2021 年臺灣國際科學展覽會
優勝作品專輯

作品編號　160024

參展科別　物理與天文學

作品名稱　四眼渦漩-混沌電路之密鑰生成器

得獎獎項　大會獎 三等獎

美國國際開發署獎

就讀學校　臺北市立第一女子高級中學

指導教師　林宗賢、陳正源

作者姓名　李宛頤

關鍵詞　混沌電路、物理不可複製函數、密鑰生成器

作者簡介

我是李宛頤，就讀於北一女中數理資優班，對於自然科學以及數學等科目都蠻喜歡的，也喜歡嘗試這些科目的難題或競賽，或是閱讀更深入的書籍。科展對我來說其實算是一個新的挑戰，因為要面對的是一種未知，且難以捉摸的東西，需要透過不斷嘗試、修正和學習，但我也在過程中學會了許多技能和態度。

摘要

本專題利用混沌電路本身的不可預測性及混亂程度，製造出作為硬體安全實現的密鑰生成器。從實現基本的蔡氏電路，並探討蔡氏電路作為硬體安全的相關應用為基礎，進而實現進階的研究改造。透過電阻、電感、電容、運算放大器等電子元件，焊接在電路板上，實現一個「四渦漩狀」的混沌電路。

本研究的最大特點，就是會製作兩個具備相同電子元件及構型的多吸引子混沌電路，但天生的元件變異性會產生「類蝴蝶效應」，再利用數位乘法器，將兩個電路之類比訊號相乘，而這個操作會形成一個密鑰生成器的混沌系統。

最後會透過軟體 MATLAB 確認電路操作和分析電路輸出信號，及所提出密鑰生成器的安全程度，將會驗證隨機性和獨特性這兩組特徵，分別計算平均及交叉相關函數來做為驗證的依據。最後從實驗中證明了「四渦漩狀」的混沌電路所產生的密鑰具有快速產生及高安全性。

This work proposes a hardware cryptographic key generator based on the inherent unpredictable and chaotic characteristics of chaos circuits. Starting from the implementation of a basic Chua circuit, we investigate the basic application of hardware security. Moreover, an advanced technique is proposed to implement a “4-scroll” chaos circuit by integrating resistors, inductors, capacitors and op amps on a circuit board.

Rather than using a single chaos circuit, this research employs two identical multi-scroll chaos circuits, in which they have small component value variation, to induce “butterfly-like effect”. With analog multipliers, the outputs of these two identical circuits would be multiplied to generate a key in a chaos system.

MATLAB is also employed to verify the operation of the proposed circuit and perform the circuit output signal analysis and the robustness of the proposed key generator. Furthermore, randomness and uniqueness are used to evaluate the cryptographic key by its mean and cross-correlation. With the experimental results, the proposed “4-scroll” circuit can generate the hardware key efficiently with high security.

壹、 研究動機

在公園中，我們看到許多小朋友在盪鞦韆時，他們的笑容隨著鞦韆的高度而綻放。綻放到令我們看傻了眼，模糊中只剩下鞦韆在擺盪，腦中頓時冒出了一條繩子，隨著鞦韆一前一後、一上一下地擺動著，再加上小朋友上下擺動時扭動身體而形成複雜的運動軌跡。這樣擺動的特性是什麼？越想越覺得有趣。

兒時的盪鞦韆經驗，在加上我們物理老師提出混沌電路這個研究題目，上網查了一些資料發現，原來這種進行不規則振盪的電路可以用數學的方式表達，而他振盪的紊亂程度，也讓我想到，為何不運用它來製造一個複雜的系統呢?

伴隨 5G 明年即將正式商轉，物聯網(IoT)時代特有的萬物皆聯網景況也近在咫尺，屆時連網物件數量將呈現猛增暴漲，物聯網技術的前期採用者，除了加速物聯網基礎建設與創新技術應用導入之外，也面臨更廣泛的安全管理風險與更嚴峻的資訊安全挑戰，因為在「萬物皆聯網」的時代，同樣也會造成「萬物皆可駭」的情境，以智慧家庭為例，當連接的設備越來越多，像是智慧電器，嬰兒監視器，室內攝影機等設備的增加，很容易成為駭客攻擊，病毒入侵，勒索軟體與網路釣魚詐騙下手的目標，隱私外洩，個資散播等後果不計其數。而車聯網的資安問題同樣也是不可忽略的，隨著自駕車的出現，車聯網彼此的串聯程度越加複雜，也將帶來一系列的安全問題，自駕車被駭客入侵使得騎在路上亂行駛或是交通號誌遭到入侵被惡意竄改，使得城市交通癱瘓並造成公共危險，背後損失也是難以估計。除了我們生活周遭，物聯網裝置甚至可以讓海外駭客控制企業網路路由器，引發大規模的阻斷服務攻擊，或是駭客駭入政府相關網站使得國家相關機密遭到竊取，引發國安危機，因此小至個人，企業，大至國家，資安的技術提升成為刻不容緩的課題。

因此，為發出的訊息加密是一件十分重要的事情。所以會想要利用這個蔡氏電路本身的混沌現象和紊亂程度，設計出一套夠複雜，夠混亂，使人難已破解的一套密鑰，而透過對基本蔡氏電路雙渦漩波型的了解，進而對非線性電路的分析，進一步把基本型的電路由雙渦漩拓展為四渦漩，把密鑰的混亂性及非相關性進一步的提升。

貳、 研究目的

在非線性科學中，混沌現象指的是一種確定的但不可預測的運動狀態。它的外在表現和純粹的隨機運動很相似，即都不可預測。但和隨機運動不同的是，混沌運動在動力學上是確定的，它的不可預測性是來源於運動的不穩定性，或者說混沌系統對無限小的初值變動特別敏感性，即初始值的微小差別經過一段時間後可以導致系統運動過程的顯著差別，其次它還具有遍歷性和內隨機性等複雜特徵。

如果把混沌信號與發送信號經過調製處理後再進行發送，這就會增加信號的破譯難度，所以混沌系統特別適合用於保密通信領域。1983 年，美國加州大學的蔡少棠教授與日本早稻田大學進行學術交流時發明了蔡氏電路[1]，蔡氏電路是非線性電路中能產生豐富複雜動力學行為的最簡單、最有效的電路。目前，蔡氏混沌電路在很多領域都已經得到廣泛的應用，但利用蔡氏電路設計保密通信電路時會存在如下問題 ：

1. 雖然蔡氏混沌電路具有混亂的振盪行為，但是其電路行為仍然可以用數學的公式描述出來，因此嚴格上來講此電路的行為雖然是混亂的，但是仍然亂中有序。單純的使用一個蔡氏電路來產生通訊上所需要的密鑰，這樣的技術在過去的文獻已經有人探討且使用， 雖然產生的數位密碼看起來是隨機的，安全性仍然是不足的。

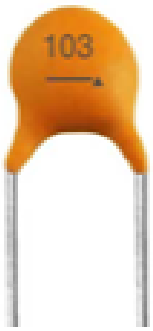
2. 蔡氏混沌電路本身俱備的蝴蝶效應，也就是說一點點初始條件的不一樣都會導致於最後行為的不可預知。但在實際使用電路的時候，我們會傾向清除電路裡面所有的電流電壓，使初始條件為零 ，因此要精準地利用蝴蝶效應的特性在蔡氏電路當中，比較不容易實現。

所以傳統蔡氏電路運用在通訊的密鑰產生器具備<u>安全性不足</u>且<u>實際使用上面的不易</u>，我們在這一個研究作品當中將提出利用兩個看似一樣的蔡氏電路，但具備物理不可重複性的概念中 ，彼此的交互作用產生高安全性的通訊密鑰。

參、 研究設備及器材

一、電子零件

(一) 電容 103 (10nF), 104 (100nF)

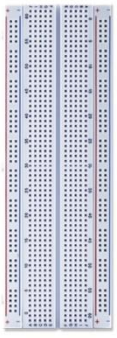


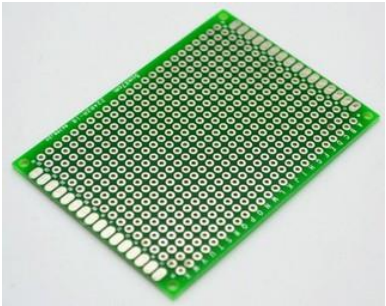
(二) 電感 (20 mH)

(三) 電阻及可變電阻

(四) 運算放大器 (TL082 CP)

(五) 麵包板/萬用電路板



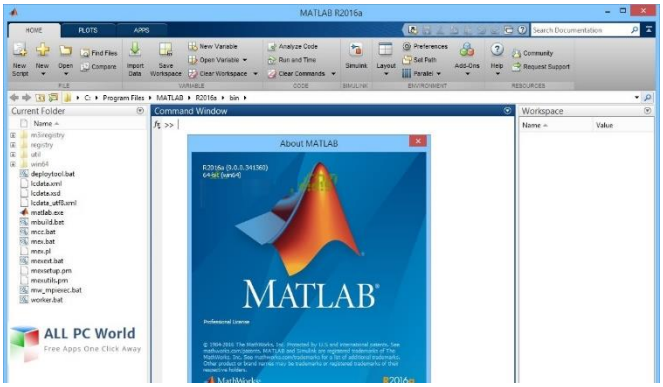


二、儀器

(一) 數位儲存示波器(Tek-1025B-EDU)

(二) 電源供應器 (GPS 3303)

(三) 軟體



三、實驗架設

如圖 3-1 所示，麵包板是不需要經由焊接過程，就可以將本研究蔡氏電路中所使用的電子元件加以連接，由於蔡氏電路是振盪電路，把電源供應器接上，就可利用示波器觀察波形，而 Tek-1025B 數位儲存示波器可儲存 2500 點電壓對時間的 EXCEL 格式輸出，MATLAB 可讀入 2500 點電壓並進行數據分析。由於示波器僅可儲存 2500 點，我們可用電路的 MATLAB 等效模型，做較長的數序做進一步分析。

在執行本研究一開始是使用麵包板來完成電路，但由於麵包板本身只是把元件插上去，因此元件會有接觸不良的問題，在四渦漩的混沌電路研究中，我們直接使用萬用電路板，如圖 3-2 所示，透過焊接的方式以及繞線棒提供更穩定的操作。

