EUROCRYPT 2014
Rump Session Programme

1800–1810 IACR Award Ceremony (Christian Cachin)

1810–1820 Cryptanalysis of EUROCRYPT 2014 (Phong Nguyen; Elisabeth Oswald)

1820–1825 Practical Complexity Cube Attacks on Round-Reduced Keccak Sponge Function (Itai Dinur; Pawel Morawiecki; Josef Pieprzyk; Marian Srebrny; Michal Straus)

1825–1830 Proving Security of Witness Encryption (Craig Gentry; Allison B. Lewko; Brent Waters)

1830–1835 A new approach to proving security of obfuscation (Craig Gentry; Allison Lewko; Amit Sahai; Brent Waters)

1835–1840 Secure and Effective Methods for Increasing Citation Cost (Alptekin Kupcu)

1840–1843 Crypto design contest (Sasha Boldyreva)

1843–1910 Break

1910–1915 CryptoSMT (Stefan Kolbl; Christian Rechberger)

1915–1920 A Model for Adversarial Wiretap Channel & Secure Message Transmission (Rei Safavi-Naini; Pengwei Wang)

1920–1925 AEZoo (Stefan Kolbl; Martin Lauridsen; Christian Rechberger; Tyge Tiessen)

1925–1930 From ORAM to Oblivious Computation in 273 Seconds (Marcel Keller; Peter Scholl)

1930–1935 Verifiably random secure curves (Daniel J. Bernstein; Tung Chou; Chitchanok Chuengsatiansup; Andreas Huelsing; Tanja Lange; Ruben Niederhagen; Christine van Vredendaal)

1935–1945 NEW! Announcing the Best Crypto Competition! NEW! (Bart Preneel; Celine Blondeau; D. Julius B.; Edward Snowden; Gaetan Leurent; Greg Rose; Keith Alexander; Kenny Patterson; Kevin Igoe; Orr Dunkelman; Roberto Ava...; Simon Speck; Stefan Lucks; Tanja Lange)

1945–1950 Closing remarks