DATE : 2020/1/8

Department of Electrical and Electronic Information Engineering		ID	M153269
Name	Hidetaka Masaoka		

Supervisor	Shuichi Ichikawa

Abstract

Title	Random number generation from internal states and timing fluctuation in microprocessor

Random Numbers are used as a basis of security for many applications. Unpredictable random number generator (URNG) is a random number generator that is practically unpredictable. URNG generates the random numbers mainly from internal states of central processing unit (CPU). Suciu et al. (2011) proposed an URNG that uses performance counters (PFCs) of CPU as the entropy sources. However, previous works including Suciu et al. have not evaluated random numbers quantitatively with respect to the timing factors in CPU and operating system (OS).

This research examines the effects of timing factors to the randomness derived from URNG. First, random numbers were generated based on the method of Marton et al. (2017). The experiment environment consists of Intel Core-i5, Ubuntu18 and PAPI (performance application programming interface) library. This research examined the effect of the timing factors by using nanosleep() function and the background application. The quality of random numbers, the generation rate, and the numbers of interrupts and context switches are also examined. The random numbers are generated by XOR-ing 5 PFCs (lowermost 8-bit value), which are PAPI BR PRC, PAPI BR UCN, PAPI LD INS, PAPI LST INS, and PAPI TOT CYC with nanosleep() in the loop. The request time of nanosleep() was designated between 1 [ns] and 10 [ms]. Though the derived random numbers failed in DIEHARD test for all cases, the quality of random numbers improved for 1 [ms] or larger. The generation rate decreased accordingly in larger request time, while the numbers of interrupts and context switches increased. When a background application (e.g., HimenoBMT, IOzone, and STREAM) was executed with URNG and nanosleep(), the derived numbers passed DIEHARD test regardless of request time and background application. By examining five PFCs independently (without XOR), it was found that PAPI TOT CYC passed DIEHARD test for the request time larger than 10 [ns]. This results suggests that the source of entropy comes from the fluctuation of sampling time, as PAPI TOT CYC simply counts the number of system clock cycle.

Finally, a linear feedback shift register (LFSR) was implemented in PULPino micro controller unit (MCU). The random values were sampled from the lowermost 32 bit of 128-bit LFSR circuit under FreeRTOS environment. In this method, the derived numbers passed DIEHARD test, regardless of using background application STREAM.