NANYANG TECHNOLOGICAL UNIVERSITY

Thanks and Best Paper Award

Thomas Peyrin, FSE 2016 PC-chair
Nanyang Technological University
Singapore

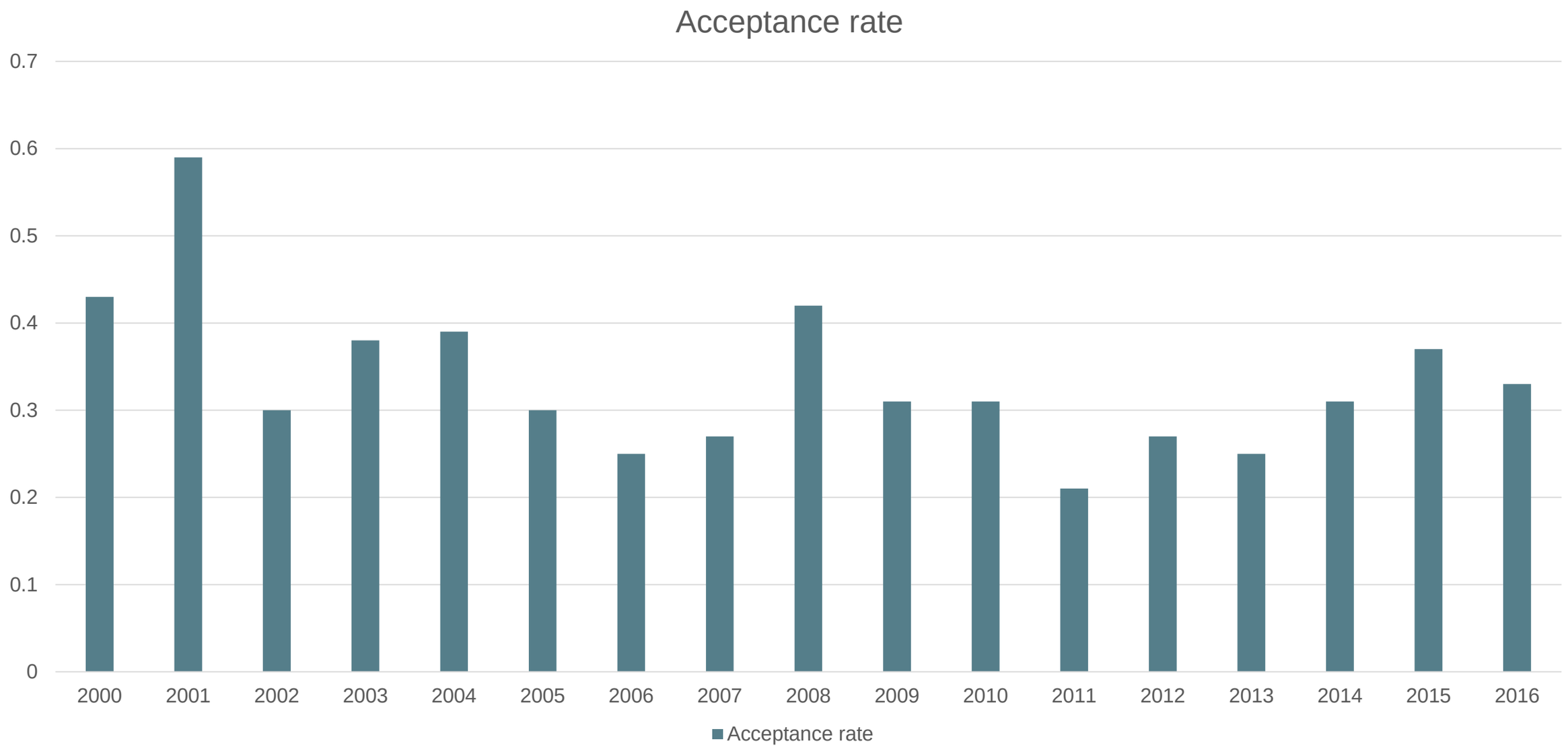
23rd International Conference on Fast Software Encryption