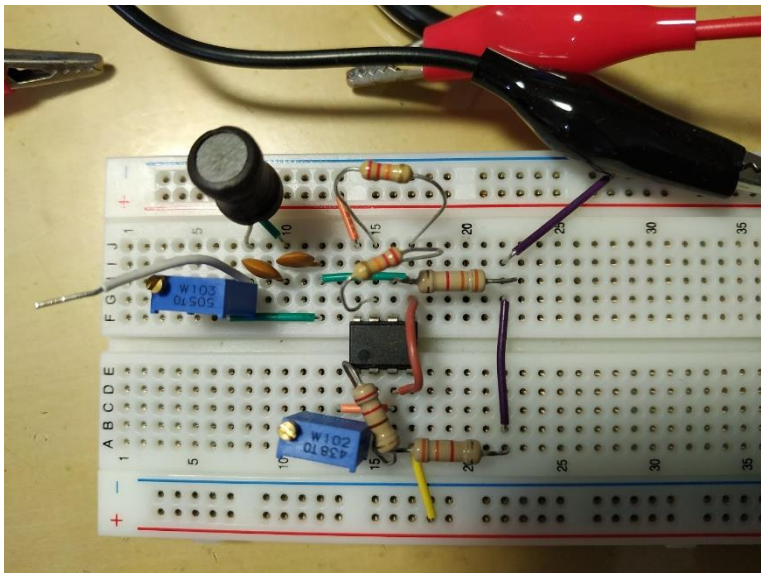


圖 3-1 麵包板上的蔡氏電路

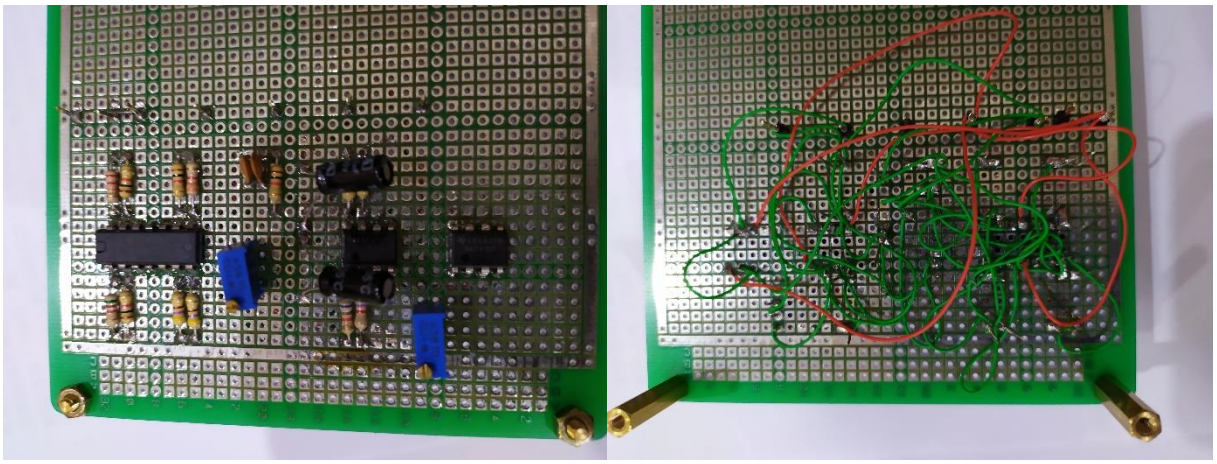


圖 3-2 萬用電路板上的蔡氏電路

肆、 研究過程或方法

一、研究步驟

(一) 發展研究架構。

(二) 原理分析與文獻探討。

1. 關於「混沌系統」。

2. 關於「蔡氏電路」。

3. 關於「蝴蝶效應」。

4. 關於「物理不可複製函數」。

5. 關於 MATLAB。

(三) 探討「蔡氏電路」輸出

1. 「蔡氏電路」輸出電壓 YT 及 XY 圖

2. 用「XY」軸建立二位元碼輸出判準。

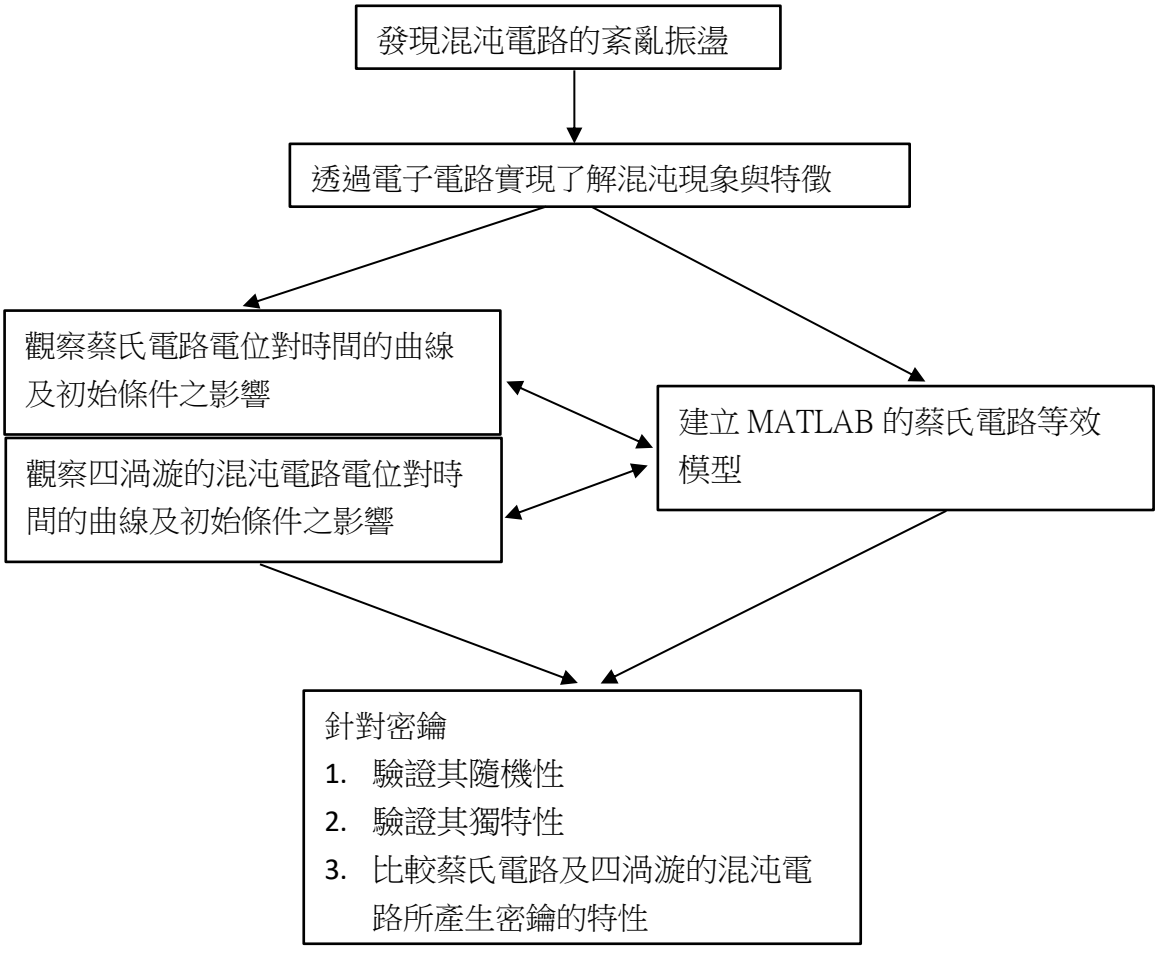
3. 蝴蝶效應模擬圖。

4. 物理不可複製函數輸出圖。

二、發展研究架構

「混沌電路可以產生硬體密鑰 ？！ 」當一個系統的處於振盪狀態，所產生的信號及量，是週期性的，所以並不適合用於密鑰產生。但若是系統處於一種混沌振盪的狀態時，基本上既是「振盪中存在另一種振盪」，此種特殊的電路運作狀態特別適合加密的密鑰產生器。

我們從發現混沌電路[2]的紊亂振盪這樣象後，提出「結合蔡氏電路及物理不可複製函數」的研究假設，透過實驗及模擬確定其隨機性及獨特性。研究架構圖如下:



三、原理分析與文獻探討

(一) 混沌系統

混沌理論是一種兼具質性思考與量化分析的方法，用以探討動態系統中**無法用單一的數據關係，而必須用整體，連續的數據關係才能加以解釋及預測之行為**。

「一切事物的原始狀態，都是一堆看似毫不關聯的碎片，但是這種混沌狀態結束後，這些無機的碎片會有機地匯集成一個整體。」

混沌一詞原指發現宇宙混亂狀態的描述，古希臘哲學家對於宇宙之源起即持混沌論，主張宇宙是由混沌之初逐漸形成現今有條不紊的世界。在井然有序的宇宙中，科學家經過長期的探討，逐一發現眾多自然界中的規律，如大家熟知的萬有引力、槓桿原理、相對論等。這些自然規律都能用單一的數學公式加以描述，並可以依據此公式準確預測物體的行徑。

近半世紀以來，科學家發現許多自然現象即使可以化為單純的數學公式，但是其行徑卻無法加以預測。如氣象學家愛德華·諾頓·勞侖次發現簡單的熱對流現象居然能引起令人無法想像的氣象變化，產生所謂的「蝴蝶效應」。60年代，美國數學家史蒂芬·斯梅爾發現某些物體的行徑經過某種規則性變化之後，隨後的發展並無一定的軌跡可循，呈現失序的混沌狀態。

(二) 蔡氏電路

近年來，混沌在非線性科學，信息科學。保密通信以及其他工程領域已獲得廣泛的應用，在混沌電路方面，也提出了許多新的方法來設計各種不同類型的混沌電路，蔡氏電路算是當前最有代表性的一種，其電路結構已成為理論和實驗研究混沌系統的一個範例，再此基礎上，人們還進一步研究了蔡氏電路的其他形式，如對偶蔡氏電路，變形蔡氏電路，多渦漩蔡氏電路，但都是依照著典型的蔡氏電路模型，也就是用電容，電感，電阻和非線性電阻。來構接蔡氏電路

在表現混沌行為之前，一個由標準部件(電容，電阻，電感)所製作的自振盪電路必須滿足三個標準:

1. 一個或者多個的非線性元件

2. 一個或者多個的本地主動電阻

3. 三個或者更多的能量儲存元件

蔡氏電路即是滿足這三個標準最簡單的電子電路，其中的能量儲存元件是由兩個電容(C_1 及 C_2)和一個電感(L)所形成。有一個電阻(R_P)，還有用兩個運算放大器(TL082)製作的一個非線性電阻。

通過電路學定律的應用，在圖4-2-1所示蔡氏電路，可以建立精準的數學模型，是三個變量$V_1(t), V_2(t), i_L(t)$，三個非線性常微分方程的系統，如方程式(1)-(3)所示

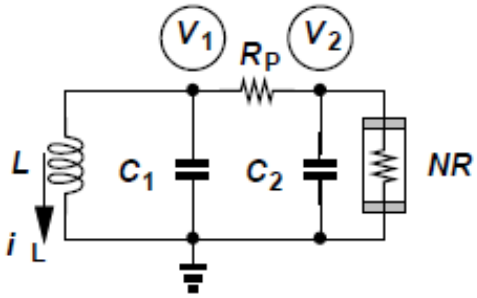


圖 4-2-1 原始蔡氏電路

在圖 4-2-1 中，*NR* 為一非線性電阻，可由圖 4-2-2 中的兩個運算放大器及數個電阻所組成，

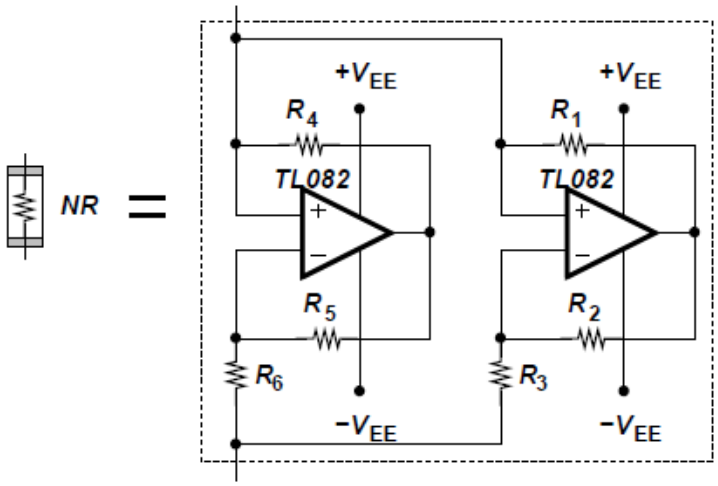


圖 4-2-2 *NR* --- 非線性電阻

三個微分方程[3]可由 KCL 於 V_1 及 V_2 兩節點寫出，在本研究中所用到電子元件之值記錄於表 4-2-1 中，

$$C_1\frac{dV_1}{dt}=\frac{1}{R_P}(V_2-V_1)-I_L \quad (1)$$

$$C_2\frac{dV_2}{dt}=\frac{1}{R_P}(V_1-V_2)-NR(V_2) \quad (2)$$

$$L\frac{dI_L}{dt}+I_LR_L=V_1 \quad (3)$$

表 4-2-1 蔡氏電路中電子元件值

元件	值	元件	值	元件	值
L	20 mH	R_1 (可調)	245 Ω	R_4	22 kΩ
C_1	100 nF	R_2	220 Ω	R_5	22 kΩ
C_2	10 nF	R_3	2.2 kΩ	R_6	3.3 kΩ
R_p(可調)	1.6 kΩ				

