# 國立清華大學 電機工程學系
# 實作專題研究成果報告

## FinFET Semiconductor Device Design for PUF Application

## 應用於 PUF Security 的鰭式電晶體之半導體元件設計

專題領域：電子領域

組　　別：A398

指導教授：林崇榮教授

組員姓名：賴駿家、廖炫華

研究期間：112年9月11日至113年6月21日止，共10個月

# I. 報告摘要

本研究提出利用 Physical Unclonable Function (PUF) 作為隨機性的來源，利用製程上的物理變異來實現這種隨機性。因為製程上的物理變異受到眾多因素的影響，例如製作環境、溫度、公差等，導致這些變異難以預測或分析。我們的研究動機在於利用這種特性去設計電路，將高度隨機的特性應用於晶片中的密鑰生成，PUF 就像是晶片中的獨特指紋，具有唯一性，即這項元件擁有不可複製的特徵，類似於現今手機或電子鎖所使用的虹膜、指紋、臉部等生物特徵作為唯一的金鑰。

近年來為了應對 AI 和演算法的威脅，開始陸陸續續發明了各式各樣 PUF，其中包含 Ring Oscillator PUF、Erasable PUF 或是 Multi-PUF 等等，但是這些設計各有優缺點，像是 Ring Oscillator PUF 特別容易受到 side channel attacks 的影響，或是 Erasable PUF 幾乎都會被現今的機器學習模型所破解，甚至有些傳統的 PUF 較難相容於電路之中，因此我們研究旨在高隨機性、易相容於積體電路中，並且能夠在各種環境中穩定輸出隨機性的結果。

本研究主要探討的是新型互補元件的 PUF，主要是以電晶體的 gate-to-source 或是 gate-to-drain 產生隨機性的崩潰，形成一端高電阻、另一端低電阻的互補對，此隨機性的崩潰主要來自製程上的物理變異，因此其隨機性非常穩定，並擁有完整的輸出響應，由於是內部隨機性物理不可複製函數的裝置，並且能夠具備抗讀取干擾以及溫度變化，所以在先進的積體電路整合也相對容易，具有高競爭優勢。

# II. 報告內容

## 1. 背景與動機

近年來隨著機器學習和 AI 的快速發展，破解晶片並竊取其資料變得越來越容易，因為現今機器學習的模型已經發展得相當成熟，像是利用邏輯回歸(Logistic Regression)、Support Vector Machine (SVM)，或是運用多層的神經網路去分析足夠多的激勵-響應對(Challenge Response pair)，訓練完的模型不僅有著極高的正確率，甚至還能預測新的 CRP，破解晶片變成一件輕而易舉的事情，因此硬體安全成為現今不可忽視的議題。

物理不可複製函數(PUF) 是一種基於硬體的安全技術，用於產生唯一的、不可複製的數字指紋，其目的是為了防範晶片中的資料被竊取、讀取，尤其在過去幾年中，演算法和人工智能的快速發展使得硬體安全也受到了威脅，因此人們開始致力於研發各種 PUF，為了提升硬體的安全性。

由於 PUF 擁有唯一性與隨機性，因此其包含了下列的特質。首先，在 CRP 的操作過程中，一個激勵一定會對應輸出一個響應，但是即便輸入相同激勵在通一個系統中，響應也不一定會相同，因為操作過程中可能會有雜訊的干擾。儘管如此，PUF 必須要含有可靠度和獨特性，可靠度(Reliability)指的是當施加多組相同的激勵時，無論任何溫度和各種雜訊的干擾下，輸出的響應要越接近彼此。獨特性(Uniqueness)則是剛好相反，當施加多組不同的激勵時，無論任何溫度和各種雜訊的干擾下，輸出的響應要相差越多，唯有 PUF 含有上述特質，才能辨識合法的使用者或是在電路中區分不同的裝置和使用者，以達到保護元件的效果。

## 2. 研究目的

由於 PUF 必須具備隨機性和唯一性，依照隨機性性質的不同又可以分成明確引入隨機性和內部隨機性。明確引入隨機性 PUF 需要額外的材料和製程步驟，像是光學物理不可複製函數(Optical PUF)、塗層物理不可複製函數(Coating PUF)等，這類型的 PUF 雖然較不受外在環境的影響，但也因為需要額外的材料，如光學物理不可複製函數需要額外的透明材料(Optical token)，其參雜隨機位置的光散射粒子，透過外在的雷射光去照射此材料，最後顯示出隨機的響應圖形，其缺點也非常明顯，就是難以相容於先進的積體電路。

