動態金鑰產生器及其應用

樹德科技大學電腦與通訊系

摘要

現今社會人們對於資料的私密性相當重視，因此當資料進行兩地傳遞時，如何提昇及確保其通訊內容的保密性，便成為相當重要的課題。本作品利用混沌同步理論，產生隨機之動態金鑰，並進一步使用盛群所提供之 HT46R24、應用此動態金鑰並結合 RSA 加解密原理，來設計並實現保密通訊系統，此系統不但具有相當高的保密功能，且和先前以 VCO (壓控振盪器)為主的調變技術[1]比較，更具其穩定性。而本作品為了解決傳接兩端 AD 轉換以及混沌訊號同步的誤差，設計了臨界值緩衝區，同時也進一步設計 SRAM 分頁資料處理的功能，用以實現本作品之語音**即時**加密及傳送。此作品之成果，充分展現，理論及實作的結合性，對於混沌系統訊號在數位保密上的應用上，有一定程度上的貢獻及參考價值。同時顯而易見的，本結果也可很容易地擴展應用於任何數位訊號的加解密。

1. 前言

自從氣象學家 Lorenz 提出蝴蝶效應(Butterfly Effect)，論述某非線性系統(氣象系統)即使初期條件僅有微小差距，卻可能造成未來結果巨大的變化及差異，這正說明了混沌系統對於初始條件敏感以及不可預測等特性。然而近年來，混沌控制理論的崛起，不但開啟了科技的新視界，再加上混沌訊號特有的不可預測及具有寬廣頻譜的特性，更使得混沌系統成為設計保密通訊系統時的新寵兒。因此，本作品結合混沌理論及 RSA 加解密運算的設計理念，利用混沌訊號直觀上像雜訊，且難以預測的特性，來設計動態金鑰產生器，並用來做為隨機選擇 r 及 PK 值的依據， 提供資料更安全及更可靠的加解密模式；而本作品不僅著重於混沌系統理論和 RSA 加密原理的結合及實現，更提出 SRAM 分頁資料處理功能來應用在本作品中，使本作品能達成語音的即時傳送功能。

本作品所使用的 IC 為盛群所提供之 HT46R24，其主要工作在於處理 RSA 大量的冪次與取餘數運算、A/D 轉換以及傳送等功能，所以盛群 HT46R24 為本作品中最重要的核心。

2. 工作原理

根據文獻[1]可得知，使用混沌訊號來調控 VCO(壓控振盪器)做為加解密之依據，其中最大的問題就是由於 VCO 對於微小電壓值極為敏感，所以主-僕混沌系統之間的微小誤差，就可能造成資料解密錯誤，所以本作品提出新的加密方法，利用混沌訊號作為一種隨機選擇 r 模組以及 PK 值的依據，將系統所產生之 Random Key 做 RSA 加密運算，其加密原理將在稍後詳述，故本作品中盛群 MCU 將負責大量的 RSA 加解密運算、AD 取樣以及傳輸等功能，而加解密必需建構在主僕混沌系統同步之上，因此，此作品的實現包含了兩大重要部分: (1) 動態金鑰產生器-主僕混沌系統同步控制原理 (2) RSA 加解密機制，以下就這兩大部分加以詳述：

2.1 動態金鑰產生器-主僕混沌系統同步控制原理：

要利用混沌系統於傳送和接收端，產生一動態隨機之金鑰，並應用在通訊保密上最重要的一點就是必需使傳送端(Master)與接收端(Slave)之混沌訊號確實達到同步；然而若要使一個複雜的動態的非線性系統達到雙端同步，一個好的控制器是功不可沒的，因此本作品運用工程中使用最為廣泛的控制器:比例-積分控制器(Proportional-Integral, PI)簡稱為 PI 控制器，來達到混沌系統同步的要求。由於 PI 控制器具有簡單的結構，成本低廉與可接受的穩定控制結果，於是成為工業控制上最常用的主要控制器，其中 PI 控制器工作原理如圖 1 所示：

