FSE 2017 rump session -- programme

- 16.45 FSE 2017 stats
  (María Naya-Plasencia, **Bart Preneel**)
- 16.52 An easy attack on AEZ
  (**Gaëtan Leurent** and the BRUTUS team)
- 16.57 Challenges in Authenticated Encryption
  (**Daniel J. Bernstein** and ECRYPT-CSA)
- 17.00 Cryptanalysis of PMACx, PMAC2x, and SIVx
  (Kazuhiko Minematsu and **Tetsu Iwata**)
- 17.04 A Block Cipher with Provable Security against Key Recovery
  (Tetsu Iwata, **Yu Sasaki**, Yosuke Todo and Kan Yasuda)
- 17.09 A New Structural-Differential Property of 5-Round AES
  (**Lorenzo Grassi**, Christian Rechberger and Sondre Rønjom)
- 17.14 A new submission to the SNAKE OIL CRYPTO competition
  (**Roberto Avanzi**, @FakeIACR, Diego Aranha)
- 17.16 A Statement on Standardization
  (Orr Dunkelman, Atul Luykx, **Léo Perrin**)
- 17.19 Lightweight Crytography at the Univ. of Luxembourg
  (CryptoLUX Team, **Léo Perrin**)
- 17.21 Digital Signatures from Symmetric-Key Primitives
  (**Christian Rechberger**)
- 17.26 The LowMC Cipher breaking challenge
  (**Christian Rechberger**)
- 17.29 The Skinny competition
  (**Thomas Peyrin** and Skinny team)
- 17.31 Walsh Spectrum Analysis on Sampling Distributions
  (**Yi Lu**)
- 17.34 SPHINCS Benchmarks
  (**Stefan Kölbl**)
- 17.36 A New Fundamental Structural Property on AES
  (**Navid Ghaedi Bardeh**, Sondre Rønjom)
- 17.41 Ketje Cryptanalysis Prize
  (**Joan Daemen** and Keccak Team)
- 17.44 FSE 2018
  (**María Naya-Plasencia**)
- 17.47 Arigatou Gozaimasu
  (**Anne Canteaut**)