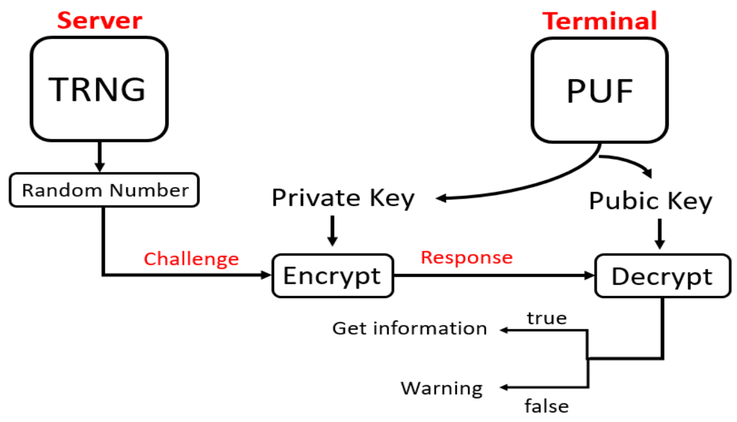
IoT Security - PUF and TRNG design
物聯網之安全 - 物理不可克隆技術與真隨機亂數產生器

組別：A35　指導教授：張孟凡　組員：林楷平、鄭皓謙

一、前言

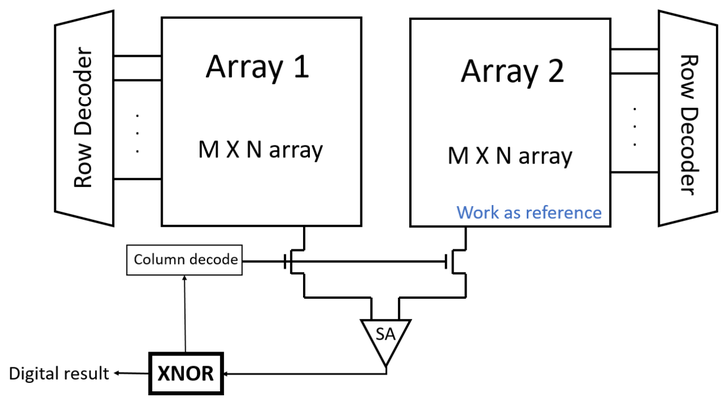
隨著物聯網的快速發展，個人資料的安全性也需要得到相對應的提升，才不會有個資暴露的風險。除了用軟體加密解密的方式可以達到目的外，我們也可以利用硬體獨特的物理特性來實現，PUF（Physical Unclonable Function，物理不可克隆技術）與TRNG（True Random Number Generator，真隨機亂數產生器）就是兩種利用了這個特性的電路。

PUF是利用製程的隨機變異性，產生每個晶片自己獨特的密碼，如同人的指紋TRNG則是利用元件內部的隨機物理現象，產出不可預測的亂數，類似擲硬幣的概念。而將PUF與TRNG為基礎而成的系統，可以作為一個個人資訊的保護措施，利用PUF在終端給予電路一個獨一無二的密碼，伺服器端的TRNG產生亂數，經過加密解密的過程後，可以讓人們取得有價值性的資訊，也可以保護資訊的安全。

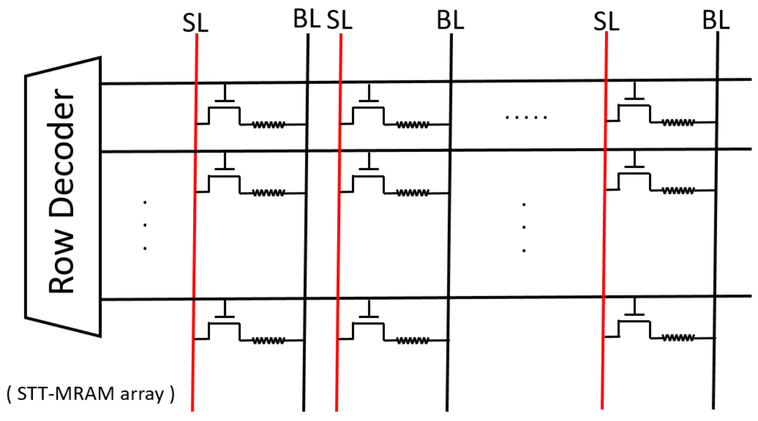


二、PUF Design

為了能解決unstable bits的問題，我們想出利用XNOR的特性，找出unstable bits的位置。我們設計的STT-MRAM array PUF(下圖)，一部分的array設計為參考值，作為Sensing amplifier的參考電流，經過Sensing amplifier後，就可以輸出數位的0還有1，不過其中混有unstable bits，所以我們再加入一個XNOR的邏輯閘，這樣假如遇到unstable bit，也就是不穩定0或1，那「A XNOR B」之後的結果就會得到數位「0」，就可以找出哪個cell是unstable bit了。