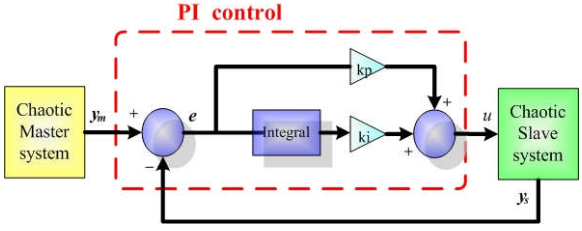

圖 1： PI 控制器原理圖

圖 1 中左方主混沌系統(Chaotic Master system)傳送單一狀態 y_m 經由公共通道至 PI 控制器，此時控制器會將訊號 y_m 與僕混沌系統(Chaotic Slave system)所產生的訊號 y_s 相減形成動態誤差 e，並將誤差 e 乘上 kp 倍與 e 的積分乘上 ki 倍相加後，回授至僕混沌系統，如此經由適當的選擇 kp 值與 ki 值，可使誤差 e 會趨近於 0，此時主僕混沌系統即達成雙端同步。然而如何設計 PI 控制器中最佳的 kp 值與 ki 值，使得主僕混沌系統得以同步，也是設計控制器重要的一環，除了傳統的經驗法則外，本作品特別運用進化演算法(EP)[2-4]來求得 PI 控制器所需之增益參數，而 EP 演算法概念之流程圖如圖 2 所示：

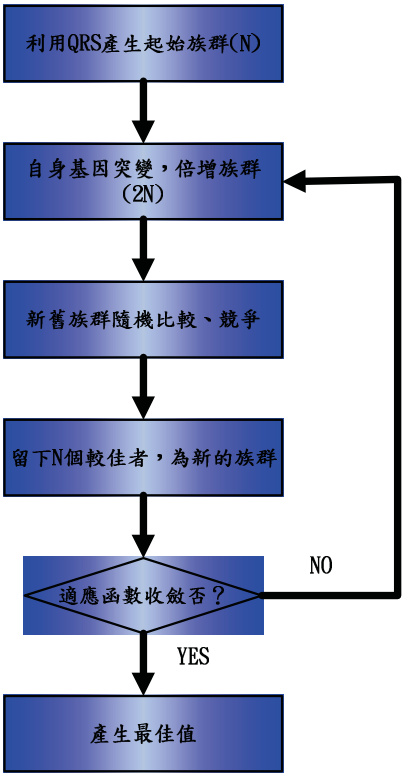

圖 2： EP 進化演算法之流程圖。

因此利用上述之方法，透過程式的寫作，即可順利求得最佳之 kp 值與 ki 值，並使 Master-Slave 之 Sprott 混沌系統達到同步，

2.2 RSA 加解密原理

RSA 係屬非對稱加密演算碼(Asymmetric algorithm)[5-6]，其主要特徵如下：資料加密與資料解密使用不同的金鑰，以公開金鑰(Public key)加密，以私密金鑰(Private key)解密，以公開金鑰(Public key)產生密碼，公開金鑰公諸於大眾，私密金鑰則由個人自行保存，兩個金鑰彼此配對使用，稱為「金鑰對」(Key pair)。

RSA 加解密原理步驟：

(1).先選取任意選擇兩個大質數 p 及 q 。
(2).計算 $r = p \times q$ ，r 定義為模。
(3).計算歐拉函數 $\phi(r) = (p-1) \times (q-1)$ 。
(4).選擇一整數 PK ，使得 $GOD(PK, \phi(r)) = 1$ 。
(5).利用算式 $PK \times SK = 1 (\mathrm{mod}\, \phi(r))$ 計算出 SK 。
(6).(PK, r) 定義為公開金鑰，$(SK, \phi(r))$ 定義為私密金鑰。
(7).限定明文 M 值範圍從 0 到 $r-1$，利用加密公式 $C = M^{PK} \bmod r$ 計算出密文。
(8).密文 C 則可利用解密公式 $M = C^{SK} \bmod r$ 計算出明文 M 。

