Abstract

A blackbox secret sharing (BBSS) scheme works in exactly the same way for all finite Abelian groups G; it can be instantiated for any such group G and only black-box access to its group operations and to random group elements is required. A secret is a single group element and each of the n players' shares is a vector of such elements. Share-computation and secret-reconstruction is by integer linear combinations. These do not depend on G, and neither do the privacy and reconstruction parameters t, r. The expansion factor is the total number of group elements in a full sharing divided by n.In this talk, we introduce a novel, nontrivial, effective construction of BBSS based on coding theory instead of number theory. For threshold-BBSS we also achieve minimal expansion factor O(\log n). Our method is more versatile. Namely, we show, for the first time, BBSS that is near-threshold, i.e., r-t is an arbitrarily small constant fraction of n, and that has expansion factor O(1), i.e., individual share-vectors of constant length. We also show expansion is minimal for near-threshold and that such BBSS cannot be attained by previous methods. Our general construction is based on a well-known mathematical principle, the local-global principle. More precisely, we first

construct BBSS over local rings through either Reed-Solomon or algebraic geometry codes. We then ``glue'' these schemes together in a dedicated manner to obtain a global secret sharing scheme, i.e., defined over the integers, which, as we finally prove using novel insights, has the desired BBSS properties.