為了建立 MATLAB 的蔡氏電路等效模型，*NR* 此非線性電阻，可用透過歐姆定律及電路分析而得到下列公式(4)描述，整體而言，如圖 4-2-3 所示，非線性電阻有三個操作區間，是由 E_1 及 E_2 所決定，三個操作區間分別呈現出三個等效電阻 $\frac{1}{m_0}$、$\frac{1}{m_1}$ 及 $\frac{1}{m_2}$。

$$E_1=+V_{EE}\times\frac{R_3}{R_2+R_3}$$

$$E_2=+V_{EE}\times\frac{R_6}{R_5+R_6}$$

$$m_0=-\frac{R_2}{R_1R_3}-\frac{R_5}{R_4R_6} \quad (4)$$

$$m_1=\frac{1}{R_1}-\frac{R_5}{R_4R_6}$$

$$m_2=\frac{1}{R_1}+\frac{1}{R_4}$$

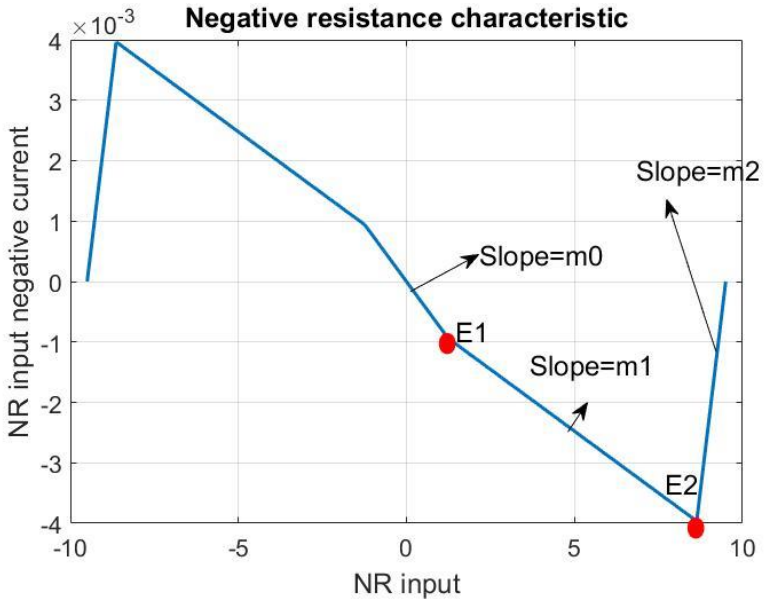


圖 4-2-3 *NR* 之電流 vs. 電壓

R_1、R_2、R_3 及 TL082 形成一負電阻，R_4、R_5、R_6 及 TL082 形成另一負電阻，並且用 TL082 的極值 $(+V_{EE}/-V_{EE})$ ，我們可用多項式回歸的方式找出等效 *NR* 的方程式 (5)

$$y = 4.4^{-6} \times x^3 - 6.55^{-4} \times x \qquad (5)$$

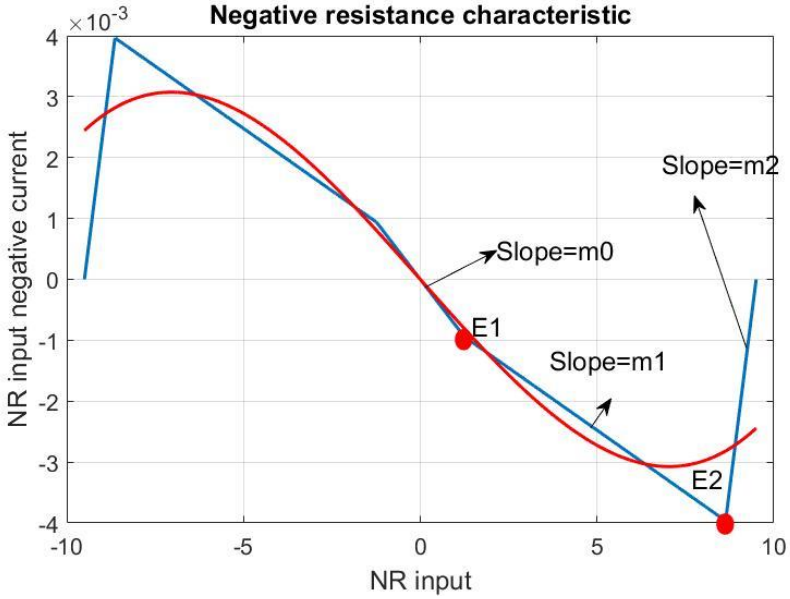


圖 4-2-4 三階多項式(紅線)去近似 NR

我們在建立等效的電路模型的時候，對此非線性電阻，如圖 4-2-4 所示，我們可以使用三階或更高階的多項式去描述它， 當然也可直接利用輸出對輸入的相對關係，分區段地用 m_0-m_2 及 $E_{1,2}$ 描述， 兩者之間都有非常類似的模擬結果。

針對雙渦漩的蔡氏電路，我們是利用非線性電阻中不同的負電阻來產生雙穩定的振盪，其中振盪會在斜率(NR 的轉導)是比較小(m_1)的地方產生，此地方所對應的負電阻相

對是比較大的，透過這樣的觀察，我們思考如何把蔡氏電路的雙渦漩或者是雙振盪的行為把它延伸及擴大，當然所需要的就是要構建一個具有多斜率的非線性電路。

我們藉由參考文獻中的負電阻產生器及正電阻產生器 [4]，在延展電路中，我們使用了一個正電阻產生器及兩個負電阻產生器，再利用不同的斜率及操作區間我們可以產生非線性的電阻如圖 4-2-5 所示。很明顯的這一個延展的負電阻產生器其具備的斜率段落較單純的雙渦漩設計更具多樣性，而其中此電路有四個斜率比較平坦的地方，所以我們可預計的時電路可以產生四個渦漩。

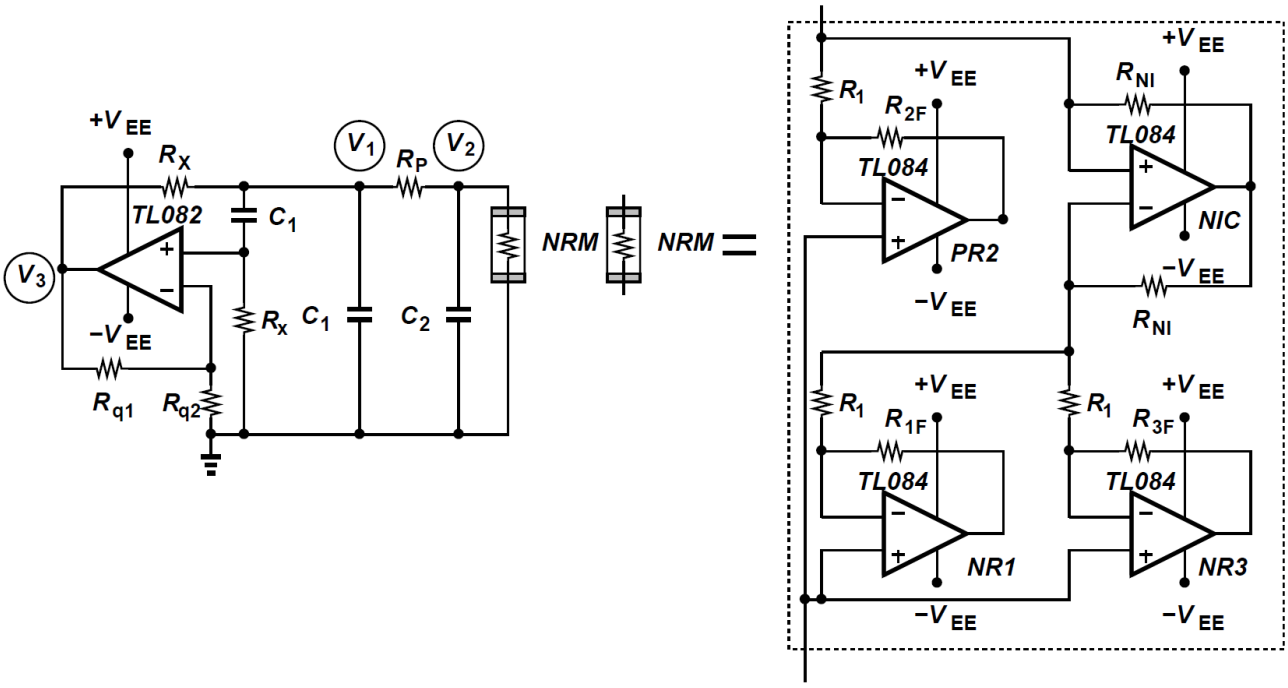


圖 4-2-5 四渦漩混沌電路及 *NRM*---四分段(4-segment piecewise linear) 非線性電阻

同樣地，三個微分方程(4)-(6)可由 KCL 於 V_1 、V_2及 V_3 三節點寫出，其中 $k=1+R_{q1}/R_{q2}$，在本研究中的 四渦漩混沌電路所用到電子元件之值記錄於表 4-2-2 中，

$$C_1\frac{dV_1}{dt}=\frac{1}{R_P}(V_2-V_1)+\frac{(k-1)V_3-kV_2}{kR_P} \quad (4)$$

$$C_2\frac{dV_2}{dt}=\frac{1}{R_P}(V_1-V_2)-NRM(V_2) \quad (5)$$

$$C_2\frac{dV_3}{dt}=\frac{k(V_2-V_1)}{R_P}+\frac{(k-2)V_3-k(V_1)}{R_x} \quad (6)$$

我們可以利用下列的公式(7)來描述這個四分段(4-segment piecewise linear) 的非線性負電阻，及其操作的區間，此種概念當然可以繼續延展而電路的複雜度將因此而增高，在本專題研究中，我們則是透過由二變四是來觀察密鑰產生的收斂性及其相關性。

$$\boldsymbol{i = NRM(v) = \sum_{m=1}^{3} (-1)^m \left[G_{bm} v + 0.5(G_{am} - G_{bm}) \times \left(|v + E_{pm}| - |v - E_{pm}| \right) \right]} \quad (7)$$

其中 $\boldsymbol{G_{am} = \frac{1}{R_{mF}}}$ ，$\boldsymbol{G_{bm} = \frac{1}{R_1 + R_{mF}}}$，$\boldsymbol{E_{pm} = \frac{R_{mF}}{R_1}}$

圖 4-2-5 分別有正電阻 PR2 及 負電阻 NR1 及 NR3，透過不同操作區間 E_{p1}-- E_{p3} 區間，進而合成出圖 4-2-6 的 NRM (Negative resistance – mult-segment) ，

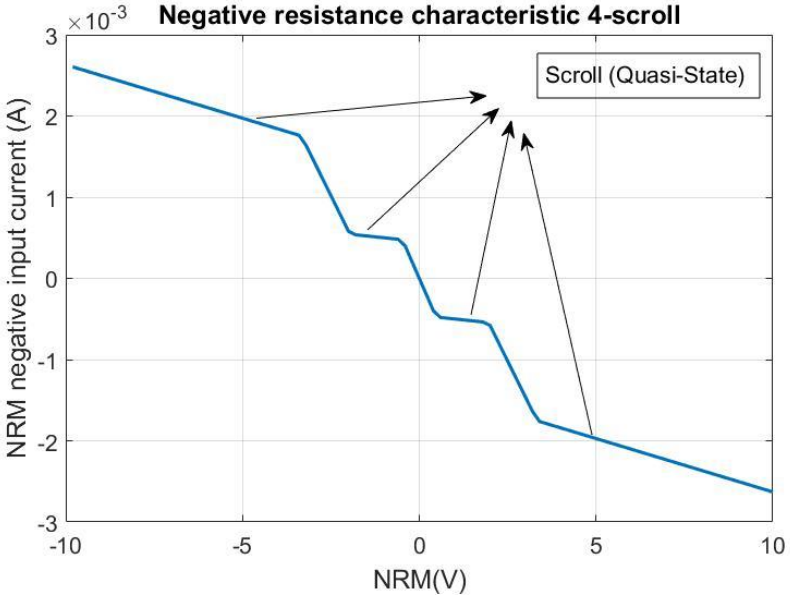


圖 4-2-6 *NRM* 之電流 vs. 電壓

表 4-2-2 四個渦旋混沌電路中電子元件值

元件	值	元件	值	元件	值
C_1	100 nF	R_p (可調)	1.9 kΩ	R_{1F}	3.1 kΩ
C_2	6.6 nF	R_1	1 kΩ	R_{2F}	5 kΩ
R_x	500 Ω	R_{NI}	500 Ω	R_{3F}	22 kΩ
R_{q1}/ R_{q2}(可調)	6.6kΩ /3.2kΩ				

