1163-94-282 **Pantelimon Stanica*** (pstanica@nps.edu). *A multiplicative differential uniformity of block ciphers' Sboxes.*

Inspired by a practical attack on block ciphers based upon a modification of the differential attack in [N. Borisov, M. Chew, R. Johnson, D. Wagner, *Multiplicative Differentials*, Fast Software Encryption, FSE 2002], we defined recently (2019) a new (output) multiplicative differential, and the corresponding differential uniformity. Quite a few papers have appeared within months on this new notion that is interesting from both a mathematical and cryptography perspective. Here, we go through some of the results that were developed in the past year connected to this concept. For example, we find the c-differential uniformity of the inverse function (as used in the Advanced Encryption Standard), as well as some other (almost) perfect nonlinear functions, in both even and odd dimensional binary finite fields, just to mention a few such results. The proof methods are number theoretical in nature. Also, the c-differential uniformity of some real-life ciphers' Sboxes will be displayed. (Received August 31, 2020)