Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 10, October : 2024

GDI based power optimised synchronous True Random Number Generator

[1]NAGAVARAPU GREESHMA, [2]RAMOJU BHEEMA SANKARAM
[1]PG Student, VLSI, Srinivasa Institute of Engineering and Technology, Cheyyeru Gunnepalli, A.P
[2]Assistant Professor, Dept. of ECE, Srinivasa Institute of Engineering and Technology, Cheyyeru Gunnepalli, A.P

ABSTRACT: It is desirable to generate a random key with a uniform distribution on all of its possibilities, so an adversary will have to try all of the options without a defined order. Processes that can generate a random number as the key are called Random Number Generators (RNGs). Note that the design of the RNG itself, as part of the encryption scheme, is also assumed to be publicly known. this existing method , STT-MTJ is used to construct an asynchronous true random number generator (TRNG) with low power and a high entropy rate. The asynchronous design enables decoupling of the random number generation from the system clock, allowing it to be embedded in low-power devices. The emerging Spin Transfer Torque Magnetic Tunnel Junction (STT-MTJ) technology exhibits interesting stochastic behavior combined with small area and low operation energy. This proposed process proposes a Design of single edge triggered low power d Flip Flop using GDI(Gate Diffusion Input Technique).As a result using GDI power consumption is Reduced and features the best power delay product. Proposed TRNG is designed using above modified GDI based D ff. The operation of the D flip flop is analyzed and simulated using Tanner EDA. The main aim of this work to minimize the power dissipation using GDI Technique. It is called Gate Diffusion Input Technique because the inputs are directly diffused into the gates of the transistors of N type and P type devices. This Negative edge triggered D flip flop is designed using Master slave configuration and both contains four GDI cells, and the sampling is done on the falling edge of the clock signal.

Index Terms: True random number generator, Spin Transfer Torque Magnetic Tunnel Junction, hardware security, Gate Diffusion Input.

INTRODUCTION: Computer systems and telecommunications play an important role in modern world technology. The communication and data transfer through computers touches almost every aspect of life, i.e. transferring data, tracking personal data, trading over the internet, online banking

and sending emails. As more vital information is transferred through wire or wireless means, the need to safeguard all this data from hackers is growing. All these security concerns emphasize the importance of developing methods and technology for the transformation of data to hide its information content, prevent its modification, and prevent unauthorized use. Random number generation is a fundamental process for protecting the privacy of electronic communications. It is a key component of the encryption process that protects information from attackers by making it unreadable without the proper decryption process. Since the strength of an encryption mechanism is directly related to the randomness of the binary numbers used in it, there has been an enormous need to design and develop an efficient random number generator that can produce true random numbers to implement a safe and secure cryptographic system. In addition to cyber security, random number generators (RNGs) are a vital ingredient in many other areas such as computer simulations, statistical sampling, and commercial applications like lottery games and slot machines. Random numbers are needed in some areas in computer science, such as authentication, secret key generation, game theory, and simulations. In these applications, particularly numbers should have good statistical properties and be unpredictable and nonreproducible. The number generation in the literature is performed in two different ways as deterministic and nondeterministic [1, 2]. PRNGs (Pseudo Random Number Generators), which are deterministic random number generators, generate numbers with fast, easy, inexpensive, and hardware independent solutions. The statistical qualities of these numbers produced are close to the ideal. PRNGs must meet the requirements specified in Table 1 to be used especially for authentication and key generation [3–5]. Therefore, nondeterministic functions are added to the output functions of PRNGs to guarantee these requirements. TRNGs (True Random Number Generators), which are nondeterministic random number generators, present slower, more expensive, and hardware-dependent solutions compared to PRNGs. Contrary to PRNGs, there is no need to include extra components in the TRNG system designs for R2, R3, and R4 requirements. Because of the unpredictability of random numbers generated by the use of high noise sources with high entropy in TRNGs, it is assumed that the R2 requirement is met. If the R2 requirement is satisfied, then it is assumed that the R3 and R4 requirements are also satisfied. To meet the R1 requirement in TRNGs,

postprocessing techniques are applied on the random numbers obtained by sampling from noise sources. This eliminates the statistical weaknesses of random numbers at the output of the TRNG. In addition, postprocessing techniques eliminate potential weaknesses and make TRNG designs strong and flexible [6, 7]. Recently, there have been studies performed on random number generation from human-based noise sources [8–12]. Elham et al. showed that two different people would produce different random numbers and that these numbers could be used as biometric signatures [8]. Xingyuan et al. proposed a TRNG structure using a one-dimensional chaotic map based on mouse movements. The proposed structure showed that NIST tests were successful and could be used on personal PCs [9]. Hu et al. performed real random number generation by observing mouse movements of computer users. The statistical properties of the binary number generators generated from mouse movements of three different users were examined by the NIST test suite. Three chaos-based approaches were proposed to eliminate similar motions generated by the same user. Successful results were also achieved with these approaches [10]. Rahimi et al. used two different ECG signals for the cryptographic key generation and suggested two different approaches. The security analyses of keys obtained by both approaches were tested with distinctiveness, randomness, temporal variance, and NIST and successful results were obtained [11].

