***When Not All Bits Are Equal:***

***Incorporating 'Worth' Into Information-Flow Measures***

Approaches to quantitative information flow (QIF) traditionally have assumed that all leaks involving a given number of bits are equally harmful. The assumption is unrealistic, so a new approach to QIF is described. Here, secrets are defined in terms of fields, where derived secrets obtained by combining these fields can be assigned a different “worth” (perhaps in proportion to the harm that would result from disclosure). New measures that incorporate worth into QIF are then defined; they generalize probability of guessing, guessing entropy, and Shannon entropy. A lattice of information is derived to provide an underlying algebraic structure for an adversary’s state of knowledge in this more general setting. This is joint work with Mario Alvim and Fred Schneider.