New results in generating true random numbers on simple microcontrollers

Josef Hlavac, Simona Buchovecka, Robert Lorencz
Czech Technical University of Prague, Czech Republic

Abstract

As presented last year on CryptArchi, it is well possible to generate true random numbers even on simple microcontrollers. In this talk, we present new results in the area. In particular, we present the outcomes of experiments with the influence of various on-chip peripherals, such as the LCD controller, on the TRNG operation. We also tried more types of microcontrollers to verify the consistency of the method and present the results.