A Magnetic Tunnel Junction Based True Random Number Generator with Conditional Perturb and Real-Time Output Probability Tracking

Won Ho Choi*, Yang Lv*, Jongyeon Kim, Abhishek Deshpande, Gyuseong Kang, Jian-Ping Wang, and Chris H. Kim
Dept. of ECE, University of Minnesota, 200 Union Street SE, Minneapolis, MN 55455, USA, Email: choi0444@umn.edu, *equal contribution

Abstract

This work experimentally demonstrates for the first time a True Random Number Generator (TRNG) based on the random switching probability of Magnetic Tunnel Junctions (MTJs). A conditional perturb and real-time probability tracking scheme is proposed to enhance the reliability, speed, and power consumption while maintaining a 100% bit efficiency.

Introduction

True Random Number Generators (TRNG) are specialized circuits used in a wide variety of applications ranging from cryptography and hardware based security to statistical sampling and advanced simulation techniques. Traditional CMOS based TRNGs utilize physical noise present in CMOS circuits such as thermal noise, random telegraph noise, and oscillator jitter. However, existing CMOS based TRNGs require extensive post-processing to ensure a high level of randomness in the output bits, which incurs a significant performance, power, and area overhead [1]. The goal of this work is to develop a new class of TRNGs based on the random switching probability of Magnetic Tunnel Junctions (MTJs) for compact area, simpler design, high throughput, and reliable operation. In particular, we propose a conditional perturb and real-time output probability tracking scheme to achieve a 100% bit efficiency (or 100% useable bits) while improving the reliability, speed, and power. An additional benefit of MTJ-based TRNG is that it can be readily implemented using an existing STT-MRAM array with negligible circuit overhead.

The Spin Transfer Torque (STT) switching phenomenon in an MTJ (Fig. 1) is subject to random thermal fluctuation noise which gives rise to a switching probability contour map as shown in Fig. 2 [2]. By applying an optimal "perturb" pulse

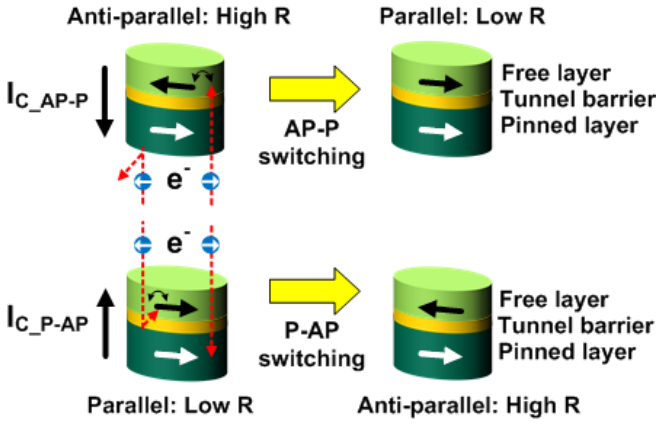

Fig. 1. Illustration of Spin Torque Transfer (STT) switching principle in Magnetic Tunnel Junction (MTJ).

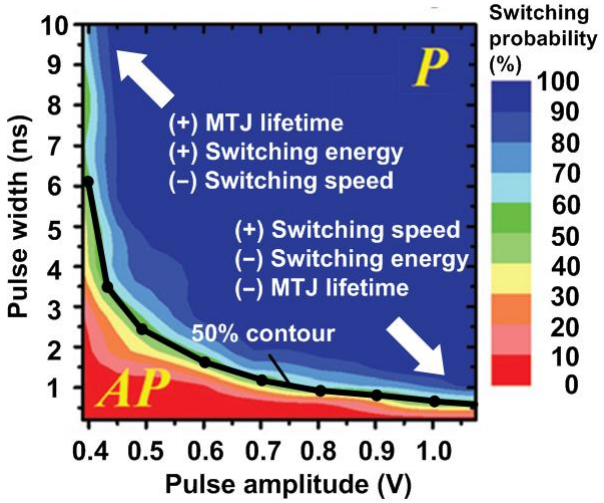

Fig. 2. MTJ switching probability as a function of pulse width and pulse amplitude [2] (AP→P switching direction).

