CAKE: Code-Based Key-Exchange

• What: A key-exchange protocol
  • A planned submission to NIST call on post-quantum cryptography

• Who (team):  
  • Paulo Barreto (University of Washington)  
  • Shay Gueron (University of Haifa and Amazon Web Service)  
  • Tim Güneysu (University of Bremen & DFKI)  
  • Rafael Misoczki (Intel Labs)  
  • Edoardo Persichetti (Florida Atlantic University)  
  • Nicolas Sendrier (INRIA)  
  • Jean-Pierre Tillich (INRIA)

• Features: Eat the cake and have it too
  • Leverages QC-MDPC McEliece Encryption Scheme [Misoczki, Tillich, Sendrier, Barreto, 2013]  
  • Not affected by reaction-attack against MDPC decoding [Guo, Johansson, Stankovski, 2016]  
  • Formal security proof (IND-CCA2)  
  • Competitive performance