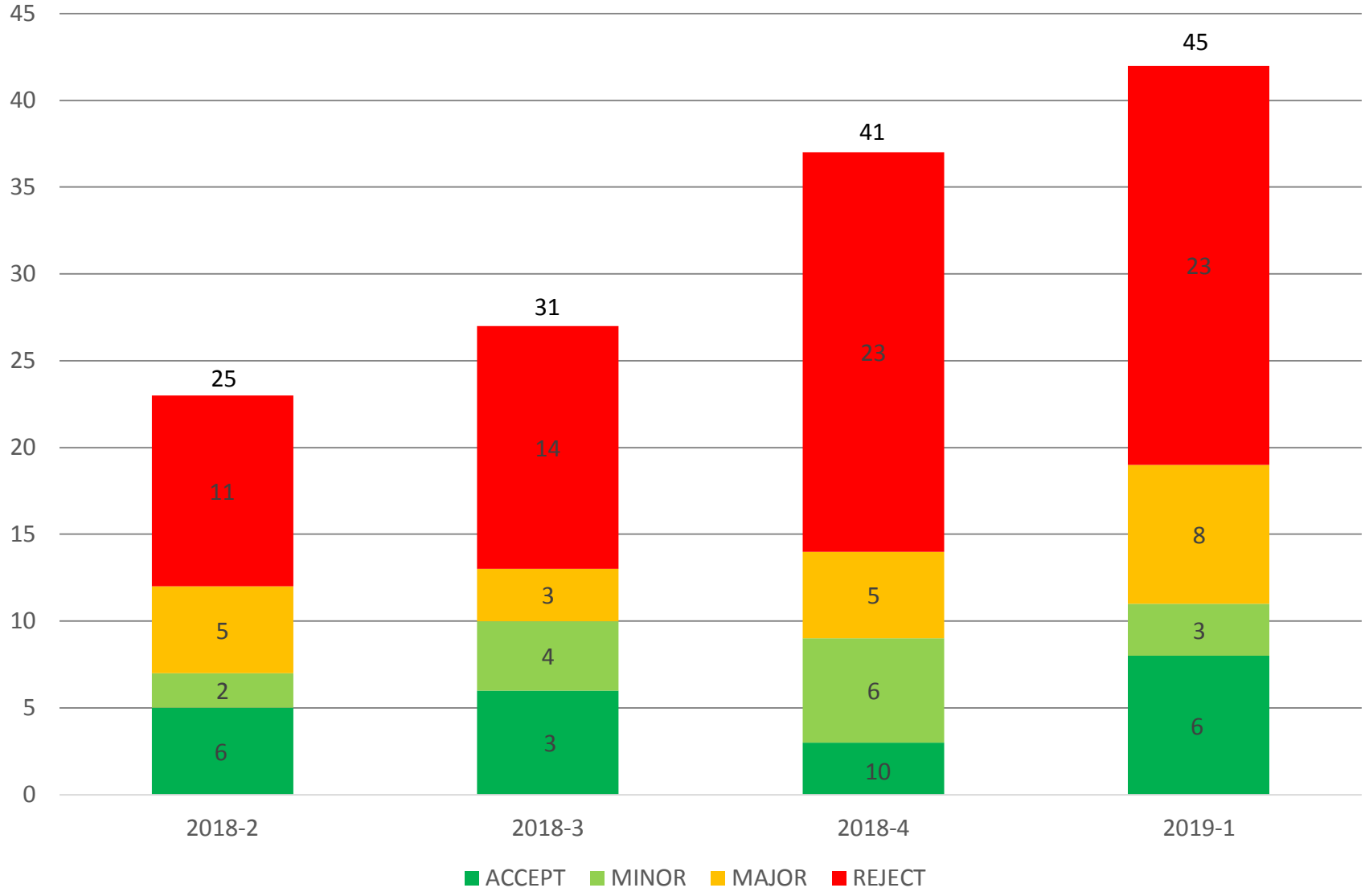
**Florian Mendel** (Infineon Technologies)