在 RSA 加密原理加密的過程中，是使用區塊加密法，亦即當使用者要傳送訊息給某人時；將訊息分成數個區塊，且區塊大小比 r 的值要小。而本作品主要利用 RSA 加解密的觀念，以混沌訊號非線性且類似隨機的特性做為動態金鑰選擇之依據，來做為加解密的應用。下列圖示為應用混沌訊號選擇模組合 r 及 PK 值之示意圖：

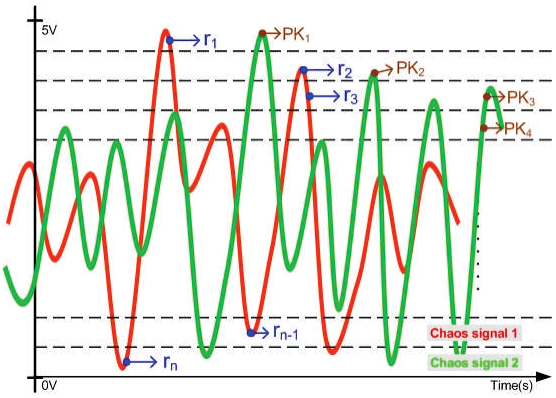

圖 3： r 與 PK 選擇示意圖

圖 3 中紅線為混沌系統其一混沌訊號，將混沌訊號 AD 轉換後之數位資料分割成 n 等分，每個部分代表不同的 $r = p \times q$ (p 、q 為自定義，目的為避免值過小或過大)，因此當訊號落在不同的電壓位準，也代表著更換模組合；而綠線為混沌系統另一混沌訊號，同樣的將混沌訊號 AD 轉換後之資料分割成 n 等份，且每個區間分別代表不同的 PK 值，因此兩種不同的混沌訊號，隨機的選擇模組合與 PK 值，同時也會直接影響 $\phi(r)$ 及 SK 產生的值，如此即可將欲傳送之資料 M 利用原理步驟 7 加密公式來加密，接收端亦可計算出 SK 並利用原理步驟 8 公式來解密，藉此動態選擇金鑰及模組合我們稱之為「動態金鑰產生器」。

3. 作品結構

本作品之系統結構方塊圖如圖 4 所示，圖 4 中左方為傳送端，右方接收端；首先將混沌系統之 x_2 及 x_3 訊號透過盛群 HT46R24 的 A/D 轉換介面轉換為數位資料，由於 A/D 轉換模組之

解析度為 10 個 bits，因此可利用 x_2 及 x_3 混沌訊號的 LSB 4bits 合成一組為 1 byte 的 Random Key，接著利用前述工作原理所提出之結合混沌之 RSA 加密方式，選擇出一組 r 與 PK 值將 Random Key 加密，並且利用此 Random Key 將欲傳送之語音數位資料加密；而接收端之僕混沌系統在接收到主混沌系統之 x_1 同步訊號後會隨即建構出所有同步響應狀態，此時由於接收端之混沌訊號已經與傳送端同步，因此也代表著接收端可以選擇出與傳送端一致的 r 與 PK 值，進一步可以求出正確的 SK 值並利用前述 RSA 解密方法將 Random Key 解出，以解出正確的語音數位資料。

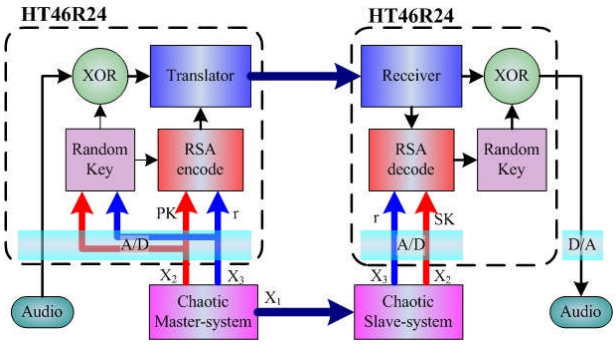

圖 4： 系統結構方塊圖

3.1 硬體部分

本作品所採用的混沌系統為 Sprott 電路[7]，其 Master-Slave 系統表示如下：

Master Sprott 方程式：

$$\dot{x}_{m1} = x_{m2}$$
$$\dot{x}_{m2} = x_{m3}$$
$$\dot{x}_{m3} = -1.2x_{m1} - x_{m2} - 0.6x_{m3} + 2sign(x_{m1})$$
$$y_m = x_{m1}$$