LITERATURE REVIEW: This section highlights the literature survey which has been done to review the critical points of the related works in recent days. In an irreversible circuit, if one bit information is lost then at least KTln2 joules of energy is dissipated. Where K is Boltzmann's constant and T is absolute temperature. This was stated by Landauer R in 1961[1]. In 1973, Bennett[2] proved that, KTln2 joules of energy dissipated due to information loss in irreversible circuit can be controlled by reversible logic where the reversible circuit allows to reproduce the inputs from output resulting in no information loss. He also showed that reversible systems can do the same computations as the classical or irreversible systems at same efficiency. This leads to the evolution of reversible logic based systems. Any reversible gate should have equal number of inputs and outputs such that, inputs can be recovered uniquely from outputs at any point of time. In paper [3], by Shibinu

A.R , Rajkumar, a 4- bit LFSR design using Muller expression is proposed. This paper also gives realization of both edge triggered and level triggered D flip flop using reversible logic. At the end, comparative analysis has been given between conventional LFSR and Reversible LFSR. From this it is observed that, the proposed technique is efficient than conventional technique in implementing LFSR in terms of cost metrics like power, quantum cost, garbage output and gate count. D. Muthih and A. Arockia Bazil Raj [4] have presented a parallel architecture for designing high speed LFSR and explained that, BCH encoders and CRC operations are normally carried out by using LFSR. A novel approach for high speed BCH encoder is proposed. This paper presents two key points. First, it presents a linear transformation algorithm for converting a serial LFSR into parallel architecture, which can be used for generating polynomials in CRC and BCH encoders. Secondly, a new approach is proposed to amend parallel LFSR into pipelining and retiming algorithm. In paper [5], authors have presented two design approaches for designing reversible D FF with asynchronous set/reset which are optimized in terms of quantum cost, delay and garbage outputs. It also includes the design of 3 bit LFSR using two design approaches. The application of these FF's as LFSR is designed and discussed. The application of LFSR as pseudo random bit sequence generator is proposed. The paper is concluded with the comparative analysis of proposed approaches against performance parameters like garbage output, delay and quantum cost. Research paper [6], presents three different automated techniques for implementing LFSR as well as D flip flop so that the layout area and power consumption will be minimized. It is illustrated that LFSR is key component to provide self-test of an Integrated Circuit (IC). This paper implements LFSR upto layout level which will be a key component for low power application. The research explores the LFSR as well as D flip flop using different architecture in a 0.18μm CMOS technology; so that the layout area will be minimized and consumes less power. In paper [7], authors have presented a new approach for data compression and low- power test. This paper highlights the drawback of data compression schemes based on LFSR reseeding which increases the power dissipation and provides a new encoding scheme for reducing the power dissipation. With this background work, this paper mainly aims at design and implementation of an 8 bit LFSR using reversible logic for low power applications.

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 10, October : 2024

EXISTING METHOD: MTJ-based STT-MRAM System:

Spin-transfer-torque magnetic random-access memory (STT-MRAM) has attracted a lot of attention as a potential candidate for the forthcoming generation of high-density integrated non-volatile memory. [11]. A magnetic tunnel junction stores the information in the memory [12]. In general, it is far more trustworthy than magnetic quantum cellular automata. As shown in Figure 2, MTJ is a bit-memory cell that might store information in artificial neurons and synapses, nanomagnets, Bayesian inference engines, Boolean logic gates, and Boltzmann machines. Three elliptical layers make up this construction [13]. Between an insulator and a spacer layer are ferromagnetic outer layers. One of the ferromagnetic layers in one of the two stable orientations is a hard or fixed ferromagnetic layer with permanently aligned magnetization. Another choice is to utilize a soft or free layer of ferromagnetic material, which can have its magnetism point in one of two stable directions and encodes the bit information. The electrical resistance between the two ferromagnetic layers could be used to decode the encoding bit of the soft layer. The resistance drops dramatically when the two layers' magnetizations are parallel, but jumps up dramatically when they're antiparallel. [14].

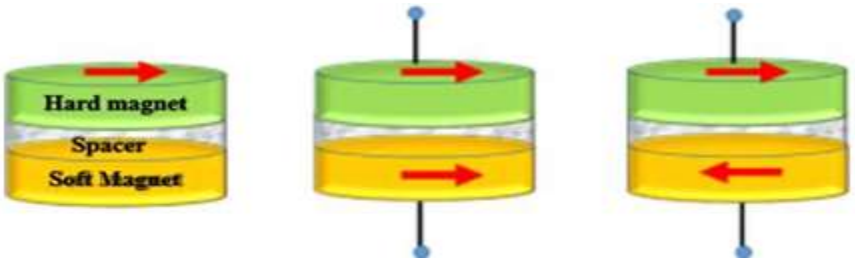

Figure1 : Low Resistance & High Resistance .