Basic Stats

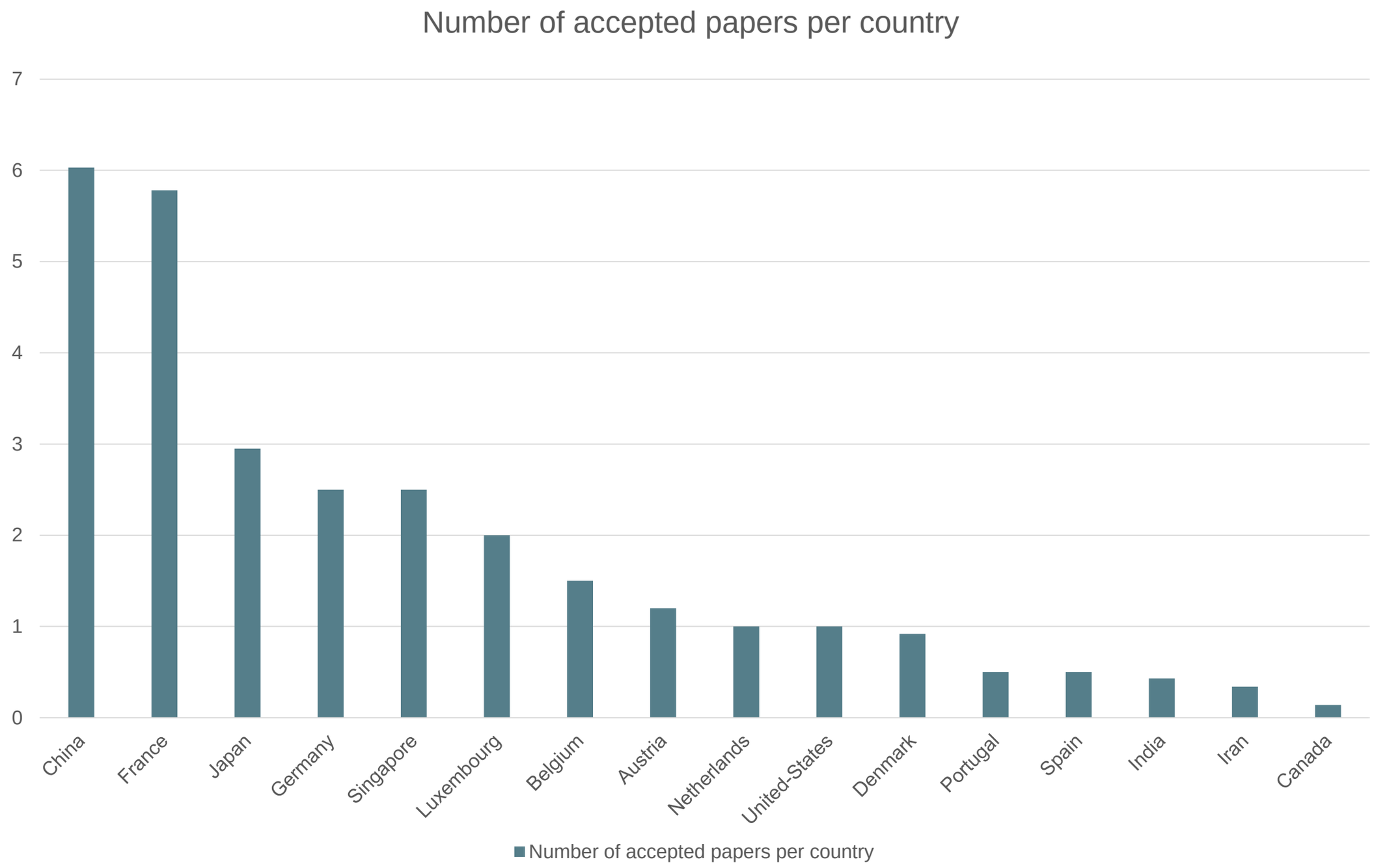
- **91 submissions** among which **86** were valid

Basic Stats

- **91 submissions** among which **86** were valid
- **29 accepted papers** (29/86 = 33.7% acceptance rate)



