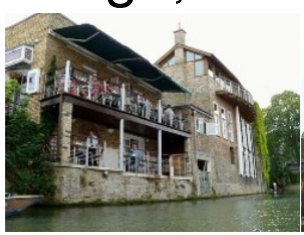
Eurocrypt 2012

David Pointcheval and Thomas Johansson

Ecole Normale Supérieure and Lund University

April 15–19, 2012 – Cambridge, UK




Review Process

- 32 PC members
- Submission deadline: September 30th
- 191 Submissions
- Review period: October 4th – November 7th
- 177 External reviewers
- 604 Reviews
- Discussion period: November 7th – December 7th
- 738 Messages
- Notification: December 7th
- 41 Accepted papers

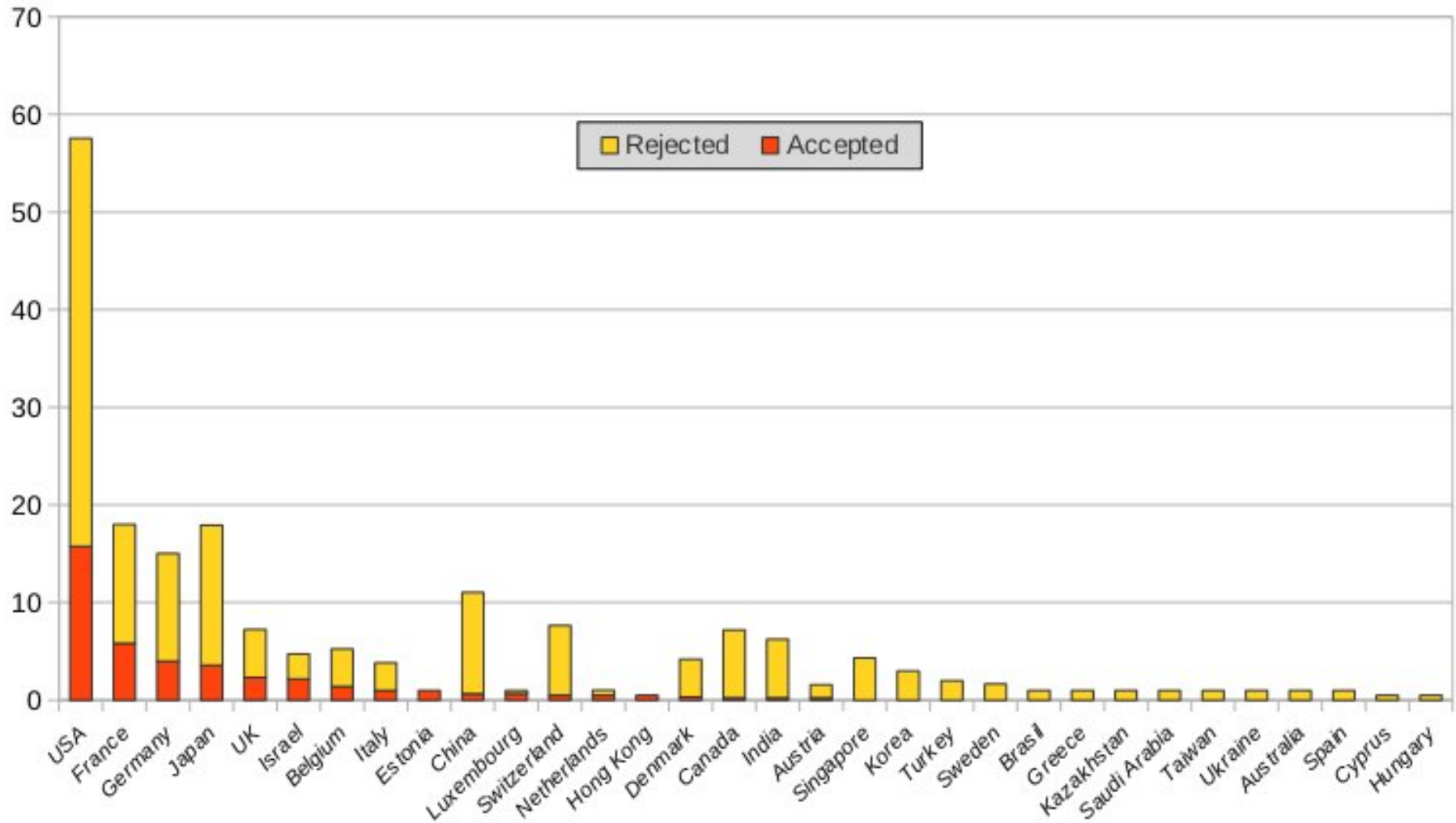
PC Members

Masayuki Abe
John Black
David Cash
Dario Catalano
Jean-Sébastien Coron
Orr Dunkelman
Marc Fischlin
Pierre-Alain Fouque
Steven Galbraith
Henri Gilbert
Louis Goubin
Jens Groth
Dennis Hofheinz
Tetsu Iwata
John Kelsey
Aggelos Kiayias
Arjen Lenstra
Benoit Libert
Yehuda Lindell
Kaisa Nyberg
Thomas Peyrin
Krzysztof Pietrzak
Vincent Rijmen
Thomas Ristenpart
Kazue Sako
Palash Sarkar
Igor Shparlinski
Martijn Stam
Vinod Vaikuntanathan
Ivan Visconti
Xiaoyun Wang
Duncan Wong

External Reviewers

Michel Abdalla
Adi Akavia
Joël Alwen
Elena Andreeva
Giuseppe Ateniese
Nuttapong Attrapadung
Man Ho Au
Paul Baecher
Thomas Baignères
Foteini Baldimtsi
Paulo Barreto
Aurélie Bauer
Stephanie Bayer
David Bernhard
