

スピン注入磁化反転を用いた乱数発生器

福島 章雄、薬師寺 啓、久保田 均、湯浅 新治、安藤 功児

産業技術総合研究所 エレクトロニクス研究部門 スピントロニクスグループ

【はじめに】

磁気抵抗素子とは、非磁性層を二つの強磁性層で挟んだ構造を持ち、強磁性層の磁化の向きに応じて抵抗値が変化する素子である。今では、磁気抵抗素子はハードディスクの読み取りヘッドなどの磁気センサ、あるいは磁気ランダムアクセスメモリ (MRAM) として応用されている。

これまで、磁気抵抗素子の磁化の向きを変化させるためには、外部から磁場を与えることが不可欠と考えられているが、近年、非常に微細な磁気抵抗素子 (面積で 100 nm 角程度、厚み数 nm 程度) においては、スピン偏極電流によるトルク (spin-torque) によって、磁化反転が可能であることが実証された。この現象は、電流のみで磁化反転を起こさせるため、スピン注入磁化反転と呼ばれている^[1]。

Attempt time (スピンの揺らぎに関する時定数 ~1 nsec) より長い電流パルスによるスピン注入磁化反転は、熱活性化モデルで記述できる現象である^[2]。反転確率は、反転電流閾値 (反転確率が 0.5 となる電流値) 近傍で、電流値に対して一様に増加し、増加の割合は熱安定性パラメータ Δ (2つの状態のエネルギー差と熱エネルギーの比) に反比例することが知られている^[3]。すなわち、電流値を反転電流閾値近傍に設定することで、反転確率のみを制御するデバイス (乱数発生器) を作成することが可能となる。

一方、現代における高度情報化社会の要求として、高度なセキュリティ通信がある。高度な暗号には、高速な物理乱数発生器が必要となる。スピン注入磁化反転を用いた乱数発生器は、毎回のスイッチングの結果を乱数として取り出すため、純粋な物理乱数発生器であり、MRAM と同様、不揮発で高速な動作が可能という特徴を持つ。我々は、スピン注入磁化反転を用いた物

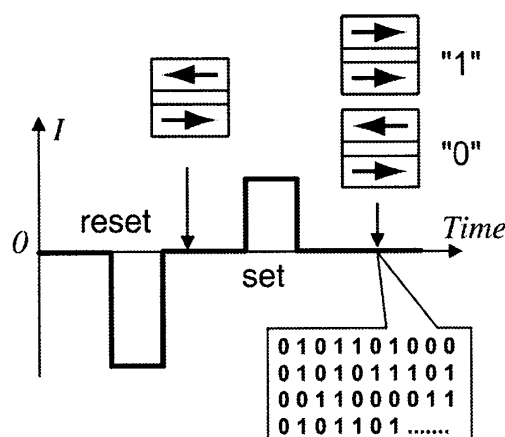


図1 スピン注入磁化反転による乱数発生の手順。

理乱数発生器 (これを Spin dice と名付けた) を提案している^[4]。

【実験】

Spin dice により乱数を作成し、その乱数のランダムネスを評価した。磁気抵抗素子として、MgO-MTJ (MgO 障壁層を持つ磁気抵抗素子) を用いた。MTJ の構成は、バッファ/反強磁性層/磁化固定層 (CoFeB 3nm)/MgO 1nm/磁化自由層 (CoFeB 2nm)/キャップ層であり、150×60 nm の大きさに加工したものを使用した。平行状態での抵抗値は 180 Ω であり、磁気抵抗比は 100% 程度であった。シフト磁場の小さいサンプルを選択し、磁場 0 で乱数発生実験を行った。

図1に実験の手順を示す。まずリセットパルス電流により、磁化固定層と磁化自由層の向きを反平行に揃え、その後、セットパルス電流を磁化自由層が反転する方向に与える。パルス電流の幅は 50 μsec である。セット電流の値を反転電流の閾値近傍に調整することにより、反転確率を 0.5 とすることが出来る。反転成功を “1”、反転失敗を “0” に割り当てることによって、各々のスイッチングの結果から二値化した乱数を得ることが出来る。

“Random number generator by current induced magnetization switching,” Akio Fukushima, Kay Yakushiji, Hitoshi Kubota, Shinji Yuasa, Koji Ando, *National Institute of Advanced Industrial Science and Technology*.