Slave Sprott 方程式：

$$\dot{x}_{s1} = x_{s2}$$
$$\dot{x}_{s2} = x_{s3} + u$$
$$\dot{x}_{s3} = -1.2x_{s1} - x_{s2} - 0.6x_{s3} + 2sign(x_{s1})$$
$$y_s = x_{s1}$$

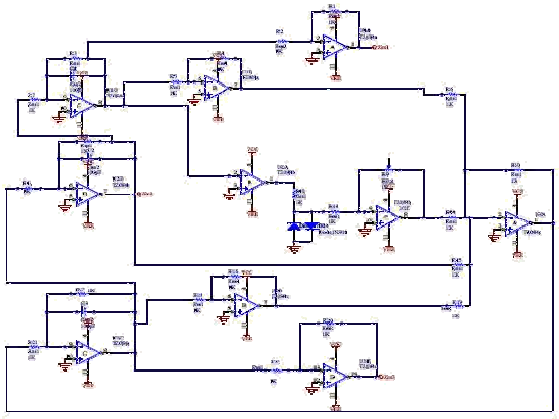

圖 5： Master Sprott 電路圖。

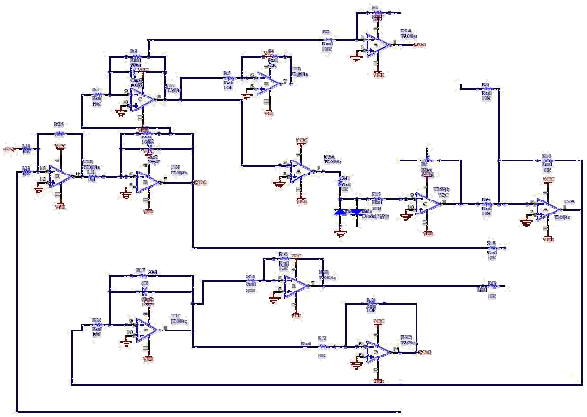

圖 6： Slave Sprott 電路圖。

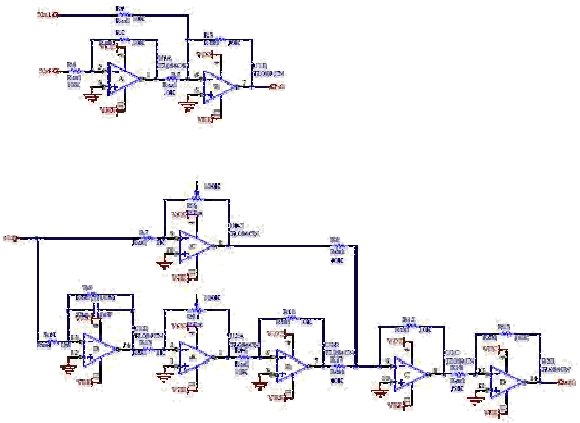

圖 7： PI 控制器電路圖。

其中 x_{m1}, x_{m2}, x_{m3} 為 Master 端之混沌狀態，x_{s1}, x_{s2}, x_{s3} 為 Slave 端之混沌狀態，y_m, y_s 分別為 Master 與 Slave 之輸出，u 為此 Master-Slave 系統所應用之 PI 控制器。故上述方程式可利用 OP 運算放大器、電容及電阻等元件加以實現出來，如圖 5、圖 6 及圖 7 所示。

3.2 軟體部分

在軟體的部分，由於 RSA 運算中包含大量的冪次以及取餘數運算，因此為了能夠做到即時傳輸語音的功能，本作品定義了資料訊框(Data Frame)，目的就是為了解決即時傳送的問題，其方塊圖如下：