whose width and amplitude correspond to the 50% switching probability contour, the final resolved state of the MTJ will depend solely on the random thermal noise, producing an unbiased random output bit. In this work, we address the two main considerations for a high quality TRNG design: (1) achieving the optimal trade-off between switching speed, power, and lifetime, and (2) ensuring a 50% switching probability under different PVT conditions.

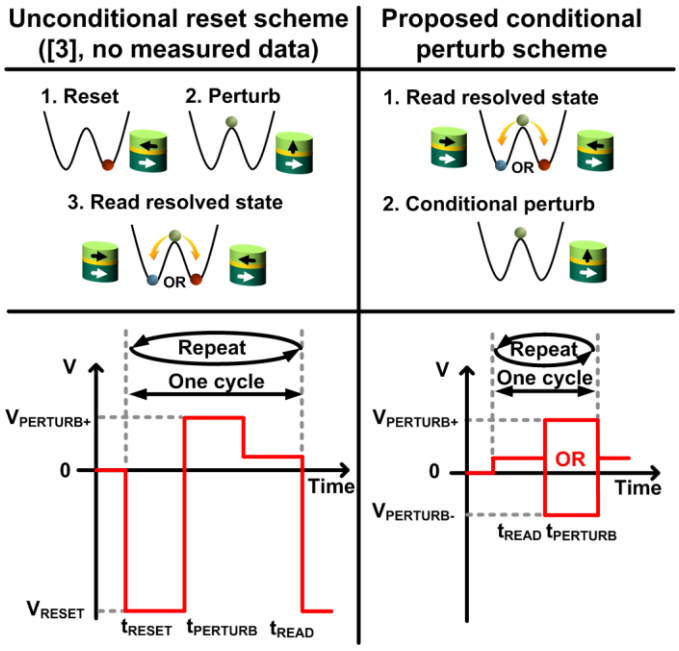

Fig. 3. Random number generation schemes: (left) unconditional reset scheme and (right) the proposed conditional perturb scheme.

Conditional Perturb Scheme

The working principles of the conventional unconditional reset scheme [3] (concept only) and the proposed conditional perturb scheme are described in Fig. 3. The conventional technique applies an initial reset voltage (V_{RESET}) large enough to force the MTJ into a reset state (i.e., AP). Subsequently, a smaller perturbation voltage $V_{PERTURB+}$ in the opposite direction (i.e. AP to P) is applied to induce STT switching with a 50% probability. Finally, the resolved state is read out using a small read voltage (V_{READ}). The proposed scheme, on the other hand, perturbs the cell according to the previously sampled MTJ state, thereby eliminating the reset phase all together. Fig. 4 shows a high level comparison between the two schemes. The advantages of the proposed technique are threefold. First, the absence of a reset phase enhances the lifetime of the MTJ as illustrated in the time-to-breakdown measurements in Fig. 5 [4][5]. Unlike in STT-MRAM application where the cell is accessed infrequently, MTJs for TRNGs need to be accessed continuously throughout the lifetime of the product (e.g. 10 yrs) making lifetime related issues a first rate concern. Second, random bits can be generated at a faster rate since no reset is required and the perturb and read operations can be made relatively fast. Finally, the energy dissipation is lower for the proposed conditional perturb scheme.

	Unconditional reset scheme ([3], no measured data)	Proposed conditional perturb scheme
Bit rate	1X (Slow) 1bit / (t_{RESET}+$t_{PERTURB}$+t_{READ})	1.67X (Fast) 1bit / (t_{READ}+$t_{PERTURB}$)
Switching energy	1X (High) E_{RESET}+$E_{PERTURB}$+E_{READ}	0.29X (Low) E_{READ}+$E_{PERTURB}$
MTJ lifetime	Short time-to-breakdown	Long time-to-breakdown
Design overhead	Strong reset driver	Polarity detection, symmetric AP→P and P→AP switching

Fig. 4. TRNG performance comparison between the unconditional reset and the proposed conditional perturb schemes.

