Paper title and authors; where appeared. *Entity Authentication and Key Distribution,* by Mihir Bellare and Phillip Rogaway. Published in August 1993; originally appeared in *Advances in Cryptology - Crypto '93 Proceedings,* Springer-Verlag.

What is the main problem this paper attacks? Previous works had discussed the problems of secure mutual entity authentication (MA) and authenticated key exchange (AKE) informally. It followed that protocols based on these previous works attempting to solve these problems were ambiguously correct, and it was unclear precisely what parts of these protocols were important to the given problem.

What solution does the paper propose? This paper defines MA and AKE as concisely as previous works had cryptographic primitives. It starts with the simple assumption of a pseudorandom generator, precisely defines a run of a protocol, adversarial powers, and related concepts, and eventually builds up to definitions of secure MA and AKE.

What central idea did the authors use to solve it? The participants in a protocol are represented as oracles which can be queried by a probabilistic adversary. For MA the goal of the adversary is to get an oracle to accept a conversation which doesn't precisely match any which has taken place on another oracle. For AKE the goal of the adversary is to distinguish a session key from an arbitrary random string produced by the same distribution. If the relevant adversarial goal cannot be fulfilled with more than negligible probability, and the protocol components fit together sensibly, then the protocol fulfills the given security property.

What is a weakness or limitation of the paper? The notion of matching of oracle conversations is perhaps too strong since it requires oracle conversations to match *precisely* at every step; it could be extended to only compare values specifically relevant to authentication.

Why is this paper important? This paper rounds-out the set of precisely probabilistically defined cryptographic primitives. It allows protocol developers to formally prove or disprove that a particular protocol is useful for MA or SKE. This work further allows for construction of a realistic MA or AKE scheme by substituting a concrete pseudorandom generator for the abstract one used in the proofs. It furthermore provides several examples of efficient MA and AKE protocols which could be studied or extended in future works.