**program co-chairs**

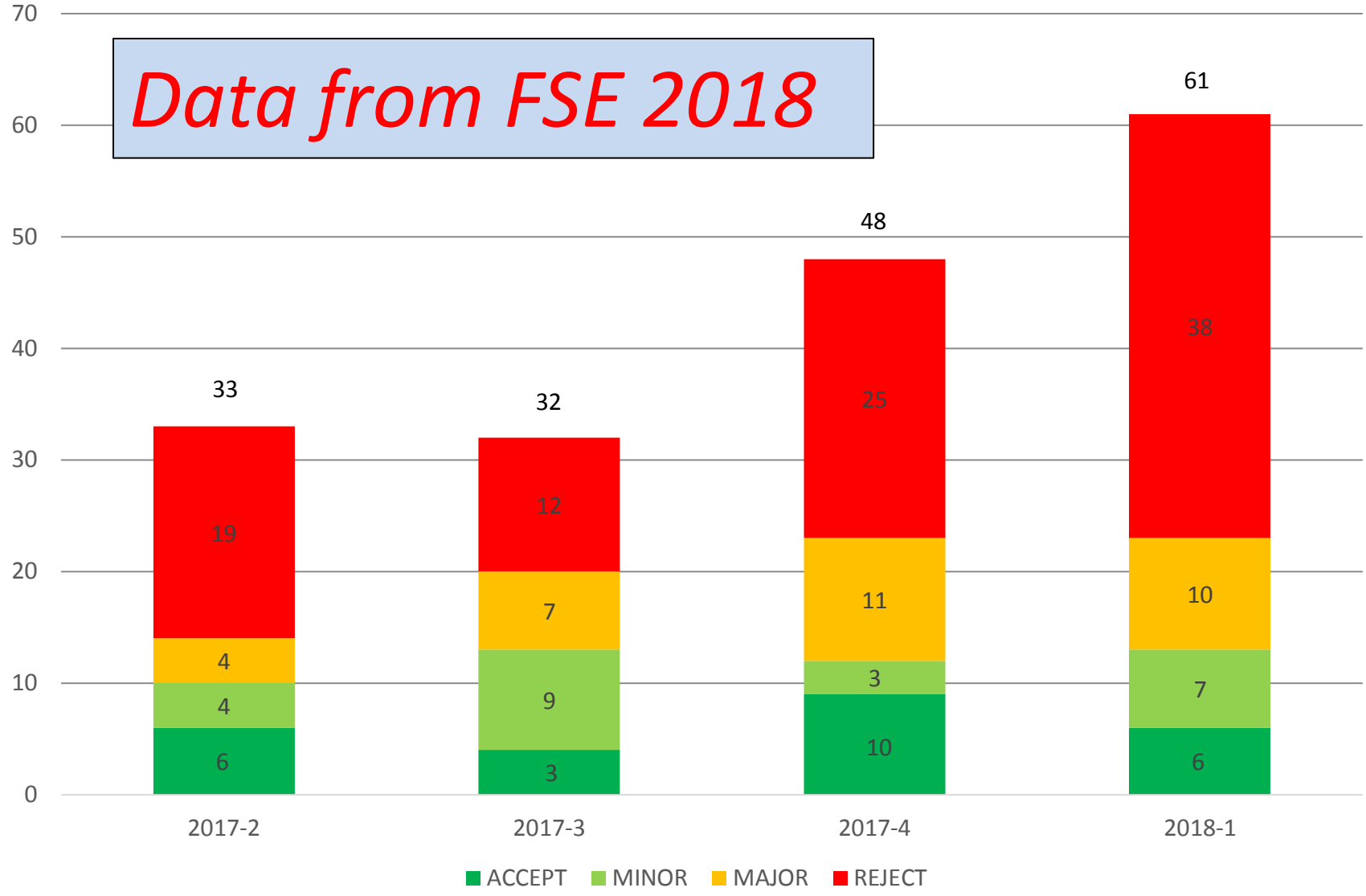
# IACR Transactions Symmetric Cryptology (ToSC)

