Asymmetric All-or-nothing Transforms

Douglas Stinson*, Navid Nasr Esfahani, University of Waterloo

A (symmetric) t-all-or-nothing transform is a bijective mapping defined on the set of s-tuples over a specified finite alphabet. It is required that knowledge of all but t outputs leaves any t inputs completely undetermined. There have been numerous papers developing the theory of AONTs as well as presenting various applications of AONTs in cryptography and information security. In this talk, we discuss *asymmetric all-or-nothing transforms*. We replace the parameter t by two parameters t_{out} and t_{in}, where $t_{in} \leq t_{out}$. The requirement is that knowledge of all but t_{out} outputs leaves any t_{in} inputs completely undetermined. When $t_{in} < t_{out}$, we refer to the AONT as *asymmetric*. We give several constructions and bounds for various classes of asymmetric AONTs, especially those with $t_{in} = 1$ or $t_{in} = 2$. We pay particular attention to *linear* transforms, where the alphabet is a finite field and the mapping is linear.

Keywords: all-or-nothing transform