# A Low-Cost Lightweight Random Number Generator Implementation

Mala Mitra
*Department of Electronics and Communication Engineering, PESIT, Bangalore South Campus, Bangalore.*

## Abstract

*In this paper, a true random number generator based on operational amplifiers is proposed. The circuit consists of an operational amplifier with a positive feedback. It is a Schmitt trigger without any applied input signal. The circuit gives a positive (bit 1) or negative (bit 0) saturated output voltage depending on the polarity of the differential input governed by the thermal noise voltage of the resistors. There is no need to amplify the noise voltage. The circuit response is analyzed with TINA-TI tool. The circuit is implemented using IC LM741 operational amplifier chip as well as on the on-chip operational amplifiers of the MSP430 microcontroller. Due to low data-rate, a small volume of data should be generated. These random data can be used as a seed value for a pseudo random number generator. The data passed NIST test. The generator can be implemented on WISP RFID tags, which have built-in MSP430 microcontrollers.*

***Keywords:*** NIST test, Operational amplifiers, Probability, Programmable circuits, Random number generation, Thermal noise.

## 1. Introduction

Random Number Generators (RNGs) are required in many fields of technology. It may be a Monte-Carlo simulation or an optimization with Genetic Algorithm, or a digital circuit testing or a privacy and security algorithm. The robustness of the technology is primarily dependent on the quality of the Random Number Generator (RNG). Many RNGs have been proposed in recent times and in the past [1 - 24]. Depending on the operating principle, RNGs are classified into two categories: True Random Number Generators (TRNGs) and Pseudo Random Number Generators (PRNGs).

In a True Random Number Generator (TRNG) the input is extracted from a natural phenomenon which we believe to be random from our age-old experience. Gaussian random thermal noise voltage in a resistor is a popular choice for a TRNG input. A very common strategy is to amplify this noise and to get random numbers from the polarity of the amplified noise with the help of a comparator. So far the output bit string showed non-random behavior as deterministic noise of the amplifier dominated over the input random thermal noise and the finite bandwidth of the amplifier colored the white noise [17].

Though a PRNG produces output bits by deterministic processes the complexity of the algorithm makes the bits to appear as random or unpredictable. Use of a mathematical series or use of sea of gates e.g. combination of shift registers and XOR gates is a standard practice. The generation starts from an initial state or seed value. A PRNG gives the same sequence of random numbers if the same seed value is used. Since the PRNG algorithm is available from the product and open to all the unpredictability of the bits lie with the secrecy of the seed value used. In an automated system like RFID user cannot input this secret or unpredictable value. If date or time is used as seed, unpredictability is lost. Apart from this problem, PRNGs are very efficient. Some of the recently proposed PRNGs [3, 4] pass the NIST test [25], the statistical test suite to certify that the data is unpredictable. Unlike TRNGs, PRNGs can deliver bits at a high data-rate with nominal power consumption. For a low-cost solution, the algorithm can be implemented in the already existing microcontroller. As a contrast to PRNG, a TRNG delivers bits at a low data-rate with high power consumption. All the reported TRNGs need analog circuits with complex controls. That makes it very difficult to fabricate and characterize the chip. In some cases, a part of the design is implemented on Si. In most of the cases, only simulated results are reported. In some cases, the product prototype is not lightweight. The main advantage of TRNG is: it does not require a seed value. A recent idea is to combine a TRNG and a PRNG [26]. A TRNG may be used to create a low volume of data needed for the seed value of the PRNG.

In this work, a TRNG is proposed that is suitable for generation of seed values. The TRNG is implemented on IC LM741 operational amplifier (op-amp) chip and on the operational amplifiers (op-amps) of the MSP430 microcontroller as well. The technology can be used in the popular WISP RFID tags with built-in MSP430 microcontrollers. MSP430 microcontroller is widely used for RFID tags as it can operate at ultra-low power and it provides a great computational facility. C. Pendl *et al.* [27] showed that, ECC, a very computationally intensive asymmetric cryptographic algorithm for information security can be implemented on MSP430 microcontroller. Further, MSP430 has in-built security sensors useful for RFID tags. RFID tags are prone to temperature and power attacks [28]. An adversary may make a temperature attack by deliberately changing the ambient temperature of the tag. Due to temperature variation, some of the bits may become predictable. MSP430 has an in-built temperature sensor that may be used to interrupt bit generation when the temperature goes out of range to prevent malfunction of the RNG. In case of a power attack, adversary's detector transmits less power to a passive RFID tag to predict the bits. The brownout detector of MSP430 can take care of this situation. Table 1 and 2 shows the interesting features of the recently proposed RNGs. It can be observed from the Tables that for TRNGs either power consumption is very high or data-rate is low. Sometimes it does not pass the NIST test. Implementation complexity is also there. PRNGs work fine but seed value requirement may create a problem. In the next section the theory of random number generation for this TRNG is discussed.