- 4 submission deadlines per year
- Rebuttal phase
- Decision after 2 months
  - ACCEPT
  - MINOR REVISION
  - MAJOR REVISION
  - REJECT
- Long papers
- SoK papers
- Hope to get included in Thomson ISI in 2020

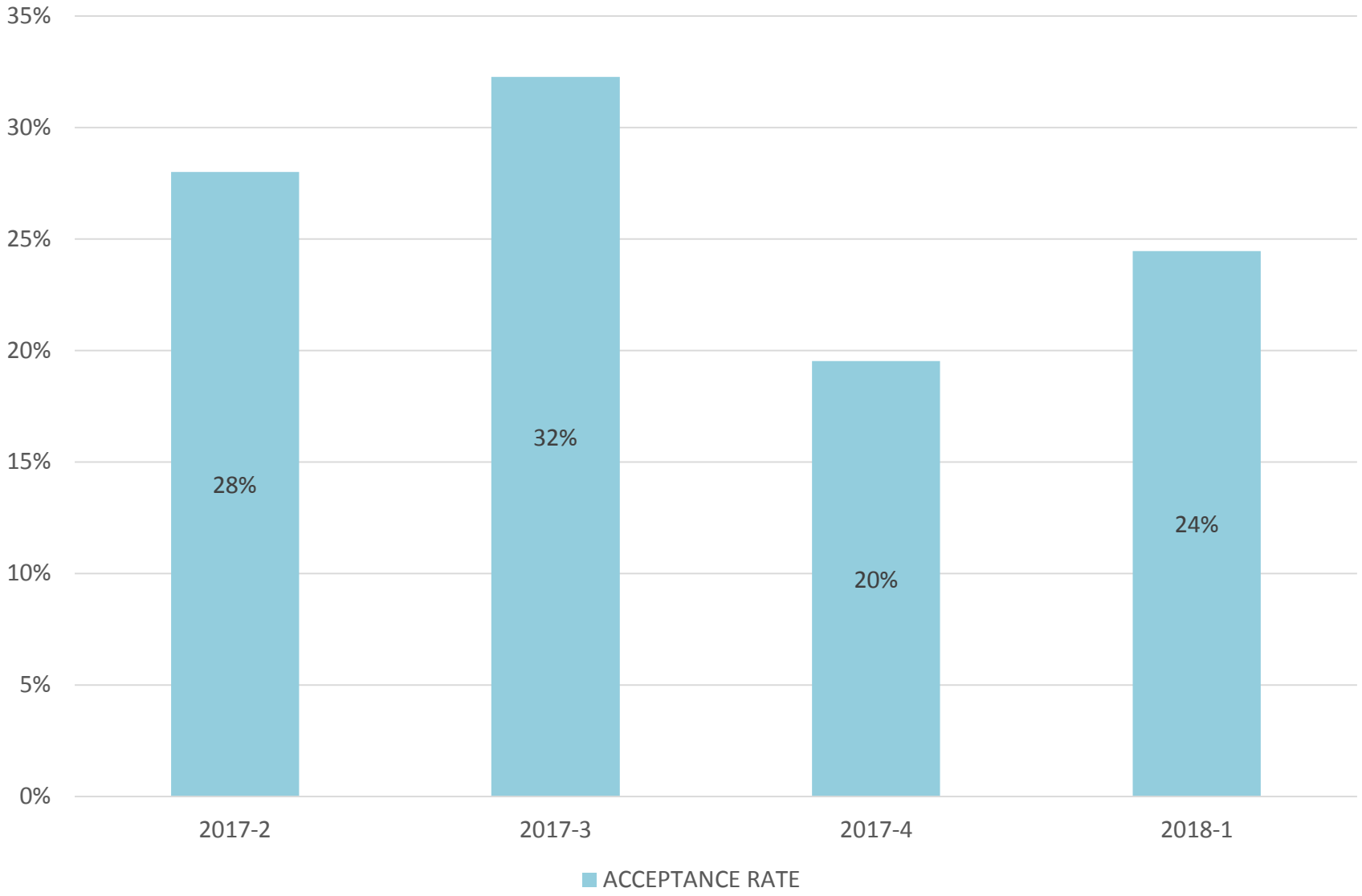
# Statistics: 142 submissions (122 new)



