Compact floating-gate true random number generator

P. Xu, Y.L. Wong, T.K. Horiuchi and P.A. Abshire

A compact true random number generator (RNG) integrated circuit with adjustable probability is presented. Hot-electron injection is used in a floating-gate MOSFET to program the probability. Measurements show no cross-correlation between adjacent RNG circuits, allowing multiple RNGs to be easily integrated.

Introduction: Random number generation is indispensable in cryptography, scientific computing and stochastic computing. In cryptography, the quality of randomness of the generator is critical for security [1]. The pseudo-RNG generates sequences using a deterministic algorithm, so the sequence inevitably repeats and becomes predictable. A true RNG is nondeterministic and unpredictable, often relying on the randomness of physical noise. IC-compatible, true-RNG circuits are increasingly required in system-on-chip solutions for secure communication and stochastic computation. Noise amplification with thresholding, oscillator sampling, discrete-time chaos and metastability have all been used previously in IC-based RNGs [2, 3]. In this Letter, we present a new, true-RNG IC using the competition between noise sources. The circuit is very compact with less than 20 transistors. We use hot-electron injection in floating-gate MOSFETs in a negative feedback configuration to cancel fabrication mismatch and set the probability close to 50%. In the results to follow, we demonstrate high-quality randomness and robustness against interference by observing bit sequences generated by fabricated chips.

Circuit design: The core of our RNG is a clocked, cross-coupled differential pair comparator, as shown in Fig. 1, with input voltages V_{i+} and V_{i-}. The same circuit has previously been used in an adaptive comparator for offset cancellation [4]. When V_{clk} is logic high, $V_{o+} \simeq V_{o-}$. When V_{clk} becomes logic low, transistor M5 shuts off, V_{o+} and V_{o-} are nearly equal and the circuit is in its metastable state. If V_{g+} is significantly higher than V_{g-}, V_{o+} increases rapidly and V_{o-} decreases rapidly. This positive feedback leaves V_{o+} close to V_c and V_{o-} close to ground. If V_{g+} is significantly lower than V_{g-}, the opposite happens. When V_{g+} is very close in value to V_{g-}, thermal noise and $1/f$ noise that produce fluctuations in the drain currents of M1 and M2 will dictate the outcome. The final result depends on the sign of the imbalance, $V_{o+} - V_{o-}$, which triggers positive feedback after transistor M5 shuts off.

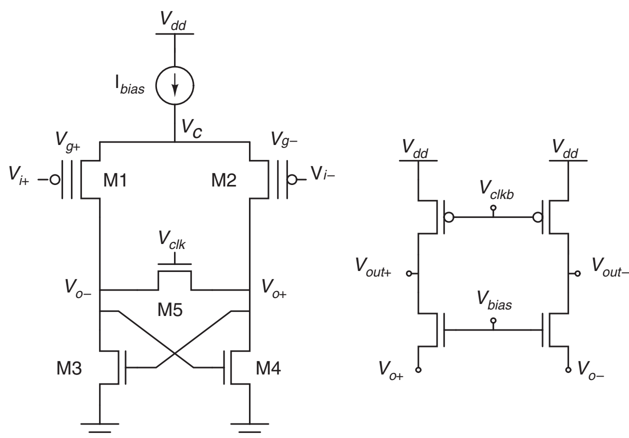

Fig. 1 *RNG circuits: clocked comparator (left), dynamic buffer (right)*

Fabrication mismatch in an uncompensated circuit would likely permanently bias the circuit to one solution. In this circuit, floating-gate inputs to a *p*-FET differential pair allow the mismatch to be compensated for [4]. Since there is no direct electrical connection to the floating gate, its potential is determined by capacitive coupling to nearby nodes and charge stored on the node. The voltage at the floating gate can be modified with fine resolution by hot-electron injection or tunnelling mechanisms. The circuit uses a nominal power supply of 5 V, which is sufficient for injection, and a 15 V supply for tunnelling used only during initialisation.

By controlling the common-mode voltage of the floating gates, we operate the circuit such that hot-electron injection occurs only on the side where the output voltage is close to ground. When one floating gate is higher in voltage than the other, the comparator output on that side will be pulled low. Over multiple clock cycles hot-electron injection works in negative feedback to equilibrate the floating-gate voltages. This is the equilibrium point around which the circuit operates as an RNG. We use a dynamic buffer, driven by the complement of the same clock, to convert the voltage at V_{o+} or V_{o-} into a digital signal.