## 2. Theory

The theory of random number generation in a dual supply op-amp is much simpler as compared to that generated from a single supply op-amp. In this paper, both the cases are discussed. Figure 1 gives the circuit configuration of an rng with a dual supply op-amp. This is a Schmitt trigger circuit without any input signal. The positive and negative supplies are replaced by clock named as Clock and inverted clock named as ClockN. When Clock and ClockN are at 0 voltages the circuit output becomes 0 volt. At the instant when Clock becomes positive and ClockN negative the output saturates to a positive or a negative value. The polarity of the output is decided by the polarity of the difference input, resultant thermal noise voltages across the resistors in this case. Since the polarity of the output is dependent only on the resultant polarity of the thermal noise voltages it is truly random.

The bi-stable states of a Schmitt trigger circuit was tried earlier to generate random numbers. Random thermal noise was amplified and applied to the Schmitt trigger circuit input. Two unanticipated problems occurred. Firstly, amplification introduced deterministic noise. Secondly, the trigger points were too closely spaced to change the output state [29]. It is to be noted that, in the proposed circuit, noise is not amplified its polarity at the instant of active supplies decides the output.

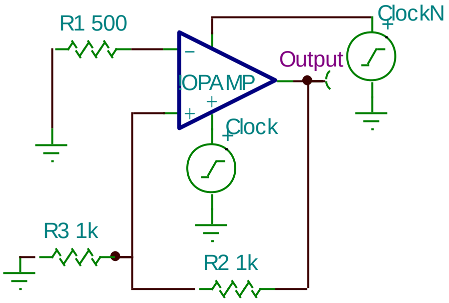

Figure 1. Random Number Generator Circuit

For a single positive supply op-amp a difference input $V_{diff}$ with a positive polarity is most likely to latch the output at $V_{sat}$, the saturation voltage. If the input is changed in subsequent instants, output remains $V_{sat}$ as long as the op-amp is on. For a negative polarity input at switch on, the output becomes zero and does not latch. At the next instant if the polarity is positive, the output latches. If the op-amp remains on for a finite time the polarity must become positive at some instant and the output will be always $V_{sat}$. Let us assume that, the op-amp remains on for slew time or the time taken by the output to change its state. The output will become $V_{sat}$ if at the $0^{th}$ instant or switch on instant $V_{diff}$ is positive. At the time of switch off the output will reach the highest level n corresponding to $V_{sat}$. A first time positive $V_{diff}$ at a later instant will reduce the output proportionately. In mathematical notations:

$$V_{diff} = V_{th} + V_{offs} + V_{fb} \qquad (1)$$

where $V_{th}$ is the combined random thermal noise for the three resistors at any instant, $V_{offs}$ is the offset voltage usually kept negative for a single supply op-amp to avoid thermal noise effects. $V_{fb}$ is the feedback voltage and can be given as:

$$V_{fb} = \frac{R_3}{R_2 + R_3} V_{out} \qquad (2)$$

At the time of switch on or instant 0, the output voltage should be kept zero:

$$V_{out}(0) = V_{fb}(0) = 0 \qquad (3)$$

$V_{th}$ can be negative or positive with equal probability of 0.5. The probability of positive $V_{diff}(0)$ is less than 0.5 as $V_{offs}$ is negative. If $V_{diff}$ (0) is positive the voltage build up at the output starts. However, that build up may get destroyed at the next instant due to a dominating negative $V_{th}$. The next instant is defined when the $V_{th}$ can change its polarity. The time between 2 consecutive instants $t_{re}$ depends on electron response time and $t_{re}$ « T. where, T is the slew time, the time taken by the op-amp to change its output state. Let the op-amp is kept on for T. Let there be n+1 instants or n time slots then:

$$T = nt_{re} \qquad (4)$$

Thus, there are (n+1) output states corresponding to (n+1) generation instants. A positive $V_{diff}$ does not guarantee a build up. It may get destroyed in subsequent instants. Assuming the output voltage develops linearly with time the output voltage at instant 1 for a positive $V_{diff}$ (0):

