Abstract

Starting with Shoups seminal paper [24], the generic group model has been an important tool in reductionist security arguments. After an informal explanation of this model and Shoups theorem, we discuss the danger of flaws in proofs. We next describe an ontological difference between the generic group assumption and the random oracle model for hash functions. We then examine some criticisms that have been leveled at the generic group model and raise some questions of our own.