

True Random Number Generator Harvesting Entropy from Stochastic Switching Time of MTJ

應用於亂數產生器之 MTJ 的隨機轉換 時間

組別:A64 組員:李睿 指導教授:張孟凡

Abstract

亂數產生器在數據傳輸中有著關鍵作用，由於現今的傳輸過程中都會先將資料加密，加密的過程需要用到金鑰，而金鑰可以從亂數產生器生成，因此亂數產生器的好壞可以決定到資料傳輸的安全程度。在大多數情況下，亂數是由 PRNG（偽亂數產生器）生成的，但是這種發生器有其局限性[1]，因此 TRNG（真亂數產生器）被提出了。它通過其隨機的物理屬性生成隨機數，而物理特性會表現在干擾發生時，像是熱干擾或電壓干擾時。干擾會影響數位電路的輸出，而受干擾的輸出，會被拿來當作亂數使用。因此，我們稱干擾作為「熵」的來源，可用於設計 TRNG。

在此實驗中，提出了一個 MRAM TRNG 的架構。一般來說，MRAM TRNG 是藉由寫入一個 bit data 所需的時間或者是寫入資料為1成功的機率來做為「熵」的來源。前者需要精度不錯的計數器或是可以用來判斷時間長短的電路，後者則需要額外的電路去確保使用的電壓，剛好可以使寫入的成功率達到50%，除此之外，還需要一些後製方式去確保亂度可以達到要求，這會使得成本高於前者。因此在這次實驗中，運用前者來產生隨機數的。為了計算通過的時間，用了計數器去計算，但由於高位元的振動頻率較小，容易導致高位元的 entropy 較低，但有時候高位元 entropy 的值與標準該有的值相差一點，因此為了避免浪費，藉由 XOR 邏輯閘來達到更好的結果。計數器有幾個位元也會影響到亂度的表現，所以在最後，會判斷幾個位元的計數器，可用隨機數的數量較多，來當作此次實驗的架構，並與沒有 XOR 邏輯閘的結果做比較，最終發現當 counter 的 bit 數為5時，有最好的表現，且會發現到6bit counter MSB 的 entropy 值就很小了，因此也就沒有往7bit counter 做的必要了。

Introduction

由於 MRAM 寫入資料所需時間的分布，可以使計數器的 LSBs 直接拿來當成亂數，然而仔細觀察可以發現有些 MSBs，離可以被當作亂數的標準相差一點，因此本實驗中提出使用 XOR 利用這些 MSBs，產生更多的亂數。由於 XOR 的特性，可以使得兩個離標準相差不大的位元經過運算後，變成可以被使用的亂數，而被當作亂數的條件為

shannon entropy = $\sum_{x \in X} -p(x) \log_2 p(x) \geq 0.995$ X is a finite set with probability p。

假設高位元(x1)得到 1 的機率為 $0.5 + X_1$ ，高位元(x2)得到 1 的機率為 $0.5 + X_2$

$$P(x1 \otimes x2 = 1) = (0.5 - X_1) * (0.5 + X_2) + (0.5 - X_2) * (0.5 + X_1) = 0.5 - 2X_1X_2$$

$$P(x1 \otimes x2 = 0) = (0.5 + X_1) * (0.5 - X_2) + (0.5 + X_2) * (0.5 - X_1) = 0.5 - 2X_1X_2$$

不過 X_1 跟 X_2 的值必須坐落在 $-0.14 \sim 0.14$ ，才能使 $P(x1 \otimes x2 = 0)$ ，會很接近 0.5，假設極端值， X_1 跟 $X_2 = 0.1 \Rightarrow P(x1 \otimes x2 = 0) = 0.54$ ，而 shannon entropy = 0.9956，如此一來，便可讓那些差一點達到標準的位元，能被拿來當作亂數了。

而在報告最後，會比較不同位元數的 counter，產生出的亂數多寡，來說明 XOR gate，所造成的影響，而這些 MRAM TRNG 產生的亂數，都通過了 NIST 800-22 的測試，因此可以說這次的 MRAM TRNG 是成功的