$$V_{out}(1) = \frac{t_{re} V_{sat}}{T} \qquad (5)$$

The output voltage build up can be destroyed for negative $V_{diff}$ for the condition obtained from Eq. 1:

$$0 < -[V_{th}(1) + V_{offs}] > V_{fb}(1) \qquad (6)$$

Let $p_{gen}$ be the probability that generation takes place. Clearly $p_{gen}$<<0.5 due to (i) negative offset voltage and (ii) possibility of destruction of positive voltage build up. The probability that at instant 0 generation takes place is $p_{gen}$. The probability that at instant 1 generation takes place is the joint probability of: (i) no generation at instant 0 of probability 1 – $p_{gen}$ and (ii) generation at instant 1 of probability $p_{gen}$ and is given by: (1-$p_{gen}$) $p_{gen}$. The probability approximates to $p_{gen}$ as $p_{gen}$ <<1. Similarly the probability that at instant 2 generation takes place is the joint probability of: (i) no generation at instant 0, (ii) no generation at instant 1, and (iii) generation at instant 2 and is given by: $(1-p_{gen})^2$ $p_{gen}$. The probability approximates to $p_{gen}$ as $p_{gen}$ <<1. From this analysis, one can see that, generation instants are almost equally probable. The generated output voltages in the range 0 to $V_{sat}$ forms a continuous pattern as $t_{re}$ <<T and are roughly equally probable. If these analog voltages are expressed in binary it is expected that the bits will be random. The next section gives the implementation and measurement details of these circuits.

## 3. Measurement results

The circuit given in Figure 1 was implemented on a breadboard with IC LM741 dual-supply op-amp. Instead of using clock pairs the supply switch was made on-off. This eliminates the possibility of a clock skew and a residual charge build-up (discussed in Sec. 2) at the output. For the dual supply op-amp 289 data were collected. Some of the tests in NIST require $10^6$ bits. Only those tests with recommended data size less than 289 were carried out. The details of the tests were reported elsewhere [30]. All the tests were passed.

The proposed circuit was also implemented on the three op-amps available in the MSP430FG4618 microcontroller. The circuit configuration requires two modifications from Fig. 1: (i) instead of dual supply only a single positive supply is available (ii) instead of a clock pair programming language instructions were used to make it on/off. Unfortunately, there is no instruction available in MSP430 to connect the on-chip resistors in the positive feedback mode. Op-amp was configured in general-purpose mode with the two inputs and the output connected at three port pins. External resistors were connected to these pins.

In MSP430 three slew rates are available. The slowest slew rate, 0.3 V/µS, was selected. This gives a slew time of 8.933 µS for the saturation voltage same as supply voltage $V_{CC}$ =2.68 V. As discussed in sec. 2, it is expected that the op-amp should produce equally probable output between 0 and 2.68 V, if it is switched on for the slew time. For a switch on of 8.9 µS the observed output was close to zero for most of the time. The switch on time was increased approximately to a value of 11 µS where the binary equivalents of the outputs gave equal number of 0s and 1s. The increase in time might be due to a latency required by the op-amp to get on after the instruction is executed in MSP430. This latency was also observed in simulation as discussed in Sec. 4. The time was adjusted only once, no further adjustment was necessary for long time use heating or ambient temperature variation.

For further applications, the analog output voltage can be converted to binary with the use of the on-chip ADC. In this work, for data analysis the analog voltage was measured at a port pin with a voltmeter with 2 decimal point resolution, and typed to a data-file. The voltage should be scaled in the range 0 to 255 for 8 bit binary. To avoid the round-off error, which is, slightly deterministic each analog voltage is multiplied by 100 and converted to 8 bit binary. For analog values greater than 2.55 the most significant bit was thrown. In this way 4 bits were ignored that is immaterial for a statistical test.

At every switch on the output voltage or the residual charge at the output should be zero. To ensure that, the op-amp was switched off for 5.5 µS followed by a negative feedback configuration for 11 µS and then switch off for 5.5 µS. For negative feedback same instruction as positive feedback was used except the + and – inputs were interchanged. Table 3 gives the sequence. The sequence repeats after 6 time-slots.

