DR. VALENTIN SUDER, UVSQ

Two Notions of Differential Equivalence on Sboxes

In this work, we discuss two notions of differential equivalence on Sboxes. First, we introduce the notion of *DDT-equivalence* which applies to vectorial Boolean functions that share the same difference distribution table (DDT). Next, we compare this notion, to what we call the γ-*equivalence*, applying to vectorial Boolean functions whose DDTs have the same support. We discuss the relation between these two equivalence notions and provide an algorithm for computing the DDT-equivalence and the γ-equivalence classes for a given function. We study the sizes of these classes for some families of Sboxes. Finally, we prove a result that shows that the rows of the DDT of an APN permutation are pairwise distinct. (Joint work with Christina Boura, Anne Canteaut and Jérémy Jean).