The RNG has been fabricated in a commercially-available 0.5 µm CMOS technology with two polysilicon layers and three metal layers. One RNG occupies an area of only 1.83×10^{-2} mm^2. The layout was not optimised for minimum size, but special attention was paid to make the layout as symmetrical as possible. The RNG is surrounded by a guard ring to reduce interference from neighbouring circuits. There are eight RNGs in the fabricated chip.

Statistical tests: For the first test of randomness and independence, we examined the autocorrelation and cross-correlation of generated bit sequences with inputs V_{i+} and V_{i-} connected to ground. The experiments match the theory closely, i.e. an independent, identically distributed (i.i.d.) random bit sequence with probability p of 1 has an autocorrelation function $R(n) = p$ for $n = 0$, and $R(n) = p^2$ for $n \neq 0$, and its power spectrum density (PSD) is flat across all frequencies except for a DC component from the nonzero mean. Two i.i.d. sequences with probability p have a cross-correlation function $R(n) = p^2$ for all n and the cross-spectral density is also flat across all frequencies except for a DC component. Fig. 2 shows the PSD of one bit sequence. Fig. 3 shows the autocorrelation of one sequence and cross-correlation of two sequences. Existing methods can readily remove small biases in the probability [1] caused by injection mismatch. An exclusive-OR (XOR) of multiple independent random sequences will exponentially converge to an equal probability of 0 and 1 and simultaneously eliminate slight anti-correlation between adjacent bits, caused by kickback noise in the comparator and visible in Fig. 3 for $n = 1$.

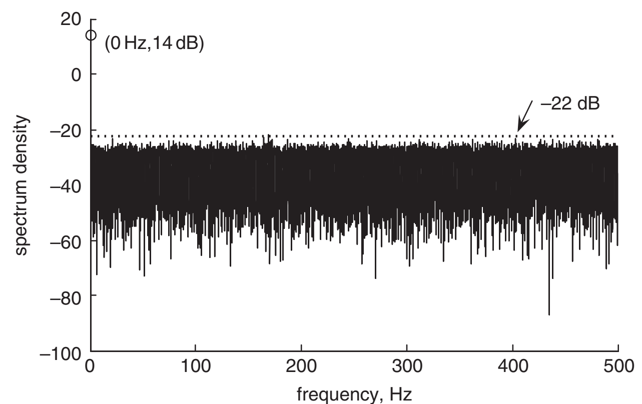

Fig. 2 *PSD for one bit sequence at sampling frequency 1 kHz (similar results are obtained for measurements up to 200 kHz)*

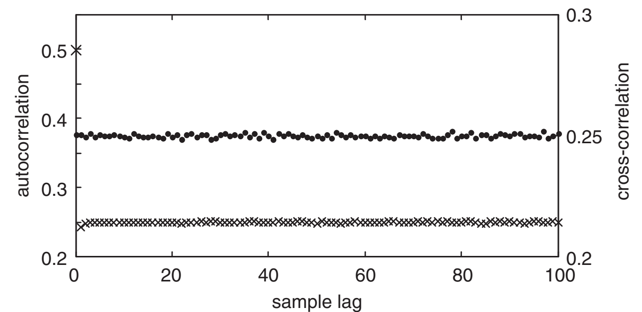

Fig. 3 *Autocorrelation for bit sequence from one RNG (x) and cross-correlation between bit sequences from two RNGs (●)*

For clarity, only data up to sample lag of 100 is shown

For a rigorous test of the RNG circuit, we applied a battery of benchmark statistical tests developed by the National Institute of Standards and Technology (NIST). The test suite includes a total of 16 different tests [5]. 20 sequences of 10^6 bits from the XOR of four RNGs were evaluated against all 16 tests. They passed all tests with a significance level of 0.01 except for the overlapping template matching test, missing 3 of 148 templates by a small margin (0.90 pass rate against a 0.92 threshold).

Adjustable probability: The probability of the bit sequence can be adjusted by tuning the DC input voltage applied between V_{i+} and V_{i-} while the circuit is operating near the metastable state. Fig. 4 shows the probability as a function of the input offset voltage. At each offset voltage, sequences of 10^5 bits are collected and partitioned into ten sub-sequences from which the mean and standard deviation of the probability are computed.

