Paper title and authors; where appeared. Soundness of Formal Encryption in the presence of Active Adversaries. *Daniele Micciancio and Bogdan Warinschi*

What is the main problem this paper attacks? The authors develop a method to reason about the security of honest parties exchanging arbitrary messages in the presence of adversaries that may interact with the honest parties in realistic ways.

What solution does the paper propose? Consider a set of secure states S. Using a symbolic transition model, prove that S is closed under the allowable transitions (including adversary transitions). If the allowable transitions are chosen correctly (the preserve the "negligible probability" relation), this translates into a proof of security in the classical sense.

What central idea did the authors use to solve it? Since "negligible probability" is an equivalence class, we can consider operations that preserve the equivalence relation, and thus dispense of probabilities altogether when using some primitives known to be secure

What is a weakness or limitation of the paper? The paper considers only fixed protocols between two parties, and cannot handle more parties or sets of possible protocols. Some of the allowable transitions are lacking; ex: forwarding unknown encryptions etc. Only security (the inability to tamper with messages without detection) is considered, but not secrecy (the inability for certain information to be derived by an adversary).

Why is this paper important? It is the first paper giving a simple method for translating logic proofs into computational proofs including active adversaries. Further, it does not require those nasty probability proofs (though it is not the first to do this).