A Low-Cost Low-Power Ring Oscillator-based Truly Random Number Generator for Encryption on Smart Cards

The design of a low-cost low-power ring oscillator-based truly random number generator (TRNG) macro-cell, suitable to be integrated in smart cards, is presented. The oscillator sampling technique is exploited and a tetrahedral oscillator with large jitter has been employed to realize the TRNG. Techniques to improve the statistical quality of the ring oscillator-based TRNGs’ bit sequences have been presented and verified by simulation and measurement. Post digital processor is added to further enhance the randomness of the output bits. In standard CMOS process, the proposed TRNG fabricated in HHNEC 0.13 has an area as low as 0.005 mm². Powered by a single 1.8 V supply, the TRNG has a power consumption of 40 µW. Bit rate of the TRNG voltage, the TRNG has a power consumption of 40 µW after post processing is 100 kb/s. The proposed TRNG has been made into an IP and successfully applied in an SD card for encryption application. The proposed TRNG has passed the NIST tests and Diehard tests.