(三) 蝴蝶效應

蝴蝶效應是指在一個動態系統中，初始條件的微小變化，將能帶動整個系統長期且巨

大的連鎖反應，是一種混沌的現象，蝴蝶效應在混沌學中也常出現

蝴蝶效應的來歷是在1963年的一次實驗中，美國麻省理工學院氣象學家勞倫茲用電腦求解模擬地球大氣的13個方程式。為了更細緻地考察結果，在一次科學計算時，勞倫茲對初始輸入數據的小數點後第四位進行了四捨五入。他把一個中間解0.506取出，提高精度到0.506127再送回，前後計算結果卻偏離了十萬八千里，前後結果的兩條曲線相似性完全消失了。根據常識，同樣的程式和數據顯然會導致同樣的結果。但是第二次的預報結果與上一次大不一樣。開始他認為是電腦的故障，排除了這種可能後，他發現，他輸入的不是完整的數據。再次驗算發現電腦並沒有毛病，洛倫茲發現，由於誤差會以指數形式增長，在這種情況下，一個微小的誤差隨著不斷推移造成了巨大的後果。勞倫茲在美國《氣象學報》上發表了題為"確定性的非周期流"的論文，提出了在確定性系統中的非周期現象。第二年，他發表了另外一篇論文，指出對於模式中參數的微小改變將導致完全不一樣的結果，使有規律的、週期性的行為，變成完全混亂的狀態。於是，勞倫茲認定：事物發展的結果，對初始條件具有極為敏感的依賴性。他於是認定這為：“對初始值的極端不穩定性”，即混沌，又稱蝴蝶效應。他說，一隻南美洲亞馬遜河流域熱帶雨林中的蝴蝶，偶爾扇動幾下翅膀，可能在兩周後在美國德克薩斯引起一場龍捲風。其原因在於：蝴蝶翅膀的運動，導致其身邊的空氣系統發生變化，並引起微弱氣流的產生，而微弱氣流的產生又會引起它四周空氣或其他系統產生相應的變化，由此引起連鎖反映，最終導致其他系統的極大變化。勞倫茲把這種現象戲稱做"蝴蝶效應"，意思即一件錶面上看來毫無關係、非常微小的事情，可能帶來巨大的改變。

蝴蝶效應是指在一個動態系統中，初始條件的微小變化，將能帶動整個系統常其且巨大的連鎖反應，是一種混沌的現象，蝴蝶效應在混沌學中也常出現

也就是說，事物發展的結果，對初始條件有極為敏感的依賴性，也就是對「對初始值的極端不穩定性」，此即為混沌。

(四) 物理不可複製函數 [5] (PUF)

PUF 是一種在實體系統上給入特定的輸入挑戰(Challenge)會得到對應的輸出回應(Response)的技術，它是利用矽晶片產生時，元件的製程變異(Process Variation)，使得每個晶

片的物理特性有所偏移(如電晶體的寬度)，由於每個晶片都有自己獨特的變異，因此可作為密鑰來認證每個晶片正當性。

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

評估一個PUF，有幾個準則： PUF 給入挑戰後產生的輸出回應是否相當隨機，相同的PUF 彼此間的輸出回應是否具有獨特性等。本研究受限於有限的樣本，將僅對隨機性及獨特性進行介紹[6]。

1 隨機性(Randomness):

隨機性代表同一個PUF 在相同溫度、工作電壓下，隨機給入多組不同的挑戰而產生的一連串輸出回應，0 與1 的個數是否平均。

若產生的0、1 的個數越接近總數的一半(50%)，則這個PUF 具有相當的隨機性；反之，若產生的輸出回應0 或1 的個數占絕大多數，代表PUF 的隨機性相當低，也越容易被攻擊者猜到，我們將採取正規化平均值公式(6) ，去評估PUF的隨機性，愈接近零，隨機性愈好。

$$mean = \frac{\sum_1^n a}{n} \qquad (6)$$

2 獨特性(Uniqueness)

在不同晶片上，相同種類的PUF 在相同溫度、工作電壓下，給入相同的挑戰，我們會希望每個PUF 彼此之間的輸出回應都不相同，以顯示每個PUF 各自的獨特性。理想情況下，兩兩PUF 的輸出應有50%不同，

若完全一樣則失去PUF 的特色；若完全反相，也容易被攻擊者猜出。判斷PUF 的Uniqueness，我們將採取交叉相關函數 (7) ，去評估PUF的獨特性，愈接近零，獨特性愈好。

$$cor = \left| \frac{\sum_1^n a_i \times b_i}{n} \right| \qquad (7)$$

(五) 關於MATLB

MATLAB 是 MATrix LABoratory（矩陣實驗室）的縮寫，是一款由美國 The MathWorks 公司出品的商業數學軟體。MATLAB 是一種用於演算法開發、資料視覺化、資料分析以及數值計算的進階技術計算語言和互動式環境。除了矩陣運算、繪製函數/資料圖像等常用功能外。我們使用 MATLAB 中的 ode45 解三個非線性常微分方程，並利用其強大繪製圖像功能實現與蔡氏電路等效模型的分析。

儘管 MATLAB 主要用於數值運算，但因為此軟體操作簡單且容易理解又可接受 Tektronix 示波器輸出 excel 格式的資料，所以正好可以利用其設計、模擬的功能來進行研究並與實際的蔡氏電路做比對。

伍、 研究結果

一、「蔡氏電路」輸出電壓YT及XY圖

把運算放大器、電阻、電感及電容接好來實現蔡氏電路，打開電源，首先透過數位儲存示波器(1052B)觀察電壓對時間的圖，如圖 5-1-1 所示，其中，V_1 及 V_2 的振盪頻率約為 3kHz (~ $\frac{1}{2\pi\sqrt{L\times(C_1+C_2)}}$)及 550 Hz ，形成雙振盪的混沌現象蔡氏電路的操作是需要適當的選擇電子元件的值，透過可變電阻 R_p 及 R_1 適當的調整可出現混沌振盪狀態的雙渦旋"double scroll" 吸引子，圖 5-1-2 顯示出圖 5-1-1 所對應之 XY 圖。

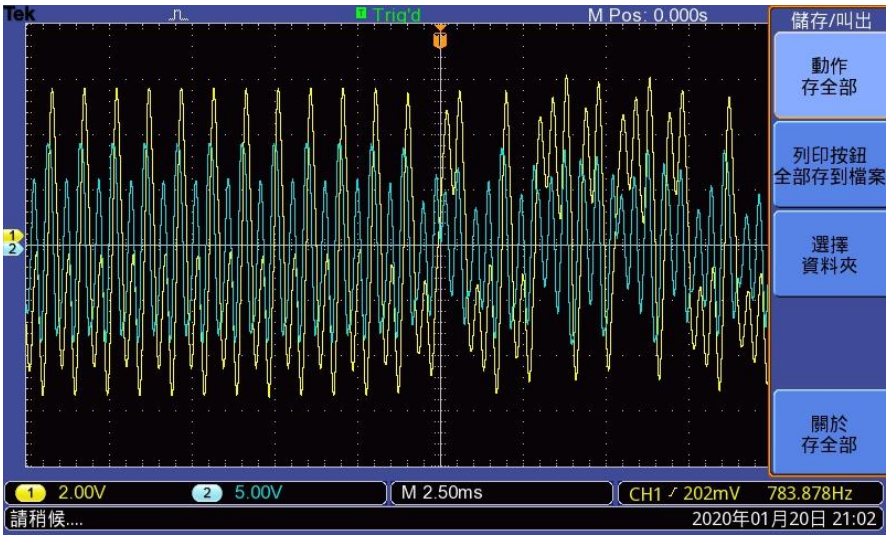


圖 5-1-1 在示波器上 V_1(藍)及 V_2(黃)電壓對時間波形圖

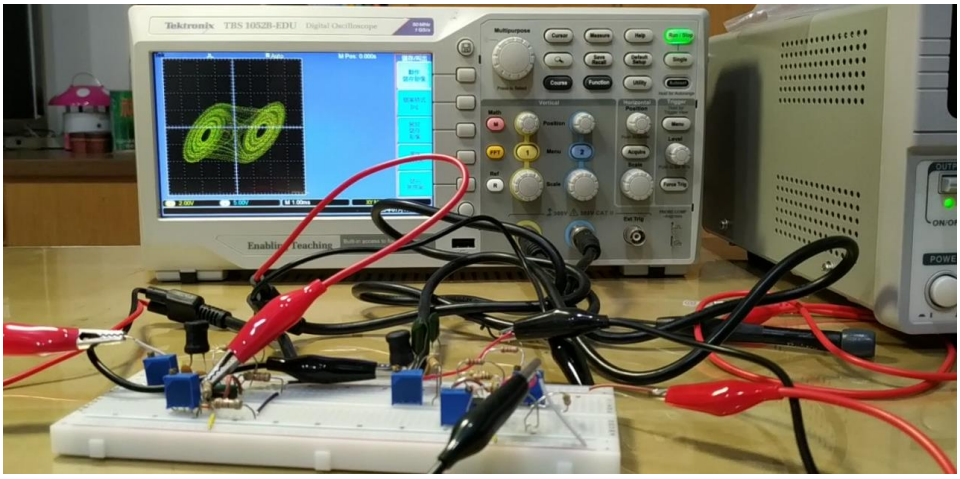


圖 5-1-2 在示波器上 V_1 及 V_2 之 XY 圖

二、用「XY」軸建立二位元碼輸出判準

圖 5-2-1 為示波器及 MATLAB 等效電路之雙渦旋吸引子圖的比較， V_1 及 V_2 是游走於 XY 平面的四個象限，透過不同的 R_p 設定，由左至右分別是 1300Ω、1600 Ω及 1800 Ω，此時蔡氏電路會處於「單純振盪」、「雙渦旋吸引子」及「陣發混沌」，藉由此圖可用於確認 MATLAB 等效電路及麵包板電路操作的一致性，除此之外，也瞭解蔡氏電路的詳細行為。

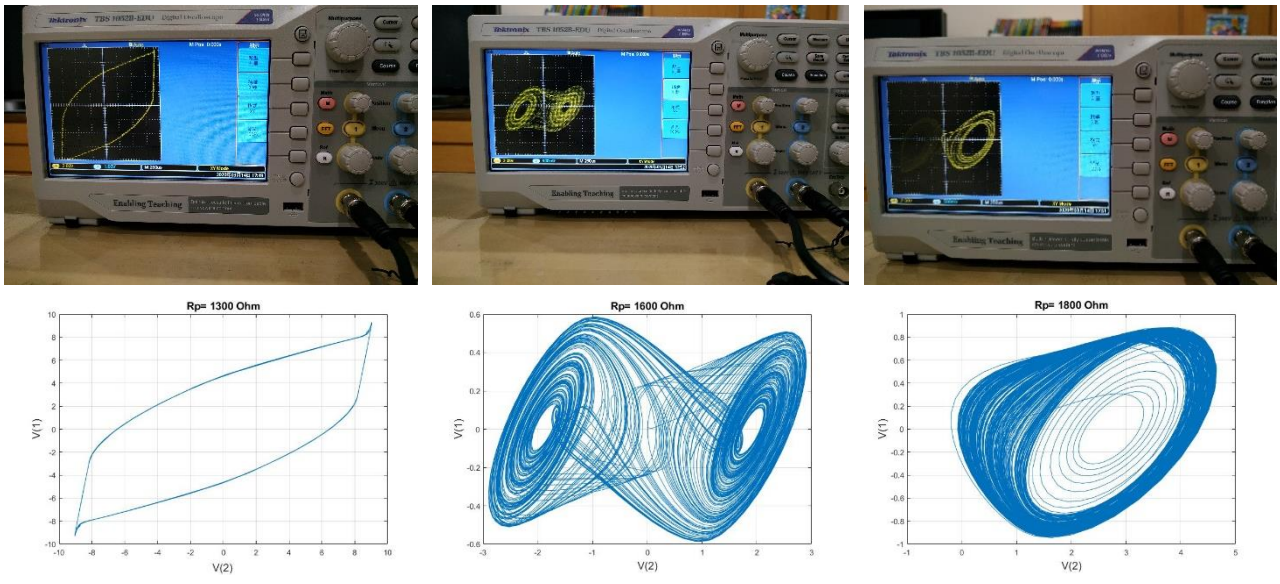


圖 5-2-1 示波器及 MATLAB 等效電路之 V_1 及 V_2 的 XY 圖 (R_p=1300Ω、1600 Ω、1800 Ω)

