# *Program chair report*

Itai Dinur  Gaëtan Leurent  Yu Sasaki

ToSC Co-Editors-in-Chief

FSE 2020

# *IACR Transactions on Symmetric Cryptology (ToSC)*

- FSE follows a hybrid journal/conference model since 2016
  - Open access journal: IACR ToSC
  - Published by Ruhr University Bochum
  - Indexed by Scopus, DOAJ
  - Selected for inclusion in the Web of Science
- 4 issues per year
  - Deadline every 3 months
  - Decision after 2 months (for regular papers)
- Rebuttal phase
- Journal-style decicions
  - Accept
  - Minor revision (conditional accept with shepherd)
  - Major revision (evaluated at the next cycle)
  - Reject-and-resubmit (can resubmit after two cycles)
  - Reject (cannot resubmit in the next two cycles)
- We also welcome Systematization of Knowledge papers (SoK), addendum and errata

# *ToSC schedule with COVID*

| Submission: | ToSC Issue | Conference |
|---|---|---|
| November $y-2$: | ToSC $y-1$ issue 1 | |
| March $y-1$: | ToSC $y-1$ issue 2 | FSE $y$ (March $y$) |
| June $y-1$: | ToSC $y-1$ issue 3 | |
| September $y-1$: | ToSC $y-1$ issue 4 | |
| November $y-1$: | ToSC $y$ issue 1 | |
| March $y$: | ToSC $y$ issue 2 | FSE $y+1$ (March $y+1$) |
| June $y$: | ToSC $y$ issue 3 | |
| September $y$: | ToSC $y$ issue 4 | |
| November $y$: | ToSC $y+1$ issue 1 | |
| March $y+1$: | ToSC $y+1$ issue 2 | FSE $y+2$ (March $y+2$) |
| June $y+1$: | ToSC $y+1$ issue 3 | |
| September $y+1$: | ToSC $y+1$ issue 4 | |
| ... | | |

# *ToSC schedule with COVID*

| Submission: | ToSC Issue | Conference |
|---|---|---|
| November 2018: | ToSC 2019 issue 1 | |
| March 2019: | ToSC 2019 issue 2 | FSE 2020 (March 2020) |
| June 2019: | ToSC 2019 issue 3 | |
| September2019: | ToSC 2019 issue 4 | |
| November 2019: | ToSC 2020 issue 1 | |
| March 2020: | ToSC 2020 issue 2 | FSE 2021 (March 2021) |
| June 2020: | ToSC 2020 issue 3 | |
| September2020: | ToSC 2020 issue 4 | |
| November 2020: | ToSC 2021 issue 1 | |
| March 2021: | ToSC 2021 issue 2 | FSE 2022 (March 2022) |
| June 2021: | ToSC 2021 issue 3 | |
| September2021: | ToSC 2021 issue 4 | |
| ... | | |

1st COVID wave 2nd COVID wave

# *ToSC schedule with COVID*

| Submission: | ToSC Issue | Conference |
|---|---|---|
| November 2018: | ToSC 2019 issue 1 | |
| March 2019: | ToSC 2019 issue 2 | |
| June 2019: | ToSC 2019 issue 3 | |
| September2019: | ToSC 2019 issue 4 | FSE 2020 (~~March 2020~~) November 2020 |
| November 2019: | ToSC 2020 issue 1 | 1st COVID wave 2nd COVID wave |
| March 2020: | ToSC 2020 issue 2 | |
| June 2020: | ToSC 2020 issue 3 | |
| September2020: | ToSC 2020 issue 4 | FSE 2021 (March 2021) |
| November 2020: | ToSC 2021 issue 1 | |
| March 2021: | ToSC 2021 issue 2 | |
| June 2021: | ToSC 2021 issue 3 | |
| September2021: | ToSC 2021 issue 4 | FSE 2022 (March 2022) |
| ... | | |

