DATE: 2021/1/8

Department of Electrical and Electronic Information Engineering		ID	M163221
Name	Hitomi Kishibe		

Supervisor	Shuichi Ichikawa

Abstract

Title	A light-weight implementation of latch-based TRNG and a method for maintaining random number quality

Random numbers have become an essential element in many security applications, and high quality random numbers are required. There are two types of random numbers: pseudo-random numbers and genuine random numbers. Pseudorandom numbers are generated based on an algorithm, so the future value can be predicted if the internal state is guessed. True random numbers are generated based on physical phenomena and require hardware support, but they are impossible to predict and reproduce. In this research, we deal with the generation of true random numbers, and consider a true random number generator (TRNG) circuit that utilizes the metastability of latches.

Hata and Ichikawa (2012) implemented a latch-type TRNG on a Xilinx Virtex-4 FXFPGA. The implementation was implemented using hard macros to improve the random number quality, which resulted in an implementation that depended on the FPGA model. Fujieda and Ichikawa (2018) implemented a latch-based TRNG with a soft macro using HDL. Although the portability and maintainability of the design were improved, the hardware cost (number of latches) of the soft macro implementation was larger than that of the hard macro implementation.

Since TRNGs operate based on physical phenomena, the quality of the obtained random numbers is affected by supply voltage, operating temperature, and other factors. Poor operating conditions or external attacks can degrade the random number quality. In order to detect malfunctions or attacks, it is necessary to inspect the output online when the TRNG is operating, and to issue a warning when the quality drops. In this study, we investigate a method for online inspection of random number quality.

The objective of this research is to maintain the random number quality while reducing the hardware cost of soft macro implementation. In order to reduce the implementation cost, the number of latches must be reduced, but reducing the number of latches reduces the entropy generated, which degrades the random number quality. However, reducing the number of latches reduces the entropy generated, which degrades the quality of the random numbers, so we use XOR to aggregate the TRNG outputs for multiple cycles to improve the quality of the random numbers. The implementation evaluation results show that the system passes the random number test even when the number of latches is reduced, and that the random number quality is higher when the bits are separated in time by XOR than when the bits are consecutive in time. In this study, we also investigate how to maintain the random number quality by increasing or decreasing the number of aggregation cycles according to the random number quality.