WILLIAM MARTIN, Worcester Polytechnic Institute, 100 Institute Road, Worcester, MA 01609, USA

Roughly independent binary random variables

In cryptography (as well as other areas, I'm sure), the effective (ab)use of random bits is of great importance. In this talk, we consider an expansion function $f\colon \{0,1\}^m \to \{0,1\}^n$ $(n > m)$ with the property that, given the uniform distribution U_m on input strings, the projection of the output $f(U_m)$ onto any t coordinates has min-entropy at least ℓ. For example, for $\ell = t$, this is just a binary orthogonal array of strength t with n factors and 2^m runs. Our goal is to significantly beat the Rao bound by allowing ℓ to drop below t.

In this talk, which is joint work with Matt Houde of EMC Corporation, I will give some preliminary bounds and constructions. Hopefully, I can motivate some experts to look into this question.