June 1989 and its fallout

Ran Canetti, TAU and BU

I will give a lightening-brief overview of the evolution of two related concepts: The simulation-based paradigm for defining security of protocols, and security against adaptive corruptions. I will then jump to the present day with exciting new advancements on both fronts.