# *ToSC schedule with COVID*

| Submission: | ToSC Issue | Conference |
|---|---|---|
| November 2018: | ToSC 2019 issue 1 | |
| March 2019: | ToSC 2019 issue 2 | |
| June 2019: | ToSC 2019 issue 3 | |
| September2019: | ToSC 2019 issue 4 | FSE 2020 (~~March 2020~~) November 2020 |
| November 2019: | ToSC 2020 issue 1 | 1st COVID wave 2nd COVID wave |
| March 2020: | ToSC 2020 issue 2 | |
| June 2020: | ToSC 2020 issue 3 | |
| September2020: | ToSC 2020 issue 4 | FSE 2021 (March 2021) |
| November 2020: | ToSC 2021 issue 1 | |
| March 2021: | ToSC 2021 issue 2 | |
| June 2021: | ToSC 2021 issue 3 | |
| September2021: | ToSC 2021 issue 4 | FSE 2022 (March 2022) |
| ... | | |

# *ToSC schedule with COVID*

| Submission: | ToSC Issue | Conference |
|---|---|---|
| November 2018: | ToSC 2019 issue 1 | |
| March 2019: | ToSC 2019 issue 2 | |
| June 2019: | ToSC 2019 issue 3 | |
| September2019: | ToSC 2019 issue 4 | FSE 2020 (~~March 2020~~) November 2020 |
| November 2019: | ToSC 2020 issue 1 | 1st COVID wave 2nd COVID wave |
| March 2020: | ToSC 2020 issue 2 | |
| June 2020: | ToSC 2020 issue 3 | |
| September2020: | ToSC 2020 issue 4 | FSE 2021 (March 2021) |
| November 2020: | ToSC 2021 issue 1 | Next FSE? Wait for next talk ... |
| March 2021: | ToSC 2021 issue 2 | 3rd COVID wave? |
| June 2021: | ToSC 2021 issue 3 | |
| September2021: | ToSC 2021 issue 4 | FSE 2022 (March 2022) |
| ... | | |

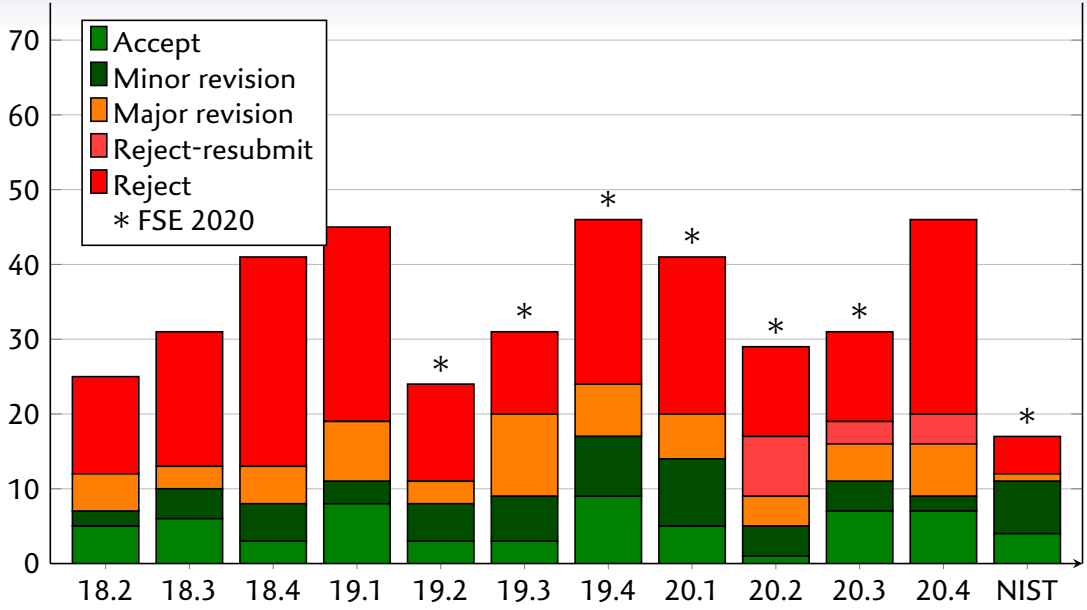
# *New in ToSC (2020)*

- Special Issue on the NIST lightweight standardization process
- New review system with HotCRP
- No page limit for long papers
  - But long papers are first evaluated on the merit/length ratio
- New decision: "Reject-and-resubmit"
  - Paper with some potential, but significant issues to address.
- Addendum and errata papers