在圖 5-2-2 中，我們可直接取的正負值(Sign Function)，在透過 exclusive-NOR(XNOR)的操作，基

本上，XNOR 為二進位的一 bit 乘法器，實現上相當簡單，如此我們就可產生如圖 5-2-1 所示 code 0 或 1 之數位密碼。蔡氏電路所產生的波形可以透過二極體所組成的橋式乘法器(圖 5-2-2)來產生 0 與 1 的密鑰，而所產生的 0 跟 1 的波形再透過示波器的擷取後，我們可以進一步來做數據的分析。

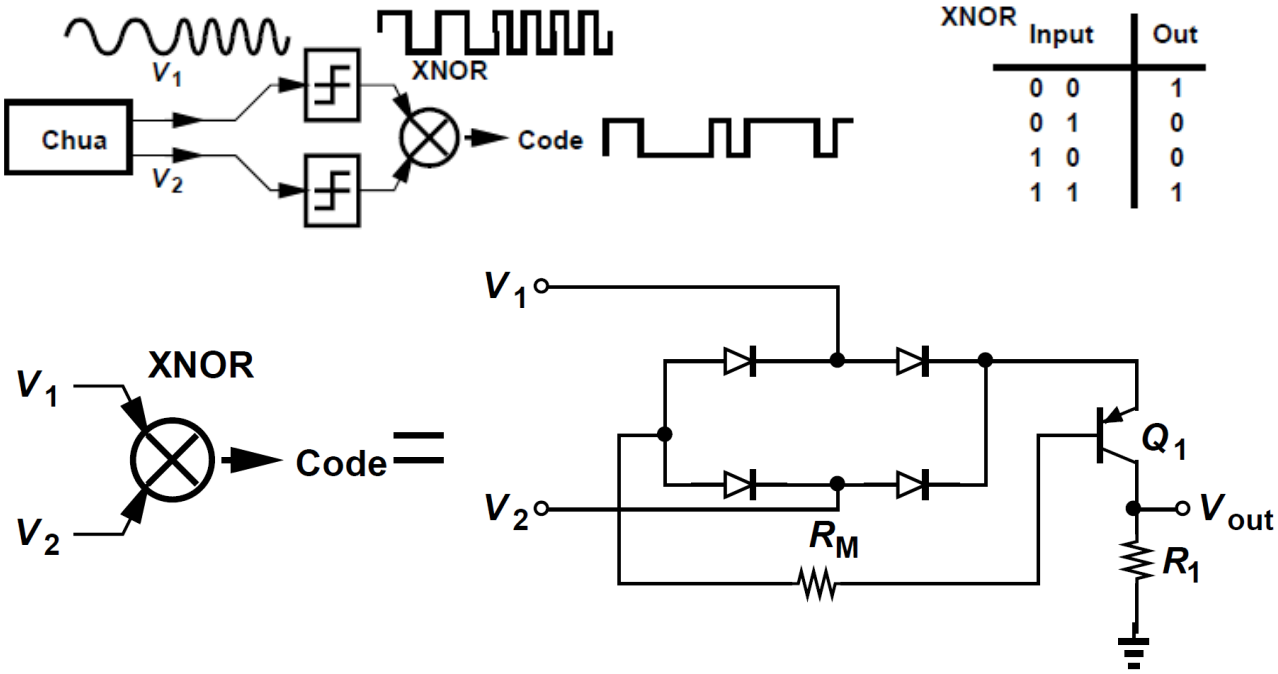


圖 5-2-2 蔡氏電路之密鑰產生器

三、四渦旋混沌電路輸出電壓YT及XY圖

從基本蔡氏電路的經驗，並不再使用電感，把運算放大器、電阻及電容接好來實現四渦旋混沌電路，同樣地，透過數位儲存示波器觀察電壓對時間的圖，如圖 5-3-1 所示，其中，觀察 V_1 及 V_3 的振盪，形成四渦旋振盪的混沌現象，圖 5-3-2 顯示出圖 5-3-1 所對應之 XY 圖。

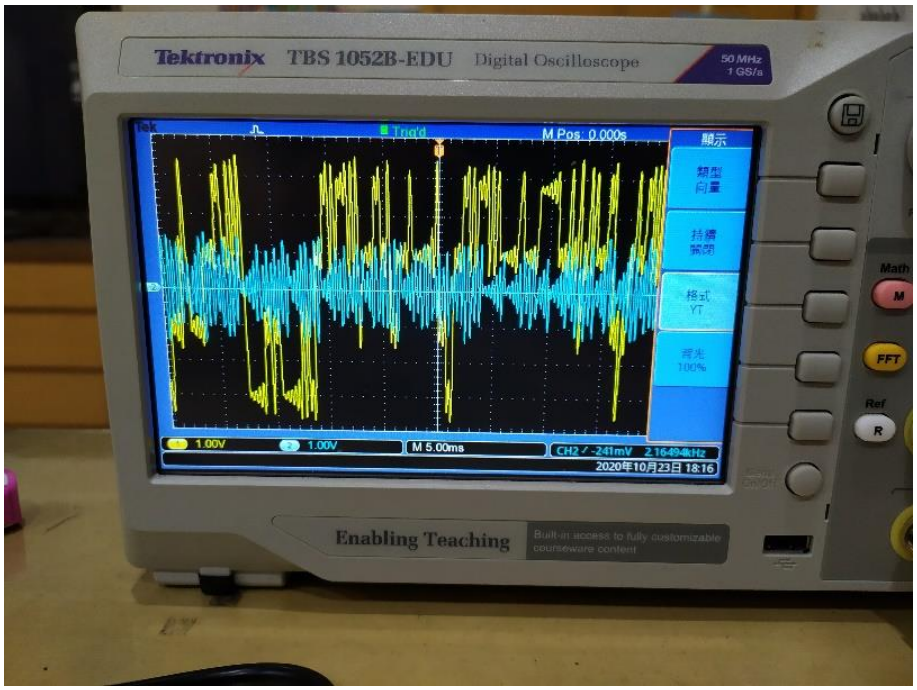


圖 5-3-1 在示波器上 V_1(黃)及 V_3(藍)電壓對時間波形圖

我也透過 MATLAB 去解出三個非線性微分方程並得到圖 5-3-3 等效電路，呈現出四渦漩吸引子圖，由 V_1 及 V_3 是游走於 XY 平面的四個象限，此圖可用於確認 MATLAB 等效電路及萬用電路板的實際電路操作的一致性。

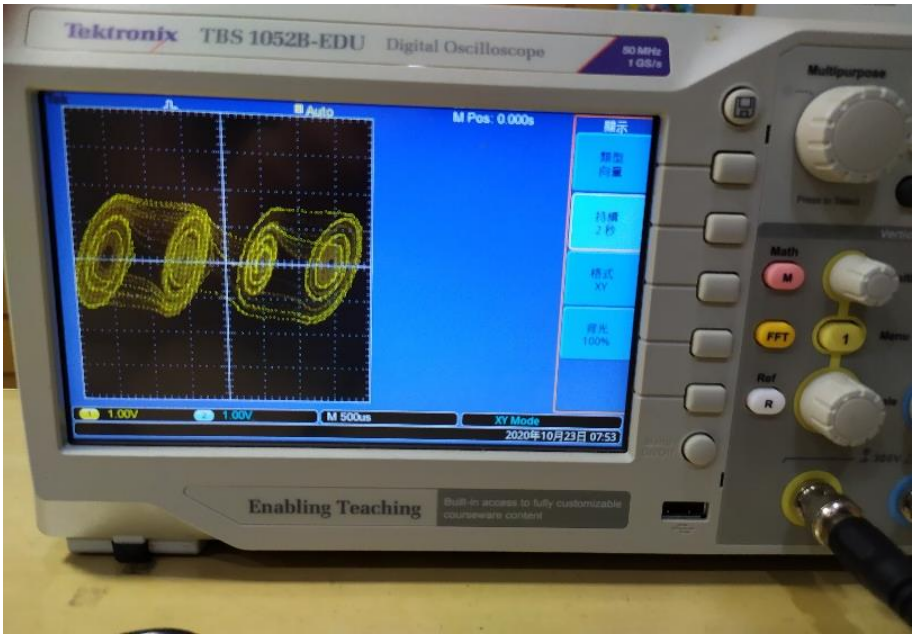


圖 5-3-2 在示波器上 V_1 及 V_2 之 XY 圖

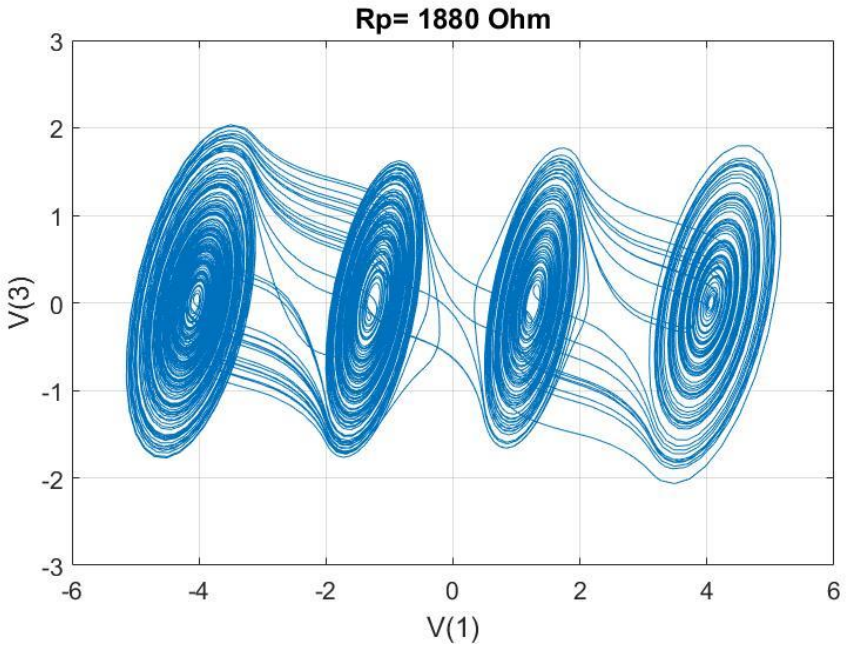
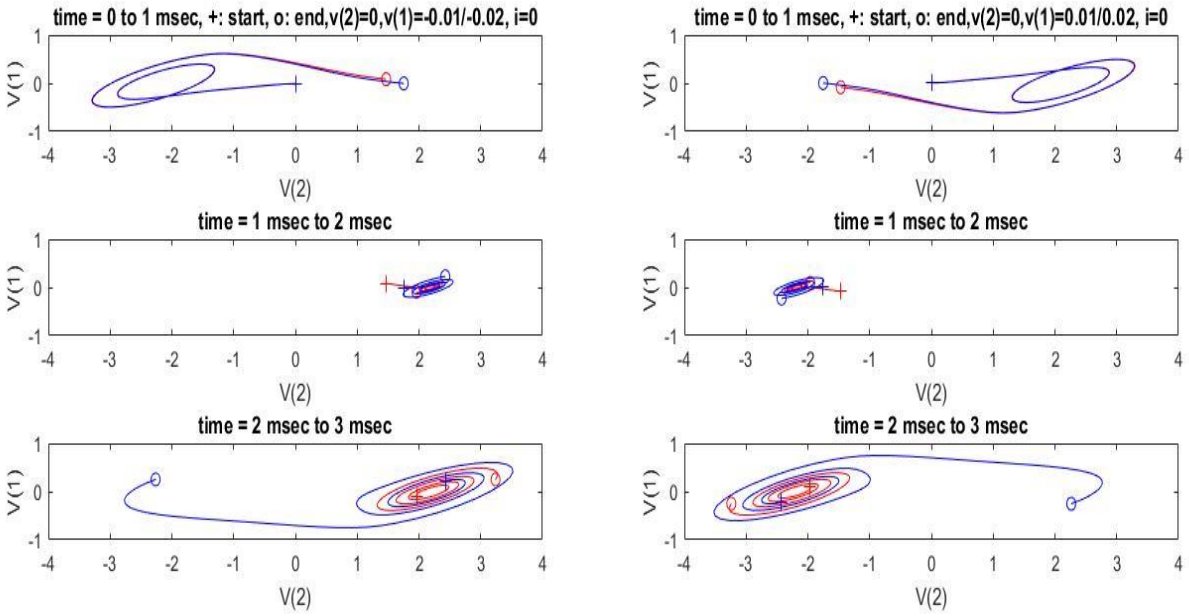