內部隨機性物理不可複製函數則是利用電路本身的物理變異差異作為隨機性，並不需要額外的製程或材料，因為其本身在製作的過程中就會產生既定的差異，其應用也非常廣泛，最常見的有電阻式隨機存取記憶體物理不可複製函數(Resistance Random Access Memory PUF)，其隨機性來源來自電阻值的分佈，通常會選擇用高阻態的電阻值作為隨機性，因為高阻態的電阻值擁有較大的標

準差，雖然這種設計較容易與積體電路做整合，但是也因為 RRAM PUF 的輸出響應取決於兩個 RRAM 電阻值的差值，因此其輸出響應會下降一半，也就是需要兩個電阻才能輸出一種輸出。為了改善這個缺點，本研究提出了新型互補元件物理不可複製函數，其一個電晶體就能同時提供高電阻值和低電阻值，並利用隨機崩潰的機制作為隨機性，以達到完整的輸出響應。

## 3. 研究方法

### a、 新型互補元件 PUF 結構

新型互補元件 PUF 由兩個 NMOS 組成，如 Fig.1所示，上方的電晶體為選取電晶電晶體，其 Drain 定義為 Bit Line (BL)、Gate 定義為 Word Line(WL)、Source 與第二個電晶體的 Gate 相接，這個電晶體的目的是以 WL 的訊號來判斷此元件是否被選中；而第二個電晶體為寫入電晶體，其 Drain 定義為 $SL_0$、Gate 與選取電晶體的 Source 相接、Source 定義為 $SL_1$，寫入電晶體的目的則是在寫入過程中隨機形成高低阻態的互補對。有了高低阻態的互補對，即可使此元件輸出0或1的數位響應，以此達到 PUF 的功能，詳細操作過程在2.(3).c.ii.討論。

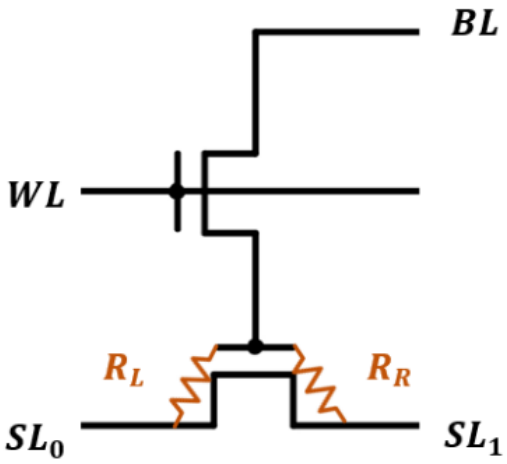


*Fig.1*

### b、 氧化層崩潰

新型互補元件 PUF 的原理為通過選取電晶體打開寫入迴路並提供電流，逐步加大寫入訊號直到寫入電晶體氧化層其中一端崩潰形成較低電阻。因為寫入電晶體左右端崩潰的順序無法被預測，幾乎為隨機的分布，因此可以被當作 PUF 使用。而也因為本研究涉及氧化層崩潰的反應，因此在研究過程中也探討以下三種常見的氧化層崩潰模型：

#### i. Precolation Model 滲透模型

此種模型用來解釋漸進式的氧化層崩潰 (Progressive Breakdown)，其原理是在電晶體遭受應力之下，電晶體的氧化層中會形成缺陷(Defect)以及電子陷阱(Trap)，這些會使電子有較高的機率從高位能的區域跳至較低位能的陷阱或缺陷，在外部應力足夠強的情況下就可能使氧化層產生導通的路徑引發所謂的電子滲透，使氧化層無法發揮其

原有的功能。

ii. Anode Hole Injection Model 陽極電洞注入模型

此模型解釋在電子因為直接穿隧(Direct Tunneling)或 F-N 穿隧(Fowler-Nordheim Tunneling)而直接穿過氧化層時，因其所帶有的電位能太高而轉變為撞擊游離能，從而生成電子電洞對，其中，電洞可能會被氧化層中的陷阱捕獲；而電子則會向陰極靠近，使電場增強。上述這兩種現象使傳導路徑產生，形成漏電流，而當陷阱捕獲的電洞數量達到臨界時，氧化層就會崩潰。

iii. Generated Subordinate Carrier Injection Model 生成附屬載子注入模型

此模型結合了陰極電子注入模型和陽極電洞注入模型，是附屬載子經由直接穿隧或 F-N 穿隧通過氧化層時因為能量差異產生的，而附屬載子即為電子與電洞，其分別是，在 Gate 施加負電壓時，附屬載子為電子；而 Gate 施加正電壓時則為電洞。與陽極電洞注入模型相同，氧化成崩潰的時機都在氧化層捕獲的附屬載子達到臨界時發生。

