Technology from Kyoto University

Compact and Low-Power Physical Random Number Generator

We are looking to out-license the technology for its commercialization.

A self-correcting circuit ensures stable operation, enabling a smaller size and over 90% lower power consumption compared to typical TRNGs.

◆Background

Random number generators are widely used in processors, secure key generation, identification (ID) number creation, and Monte Carlo simulations. True Random Number Generators (TRNGs), which generate values based on naturally occurring and unpredictable phenomena, are known to be more resistant to physical attacks compared to software-based random number generators. However, during the process of converting physical phenomena such as thermal noise into digital values within a TRNG, the randomness can be disrupted. Moreover, TRNGs require countermeasures against characteristic changes caused by factors such as component aging and temperature fluctuations. Furthermore, conventional TRNGs often include complex post-processing circuits to monitor output, provide feedback, and suppress variation. These additional circuits result in increased chip area and higher power consumption.

◆Description

This invention is a physical random number generator comprising two inverter circuits, a latch circuit capable of outputting random data, and a circuit that autonomously cancels out variations to ensure stable operation.

- **Achieves stable operation by autonomously compensating for variation (Fig. 1)**
  The probability of outputting a 1 in the standalone circuit of this technology is distributed around 0.5.
- **Significant reduction in power consumption (Fig. 2)**
  Compared to conventional TRNGs (e.g., Latch w/ calibration), the proposed TRNG (Strong Arm Latch) achieves over a 90% reduction in power consumption.

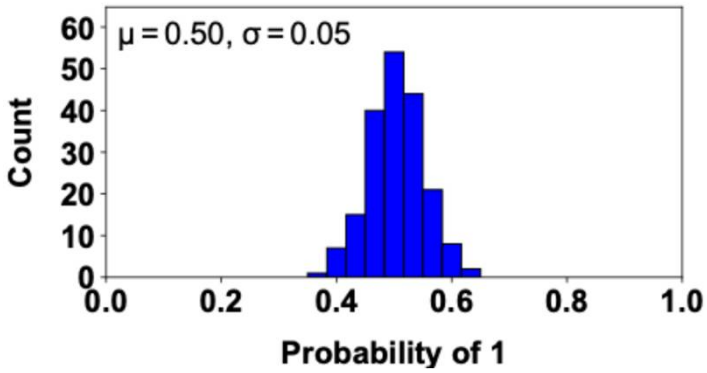

Fig. 1: Probability distribution of output "1" in a single circuit

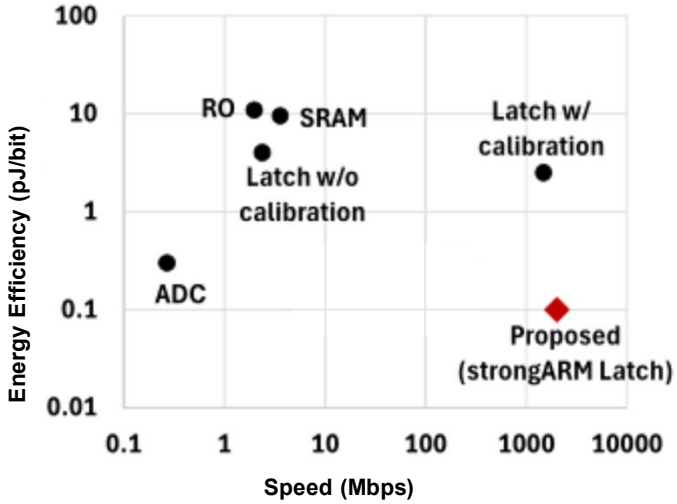

Fig. 2: Comparison between conventional TRNG and the proposed TRNG

◆Development Status

- Circuit operation verified through CMOS prototyping

◆Applications

- Devices requiring random number generation circuits (e.g.) AI, communication devices

◆Offer

- Patent License
- Option for Patent License

◆Contact

TLO-KYOTO Co., Ltd.

Mail: licensing_ku@tlo-kyoto.co.jp
Phone: +81-75-753-9150

Level 3, International Science Innovation Bldg., Kyoto Univ., Yoshidahonmachi, Sakyo-ku, Kyoto 606-8501, Japan

IAC Institutional Advancement and Communications

TLO-KYOTO