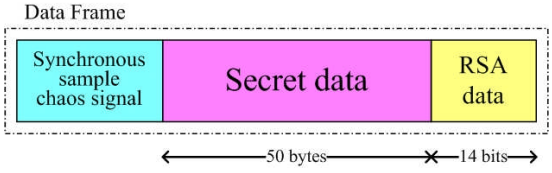

圖 8： 資料訊框

由於混沌系統是一種動態的非線性系統，為了能使傳送與接收兩端都能更正確的選擇 r 及 PK 值，因此必需讓兩端能在同一時間點對混沌訊號作 AD 取樣，所以每筆訊框皆是以混沌取樣做為開始，如此即可得到一組 r 及 PK 值，以及一組由 x_2 及 x_3 混沌訊號的 LSB 4bits 所合成的 Random Key，並開始執行 RSA 運算。

在 RSA 運算期間，本作品利用 AD 轉換時所需要的 Sample time 來做運算，並利用 AD 中斷函式，將每筆語音資料加密並加以傳送，因此系統會一直做 RSA 運算，直到語音取樣完成後便會自動跳到 AD 中斷函式將資料加密並傳送，接著傳送完後會繼續回到主程式做 RSA 運算，因此資料訊框定義了 50 bytes 目的是要能足夠 RSA 運算完成，在資料訊框最後則是將運算完成的 RSA 加密資料加以傳送。

另外值得注意的是，在利用混沌訊號選擇 r 及 PK 值時，由於不同的 IC 不同的 AD 轉換模組，以及混沌系統同步之間微小的誤差，都可能造成 MCU 在選擇時產生錯誤，尤其是當訊號處在的臨界值附近時，最容易產生錯誤，因此為了使系統能更穩定且正確的選擇，在傳送 RSA 加密資料的最後，多傳送一組參考位元：

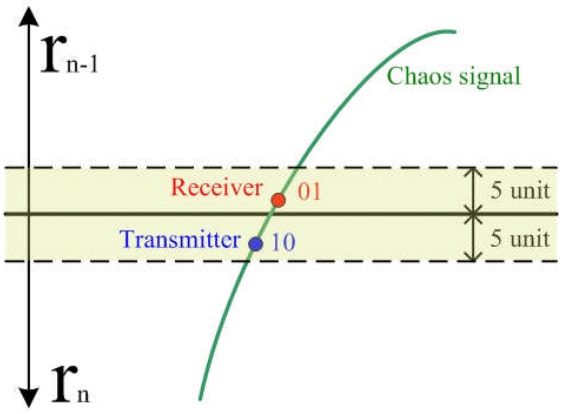

圖 9： 臨界值緩衝區示意圖

如圖 9 所示，假設圖 9 中綠線為一混沌訊號，藍點為傳送端取樣後所在位置，紅點為接收端取樣後所在位置，兩端因為微小的誤差造成選擇 r 錯誤，因此本作品設計臨界值緩衝區，如上圖所示傳送端若是處在臨界值較低處則在訊框最後傳送 10，而接收端在接收到 10 後，會因為本身取樣點處在臨界值較高處，得知與傳送端不一致，因此可強制令 r 選擇正確的值，反之，若是傳送端傳送 01 則表示傳送端目前處在臨界值較高處，因此接收端若是處在較低處也就是 10 則亦可強制切換到正確的 r 值區間。