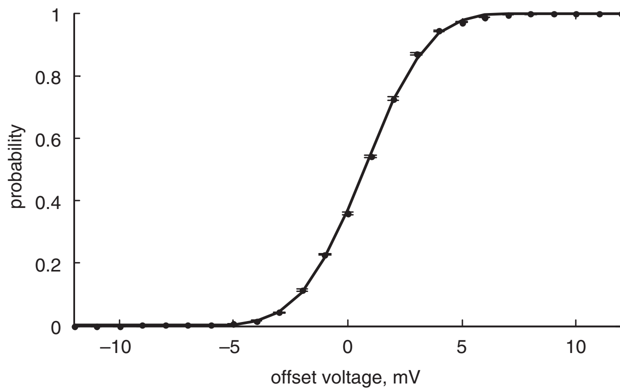

Fig. 4 *Probability against input offset*

Solid line is given by $p(v) = 0.5 \times (1 + \mathrm{erf}[(v - u)/\sqrt{2}\delta])$, where $u = 0.71$ and $\delta = 2.16$

The fluctuation of drain currents produces voltage fluctuation at V_{o+} and V_{o-}. According to the Central Limit Theorem this fluctuation can be approximated as a Gaussian random variable, so the voltage difference ΔV_o is also Gaussian. Its mean value increases with the input offset voltage. It is reasonable to model the circuit as having a fixed threshold voltage, above which fluctuations trigger positive feedback. The probability of a Gaussian random variable being larger than a fixed value is an error function of its mean value. The probability of obtaining a '1' in the sequence thus closely matches an error function. Input offset can be biased to produce very low probabilities (measured as low as 0.004% in Fig. 4) that historically have been difficult to obtain reliably.

Interference: To test the robustness of the RNG, we evaluated its performance against several common sources of interference such as power supply noise digital noise and substrate noise. We use the difference Δd between the PSD value at DC and the maximum value in the band excluding DC as an indicator of the interference noise power that is coupled into the PSD of the random bit sequence. The measured value without intentionally adding interference is 36 dB (Fig. 2). We injected sinusoidal signals of different frequencies (10 Hz, 100 Hz and 1 kHz) and amplitudes (1, 5 and 10 mV) onto the power supply voltage. The lowest Δd were 33, 26 and 21 dB for amplitudes 1, 5 and 10 mV, respectively. We used an on-chip shift register as one example of a digital circuit to evaluate the impact of nearby digital circuitry on the RNGs. The lowest Δd observed was 27 dB. We also injected noise into the substrate by driving 10 Hz, 100 Hz and 1 kHz square waves (amplitudes up to 2 V) through ESD-protected pads. The interference from these square waves was negligible, with the lowest Δd at 33 dB.

Conclusions: We have presented a novel RNG IC with good randomness and robustness to interference. Future improvements include: optimised layout for size, reduced anti-correlation, charge pumps to generate the high voltages used at initialisation, and improved control in programming the variable probability.

© The Institution of Engineering and Technology 2006

7 August 2006
Electronics Letters online no: 20062472
doi: 10.1049/el:20062472

P. Xu, Y.L. Wong, T.K. Horiuchi and P.A. Abshire (*Department of Electrical and Computer Engineering and Institute for Systems Research, University of Maryland, College Park, MD 20742, USA*)

E-mail: pxu@umd.edu

References

1 Schneier, B.: 'Applied cryptography' (John Wiley & Sons, New York, 1996)
2 Petrie, C.S., and Connelly, J.A.: 'A noise-based IC random number generator for applications in cryptography', *IEEE Trans. Circuits Syst. I*, 2000, **47**, (5), pp. 615–621
3 Ranasinghe, D.C., Lim, D., Devadas, S., Abbott, D., and Cole, P.H.: 'Random numbers from metastability and thermal noise', *Electron. Lett.*, 2005, **41**, (16), pp. 13–14
4 Wong, Y.L., Cohen, M.H., and Abshire, P.A.: 'A floating-gate comparator with automatic offset adaptation for 10-bit data conversion', *IEEE Trans. Circuits Syst. I*, 2005, **52**, (7), pp. 1316–1326
5 Rukhin, A., *et al.*: 'A statistical test suite for random and pseudorandom number generators for cryptographic applications'. NIST Special Publication 800–22, 2001