

1138-11-317      **Paul Balister\*** (pbalistr@memphis.edu), **Béla Bollobás** and **Robert Morris**. *The sharp threshold for making squares.*

Many of the fastest known algorithms for factoring large integers rely on finding subsequences of randomly generated sequences of integers whose product is a perfect square. Motivated by this, in 1994 Pomerance posed the problem of determining the threshold of the event that a random sequence of  $N$  integers, each chosen uniformly from the set  $\{1 \dots, x\}$ , contains a subsequence, the product of whose elements is a perfect square. In 1996, Pomerance gave good bounds on this threshold and also conjectured that it is sharp.

In a paper published in *Annals of Mathematics* in 2012, Croot, Granville, Pémantle and Tetali significantly improved these bounds, and stated a conjecture as to the location of this sharp threshold. In recent work, we have confirmed this conjecture. In this talk I shall give a brief overview of some of the ideas used in the proof, which relies on techniques from number theory, combinatorics, and stochastic processes. (Received February 12, 2018)