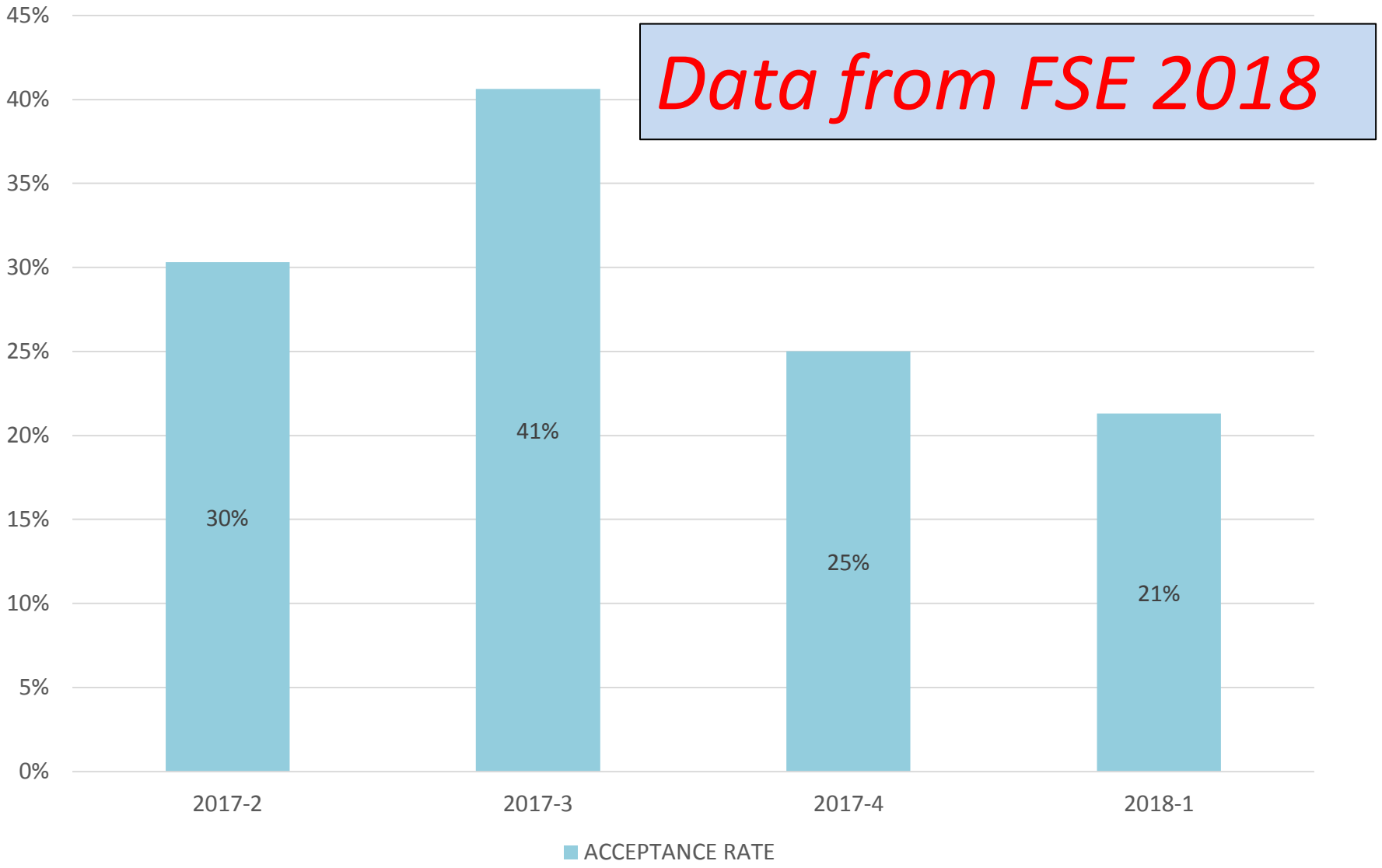
# Statistics: 174 submissions (148 new)