In each time slot of 11 µS one op-amp in positive feedback configuration produces 8 bit random data. This gives data-rate as: 8/11 Mbps=727 Kbps. The microcontroller current was measured at the power measurement jumper and was found to be 1332 µA. This gives the power consumption as: 2.68 VX1332 µA=3.57 mW. The performance of the circuit may further be improved by use of integrated resistors and design optimization. Application specific design optimization of a Schmitt trigger circuit is getting attention in recent days [31]

A low volume of data of 2368 bits was collected, as automated set-up was not ready. The data was analyzed with NIST test suite [25], the present statistical test suite to certify the unpredictability of the data. 12 out of 17 tests were done. Only those tests that need sequence length less than 2368 were done. The test suite was written in MATLAB and was tested for sequences with predictable results. These test sequences were: (i) 0000----, (ii) 11111---- (iii) 1010---.

Table 4 shows that the data qualifies for NIST test. This certifies that, the low volume of data or seed value is unpredictable. From the theory of generation, it seems the data is random and a large volume of data should pass the remaining tests as well.

## 4. Simulation results

To analyse the behaviour of random number generation for a dual-supply op-amp simulation was done in TINA-TI tool. This is a tool developed and supported by Designsoft and Texas Instruments. IC LM741 op-amp [32] was configured in TINA-TI. The circuit is given in Figure 1. In this simulator resistors cannot be modelled for thermal noise voltages. To understand the effect of thermal voltage $V_{diff}$, input pulse of amplitude - $V_{diff}$ is applied at the inverting terminal of the op-amp.

The transient simulation output is shown in Figure 2 and 3. The instantaneous amplitude of the pulse -$V_{diff}$ at the time of effective clock decides the output pulse polarity with a negation. The output was observed to remain 0 for 3.53 µs even after the clock became effective. This type of latency was observed at the time of measuremnet as well and discussed in Sec. 3. The effect of slew-rate 0.5 V/µs can be observed in the plot with a slow rise time. It can be observed from the plot the output voltage takes expected slew-time of 4 µs to rise from 0 to 2 volts. To have a good pulse shape either slew-rate has to be increased or clock-rate has to be decreased. Figure 3 shows a better output pulse for a reduced clock-rate.

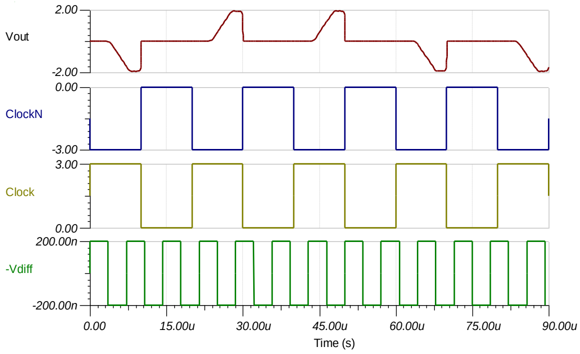

**Figure 2. Simulation 1 for LM741**

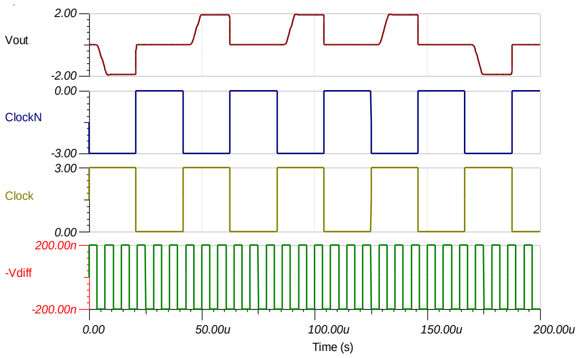

**Figure 3. Simulation 2 for LM741**

## 5. Conclusion

A true random number generator was implemented with a dual-supply operational amplifier. This was also implemented with the single-supply operational amplifiers of an MSP430 microcontroller, used widely for RFID tags. The random thermal noise voltage of the resistors at the input of an on-off mode positive feedback operational amplifier in the Schmitt trigger configuration was utilized to generate the random numbers. The data passed the NIST test, the test of unpredictability. Due to moderate power consumption and low data-rate, the data is suitable as a seed value for a pseudo-random number generator.

## 6. References

[1] Chien-Yuan Huang, W. C. Shen, Yuan-Heng Tseng, Ya-Chin King, and Chrong-Jung Lin, “A Contact-Resistive Random-Access-Memory-Based True Random Number Generator”, IEEE Electron Device Letters, vol. 33, pp. 1108 - 1110, Aug. 2012.