STT-MRAM (a kind of magneto-resistive random-access memory), which uses spinning-to-rotating torque as an example of a spintronic circuit, has advanced significantly in recent years [16]. Since flash memory (conventional non-volatile memory) has a low write endurance (105) and a high write access time compared to other non-volatile memory technologies (105 to 107 sec), while ferroelectric (FeRAM) and phase-change memory (PRAM) have written endurances of 109 to 1012, respectively,

STT-MRAM is a strong contender for universal memory. STT-MRAM, on the other hand, has a quick access time (in the range of nanoseconds) and high endurance.

STT-MTJ Devices:

A spin transfer torque (STT) magnetic tunnel junction (MTJ) is a device composed of two ferromagnetic layers with a tunnel barrier layer between them. One ferromagnetic layer, the fixed layer, has a fixed magnetization direction. The other ferromagnetic layer, the free layer, can switch its magnetization direction. In this paper, in-plane MTJs are used, where the magnetization direction of the ferromagnetic layers is in the plane of the layers. The spin-transfer torque mechanism enables the switching of orientation of the free layer magnetization. The electrons passing through a ferromagnetic layer tend to align their magnetic moment in the direction of the magnetization of the layer. Thus, electrons that pass through the fixed layer first are aligned with its magnetization direction. However, a damping process pulls the free layer magnetization to the closest stable state, requiring a sufficiently strong current for adequate time to enable a switch between the stable states. The switching processbetween the P and AP states is random [15] due to the thermal fluctuations in the ferromagnetic layers. Although the current through the MTJ pushes the magnetization of the free layer to a certain stable state (through unstable intermediate states), thermal fluctuations will make the path to that state random, resulting in a random switching time. Even if no current is applied, the state of the STTMTJ fluctuates constantly since the thermal fluctuations occur regardless of the existence of the current. The state of the MTJ also determines its resistance, where the P state resistance is marked as Ron, the AP state is marked as Roff , and Ron < Roff . The resistance of the MTJ, when it is in a state other than P or AP, is between Ron and Roff and its exact value depends on the state.

EXISTING BLOCK DIAGRAM:

