

CORR 2001-60

**Slope packings and coverings, and generic algorithms
for the discrete logarithm problem**

M. Chateauneuf*, A.C.H. Ling*, D.R. Stinson

Abstract We consider the set of slopes of lines formed by joining all pairs of points in some subset S of a Desarguesian affine plane of prime order p . If all the slopes are distinct and non-infinite, we have a *slope packing*; if every possible non-infinite slope occurs, then we have a *slope covering*. We review and unify some results on these problems that can be derived from the study of Sidon sets and sum covers. Then we report some computational results we have obtained for small values of p . Finally, we point out some connections between slope packings and coverings and generic algorithms for the discrete logarithm problem in prime order (sub)groups. Our results provide a combinatorial characterization of such algorithms, in the sense that any generic algorithm implies the existence of a certain slope packing or covering, and conversely.