CORR 2000-46

Constructions and Bounds for Unconditionally Secure Commitment Schemes

C. Blundo*, B. Masucci*, D.R. Stinson, & R. Wei*

Abstract commitment schemes have been extensively studied since they were introduced by Blum in 1982. Rivest recently showed how to construct unconditionally secure commitment schemes, assuming the existence of a trusted initializer. In this paper, we present a formal mathematical model for such schemes and analyze their *binding* and *concealing* properties. In particular, we show that such schemes cannot be perfectly *concealing*: there is necessarily a small probability that Alice can cheat Bob by committing to one value but later revealing a different value. We prove several bounds on Alice's cheating probability, and present constructions of schemes that achieve optimal cheating probabilities. We also show a close link between commitment schemes and the classical "affine resolvable designs."