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 10, October : 2024

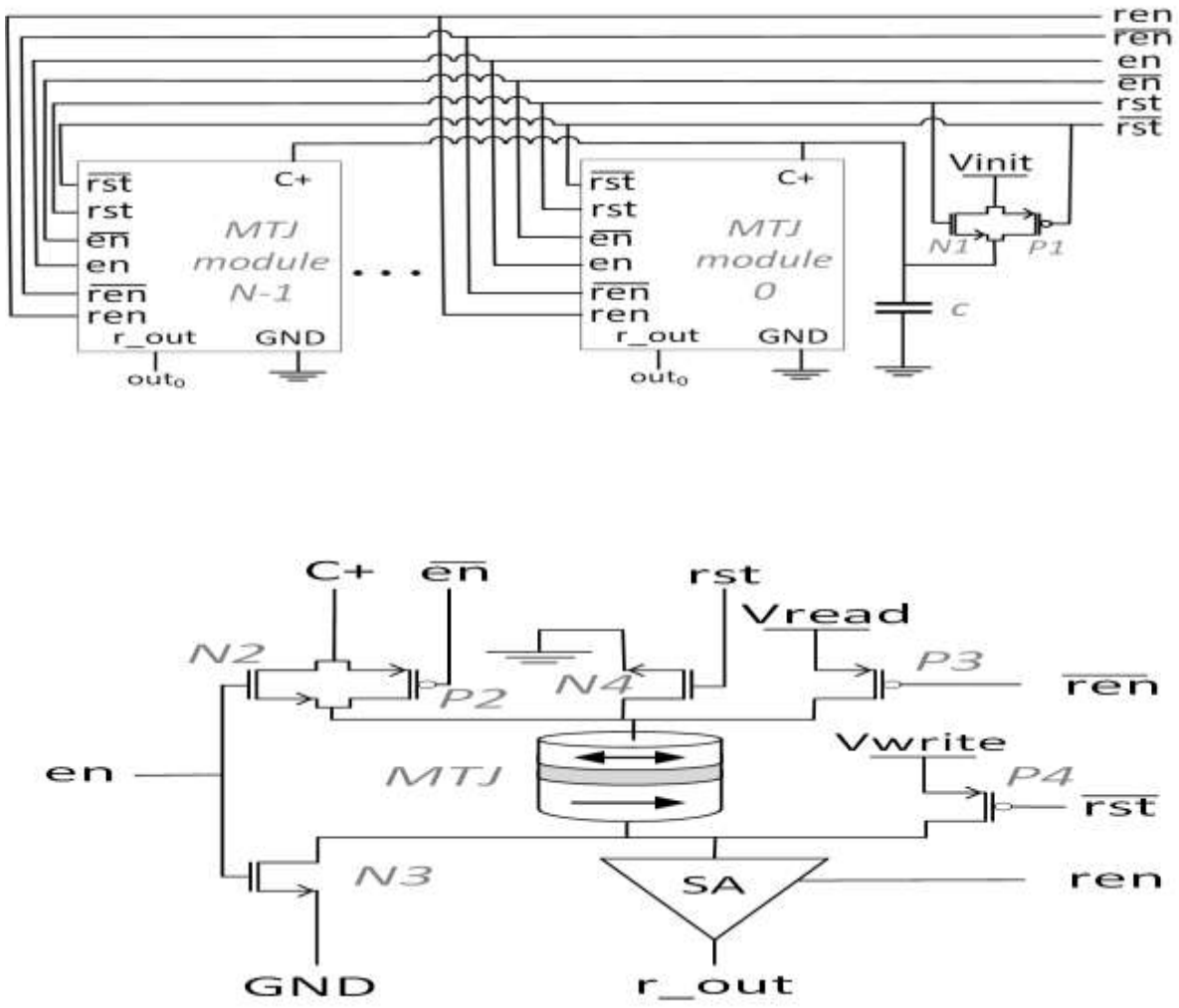

Fig2. The TRNG consists of (a) N parallel connected MTJmodules and a capacitor. (b) Schematic of the MTJ module

making the capacitor discharge faster. This lowers but does not eliminate the switching probability of the other MTJs. The third step, the Read step, applies a small current through the MTJ devices (using transistor P3), and the sense amplifiers determine the state of each. The AP/P states are interpreted as '0'/'1' respectively. Overall, the TRNG outputs an N-bit word. The proposed TRNG relies on the stochastic switching time of the MTJ as its randomness source. Unlike previously proposed TRNGs, the randomness extraction operation in the Enable step is asynchronous and does not depend on a strict time measurement. The capacitor is sufficiently discharged during the Enable step to ensure a low probability for further switching until the end of the Read step. Hence, the randomness of the

output does not change if the duration of the Enable step is longer than a certain lower bound. Thus, accurate measurement of the Enable step duration is not required. Note that although the Enable step is done asynchronously, the TRNG still uses a clock signal since a time measurement is still needed to transition between the operation steps. The proposed TRNG generates N-bit numbers and is composed of a capacitor, N STT-MTJ devices, N sense amplifiers, and transistors that serve as switches, as shown in Figure 2. The TRNG operation consists of three steps, each taking a fixed amount of time. The first step, the Reset step, charges the capacitor C to the Vinit voltage (using transistors N1 and P1) and applies a current through the MTJ devices (using transistors N4 and P4), switching them all to the AP state. The second step, the Enable step, connects C in parallel to all the MTJ devices (using transistors N2,N3, and P2). This discharges C through the MTJ devices, enabling them to switch to the P state with some probability. During the Enable step, the resistance of an MTJ drops if it is switched.

PROPOSED METHOD:

GATE DIFFUSION TECHNIQUE:

The GDI method is based on the use of a simple cell as shown in Fig. At a first glance the basic cell resembles the standard CMOS inverter, but there are some important differences: GDI cell contains three inputs – G (the common gate input of the nMOS and pMOS transistors), P (input to the outer diffusion node of the pMOS transistor) and N (input to the outer diffusion node of the nMOS transistor). The Out node (the common diffusion of both transistors) may be used as input or output port, depending on the circuit structure. But in a GDI cell this might not necessarily occur. There are some important differences between the two. The three inputs in GDI are namely-

1) G- common inputs to the gate of NMOS and PMOS

2) N- input to the source/drain of NMOS

3) P- input to the source/drain of PMOS

Bulks of both NMOS and PMOS are connected to N or P (respectively), that is it can be arbitrarily biased unlike in CMOS inverter. Moreover, the most important difference between CMOS and GDI is that in GDI N, P and G terminals could be given a supply ‘VDD’ or can be grounded or can be

supplied with input signal depending upon the circuit to be designed and hence effectively minimizing the number of transistors used in case of most logic circuits (eg. AND, OR, XOR, MUX, etc). As the allotment of supply and ground to PMOS and NMOS is not fixed in case of GDI, therefore, problem of low voltage swing arises in case of GDI which is a drawback and hence finds difficulty in case of implementation of analog circuits.

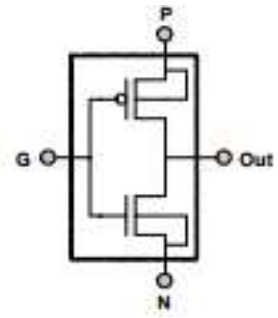

Fig3: Basic GDI Cell

Multiple-input gates can be implemented by combining several GDI cells. The buffering constrains, due to possible VT drop are described in detail in [8], as well as the technological compatibility with CMOS (and with SOI). Morgenshtein has proposed basic GDI cell shown in Fig.1 [8]. This is a new approach for designing low powerdigital combinational circuit.GDI technique is basically two transistor implementation of complex logic functions whichprovides in-cell swing restoration under certain operating condition. This approach leads to reduction in power consumption, propagation delay and area of digital circuits is obtained while having low complexity of logic design. Animportant feature of GDI cell is that the source of the PMOS in a GDI cell is not connected to VDD and the source of theNMOS is not connected to GND. Therefore GDI cell gives two extra input pins for use which makes the GDI design more flexible than CMOS design. There are three inputs in a GDI cell - G (common gateinput of NMOS and PMOS), P (input to the source/drain ofPMOS) and N (input to the source/drain of NMOS).Bulks ofboth NMOS and PMOS are connected to N and Prespectively. Table 1 shows different logic functionsimplemented by GDI logic [8] based on different inputvalues. So, various logic functions can be implemented withless power and high speed with GDI technique as comparedto conventional CMOS design.

