Monday, September 28

8h30–8h45	Registration
8h45–9h	Welcome speech
9h–10h	**Nadia Heninger** (University of Pennsylvania, USA) *How Diffie-Hellman fails in practice*
10h–10h30	Coffee break
10h30–11h30	**Aurore Guillevic** (École polytechnique and INRIA Saclay-Île-de-France, France) *Computing individual discrete logarithms faster in* $\mathbb{F}_{p^n}$ *(last step of the Number Field Sieve algorithm)*
11h30–12h30	**Cécile Pierrot** (CNRS, DGA and Sorbonne Universités, UPMC, France) *Discrete Logarithms in Medium Characteristic Finite Fields*
12h30–14h30	Lunch
14h30–15h30	**Steven Galbraith** (University of Auckland, New Zealand) *Algorithms for the ECDLP*
15h30–16h30	**Michiel Kosters** (University of California, Irvine) *Sub-exponential algorithms for ECDLP?*
16h30–17h	Coffee break
17h–18h	**Kim Laine** (Microsoft Research) *On the Security of Genus 3 Curves*
18h30–19h30	Welcome Cocktail (Sponsored by Microsoft Research)
19h30–20h30	**Rump Session**

Tuesday, September 29

9h–10h	**Enea Milio** (INRIA Bordeaux-Sud-Ouest, France) *Computation of modular polynomials in dimension 2*
10h–10h30	Coffee break
10h30–11h30	**Léo Ducas** (CWI, Netherlands) *Recovering Short Generators of Principal Ideals in Cyclotomic Rings*
11h30–12h30	**Katherine Stange** (University of Colorado, USA) *Ring Learning with Errors*
12h30–14h30	Lunch
14h30–15h30	**Peter Schwabe** (Radboud University, Netherlands) *Verifying ECC software*
15h30–16h30	**Michael Hamburg** (Cryptography Research, USA) *Complexity, security and performance trade-offs in elliptic curve libraries*
16h30–17h	Coffee break
17h–18h	**Standardisation Panel** • Daniel Bernstein (Technische Universiteit Eindhoven, Netherlands and University of Illinois at Chicago, USA) • Joppe Bos (NXP, Belgium) • Jean-Pierre Flori (Agence nationale de la sécurité des systèmes d'information, France) • Michael Hamburg (Cryptography Research, USA) • Manfred Lochter (Bundesamt für Sicherheit in der Informationstechnik, Germany) • Dustin Moody (National Institute of Standards and Technology, USA)
20h	Dinner at Café du Port

Wednesday, September 30

9h–10h	**Christian Grothoff** (INRIA Rennes-Bretagne-Atlantique, France) *Cryptography in GNUnet: Protocols for a Future Internet for Libre Societies*
10h–10h30	Coffee break
10h30–11h30	**Arnaud Tisserand** (CNRS, Université de Rennes and INRIA-Bretagne-Atlantique, France) *Hardware accelerators for ECC and HECC*
11h30–12h30	**Juliane Krämer** (Technische Universität Darmstadt, Germany) *Fault Attacks on Pairing-Based Cryptography*