BRUCE KAPRON, University of Victoria

Co-induction and Computational Semantics for Public-key Encryption with Key Cycles

Micciancio recently has shown that with a co-inductive definition of indistinguishability it is possible to obtain computational soundness for private-key cryptography in the presence of key cycles. We explore co-inductive definitions of security in public-key cryptography, and extend a soundness result of Herzog to key-cyclic expressions. We also show that a completeness result is achievable in the absence of key cycles with respect to any length-revealing encryption system. (Joint work with M. Hajiabadi)