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 10, October : 2024

S.No.	N I/P	P I/P	G I/P	Output	Function
1.	0	B	A	A'B	F_1
2.	B	1	A	A'+B	F_2
3.	1	B	A	A+B	OR
4.	B	0	A	AB	AND
5.	C	B	A	A'B+AC	MUX
6.	0	1	A	A'	NOT

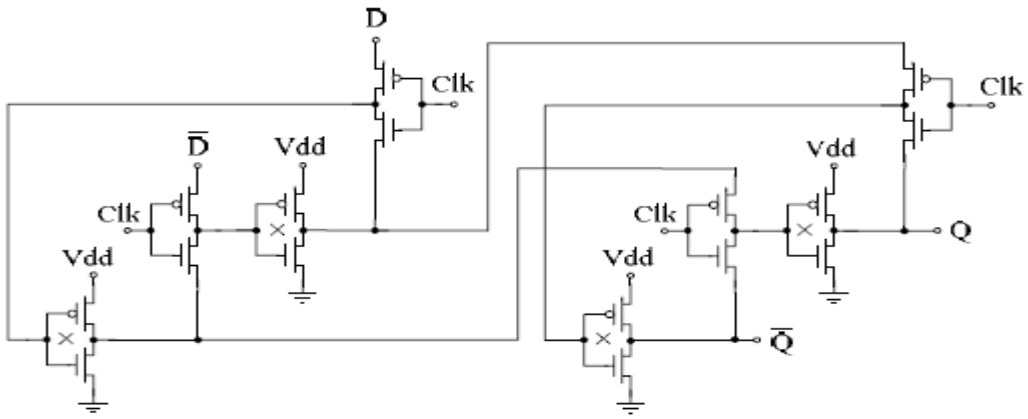

Fig4. GDI D-Flip-Flop implementation

An implementation of low power negative edge triggered D flip flop using GDI (Gate Diffusion Input) technique. The main aim of this work to minimize the power dissipation using GDI Technique. It is called Gate Diffusion Input Technique because the inputs are directly diffused into the gates of the transistors of N type and P type devices. This Negative edge triggered D flip flop is designed using Master slave configuration and both contains four GDI cells, and the sampling is done on the falling edge of the clock signal. In this the input at thefalling edge is transferred to output port. Body gates and inverters are used in this circuit. Body gates used forcreating two alternative paths as for holding state or transparent state and inverters are used for buffering of the internal signals for swing restoration .This circuit contains 18 transistors including inverters .so it is an efficientalternative for low power consumption and better performance than conventional methods..

A novel implementation of a GDI DFF is shown in Fig. It is based on the Master-Slave connection of two GDI D-Latches. Each latch consists of four basic GDI cells, resulting in a simple eight-transistor structure. The components of the circuit can be divided into two main categories: (a) *Body gates* – responsible for the state of the circuit. These gates are controlled by the Clk signal and create two alternative paths: one for transparent state of the latch (when the Clk is low and the signals are propagating through PMOS transistors), and another for the holding state of the latch (when the Clk is high and internal values are maintained due to conduction of the NMOS transistors). (b) *Inverters* (marked by ×) – responsible for maintaining the complementary values of the internal signals and the circuit outputs. An additional important role of inverters is buffering of the internal signals for swing restoration and improved driving abilities of the outputs. This partition to categories can be helpful for understanding of circuit operation and optimization. As can be seen, in body gates the transmission of the signal is performed through the diffusion nodes of the GDI cells. It might cause a swing drop of VTH in the output signals. This problem is solved by the internal invertersin their buffer role. Performance optimization of the proposed circuit can be performed by adjusting the transistor sizes (as sweep parameter in simulation) to obtain a minimal powerdelay product. This procedure is iterative and contains a sequence of separate size adjustments: (a) First, the same scaling factor is obtained for all transistors of the circuit (body gates and inverters). (b) Secondly, iterative size optimizations are applied separately to inverters and body gates (mostly by opposite shifting of the scaling factors around the “operation point” found in (a)), while targeting the minimal power-delay product. (c) For high load requirements, an additional optimization can be separately performed on the inverter of the Slave latch. The relatively compact structure of the proposed DFF, containing 18 transistors (with the inverter for complementary value of D), makes it an efficient.