本作品能做到語音即時傳送，最重要的一環就是接收端 SRAM 的分頁資料處理功能。由前述可得知，Random Key 要能正確的傳送到接收端，至少必需經過加密、傳送、與解密三個階段，而在解出 Random Key 後還必需將語音資料解密，因此將資料處理分成三個階段，首先接收端接收第一筆資料訊框編號為 1，且將 Secret data 1(加密資料)儲存在 SRAM page 1，接著由於已經接收了 RSA 資料，因此接收端會開始計算 RSA data 1，且傳送端每隔一個 AD Sample time 就會傳送一筆 Secret data，所以接收端會將資料先儲存在 SRAM page 2，如前述所說明，傳送端加密資料傳送 50 bytes 已經足夠 RSA 運算，因此接收端同樣的也足夠 RSA 運算，因此要接收第三筆資料訊框時同樣的將 Secret data 儲存在 SRAM page 3，同樣的在運算 RSA data 2，但是由於 RSA data 1 在第二資料訊框結束時已解出 Random Key，所以在接收第三資料訊框同時，也利用解出的 Random Key 將 Secret data 1 解密，依此類推，將 SRAM 分成三個 page 不斷的循環即可完成階段式的 RSA 資料運算以及資料解密等動作，製作出本作品語音即時傳送的功能。SRAM 分頁處理方塊圖，如圖 10 所示。

