# TCC 2014 Rump Session

7.45 Business Meeting + Program Chair's presentation

8.00 Yehuda Lindell, *Updates on SCAPI (the Secure Computation API)*

8.05 Kai-Min Chung, *Physical Randomness Extractors*

8.11 Claudio Orlandi, *Don't forget your key in your room!*

8.16 Bernardo David, *Homomorphic UC Commitments in Minicrypt*

8.21 Michael Walter, *SVP by Enumeration: Bridging the Gap between Theory and Practice*

8.27 Shai Halevi, *Algorithms in HElib*

8.32 Mohammad Mahmoody, *Summer School on Black-Box Impossibility Results*

— Break —

9.00 Daniel Wichs, *Outsourcing Private RAM Computation*

9.07 Claudio Orlandi, *Minimizing ANDs in free-XOR Circuits (a report)*

9.13 Rafael Pass, *iO from semantical secure multi-linear encodings*

9.18 Divesh Aggarwal, *Non-malleable codes from additive combinatorics*

9.23 Luis Brandao, *Very-efficient flipping of many coins*

9.28 Noah Stephens-Davidowitz, *How to Eat Your Entropy and Have It Too (Recovering from compromise)*

9.33 Ranjit Kumaresan, *How to Use Bitcoin to Design Fair Protocols*

9.38 Ben Fisch, Physical Zero-Knowledge Proofs of Physical Properties

9.43 Announcements of Open Postdoc Positions

9.46 Claudio Orlandi, *MPC Workshop in Aarhus before Eurocrypt*