圖 5-3-3 MATLAB 等效電路之四渦漩吸引子圖

四、蝴蝶效應模擬圖

在圖 5-4-1 中，於 MATLAB 模擬中，藉由設定 V_1 的初始條件 +-0.1/0.2(紅色/藍色)及+-0.01/0.02(紅色/藍色)可明顯看到經過數個 msec 的時間後，V_1 及 V_2 會有非常不一樣的軌跡，由表 5-4-1 可看出明顯的蝴蝶效應。



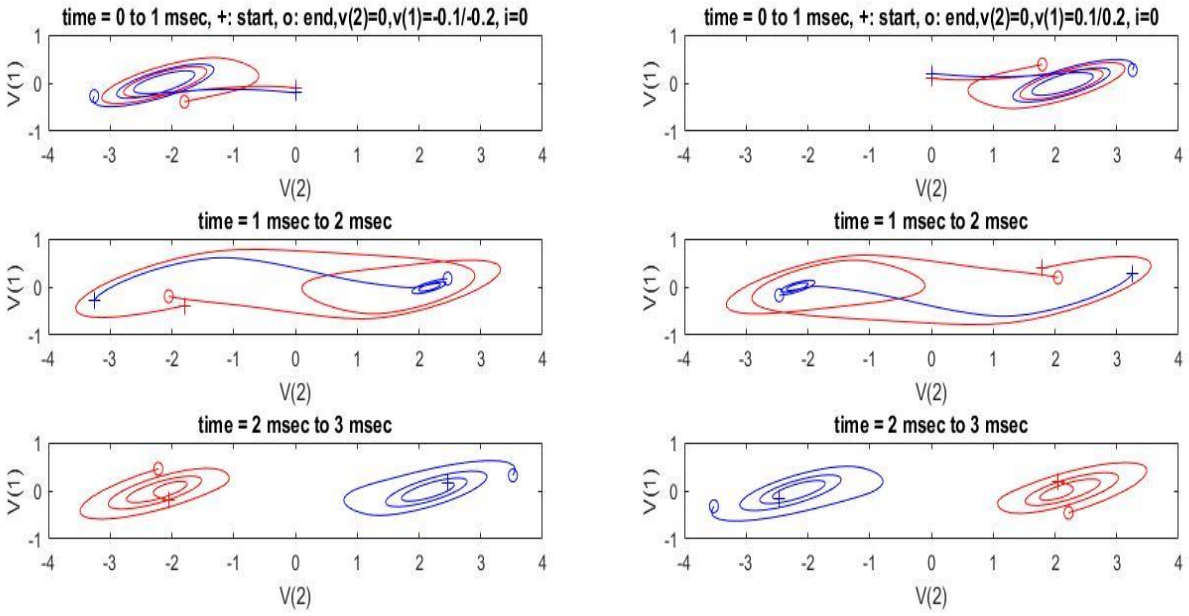


圖 5-4-1 蔡氏電路在不同初始條件下之 V_1 及 V_2 軌跡圖

表 5-4-1 不同初始條件下，V_1 及 V_2 在 1ms, 2ms 及 3ms 之電壓值

時間/初始條件 V_1 及 V_2	0.1/0.2 (V_1)	-0.1/-0.2 (V_1)	0.01/0.02 (V_1)	-0.01/-0.02 (V_1)
0	(0.1,0) / (0.2,0)	(-0.1,0) / (-0.2,0)	(0.01,0) / (0.02,0)	(-0.01,0) / (-0.02,0)
1msec	(0.3886, 1.796) / (0.2721, 3.2579)	(-0.3886, -1.796) / (-0.2721, -3.2579)	(-0.0821, -1.4692)/ (0.0035, -1.7532)	(0.0821, 1.4692)/ (-0.0035, 1.7532)
2msec	(0.1951, 2.0507)/ (-0.1722, -2.4644)	(-0.1951, -2.0507)/ (0.1722, 2.4644)	(0.0923, -1.9616)/ (-0..2307, -2.4267)	(-0.0923, 1.9616)/ (0..2307, 2.4267)
3msec	(-0.4574, 2.2202)/ (-0.3212,-3.5212)	(0.4574, -2.2202)/ (0.3212,3.5212)	(-0.2507, -3.2402)/ (-0.2516, 2.2636)	(0.2507, 3.2402)/ (0.2516, -2.2636)

從上述四個實驗我們可以看到蔡氏電路在不同的初始條件之下經過一段時間的運作之後，各個節點電壓會有截然不同的表現，初始條件差異越小，需要較長的時間才有差異化的表現， 另外根據初始值的正負差異這個電路也會有如「鏡射般」的反應， 事實上從節點電壓的軌跡圖我們也可以看到此電路本質為一偶函數。

我們也針對是四渦漩的混沌電路的蝴蝶效應作分析，如圖 5-4-2 所示，跟最基本型的二渦漩才是電路比較具有類似的行為如對稱性等，但因為具有四個振盪的型態，所以蝴蝶現象不可預測性的程度更加複雜。

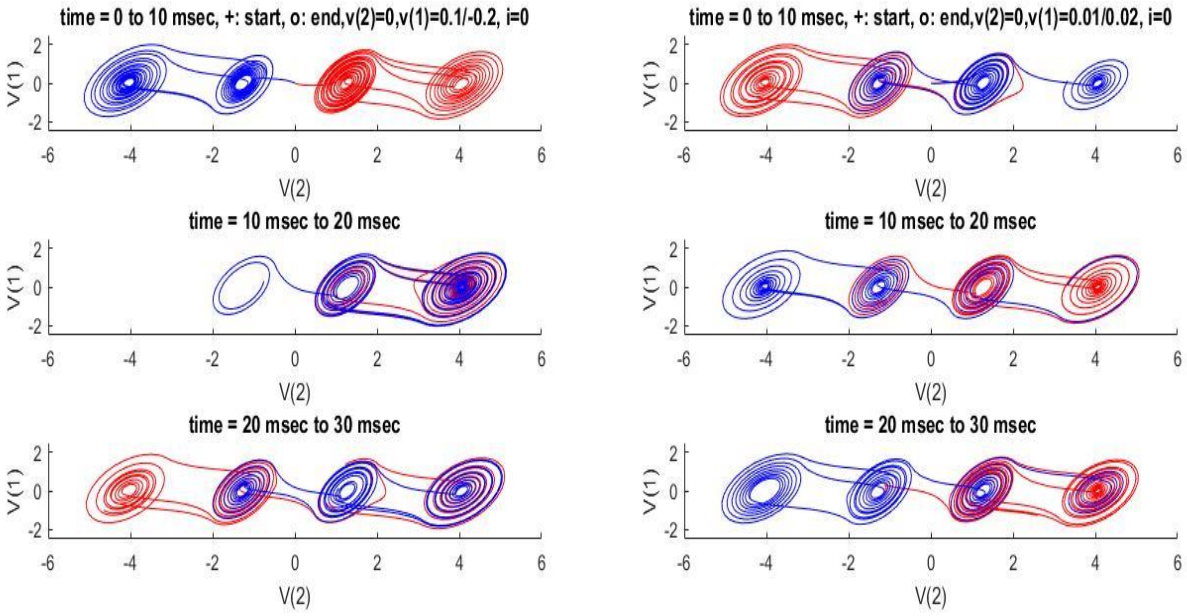


圖 5-4-2 四渦漩混沌電路在不同初始條件下之 V_1 及 V_2 軌跡圖

下列也針對蔡氏電路及四渦漩混沌電路在不同的初始條件所產生的兩個串列數列，對他們的正規的平均值及兩者之間的交叉相關函數繪製圖表，雖然電路表面是完全一模一樣的但經過長時間的運作彼此之間的關係是完全獨立，在長時間操作下，交叉相關函數會趨近零。

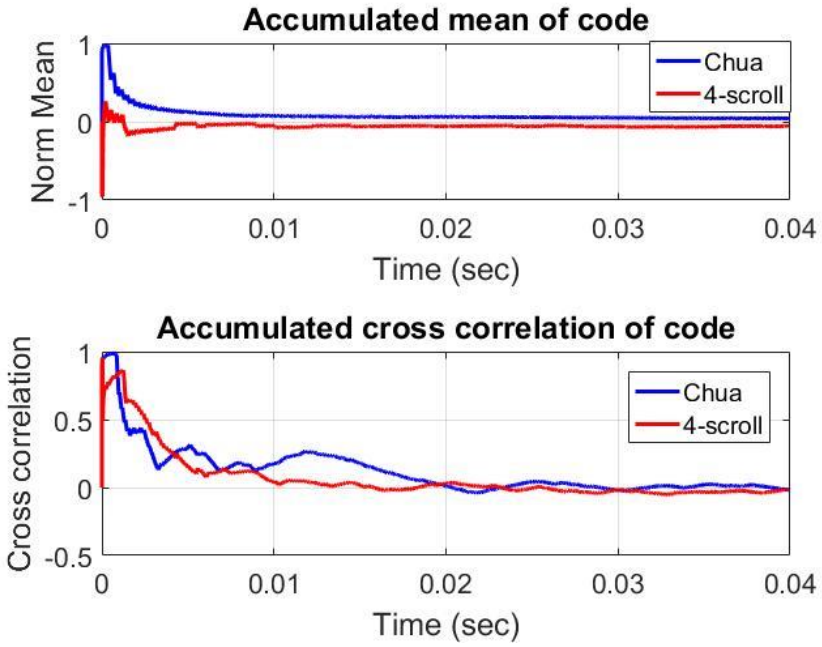


圖 5-4-3 四渦漩混沌電路平均值及平均值及兩者之間的交叉相關函數 vs. 時間

如圖 5-4-3 所示，針對蔡氏電路及四渦漩混沌電路所輸出的資料進行評估，兩者的隨機性相當的不錯，約略在 5 msec 內左右可達到 0 跟 1 的平衡輸出，而在交互相關函數的資料分析當中，我們也發現只要時間夠長，兩者的相關係數也會趨於零，不過四渦漩混沌電路的電路多變性可在 10msec 趨近於零而蔡氏電路需要 20msec 達成零相關係數，這驗證了蝴蝶效應的存在於蔡氏電路及四渦漩混沌電路當中。

不過，要製造不同的初始條件在實際的使用情形上會有一定的困難度， 因此單單只靠這種初始條件不一樣而產生密碼，其可靠度可能不高。因此，我們需加入物理不可複製的特性去提高此電路的安全性。

五、物理不可複製函數輸出圖

我們將兩個完全相同的蔡氏電路，具有同樣的運算放大器電阻電容及電感，實現在同一塊麵包板上面，如圖 5-5-1 所示， 原來在同一個蔡氏電路時下的 XY 圖是一個有規則的雙渦旋吸引子的圖(圖 5-1-2)，但是我們把其中一個電壓跨到另外一個蔡氏電路之後，其架構連接如圖 5-5-2，原先的 XY 圖會變得非常沒有規則，如同自然界所產生的雜訊，此種使電路更紊亂的操作模式提供一個更亂的數列產生器，如同蝴蝶效應一般，在蔡氏電路的某一個元件當中我們注入微小的一個差別，經過一段時間的運作之後電路本身會產生一個很大的差異化，並且隨著時間越久，兩者看似相同的電路,但本質的些微差距也會使此電路有非常不一樣的表現。