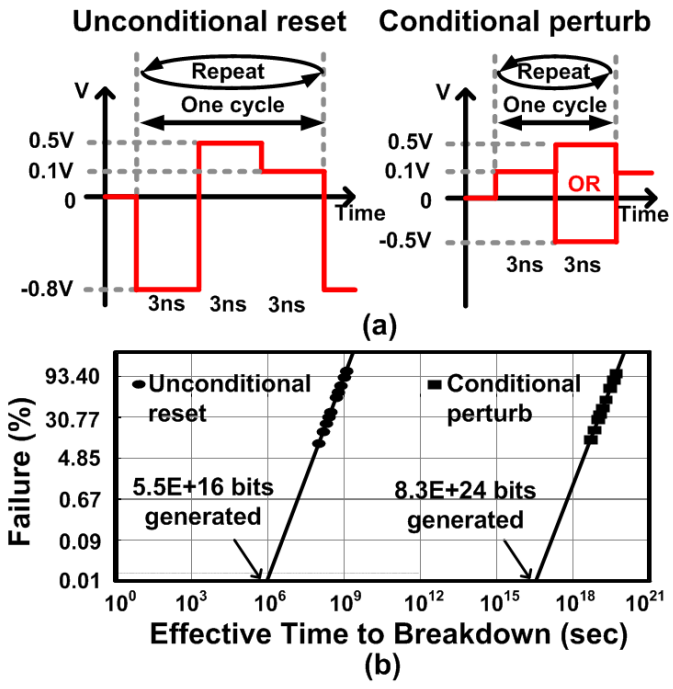

Fig. 5. (a) Timing diagrams for MTJ Time-to-breakdown (tBD) analysis (b) Lifetime comparison between the two TRNG schemes based on MTJ measurement data [4][5].

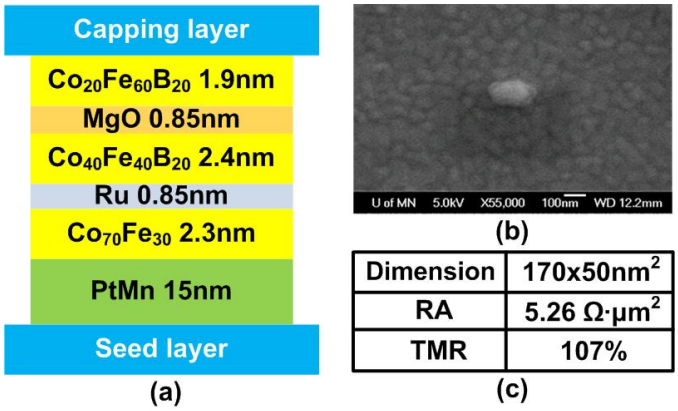

Fig. 6. (a) MTJ vertical stack structure (b) SEM image (c) key parameters of the fabricated MTJ device.

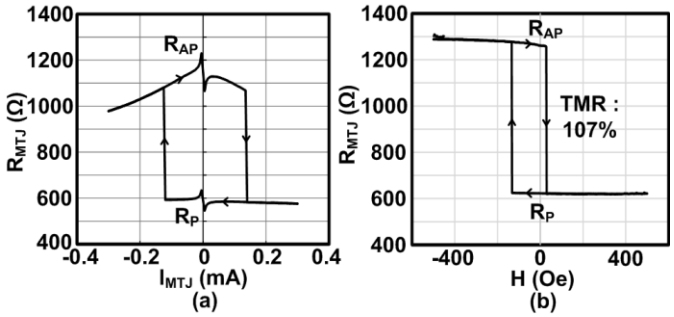

Fig. 7. Measured (a) R-I and (b) R-H hysteresis curves of the fabricated MTJ device. Data was collected while sweeping the MTJ current (a) and external field (b).

