Du
**09**
SEPT.
2024
au
**13**
DÉC.
2024

08h30
-
18h30

**2024-T3 POST-QUANTUM ALGEBRAIC CRYPTOGRAPHY**

**Post-quantum algebraic cryptography, Paris**

Institut Henri Poincaré
11, Rue Pierre et Marie Curie
75005 Paris

INSCRIPTION

Thematic programme at the Institut Henri Poincaré, Paris

The conferences and courses of this programme will also be accessible online.

**Registration is free but mandatory.**

It does not give you an automatic registration for the workshops, so please also register for each workshop you wish to attend.

Please note that the space is limited.

**Long term Visitors:**

URL of the page: https://www.ihp.fr/fr/agenda/post-quantum-algebraic-cryptography-paris&is_pdf=true

- Jean-François Biasse (University of South Florida, USA)
- Anne Broadbent (University of Ottawa, Canada)
- Giovanni Di Crescenzo (Peraton Labs, USA) TBC
- Mina Doosti (University of Edinburgh, UK) TBC
- Ramón Flores (University of Seville, Spain)
- Nadia Heninger (UC San Diego, USA)
- Kristin Lauter (Meta AI, USA)
- Thomas Koberda (University of Virginia, USA)
- Martin Kreuzer (University of Passau, Germany)
- Joachim Rosenthal (University of Zürich, Switzerland)
- Simona Samardjiska (Radboud University, NL)
- Siamak Shahandashti (University of York, UK)

**Local Organizers:**

- Christopher Battarbee (University of York)
- Olive chakraborty (CEA)

**Scientific committee:**

URL of the page: https://www.ihp.fr/fr/agenda/post-quantum-algebraic-cryptography-paris&is_pdf=true

- Romain Alléaume (Telecom Paris, France)
- Shweta Agrawal (Indian Institute of Technology, Madras)
- Daniel Cabarcas, U. Nacional de Colombia, Colombia)
- Giovanni Di Crescenzo (Perspecta Labs, USA)
- Leo Ducas (CWI Amsterdam, Netherland)
- Eleni Diamanti (Sorbonne University, France)
- Jean-Charles Faugère (INRIA Paris, Sorbonne University, France)
- Philippe Gaborit (University of Limoges, France)
- Xiao-Shan Gao (Chinese Academy of Sciences, China)
- Dorian Goldfeld (Columbia University, USA)
- David Jao (University of Waterloo, Canada)
- Thomas Johansson (Lund University, Sweden)
- Stavros Kousidis  (BSI, Germany)
- Delaram Kahrobaei (CUNY QC, GC, University of York, U.K., NYU)
- Kristin Lauter (Microsoft Research, USA)
- Dongdai Lin (Chinese Academy of Sciences, China)
- Vadim Lyubashevsky (IBM, Switzerland)
- Alexander May (Ruhr University Bochum, Germany)
- Dustin Moody (NIST, USA)
- Ludovic Perret (Sorbonne University, France)
- Diong Hieu Phan (Telecom Paris, France)
- Mellissa Rossi (ANSSI, France)
- Max Sala (University of Trento, Italia)
- Javad Shabani (NYU, Director of Quantum Center, US)
- Timothy Spiller (University of York, UK)
- Vladimir Shpilrain (City College of New York)
- Alice Silverberg (University of California, Irvine)
- Damien Stehlé (ENS Lyon, France)
- Rainer Steinwandt (University of Alabama in Huntsville, USA)
- Tsuyoshi Takagi (University of Tokyo, Japan)
- Pascal Weil (University of Bordeaux, France)
- Moti Young (Columbia University, USA)

Speaker for Summer School

Luca De Feo (IBM, Switzerland): Isogeny-based Cryptography
Thomas Debris-Alazard (INRIA, France), Code-based Cryptography
Pierre-Alain Fouque (University of Rennes, France): Lattice-based Cryptography
Delaram Kahrobaei (New York, USA, York, UK): Group-based Cryptography
Kristin Lauter (Meta AI, USA): Artificial Intelligence for Post-quantum Cryptography
Ludovic Perret (Sorbonne University, Paris, France): Multivariate-based Cryptography
Timothy Spiller (University of York, UK): Quantum Key-Distribution

URL of the page: https://www.ihp.fr/fr/agenda/post-quantum-algebraic-cryptography-paris&is_pdf=true

**INSTITUT HENRI POINCARÉ - UAR839**

Sorbonne Université / CNRS
11 rue Pierre et Marie Curie
75231 Paris Cedex 05

**HORAIRES**

L'institut :
• lundi au vendredi de 8h30 à 18h,
• fermé les jours fériés.

Le musée - Maison Poincaré :
• lundi, mardi, jeudi et vendredi
de 9h30 à 17h30,
• samedi de 10h à 18h,
• fermé le mercredi et le dimanche.

URL of the page: https://www.ihp.fr/fr/agenda/post-quantum-algebraic-cryptography-paris&is_pdf=true