氧化層崩潰後電性由電容轉變為電阻，而阻值的大小取決於氧化層崩潰後所形成的導電路徑截面積大小成反比，截面積越大阻值越小，截面積越小則阻值越大。截面積的大小與氧化層崩潰時所釋放的能量大小成正比關係，而此能量的來源是氧化層原先作為電容所儲存的能量，但要注意的是崩潰的過程中能量並不見得完全釋放，所以必須以崩潰前後所施加的電壓比較後才能得出釋放的能量。簡而言之，氧化層在崩潰後釋放出能量，並以此決定崩潰後導電路徑上的電阻值。

c、 操作機制

i. 寫入

新型互補元件 PUF 的寫入由選擇電晶體提供並限制電流，所以在 WL 施加定電壓，BL 與 Body 接地，並以增量階躍脈衝程式(Increment Step Pluse Programming)逐步提高 $SL_0$與 $SL_1$的脈衝電壓，並且在每次脈衝過後測量寫入電晶體的兩端是否有高低阻態的互補對產生，意即是否有氧化層崩潰的現象，如果互補對成功產生就停止寫入。而較令人擔心的是在一次的脈衝之中是否可能使兩端的氧化層崩潰，答案是機會非常低，因為在其中一端氧化層崩潰後形成的低電阻會使電流從那一端導出並且電流也被選擇電晶體限制，故較不容易出現兩端都崩潰的情況。

ii. 讀取

讀取操作同樣是將 WL 設定為定電壓使選取電晶體導通，不同的是讀取階段 $SL_0$與 Body 接地，$SL_1$則是接到元件的最高電壓 $V_{DD}$，並且以 BL 作為輸出的端點。當 $SL_0$端為低電阻時(即 $SL_1$端為高電阻)，BL 的電壓就會被拉低到0V，視為數位響應的0；反之，當 $SL_0$端為高電阻時(即 $SL_1$端為低電阻)，BL 的電壓就會被抬升到 $V_{DD}$，視為數位響應的1。機制如 Fig.2所示。

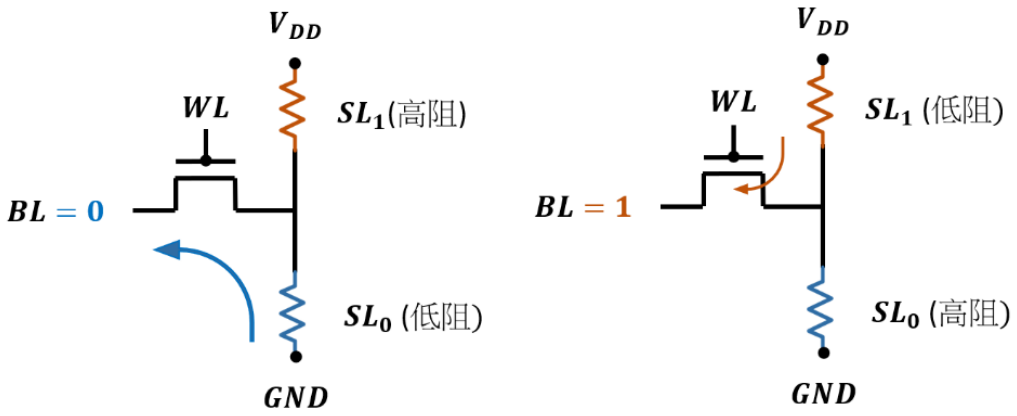


*Fig.2*

d、 陣列結構

以上的新型互補式元件 PUF 都為單一元件，只能隨機產出一個位元的硬體密鑰；不過此單一元件也可組成陣列達到產生多位元密鑰的目的，如 Fig.3 為一個2x2的陣列可產生四個位元的硬體密鑰。