The MTJ stack structure, SEM image, and summary of measured MTJ parameters are given in Fig. 6. The measured R-I and R-H hysteresis curves are shown in Fig 7. The

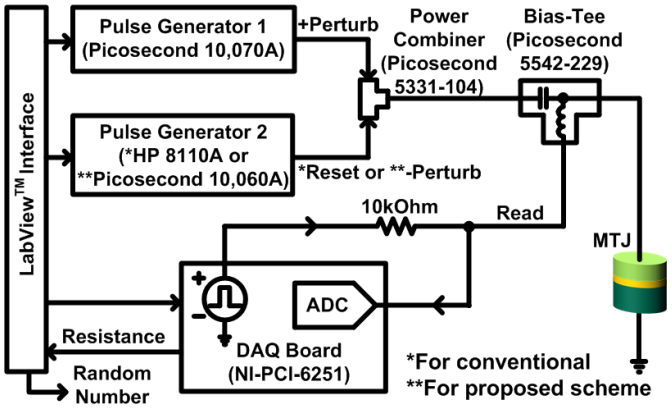

Fig. 8. Random number generator measurement setup with sub-50 picosecond pulse width resolution.

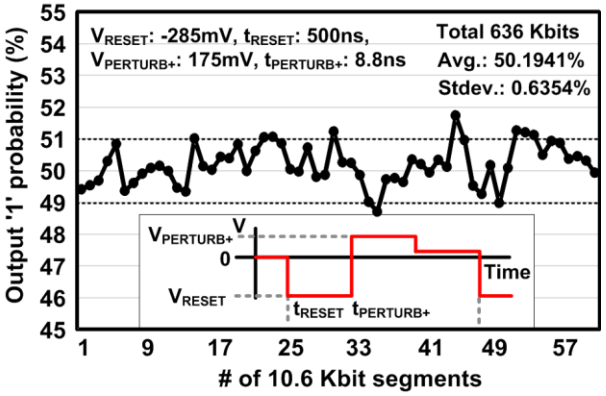

Fig. 9. Measured output '1' probability of each 10.6 Kbit segment for the unconditional reset scheme.

Unconditional reset scheme, # of segments: 55
Pass if P-value$_T$ (χ^2) > 0.0001 and Proportion > 0.9454

	Test	P-value$_T$ (χ^2)		Proportion		Pass/Fail	
1	Frequency	0.005358		0.9272		Fail	
2	Block frequency	0.637119		0.9818		Pass	
3	Cumulative Sums	0.080519 (Forward)	0.080519 (Reverse)	0.9090	0.9272	Fail	Fail
4	Runs	0.401199		1.0000		Pass	
5	Longest-Run-of-Ones	0.025193		1.0000		Pass	
6	Rank	0.266984		1.0000		Pass	
7	FFT	0.897763		1.0000		Pass	
8	Non-overlapping Template Matching	All sub-test: Pass					
9	Serial	0.224821 (P-value$_1$)	0.554420 (P-value$_2$)	0.9818	0.9636	Pass	Pass
10	Approximate Entropy	0.595549		1.0000		Pass	

Fig. 10. NIST randomness test result of 636 Kbits from the conventional unconditional reset scheme.