Daniel J. Bernstein
Sanjay Bhattacherjee
Joppe Bos
Christoph Bösch
Zvika Brakerski
Billy Brumley
Christina Brzuska
Jesper Buus Nielsen
Ran Canetti
Debrup Chakraborty
Nishanth Chandran
Donghoon Chang
Lidong Chen
Jung Hee Cheon
Céline Chevalier
Seung Geol Choi
Ashish Choudhury
Özgür Dagdelen
Bernardo David
Emiliano De Cristofaro
Jean Paul Degabriele
Claus Diem
Mario Di Raimondo
Yevgeniy Dodis
Nico Döttling
Pooya Farshim
Jean-Charles Faugère
Sebastian Faust
Serge Fehr
Dario Fiore
David Mandell Freeman
Georg Fuchsbauer
Thomas Fuhr
Eichiro Fujisaki
Jun Furukawa
David Galindo
Nicolas Gama
Sanjam Garg
Essam Ghadafi
Benedikt Gierlichs
Domingo Gomez
Sergey Gorbunov
Dov Gordon
Robert Granger
Adam Groce
Jian Guo
Carmit Hazay
Javier Herranz
Shoichi Hirose
Susan Hohenberger
Qiong Huang
Toshiyuki Isshiki
Tibor Jager
Abhishek Jain
Kimmo Järvinen
Dimitar Jetchev
Shaoquan Jiang
Stephen Jordan
Antoine Joux
Pascal Junod
Bhavana Kanukurthi
Eike Kiltz
Thorsten Kleinjung
David Kohel
Yuichi Komano
Takeshi Koshiba
Daniel Kraschewski
Kaoru Kurosawa
Fabien Laguillaumie
Mario Larangeira
Dong Hoon Lee
Jooyoung Lee
Kwangsu Lee
Kaitai Liang
Dongdai Lin
Zhen Liu
Victor Lomné
Adriana Lopez-Alt
Stefan Lucks
Anna Lysyanskaya
Vadim Lyubashevsky
Hemanta Maji