[2] M. Hamburg, P. Kocher, and M. E. Marson, "Analysis of Intel's Ivy Bridge Digital Random Number Generator", Cryptography Research Inc., March 2012. Available: http://www.cryptography.com/public/pdf/Intel_TRNG_Report_20120312.pdf. Accessed 4 October 2012.

[3] Chung-Yi Li, Yuan-Ho Chen, Tsin-Yuan Chang, and K. To, “Period Extension and Randomness Enhancement Using High-Throughput Reseeding-Mixing PRNG”, IEEE Trans. VLSI Syst., vol.20, pp. 385 - 389, Feb. 2012.

[4] M. Merhi, J. C. Hernandez-Castro, and P. Peris-Lopez, “Studying the Pseudo Random Number Generator of a Low-cost RFID Tag”, in *Proc. IEEE International Conferences RFID TA*, Sep. 2011, pp. 381-385.

[5] H. Martin, E. S. Millan, L. Entrena, P. Peris-Lopez, and J. C. Hernandez-Castro, “AKARI-X: A Pseudo-Random Number Generator for Secure Lightweight Systems”, in *Proc. 2011 IEEE 17th International On-Line Testing Symposium IOLTS*, July 2011, pp. 228 - 233.

[6] T. Sugiura, Y. Yamanashi, and N. Yoshikawa, “Demonstration of 30 Gbit/s Generation of Superconductive True Random Number Generator”, IEEE Trans. Appl. Supercond., vol. 21, pp. 843 - 846, June 2011.

[7] J. M. Segui, J. G. Alfaro, and J. H. Joancomarti, “A Practical Implementation Attack on Weak Pseudorandom Number Generator Designs for EPC Gen2 Tags”, in *Proc. Wireless Personal Communications*, July 2011, pp. 1 -17.

[8] P. Peris-Lopez, E. S. Millan, J. C. A. V. Lubbe, and L. A. Entrena, “Cryptographically Secure Pseudo Random Bit Generator for RFID Tags”, in *Proc. ICITST’10*, Nov. 2010, pp. 490-495.

[9] S. A. Wilber, "Random number generator and generation method", U.S. Patent No. 7752247 B2, 2010.

[10] H. Debiao, C. Jianhua, and H. Jin, "A Random Number Generator based on NTRU Cryptosystem", Maejo International Journal of Science and Technology, vol. 4, no.3, pp. 428 - 434, 2010.

[11] S. S. Saab, J. G. Hobeika, and I. E. Ouaiss, “A Novel Pseudorandom Noise and Band Jammer Using a Composite Sinusoidal Function”, IEEE Trans. Signal Process., vol. 58, pp. 535 - 543, Feb. 2010.

[12] Y. Yamanashi and N. Yoshikawa, “Superconductive Random Number Generator Using Thermal Noises in SFQ Circuits”, IEEE Trans. Appl. Supercond., vol. 19, pp. 630 - 633, June 2009.

[13] O. Katz, D. A. Ramon, and I. A. Wagner, “A Robust Random Number Generator Based on a Differential Current Mode Chaos”, IEEE Trans. VLSI Syst., vol. 16, pp. 1677 - 1686, Dec. 2008.

[14] C. Tokunaga, D. Blaauw, and T. Mudge, “True Random Number Generator with a Metastability-Based Quality Control”, IEEE J. Solid-State Circuits, vol. 43, pp. 78 - 85, Jan. 2008.

[15] L. Westlund, “Random Number Generator using the MSP430”, Application Report, Texas Instruments, 2006. Available: http://focus.ti.com/lit/an/slaa338/slaa338.pdf Accessed 15 December 2011.

[16] S. Yasuda, H. Satake, T. Tanamoto, R. Obha, K. Uchida, and S. Fujita, “Physical Random Number Generator based on MOS Structure after Soft Breakdown”, IEEE J. Solid-State Circuits, vol. 39, pp. 1375 – 1377, Aug. 2004.

[17] M. Bucci, L. Germani, R. Luzzi, P. Tommasino, A. Trifiletti, and M. Varanonuovo, “A High-Speed IC Random-Number Source for SmartCard Microcontrollers”, IEEE Trans. Circuits Syst. I: Fundam. Theory Appl., vol. 50, pp. 1373-1380, Nov. 2003.

