Abstract

We give an informal analysis and critique of several typical "provable security" results. In some cases there are intuitive but convincing arguments for rejecting the conclusions suggested by the formal terminology and "proofs," whereas in other cases the formalism seems to be consistent with common sense. We discuss the reasons why the search for mathematically convincing theoretical evidence to support the security of public-key systems has been an important theme of researchers. But we argue that the theorem-proof paradigm of theoretical mathematics is of limited relevance here and often leads to papers that are confusing and misleading. Because our paper is aimed at the general mathematical public, it is self-contained and as jargon-free as possible.