# Acceptance rate: 25% (or 29%)

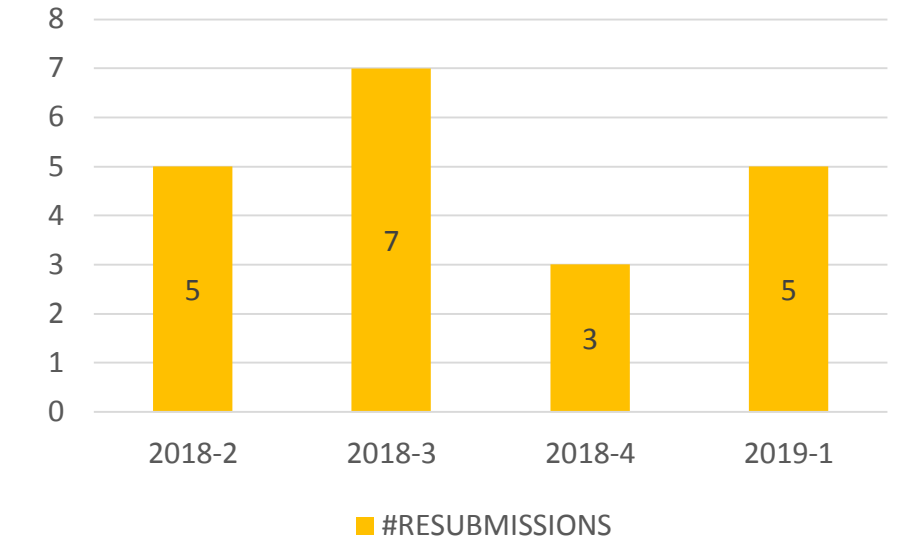


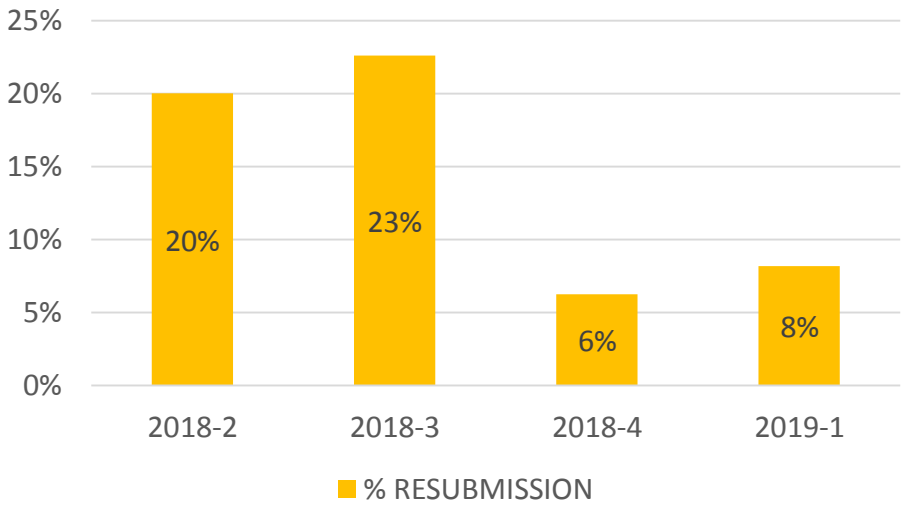
# Acceptance rate: 28% (or 32%)