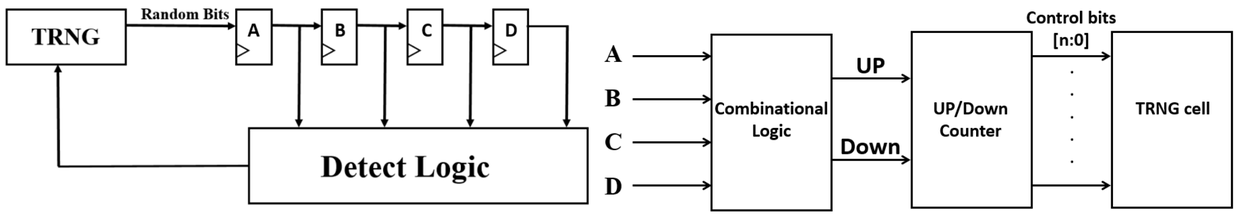


而改變Search Line電壓是為了調整0還有1的分布，上圖中XNOR邏輯閘上方有一條回溯到Search Line的電路，因為經過XNOR之後，可以知道哪些為unstable bit，所以假如出來的結果 0 或是 1 的分布不均（0比較多或是1比較多），那就可以控制Search Line的電壓，得到平均的0和1分布；如果可以隨機亂數輸入SL電壓（加入TRNG），那也可以增加流經cell電流分布，也就可以增加多一點PUF bit的使用了。



三、TRNG Design

如果要做出一個好的TRNG，我們必須確保它的隨機性，因此產出 0 與 1 的機率必須一樣是50%。當我們使用STT-MRAM來做TRNG時，產出 0 與 1 的機率會跟寫入電流有關，寫入電流越大，1 的機率會越大，電流越小則是 0 的機率會變大。但是受到PVT variation的影響，有可能在這個週期的機率是50%，到下個週期時會偏向某一邊。因此我想做一個可以動態調整寫入電流的系統，讓系統先去偵測目前產出 0 與 1 的數量，依照兩者的數量去做電流的調整。

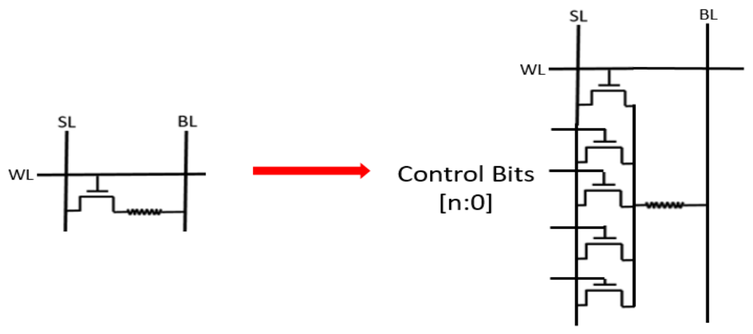


首先我們會先將TRNG產生的最後四個bits進行邏輯運算，分別為：

$$Up = !(AB + AC + AD + BC + BD + CD)$$

$$Down = !(\bar{A}\bar{B} + \bar{A}\bar{C} + \bar{A}\bar{D} + \bar{B}\bar{C} + \bar{B}\bar{D} + \bar{C}\bar{D})$$

當這4個 bits 中，0 數量比較多時，Up = 1 而 Down = 0；1 較多時則是Up = 0、Down = 1；兩者數量一樣的話，Up與Down都會等於 0。接著把Up與Down接到計數器，若0 較多時，Up = 1，計數器會往上數；1 較多時，Down = 1，計數器往下數；兩者一樣則不做動作。最後，將計數器的結果接回TRNG，原本典型的STT-MRAM是1T1R的架構，我們把它改成NT1R，用多餘的MOS控制通過的電流，達到動態調整的目的。



四、結論

在PUF的部分，我們想出利用多加入的XNOR邏輯閘，用來偵測unstable bit的位置，之後若能將unstable bit加入加密的使用，那或許可以加強密碼的強度；而TRNG的部分，我們利用Detect Logic去達到動態調整的功能，隨時針對output bits去調整寫入電流，降低PVT variation對隨機性的影響。

參考文獻：

[1] Rui Liu, Ayush Shrivastava, Pai-Yu Chen, Yu Cao, Shimeng Yu, Chaitali Chakrabarti, “A Highly Reliable and Tamper-Resistant RRAM PUF: Design and Experimental Validation,” IEEE International Symposium on Hardware Oriented Security and Trust (HOST), 2016.

[2] S.K. Mathew, S. Srinivasan, M.A. Anders, H. Kaul, S.K. Hsu, F. Sheikh, A. Agarwal, S. Satpathy, and R.K. Krishnamurthy, “2.4 Gbps, 7 mW All-Digital PVT-Variation Tolerant True Random Number Generator for 45 nm CMOS High-Performance Microprocessors” IEEE JSSC, VOL. 47, NO. 11, NOVEMBER 2012