[18] C. S. Petrie and J. A. Connelly, “A Noise-Based IC Random Number Generator for Applications in Cryptography’’, IEEE Trans. Circuits Syst. I: Fundam. Theory Appl. (until 2003), vol. 47, pp. 615 – 621, May 2000.

[19] M. Bland and G. M. Megson, “Systolic Random Number Generation for Genetic Algorithms”, Electronics Letters, vol. 32, no. 12, pp. 1069 - 1070, June 1996.

[20] P. J. Pacini and B. Kosko, “Adaptive Fuzzy Frequency Hopper”, IEEE Trans. Commun., vol. 43, pp. 2111 - 2117, June 1995.

[21] M. J. Bellido, A. J. Acosta, M. Valencia, A. Barriga, and J. L. Huertas, “Simple Binary Random Number Generator”, Electronics Letters. vol. 28, no. 7, pp. 617 - 618, March 1992.

[22] G. M. Bernstein and M. A. Liberman, “Secure Random Number Generation using Chaotic Circuits”,

IEEE Trans. Circuits Syst. (1974 – 1992), vol. 37, pp. 1157 - 1164, Sept. 1990.

[23] A. J. Al-Khalili and D. M. Al-Khalili, “A Controlled Probability Random Pulse Generator Suitable for VLSI Implementation”, IEEE Trans. Instrum. Meas., vol. 39, pp. 168 - 174, Feb. 1990.

[24] J. L. Perry, R. W. Schafer, and L. R. Rabiner, “A Digital Hardware Realization of a Random Number Generator”, IEEE Trans. Audio Electroacoust. (until 1974), vol. AU-20, no. 4, pp. 236 - 240, Oct. 1972.

[25] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, A. Heckert, J. Dray, and S. Vo, “A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications’’, NIST Special Publication 800-22 revision 1a, pp. 1 – 131, April 2010. Available at: csrc.nist.gov/rng. Accessed 15 December 2011.

[26] G. Taylor, and G. Cox, “Digital Randomness / Behind Intel's New Random-Number Generator”, IEEE Spectr., pp. 1 - 5, Sept. 2011.

[27] C. Pendl, M. Pelnar, and M. Hutter, “Elliptic Curve Cryptography on the WISP UHF RFID Tag”, *in Proc. RFIDSec*, June 2011, pp. 1 - 16.

[28] K. Nohl and H. Plotz, “24C3 Mifare crypto1 RFID completely broken”, Posted by E. Phillips, Wireless hacks, Jan 2008. Available: http://www.hackaday.com/2008/01/01/24c3-mifarecrypto1-rfid-completely-broken/. Accessed 17 May 2012.

[29] D. Curtin, S. P. Hegarty, D. Goulding, J. Houlihan, T. Busch, C. Masoller, and G. Huyet, “Distribution of Residence Times in Bistable Noisy Systems with Time-Delayed Feedback”, Physical Review, vol. E 70, no. 031103, pp. 1 – 4, Sept. 2004.

[30] M. Mitra, “A Random Number Generator for RFID Tags”, IAEME International Journal of Electronics and Communication Engineering and Technology, vol. 1, no. 1, pp. 71 – 87, Sep. – Oct. 2010.

[31] T. Matic, T. Svedek, and M. Herceg, “A Method for the Schmitt-Trigger Propagation-Delay Compensation in Asynchronous Sigma-Delta Modulator”, IEEE Trans. Circuits and Systems II: Express Briefs, vol. 59, pp. 404 - 408, July 2012.

[32] LM741 Operational Amplifier, National Semiconductor, August 2000. Available: www.national.com Accessed 5 May, 2010.

### TABLE 1. FEATURES OF RECENTLY PROPOSED PSEUDO RANDOM NUMBER GENERATORS

| Information source | Working principle | Any particular drawback | Attack immune? | NIST test results | Implemented in embedded? | Implemented on Si? | Data-rate | Power consumption |
|---|---|---|---|---|---|---|---|---|
| [3] | Reseeding mixing PRNG | Requires seed values | No | 17 out of 17 passed | No | No. Only simulation | 6.2 Gbps | 13.9 mW@200 MHz, estimated |
| [4] | PRNG of MIFARE tags | Requires seed value | No | 17 out of 17 passed | Yes | No need | 127 KBps | Not known |
| [5] | PRNG using complex logic | Requires seed values | No | Passed. Not shown | No | No. Only simulation | ~100 Kbps | ~250 nW, estimated |
| [7] | A PRNG with a TRNG for seed value | -- | No | 14 out of 17 done, 1 failed | Yes | No need | Not known | Not known |
| [8] | A PRNG using Blum Blum Shub algorithm | Requires seed values | No | No | Yes | No need | 97 Kbps | Not known |
| [11] | A PRNG using mathematical functions | Requires seed values | No | No | No | No | Not known | Not known |
| [13] | A PRNG based on differential current mode chaos | Requires seed values | No | Not done | No | Yes | Not known | 0.8 mW |

