SHLOMO HOORY, University of British Columbia
Simple permutations mix well

A naturally occurring question in cryptography is how well the composition of simple permutations drawn from a simple distribution resembles a random permutation. Although such constructions are a common source of security for block ciphers like DES and AES, their mathematical justification (or lack thereof) is troubling.

Motivated by this question, we study the random composition of a small family of $O(n^3)$ simple permutations on $\{0,1\}^n$. Specifically we ask how many randomly selected simple permutations need be composed to yield a permutation that is close to k-wise independent. We improve on previous results and show that up to a polylogarithmic factor, n^2k^2 compositions of random permutations from this family suffice. In addition, our results give an explicit construction of a degree $O(n^3)$ Cayley graph of the alternating group of 2^n objects with a spectral gap $\Omega(1/(n^2 2^n))$, which is a substantial improvement over previous constructions.

This question is essentially about the rapid mixing of a certain Markov chain, and the proofs are based on the comparison technique.