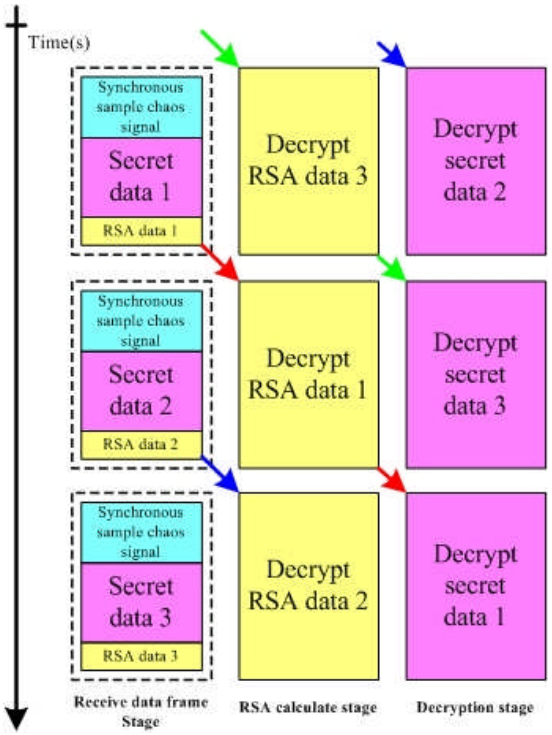

圖 10： SRAM 分頁處理方塊圖

本作品之程式流程圖大致如圖 11 及 12 所示：

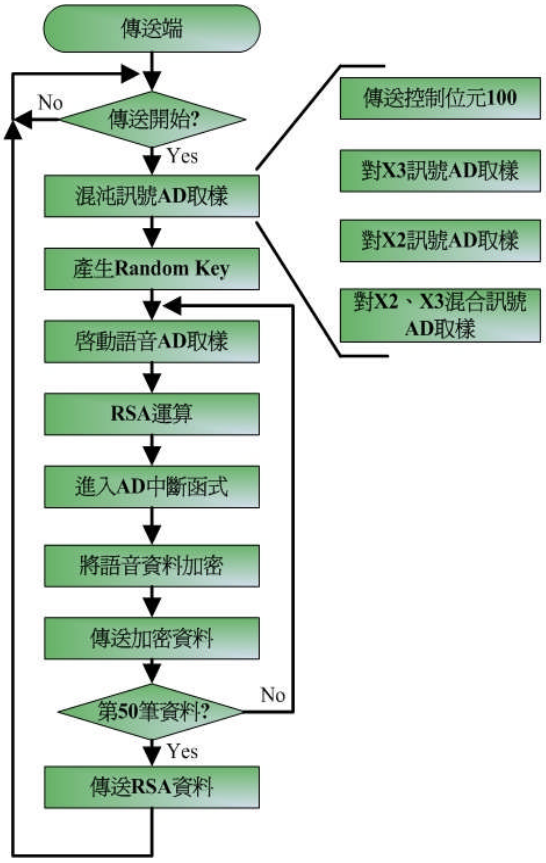

圖 11： 傳送端程式流程圖。

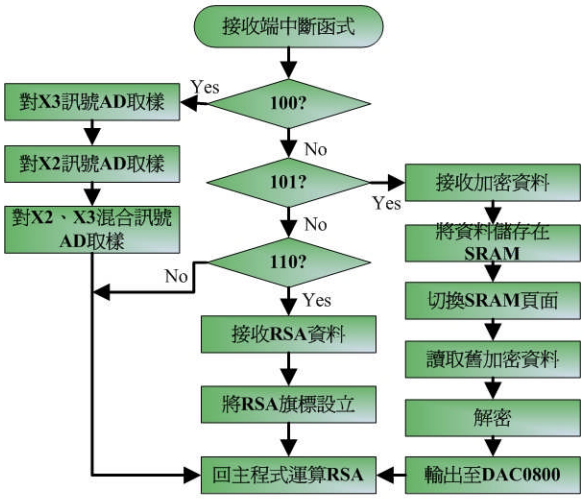

圖 12： 接收端程式流程圖。

4. 系統測試方法及結果

圖 13 及圖 14 為本作品混沌實體電路，首先將電源起動後，先測量主混沌系統是否有產生混沌訊號，如有訊號產生，則將主混沌系統之 x_1 訊號接至僕混沌系統之 PI 控制器，並測量主僕混沌系統之 x_2 及 x_3 是否有同步，如下圖所示，其中橙色線為 Master 端，青色線為 Slave 端：