### TABLE 2. FEATURES OF RECENTLY PROPOSED TRUE RANDOM NUMBER GENERATORS

| Information source | Working principle | Any particular drawback | Attack immune? | NIST test results | Implemented in embedded? | Implemented on Si? | Data-rate | Power consumption |
|---|---|---|---|---|---|---|---|---|
| [1] | Telegraphic random noise based TRNG in a CRRAM. | Bit pattern is sensitive to voltage drop across CRRAM. | No | 6 out of 17 done and passed | No | Yes | ~Kbps | Not known |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| [6, 12] | TRNG by thermal noise detection in SFQ circuit | Maintenance of superconductive temperature 4,2 $^0$K. Not portable. | No | 11 out of 17 done and passed | No | No. Only simulation | 30 Gbps | Not known. It must be very high for temperature maintenance |
| [14] | A TRNG with a meta-stability based quality control | Initialization time may be very high | Yes | 7 out of 17 done. Tests pass at a lower efficiency | No | Partly | 200 Mbps at the highest efficiency, does not pass NIST | Not known |
| [16] | A TRNG based on MOS at soft breakdown | May drift to permanent or no breakdown | No | Not shown | No | No | 50 Kbps | Not known |
| [17] | A TRNG based on direct amplification of thermal noise and further randomization | Direct amplification introduces deterministic noise | No | Not done | No | Partly | 40 Mbps estimated | 3.6 mW estimated |
| This work | A TRNG where instant polarity of themal noise decides the bits | -- | Yes | 12 out of 17 done and passed | Yes, MSP430 in WISP tag | No need | 727 Kbps | 3.57 mW |

### TABLE 3. SEQUENCE OF OP-AMP OPERATIONS*

| **Time slot in 5.5 μS →** | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** |
|---|---|---|---|---|---|---|---|---|
| Op-amp 1 | + FB | + FB | Off | - FB | - FB | Off | + FB | + FB |
| Op-amp 2 | - FB | Off | + FB | + FB | Off | - FB | - FB | Off |
| Op-amp 3 | Off | - FB | - FB | Off | + FB | + FB | Off | - FB |

*Positive (+), Negative (-), and feedback (FB)

### TABLE 4. NIST TEST RESULTS*

| **Test** | **Recommended input size** | **Input size** | **No. of sets** | **p_value pass percentege** |
|---|---|---|---|---|
| Frequency (monobit) | Sequence length $n \geq 100$ | n=100 | 23 | 100 |
| Frequency within a block | Block length $M \geq 20$, block no. $N<100$, sequence length $n=MN \geq 100$, $M>0.01n$ | n=100, M=20, N=5. | 23 | 100 |
| Runs | Sequence length $n \geq 100$ | n=100 | 23 | 100 |
| Longest run | Sequence length, n=128,<br>block length, M=8 | n=128, M=8 | 18 | 100 |
| Binary matrix rank | No. of blocks $N \geq 38$ | N=38, 2X2 matrix, n=152 | 15 | 100 |
| Discrete Fourier Transform (spectral) | Sequence length $n \geq 1000$ | n=1024 | 2 | 100 |
| Non-overlapping template matching | No. of blocks $N \leq 100$. Template size m=9 or 10 | Block-length M=70, N=1, m=9, n=70 | 33 for each template. Total template=148 | 98.64-100 for 148 p_values<br>Threshold 95.43 |
| Serial 1 | Block length $m \leq [\log_2 n]-2$. | n=16, m=2. | 148 | 99.32. Threshold 91.53 |
| Serial 2 | | | | 95.95<br>Threshold 91.53 |
| Approximate entropy | Block length $m<[\log_2 n]-5$. | n=65, m=1 | 36 | 100 |
| Cusum forward | Sequence length $n \geq 100$ | n=100 | 23 | 100 |
| Cusum backward | | | | |

$^*$p_value$\geq$0.01 to pass