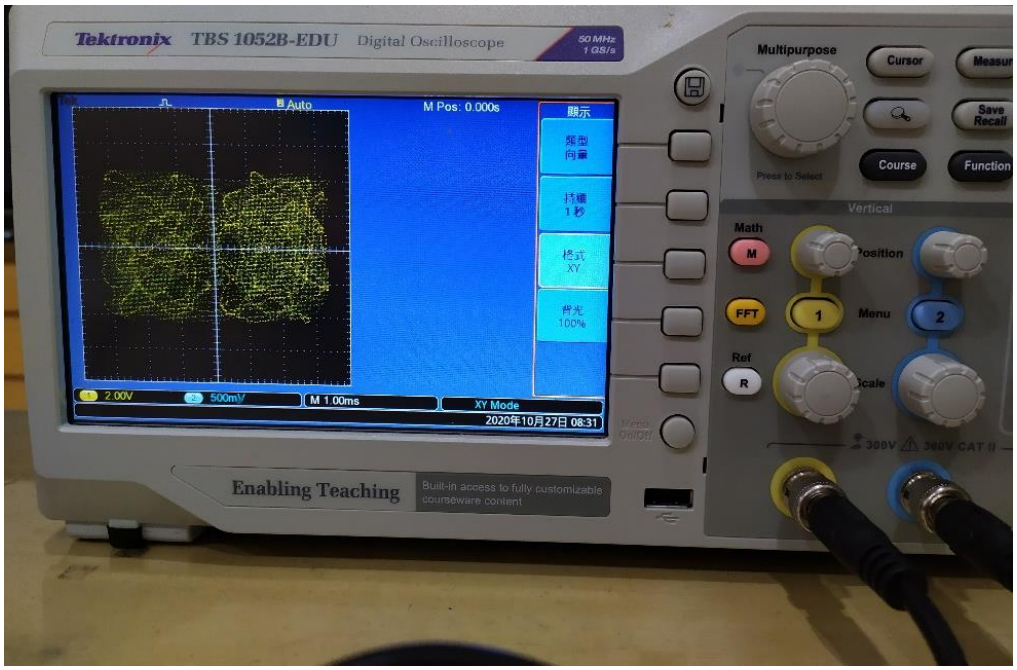


圖 5-5-1 在示波器上 V_1 及 V_2 之 XY 圖

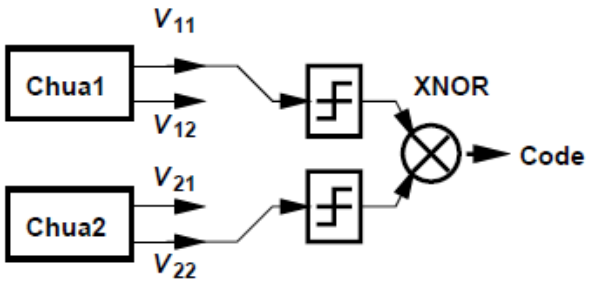


圖 5-5-2 蔡氏電路結合物理不可複製函數 (Chua1, Chua2)

圖 5-5-3 為 MATLAB 等效電路之雙蔡氏電路 XY 圖，由 V_1 及 V_2 是游走於 XY 平面的四個象限，此圖可用於確認 MATLAB 等效電路及圖 5-5-1 麵包板電路操作的一致性。

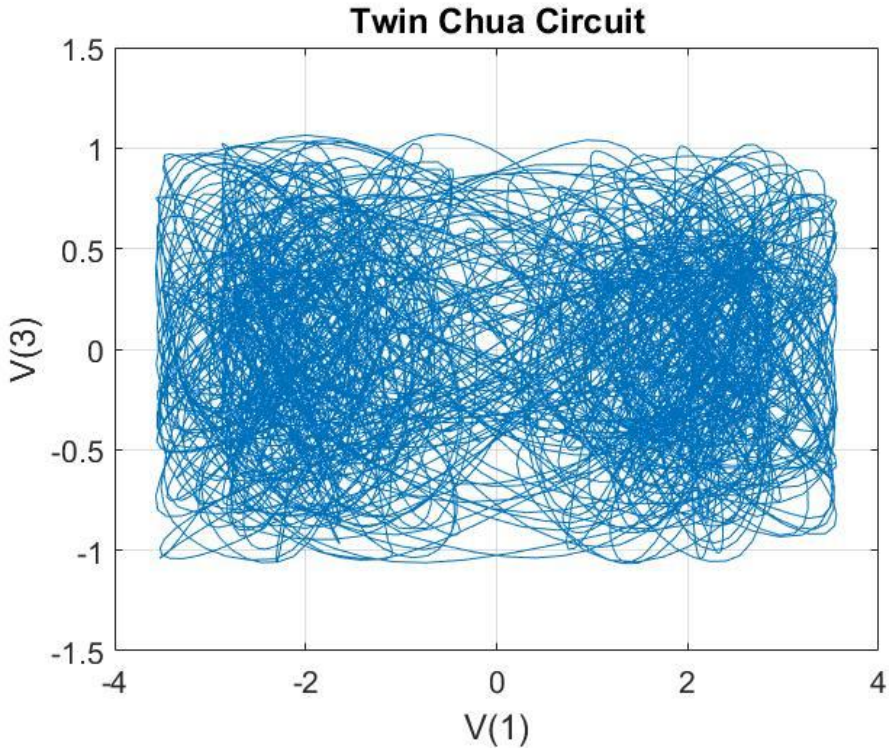


圖 5-5-3 MATLAB 中蔡氏電路結合物理不可複製函數之 V_1 及 V_2 之 XY 圖

評估蔡氏電路再加上物理不可複製函數，可針對對隨機性及獨特性進行分析。首先類蝴蝶效應也出現，如圖 5-5-4 及表 5-5-1 所示，蔡氏電路對電子元件之值的變異性也是相當敏感。

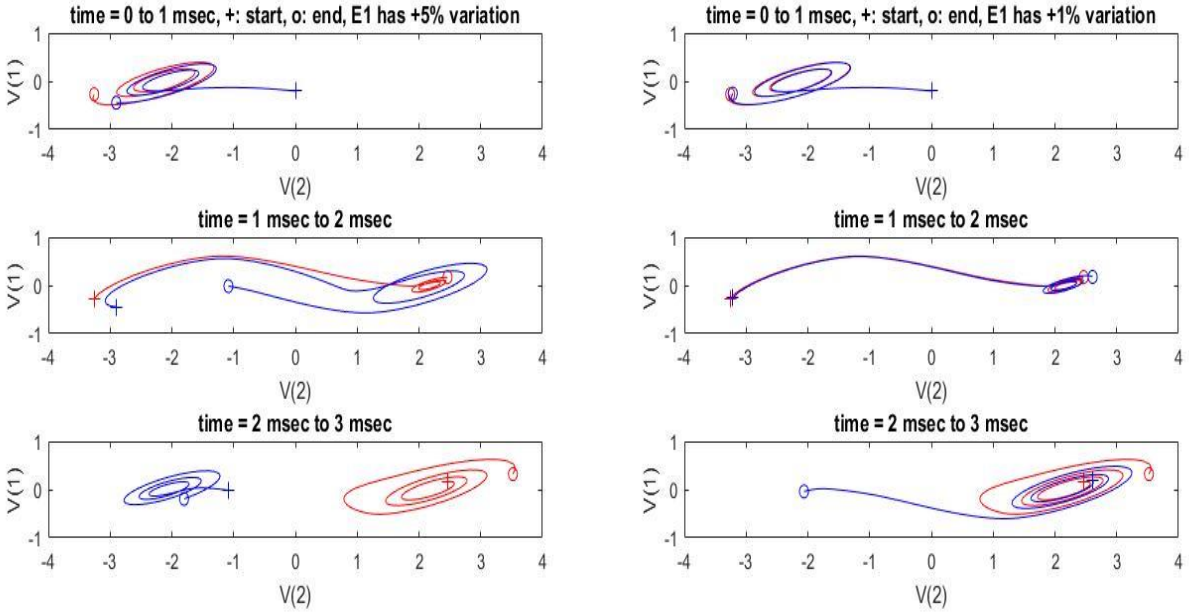


圖 5-5-4 有 PUF 且相同初始條件下之 V_1 及 V_2 軌跡圖

表 5-5-1 有 PUF 且相同初始條件下，V1 及 V2 在 1ms, 2ms 及 3ms 之電壓值

時間/E1 變異量	5%	1%
0	(-0.2,0) / (-0.2,0)	(-0.2,0) / (-0.2,0)
1msec	(-0.2721, -3.2579) / (-0.4465, -2.9013)	(-0.2721, -3.2579) / (-0.2568, -3.2156)
2msec	(0.1722, 2.4644)/ (-0.0148, -1.0848)	(0.1722, 2.4644)/ (2.4644, 2.6112)
3msec	(0.3212,3.5212)/ (-0.1928,-1.8020)	(0.3212,3.5212)/ (3.5212,-2.0631)

針對所輸出的資料其隨機性相當的不錯，可從圖 5-5-5 看出，約略在 5 msec 左右可達到 0 跟 1 的平衡輸出，利用物理不可複製的特性而產生的密鑰可以在比較短的時間內達成可使用的條件。而在交互相關函數的資料分析當中，沒有 PUF，其相關係數也會不太會趨於零，這意味的其他使用者可以比較容易用反向工程找到此密碼，而在有 PUF 的情況之下, 其相關係數不僅會趨近於零而且收斂的速度也相當的快，所需的時間大約是 30 msec。我們在這邊要特別注意一下，電路所需收斂的時間意味著我們需要消耗多少的能量以達到電路可用的狀況，在極低耗能的物聯網裝置當中這樣的快速收斂時間將是決定此設計的關鍵。

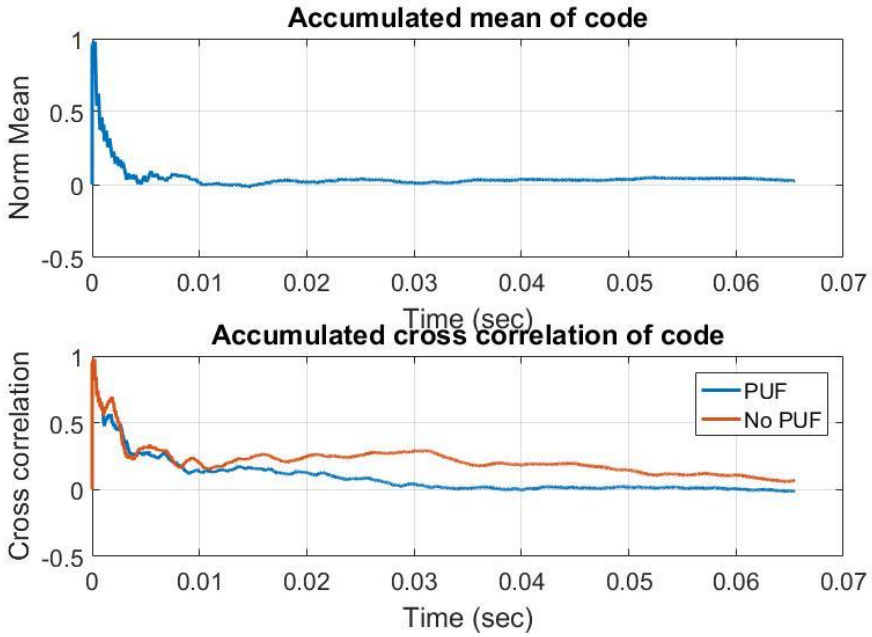


圖 5-5-5 平均值及有無 PUF 交叉相關函數 vs. 時間 (藍: 有 PUF，紅: 無 PUF)

在物理不可複製函數中我們也針對四渦漩的混沌電路分析，我們把其中一個電壓跨到另

外一個四渦漩的混沌電路之後，透過示波器波形(圖 5-5-6)及 MATLAB 等效電路(圖 5-5-7)，所產生出來密鑰的相關性及收斂性，很明顯的根據數據分析的結果，具有四個渦漩的混沌電路其必要產生的收斂性及紊亂性相對於二個渦漩的基本蔡氏電路有更複雜的行為表現，因此透過更進一步複雜的電路行為可把密鑰的複雜度及強度進一步的加強。