After Von Neumann Correction
Unconditional reset scheme, # of segments: 55
Pass if P-value$_T$ (χ^2) > 0.0001 and Proportion > 0.9454

	Test	P-value$_T$ (χ^2)		Proportion		Pass/Fail	
1	Frequency	0.181557		1.0000		Pass	
2	Block frequency	0.062821		1.0000		Pass	
3	Cumulative Sums	0.554420 (Forward)	0.055361 (Reverse)	1.0000	1.0000	Pass	Pass
4	Runs	0.514124		0.9818		Pass	
5	Longest-Run-of-Ones	0.145326		1.0000		Pass	
6	Rank	0.823537		1.0000		Pass	
7	FFT	0.000347		1.0000		Pass	
8	Non-overlapping Template Matching	All sub-test: Pass					
9	Serial	0.401199 (P-value$_1$)	0.366918 (P-value$_2$)	0.9818	0.9818	Pass	Pass
10	Approximate Entropy	0.924076		1.0000		Pass	

Fig. 11. NIST randomness test results for the unconditional reset scheme after applying the Von Neumann correction (bit efficiency: 25%).

measurement setup in Fig. 8 consists of high speed signal generators for providing $V_{PERTURB+}$, V_{RESET} or $V_{PERTURB-}$ pulses, a data acquisition board for generating the read voltage pulse and sampling the MTJ state using the same signal line, a power combiner, and a bias tee. A software program controls the pulse generators and the data acquisition board generates the timing sequences described earlier. Fig. 9 shows the measured probability of each 10.6 Kbit segment for the conventional conditional reset scheme. Note that the output probability typically needs to stay within 50±1% to pass the NIST frequency test [6]. A small number of segments fail to

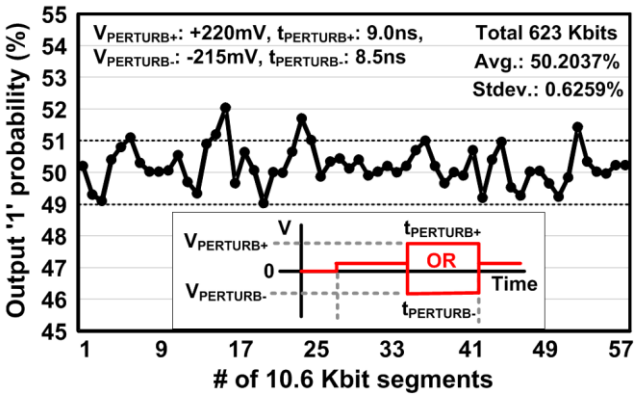

Fig. 12. Measured output '1' probability of the proposed conditional perturb scheme.

Conditional perturb scheme, # of segments: 55
Pass if P-value$_T$ (χ^2) > 0.0001 and Proportion > 0.9454

	Test	P-value$_T$ (χ^2)		Proportion		Pass/Fail	
1	Frequency	0.000831		0.9272		Fail	
2	Block frequency	0.266918		0.9464		Pass	
3	Cumulative Sums	0.037566 (Forward)	0.021999 (Reverse)	0.9272	0.9272	Fail	Fail
4	Runs	0.437274		1.0000		Pass	
5	Longest-Run-of-Ones	0.474986		0.9818		Pass	
6	Rank	0.085953		1.0000		Pass	
7	FFT	0.437274		1.0000		Pass	
8	Non-overlapping Template Matching	All sub-test: Pass					
9	Serial	0.637119 (P-value$_1$)	0.202268 (P-value$_2$)	0.9818	0.9818	Pass	Pass
10	Approximate Entropy	0.115387		1.0000		Pass	

Fig. 13. NIST randomness test result of 623 Kbits from the proposed conditional perturb scheme.

After Von Neumann Correction
Conditional perturb scheme, # of segments: 55
Pass if P-value$_T$ (χ^2) > 0.0001 and Proportion > 0.9454

	Test	P-value$_T$ (χ^2)		Proportion		Pass/Fail	
1	Frequency	0.334538		1.0000		Pass	
2	Block frequency	0.637119		1.0000		Pass	
3	Cumulative Sums	0.249284 (Forward)	0.202268 (Reverse)	1.0000	1.0000	Pass	Pass
4	Runs	0.349121		0.9818		Pass	
5	Longest-Run-of-Ones	0.200936		1.0000		Pass	
6	Rank	0.597670		1.0000		Pass	
7	FFT	0.328827		0.9636		Pass	
8	Non-overlapping Template Matching	All sub-test: Pass					
9	Serial	0.798139 (P-value$_1$)	0.924076 (P-value$_2$)	1.0000	1.0000	Pass	Pass
10	Approximate Entropy	0.080519		0.9636		Pass	

