CORR 2001-08

Universal hash families and the leftover hash lemma, and applications to cryptography and computing

D.R. Stinson

Abstract This paper is an expository treatment of the leftover hash lemma and some of its applications in cryptography and complexity.