另外，可從圖 5-5-7 看出，同樣的在 5 msec 左右可達到 0 跟 1 的平衡輸出，而在交互相關函數的資料分析當中，四渦漩的混沌電路結合物理不可複製的特性而產生的密鑰可以在更短的時間(30ms → 20ms)內達成可使用的條件。極低耗能的裝置當中更快速收斂時間將是可達成更低功耗的關鍵。

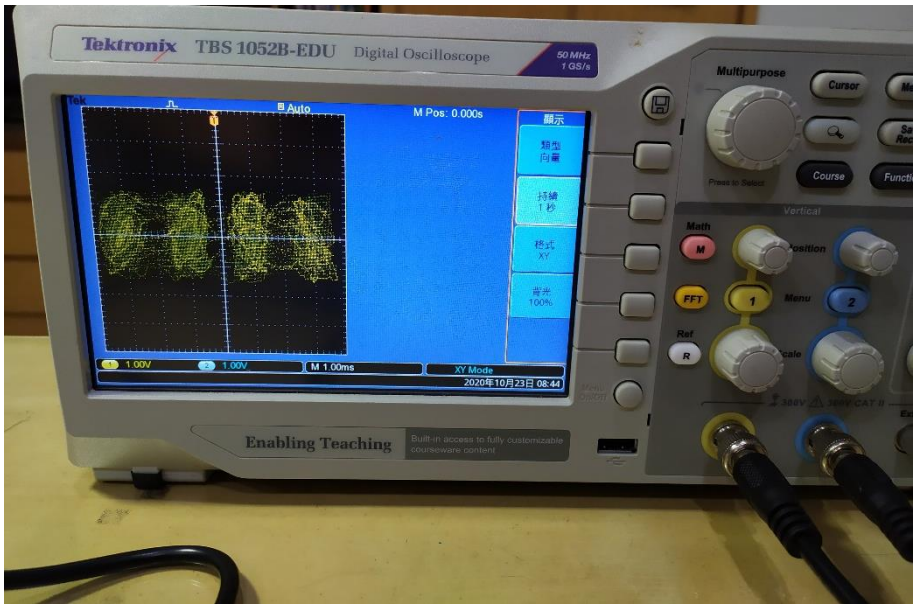


圖 5-5-6 在示波器上四渦漩的混沌電路 V_1 及 V_3 之 XY 圖

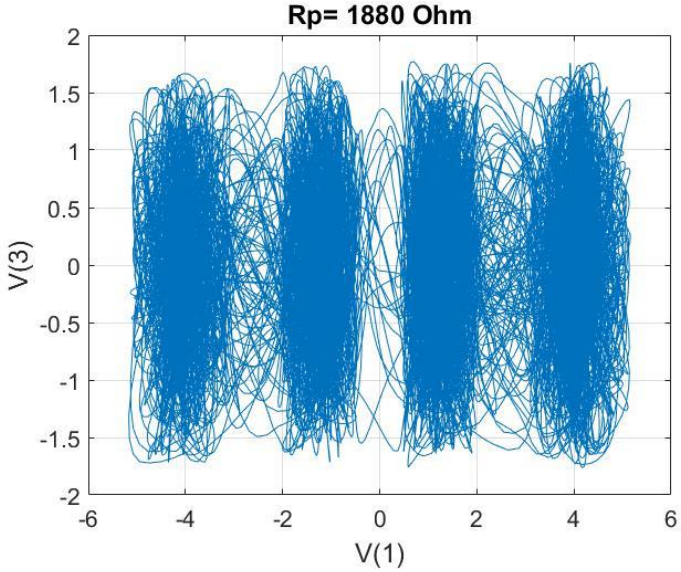


圖 5-5-7 MATLAB 四渦漩混沌電路結合物理不可複製函數之 V_1 及 V_3 之 XY 圖

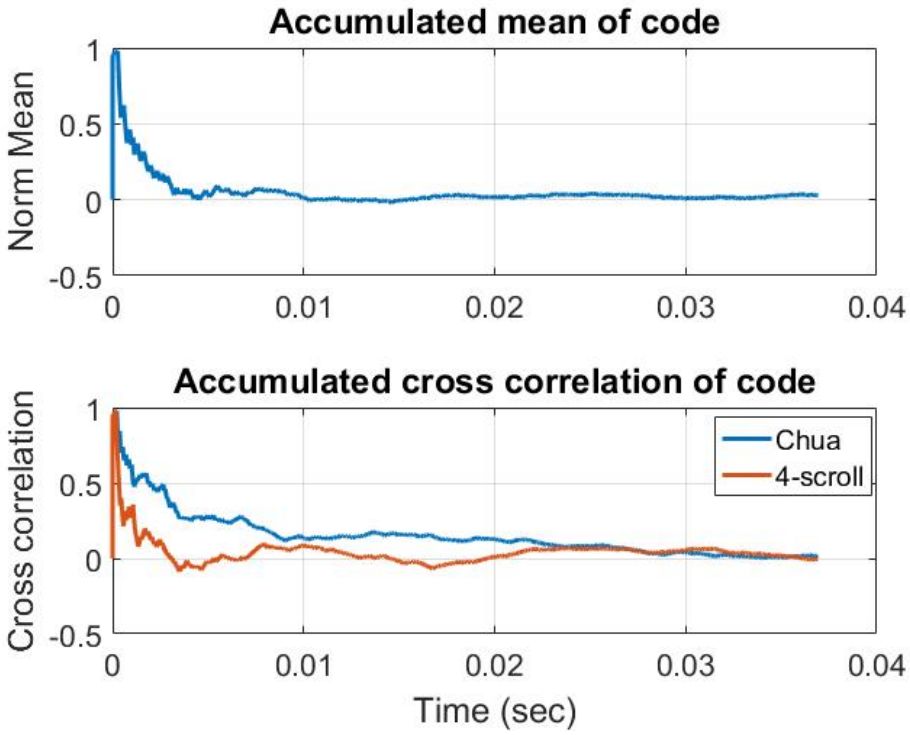


圖 5-5-8 平均值及蔡氏電路及四渦旋混沌電路 PUF 交叉相關函數 vs. 時間
(藍: 蔡氏電路，紅: 四渦旋混沌電路)

陸、 討論

一. 電路板的方式實現蔡氏電路及四渦旋混沌電路並觀察到期混沌的現象，紊亂的操作模式可以用來產生隨機的密碼。

二. 混沌電路對其初始條件極度敏感，我們可透過不同的初始條件，觀察到整個電路變化的結果。

三. 在實際的操作模式要創立不同的操作模式有其困難度， 加入物理不可複製函數的功能， 我們可以達到這些 PUF 必要的隨機性及獨特性。

四. 透過實驗及模擬的結果，再加上數據的分析我們觀察到， 1）電路震盪的頻率, 2）電路需要收斂的操作時間。透過 1)跟 2)的分析我們可歸納出， 這個蔡氏電路/四渦旋混沌電路需要大約數十個到百的操作週期才可達到極度的混沌狀態。

五. 我們並且發現到透過物理的不可複製函數功能可加速電路的收斂， 這對於需要極低功耗物聯網電路是相當有用的特性。

六. 四個渦旋的混沌電路有更複雜的電路行為表現，可把密鑰的複雜度及強度進一步的加強。

七. 傳統上，如圖 6-1 所示， PUF 的實現必須透過 N 個 (N 為數十) 看似相同的電路，然後透過不同的輸入挑戰，進而得到 2 的 N 次方不同的結果。這種方法非常的消耗硬體成本， 而在圖 6-2 中，本研究中我們所提出利用兩個看似相同的蔡氏電路，縱使在同樣的輸入條件之下也會有完全不同的反應，此種方法不減大大減少數十倍硬體的成本，而且也可產生相對安全的通訊密鑰。

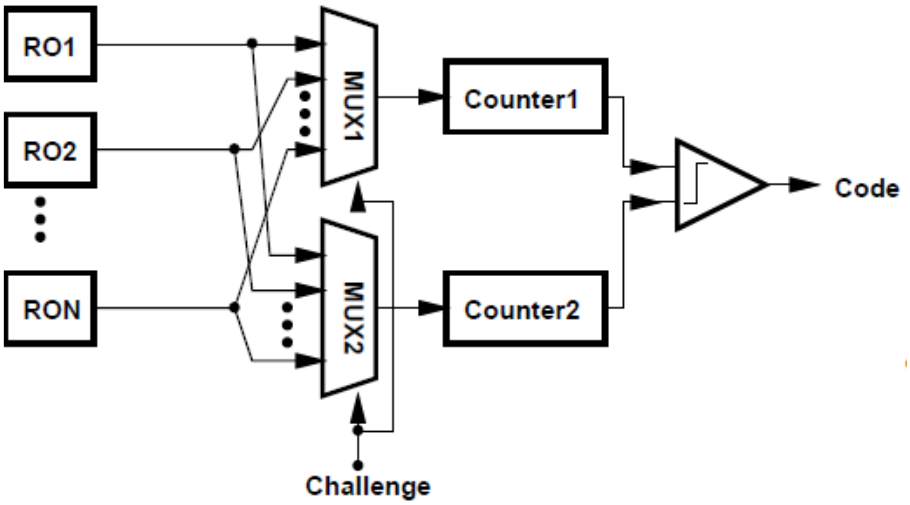


圖 6-1 傳統利用振盪器組成之 PUF

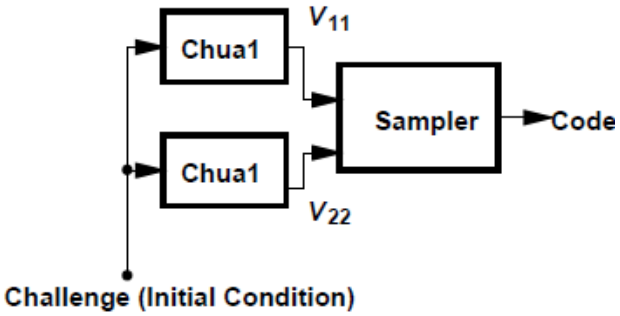


圖 6-2 本研究之蔡氏電路結合物理不可複製函數 PUF

柒、 結論

在本研究當中， 我們探討在數十年前已發明的蔡氏電路，透過實作並建立等效的電路模擬模型， 我們可以利用在此電路紊亂的操作，達成硬體安全密鑰的產生，相較於傳統架構，可省數十倍的成本。在研究過程當中， 也發覺到蔡氏電路是一個非線性的系統， 一些較基本的數學及物理分析工具並不足以描述其行為，不管在實驗和模擬當中，都發現此電路操作的多樣性，

畢竟對初始條件的敏感性，電路元件值的敏感性，甚至於本研究提出的物理不可複製函數技術的結合，除此之外，我進一步把蔡氏電路由雙渦漩拓展為四渦漩，把密鑰的混亂性及非相關性進一步的提升。期望以此研究為開端，未來希望對更複雜的混沌電路及產生密鑰的技術再做更進一步的研究。

捌、 參考資料及其他

[1] 維基百科: 蔡氏電路

[2] 維基百科: 混沌理論

[3] Chua's circuit diagrams, equations, simlulations and how to ... http://www.chuacircuits.com/ https:// www.chuacircuits.com

[4] N. Wang, et al.," Generating Multi-Scroll Chua's Attractors via Simplified Piecewise-Linear Chua's Diode," IEEE TCAS1, vol. 66, no. 12, pp. 4767-4779 Dec. 2019.

[5] 物理反複製技術 - Digitimes https://www.digitimes.com.tw/tw/dt/n/shwnws.asp?id=0000416206_tml3tfqqlfvxu57ov2iq8

[6] 陳彥霖(2018)。國立中興大學資訊科學與工程學系碩士學位論文 "強健的物理不可複製函式之設計"

【評語】160024

本研究設計兩個看似一樣的「二渦漩狀」蔡氏電路交互作用的新電路，並利用兩電路中元件在製成中難以控制的變異而產生渾沌。此現象類似蝴蝶效應，由很小的差異而產生整個電路表現不可預測性及混亂程度。此電路可用以製造出作為硬體安全實現的密鑰生成器。本研究有其新穎性，是相當不錯的作品。但是否與不可複制函數有關，還需要紮實的證據。