Avradip Mandal
Joana Marim
Damian Markham
Alexander May
Florian Mendel
Rachel Miller
Kazuhiko Minematsu
Payman Mohassel
Michael Naehrig
Koh-ichi Nagao
Svetla Nikova
Takashi Nishide
Ryo Nishimaki
Ryo Nojima
Satoshi Obana
Miyako Ohkubo
Adam O'Neill
Cristina Onete
Claudio Orlandi
Alina Ostafe
Jong Hwan Park
Kenneth Paterson
Alain Patey
Souradyuti Paul
Chris Peikert
Rene Peralta
Olivier Pereira
Ray Perlner
Ludovic Perret
Edoardo Persichetti
Marcel Pfaffhauser
Benny Pinkas
Axel Poschmann
Carla Ràfols
Ananth Raghunathan
Somindu C Ramanna
Oded Regev
Leonid Reyzin
Yannis Rouselakis
Subhabrata Samajder
Bagus Santoso
Santanu Sarkar
Alessandra Scafuro
Christian Schaffner
Sven Schäge
Werner Schindler
Martin Schläffer
Yannick Seurin
Barhum Kfir Shlomo
Thomas Shrimpton
Shashank Singh
Daniel Smith
Damien Stehlé
John Steinberger
Ron Steinfeld
Fatih Sulak
Koutarou Suzuki
Xiao Tan
Isamu Teranishi
Stefano Tessaro
Nicolas Theriault
Mehdi Tibouchi
Elmar Tischhauser
Tomas Toft
Deniz Toz
Meltem Sonmez Turan
Dominique Unruh
Kerem Varıcı
Muthu Venkitasubramaniam
Akshay Wadia
Bogdan Warinschi
Brent Waters
Daniel Wichs
Keita Xagawa
Dongsheng Xing
Guomin Yang
Kan Yasuda
Bingsheng Zhang
Yunlei Zhao
Hong-Sheng Zhou
Vassilis Zikas

