Generating true random bits on general-purpose microcontrollers

Josef Hlavac, Martin Hadacek and Robert Lorencz

Abstract

We show that it is possible to generate a truly random bitstream even on microcontrollers that lack dedicated capabilities or peripherals to do so, as long as the microcontroller in question supports two independent clock sources. We demonstrate our method with an Atmel AVR microcontroller fitted on the AVR Butterfly demonstration board. In this setup, no additional hardware is needed to generate true random numbers.
We analyze the generated random bitstream using the NIST sts-2.0b test suite and discuss the effect of certain parameters.