DOUG STINSON, University of Waterloo

Generalizations of All-or-Nothing Transforms

All-or-nothing transforms (AONTs) were originally defined by Rivest as bijections from s input blocks to s output blocks such that no information can be obtained about any input block in the absence of any output block. Numerous generalizations and extensions of all-or-nothing transforms have been discussed in recent years, many of which are motivated by diverse applications in cryptography, information security, secure distributed storage, etc. In particular, t-AONTs, in which no information can be obtained about any t input blocks in the absence of any t output blocks, have received considerable study.

Three recent generalizations of AONTs are motivated by applications due to Pham et al. and Oliveira et al. We term these generalizations rectangular, range, and restricted AONTs. Briefly, in a rectangular AONT, the number of outputs is greater than the number of inputs. A range AONT satisfies the t-AONT property for a range of consecutive values of t. Finally, in a restricted AONT, the unknown outputs are assumed to occur within a specified set of "secure" output blocks. We study existence and non-existence and provide examples and constructions for these generalizations. We also demonstrate interesting connections with combinatorial structures such as orthogonal arrays, split orthogonal arrays, MDS codes and difference matrices.

This talk is based on joint work with Navid Nasr Esfahani.