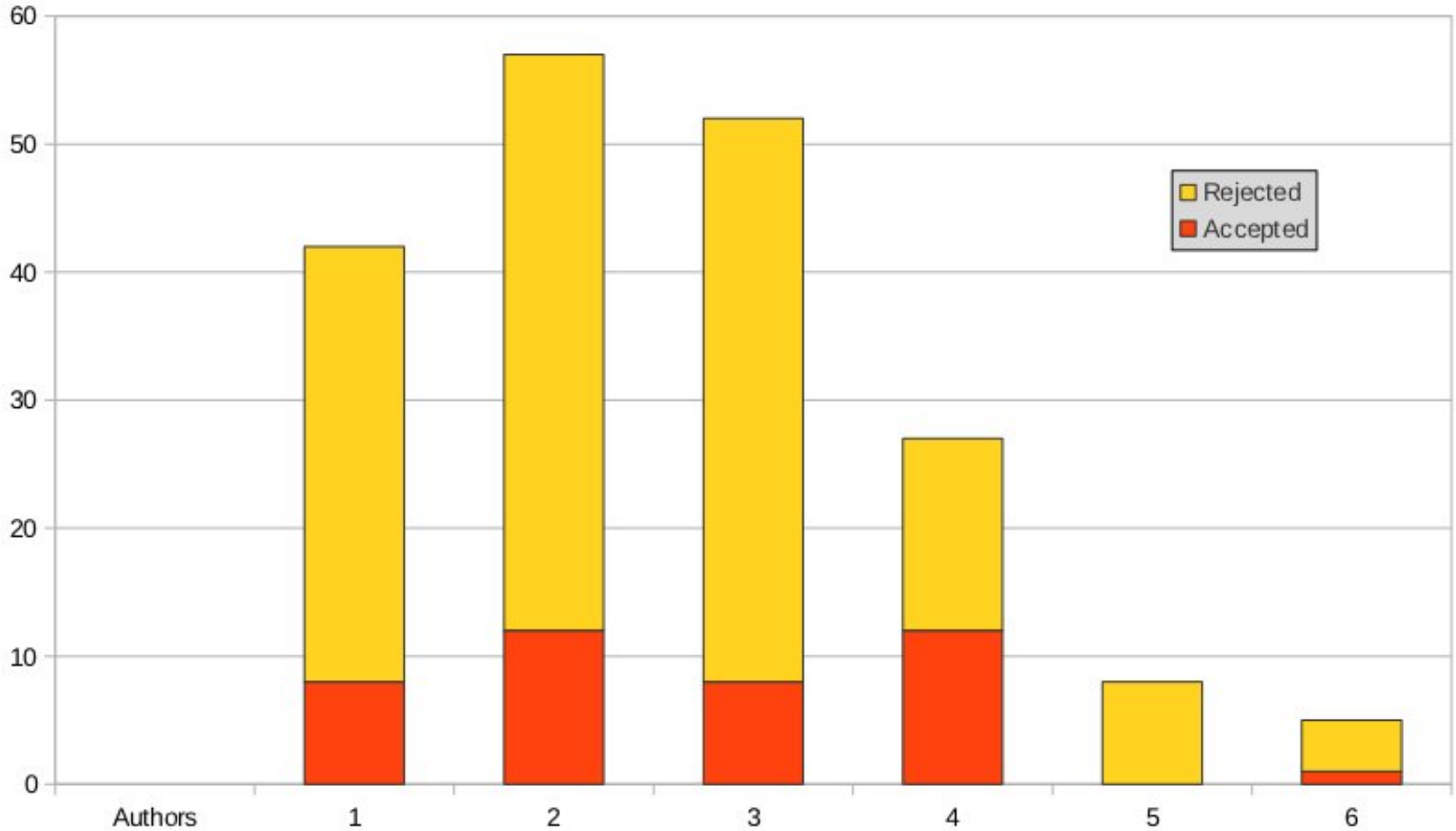
Statistics: Origins of Papers



191 submissions from 32 countries

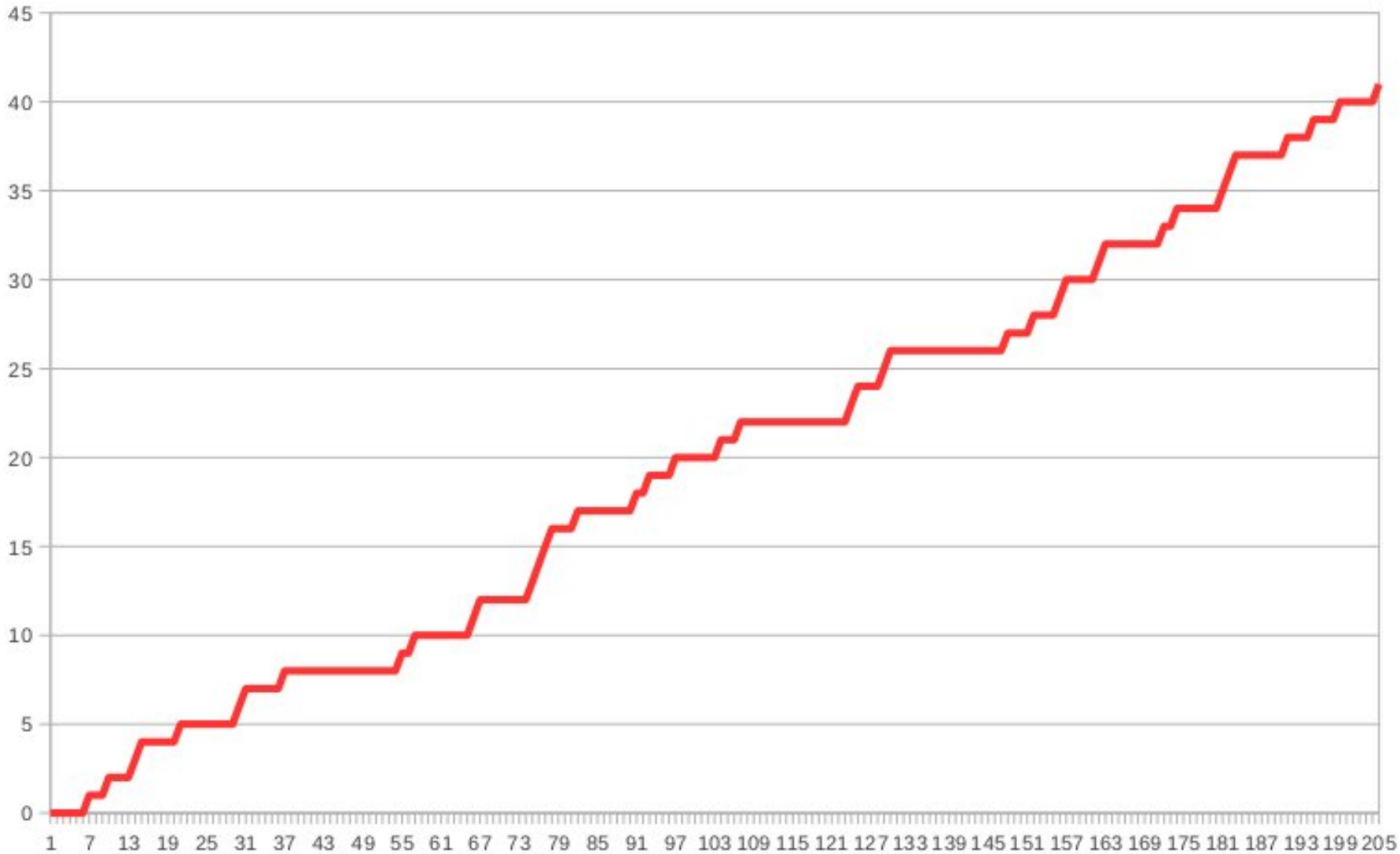
41 accepted papers from 18 countries

Statistics: Number of Authors



1 author	8 / 42	**4 authors**	12 / 27
2 authors	12 / 57	5 authors	0 / 8
3 authors	8 / 52	6 authors	1 / 5

Statistics: Submission Number



Acceptance vs. Submission number is quite uniform!

Statistics: Submission Date

The last 24 hours:

- 144 new submissions
- 312 revisions

The last hour:

- 28 new submissions
- 147 revisions

2 Invited Talks

A Tutorial on High Performance Computing applied to Cryptanalysis

by **Antoine Joux** (DGA and UVSQ, France)

Another Look at Provable Security

by **Alfred Menezes** (University of Waterloo, Canada)

Invitations to the Journal of Cryptology

Trapdoors for Lattices: Simpler, Tighter, Faster, Smaller

by **Daniele Micciancio** and **Chris Peikert**
(UC San Diego and Georgia Institute of Technology)

Key-Alternating Ciphers in a Provable Setting: Encryption Using a Small Number of Public Permutations

by **Andrey Bogdanov**, **Lars R. Knudsen**, **Gregor Leander**, **Francois-Xavier Standaert**, **John Steinberger**, and **Elmar Tischhauser**
(KUL, UCL Belgium, DTU Denmark, and Tsinghua University)

Cover and Decomposition Index Calculus on Elliptic Curves made practical. Application to a previously unreachable curve over $\mathbb{F}_p^6$

by **Antoine Joux** and **Vanessa Vitse**
(DGA and Université Versailles Saint-Quentin)

Best Paper!

Thank You!

to all

- the PC members
- the External reviewers
- the Authors of all the submitted papers
- the Speakers

to the General Chair: Nigel Smart

to all the organization team!

Enjoy the conference!