Accepted papers by country



Basic Stats

- **91 submissions** among which **86** were valid
- **29 accepted papers** (29/86 = 33.7% acceptance rate)
- **3** reviews per paper, **5** for PC-member papers

The Program Committee

- Alex Biryukov
- Christina Boura
- Céline Blondeau
- Itai Dinur
- Orr Dunkelman
- Takanori Isobe
- Tetsu Iwata
- Pascal Junod
- Gaëtan Leurent
- Florian Mendel
- Bart Mennink
- Amir Moradi
- Mridul Nandi
- Ivica Nikolić
- Svetla Nikova
- Kenny Paterson
- Christian Rechberger
- Yu Sasaki
- Yannick Seurin
- Thomas Shrimpton
- François-Xavier Standaert
- Marc Stevens
- Serge Vaudenay
- Lei Wang
- Meiqin Wang

Thanks A LOT for all your efforts !

The subreviewers

- Divesh Aggarwal
- Martin Albrecht
- Elena Andreeva
- Ralph Ankele
- Tomer Ashur
- Jean-Philippe Aumasson
- Thomas Baignères
- Subhadeep Banik
- Achiya Bar-On
- Georg T. Becker
- Christof Beierle
- Rishiraj Bhattacharaya
- Ritam Bhaumik
- Begül Bilgin
- Sonia Bogos
- Anne Canteaut
- Carlos Cid
- Joan Daemen
- Nilanjan Datta
- Jean Paul Degabriele
- Daniel Dinu
- Christoph Dobraunig
- Alexandre Duc
- Avijit Dutta
- Maria Eichlseder
- Sebastian Faust
- Matthieu Finiasz
- Thomas Fuhr
- Peter Gazi
- Lorenzo Grassi
- Vincent Grosso
- Jian Guo
- Harunaga Hiwatari
- Ashwin Jha
- Anthony Journault
- Pierre Karpman
- Elif Bilge Kavun
- Dmitry Khovratovich
- Handan Kilinç
- Miroslav Knezevic
- Stefan Koelbl
- Virginie Lallemand
- Martin M. Lauridsen
- Meicheng Liu
- Yunwen Liu
- Zhiqiang Liu
- Atul Luykx
- Marco Macchetti
- Subhamoy Maitra
- Santos Merino Del Pozo
- Sean Murphy
- Léo Paul Perrin
- Peter Pessl
- Jérôme Plût
- Romain Poussier
- Shahram Rasoolzadeh
- Francesco Regazzoni
- Jean-René Reinhard
- Oscar Reparaz
- Reza Reyhanitabar
- Bastian Richter
- Vincent Rijmen
- Arnab Roy
- Pascal Sasdrich
- Falk Schellenberg
- Tobias Schneider
- Jacob Schuldt
- Sourav Sengupta
- Kyoji Shibutani
- Siang Meng Sim
- Valentin Suder
- Tyge Tiessen
- Elmar Tischhauser
- Yosuke Todo
- Aleksei Udovenko
- Thomas Unterluggauer
- Thyla van der Merwe
- Kerem Varici
- Vesselin Velichkov
- Damian Vizár
- Wei Wang
- Alexander Wild
- Hongjun Wu
- Brecht Wyseur
- Guoyan Zhang
- Liting Zhang

Thanks A LOT for all your efforts !

The invited speaker

- **Henri Gilbert**:

  "On White-Box Cryptography"

Thanks for the great talk !

The General Chair

- **Gregor Leander**

Registration fees: $180 ($90 for students) !

Thanks for the great organisation !

Best Paper Award

And the award goes to …

Best Paper Award

And the award goes to …

Verifiable side-channel security of cryptographic implementations: constant-time MEE-CBC

José Bacelar Almeida, Manuel Barbosa,

Gilles Barthe, François Dupressoir

Invited to Journal of Cryptology

Stream ciphers: A Practical Solution for Efficient Homomorphic-Ciphertext Compression

Anne Canteaut, Sergiu Carpov, Caroline Fontaine, Tancrède Lepoint, María Naya-Plasencia, Pascal Paillier, Renaud Sirdey