RESULTS:

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 10, October : 2024

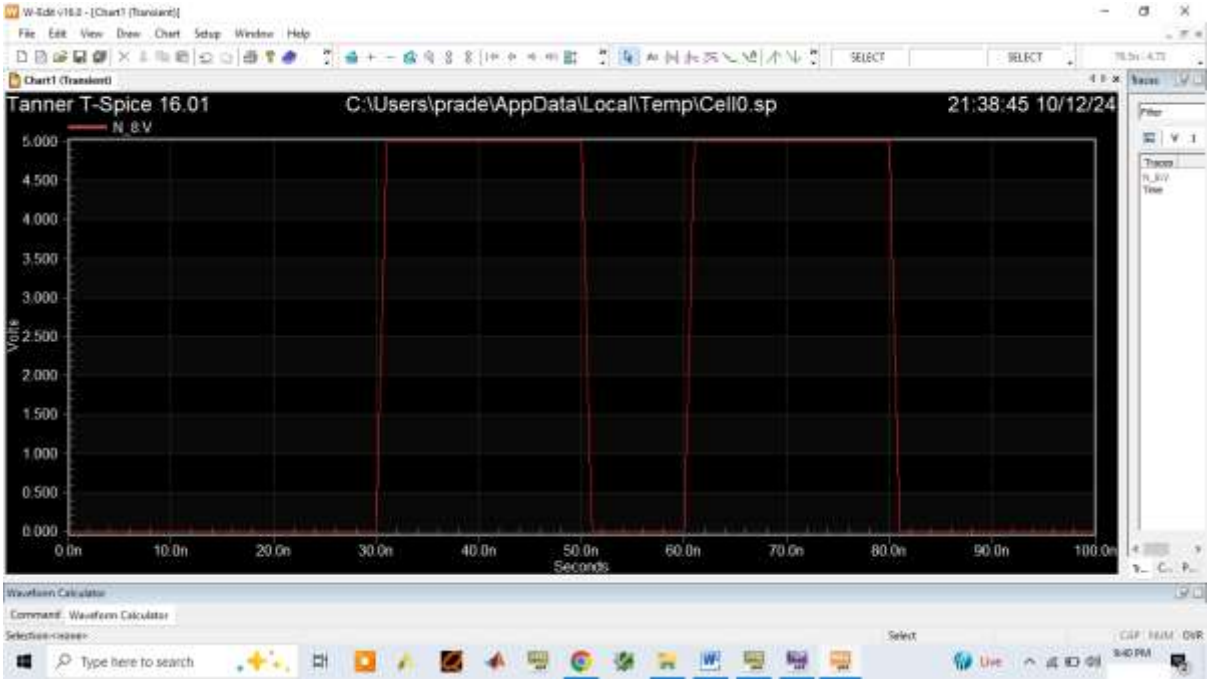

Fig5: proposed simulation result

```
General options:
        threads = 1

 Device and node counts:
              MOSFETs -       42
    MOSFET geometries -        2
           Capacitors -        1
   Transmission lines -        6
      Voltage sources -        2
          Subcircuits -        2
    Model Definitions -        2
      Computed Models -        2
    Independent nodes -       77
       Boundary nodes -        4
          Total nodes -       81
*** 10 WARNING MESSAGES GENERATED DURING SETUP


Power Results

VVoltageSource_1 from time 0 to 100
Average power consumed -> 2.723245e-015 watts
Max power 1.994715e-004 at time 3.01406e-008
Min power 4.774132e-007 at time 3.17656e-008


Parsing                         0.01 seconds
Setup                           0.07 seconds
DC operating point              0.06 seconds
Transient Analysis              0.22 seconds
Overhead                        0.73 seconds
-----------------------------------------
Total                           1.09 seconds
```

Fig6: Existing Area, power, delay results

```
General options:
        threads = 1

 Device and node counts:
             MOSFETs -      10
    MOSFET geometries -       2
      Voltage sources -       3
          Subcircuits -       0
    Model Definitions -       2
      Computed Models -       2
    Independent nodes -      16
       Boundary nodes -       5
          Total nodes -      21
*** 9 WARNING MESSAGES GENERATED DURING SETUP

Warning : Newton solver has failed due to extremely large node voltages.
        : If the circuit has very high gain and extremely large voltages (>1000V) are expected,
        : then you may use '.option vmax=0' to disable this check.
Conventional DC operating point computation failed.
Gmin stepping succeeded
Final gmin value = 1e-012, dcstep = 0

Power Results
VVoltageSource_1 from time 0 to 100
Average power consumed -> 1.540771e-013 watts
Max power 7.094801e-003 at time 1.225e-009
Min power 7.005922e-004 at time 3.27894e-009

Parsing                     0.01 seconds
Setup                       0.05 seconds
DC operating point          0.09 seconds
Transient Analysis          0.01 seconds
Overhead                    0.56 seconds
-----------------------------------------
Total                       0.72 seconds
```

Fig7: Proposed Area, power, delay results

CONCLUSION: In this paper, we presented an asynchronous TRNG that utilizes the random switching time of STT-MTJ devices. The TRNG was comprehensively evaluated in simulations using the physical equations describing the STT-MTJs. The evaluation showed that by increasing the number of STT-MTJs in the design, the TRNG can have greater entropy per output and better resilience to process variation. Furthermore, the design achieves better throughput than current CMOS TRNGs, with lower energy per bit and similar die area and power dissipation. However, finally with modified GDI based DFF based TRNG is implemented with low power and area optimised constraints.

