CORR 99-48

Almost k-wise Independent Sample Spaces and Their Cryptologic Applications

Kaoru Kurosawa*, Thomas Johansson*, Douglas Stinson

Abstract An almost k-wise independent sample space is a small subset of m bit sequences in which any k bits are "almost independent". We show that this idea has close relationships with useful cryptologic notions such as multiple authentication codes (multiple A-codes), almost strongly universal hash families, almost k-resilient functions, almost correlation-immune functions, indistinguishable random variables, and k-wise decorrelation bias of block ciphers.

We use almost k-wise independent sample spaces to construct new efficient multiple A-codes such that the number of key bits grows linearly as a function of k (where k is the number of messages to be authenticated with a single key). This improves on the construction of Atici and Stinson [2], in which the number of key bits is $\Omega(k^2)$.

We introduce the concepts of ε-almost k-resilient functions and almost correlation-immune functions, and give a construction for almost k-resilient functions that has parameters superior to k-resilient functions. We also point out the connection between almost k-wise independent sample spaces and pseudorandom functions that can be distinguished from truly random functions, by a distinguisher limited to k oracle queries, with only a small probability. Vaudenay [31] has shown that such functions can be used to construct block ciphers with a small decorrelation bias.

Finally, new bounds (necessary conditions) are derived for almost k-wise independent sample spaces, multiple A-codes and balanced ε-almost k-resilient functions.