Fig. 14. NIST randomness test results for the conditional perturb scheme after applying the Von Neumann correction (bit efficiency: 25%).

meet this criterion and consequently, the output data fails to pass the frequency and cumulative sums tests as shown in Fig. 10. Von Neumann's algorithm can be applied to remove skew in the TRNG output and pass all 10 NIST tests [1]. However, the bit efficiency (=fraction of useable bits) drops from 100% to 25%. The measurement data from the proposed scheme in Figs. 12, 13, and 14, indicate a similar level of randomness as compared to the conventional scheme.

Real-Time Output Probability Tracking

To achieve good randomness without incurring any bit efficiency loss, a real-time output probability tracking scheme that actively unbiases the output bit stream is proposed. The circuit diagram is shown in Fig. 15 where two 10 bit counters are used to calculate the output probability of each consecutive 1 Kbit segment. $t_{PERTURB-}$ is adjusted according to the digital comparator outcome while all other parameters such as $V_{PERTURB+}$, $t_{PERTURB+}$ and $V_{PERTURB-}$ are kept constant for a simple single-parameter feedback control. Note that a segment size much shorter than 1 Kbit makes the output probability fluctuate while a segment size much longer than 1 Kbit increases the locking time unnecessarily. The real-time tracking scheme was implemented in software and the measurement setup in Fig. 8 was used to verify the concept using the fabricated MTJ device. The conditional perturb scheme was used for all measurements involving real-time tracking. Measured probability of each 1 Kbit segment and the corresponding $t_{PERTURB-}$ are illustrated in Fig. 16. The minimum $t_{PERTURB-}$ step was set as 0.05ns. After an initial locking period of 65 Kbits, the output data passed all NIST randomness tests while maintaining a 100% bit efficiency (Fig. 17). Finally, we show a conceptual diagram of a TRNG implemented using an existing STT-MRAM array (Fig. 18), which could potentially allow massive generation of random numbers with negligible circuit overhead.

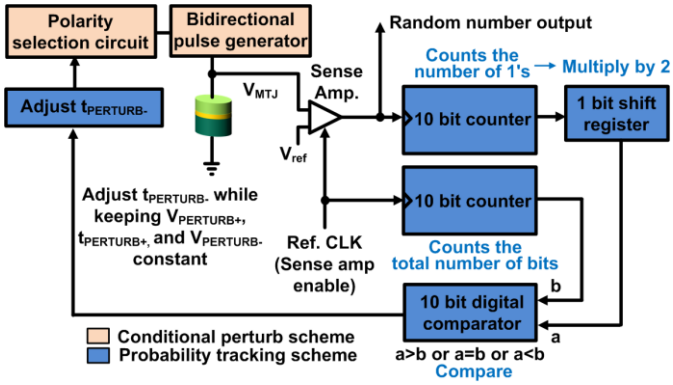

Fig. 15. Proposed MTJ-based TRNG with conditional perturb and real-time output probability tracking. The two techniques were implemented in software and experimentally verified using a real MTJ device.

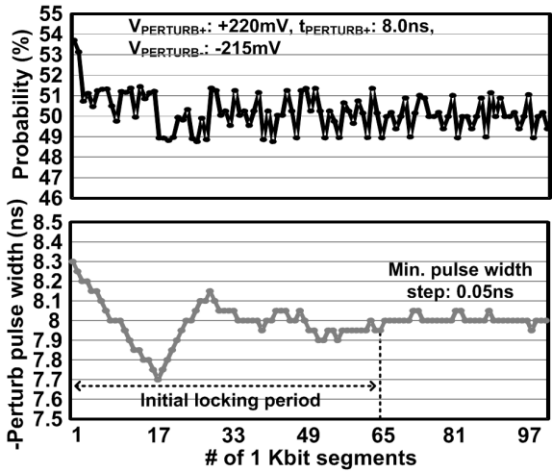

Fig. 16. Measured output '1' probability and -perturb pulse width for each 1 Kbit segment with the proposed real-time output probability tracking scheme.