FUTURE SCOPE:

The bit-swapping LFSR used by Dhanesh generates a random test sequence with low switching power by finding hamming distance between two adjacent patterns and minimizing that distance by using combinational logic. To further reduce the average power, dual threshold voltages are assigned. By using this method and finding out the critical and non-critical paths present in BIST

and then assigning a low threshold voltage for critical path, and high threshold voltage for non-critical path, a further reduction in total power, especially leakage power, can be obtained.

REFERENCES

[1] D. Eastlake, J. Schiller, and S. Crocker, "RFC4086: Randomness Requirements for Security," June 2005, accessed: January 2018. [Online]. Available: https://tools.ietf.org/html/rfc4086
[2] A. J. Menezes, P. C. V. Oorschot, and S. A. Vanstone, "Handbook of Applied Cryptography". CRC Press, 1996.
[3] I. Goldberg and D. Wagner, "Randomness and the Netscape Browser," January 1996, accessed: January 2018. [Online]. Available: https://people.eecs.berkeley.edu/~daw/papers/ddj-netscape.html
[4] Z. Gutterman, B. Pinkas, and T. Reinman, "Open to Attack: Vulnerabilities of the Linux Random Number Generator." Black Hat, July 2006. [Online]. Available: https://www.blackhat.com/presentations/ bh-usa-06/BH-US-06-Gutterman.pdf
[5] J. Kelsey, B. Schneier, D. Wagner, and C. Hall, "Cryptanalytic Attacks on Pseudorandom Number Generators," in Proceedings of the 5th International Workshop on Fast Software Encryption, 1998, pp. 168– 188.
[6] C. K. Koc, Cryptographic Engineering. Springer Publishing Company, Incorporated, 2008.
[7] S. Bhunia and M. Tehranipoor, "Chapter 12 - hardware security primitives," in Hardware Security, S. Bhunia and M. Tehranipoor, Eds. Morgan Kaufmann, 2019, pp. 311 – 345. [Online]. Available: http: //www.sciencedirect.com/science/article/pii/B9780128124772000174
[8] K. Yang, D. Fick, M. B. Henry, Y. Lee, D. Blaauw, and D. Sylvester, "16.3 A 23Mb/s 23pJ/b Fully Synthesized True-Random-Number Generator in 28nm and 65nm CMOS," in 2014 IEEE International Solid-State Circuits Conference Digest of Technical Papers (ISSCC), February 2014, pp. 280–281.
[9] S. Srinivasan, S. Mathew, R. Ramanarayanan, F. Sheikh, M. Anders, H. Kaul, V. Erraguntla, R. Krishnamurthy, and G. Taylor, "2.4GHz 7mW All-Digital PVT-Variation Tolerant True Random Number Generator in 45nm CMOS," in 2010 Symposium on VLSI Circuits, June 2010, pp. 203–204.
[10] H. Akinaga and H. Shima, "Resistive Random Access Memory (ReRAM) Based on Metal Oxides," Proceedings of the IEEE, vol. 98, no. 12, pp. 2237–2251, December 2010.
[11] H.-S. P. Wong, S. Raoux, S. Kim, J. Liang, J. P. Reifenberg, B. Rajendran, M. Asheghi, and K. E. Goodson, "Phase Change Memory," Proceedings of the IEEE, vol. 98, no. 12, pp. 2201–2227, December 2010.
[12] H. . P. Wong, H. Lee, S. Yu, Y. Chen, Y. Wu, P. Chen, B. Lee, F. T. Chen, and M. Tsai, "Metal-Oxide RRAM," Proceedings of the IEEE, vol. 100, no. 6, pp. 1951–1970, June 2012.
[13] M. Wang, W. Cai, K. Cao, J. Zhou, J. Wrona, S. Peng, H. Yang, J. Wei, W. Kang, Y. Zhang, J. Langer, B. Ocker, A. Fert, and W. Zhao, "Current-Induced Magnetization Switching in Atom-Thick Tungsten Engineered Perpendicular Magnetic Tunnel Junctions With Large Tunne Magnetoresistance," Nature Communications, vol. 9, no. 671, February 2018.
[14] G. Hu, J. H. Lee, J. J. Nowak, J. Z. Sun, J. Harms, A. Annunziata, S. Brown, W. Chen, Y. H. Kim, G. Lauer, L. Liu, N. Marchack, S. Murthy, E. J. O'Sullivan, J. H. Park, M. Reuter, R. P. Robertazzi P. L. Trouilloud, Y. Zhu, and D. C. Worledge, "Stt-mram with double magnetic tunnel junctions," in 2015 IEEE International Electron Devices Meeting (IEDM), Dec 2015, pp. 26.3.1–26.3.4.
[15] T. Devolder, J. Hayakawa, K. Ito, H. Takahashi, S. Ikeda, P. Crozat, N. Zerounian, J.-V. Kim, C. Chappert, and H. Ohno, "Single-Shot Time- Resolved Measurements of Nanosecond-Scale Spin-Transfer Induced Switching: Stochastic Versus Deterministic Aspects," Physical Review Letters, vol. 100, p. 057206, February 2008.
[16] E. I. Vatajelu, G. D. Natale, and P. Prinetto, "STT-MTJ-Based TRNG with On-The-Fly Temperature/Current Variation Compensation," in 2016 IEEE 22nd International Symposium on On-Line Testing and Robust System Design (IOLTS), July 2016, pp. 179–184.