System Introduction

在 Fig.1，Q0, Q1, Q2, Q3, Q4 是這個 MTJ 的 output，開關 stop 在模擬時，我是用可變電阻代替，當開關變成 open，電阻變成 1000Meg ohm，開關 closed，電阻變成 1ohm，而在模擬時用來代替 MTJ 的也是可變電阻，當 MTJ 在 P 狀態時，電阻為 1k ohm，而在 AP 狀態時，電阻為 2.5k ohm。而模擬時所使用的 switching time 分三個情況， -25°C 時，switching time = $\text{agauss}(500\text{n}, 33.33\text{n} * 6, 6)$ ， 25°C 時，switching time = $\text{agauss}(250\text{n}, 16.75\text{n} * 6, 6)$ ， 100°C 時，switching time = $\text{agauss}(197.5\text{n}, 12.54\text{n} * 6, 6)$ 。當啟動 TRNG 時，data 等於 1，reset 等於 1，讓 counter 歸零，接著 reset 等於 0，TRNG 開始震動，直到資料寫入成功，記錄輸出的結果，然後再讓 data 等於 0，將 MRAM 寫成狀態 AP，等待下一次啟動 TRNG，如 Fig.2 所示。Fig.3 為 MRAM TRNG 啟動一次，各個電壓的表現情況，BL 電壓上升代表寫入成功。

使用 2T1J 而非 1T1J 的原因是因為，前者可以操作較低電壓，且消耗的能量較少 [2]，且操作在較低電壓下，寫入資料所需時間的分布也會變大，有助於 MRAM TRNG 的表現 [2]，使用三個 inverter 去偵測資料寫入成功與否。