# *FSE 2020 program*

- 64 papers from ToSC 2019 (2-4) and 2020 (1-3)
- 12 papers from the Special issue on the NIST Lightweight Standardisation Process
- 2 Invited talks
  - Kazuhiko Minematsu
  - Thomas Peyrin
- 2 Ask Me Anything sessions
  - Joan Daemen
  - Kaisa Nyberg
- Rump Session
  - Chairs: Bart Mennink, Brice Minaud

# Decision statistics



# *Acceptance rate*

- 202 submissions for ToSC 2019 (2-4) and 2020 (1-3)
  - 32% accepted (64 papers)
- 158 new submissions
  - 40% accepted?
- 44 major revisions received (1 not submitted)
  - 35 accepted
  - 7 rejected
  - 2 major revision

# *Program committee (2019)*

- Frederik Armknecht
- Tomer Ashur
- Subhadeep Banik
- Zhenzhen Bao
- Christof Beierle
- Christina Boura
- Anne Canteaut
- Carlos Cid
- Joan Daemen
- Patrick Derbez
- Christoph Dobraunig
- Orr Dunkelman
- Maria Eichlseder
- Pierre-Alain Fouque
- Takanori Isobe
- Jérémy Jean
- Pierre Karpman
- Stefan Kölbl
- Virginie Lallemand
- Gregor Leander
- Jooyoung Lee
- Stefan Lucks‘<
- Atul Luykx
- Willi Meier
- Florian Mendel
- Bart Mennink
- Brice Minaud
- Kazuhiko Minematsu
- Nicky Mouha
- Samuel Neves
- Kaisa Nyberg
- Léo Perrin
- Thomas Peyrin
- Bart Preneel
- Hadi Soleimany
- Ling Song
- Francois-Xavier Standaert
- Marc Stevens
- Siwei Sun
- Elmar Tischhauser
- Yosuke Todo
- Gilles Van Assche
- Damian Vizár
- Kan Yasuda

# *Program committee (2020)*

- Elena Andreeva
- Frederik Armknecht
- Tomer Ashur
- Subhadeep Banik
- Zhenzhen Bao
- Christof Beierle
- Patrick Derbez
- Christoph Dobraunig
- Orr Dunkelman
- Maria Eichlseder
- Vincent Grosso
- Jian Guo
- Takanori Isobe
- Tetsu Iwata
- Jérémy Jean
- Pierre Karpman
- Nathan Keller
- Stefan Kölbl
- Virginie Lallemand
- Gregor Leander
- Jooyoung Lee
- Stefan Lucks
- Willi Meier
- Brice Minaud
- Kazuhiko Minematsu
- Nicky Mouha
- Kaisa Nyberg
- Léo Perrin
- Thomas Peyrin
- Bart Preneel
- Yann Rotella
- Yannick Seurin
- Siang Meng Sim
- Hadi Soleimany
- Ling Song
- Siwei Sun
- Yosuke Todo
- Aleksei Udovenko
- Gilles Van Assche
- Damian Vizár
- Qingju Wang

# *Thank you*

- Managing Editor: Gregor Leander
- Technical support: Friedrich Wiemer, Phil Hebborn, Linda Groß
- Submission system: Shai Halevi, Kevin McCurley

- General Chair: Christina Boura
- Virtual Conference Organizers: Kevin McCurley, Kay McKelly
- FSE Steering Committee:
  - Anne Canteaut, chair
  - Bart Preneel
  - Orr Dunkelman
  - Tetsu Iwata
  - Gregor Leander
  - Florian Mendel
  - Maria Naya Plasencia
  - Thomas Peyrin
  - Yu Sasaki

# *Best paper award*

- Elected a best paper from ToSC 2019 (2-4) and 2020 (1)
- Planned to announce it in March...

# FSE 2020
# Best Paper Award

Yaobin Shen and Lei Wang

On Beyond-Birthday-Bound Security:
Revisiting the Development of
ISO/IEC 9797-1 MACs

Gaëtan Leurent and Yu Sasaki
Program Co-Chairs