*Data from FSE 2018*

# Resubmissions after major revision



# New Publication Model

- Cite ToSC from other ISI Journals (DCC, JoC, LNCS)
- Everything published has been reviewed: if you need more than 20 pages, go for a long paper
- Want also SoK (systematization of knowledge)
- High work load for revisions
- Style file may need some minor improvements but please don’t hack the LaTeX
- Camera ready means camera ready
- Use standard bib file: DBLP or https://cryptobib.di.ens.fr/

# New Challenge This Year

ToSC 2018 Volume 2
- Submission: 1 March 2018
- Rebuttal: 4-7 April 2018
- Decision: 1 May 2018

ToSC 2018 Volume 3
- Submission: 1 June 2018
- Rebuttal: 4-7 July 2018
- Decision: 1 August 2018

ToSC 2018 Volume 4
- Submission: 1 September 2018
- Rebuttal: 4-7 October 2018
- Decision: 1 November 2018

ToSC 2019 Volume 1
- Submission: 23 November 2018
- Rebuttal: 2-6 January 2019
- Decision: 23 January 2019

ToSC 2019 Volume 2
- Submission: 1 March 2019
- Rebuttal: 8-11 April 2019
- Decision: 1 May 2019

ToSC 2019 Volume 3
- Submission: 1 June 2019
- Rebuttal: 8-11 July 2019
- Decision: 1 August 2019

ToSC 2019 Volume 4
- Submission: 1 September 2019
- Rebuttal: 8-11 October 2019
- Decision: 1 November 2019

ToSC 2020 Volume 1
- Submission: 23 November 2019
- Rebuttal: 2-6 January 2020
- Decision: 23 January 2020

# Program Committee

Frederik Armknecht
Subhadeep Banik
Daniel J. Bernstein
Alex Biryukov
Christina Boura
Anne Canteaut
Carlos Cid
Joan Daemen
Patrick Derbez
Itai Dinur
Christoph Dobraunig
Orr Dunkelman
Maria Eichlseder
Jian Guo
Takanori Isobe
Tetsu Iwata
Jérémy Jean
Pierre Karpman
Nathan Keller
Stefan Kölbl
Virginie Lallemand
Gregor Leander
Jooyoung Lee
Gaëtan Leurent
Stefan Lucks
Subhamoy Maitra
Willi Meier
Bart Mennink
Nicky Mouha
María Naya-Plasencia
Samuel Neves
Ivica Nikolić
Kaisa Nyberg
Bart Preneel
Arnab Roy
Martin Schläffer
Yannick Seurin
Hadi Soleimany
Ling Song
Marc Stevens
Elmar Tischhauser
Yosuke Todo
Gilles Van Assche
Damian  Visár
Lei Wang

# Thank you

General chair: Jérémy Jean

Invited speaker: Gregor Leander, María Naya-Plasencia, Jian Guo

Rump session chairs: Pierre Karpman and Brice Minaud

Sponsors:


PÔLE D'EXCELLENCE CYBER

CryptoExperts
WE INNOVATE TO SECURE YOUR BUSINESS

ENS | PSL

THALES

IDEMIA
augmented identity

îledeFrance

Inria

Ledger

cybercrypt
a world immune to cyber attacks

# Thank you

Managing Editor ToSC: Gregor Leander

Technical support: Shai Halevi, Friedrich Wiemer

FSE Steering Committee:

- Anne Canteaut, chair
- Orr Dunkelman
- Tetsu Iwata
- Gregor Leander
- Florian Mendel
- María Naya-Plasencia
- Thomas Peyrin
- Bart Preneel
- Yu Sasaki

# Thank you!

# Best Paper Award

## Partitions in the S-Box of Streebog and Kuznyechik

Léo Perrin