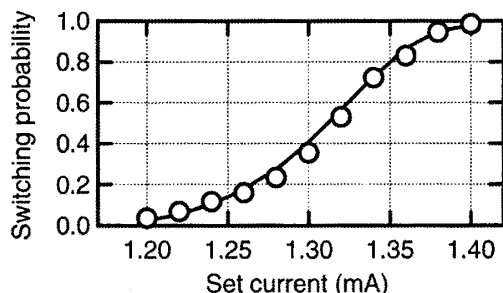


図2 反転確率のセット電流に対する依存性。実線は熱活性化モデルへのフィッティングを示す。

【結果】

図2に反転確率のセット電流に対する依存性を示す。反転確率はそれぞれ1000回の繰り返し測定から求めた。反転電流閾値は1.3 mAであり、反転確率のセット電流依存性は、熱活性化モデルと良く一致した。熱活性化モデルへのフィッティングから、 $I_{c0} = 1.83 \text{ mA}$, $\Delta = 40$ を得た。

次にセット電流を1.3 mAとし、10000回の繰り返し測定から乱数列を作成した。“1”の出現数は4517であり、“0”の出現数は5483であった。この10000点のデータのランダムネスを評価するために、ランテストとポーカーテストを行った。ランテストは、“1”あるいは“0”の連続する事象の発生確率が指数的に減少すること、ポーカーテストは、“001”、“010”、“100”など同じ発生確率が期待される事象の均等性を評価するものである。図3にランテストと、3bit-ポーカーテストの結果を示す。“1”、“0”の両者において連続事象の発生確率は指数的に減少し、“001”、“010”、“100”と(“110”、“101”、“011”)の両者のグループにおいて発生確率がほぼ均等であることが解る。これらの結果から、Spin diceにより生成した乱数は良好なランダムネスを持つことが示された。

【結論】

MgO-MTJにおけるCIMSを用いて乱数発生を行った。発生した乱数のランダムネスをランテストと、3bit-ポーカーテストで評価した。結果は、単一事象での確率から期待される結果とよく一致した。

MgO-MTJのCIMSによる乱数発生器(spin dice)は、不揮発かつ高速な動作が可能、集積化が容易という特徴を持つ、次世代の高速物理乱数発生器として大いに期待できる。

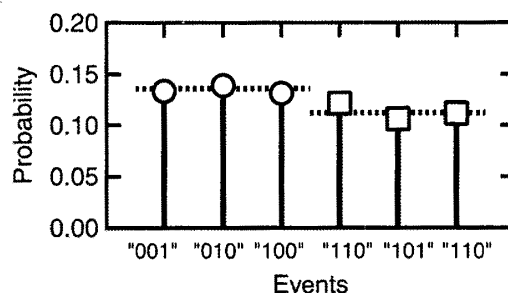
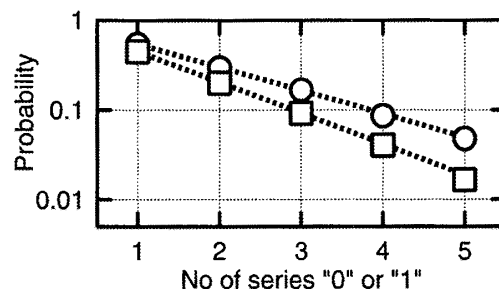


図3 上図：ランテストの結果。○は“1”、□は“0”の場合を示す。下図：3bit-ポーカーテストの結果。両図とも、点線は単一事象の“1”、“0”の確率から見積もった期待値を示す。

【謝辞】

有益な議論をしていただいた産総研・情報セキュリティセンター、今福健太郎氏に感謝する。この研究はNEDO「スピントロニクス不揮発機能技術プロジェクト」の支援により行われた。

【参考文献】

- [1] J. C. Slonczewski, J. Magn. Mater. **159** (1996), L1.
- [2] R. H. Koch *et al.*, Phys. Rev. Lett. **92** (2004), 088302.
- [3] M. Pakala *et al.*, J. Appl. Phys. **98** (2005), 056107.
- [4] A. Fukushima *et al.*, 応用物理学会 2007 秋, 7p-S-15; 52nd MMM conference, DE-11.