下圖為這次實作的電路圖與操作流程。由於只需要用一個 cell，來看其產生的輸出，便可了解其他 cell 的表現，因此在這次模擬中，只模擬了一個 cell。

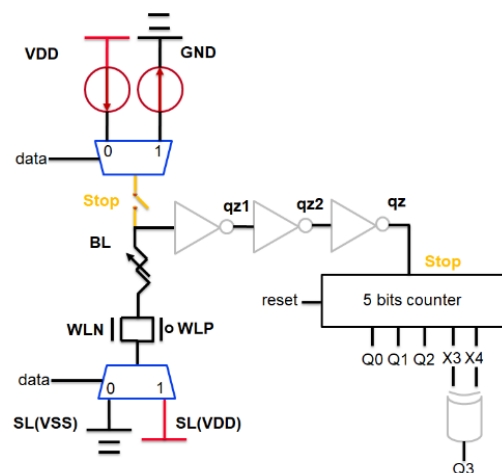


Fig.1 MRAM TRNG 架構

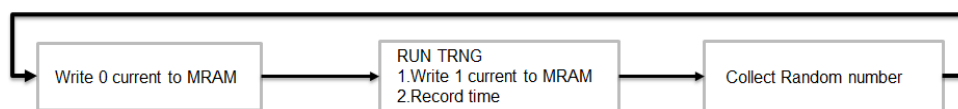


Fig.2 MRAM TRNG 操作流程圖

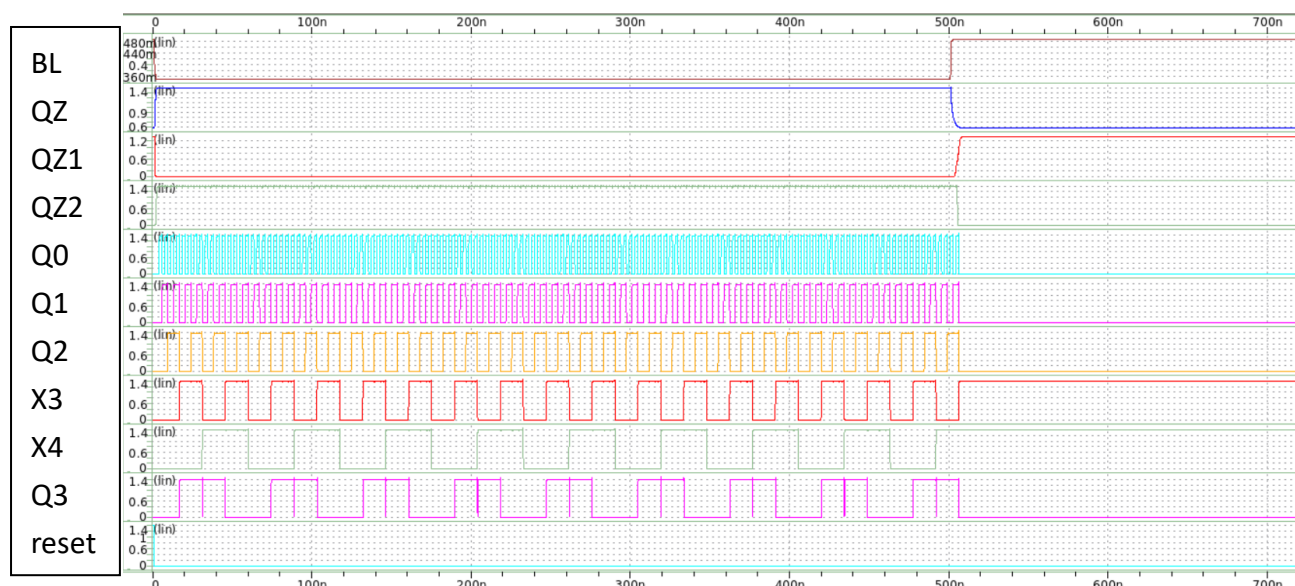


Fig.3 電壓在操作過程中的變化

Conclusion

5bit counter 有 XOR 可以在較少的面積下，產生與 6bit counter 無 XOR 一樣多的亂數，因此可以知道添加 XOR 可以讓亂數的產生更有效率。Fig.5 是將產生的亂數去跑 NIST 800-22 得出的結果，而結果說明了這個 MRAM TRNG 產生出來的數的確是亂數。

不同位元數的 counter	有無 XOR	Number of usable bits
4bits counter	無XOR	3
	有XOR	3
5bits counter	無XOR	3
	有XOR	4
6bits counter	無XOR	3
	有XOR	4

Fig.4 不同 bit 數的 counter，可用的亂數數量比較

Test	P value		Proportion		Success/Fail
Frequency	0.53		1		Success
Block Frequency	0.35		1		Success
Runs	0.06		1		Success
Longest Run of Ones	0.53		1		Success
FFT	0.35		1		Success
Approximate Entropy			1		Success
Cumulative Sums			1	1	Success
Serial			1	1	Success
Non-overlapping Template Matching			Pass 97.3% of the sub-test		

Fig.5 NIST 800-22 結果

心得感想

在剛開始專題課程開始時，張孟凡教授便告訴我們，在他的專題中，他期待我們可以在這之中，了解到創新電路的困難與挫敗，與其在研究所因為提不出新想法，寫不出論文而延畢，不如在這次專題，先有經驗。

學習電路設計最基本的就是兩件事，分析了解別人的電路和設計自己的電路並且可以提出優缺點，這兩件事說來容易，但真時開始著手後才發現困難重重，尤其是分析優缺點這件事。教授在上學期時，先讓我們閱讀 paper，累積對於電路應用相關知識，而且不只要看懂 paper 中描述的理论，最重要的是找出他們的電路有那些缺點是 paper 裡沒有提到的，因為我們常常在報告時，助教們問我們說這個電路的優點時，我們都可以回答得出來，但一旦問到缺點，就沒有任何想法，我想這個技能，是我在這個專題中最大的收穫。

在真的開始設計電路時，挫敗感更是不斷出現。我花了很長時間想出一個架構，然而在查閱相關資料時，總是發現其實早就有人提出來了，甚至是架構上比我更加完善與完美的方式。我想這就是教授在專題討論時常說的，設計的好與壞不是最重要的，重要的是我們在這次經驗中學到了甚麼，想辦法去超越其他人。最後感謝張孟凡教授的開了這麼有趣的題目，讓我可以在做專題這麼辛苦的事情中，仍然能保持著愉悅與向上的態度。

Reference

- [1] K. Yang et al., “A 28 nm integrated true random number generator harvesting entropy from MRAM,” in Symp. VLSI Circuits Dig. Tech. Papers, pp. 171–172, Jun. 2018.
- [2] K. T. Quang, S. Ruocco, and M. Alioto, “Voltage scaled STT-MRAMs towards minimum-energy write access,” IEEE J. Emerg. Sel. Topics Circuits Syst., vol. 6, no. 3, pp. 305–318, Sep. 2016