[17] A. Fukushima, T. Seki, K. Yakushiji, H. Kubota, H. Imamura, S. Yuasa, and K. Ando, "Spin Dice: A Scalable Truly Random Number Generator Based on Spintronics," Applied Physics Express, vol. 7, no. 8, p. 083001, 2014.
[18] S. Oosawa, T. Konishi, N. Onizawa, and T. Hanyu, "Design of an STT-MTJ Based True Random Number Generator Using Digitally Controlled Probability-Locked Loop," in 2015 IEEE 13th International New Circuits and Systems Conference (NEWCAS), June 2015, pp. 1–4.
[19] Y. Qu, J. Han, B. F. Cockburn, W. Pedrycz, Y. Zhang, and W. Zhao, "A True Random Number Generator Based on Parallel STT-MTJs," in Design, Automation Test in Europe Conference Exhibition (DATE), 2017, March 2017, pp. 606–609.
[20] Y. Wang, H. Cai, L. A. B. Naviner, J. Klein, J. Yang, and W. Zhao, "A Novel Circuit Design of True Random Number Generator Using Magnetic Tunnel Junction," in 2016 IEEE/ACM International Symposium on Nanoscale Architectures (NANOARCH), July 2016, pp. 123–128.
[21] S. Ghosh, "Spintronics and Security: Prospects, Vulnerabilities, Attack Models, and Preventions," Proceedings of the IEEE, vol. 104, no. 10, pp. 1864–1893, October 2016.
[22] E. Barker and J. Kelsey, "Recommendation for Random Number Generation Using Deterministic Random Bit Generator," NIST, Tech. Rep. SP 800-90A Revision 1, June 2015.
[23] W. Kan, "Analysis of Underlying Assumptions in NIST DRBGs," IACR Cryptology ePrint Archive, vol. 2007, p. 345, 2007.
[24] Y. Lao, Q. Tang, C. H. Kim, and K. K. Parhi, "Beat Frequency Detector– Based High-Speed True Random Number Generators: Statistical Modeling and Analysis," Journal on Emerging Technologies in Computing Systems, vol. 13, no. 1, pp. 9:1–9:25, April 2016.
[25] S. P. Vadhan, "Pseudorandomness," Foundations and TrendsR in Theoretical Computer Science, vol. 7, no. 1–3, pp. 1–336, 2012.
[26] S.-H. Kwok, Y.-L. Ee, G. Chew, K. Zheng, K. Khoo, and C.-H. Tan, "A Comparison of Post-Processing Techniques for Biased Random Number Generators," in Information Security Theory and Practice. Security and Privacy of Mobile Devices in Wireless Communication, C. A. Ardagna and J. Zhou, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2011, pp. 175–190.
[27]. Manoj Sharama, Dr. Aarti noor, shatish Chandara Tiwari, Kunwar singh, International

conference on Advances in recent Technologies in computation and computing ,IEEE 2009

[28]. Jin-fa Lin, Ming-Hwa Sheu and Peng-siang Wang, A low power dual mode pulse Triggered flip flop using Pass transistor logic, IEEE 2010
[29]. Wing –shan Tam, Sik-Lam siu,Chi wah kok and Hei wong, International conference of Electron Devices and solid state circuits, IEEE 2010
[30]. K.G Sharama ,Tripti Sharama , B.P singh and Manisha sharama, Modified Set D flip flop Design for Low power Vlsi applications.IEEE 2011
[31]. Panshul Dobriyal, Karna sharama,Manan Sethi ,Geetanjli Sharma, A high performance D flip flop Design with low power clocking system using MTCMOS Technique, IEEE 2012
[32]. Y.syamala, K.Srilakshmi and someshkar varma, Design of Low power CMOS logic circuits using Gate Diffusion Technique,international Jouranal of VLSI design & communication systems (VLSICS) ,vol. 4,No. 5,October 2013,
[33]. N.Vishnu Vardhan Reddy, C.Leela mohan & M.srilakshami, GDI based subthreshold low power D flip flop,International jouranal of VLSI and Embedded system,2013
[34]. Amit Grover , Sumer singh, D flip flop with different Technologies, Advanced engineering technology and application,2014
[35]. Jin –Fa Lin, Low power pulse triggered Flip flop design based on a signal feed Through Scheme, IEEE Transactions on very Large scale integration (VLSI) systems ,Vol.22,No.1.Januarary 2014.