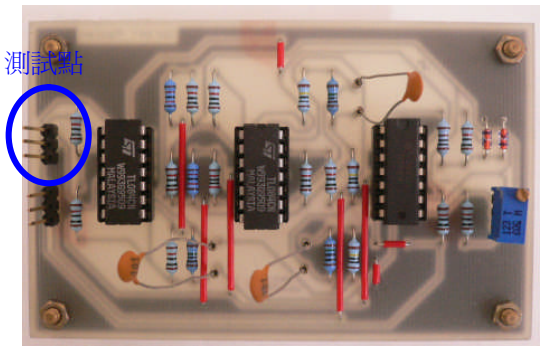

圖 13： 主混沌系統實體電路。

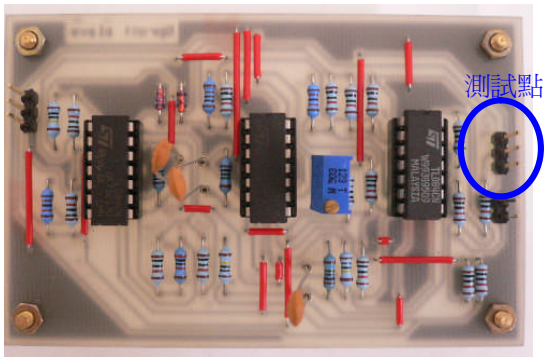

圖 14： 僕混沌系統實體電路。

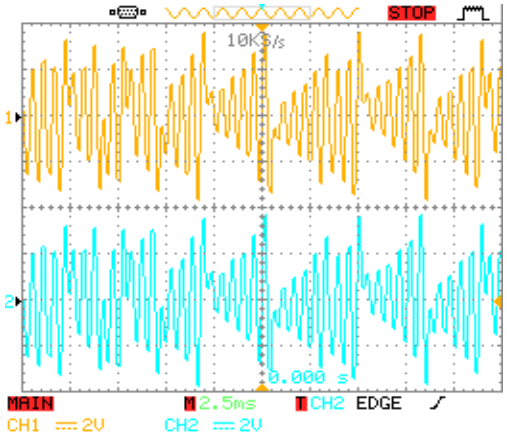

圖 15： Master-Slave x_2 訊號同步圖。

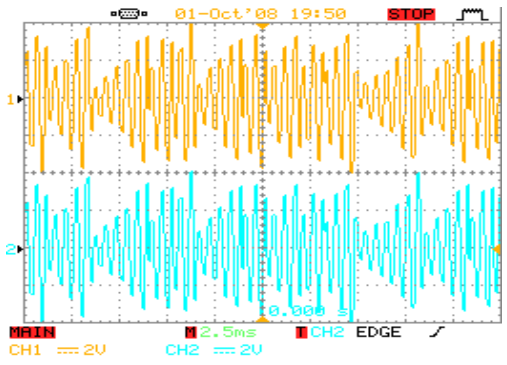

圖 16： Master-Slave x_3 訊號同步圖。

確定兩端之混沌系統已達成同步後，將 x_2 及 x_3 訊號輸入至 MCU 電路之混沌訊號輸入點，即可按下傳送按鈕開始傳送，其加密前語音訊號與解密後之語音訊號如圖 18 所示，橙色線為加密前語音訊號，青色線為解密後之語音訊號。

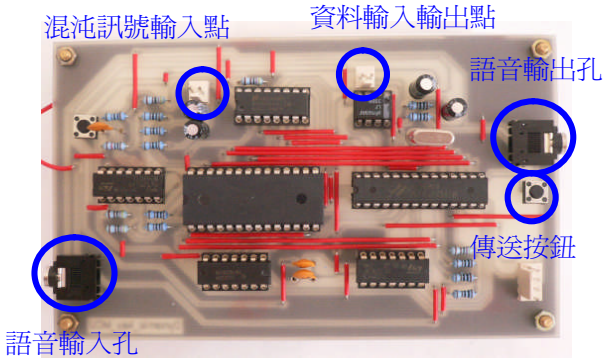

圖 17： MCU 實體電路圖。

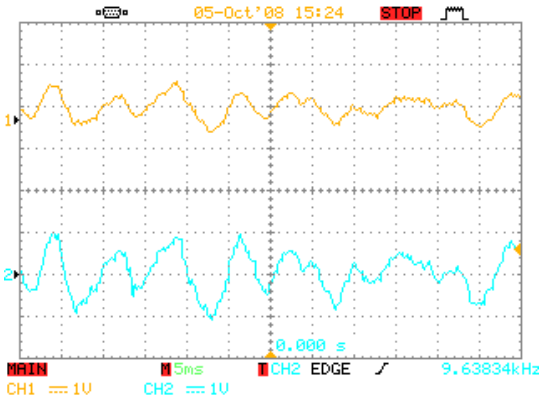

圖 18： 語音加密前與解密後訊號量測圖。

5. 參考文獻

[1] 郭俊驛，以 Chaotic Shift Keying (CSK)為基礎之混沌數位保密通訊系統製作，2007，第三屆盛群盃 HOLTEK MCU 創意大賽複賽報告。

[2] Fogel, D. B., Evolutionary Computation: Toward a New Philosophy of Machine Intelligence, John Wiley and Sons, New York, USA. 1995.

[3] Wei-Der chang and Jun-Juh Yan, “Optimum Setting of PID Controllers Based on Using Evolutionary Programming Algorithm” , Joumal of the Chinese Lnstitute of Engineers, vol. 27, no. 3, pp.439-442,2004.

[4] Hao Zhang , Xi-Kui Ma , Wei-Zeng Liu, “Synchronization of chaotic systems with parametric uncertainty using active sliding mode control”, Chaos , Solitons and Fractals, vol.21, pp. 1249-1257, 2004.

[5] 賴威志，洪莊榮，潘冠文，周宛靖，RSA 加密演算法, **http://oasis.csie.ntu.edu.tw/2006_fall_network/slides/7**

[6] 朱榮祿，洪志遠，林宴弘，RSA 加解密系統及其單晶片實現, **吳鳳技術學院 保全管理學系.**

[7] D.I.R. Almeida, J. Alvarez, J. G. Barajas, Robust synchronization of Sprott circuits using sliding mode control, Chaos, Solitons & Fractals, 30(2006):11-18.

[8] 李文昌，HT46 系列微控制器理論與實習 C 語言版，宏友圖書開發股份有限公司。

[9] HT-IDE3000 使用手冊，盛群半導體股份有限公司。

[10] HT46R232/HT46C232 A/D Type 8-bits MCU, 盛群半導體股份有限公司。