1139-20-354 **Riccardo Aragona**, **Marco Calderini**, **Antonio Tortora** and **Maria Tota***
(mtota@unisa.it), DipMat - Università di Salerno, Via Giovanni Paolo II, 132, 84084 Fisciano, SA, Italy. *On the primitivity of PRESENT and other lightweight ciphers.*

We provide two sufficient conditions to guarantee that the round functions of a translation based cipher generate a primitive group. Furthermore, under the same hypotheses, and assuming that a round of the cipher is *strongly* proper and consists of m-bit S-Boxes, with $m = 3, 4$ or 5, we prove that such a group is the alternating group. As an immediate consequence, we deduce that the round functions of some lightweight translation based ciphers, such as the PRESENT cipher, generate the alternating group. (Received February 16, 2018)