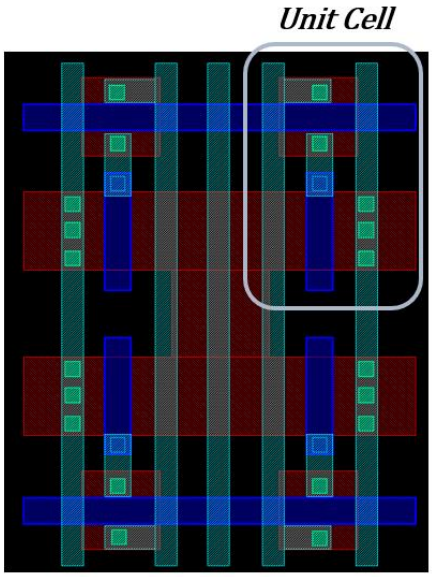


*Fig.3*

## 4. 研究結果

a、 互補對阻值測量

如同上述寫入操作在 WL 施加定電壓1.2V，並將 BL 與 Body 接地，用增量階躍脈衝程式以0.1V 的步進提高 $SL_0$與 $SL_1$的電壓，並設定每次脈衝的時長為1毫秒，在每次脈衝過後測量寫入電晶體的兩端是否有高低阻態的互補對產生，若發現互補對順利產生則停止脈衝，同時測量兩端所形成的電阻阻值。結果如 Fig.4所示，在寫入並測量多組新型互補元件 PUF 後，以累積機率對阻值作圖，藍色線低阻態阻值，而橘色線為高阻態阻值，從圖表可以得知，即便在最低可能出現的高阻態阻值以及最高可能出現低阻態的阻值之下，讀取的窗口也能夠保持在100倍左右，這顯示了此互補對可以很好的形成區分使輸出的電壓能夠保持0/1的數位響應。

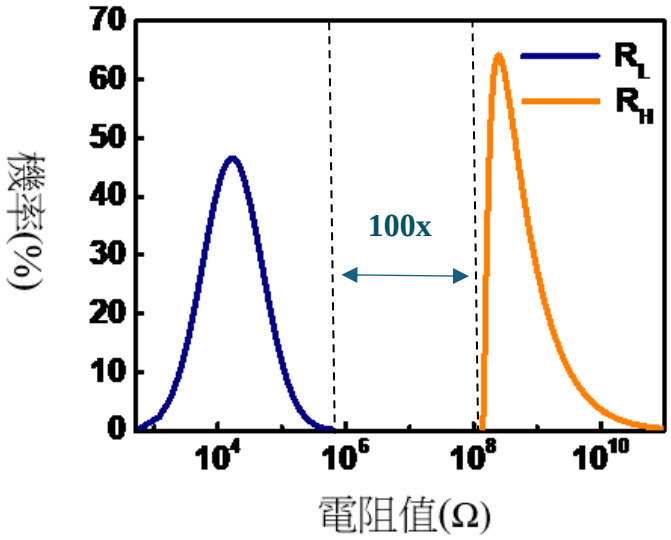


*Fig.4*

b、 隨機性測量

存在隨機性是 PUF 所必須具備的基本要素，所以本研究中也測量此種 PUF 是否具備足夠的隨機性，在前述的互補對阻值測量中，同時我們也統計了 BL 輸出為數位響應0或1的情況，並同樣以累積機率對 BL 輸出的數位響應作圖，得到 Fig.5，結果出現0/1的情況比例接近為1:1，也就是兩種響應出現的機率都各約為50%。這樣的結果展現此互補元件具有良好的隨機性，沒有偏向其中一端崩潰的情況。

