TOYOHASHI UNIVERSITY OF TECHNOLOGY
Master Technology, Create Technology

No. 7, June 2012

Research highlights

Digital generation of true random numbers for computer security

The generation of true sets of random numbers is critical for secure computer system networks. True random number generation (TRNG) is carried out by analog electron circuits, which are expensive and difficult to integrate with digital technology.

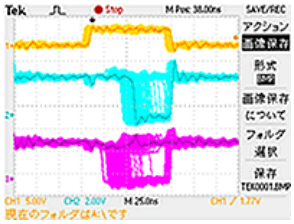
Here, Hisashi Hata and Shuichi Ichikawa describe the design and implementation of TRNG from fully digital circuits by exploiting the metastability the RS latch.

The TRNG is comprised of only logic gates enabling ease of integration with logic LSI. Notably, the RS latch is implemented as a 'hard macro' to ensure randomness by minimizing signal skew and load imbalance of internal nodes.

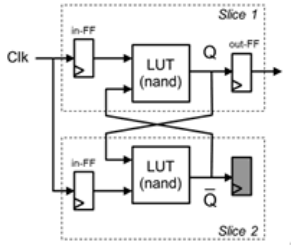
The TRNG has 256 latches, occupies 580 slices, and achieves 12.5 Mbps output.

▪Hisashi Hata and Shuichi Ichikawa
▪ FPGA Implementation of metastable-based true random number generation
▪IEICE Trans. Inf. & Syst. **E95-D**, 426–436, (2012)

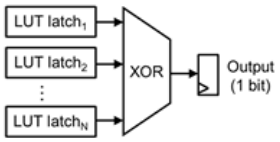
Shuichi Ichikaw a



Observed metastability of an RS latch



LUT latch: an RS latch, implemented w ith tw o LUTs in FPGA device



Practical configuration of a TRNG