

# Eurocrypt 2009

April 26-30, Cologne, Germany  
Maritim Hotel



## Call for Papers

Original papers and posters on all technical aspects of cryptology are solicited for submission.

<http://www.iacr.org/conferences/eurocrypt2009/cfp.html>

## Important Dates

<b>Submission deadline:</b>	September 3rd, 2008
<b>Poster submission (new):</b>	October 10th, 2008
<b>Acceptance notification:</b>	December 19th, 2008
<b>Poster notification:</b>	December 19th, 2008
<b>Final version due:</b>	January 23rd, 2009
<b>Conference:</b>	April 26th – 30th, 2009

## Program Committee

**Paulo Barreto** (University of Sao Paulo, Brazil)  
**Alexandra Boldyreva** (Georgia Institute of Technology, USA)  
**Colin Boyd** (Queensland University of Technology, Australia)  
**Xavier Boyen** (Voltage Inc., USA)  
**Mike Burmester** (Florida State University, USA)  
**Orr Dunkelman** (ENS Paris, France)  
**Serge Fehr** (CWI Amsterdam, The Netherlands)  
**Marc Fischlin** (TU Darmstadt, Germany)  
**Pierre-Alain Fouque** (ENS Paris, France)  
**Craig Gentry** (Stanford University, USA)  
**Nick Howgrave-Graham** (NTRU Cryptosystems, USA)  
**Thomas Johansson** (Lund University, Sweden)  
**Antoine Joux** (DGA and University of Versailles, France)  
**Jonathan Katz** (University of Maryland, USA)  
**Kwangjo Kim** (ICU, Korea)  
**John Kelsey** (NIST, USA)  
**Kaoru Kurosawa** (Ibaraki University, Japan)  
**Reynald Lercier** (DGA/CELAR and University of Rennes, France)  
**Anna Lysyanskaya** (Brown University, USA)  
**Rafail Ostrovsky** (UCLA, USA)  
**Pascal Paillier** (Gemalto Security Labs/Cryptography & Innovation, France)  
**Duong Hieu Phan** (University of Paris 8, France)  
**Christian Rechberger** (IAIK, Graz University of Technology, Austria)  
**Werner Schindler** (Bundesamt für Sicherheit in der Informationstechnik, Germany)  
**Thomas Shrimpton** (Portland State University and University of Lugano)  
**Nigel Smart** (University of Bristol, UK)  
**Rainer Steinwandt** (Florida Atlantic University, USA)  
**Christine Swart** (University of Cape Town, South Africa)  
**Christopher Wolf** (Ruhr-University Bochum, Germany)

## Organizational Committee

All correspondence and/or questions should be directed to either of the

### Organizational Committee members:

#### **Antoine Joux** *Program Chair*

DGA and Université de Versailles  
45 avenue des Etats-Unis  
78035 Versailles, Cedex, France  
Phone: +33 1 39 25 43 23  
Email: [Antoine.Joux@prism.uvsq.fr](mailto:Antoine.Joux@prism.uvsq.fr)

#### **Alexander May** *General Chair*

Ruhr-University Bochum  
Universitätsstraße 150, NA 5/73  
44780 Bochum, Germany  
Phone: +49 234 32 23261  
Email: [alex.may@ruhr-uni-bochum.de](mailto:alex.may@ruhr-uni-bochum.de)

#### **Co-Chairs**

Roberto Avanzi  
Christof Paar  
Ahmad Sadeghi  
Jörg Schwenk  
Christopher Wolf



Horst Görtz Institute  
for IT-Security