Raw data after probability tracking
Conditional perturb scheme, # of segments: 55
Pass if P-value$_T$ (χ^2) > 0.0001 and Proportion > 0.9454

	Test	P-value$_T$ (χ^2)		Proportion		Pass/Fail	
1	Frequency	0.102947		1.0000		Pass	
2	Block frequency	0.019203		0.9636		Pass	
3	Cumulative Sums	0.012910 (Forward)	0.366928 (Reverse)	1.0000	1.0000	Pass	Pass
4	Runs	0.582910		1.0000		Pass	
5	Longest-Run-of-Ones	0.201928		1.0000		Pass	
6	Rank	0.693028		0.9818		Pass	
7	FFT	0.381291		1.0000		Pass	
8	Non-overlapping Template Matching	All sub-test: Pass					
9	Serial	0.283910 (P-value$_1$)	0.683921 (P-value$_2$)	0.9818	0.9636	Pass	Pass
10	Approximate Entropy	0.334538		1.0000		Pass	

Fig. 17. NIST randomness test results for the proposed MTJ-based TRNG with conditional perturb and real-time output probability tracking. Note that output bits after the initial locking period are used for the randomness test.

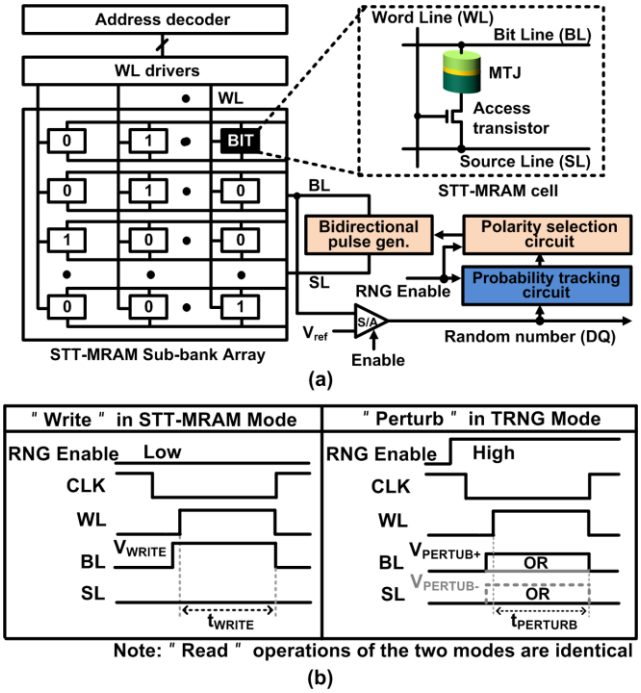

Fig. 18. (a) Conceptual diagram of a TRNG circuit implemented using an existing STT-MRAM array (b) "Write" and "Perturb" timing diagrams of STT-MRAM and TRNG modes.

Acknowledgements

This work was supported in part by C-SPIN, one of six centers of STARnet, a Semiconductor Research Corporation program, sponsored by MARCO and DARPA. The authors would also like to thank Vijay Reddy at TI for technical discussion.

References

[1] K. Yang, et al., ISSCC, pp. 280, 2014.
[2] H. Zhao, et. al., JAP, pp. 07C720, 2011.
[3] S. Yuasa, et al., IEDM, pp. 3.1.1, 2013.
[4] C. Yoshida, et al., IRPS, pp. 139, 2009.
[5] W. R. Hunter, IRPS, pp. 72, 1999.
[6] A. Rukhin, et al., NIST Pub 800-22, 2010.