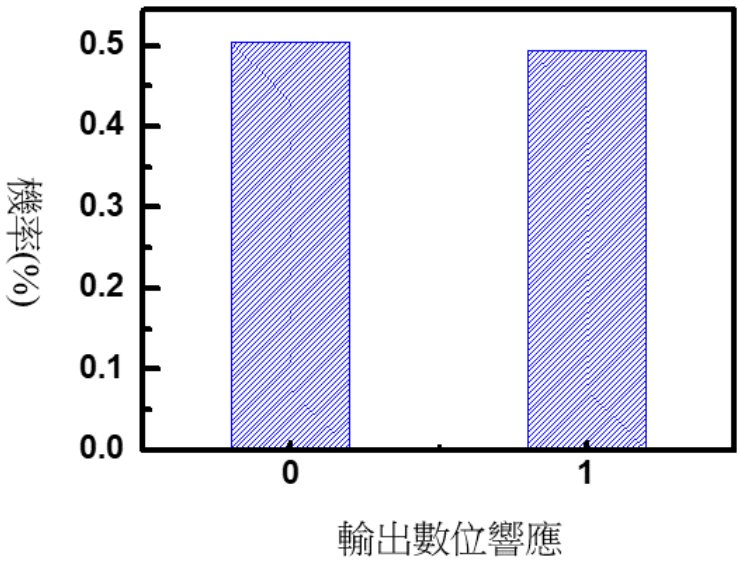


*Fig.5*

c、 可靠度測試

i. 抗讀取干擾

為了測試此元件是否能夠持續讀寫不會造成密鑰失效或錯誤，我們將新型互補元件 PUF 作一萬秒的讀取測試，同時監控 BL 輸出電壓以及互補對的阻值，觀測高阻態端的氧化層是否會因為長時間讀寫而崩潰，從而使互補對失效。測量結果顯示，在一萬秒的連續讀寫情況下 BL 輸出的電壓與互補對的阻值都沒有明顯的變化，因此我們認定此種元件具有抗讀取干擾的特性。

ii. 抗溫度干擾

為了測試此元件是否能夠承受在不同的溫度底下不會造成互補對失效，我們將元件放入恆溫控制器使之維持在85℃的溫度下，發現有元件的低阻態端阻值有上升的情況，我們認為是因為氧化層的重新修復導致寫入時擊穿的氧化層導通路徑截面積縮小或是路徑封閉，不過，即使在低阻態阻值上升的情況下，與高阻態的阻值仍有10倍以上的差距，根據分壓定律，BL 的輸出電壓依舊能夠明顯區別0出與1的數位響應，因此我們認為此元件具有一定的抗溫度干擾。

## 5. 結論

本研究所提出的新型互補元件 PUF，以 RRAM PUF 做為發想，同樣以元件阻值的高低阻態作為隨機性的來源，以一個 N 型電晶體通過製程帶來的微小變化使 Gate 到兩端氧化層能夠承受電壓不同的特性來擊穿其中一端，在同一個電晶體中實踐同時存在高低阻態的互補對。並且在後續的測量當中也證明此元件符合 PUF 所要求的隨機性以及良好的高低阻態分布。同時，新型互補元件 PUF 存在以下優點：相容於現代先進製程、抗讀取干擾、抗溫度干擾的特性、能夠輕易組成陣列達到更安全的密鑰。但是如討論寫入機制所提到，此元件有機會在寫入時同時擊穿兩端氧化層，所以我們認為未來若是能夠發想其他回饋機制使寫入時兩端氧化層不會都變為低阻態的情況，那麼此項元件會具有相當好的競爭力。

# III. 心得

在這兩個學期的專題課程中，我們從閱讀論文開始，一步步構建對於物理不可複製函數（PUF）的相關知識。這個過程不僅讓我們深入了解 PUF 技術的原理和應用，也讓我們意識到這個領域對現代硬體的重要性。透過文獻的閱讀和背景知識的累積，我們更能夠在研究、發想與實踐上更自由地發揮創意，這也激發了我們對 PUF 元件的求知動力。

而在後續的設計與測量過程中，我們學習到如何操作測量儀器。能夠親自動手操作是一個寶貴的經驗與學習，讓我們深刻體驗到，經過大學三年基礎科目的學習後，終於能夠親手做出東西的感動。因此，我們覺得這項專題研究也像是對我們過去三年學業的一次驗收。正是有過去的那些努力、知識的累積，才讓我們能夠在專題研究中面對迎面而來的各種未知與困難。

當專題研究告一個段落後，回想起共同面對的種種，我們深刻體會到合作、溝通還有隊友的重要性。有隊友在旁邊一起做事、一起思考，激發出的討論、辯論會使人更加專注，也能藉此碰撞出更多靈感。同時，這樣的合作也增進了我們的表達能力，磨練了與人相處的模式。

這兩個學期的專題研究不僅讓我們學到了關於 PUF 技術的知識，更重要的是，它培養了我們的動手能力、合作精神和解決問題的能力。這對我們未來的學術和職業生涯都將是極為寶貴的財富。

最後我們想謝謝林崇榮教授願意成為我們的指導教授，也感謝林唯華、陳冠儒學長帶著我們討論論文、教會我們操作儀器以及給予我們其他種種的幫助。